UNIVERSITY OF HERTFORDSHIRE SCHOOL OF COMPUTER SCIENCE.

“Near Real-Time, Semi-Automated Threat Assessment of Information Environments”

A thesis submitted to the University of Hertfordshire
in partial fulfilment of the requirements of the degree of

Doctor of Philosophy

May 2022

Supervisors:

Dr Stilianos Vidalis.

Dr Andrew Jones.

Dr Catherine Menon.

Author: Gaurav

University of Hertfordshire.

Abstract

Centre for Computer Science and Informatics Research (CCSIR)
School of Computer Science.
Doctor of Philosophy.
By Gaurav

Threat assessment is a crucial process for monitoring and defending against potential threats in an organization's information environment and business operations. Ensuring the security of information infrastructure requires effective information security practices. However, existing models and methodologies often fall short of addressing the dynamic and evolving nature of cyberattacks. Moreover, critical threat intelligence extracted from the threat agents lacks the ability to capture essential attributes such as motivation, opportunity, and capability (M, O, C).

This contribution to knowledge clarification introduces a semi-automatic threat assessment model that can handle situational awareness data or live acquired data stream from networks, incorporating information security techniques, protocols, and real-time monitoring of specific network types. Additionally, it focuses on analysing and implementing network traffic within a specific real-time information environment.

To develop the semi-automatic threat assessment model, the study identifies unique attributes of threat agents by analysing Packet Capture Application Programming Interface (PCAP) files and data stream collected between 2012 and 2019. The study utilizes both hypothetical and real-world examples of threat agents to evaluate the three key factors: motivation, opportunity, and capability. This evaluation serves as a basis for designing threat profiles, critical threat intelligence, and assessing the complexity of process. These aspects are currently overlooked in existing threat agent taxonomies, models, and methodologies.

By addressing the limitations of traditional threat assessment approaches, this research contributes to advancing the field of cybersecurity. The proposed semi-automatic threat assessment model offers improved awareness and timely detection of threats, providing organizations with a more robust defence against evolving cyberattacks. This research enhances the understanding of threat agents' attributes and assists in developing proactive strategies to mitigate the risks associated with cybersecurity in the modern information environment.

Acknowledgements.

First, my gratitude goes to the University of Hertfordshire for providing the infrastructure and opportunity for my PhD and allowing me to start a career in academia. I would like to thank my primary supervisor and research mentor, Dr Stilianos Vidalis, for the support of my PhD and related research. I am grateful for his commitment to providing me with guidance even late in the evening or on weekends. His broad knowledge and his patience were a massive help throughout the whole of the PhD.

Further, I would like to express my gratitude to Dr Andrew Jones and Dr Catherine Menon, my secondary supervisor, for their valuable inputs and support. My thanks also go to Dr Raimund Kerner, Research leader of the University of Hertfordshire research group, for his invaluable feedback and suggestions. I thank Anuja for her patience and her interest in abstract topics that are not hers. Her cheerful and supportive attitude was a big help throughout this project, and I am ever grateful to her for leading me onto this path. Her hilarious personifications of certain aspects of my work, complete with pictures and all, is only one of many examples of her brilliant way of supporting me.

Although I do not know these people personally, I want to give a shout out to Paul Gruba and David Evans for his book " How to Write a Better Thesis", showing that complicated things can be explained with only words, sentences, paragraphs, and chapters etc., and Barbara Kamler and Pat Thomson, for book "Helping Doctoral Students", advocating the fact that research is not as tricky as common belief suggests and that it can be taught to anyone.

Last but not least, I want to thank my family and friends from abroad for their continuous support and their willingness to visit us regularly.

List of Research Paper Publication

Journals: (PhD Publications)

1) "Analysis and Implementation of Threat Agents Profiles in Semi-Automated manner for a Network Traffic in Real-Time Information Environment" was published in Electronics Journal of Cybersecurity and Data Science Volume 10, Issue 15, July 2021. **(Indexes: SCI (Science Citation Index), Impact Factor-2.397)**
2) "Analysis and Implementation of Semi-Automatic Model for Vulnerability Exploitations of Threat Agents in NIST Databases" was published in the Springer Editorial System for Journal of Multimedia Tools and Applications Volume 12, Issue 23, November 2022. **(Indexes: SCI (Science Citation Index) Impact Factor-4.438)**
3) "A Survey on Layer-wise Security attacks in IoT: Attacks, Countermeasures, and Open-Issues." was published in Electronics Journal of Ambient Intelligence in IoT Environments Volume 10, Issue 31, September 2021. **(Indexes: SCI (Science Citation Index), Impact Factor-2.397)**

Conferences:(PhD Publications)

4) "Study and Analysis of Threat Assessment Model and Methodology in Real-Time Informational Environment "was published at IEEE Bombay Section Signature Conference (IBSSC 2021) in Gwalior, India. **(Indexes: Scopus, Impact Factor-6.397)**
5) "Killing Your Device via Your USB Port" was published at International Symposium on Human Aspects of Information Security & Assurance (H.A.I.S.A. 2019) in Nicosia, Cyprus. **(Springer Conferences).**

Patent's :(PhD Publications)

6) A patent is under processing on "Threat Assessment Model of Network in Next to Real-Time Environment"(**Office of the Controller General of Patents, Design & Trademark Department for the Promotion of Industry Trade Ministry of Commerce & Industry, Government of India**).

Journals:(Other Publication During PhD)

7) "Enhanced Reliable Reactive Routing (ER3) Protocol for Multimedia Application in 3D Wireless Sensor Networks" was published in Springer Journal of Multimedia Tools and Applications - Springer Transaction manuscript number is- MTAD-D-17-00032R1 in September 2017. **(Indexes: SCI (Science Citation Index) Impact Factor-2.313)**
8) "Automated Passive Income from Stock Market Using Machine Learning and Big Data Analytics with Security Aspects." is communicated in the Wiley Online Library for the

Journal of Concurrency and Computation: Practice and Experience (CCPE). **(Indexes: SCI (Science Citation Index) Impact Factor-1.536)**

Patent's:(Other Publication During PhD)

9) A patent is communicated in India on "Neural Network-Based Emergency Medical Service System Integrated with ARIMA Model for Forecasting"(**Application No. 202221006822**).

Contents.

Lists of Figures.

List of Tables.

Chapter – 1 Introduction

1.1 The Problem

"Security is about the protection of assets. This definition implies that you must know your assets and their value" (Gollmann, 2010). In today's ever-changing interconnected world, where corporate mergers and dominance prevail, understanding one's assets has become a complex problem that demands both time and expert knowledge. Cybersecurity plays a critical role in safeguarding computer systems and network's confidentiality, integrity, and availability. In the age of information technology, organizations often struggle to fully comprehend the nature, attributes, and behaviour of threat agents that could potentially target their assets. The challenge lies in providing companies or organizations with a secure environment that enables them to effectively counter threat agent attacks without depleting all system resources. This is where risk assessment methods or models come into play (Boban, 2010); (Tevis and Hamilton Jr, 2006), recognizing the need to perform multiple threat assessments for identifying and analysing various threats in the contemporary information environment, ensuring the security of organizations and their network processes becomes paramount. The continuous iteration of threat assessment processes plays a crucial role in mitigating risks within the modern information environment. However, conducting effective threat assessments is hindered by resource limitations, complexity, and the vast amount of data in the current semi-automated threat assessment information environment, driven by socially derived knowledge and virtual computing.

This doctoral thesis aims to address the research gap within today's "information ecosystems," which encompass extensive and diverse infrastructures containing data from various sensors. To enable analysis and decision-making support, tools should offer real-time comprehension of situation awareness and threat assessments, acting as a solution for handling the vast volume of data in such environments. The thesis will delve into state-of-the-art threat agent analysis models and methodologies while addressing procedural and technological challenges through the application of significant data analytics principles.

To conduct these threat assessments, the author must gather various types of data, such as IDS (intrusion detection system) and PCAP (packet capture) files. However, the diverse

range of criteria associated with threat agents presents a significant challenge when it comes to analysing them. It becomes a massive undertaking because of the sheer variety of factors that need to be considered and evaluated during the analysis process. According to various studies (Bloom, 1970; Icove, Seger and VonStorch, 1996; Kabay, 1996; Blyth and Kovacich, 2001; A Jones, 2002; Andy Jones, 2002; Morakis, Vidalis and Blyth, 2003; Vidalis and Jones, 2003; Baker and Prasanna, 2004; Goel, Pon and Menzies, 2006; Scholand et al., 2007; Kaufman, 2009; Gollmann, 2010; Khandekar et al., 2010; Sesia, Toufik and Baker, 2011; Clancy, 2011; Damnjanovic et al., 2011; Ghanem et al., 2012; Lichtman et al., 2013; Cao et al., 2013; Matthews and Matthews, 2014; Lessler et al., 2016; Marcellino et al., 2017; Rao et al., 2017) on the modern threat assessments models, the author objective is to identify and analyse multiple threat agents and the associated threats faced by different types of wireless and wired network channels. The aim of the PhD is to develop a novel model that can effectively identify and analyse the number and types of threat agents in the modern information environment. A key characteristic of this new model should be its ability to address security concerns related to tampering, information disclosure, spoofing, denial of service, repudiation, and elevation of privilege within the contemporary information environment.

Furthermore, the nature of small businesses lies in their agility and ability to embrace and adapt to changes more quickly than larger businesses (Gamble et al., 2020). More swiftly than large enterprises, small business sectors are transforming their industries (Fresner et al., 2017). Small companies embrace IoT (internet of things) and electronic commerce (e-commerce) to leverage their limited resources and expand their customer base (Yu and Zhang, 2017).

Small enterprises have achieved remarkable success through the utilization of information technology. The majority of companies in today's business landscape fall into the category of small and medium-sized enterprises (SMEs). To facilitate government support programmes tailored specifically for small businesses and enable access to financing opportunities, it becomes essential to clearly understand what constitutes an SME. This includes various types of companies such as contractors, internet merchants, freelancers, independent contractors, and self-employed individuals.

By establishing this understanding, other small businesses can be motivated to adopt real-world threat assessment practices and information technology associated with e-commerce. This would contribute to enhancing their security measures and adopting effective strategies to mitigate risks in the rapidly evolving digital landscape.

According to the Oxford Dictionary (Matthews and Matthews, 2014), threats can be defined as:-

"A statement of an intention to inflict pain, injury, damage, or other hostile action on someone in retribution for something is done or not done."

But on the other hand, according to the Federal Information Processing Standards (FIPS)

"Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability".

According to (Goel, Pon and Menzies, 2006), a threat to a system can also be defined as:

"A circumstance or event that has the potential to cause harm by violating security."

Indeed, cybersecurity poses a significant challenge for digital businesses, including small enterprises. On the one hand, small businesses often lack the financial resources and established infrastructure to allocate budgets for dedicated security personnel or the latest technologies capable of effectively mitigating cyberattacks. Consequently, they face an elevated risk of falling victim to security breaches and threats. Real-time threat assessments have revealed that small businesses frequently operate with a limited number of employees, particularly during the start-up phase. This constraint further restricts their ability to hire a dedicated security professional to manage and address the risks present in the dynamic and semi-automated informational environment they operate in.

Given these circumstances, it becomes crucial for small businesses to explore alternative strategies and cost-effective solutions to enhance their cybersecurity posture. Collaborative efforts, leveraging outsourced security services, and implementing robust security practices

within the limitations of available resources are some potential avenues for mitigating risks and protecting their digital assets (Goel, Pon and Menzies, 2006). At the same time, studies have consistently shown that small businesses or industries are more susceptible to cybercrime than are their larger counterparts. This heightened vulnerability can be attributed, in part, to the scarcity of cybersecurity professionals available to small businesses. The limited availability of skilled cybersecurity personnel poses challenges for small businesses in establishing robust security measures and effectively defending against cyber threats.

Consequently, small businesses become attractive targets for cybercriminals who perceive them as more accessible and potentially more lucrative victims. The theft of data and information through cybercrime incidents can disproportionately impact small businesses because of their limited resources and capacity to recover from such incidents.

To address this disparity, small businesses should explore alternative approaches to bolster their cybersecurity posture. This includes leveraging cost-effective security solutions, implementing robust security practices, and investing in employee training on cybersecurity awareness and best practices. Seeking guidance from external cybersecurity service providers or collaborating with industry associations and government initiatives that support small businesses in enhancing their cybersecurity defences can also be beneficial.

Additionally, raising awareness about the importance of cybersecurity and fostering a culture of security within the small business community can contribute to mitigating the risks associated with cybercrime (Kabay, 1996). It is a concerning reality that those who are less capable of protecting themselves from cyberattacks or cybercrime, such as small businesses or industries, tend to be victimized more frequently. The consequences of such attacks can be severe, resulting in significant losses for the affected companies or organizations.

The potential impact of information or computer-based cybercrime is indeed disastrous. It can lead to business or organizational failures, financial liabilities, and even personal liabilities for the individuals involved in running those organizations. The loss of critical data, intellectual property theft, disruption of operations, damage to reputation, and financial repercussions can devastate small businesses.

To mitigate these risks, it is crucial for small businesses to recognize the importance of prioritizing cybersecurity and taking proactive measures to protect their systems and data. Implementing robust security measures, investing in employee training, regularly updating and patching software systems, and staying informed about the evolving threat landscape are all essential steps in safeguarding against cyberattacks.

Moreover, seeking professional assistance, collaborating with cybersecurity service providers, and staying abreast of industry best practices can significantly enhance a small business's ability to defend against cyber threats and minimize the potential for business failure, financial liabilities, and personal liabilities (Kabay, 1996). Studies show that the average spending or loss is about ten times bigger when a computer is used than when any cybercrime is committed without it (Pandelică, 2020). These problems resulting from the vulnerabilities associated with computer-based crimes, including cyberattacks, are expected to worsen before they improve, as observed by cybersecurity practitioners and experts. The ever-evolving nature of technology and the increasing sophistication of cyber threats contribute to this trend.

A recent example highlighting this relationship is the distributed denial of service (DDoS) attacks executed on multiple e-commerce and web-based businesses. DDoS attacks involve overwhelming a target system with a flood of traffic, rendering it inaccessible to legitimate users. These attacks can cause significant disruptions, financial losses, and damage to affected businesses' reputations. As technology advances, cybercriminals continually adapt their tactics, techniques, and procedures, making it challenging to eliminate cyber threats entirely. The expanding attack surface resulting from the growing connectivity of devices and the increasing reliance on digital infrastructure further exacerbates the issue.

To address this situation, it is crucial for businesses and organizations to continuously invest in robust cyber defences, stay updated on emerging threats, and adopt proactive security measures. Collaboration between industry stakeholders, sharing threat intelligence, and implementing effective incident response plans are essential for combating cyberattacks and minimizing their impact. Ultimately, while the challenges posed by computer-based crimes may continue to grow, a proactive and holistic approach to cybersecurity can help mitigate risks and protect businesses and organizations from potential harm (Salim, Rathore, and Park,

2020). The use of technologies characterizes the pursuit of information security, policies, procedures, and operational practices to maintain the desired level of confidentiality, integrity, and availability of information systems and assets (Kaufman, 2009). The critical information infrastructure encompasses all components of real-world information technology within the comprehensive framework of a country or nation's organization. While some of these elements are owned by government entities, a significant proportion belong to the industrial sector and other non-governmental organizations. As a result, the responsibility for safeguarding the security of these tangible information assets against cyberattacks or threats is diffused across various entities within the country or nation.

This diffusion of responsibility can introduce complexities and challenges in ensuring comprehensive security measures. To address this, many countries have established and enforced regulatory structures that govern and guide organizations in protecting their critical information infrastructure. These regulations aim to develop a framework for organizations to follow in implementing security measures, risk management practices, incident response protocols, and compliance requirements.

By imposing regulatory obligations, governments seek to promote a higher level of security awareness and accountability among organizations. These regulations often include specific requirements, such as maintaining updated security protocols, conducting regular risk assessments, implementing incident response plans, and adhering to industry-specific standards or frameworks. The enforcement of regulatory structures helps create a more coordinated and standardized approach to protecting critical information infrastructure across the country or nation. It fosters a culture of cybersecurity and emphasizes the importance of safeguarding information assets from potential threats.

While regulatory structures may introduce additional compliance obligations for organizations, they play a vital role in establishing a baseline of security practices and mitigating the risks associated with cyber threats to the critical information infrastructure (Kaufman, 2009). The challenge of ensuring real-world information security in the current context is significant. The increasing interconnectivity of businesses within organizations and their interactions with customers, sellers, vendors, contractors, subcontractors, and even competitors brings both opportunities and risks. The growing reliance on new technologies

and information systems, driven by high demands, further amplifies the need for robust security measures.

To remain competitive in today's market, organizations must focus on enhancing functionality and prioritizing security. However, each connection made to external entities introduces potential vulnerabilities to systems. Cybercriminals, terrorists, hackers, and even foreign government's security organizations and military forces can exploit these vulnerabilities to compromise the security of the organization's information assets. It is crucial for organizations to adopt a comprehensive and proactive approach to address these challenges. This includes implementing robust cybersecurity measures such as the following:

a) Conducting regular security assessments and risk analyses to identify vulnerabilities and develop appropriate mitigation strategies
b) Implementing strong access controls and authentication mechanisms to ensure only authorized individuals have access to critical systems and information
c) Encrypting sensitive data in transit and at rest to protect against unauthorized access or interception
d) Implementing intrusion detection and prevention systems to monitor network traffic and detect suspicious activities
e) Training employees on cybersecurity best practices and promoting a culture of security awareness within the organization
f) Establishing incident response plans to effectively and swiftly respond to security incidents and minimize their impact

Collaboration and information sharing between organizations, industry sectors, and government entities also plays a crucial role in addressing the evolving security landscape. By working together, sharing threat intelligence, and implementing industry best practices, organizations can enhance their overall security posture and mitigate the risks posed by various threat actors. Ultimately, prioritizing both security and functionality is essential for organizations to navigate the challenges of the real-time informational environment and remain competitive while safeguarding their critical information assets (Kaufman, 2009). The risk of successful theft, misappropriation, or destruction of valuable real-time threat assessment information assets by insider intruders is also on the rise. The increased

connectivity and reliance on technology in the modern informational environment create new avenues for potential insider threats. Insider threats refers to individuals who have authorized access to an organization's systems, data, or facilities and misuse that access for malicious purposes. These insiders may include employees, contractors, or other trusted individuals with privileged access to sensitive information.

As technical education in threat assessment of informational environments becomes more critical, organizations face challenges in adequately preparing their workforce to understand and mitigate these risks. The evolving nature of cyber threats and the complex landscape of information systems require specialized knowledge and skills to effectively assess and address potential risks. To tackle these challenges, organizations should consider implementing the following measures:

- **Comprehensive security training:** Provide employees with regular and up-to-date training on cybersecurity best practices, emphasizing the importance of protecting sensitive information and identifying potential insider threats.
- **Access control and monitoring:** Implement stringent access controls and monitoring mechanisms to ensure that individuals only have access to the information necessary for their job roles. Regularly review and audit access privileges to prevent unauthorized access.
- **Incident response and reporting:** Establish clear protocols for reporting and responding to security incidents, including suspicious activities by insiders. Encourage a culture of reporting any potential concerns or anomalies observed within the organization.
- **Continuous monitoring and auditing:** Regularly monitor and audit system logs, network traffic, and user activities to detect any unusual behaviour or unauthorized access attempts. Implement technologies and tools that provide real-time alerts and threat intelligence to proactively identify insider threats.
- **Insider threat Programmes:** Develop and implement formal insider threat programmes that involve cross-functional collaboration between HR, IT, and security departments. These programmes should focus on early detection, prevention, and response to insider threats.

By prioritizing technical education in threat assessment, organizations can better equip their employees with the knowledge and skills needed to understand and address the growing risks associated with insider threats in the modern informational environment (Longhurst et al., 2020). Securing computer network systems and communication links between hosts and clients is indeed a challenging and essential task. The computer systems and networks utilized by industry, businesses, and government-owned organizations often rely on commercial products. However, these products were not originally designed with security as their primary focus, which can lead to numerous flaws and weaknesses in real-time threat assessments of informational environments.

It is crucial to recognize that security cannot be an afterthought in the design and implementation of computer systems and networks. Organizations need to prioritize security considerations from the outset and implement appropriate measures to protect their networks and sensitive information. One of the highlighted issues is the lack of automated and time-efficient network threat and vulnerability assessments using current models or techniques. Traditional methods of conducting threat and vulnerability assessments often involve manual processes, which can be time-consuming and prone to human error. As the threat landscape evolves rapidly, organizations need more efficient ways to assess and address vulnerabilities to stay ahead of potential attackers.

Organizations can explore and adopt advanced techniques and technologies for automated threat and vulnerability assessments to address this challenge. This may include leveraging artificial intelligence (AI) and data analytics to analyse network traffic, identify potential vulnerabilities, and assess the overall security posture in real time. Additionally, organizations should stay informed about the latest security updates and patches for their commercial products. Regularly updating software, implementing security patches, and following best practices for network configuration can significantly enhance the security of computer systems and networks.

Furthermore, organizations may consider engaging with security experts or employing dedicated security professionals who can provide expertise in conducting efficient and effective threat assessments. These professionals can help implement robust security measures, perform regular assessments, and address any vulnerabilities or weaknesses

identified. By combining automated threat assessment technologies, timely software updates, and expert guidance, organizations can enhance their ability to identify and mitigate risks in real-time informational environments and improve the overall security of their computer systems and networks. (Blyth and Kovacich, 2001).

1.2 Hypothesis.

In a contemporary semi-automated information environment, this study's hypothesises that a threat agent analysis assessment model can be created to identify the threats. The twenty-first century has seen numerous concerns about security in electronics networks and information systems. The rapid increase in the number of network users and the value of their transactions has led to rapid growth in security issues. Security has now reached a critical point where it represents a prerequisite for further developing the electronics business and the functioning of the whole economy (Rao et al., 2017). The number of companies within an organization or within particular industries connected to buyers, sellers, vendors, contractors, subcontractors, and even rival contractors is expanding daily. More security and functionality is needed to remain competitive in the market of the real-time informational environment, with the customer, vendor, sub-contractor, and even competitors increasingly required to stay competitive and functional in the global economy. Yet every connection adds to the vulnerability of a systems to hackers, criminals, terrorists, and even the security organs and military forces of foreign governments. Nowadays, most of them are connected to the network because of their needs and security concerns, all using the network services. Threat agent profiling is essential for developing a comprehensive and effective cybersecurity strategy. By understanding the who, what, why, and how behind potential threats, organizations can better protect themselves, allocate resources wisely, and stay ahead of evolving cyber threats.

With the appropriate use of state-of-the-art technology and the introduction of an appropriate architecture, such as the design of footprints, it is considered possible to undertake a security threat assessment of a large number of datasets while a computer network attack is in progress (Ghanem et al., 2012). By harnessing cutting-edge technology and implementing an appropriate architectural framework, such as the creation of digital profiles of threat agents, it becomes feasible to conduct a comprehensive security threat assessment across a vast array

of datasets. These profiles, often referred to as “footprints,” represent the tangible outcomes of the initial reconnaissance phase. Footprints are the results or output of the reconnaissance phase. Footprints are used for gathering information about target systems or computer systems and the entities of the systems in them. After collecting all this information, a hacker would be able to use several tools and technologies of the network. The threat agent analysis assessment model will be developed to meet the needs of networks, especially the systems dealing with the high speed of the internet.

1.3 Objectives

This thesis aims to develop a semi-automatic threat assessment model capable of handling live data, incorporating prevailing information security strategies and monitoring protocols specific to certain network types within the real-time informational environment.

The objectives of the research work are as follows: -

1.3.1 Research Objective.

- Research on the state of the art of tools and technologies for threat assessment. Analysis of the modern information environment deduces several characteristics/attributes that must be included and measured in a threat agent analysis assessment model.
- Analysis of state of the art in threat agent analysis models & methodologies. I plan to prepare a semi-automatic model for the near real-time semi-automated threat assessment planning later to undertake a number of experiments to collect primary data regarding the performance of the models. But the objective is to identify and analyse them with the new tools and existing state-of-the-art technologies and group them into families on the basis of various threat assessment parameters.

1.3.2 Development Objective.

- In the development objective, the main aim is to develop a model that has the capability to identify the threat in the informational environment. “A threat assessment is a statement of threats related to vulnerabilities of company assets and

agents, and a statement of believed capabilities that those threat agents possess"(Sharma et al., 2022).

- Design/Implement the threat agent analysis model and determine the results by conducting a number of experiments using software tools and hardware for modern informational environment networks. One of the key development objectives is the dissemination strategy for designing and implementing a model.
- The exploitation plan will similarly address the model's limitations in the future part. The primary method is to develop a new model for the semi-automated informational environment that should identify and eliminate attacks like tampering, information disclosure, spoofing, denial of service, repudiation, elevation of privilege, etc.

1.3.3 Evaluation objective

- In the evaluation objective, the main aim is to evaluate the new model that has been developed for the analysis of threats in the information environment on the basis of a comparison with the other models, the efficiency of the model, and the existence of the output generated by the different models, etc. The comparisons will be carried out on the basis of a number of parameters and characteristics of the other models, such as impact analysis, vulnerability identification, vulnerability complexity calculation, etc. Implementing algorithms for calculating threat agent groups based on the asset attributes and evaluating the assets of the threats assessments in a semi-automated information environment will be achieved with the help of quantitative, qualitative, hybrid, and knowledge-based techniques.

1.4 Research Question

The research question for the "Near Real-Time Semi-Automated Threat Assessment of Information Environment" is that CTI (cyber threat intelligence) data-driven threat agent profiling can be used to calculate threat agents' motivation and capabilities attributes in the context of a continuous threat assessment.

Research items (raised) are as follows: -

- **Cyber threat intelligence:** Information regarding recent or upcoming attacks on an organisation is obtained through various sources known as CTI. The data is

subsequently processed, polished, and arranged in order to reduce and neutralize cybersecurity risks.

- **Profiling:** Digital profiling, which uses data obtained about activities, personality traits, and interactions on the internet to build personas for criminals used in cybercrime investigations, is employed by investigators in the cyber world, much like it is in the real world of traditional crime.
- **Motivation and capability:** Motivating cybersecurity practitioners entails educating them about the potentially devastating effects of a cyberattack on the firm and even on themselves. The term capability refers to an organization's capacity for cybersecurity, the effectiveness of its security measures, and its capacity to respond to and recover from cybersecurity threats.
- **Threat agent:** A threat agent is a scenario and approach that could unintentionally trigger a vulnerability, or the aim and strategy geared towards intentionally exploiting a vulnerability.
- **Threat assessment:** A systematic procedure for identifying, investigating, evaluating, and managing potentially dangerous or violent events is known as threat assessment.

The modern risk assessments methods or models recognize that there is a need to perform threat assessments (automatically) in order to identify/analyse various threats in the modern information environment(Longhurst et al., 2020). Concern about security and continuous threat assessments may help generate the paradox of warning about the cyber operations performed in the information environment. This thesis endeavours to identify the research gap in the (semi-automated) information environments, which consist of large heterogeneous infrastructures hosting a large amount of data collected from different platforms. Decision aid tools should understand situational awareness and critical intelligence feeds of threats in real-time informational environments to analyse or identify a solution for such an issue of a large amount of data.

In the modern knowledge-based, socially driven, virtual computing era, threat assessments are hindered by a lack of resources, complexity, and size of data. Information environments are large heterogeneous infrastructures, hosting a large amount of data collected from different types of platforms with the help of a number of tools. The purpose of the research is to introduce a novel threat analysis model that will enable us to take advantage of the vast

amount of data collected by a large number of platforms designed to identify suspicious traffic, malicious intentions, and network attacks in an automated manner.

1.5 Project Methodology

Multiple research papers are being analyzed to study various existing threat agent analysis models and the modern information environment networks. However, despite this extensive analysis, there is a lack of clear explanations for threat analysis and risk management that take into account numerous parameters of these models. The lack of clarity in these existing models has impeded the ability to fully comprehend the diverse dimensions of potential threats and their management. This dearth of understanding may hinder the development of robust strategies to safeguard critical assets and information, leaving organizations vulnerable to a multitude of risks. So, the thesis aims to design a new model with the help of a recent research methodology that clearly explains all the threat assessments perfectly. In developing a model, the author will make use of several modern research methodologies and tools such as SNORT, CRAMM, PASTA, CARROLL, SUMMER, ARIES, STRIDE, OCTAVE, VAST, etc. Also required is a knowledge of C language, XML, and python for designing pseudo-code to analyse vulnerability complexity, impact, and Threat Mitigation (Andy Jones, 2002; Morakis, Vidalis, and Blyth, 2003; Vidalis and Jones, 2003).

The model will be tested on various operating system platforms (environments). For such testing, virtual machine technology, live networks, and penetration testing are required to analyse threat assessments in an information environment. The model will also be necessary to explore some of the recent penetration testing tools and an understanding of the basic commands of Snort and Wireshark for calculating the vulnerable data (A Jones, 2002; Lessler et al., 2016; Marcellino et al., 2017).

Mathematical equations and statistics are used for calculations and comparisons with the other models in terms of complexity and efficiency to identify the threat in the informational environment. Integral mathematics may also be needed to calculate or analyse the threat in an information environment (Damnjanovic et al., 2011).

Designing the model may require several software tools and modern hardware research methodologies, such as networking protocols and various algorithms of threat assessments from a software point of view. From a hardware perspective, it may require some technology

related to the field-programmable gate array or embedded ARM processors. The complexity (especially area complexity) will be calculated with the help of hardware tools. A platform (VHDL or Verilog) may be needed to communicate between software and hardware tools (Khandekar et al., 2010; Cao et al., 2013; Lichtman et al., 2013).

In the evaluation objective, the main aim is to evaluate the new model developed to analyse threats in the information environment based on a comparison with the other models, efficiency of the model, existence of the output generated by the different models, etc. The comparisons will be carried out based on the cardinal number of a framework (parameters) and characteristics of the other models, such as impact analysis, vulnerability identification, vulnerability complexity calculation, impact analysis, and identification and complexity calculation (Icove, Seger and VonStorch, 1996; Baker and Prasanna, 2004).

The experimental set-up of the model will carry out the calculation using C, C++, and Python interpreters/compilers as software. The hardware required is two or more data collection systems: the testing set-up's cable to connect with the network, a high-speed internet connection to attract the attackers, and virtual machines (VMs) installed in a system so that more than one operating system platform can be used to collect the data for testing. The basic or recent technology that is preferably to use to do such an experiment is penetration testing and specific testing by other IDS/IPS (intrusion detection system and intrusion prevention system) algorithms as one method for analysing the performance of the model (Bloom, 1970).

Furthermore, in order to learn more about semi-automated threat assessment in an educational setting, I intend to attend as many seminars, conferences, or expert speeches as possible.(Araki et al., 1996). The list of activities carried out to design and implement the model can be assessed in a number of sub-activities, including the following:

Activity 1- Analysis of environment used by source and target machine.

The number of virtual machines deployed on the server is analysed in this activity in order to grasp the state of the art cast-off by any firm. Later, the communication channel will be examined to determine how each component of organization is used to transport information/data among them. Finally, the network's connection to the internet, i.e., the

firewall utilized to guarantee security for the enterprise, is examined. The following sub-activities will be carried out for vulnerability identification and threat analysis:

1. Identifying vulnerable network ports using fundamental penetration testing methods.
2. Identifying the road map the threat agent uses to breach the network by executing a collection of protocols.

Activity 2- Research methodologies for identifying the components and technology needed to create a semi-automatic model.

The goal of this activity is to examine and analyse existing technology utilized by a variety of models and methodologies in order to comprehend the state of the art used to accomplish them. To carry out this task, the following sub-activities will occur:

1. The existing model will be studied and analysed in the literature review phase, with the primary goal of identifying the technology employed by them and the roadmap cast-off in order to evaluate the threat agent in an organisation.
2. The next step is comprehending the various models' approaches to designing and implementing their model/methodology.
3. Identifying the current model and methods' weaknesses, advantages, and gaps is the final step. Based on the identification, building and constructing the semi-automatic model using the necessary tools and technologies would be possible. The simulated architecture will undergo validation and verification. The specifics of this activity will be discussed in chapters 2 and 3, where relevant work and research techniques are covered in depth.

Activity 3: Create and deploy the model's simulation architecture on the ESXi server.

The component of the model will be designed and implemented on the server using a number of VMs put on it in this activity. Based on the needs and gaps discovered during analysis of the current model and methods. This activity will have the following sub-activities:

1. Analysis of the number of tools for capturing the data stream on the server, i.e., information gathering. In this activity, the tool identification will be determined for the model based on the semi-automatic design requirements.
2. Determine the optimal tool for vulnerability analysis based on the semi-automatic model requirements. In this activity, I will evaluate the vulnerable port identification list of common vulnerabilities exposures (CVEs) linked with the target machine.
3. Using the CVE list, determine the threat agent's environment, attack vectors cast-off by the threat agent, prerequisites inputs, and potential output.

Activity 4: Threat assessment (evaluation)

Numerous experiments will be conducted in this activity to evaluate the model. With the aid of penetration testing phases, the simulation architectural communication channel will first be validated to assess connectivity (e.g., by running a ping command to each component). There are a number of different sub-actions that will be completed for the evaluation, including the following:

1. The PCAP file-based data gathering from the server.
2. Extracting the necessary attributes from PCAP files in order to learn more about the threat agent.
3. Running the extraction-related Python code to provide the model with a semi-automation feature.

Activity 5: Calculating the Threat agent and attributes

With the aid of a Python script, the semi-automatic model in this activity will extract the necessary attributes from the PCAP files and identify the source IP, destination IP, the protocol used, the active layer, the source port, the location of the threat agent (longitude and latitude), and the internet service provider used by the threat agent. To analyse the calculation of the threat agent attribute, numerous sub-activities are carried out, including:

1. The motivation factor is established using a probabilistic approach in order to pinpoint the threat agent's motivation for infiltrating the network.
2. The opportunity factor is identified using the fundamentals of penetration testing to determine the weak points in the environment that allow threat agents to infiltrate an organization's network.
3. A variety of parameters, including time spent on the network, the highest protocol accessed, source port targets, and the sorts of activities carried out by threat agent groups, determine the capacity factor. The specifics of the traits are covered in the results and discussion section of chapter 4.

Activity 6: Vulnerability assessment

The vulnerable port will be determined in this activity, and the list of associated CVEs will be determined using Kali Linux. The identification of the environments utilized during network penetration, attack pathways, required input, and potential output is analysed using the CVE list.

Activity 7: Mitigation of impact and threats

The impact of the threat agent on the business's assets will be determined in this activity, and mitigation strategies can be adopted or proposed to the company based on the impact and the approach used to enter the network.

1.6 Thesis Planning

According to the proposed plan, the thesis will take five years to complete, including 30 days of vacation per year. The suggested start date is **19 December 2016,** and the recommended end date is **30 November 2021**.

The thesis will be split into three work packages that span four phases. Milestones are identified and implemented in each work package section.

Phases of project/years	**Phase1**	**Phase2**	**Phase3**	**Phase4**	**Comments/suggestions.**
2017	-Analysis of all the current models and methodology used for modern informational environments (completed by October.)	- Review literature to identify variables benchmarking of cyber fraud patterns and internet threats (completed by October.)	Literature review to identify all the current models and methodology used for modern information environments and why they cannot secure the networks. (completed by October.)	-Analysis of threat attacks on the modern informational environment networks (completed by December.)	-Publishing papers on the prevention/detection of modern semi-automated real-time information environment networks in standard journals/conferences.
2018.	-Continue the	Identify the	-Analyse &	-Study and	-Publishing

	work from the prior year while putting it into practice.	standard features of the existing models of threat assessments and analyse the IDS algorithms of modern information environments (completed by October.)	implement of algorithms for prevention of threats and attacks in modern informational environment networks (completed by October.)	analyse various new models and methodologies used to identify the threats in modern informational environments (completed by December.)	papers on the Prevention/detection of modern semi-automated real-time information environment networks in standard journals/conferences.
2019	-Carry forward the previous year's work and supplement it with a new one.	Compare of various platforms e.g., TensorFlow and techniques concerning the existing model.	-Identification of tools and platforms to design a model.	Implement raw data collected from the ESXi server in PCAP files.	-Analyse existing models and methodological approaches to address the threat assessment.
2020	-Continue the work from the previous year while putting it into practice.	Implement threat agent profile and analyse critical threat intelligence feed to the threat agents identified in the ESXi	-Design of semi-automatic model for threat assessment.	-Evaluate of semi-automatic model in next-to-real-time environment.	-Publish papers on preventions/detection of modern semi-automated real time

		server.			
2021	-Continue last year's work and put new ideas into practice.	-Execute a penetration test against a final model design and analyse the vulnerabilities of modern information environments.	-Compare results with standard published work in SCI (Science Citation Index) journals (completed by September.)	-Write thesis and final submission (completed by November.)	-Publish papers on the prevention/detection of modern semi-automated real-time information environment networks in standard journals/conferences.

Table 1 Project Planning.

1.7 Risk Assessment.

1. **Research the state of the art of tools and technologies for threat assessment.**

This objective aims to examine current technologies, methodologies, and models for analysing potential threats in the information environment, as outlined in research (Lee et al., 2015). Despite there being numerous models available, the focus is on identifying and analysing them using modern tools and advanced technologies and categorizing them into groups based on different threat assessment criteria.

2. **Prepare a prototype model for the near real-time semi-automated assessment of the threat.**

The objective is to develop a threat agent analysis model that can identify and analyse potential threats in the contemporary information environment, as described in (Patel, Stuber and Pratt, 2004). The model is designed to address tampering, information disclosure, spoofing, denial of service, repudiation, and elevation of privilege, with the aim of enhancing security in the modern information landscape. The model features unique characteristics that enable it to deal effectively with these threats.

3. **Undertake several evaluation experiments to collect primary data regarding the performance of the models.**

The objective involves subjecting the threat assessment model for the information environment to a series of evaluation tests and experiments to demonstrate its effectiveness in identifying potential threats. The primary data will be gathered through penetration testing and system investigations that involve creating honey traps to lure in unauthorized hackers and threat agents seeking to gain access (Clancy, 2011). Once the data collection is complete, the model will undergo vulnerability testing to determine the extent of damage caused by these hackers and unauthorized agents. To enhance the model's vulnerability assessment capabilities, the analysis and identification of potential threats in the information environment will be conducted using vulnerability tree methods.

1.8 Thesis Structure Overview and Orientation.

There are many desirable benefits to the implementation and use of threat assessment in a cybersecurity and information environment. The model consists of parallel computing and functions in a distributed system manner. Previously encountered threats in the modern environment can easily be detected and eliminated. In contrast, new threats must be seen and addressed over a slower time scale using various threat assessment technologies (Clancy, 2011; Sesia, Toufik and Baker, 2011). The other benefit of threat assessments is that each network system operates in different ways, so if a hacker or an unauthorized person can evade the defence of one network system, they cannot necessarily invade the other network system.

These primary properties can be considered a design principle for a computer security system used in an information environment (Scholand et al., 2007). Many of them are not new, but there is still a gap between the models and methodologies that can be implemented at the strategic level of the networking environment. I believe that through the proper use of all those properties, the threat assessment system can help design a more secure computer system. I plan to introduce through the PhD study another method that will combine all of them, which can be helpful in developing a solution to generate a safe networking environment.

Chapter 2 starts with an analysis of the various existing models and methodologies. It discusses the related work. Chapter 3 labels the necessities of research methodology and the experimental set-up of the proposed system. Chapter 4 presents the actual results and discussion for practical system experimentation. Chapter 5 discusses the vulnerability exploitation of the common vulnerabilities and Exposures list available in the NIST database, and Chapter 6 concludes the thesis.

Chapter – 2 Related Work and Background

2.1 Chapter Overview

In this chapter, all the research and literature reviews conducted during the process are discussed in detail. The threat agent analysis model and methodology are developed based on the study and analysis of threat agents found in the real-time informational environment. These models and methodologies are designed to address the needs of the analysed and assessed environment. They serve as dynamic system frameworks aimed at understanding the value of an organization's assets and the threats posed by attack agents to the business. The key findings and conclusions of the threat assessment rely on information extracted from identified threat agents, utilizing several attributes such as threat profiling, critical threat intelligence, and impact assessment based on the threat's motivation, opportunity, and capability to target an organisation or business. The threat models and methodologies enable proactive cybersecurity threat assessment in an informational environment.

Furthermore, further investigation into the footprints (incidents) of the threat agents and the results generated by various models and methodologies reveal different approaches employed by existing models and methodologies. This research will present the weaknesses and limitations of the existing risk assessment models and methodologies, illustrating how they fail to provide a comprehensive and detailed analysis of captured network packets based on the main attributes of threat agents: motivation, opportunity, and capability.

This chapter provides a detailed analysis of various models and methodologies based on multiple attributes extracted from the PCAP files captured by these models and methodologies. Attributes such as time (in min/sec), highest protocol, TCP protocol, source IP address, destination IP address, source port, destination port, total packet length, city, region, country, latitude, longitude, and internet service provider are used by cybersecurity practitioners for threat assessment evaluation and the design of vulnerability attack trees in the result phase. Based on this analysis, I will propose threat assessment models that incorporate automatic or semi-automatic features for analysing PCAP files and utilize interactive techniques to effectively design vulnerability attack trees with optimized complexity compared with existing models and methodologies.

2.2 Information Environment

Individuals, organizations, and systems involved in collecting, processing, disseminating, or acting on information are referred to as information workers. Consequently, evaluating every information environment requires considering a variety of characteristics. Some general starting points include location, population, communications technology, media, and societal institutions. Information encompasses a wide range of concepts and phenomena, encompassing both processes and material states that are intricately connected. Information can be perceived as a product, including information as an object, resource, commodity, or what is transmitted through a channel, such as a pipeline or the contents of a medium. In this thesis, hypothetical and real-world examples of threat agents are used to analyse their attributes (motivation, capability, and opportunity) that are not covered in standard threat agent taxonomies.

Recognizing that information can also refer to data is crucial within this domain. Many argue that the quality of information cannot be guaranteed in most cases. Consequently, the information domain encompasses all information about the world, while our engagement with it contextualizes the information and establishes a channel for information flow. The cognitive domain ultimately exists within decision-makers minds, and identifying its aspects can be challenging since each human mind has a unique perspective. The essential qualities of the information domain can be divided into three main dimensions: information domain quality, information domain reach or dissemination, and information domain interaction quality. The quality of information is determined by attributes such as completeness, correctness, currency, accuracy, consistency, relevance, timeliness, and assurance. Insufficient information will only provide a partial picture of the problem, while incorrect or erroneous information will fail to reflect the situation accurately. An information need is defined as a measurable set of information, including its quality, reach, and interaction features, required to plan and/or execute an activity. The minimum information required is described as the set necessary to perform the task at hand and meet the effectiveness criteria of the task leader or degree manager.

The information position of a stakeholder refers to the sum of its richness, reach, and interaction quality at any given time. This represents the stakeholder’s informational

capacity. Once the information requirements have been determined for planning or developing operations at any level, it is essential to identify the information's controllers and/or owners and evaluate their condition. Stakeholders are identified through a procedure or activity that involves gathering information on key players and their roles within the information ecosystem. The objective of this process is to identify participants and their functions. The two activities comprising the process are identifying stakeholders and defining stakeholder duties. Each input and output in this process is assigned an identifying number to facilitate data tracing between operations.

Modelling involves identifying system boundaries and gathering details on system interfaces and their interactions with the environment. The size of the environment under review may vary depending on the size of the organization. Attempting to depict the entire atmosphere can quickly become overwhelming for the assessor. The objective is to identify external points of access and internal points of entrance into various subsystems. The two activities in this process are system identification and control assessment.

Designing an information environment for the semi-automatic threat assessment model involves integrating multiple components that assist in identifying and assessing potential threats. The design aspects for the information environment include the following:

- Data sources: The first step is identifying the data sources required to feed the model, which may include internal data such as incident reports, security logs, and surveillance footage, as well as external sources such as news feeds, social media, and government threat assessments. The data must be collected, organized, and integrated into a centralised database to facilitate efficient analysis.
- Model: The model should be designed to identify patterns and anomalies in the data, detect potential threats, and prioritize them based on severity and likelihood. It may incorporate machine learning algorithms, natural language processing tools, and statistical models. The model should be customisable to meet the needs of different stakeholders.
- User interface: The user interface should enable users to interact with the model and access generated insights. It may include dashboards, heat maps, timelines, social network graphs, and other visualizations that can be customized for different

stakeholders. The user interface should provide the necessary insights for informed decision-making and proactive threat mitigation.

- Collaboration and workflow: The information environment should facilitate collaboration and workflow among different stakeholders involved in the threat assessment process, including security personnel, law enforcement, and other relevant authorities. The platform should enable stakeholders to share information, communicate effectively, and work together to mitigate potential threats.
- Data security and privacy: The information environment must ensure the security and privacy of the data. This may involve implementing access controls, data encryption, and other security measures to prevent unauthorized access or data breaches. Compliance with relevant laws and regulations regarding data privacy and security is crucial.

Designing an information environment for the model requires integrating multiple components, including data sources, the model, the user interface, collaboration and workflow, and data security and privacy. The platform should provide decision-makers with the necessary insights to make informed decisions and take proactive measures to mitigate potential threats.

Addressing cybersecurity for complex systems, particularly cyber-physical systems, such as smart grids, autonomous car systems, medical monitoring devices, industrial control systems, and IoT device networks, requires a strategic approach and planning. This research examines several models and methodologies for threat assessment, vulnerability analysis, and independent operation for identified threats in a network (Maier, 1998). A detailed study of existing models and methodologies is conducted to understand the approaches they follow to determine network threats. The nature of a cyber-physical-system implies potential hazards that can compromise its integrity, targeting various system vulnerabilities. Traditional threat modelling methods are used in the initial development cycle to address this problem (Boban, 2010)-(Tevis and Hamilton Jr, 2006). Many models employ manual techniques for analysing threats and vulnerabilities. It can be concluded that identifying threats in a network and finding vulnerabilities can be time-consuming or challenging. This chapter will address all the research questions, including how existing models and methodologies evaluate the impact of identified threats in the network and analyse vulnerabilities.

Furthermore, this study considers both analytical and hypothetical approaches, examining real-world examples such as the WorldCom fraud, where the attack was executed by top management, including the CEO, accountants, and mid-level employees. According to the final reports generated by ACFE in 2008, schemes involving multiple perpetrators resulted in a median loss over four times higher than schemes committed by a single perpetrator (Leitch, 2012). The study incorporates various sources of information, focusing on scientific research to present a holistic and up-to-date perspective. Sources include the NIST database, penetration testing reports, industry reports, security and privacy journal articles, and scientific papers retrieved through IEEE.org, Google Scholar, Wiley journals, university learning resources, and manual internet searches. Limitations of existing models and methodologies are identified through the study and analysis of the NIST database for vulnerabilities, while profiling techniques illustrated in STIX, TAXII, CybOX, MILE (Sharma, Vidalis, Menon, Anand and Pourmoafi, 2021), open indicator of compromises, etc., aid in effective analysis of threat agent groups. This helps generate alarms for incident management practitioners in handling advanced persistent threat scenarios.

In the context of threat assessments, situation awareness refers to understanding and perceiving one's environment, including identifying, comprehending, and projecting threats and risks (Erola *et al.*, 2017). It involves gathering and processing relevant information to form an accurate understanding of the situation at hand, enabling individuals or organizations to make informed decisions and take appropriate actions to mitigate potential threats.

Threat assessments involve evaluating and analysing potential risks, hazards, and dangers that may harm or damage individuals, organisations, or assets. These assessments aim to identify, assess, and prioritize threats based on their likelihood, potential impact, and target vulnerability. Threat assessments typically involve a systematic approach, including data collection, analysis, and interpretation to generate actionable intelligence.

In the context of threat assessments, situation awareness plays a crucial role by providing a comprehensive understanding of the current situation and potential threats. It encompasses the following key concepts:

- Perception: Situation awareness begins with perceiving and detecting relevant environmental cues or information. This can include gathering data from various

sources such as surveillance systems, intelligence reports, human sources, or open-source information.

- Comprehension: Once the information is collected, it needs to be processed and analysed to form a coherent and accurate understanding of the situation. This involves interpreting the data, identifying patterns, and recognizing potential threats or risks.
- Projection: Situation awareness also involves the ability to anticipate future developments and project how the situation might evolve. This requires considering various factors, such as the capabilities and intentions of potential threats, and assessing the potential consequences of their actions.
- Decision-making: Based on the understanding gained through situation awareness, informed decisions can be made to mitigate or respond to threats effectively. These decisions may involve implementing security measures, allocating resources, or adjusting operational plans.
- Adaptability: Situation awareness is not static but requires ongoing monitoring and adjustment. It involves continuously updating and reassessing the understanding of the situation as new information becomes available or circumstances change.

By integrating situation awareness into threat assessments, individuals or organizations can enhance their ability to detect, analyse, and respond to potential threats effectively. It allows for a proactive approach to security by enabling timely and appropriate actions to reduce vulnerabilities and mitigate risks.

The existing models and methodologies employ various approaches to conduct threat assessments and vulnerability analyses for identified threats in a network. During the thorough analysis of their policies, which encompass the approaches followed by several existing models and methodologies, I have identified gaps and limitations in their techniques to achieve the desired goal. One standard limitation is the absence of threat profiling and the failure to analyse cyber threat intelligence feeds for the threat agents (Boban, 2010)-(Tevis and Hamilton Jr, 2006). Some of the models rely on manual threat assessment, resulting in the high complexity and vague performance of the process. A significant limitation identified in the existing models and methodologies is the lack of evaluation of the motivations, opportunities, and capabilities (M,O,C) attributes of threat agents. While some models touch upon motivation, it is not thoroughly addressed during the evaluation phase (Boban, 2010)-

(Tevis and Hamilton Jr, 2006). A detailed explanation can be found in the related work section. Cybersecurity practitioners have described their work using various models and methodologies for analysing PCAP files or data stream captured during threat assessments (Sharma, Vidalis, Menon, Anand and Pourmoafi, 2021).

To address the research topic, I will start by analysing and examining several models and methodologies used in similar studies conducted by other researchers, as depicted. The process involves extracting valuable information from the PCAP files captured by the existing models and methodologies. This information will be used to classify threat agents based on their attributes (Blyth and Kovacich, 2001; A Jones, 2002; Vidalis and Jones, 2003; Gamble et al., 2020; Pandelică, 2020; Sharma, Vidalis, Menon, Anand and Pourmoafi, 2021). Later, I will compare several existing models and methodologies, assessing their strengths and limitations, in order to determine the threat and vulnerability analysis for the attack.

2.3 Related Work

The first criterion for comparison is the existing models and methodologies, which employ different approaches to threat analysis in the information environment. I then determine the strengths and weaknesses of these models/methodologies. It is evident that no single model or methodology is perfect in all aspects of conducting threat assessment in a real-time network. Each method has been developed with different perspectives and follows distinct approaches. Some strategies prioritize assets, others focus on attackers, and some concentrate on threat agents, among other considerations. As a result, each method possesses strengths and weaknesses that are associated with the approaches they employ to accomplish their goals/tasks.

Nicholas J et al. (Puketza et al., 1996) The models were analysed with the help of IDS software testing and the use of a UNIX-based platform. It states that an IDS identifies unauthorized access, misuse, and abuse of computer network systems. They present a detailed methodology, including a strategy for test case selection and specific testing procedures. These methodologies were tested on NSM (Network Security Monitor), an IDS developed at UC Davis. The authors also provide background information on IDS. The experimental set-up of the IDS methodology helped identify its capabilities and knowledge.

The tools used for testing the IDS methodology systematically evaluated and measured the effectiveness and performance of IDS, as presented in the paper.

Pilgermann, Blyth and Vidalis, 2006 the tool used for analysis in the study are IOIDS (Inter-organizational Intrusion Detection System) and G4DS (Grid for Digital Security), both based on Knowledge Grid technology. The authors illustrated the concept by combining IDS with grid technology to address threat assessment issues in real-world information systems. They discovered a new approach for security audit data by combining grid technology with trust relationships and commodities results. The authors also explained the concept of G4DS analysis.

IOIDS, an inter-organizational intrusion detection system, is being constructed using a modular approach. This approach includes the following key elements:

- Overview of the parties and components involved.
- Information about data processing from IOIDS layers.
- Focus on adjacent components of G4DS layers.
- Connection or interaction with third-party event generators.

In this research, the authors propose IOIDS as a means to enhance secure information/knowledge transfer over the internet. The peer-to-peer-based communication, facilitated by G4DS, ensures the secure movement of a wide range of data.

Dharmapurikar and Lockwood, 2006 The tool used for analysis in the study is Snort string sets, Bloom Filter, and FPGA (Field-Programmable Gate Array) tools for analysis. The authors describe the need for high-speed filtering and assessment of packets in a network using a fast multi-pattern matching algorithm. While this algorithm is known for its highly proactive memory accesses, its performance was still a bottleneck. Hence, hardware-accelerated algorithms are required for line-speed packet processing in a network. The authors present a hardware-implemented pattern-matching algorithm for content filtering applications, which can be scaled for numerous patterns, speeds, and pattern lengths. This algorithm, known as the Bloom Filter, is based on a multi-hashing data structure.

Constructing Bloom Filters using FPGA and VLSI (very large-scale integration) technology enables efficient memory access and accelerates string matching.

The authors implement an efficient algorithm capable of scanning thousands of small patterns up to 16 bytes at multigigabit-per-second speeds, using a manageable amount of on-chip memory and a few megabytes of external memory. Subsequently, they improve the algorithm to handle larger strings and reduce the need for additional on-chip memory. The authors then develop a scalable and fast multi-pattern matching algorithm for network intrusion detection systems (NIDS) based on the principles of Bloom Filters. This algorithm reduces memory access through the use of Bloom Filters and increases overall speed. In the latter part of the study, they extend the algorithm to incorporate the Aho-Corasick algorithm, enabling it to handle large strings effectively.

2.3.1 Analysis of Traffic Networks

To ascertain the characteristics and aspects of the network used by a number of cybersecurity practitioners, the network is investigated and analysed in this section. Li and Trappe, 2007 The tool utilizes the ORBIT Wireless Testbed 802.11 for analysis. The authors of the study elaborate on the vulnerability of wireless networks to spoofing attacks and propose a non-cryptographic mechanism for detecting such attacks, eliminating the need for cryptographic keys. They introduce the concept of forge-resistance relationships, which involve examining the consistency of transmitted packets to identify anomalous activities within wireless networks. The ORBIT Wireless Testbed 802.11 serves as the tool for conducting experiments and evaluating the results.

In their research, the authors delve into various monotonic relationships found in the sequence number fields. They also introduce a supplemental identifier field, designed explicitly for differentiating between anomalous activities and congestion in the context of time for reverse one-way function chain traffic statistics. By leveraging these relationships, the authors develop a classifier for multi-level threat assessments, utilizing an experimental set-up within the orbit wireless testbed. This testbed proves instrumental in examining the mentioned relationships and their effectiveness in countering spoofing attacks in wireless networks. The authors present an alternative method to the traditional approach of identifying spoofing in wireless networks, proposing two distinct families of relationships.

The first relationship family involves including an additional field during packet transmission, while the second family relies on an implicit property observed during the transmission and reception of packets. Furthermore, the authors suggest that analyzing inter-arrival statistics for traffic scenarios can aid in identifying anomalous activities within wireless networks. They devise a new forge-resistance consistency check known as RRCCS to enhance threat detection in wireless networks. Notably, this check proves advantageous in scenarios where maintaining keying is practically challenging. RRCCS exhibits a fundamental property in wireless networks, because it can detect threats without relying on the practical feasibility of maintaining keys.

Polychronopoulos et al., 2007 The "Sensor Fusion for Predicting Vehicles' Path for Collision Avoidance Systems" study employs MATLAB/NS2,3 as the analysis tool. The research focuses on optimizing the hand-off procedure's complexity, including time and area, through effective network mobility management to ensure seamless internet connectivity for mobile devices. When users attempt to transition from one subnet to another, the handoff action is executed on the mobile device. However, this action can potentially disrupt real-time services such as mobile TV or VoIP because of the mobility of the devices. The authors specifically address the challenges posed by fast-moving vehicles, which can result in packet loss and hand-off issues, consequently reducing network throughput.

To tackle the problem at hand, the authors explore rollout algorithms, which serve as practical heuristics for the single-vehicle routing problem with stochastic demands (VRPSD). VRPSD is a well-known logistics model that accounts for uncertainty. However, these algorithms can be computationally intensive, considering the complexity of the problem they address.

Pontarelli, Bianchi and Teofili, 2012 The "Traffic-Aware Design of a High-Speed FPGA Network Intrusion Detection System" study utilizes Sort NIDS, Xilinx vertex-II, and INVEA COMBO-LXT as the analysis tools. The authors mainly focus on the network intrusion detection system. The ability to swiftly update the supported rule sets and detect new emerging attacks makes FPGAs a very appealing technology. The study investigates the emerging trade-offs and advantages, showing that resources can be saved up to 80% when processing near-real-world packet traffic statistics from an operator backbone.

The demand for network security has increased because of new internet threats, and NIDS plays a salient role in this context by analysing network traffic. The study explains Gilder's and Moore's laws as they pertain to logic resources and proposes a better way to parallelize NIDS architecture. It also analyses Snort rules and their related categorization policies, aiming to narrow down the CPU usage and memory consumption of Snort.

In the second part, real-world traffic analysis is conducted to determine the sizing of hardware modules using adaptive algorithms. The study implements the hardware modules and examines the trade-offs related to speed and area for different SMEs. The delay in transferring a packet is calculated using a multiplexing approach. The study applies hardware circuit pattern matching with the help of deterministic finite automata (DFA) and non-deterministic finite automata (NFA). The basic architecture used is the shift-and-compare architecture, which is developed in three steps: first, a well-known Snort NIDS is used to analyse the relevant rule set; second, the hardware implementation of individual SMEs supporting such rule subsets is optimized; and finally, the system is dimensioned based on network traffic packet demographics gathered experimentally from a real-world operator's deployment.

2.3.2 Study of Data Stream and Threat Modelling

In order to ascertain the characteristics aspects of the data used by the number of cybersecurity practitioners, investigation and analysis of the data are conducted in this section. The evaluation of various techniques for gathering information from an organization's network. (Pan, Morris and Adhikari, 2015) utilizes a real-time digital simulator (RTDS), energy management system, and Snort as the analysis tools. The study presents a systematic and automated approach to building a hybrid IDS that combines signature-based and specification-based IDS features. The data mining technique known as common path mining is employed to automatically and accurately learn patterns from the fusion of synchro-phasor measurement data and power system information. A prototype of the IDS was developed, authenticated, and executed. It successfully classifies disturbances, regular control operations, and cyber-attacks within the distance protection scheme of a two-line, three-bus power transmission system.

The next-generation power system, also known as the smart grid, heavily relies on advanced technologies such as synchro-phasor systems for wide-area monitoring and control to meet the increasing demands for reliable energy. However, these advancements bring security challenges, as demonstrated by the vulnerability of technologies such as Ethernet to cyberattacks. The US Government Accountability Office has concluded that current guidelines are insufficient to implement the smart grid securely. The study also explores related IDS scenarios used for security purposes, such as IDS for intelligence electronic devices and network-based IDS. In 2013, an IDS was explicitly proposed for synchro-phasor systems to detect cyberattacks.

Additionally, in 2009, an IDS was presented that utilized anomaly detection techniques to identify patterns. Collectively, these approaches aim to uncover malicious payloads and detect illegitimate changes in the physical system. The study utilizes sequential data-mining techniques, focusing on time-ordered data related to activity patterns. The FP-Growth Algorithm is employed in the training process to mine frequent sequential patterns from power system data. The KDD standard path mining algorithm is utilized for fault detection. The IDS achieved a correct classification rate of 90.4% for tested scenario instances, and the average detection accuracy for zero-day attack scenarios was 73.43%. The future IDS is intended to perform real-time classification based on live system inputs.

Lichtman et al., 2016 The study utilize the Sanjole LTE Sniffing tool for analysis. The research aims to investigate LTE's vulnerabilities to RF (radio frequency) jamming, spoofing, and sniffing and assess various physical layer threats that can affect communication networks. LTE, standardized by 3GPP, offers improved coverage, enhanced system capacity, high spectral efficiency, low latency, high data rates, and cost-effectiveness. The threats can be categorized into two groups: (a) denial of service (DOS) attacks and (b) information extraction attacks.

The study primarily focuses on jamming, which targets the receiver in an RF attack vector, and cyber-attacks on the network attack vector. LTE utilizes OFDMA (orthogonal frequency-division multiple access) for downlink and SC-FDMA (single-carrier frequency-division multiple access) for uplink access. Two types of jamming attacks are considered:

synchronous jamming attacks and asynchronous jamming attacks. Performance and security testing may also be conducted using TEMS and NEMO.

Further analysis and experimentation are required to compare the safety and performance of different mitigation techniques. The study seeks to identify effective measures to mitigate the impact of jamming, spoofing, and sniffing on LTE/LTE-A networks, ensuring the reliability and security of communication systems.

Ambusaidi et al., 2016 utilizes the Least Square Support Vector Machine-based IDS (LSSVM-IDS) as the analysis tool. The authors address the issue of the data containing redundant and irrelevant features, which poses long-term challenges for network traffic categorization. These features slow down the categorization process and hinder classification decisions, especially when big data is being dealt with. To tackle this problem, the authors propose a mutual information-based algorithm that identifies the most relevant features for categorization. This algorithm, named LSSVM-IDS, handles both linear and non-linear dependent data features.

The performance of LSSVM-IDS is evaluated using three IDS datasets: KDD (Knowledge Discovery and Data) Cup 99, NSL-KDD (Network Socket Layer Knowledge Discovery and Data), and Kyoto 2006+ datasets. The evaluated results demonstrate improved accuracy and lower computational cost compared with state-of-the-art methods. The construction of an IDS requires two major building blocks: a robust categorization method and coherent feature selection algorithms. The authors address this challenge by proposing a filter-based feature selection algorithm called Flexible Mutual Informational Feature Selection (FMIFS). FMIFS is an enhanced version of Mutual Information Feature Selection (MIFS) and Modified Mutual Information Feature Selection (MMIFS). It reduces feature redundancy more effectively than Battisti's algorithm and helps solve linear equations for categorization problems instead of quadratic programming problems.

The authors present evaluated results regarding categorization detection rate, F-measures, false-positive rate, and accuracy, comparing them with existing detection approaches for cyber-attacks, particularly denial of service (DoS) attacks and computer malware. They

suggest that further performance improvements can be achieved by using an enhanced optimizing search strategy in a network.

In conclusion, the study provides an effective approach for building an IDS by utilizing the LSSVM-IDS tool and a filter-based feature selection algorithm. The evaluated results demonstrate the superiority of the proposed method over other algorithms in terms of accuracy, detection rate, F-measures, and false-positive rate for various cyber-attack types, including DoS, probe, user-to-root (U2R) attacks, and remote-to-user (R2L) attacks.

Gelso and Sjoberg, 2017 et al. study "Consistent Threat Assessment in Rear-End Near-Crashes Using BTN and TTB Metrics, Road Information, and Naturalistic Traffic Data" utilizes MATLAB and data-mining algorithms for clustering the datasets. Rear-ended crashes are among the most frequent traffic accidents, and collision avoidance systems (CAS) algorithms are being developed to prevent them. However, these algorithms currently rely on simplified models of vehicle motion based on constant velocity and acceleration, which leads to issues in vehicle motion and behaviour prediction. Assumptions based on constant velocity and acceleration can result in potential collision hazards in traffic data systems.

The authors identify and address these hazards by collecting data from Euro-FOT (European field operational test on activity safety systems) and aim to resolve them by enhancing the information model regarding the deceleration pattern of CAS algorithms. Two metrics, time-to-brake (TTB) and brake-threat-number (BTN) are used to estimate the hazards. The authors propose a new algorithm called CTALMA (consistent threat assessment for longitudinal motion algorithm), which provides in-depth analysis through three test examples:

- Determining events related to rear-end crashes.
- Applying K-means clustering techniques.
- Identifying three clusters with increasing average levels of potential collision hazards.

In Europe, various CAS algorithms are employed daily to prevent accidents. However, they often work on constant acceleration and velocity, which limits their ability to accurately predict traffic situations and leads to rear-end crashes. The authors developed the CTALMA algorithm to address this limitation, which operates based on real-time traffic position. If any

issues arise during the vehicle's motion, it generates an alert to the driver and activates the automatic brake systems to respond to the current situation. The authors tests the CTALMA algorithm using MATLAB tools on various collected datasets. The algorithm addresses all vehicle motions and provides illustrations for three live examples:

- Identification of events related to rear-end crashes.
- Application of K-means clustering techniques.
- Identification of three clusters with increasing average levels of potential collision hazards.

This algorithm helps prevent false alarms for collisions and provides accurate estimates of the vehicle's velocity and acceleration through the CTN (time-to-brake) and BTN (brake-threat-number) matrices.

Maheshwari and Prasanna, 2016 et al. is a tool used to analyse Microsoft products using STRIDE (S-Spoofing, T-Tampering, R-Repudiation, I-Information disclosure, D-Denial of Service, E-Elevation of privilege). The authors demonstrate an understanding of threat detection and creating an environment that reduces the likelihood of malicious activity by integrating risk assessments and threat modelling into the SDLC process.

This paper conducts threat modelling for risk assessment purposes, specifically focusing on identifying risks in software-based systems. The authors used STRIDE to analyse the life insurance system and successfully identified and detected 50% of software defects during the design phase of the SDLC. They also discuss how the model helps in identifying and categorizing threats based on prioritization. However, they only analysed the life insurance system using STRIDE and did not evaluate the impact of threats based on capability, opportunity, and motivation to penetrate the system. Additionally, they lack an evaluation of vulnerability for identifying threats. Furthermore, the authors did not address threat mitigation as proposed in the abstract.

2.3.3 Threat Agents and Attributes

The purpose and technique are intended to target the deliberate exploitation of a vulnerability or a circumstance and technique that might unintentionally create a vulnerability. Threat

modelling is a systematic approach with the following goals: identifying security needs, locating security risks and potential vulnerabilities, determining the criticality of threats and vulnerabilities, and ranking remedial options. Ikuya Morikawa et al. (Morikawa and Yamaoka, 2011) " Threat Tree Templates to Ease Difficulties in Threat Modelling" tool used to do analysis is STRIDE (S-Spoofing, T-Tampering, R-Repudiation, I-Information disclosure, D Denial Of Service, E-Elevation of privilege.) and DREAD (Damage, Reproducibility, Exploitability, Affected users & Discoverability). This tree is being used to identify the threat, which helps determine its risk assessments and countermeasure. The authors propose creating a threat tree with several branches representing the many possible attack scenarios and corresponding vulnerabilities and countermeasures for such attacks. This tree is used to identify the threat, which helps determine its risk assessments and countermeasure. They also designed a filtering out of irrelevant scenarios. In this section, the author illustrated threat modelling and the role of threat trees' role in data flow diagrams and various notable features. They suggested that the threat tree cannot detect the attack scenario against an entire system from the patterns. To address such a problem author used the threat tree template. They made six threat tree templates for each of the threats analysed by STRIDE. The authors suggested using threat tree templates to address the threats rather than threat trees because threat tree templates are more efficient in identifying the attack scenarios or more paths as compared to threat trees. The main limitation of this threat tree template is that it can be used for specific attack scenarios, not real-world environments.

Michael Shin et al. (Shin, Dorbala and Jang, 2013) "Threat Modelling for Security Failure-Tolerant Requirements" is a tool used to conduct analysis using Case models (misuse and abuse) and HAZOP (hazard & operability analysis). The research describes an approach to modelling security threats and addressing security failures associated with these threats. The authors assume that core security measures of an application, such as authentication, access control, cryptosystems, or digital signatures, can be compromised in a real-world environment. They used internet banking applications as an illustration for the proposed approach. The main objective of security failure-tolerant services is to minimize the impact of threats on relevant assets, even in cases where core security is compromised. The authors discuss the use of HAZOP, misuse cases, abuse cases, soft interdependency graphs, and CORAS to analyse threats in various attack scenarios. In this context, the authors aim to address the issues faced when core security is breached while using internet banking is being

used for fund transfers or other services. One limitation of this model is that it assumes that all core security measures are compromised in real-time environments. However, this may not always be the case, and not all scenarios need to be analysed.

"The field of threat agent profiling and analysing cyber threat intelligence has recently received significant attention. Researchers have proposed various models and methodologies designed to detect or prevent attacks." (Legg et al., 2013) and (Bishop et al., 2014). Likewise, Vidalis et al. (Vidalis, Jones and Blyth, 2004) briefly addresses the TAME (threat assessments model for EPS) methodology for threat assessments in real-time informational environments and provide a high-level overview of its phases and process while performing threat assessments. They compare the TAME (threat assessments model for EPS) methodology with other methods based on a number of parameters, such as sting, effectiveness, and understanding of information security from the threat. TAME is the upgrading version of METEORE 2000 for the micropayment system (MPS). In the initial phases, the authors analyse a number of methodologies, Alberts 1999, 2001, Baker 1998, Bayne 2002, Blyth 2003, Dimitrakos 2001, Forte 2000, Hancock 1998, Jones 2002, Nichols 2001, etc. and they found that all work on the waterfall model principle. Still, such an approach is unsuitable for the micro payment system. So, they developed a new methodology i.e., TAME which has ability to resolve the issues related to MPS. TAME works simultaneously in four phases named as:

- Scope of assessments.
- Threat agent and vulnerability analysis.
- Scenario construction and system modelling.
- Evaluation.

According to these phases, TAME determines the level of security required for a particular organization and its system. All four stages work simultaneously, with inputs from one phase becoming outputs for another phase. Likewise, inputs and outputs are generated from TAME, depending on the threat assessment requirements. The authors concludes that the assessor serves as an asset for better understanding and analysing an organization's systems within the TAME framework.

Morakis et al. Vulnerabilities and their exploitation cycle can be measured using various tools such as COPS, NESSUS, SYSTEM SCANNER, RETINA, NET RECON, WHISKER, and CYBER COB. In this work, the author focuses on addressing data problems in the informative environment, particularly cyberattacks. The authors propose the use of vulnerability tree analysis to tackle long-standing issues faced by several organizations. The approach involves constructing a knowledge information hierarchy in an object-oriented tree and developing a formal model to analyse vulnerabilities in relation to potential attack scenarios targeting computer systems. The primary objective is to classify vulnerabilities in depth, understand why specific attacks occurred on particular data/assets, and analyse footprints and threat agent scenarios for exploiting vulnerabilities. The main goal of vulnerability tree analysis is to detect and address attacks at early stages before causing significant damage to real-world information systems.

The authors illustrate various tools capable of analysing the vulnerability of complex organizational environments, including COPS, NESSUS, SYSTEM SCANNER, RETINA, NET RECON, WHISKER, and CYBER COB. However, they suggest that these tools are insufficient in today's modern electronic era of cybercrime because they fail to address hazards such as fault-tree analysis, checklists, event-tree analysis, cause-consequence analysis, etc. To overcome these limitations, the authors combine vulnerability tree analysis with object-oriented trees and effectively addresses these hazards using Boolean mathematics.

Gerald L. et al. (Vidalis and Jones, 2006) point out that threat agents can gain unauthorized access to computer systems in real-world informational environments through various means. They acquire the motivation, capability, and opportunity to perform such damage in network systems from different sources. The author provides an illustration of threat agents and their attributes, functions, and impact on informational systems networks. The author also analyses digital attacks that occurred in 2002 across several countries.

In real-world informational environments, the threat agents consist of various elements such as a threat agent catalogue, historical data, technical reports from enterprises, reports from business environments, reports from physical environments, current knowledge/information, current knowledge of stakeholders, current knowledge of the staff, and a list of stakeholders.

They identify that the threat agents of real-world informational environments consist of:

- Threat agent catalogue.
- Historical data.
- Technical report enterprises.
- Reports of business environments.
- Reports of physical environments.
- Recent knowledge/information.
- Current knowledge of stakeholders.
- Current knowledge of the staff.
- List of stakeholders.

The thesis evaluates the capabilities, motivations, opportunities, and impact of threat agents using a three-dimensional matrix mathematics approach. Each factor is assessed using metrics and ESA (empowered small agents) threat agents. The analysis reveals that the threat agents in 2002 caused worldwide economic damage of $35 million to the European Union. Considering the significant cost of damage, it is crucial for system security officers to possess comprehensive knowledge and information about threat agents and employ adequate risk management strategies to protect informational systems from cyberattacks.

2.3.4 Study of Threat Agents

The purpose and technique are intended to target the deliberate exploitation of a vulnerability or a circumstance and technique that might unintentionally trigger a vulnerability. Adetorera Sogbesan et al. (Sogbesan et al., 2012) developed a model to identify the MERIT (management & education of risk of insider threat) based on the study of insider threat concerning the institute of CERT/USSS. This MERIT provides the facility to mitigate the insider threat of an organization, and the key finding is to make the case study of individual threat agents, i.e., collision threat. MERIT models the case studies on the insider threat for an organization. Based on that, threat assessments have been conducted to determine the impact of danger on the business. They also show some figures for losses based on studies done by USSS/CERT. They categorize the insider attack based on the ex-employee, or the financial gain of any vital position held by an employee in an organization. Based on the number of organizations, 69% of companies measured stated data theft events (not external attacks). These threats originated from inside the organization. At the same time, a massive 91% of

companies testified to not having operative detection systems for recognizing an insider threat. The MERIT model has a limitation/shortcoming in analysing compressive pattern analysis based on motivation and behavioural characteristics. The MERIT model cannot address the motivation factor of a collision attack. They are not able to explain the capability of an insider threat.

Casillo, M. et al. 2019 “Embedded Intrusion Detection System for Detecting Attacks over CAN-BUS” design a model based on AIC (availability, integrity, and confidentiality). The authors addressed the issues related to cyberattacks on the automotive vehicle system. They introduce the automotive IDS embedded method for the CAN (controlled area network) BUS. Referencing the Bayesian network approaches, identifying malicious messages to the connected devices to the vehicles is accomplished. This paper identifies the snag for the IoT devices connected to automotive vehicles and their attacks while using automation and suggests machine learning approaches, particularly the Bayesian network approach to cope with the cyber-attacks on the CAB bus. The authors used the CARLA simulator to provide the solution. The Python library and several APIs were cast off for clustering the data and FPGA techniques for developing the model’s architecture.

Lombardi, M. et al. “EIDS: Embedded intrusion detection system using machine learning to detect attack over the can-bus” introduce an IDS approach to identify the threats in automated vehicles, particularly CAN buses. The author cast off the development of an IDS approach with the help of machine learning techniques through the Bayesian network approach to detect possible attacks on the CAN bus. The main benefit of developing an IDS approach was using the embedded framework for designing and determining the non-linear message flow. The rebuke faced by the connected IoT devices and the intelligent device for self-driving vehicles was identified with the help of an introduced IDS approach in the research.

These related works show that accessing a real-world data stream is enormously challenging. Thus, researchers synthesize data into several groups based on the threat agents identified in a network. The existing model and methodology did threat assessment manually, due to which their complexity is exorbitant. This research predominantly wants to epitomize the volume and variety of data analysed in a modern real-world information environment and display how this could be pooled to form an overall threat assessment for each PCAP file. We also want to exhibit a wide range of threat scenarios as epitomized by our data collected from the

real world in a specific environment and show how our profiling and CTI system of threat agents would detect the different attacks based on the patterns identified.

2.4 Threat Profiling

The first step in developing a secure application involves researching the goals and methods of potential adversaries. Adversaries are seen as threats to the application because of their intentions and motivations. Threat profiling is a systematic process of identifying and documenting all potential security threats. By studying various threats directed at the organization in detail, security teams can gain a better understanding of the level of sophistication of these threats and their exploitation strategies. This helps in identifying potential vulnerabilities in the organization's security posture. With knowledge of the threats, threat profiles provide incident management teams with valuable threat intelligence information. This information can be used to analyse individual threat scenarios or campaigns, enabling proactive measures to anticipate and mitigate future attacks.

Three common network security vulnerabilities that are particularly harmful to businesses are often identified:

- Malware
- DDoS (distributed denial-of-service)
- Sophisticated persistent threats.

Threat profiling is a strategic process used in cybersecurity to assess and understand potential security threats and vulnerabilities an organisation faces. It involves systematic research and analysis of adversaries' goals, motivations, and methods, aiming to build a comprehensive picture of potential risks to the organisation's security. Here's a breakdown of what threat profiling entails based on the threat assessment:

- **Researching Adversaries:** The process begins by studying potential adversaries who may target the organisation's systems or applications. This includes understanding their intentions, motivations, and the tactics they might employ to compromise security.

- **Identifying and Documenting Threats:** Threat profiling involves systematically identifying and documenting all possible security threats. This can include various types of threats, such as malware, distributed denial-of-service (DDoS) attacks, sophisticated threats, and many more.
- **Understanding Threat Sophistication:** By studying these threats in detail, security teams gain insights into the level of sophistication of potential adversaries. This understanding helps in assessing the potential impact and severity of the threats.
- **Identifying Vulnerabilities:** Through threat profiling, security professionals can identify potential weaknesses or vulnerabilities in the organisation's security posture.
- **Providing Threat Intelligence:** Threat profiles serve as a valuable source of threat intelligence. This information is used to keep incident management teams informed about potential threats.
- **Proactive Measures:** Armed with knowledge about potential threats and vulnerabilities, organisations can take proactive measures to enhance their security posture.

2.5 Threat Agent Attribute Calculation

Threat agent attribute calculation is the activity of calculating the attributes of each agent using threat agent information from activities and phases in order to identify the threats that the company confronts. According to several theories, three components must be present for a threat agent to exploit a vulnerability: capability, motivation, and opportunity. In these tasks, each of these parameters will be calculated. In this phase, I will combine the threat agent list and the vulnerable ports to create a matrix that displays all the interactions between the two. These exchanges represent the enterprise's threats. It is then necessary to calculate the impact of each engagement on the enterprise. This is the result of another process. A multidimensional matrix, specifically a three-dimensional matrix, is required in this operation. The strategy aims to detect the risks that the filtered threat agents can manifest by exploiting the filtered vulnerabilities of the system assets found during the enterprise's activity analysis. The following activities are included:

- Threat agent capability calculation
- Threat agent opportunity calculation
- Threat agent motivation calculation

- Threat identification is all steps in the threat agent capability calculation process.

In addition to calculating the attributes of threat agents, the threat agent attribute calculation phase also involves further analysis and assessment. It considers threat agent's capability, motivation, and opportunity to exploit vulnerabilities within the enterprise's systems. During the threat agent capability calculation, the focus is on evaluating the technical expertise, resources, and knowledge possessed by threat agents. This assessment helps determine their ability to successfully carry out attacks or breaches.

Threat agent opportunity calculation involves assessing the potential pathways or vulnerabilities that may provide an opportunity for threat agents to exploiting. It considers factors such as weak access controls, outdated software, or unpatched systems that could create openings for attacks. The threat agent motivation calculation aims to understand the driving factors or incentives behind the threat agent's actions. This could include financial gain, competitive advantage, political motives, or other underlying motivations influencing their decision to target the enterprise's systems. Through these calculations, the enterprise gains insights into the potential threats it faces and can prioritize its security efforts accordingly. By understanding threat agent's capabilities, opportunities, and motivations, organizations can develop more effective countermeasures and risk mitigation strategies to protect their systems and assets. It's important to note that threat identification is integral to the threat agent capability calculation process. This involves identifying specific threats posed by threat agents based on their capabilities, motivations, and opportunities. This comprehensive understanding of the threats allows organizations to develop appropriate security measures and response plans to safeguard their systems.

2.6 Comparison of Models and Cybersecurity Tools

The different models, methodological approaches, and techniques will be described in this section. However, threat agent analysis modelling is a proactive strategy for determining the threat agents in a real-time informational environment. It involves identifying potential threat agents and developing models/methodology procedures to detect and respond to the identified threat agents. Threat modelling can help the organization or business prioritize its identified threats in a network and distribute resources effectively. The various models and methodologies are described below in table 2. The methodologies and models examined

across multiple research papers have several shortcomings and limitations to threat assessment analysis of threat agents found next to the real-time informational environment. However, an investigation is time-consuming and expensive. All the investigated models and methodologies follow the waterfall method for evaluation and generating outputs. It implies they are not malleable enough to subsist with many changes to their data stream (inputs) during the threat assessment (Sharma, Vidalis, Menon, Anand and Kumar, 2021). UKERNA et al. in (Leyland and Brooks, 1996) (Saunders, 2002) claim that "the most conservative statistics indicate that every single computer system in the whole of the world, which is connecting to the Internet will be the target of an attack across the network, at least once a week." Furthermore, these models and methodologies use the probabilities approach to evaluate the threat's likelihood without considering the threat agents' likelihood. Just the concept of using probabilities significantly underestimating the validation of the methods. None of the methods is trying to model the examined systems in the business environment. Therefore, the various assumptions are determined, and these assumptions will lead to errors in evaluating vulnerabilities attack vectors and threat agent's groups identified in a network. Most of the models only consider the impact of threat on financial losses.

Models or/and Methodology (Tools)	**Explore & assess threats to business operations concerning the type of business**	**Determine what policies, standards & controls are worth implementing to reduce threats, awareness & understanding of stakeholders**	**Assess compliance with standards & control effectiveness**	**Ability to evolve and react to external stimuli as they happen**	**Suitable for SMEs (cost.)**	**Automated (Semi.)**
GSTool(Oreku and Mtenzi, 2017)	✓	×	✓	×	✓	×
Splunk(Bruzzese, 2019)	×	× & ✓			✓	✓
Proteus(Bose et al., 2017)	×	✓	✓	✓	✓	✓
Alien Vault(Abu et al., 2018)	×	× & ✓	✓	✓		✓
MIGRA Tool(Mosca, 2018)	✓	×	✓		✓	✓
NUIX(Rughani, 2017)	×	×	×	×	×	✓
Archer(Archer, 2014)	✓		✓			✓
IRM Security(Ani, He and Tiwari, 2019)	×	×	×	×	×	✓
RiskIQ(Schwarz	×	×	×	×	×	✓

and Creutzburg, 2021)						
SATAM(Sharma, Vidalis, Menon, Anand and Kumar, 2021)	✓	✓	✓	✓	✓	✓

Table 2 Models Vs. SATAM(Schwarz and Creutzburg, 2021)(Bruzzese, 2019)(Fresner et al., 2017)(Longhurst et al., 2020)(Sharma, Vidalis, Menon, Anand and Kumar, 2021)(Cappelli, Moore and Trzeciak, 2012).

Table 2 compares the number of models and methodologies based on the tools and approaches used to address the threat agent groups identified in the network. A tick indicates that they are compatible to perform the operation, and the cross indicates they are not compatible to perform the operation while analysing the threat agents during threat assessment for any organizations or business of the nations. Some of the blocks show both conditions are compatible while performing threat and vulnerability analysis of the network based on the upgraded version of the tool that has been used for determining the threat agents' attributes. The complete analysis was carried out based on the study of the characteristics of the models and methodology used to perform the threat assessments.

1. GSTool (Oreku and Mtenzi, 2017:)
    a. It explores and assesses threats to business operations concerning the type of business.
    b. It does not determine what policies, standards, and controls are worth implementing to reduce threats or raise awareness and understanding among stakeholders.
    c. It assesses compliance with standards and control effectiveness.
    d. GSTool is a model/methodology that focuses on exploring and assessing threats to business operations based on the specific type of business.
    e. It does not determine what policies, standards, and controls should be implemented to mitigate threats or increase stakeholder awareness and understanding.
    f. GSTool assesses compliance with standards and evaluates the effectiveness of controls. It has the ability to evolve and react to external stimuli as they occur.
    g. This model is suitable for small and medium-sized enterprises in terms of cost. It is not fully automated.
2. Splunk (Bruzzese, 2019:)
    a. It does not explicitly explore and assess threats to business operations concerning the type of business.

b. It determines what policies, standards, and controls are worth implementing to reduce threats and raise awareness and understanding among stakeholders. It does not assess compliance with standards and control effectiveness.
c. Splunk is a tool that is not explicitly designed for exploring and assessing threats to business operations concerning the type of business.
d. It does, however, assist in determining suitable policies, standards, and controls to reduce threats and enhance stakeholder awareness and understanding. Splunk does not explicitly assess compliance with standards and control effectiveness.
e. It has the ability to evolve and react to external stimuli in real time. This tool may have varying costs depending on the specific implementation and requirements. It can be partially automated.

3. Proteus (Bose et al., 2017:)
    a. It does not explore and assess threats to business operations concerning the type of business.
    b. It determines what policies, standards, and controls are worth implementing to reduce threats and raise awareness and understanding among stakeholders.
    c. Proteus is a model/methodology that does not directly explore and assess threats to business operations concerning the type of business.
    d. It focuses on determining the appropriate policies, standards, and controls to mitigate threats and enhance stakeholder awareness and understanding.
    e. Proteus includes an assessment of compliance with standards and the effectiveness of controls.
    f. It assesses compliance with standards and control effectiveness. It has the ability to evolve and react to external stimuli as they happen.
    g. It is suitable for SMEs in terms of cost.
    h. It is automated.
4. Alien Vault (Abu et al., 2018:)
    a. It does not explore and assess threats to business operations concerning the type of business.
    b. It determines what policies, standards, and controls are worth implementing to reduce threats and raise awareness and understanding among stakeholders.

c. It assesses compliance with standards and control effectiveness.
d. It has the ability to evolve and react to external stimuli as they happen.
e. It is suitable for SMEs in terms of cost.
f. It is partially automated.

5. MIGRA Tool (Mosca, 2018:)
    a. It explores and assesses threats to business operations concerning the type of business.
    b. It does not determine what policies, standards, and controls are worth implementing to reduce threats or raise awareness and understanding among stakeholders.
    c. It assesses compliance with standards and control effectiveness.
    d. It has the ability to evolve and react to external stimuli as they happen.
    e. It is suitable for SMEs in terms of cost.
    f. It is automated.
6. NUIX (Rughani, 2017:)
    a. It does not explore and assess threats to business operations concerning the type of business.
    b. It does not determine what policies, standards, and controls are worth implementing to reduce threats or raise awareness and understanding among stakeholders.
    c. It does not assess compliance with standards and control effectiveness.
    d. It does not have the ability to evolve and react to external stimuli as they happen.
    e. It is suitable for SMEs in terms of cost.
    f. It is partially automated.
7. Archer (Archer, 2014:)
    a. It explores and assesses threats to business operations concerning the type of business.
    b. It does not determine what policies, standards, and controls are worth implementing to reduce threats or raise awareness and understanding among stakeholders.
    c. It assesses compliance with standards and control effectiveness.

d. It does not have the ability to evolve and react to external stimuli as they happen.
e. It is suitable for SMEs in terms of cost.

8. IRM Security (Ani, He and Tiwari, 2019:)
    a. It does not explore and assess threats to business operations concerning the type of business.
    b. It does not determine what policies, standards, and controls are worth implementing to reduce threats or raise awareness and understanding among stakeholders.
    c. It does not assess compliance with standards and control effectiveness.
    d. It does not have the ability to evolve and react to external stimuli as they happen.
    e. It is suitable for SMEs in terms of cost.
    f. It is partially automated.
9. RiskIQ (Schwarz and Creutzburg, 2021:)
    a. It does not explore and assess threats to business operations concerning the type of business.
    b. It does not determine what policies, standards, and controls are worth implementing to reduce threats or raise awareness and understanding among stakeholders.
    c. It does not assess compliance with standards and control effectiveness.
    d. It does not have the ability to evolve and react to external stimuli as they happen.
    e. It is suitable for SMEs in terms of cost.
    f. It is partially automated.
10. SATAM (Sharma, Vidalis, Menon, Anand, and Kumar, 2021:)
    a. It explores and assesses threats to business operations concerning the type of business.
    b. It determines what policies, standards, and controls are worth implementing to reduce threats and raise awareness and understanding among stakeholders.
    c. It assesses compliance with standards and control effectiveness.
    d. It has the ability to evolve and react to external stimuli as they happen.

e. It is suitable for SMEs in terms of cost.
f. It is automated.

However, the threat can have an impact on various levels of the business of an organization. The generic framework for the e-commerce business of an organization represents a fine example of all these different levels. This comparison illustrated which model/methodology can analyse threat agent identification, vulnerability identification, assets of an organization, and stakeholder identification of an organization and follows the ISO standards & control (17799 & 15408). Finally, it illustrated which type of approach is used, such as the probabilistic and hierarchical approaches to analyse identified threats next to the real-time informational environment. The literature review identified some limitations and gaps in the existing models and methodology, briefly illustrated in table 3. The existing models are missing a business analysis factor under which environment or platform a business operates. The existing models/methodologies follow the waterfall development model for threat assessments, but this approach is unsuitable for all platforms. They cannot address all different security layers such as firewall, IDS and IPS, etc. They either follow a strategic approach (formulation and implementation of significant goal based on consideration of resources and assessments of internal and external environments in which the organisation operates); or a tactical approach (the best tactics or method for each situation that arises while analysing the threats) or both for threat/risk analysis. The existing model/methodology could not provide automatic features for analysing threats and operating in a centralized manner. The existing models lack the motivation factor for the identified threats (Sharma, Vidalis, Menon, Anand and Pourmoafi, 2021).

Models/methodology	**Threat agent identification**	**Vulnerability identification**	**Assets**	**Stakeholder identification**	**ISO standards & control (17799 &15408**	**Probabilistic approach**	**Hierarchical approach**
CRAMM(Boban, 2010)	×		✓	×	✓ & ×	✓	✓
ARiES(Bagstad et al., 2011)	×	×	✓	×	×	✓	×
Pfleeger(Pfleeger, 2009)	×	✓	✓	×	×	✓	×
Caroll(Xu et al., 2011)	×	✓	✓	×	×	✓	×
Summers(Summe	✓	✓	✓	×	×	✓	×

rs, 1997)							
COBRA(Addison, 2002)	×	✓	✓	×	✓ & ×	Not applicable.	Not applicable.
FRAP(van Royen et al., 2008)	×	✓	✓	✓	×	×	×
OCTAVE(Alberts, Dorofee and Allen, 2001)	✓	✓	✓	✓	✓ & ×	✓	✓
TAME(Vidalis and Jones, 2003)	✓	✓	✓	✓	×	×	✓
Jones(A Jones, 2002)	✓	×	×	×	×	×	✓
Amenza(Ingoldsby, 2010)	✓	×	×	✓	×	✓	✓
VIM(Tevis and Hamilton Jr, 2006)	✓	×	✓	×	×	×	✓
SATAM (Sharma, Vidalis, Menon, Anand and Kumar, 2021)	✓	✓	✓	✓	×	✓	✓

Table 3 Comparison of methodology and model(Boban, 2010) (Bagstad et al., 2011) (Pfleeger, 2009) (Xu et al., 2011)(Samuel, Aalab and Jaskolka, 2020)(A Jones, 2002; Vidalis and Jones, 2005, 2006; Gollmann, 2010; Sharma, Vidalis, Anand, et al., 2021; Sharma, Vidalis, Menon, Anand and Kumar, 2021).

In table 3, the comparison is carried out based on the approaches, technology and attributes used by the number of models and methodologies. A tick indicates that the model is compatible with performing the operation, while the cross tick indicates they are inconsistent with such approaches. Similarly, both a tick and cross together indicates that the upgraded version of the model can perform the operation for a network's threat and vulnerability analysis. The table is designed and implemented based on the analysis of existing models and methodological approaches used to determine the threat agent groups from the network. The 'Not applicable' means that the model and methodology do not use particular approaches or characteristics.

The table compares different models/methodologies based on their approach to threat agent identification, vulnerability identification, stakeholder identification, ISO standards and controls, probabilistic approach, and hierarchical approach. It also indicates the inclusion or exclusion of certain elements, such as assets and the applicability of certain factors in each model/methodology.

- **Threat agent identification:** Indicates whether the model/methodology includes the identification of threat agents (whether it is marked as a checkmark (✓) or a cross (✗).
- **Vulnerability identification:** Indicates whether the model/methodology includes the identification of vulnerabilities.
- **Assets:** Indicates whether the model/methodology includes the identification of assets.
- **Stakeholder identification:** Indicates whether the model/methodology includes the identification of stakeholders.
- **ISO standards and control (17799 & 15408):** Indicates whether the model/methodology considers ISO standards and controls.
- **Probabilistic approach:** Indicates whether the model/methodology follows a probabilistic approach.
- **Hierarchical approach:** Indicates whether the model/methodology follows a hierarchical approach.

Based on the information provided in the table, each model/methodology is evaluated and marked accordingly for these different aspects. It is important to note that the table provides a comparative overview of different models/methodologies based on specific criteria. Further details about each model/methodology would be necessary to understand their specific characteristics and approaches in more depth :

1. Threat agent identification: This element refers to the inclusion or exclusion of the identification of threat agents in the model/methodology. Threat agents are individuals, groups, or entities that have the potential to exploit vulnerabilities and pose a threat to an organization's assets or systems. Models/methodologies that include threat agent identification aim to understand potential adversaries' characteristics, motivations, and capabilities.
2. Vulnerability identification: This element indicates whether the model/methodology includes the identification of vulnerabilities. Vulnerabilities are weaknesses or flaws in a system or application that threat agents can exploit. Identifying vulnerabilities is

crucial for understanding the potential avenues of attack and taking appropriate measures to mitigate them.

3. Assets: The inclusion or exclusion of assets refers to whether the model/methodology considers the identification of assets. Assets are a system's valuable resources, information, or components that need protection. Identifying assets helps prioritize security efforts and allocate resources effectively to safeguard the most critical components.
4. Stakeholder identification: This element denotes whether the model/methodology includes the identification of stakeholders. Stakeholders are individuals, groups, or entities with an interest or involvement in the security of the system. Identifying stakeholders helps understand their perspectives, concerns, and roles in the security process, enabling better communication and collaboration.
5. ISO standards and control (17799 & 15408): This element indicates whether the model/methodology takes into account ISO standards and controls, specifically ISO 17799 and 15408. ISO 17799, also known as ISO/IEC 27002, provides guidelines and best practices for information security management. ISO 15408, also known as Common Criteria, is an international standard for evaluating and certifying the security of IT products and systems. Considering these standards ensures adherence to established industry practices and compliance requirements.
6. Probabilistic approach: The presence or absence of a probabilistic approach signifies whether the model/methodology employs probabilistic techniques in its analysis. A probabilistic approach involves assessing risks and threats based on probabilities, likelihoods, and statistical data. It allows for the quantitative analysis of threats and their potential impact, providing a more comprehensive understanding of the security landscape.
7. Hierarchical approach: Including or excluding a hierarchical approach indicates whether the model/methodology follows a hierarchical structure for organizing and analysing threats and vulnerabilities. A hierarchical approach involves categorizing threats and vulnerabilities based on their severity, impact, or priority. It helps prioritise mitigation efforts and allocate resources based on the criticality of the identified risks.

Each model/methodology in the table is evaluated based on these elements. A checkmark (✓) indicates the element is included, while a cross (✗) indicates its exclusion. By considering these elements, organizations can choose a model/methodology that aligns with their specific requirements and priorities for threat analysis, vulnerability assessment, stakeholder engagement, and compliance with ISO standards.

2.7 Benchmark for Evaluation Experiments

Benchmark experiments are empirical techniques for analysing statistical learning algorithms on one or more datasets. They can be used to evaluate a group of algorithms, identify the optimal hyperparameters for an algorithm, or assess an algorithm's sensitivity. The structural requirements that account for the distribution of data processing capabilities among structural units and components located in the bottom tier of the structural configuration are used to derive performance benchmarks. Researchers can learn about the precision of non-experimental research designs through experimental benchmarking. To calibrate bias, one might specifically compare observational data to experimental findings. An experiment provides the researchers with an objective estimation of their parameter of interest under normal circumstances. The results of the observational study can then be compared to this estimate.

Models	**Characteristics/features**	**Advantages**	**Disadvantages(shortcomings and limitation)**
PASTA	Determining mitigating techniques effectively; they are effectively working for risk management; maintaining good relations and collaboration with stakeholders; built-in prioritization of threat agents; time-consuming process but has rich in the documentation.	It aims to bring business objectives and technical requirements together; it uses seven stages, each with multiple activities to do the analysis.	It is not static; just a one-time assessment can be achieved; It does not operate in a vacuum; security testing deliverables are adversarial; integrated disciplines are needed via a unifying methodology.

STRIDE	Determining mitigating techniques effectively; easy to use but time-consuming as well.	It evaluates the system detail design. with the help of designing data-flow diagrams (DFDs), STRIDE is cut off to identify system entities, events, and system boundaries.	Microsoft adopted it in 2002, but unfortunately, Microsoft no longer maintains STRIDE; It is implemented as part of the Microsoft security development lifecycle (SDL).
OCTAVE	Determining mitigating techniques effectively; they are effectively working for risk management; maintaining good relations and collaboration with stakeholders; built-in prioritization of threat agents; effective results repeatedly; explicitly designed in a scalable manner; time-consuming process but rich in the documentation.	Automatically update risk exposure; maintain accurate and up-to-date risk profile; reduce attack surface and promote consistent security policy; produce measurable security; align mitigation strategy.	It isn't easy to use; it is not thoroughly documented as compared to other models. virtually no access to existing data regarding the methodology.
Trike	Determining mitigating techniques effectively; effectively working for risk management; maintaining good relations and collaboration with stakeholders; built-in prioritization of threat agents; time-consuming process but has rich documentation; encourages collaboration among stakeholders; components	Open-source threat modelling process; both the application implementation and capabilities are determined; reconstruction of the model can be achieved with the help of data flow diagrams.	It is used to satisfy the security auditing process; they construct a risk model based on assets, roles, actions, and calculated risk exposure.

	working in an automated manner.		
Quantitative TMM	Built-in prioritization of threat agents; components are working in an automated manner; consistent results.	It aims to address a cyber-physical system with complex interdependences concerning its components; portable.	They are not supporting automation and tool integration with SDLC.
CVSS	Built-in prioritization of threat agents; consistent results; components working in an automated manner; the threat agent's calculations are not in a transparent manner.	It produces a numerical severity score; the CVSS score helps to determine the threat agent attributes.	Insufficient documentation: CVSS score is not a measure of actual risk; this model does not consider the network's critical threat intelligence environment.
LINDDUN	Determining mitigating techniques effectively; built-in prioritization of threat agents; time-consuming and high complexity.	Likability; anonymity; identifiability; non-repudiation; confidentiality; disclosure of information	Privacy-preserving authentication; access control technique.
Attack Tree	Determining mitigating techniques effectively; consistent results; easy to use.	Capable of providing risk estimates for specific situations, a conceptual diagram showing how an asset or target might be attacked.	They are static and have, the ability to scale resources.

Table 4: Strengths and Limitations of Models and Methodology (A Jones, 2002; Vidalis and Jones, 2003; Fresner et al., 2017; Yu and Zhang, 2017; Pandelică, 2020; Sharma, Vidalis, Menon, Anand and Pourmoafi, 2021) (Sharma, Vidalis, Menon, Anand and Kumar, 2021)**.**

The table provides a comparison of different threat modelling methodologies/models, highlighting their characteristics, advantages, and disadvantages of each model in more detail.

PASTA stands for process for attack simulation and threat analysis. It effectively determines mitigating techniques, promotes risk management, and emphasizes stakeholder collaboration. It prioritizes threat agents and involves a time-consuming process but yields rich documentation. PASTA aligns business objectives with technical requirements and follows a structured approach with seven stages for analysis. However, it is not a one-time assessment and requires integrated disciplines, and its security testing deliverables can be adversarial.

STRIDE, which stands for spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege, evaluates system detail design. It is relatively easy to use but can be time-consuming. STRIDE utilizes DFDs to identify system entities, events, and boundaries. Microsoft initially adopted STRIDE in 2002, but it is no longer actively maintained and has been integrated into the Microsoft security development lifecycle.

OCTAVE (operationally critical threat, asset, and vulnerability evaluation) is another effective methodology for risk management. It promotes collaboration with stakeholders, prioritizes threat agents, and provides repeatable results. OCTAVE is explicitly designed to be scalable and time-consuming, resulting in comprehensive documentation. It offers benefits such as automatic updating of risk exposure, maintaining accurate risk profiles, reducing attack surface, and promoting consistent security policy. However, OCTAVE can be complex to use, lacks extensive documentation compared with other models, and may have limited access to existing data.

Trike is an open-source threat modelling process that effectively determines mitigating techniques and encourages collaboration among stakeholders. It involves a time-consuming process but results in rich documentation. Trike allows for the determination of application implementation and capabilities, as well as the reconstruction of models using DFDs. It is commonly used for security auditing, constructing risk models based on assets, roles, actions, and calculated risk exposure.

Quantitative TMM (threat modelling methodology) prioritizes threat agents and operates in an automated manner, providing consistent results. It explicitly addresses cyber-physical systems with complex interdependencies and offers portability. However, it does not support automation and tool integration with the software development lifecycle.

CVSS (common vulnerability scoring system) incorporates built-in prioritization of threat agents and components working in an automated manner. It produces a numerical severity score that helps determine the attributes of threat agents. However, CVSS has limitations, such as insufficient documentation, as the score itself is not a measure of actual risk. Additionally, it does not consider the critical threat intelligence environment of the network.

LINDDUN focuses on determining effective mitigating techniques, prioritizing threat agents, and addressing aspects such as privacy-preserving authentication and access control. However, it can be time-consuming and complex, and it lacks features such as likability, anonymity, identifiability, non-repudiation, and disclosure of information.

Finally, Attack Tree is an effective methodology for determining mitigating techniques with consistent results and ease of use. It provides risk estimates for specific attack scenarios and visualizes how assets or targets can be attacked. However, Tree has limitations in terms of scalability and the ability to scale resources.

In summary, each threat modelling methodology/model has its own characteristics, advantages, and disadvantages. It is essential to consider the specific requirements and context of the security assessment to choose the most suitable approach.

2.8 Conclusion

The study and analysis of existing models and methodology have shown that the threat impact on the organization is not practical. Some models analyse the data collected during the threat assessment but cannot address the attributes of threat agents and critical threat intelligence feed to it. Some models claim that they can identify the motivation of threats. Unfortunately, they are not able to address it effectively. Our comparison study of the model shows that the TAME model is much better than the existing models. If TAME performs the analysis

automatically with the help of some tools such as TensorFlow, then complexity will be effective and more optimized.

In conclusion, some findings generated by the models/methodology are incorporated and contracted at several points to the determination rendered by the model. Therefore, it is suggested that the existing model/methodology is inadequate compared with threats identified in a network of informational environments. So, it is recommended that the cybersecurity team consider the attribute carefully while generating the final reports.

The growing number of cybercrime incidents cost the worldwide economy more than $1 trillion, more than 50% of a 2018 report that put global losses approximately $600 billion. It is the recent data valid untill December 2020. Based on these figures, it is apparent that existing models and methodologies cannot address the modern threats in the network of real-time informational environments. In the future, modern security methods need to acknowledge the recent threat agents and develop a new approach to eliminate the threat cost-effectively and optimize the complexity. The proposed model must understand how the business uses e-commerce and be capable of addressing the multidimensional matrix of information security. The future model will take into consideration the spiral development approach, the operational approach (functional level strategy leads to operational process means analysing the threat from situational awareness data and comparing it with the historical data, which helps to improve the effectiveness or efficiency to identify the hazards in a network) and operating in a distributed manner while performing for threat analysis. Maintaining a database consisting of profiles of threat agents and a critical intelligence feed is necessary, which helps evaluate newly identified threats in a network. It can also automatically assess the motivation, opportunity, and capability of the hazards identified in a network. Therefore, complexity will be more effective.

Chapter – 3 Research Methodology and Specification of Semi-Automatic Model

This chapter describes the methodology used to design the research required to implement the model for this thesis. The theory outlined in Chapter 2 has an impact on the models that were chosen. This chapter constructs the central argument of this research, drawing upon the findings from the literature search as presented in Chapter 2. Concurrently, it introduces the semi-automatic threat assessment model to the reader. A comprehensive overview of the activities and processes of SATAM is provided, supported by high-level diagrams and figures. Appendix I lists the inputs to the model, while GitHub link provided in result section presents the outputs.

After elucidating the model, an illustrative scenario demonstrates the potential benefits an enterprise could derive by employing SATAM in contrast to an existing threat assessment approach. It is important to note that this simplified scenario is not intended to fully convince the reader of the model's efficiency. Rather, its purpose is to pique the reader's interest and stimulate curiosity about the effectiveness of the model and its capacity to enhance enterprises comprehension of cybersecurity aspect.

3.1 Introduction

The research methodology refers to the overall approach and framework used to conduct the study. It outlines the systematic process followed to collect, analyse, and interpret data in order to address the research objectives and answer the research questions. In the context of the thesis, the research methodology involves the specific methods, techniques, and procedures employed to investigate the "Near Real-Time Semi-Automated Threat Assessment of Information Environment" in the field of cyber threat intelligence (CTI).
The research methodology for developing a threat assessment model in cybersecurity can be divided into several steps:

a. **Problem identification:** The first step is identifying the problem the model aims to solve. This could be the lack of a comprehensive approach to threat assessment in cybersecurity that considers live data.

b. **Literature review:** The second step is to conduct a comprehensive literature review to identify existing models, frameworks, and approaches for threat assessment and data stream in cybersecurity. This review should help identify gaps and limitations in existing models and inform the development of the model.
c. **Conceptual framework development:** Based on the literature review, the conceptual framework for the model should be developed. This framework should include the critical components of the model, such as the data sources, algorithms, and metrics that will be used to assess the threat agent groups.
d. **Data collection:** The next step is to collect data to validate and refine the model. This could involve collecting threat intelligence data, network traffic data, and other relevant data sources to inform the development and testing of the model.
e. **Model development and testing:** The model should be developed and tested using the data collected in the previous step. The model should be refined and adjusted based on testing results and feedback from cybersecurity experts.
f. **Evaluation:** The final step is to evaluate the effectiveness of the model. This could involve comparing the model's performance to existing models, conducting a cost-benefit analysis, and assessing the practicality and scalability of the model.

The research methodology for developing a model in cybersecurity should involve a comprehensive approach that includes problem identification, literature review, conceptual framework development, data collection, model development and testing, and evaluation. This methodology should help ensure that the model is effective, practical, and scalable and addresses the limitations of existing approaches to threat assessment in cybersecurity.

3.2 Research Approaches

Research is the art of conducting scientific research to discover new information. The research was referred to as a “systematised effort to gather new knowledge”(Kothari, 2004). Another approach to describe research is a systematic, scientific search for answers to a particular issue. The research methodology can be divided into categories, i.e., quantitative, qualitative, assorted, etc. Furthermore, the quantitative approach illustrates the experimental measurements of the model.

In contrast, qualitative research illustrates the theoretical measurements of the attributes of the threat agents, and finally, the assorted is the mix of both experimental and theoretical

analysis and implementation design. The SATAM model was cast-off all the research methodologies for designing and implementing the architecture. The detailed explanation of these approaches used for the model is as follows:

a. The number model and methodology are studied and analysed in the theoretical approach. While conducting analysis, the methods and tactics employed by these models and methodologies aid in determining the threat agent groups and their shortcomings and limitations. Research identifies the gaps and loopholes while completing the threat assessment for an organization's network based on the approach used by the existing model and methodology. The thesis identifies the strategy to address RQ-1 (research question) in accordance with the literature review analysis of models. The blueprint of the simulation architecture has been created, and the fundamental requirements for developing the SATAM have been determined.

b. Using a number of virtual machines on the blue net, red net, and black net teams concurrently, the simulation architecture has been constructed in the experimental technique on the server's cyber range. All of the architecture's components have been connected through a secure communication channel enabled by the firewall, allowing for secure communication between them. Based on the severity of the attacker groups on the server, the DMZ is additionally installed on the server's cyber range. Installing DMZ on a server is done chiefly to handle attacks that have a high impact on assets and to manage the intensity of the attackers. The simulation architecture has successfully undergone validation and verification.

c. Finally, chapter 2 provides a full explanation of the many ways method that were used after all the research was done and they had been analysed and discarded from the models and methodology. The experimental outcomes of the simulation architecture from the experimental methodology come together in such a way that the model is installed on the server with all of the software and hardware necessary for the threat and vulnerability analysis of the threat agent groups identified on the specific network of an organization.

The demands and requirements of the threat assessment serve as the foundation for the difficulties defined by this research. The literature review's complications and results serve as

the foundation for the research questions. The research questions are used to derive the research aim, which is subsequently confirmed. Various models' assessed cybersecurity maturity level is then utilized to offer suggestions and an action plan to achieve higher levels. The development of a comprehensive cybersecurity framework follows. The work is regarded as applied research because it tries to resolve a real-world cybersecurity problem in an existing model.

3.3 Research Purpose

Utilizing scientific methods, the research aims to provide answers to open-ended issues. Depending on its objective, research can be categorized as preliminary, pictorial, or interpretive.

- **Preliminary:** This is a term that can be defined or denotes the study or analysis of a new topic or term in an illustrative or explanatory manner. Such a study aims to find existing technologies and methodologies that can be used to build and implement a model and methodology. Based on the preliminary information, the model's data flow diagram has been created.
- **Pictorial or interpretive:** The definition of pictorial is to ascertain the answers to questions such as who, what, how, and when technology implementation has been accomplished. The strengths and weaknesses/limitations of the current models and methods have been recognized with the use of visual study, and the design and implementation of the model process have been based on these specifications.

The research methodology used for the thesis combines preliminary and pictorial research conducted during the literature review. An exploratory research approach is used in the early stages to identify existing frameworks and models for cybersecurity, determine existing cybersecurity concerns and challenges, and gain fresh insights into the study topic. First, the information obtained from the exploratory research was used to identify research gaps and develop research questions. To determine how to estimate the cybersecurity maturity model, enable proactive cybersecurity, and apply a cybersecurity framework for threat assessment.

The primary aim of this research is to utilize the semi-automatic threat assessment model (SATAM) to enhance threat assessment methodologies in the field of cybersecurity. Specifically, the research seeks to achieve the following objectives:

a) Evaluate the effectiveness of the SATAM model in identifying and analysing potential threats to an organization's information systems and networks.
b) Investigate the applicability of the SATAM model across various industries and sectors, considering their unique cybersecurity challenges and requirements.
c) Enhance the SATAM model by incorporating additional risk assessment factors and metrics, allowing for a more comprehensive and accurate evaluation of threats.
d) Assess the reliability and validity of the SATAM model in predicting and mitigating cybersecurity incidents and vulnerabilities.
e) Explore the integration of advanced technologies, such as machine learning, into the SATAM model to improve threat detection and response capabilities.
f) Provide practical recommendations and guidelines for organizations to implement the SATAM model effectively and integrate it into their existing threat assessment frameworks.

By addressing these research objectives, this study aims to contribute to the advancement of threat assessment practices in cybersecurity and support organizations in their efforts to proactively identify and mitigate potential threats to their critical information assets.

3.4 Research Blueprint

According to (Yin et al., 2017), the research blueprint (strategy) follows the primary five action plans, which are a literature survey, fundamental analysis, methodologies (historical), case study, and experimentation (conducted). The order of blueprints is determined by the need for building and implementing a threat agent analysis model. In this phase, plan development is carried out based on the research questions identified in Chapter 2. The plan's execution will be followed by the research item identified in the research question section. The first plan is to simulate the architecture design on the cyber range based on model requirements, followed by related work accomplished during the research and analysis of a number of models and methodologies. In addition, the semi-automatic function will be introduced using a case study obtained while analysing the models and methodology. To

offer automatic characteristics in the model, the Jupyter Notebook's Python libraries were widely employed to interface with data stream gathered during the threat assessment of the (ESXI) server. The primary or required attributes from the PCAP file will be extracted based on the threat assessment for the information environment. The threat agent group profiling will be archived, and an incident report will be created. Finally, the experiment will be carried out in accordance with the threat and vulnerability evaluations. Using the same research technique to answer all of the RQs will aid in coordinating the job, saving both time and effort.

3.5 Research Sustainability and Uncertainty

The study's sustainability and uncertainty can be established by soliciting feedback/comments and suggestions from research investigators and disseminating the findings in journals and conferences. Even the auditor process will be carried out by the supervisor, co-supervisors, and cybersecurity specialists, and based on the feedback and suggestions gained during such process, verification and validation of the model may be accomplished. This study's construct validity was improved by using multiple sources (such as data collection through interviews and documents) and review by key informants. Additionally, to increase the reliability, the results were documented using easily accessible information sources, such as online databases. Some of the study's data was not disclosed because of sensitivity issues, which restricted its accessibility and reproducibility for other researchers.

The model is a comprehensive framework used to assess and manage cybersecurity risks. A critical aspect of the model is its ability to address sustainability and uncertainty, which are vital considerations in ensuring the effectiveness and relevance of cybersecurity strategies.

Sustainability in the context of cybersecurity refers to the ability of a security framework to adapt and evolve over time in response to changing threats and risks. Cybersecurity threats are constantly evolving, and organizations must keep up with the changing landscape to maintain their security posture. The model promotes sustainability by emphasizing the importance of continuous monitoring and assessment of cybersecurity risks and the need for regular updates and adjustments to security strategies and protocols.

Uncertainty is another essential consideration in cybersecurity, as threats and risks can be unpredictable and difficult to anticipate. The model addresses uncertainty by incorporating a

risk-based approach that emphasizes the importance of identifying and prioritizing high-risk areas and the need for contingency planning and response strategies. The model also emphasizes the importance of collaboration and communication between stakeholders, including security teams, management, and other relevant parties, to effectively manage and mitigate risks.

In addition, the model encourages the use of advanced technologies and tools, such as machine learning, to help organizations better anticipate and respond to cybersecurity threats. These technologies can provide valuable insights into emerging threats and help organizations avoid potential risks.

Overall, the model provides a comprehensive framework for addressing sustainability and uncertainty in cybersecurity. By promoting a risk-based approach, emphasizing the importance of continuous monitoring and assessment, and encouraging collaboration and the use of advanced technologies, the model can help organizations stay ahead of the evolving cybersecurity landscape and maintain their security posture over time.

3.6 Research Process

A set of steps is included in the research process to do research. The pertinent literature was evaluated from journals, conference proceedings, theses, technical reports, standards, and open-access sources. The outcomes of the actions carried out during the research process were published in papers for conferences and scholarly journals. In this study thesis, results were also collated and summarized. The model delineates collecting the data stream or network traffic from the server's name ESXi at the University of Hertfordshire in the cybersecurity laboratory. The model is able to address the threat assessment for the threat agents of any information environment. This data collection can be consummate with the help of several software tools such as 'SolarWinds Deep Packet Inspection and Analysis, Paessler Packet Capture, ManageEngine NetFlow Analyzer, Omnipeek Network Protocol Analyzer, Tcpdump, WinDump, Tshark, and Wireshark' (Alomar et al., 2020). Chapter 2 describes the types of data collected from the network to assess the threat agents identified in an informational environment. The capabilities of the collection tools, also described in detail with the help of the literature review in the previous chapter, help me select the mechanism for collecting data streams from the university server. In this work, I have used the Wireshark tool to collect the data from the server. The impetus stipulates the Wireshark tool for

collecting data because it provides the facility to save the collected data in a .CSV format file (Mahmud et al., 2018). Comparing the available tools, the extraction of information about vulnerable ports by threat agents from the captured data on the small server appears most efficient when utilizing .CSV formatted files. This approach allows for easy unsheathing of critical insights and vulnerabilities from the dataset (the uprooting of information about the vulnerable ports perpetrated by threat agents on the captured data from the little server utilitarian to be unsheathed from .CSV formatted files compared to the other tools available, showcases the unparalleled efficiency and ease of extracting critical insights and vulnerabilities from the dataset.) To ascertain the methodology illustrated in the previous chapter, threat assessment for the collected data from the server are achieved by several phases followed by the semi-automatic model.

- Phase 1- Extraction of threat agent attributes from data stream.
- Phase 2- Extraction of threat agent source and destination IP address.
- Phase 3- Extraction of CVE list based on threat agent source IP address.
- Phase 4- Implement the vulnerable ports for the identified CVE list of threat agents.
- Phase 5- Implement the threat agents based on the CVE list of the NIST database.

3.7 Overarching Research Methodology

The overview of the research methodology in accordance with the existing threat assessment models and methodologies, it is evident that they are inadequate for addressing the requirements of a system like those discussed in chapter 2. Despite considerable discourse surrounding the current model and methodologies, a clear differentiation between threat and threat assessment is still lacking. Following an analysis of the prevailing model and methodologies, a more appropriate approach tailored to datasets derived from the EXSI server at the University of Hertfordshire was developed. It should be noted that all the assessed frameworks adhered to the waterfall development model, which proved to be unsuitable for handling datasets from the EXSI server. These datasets are inherently sensitive and subject to frequent changes. Because of their characteristics, as well as their lifecycle and global scope, a waterfall assessment model would be overly rigid and slow in its application. This would demand significant time and effort to yield results, of which only a portion would prove beneficial to the business conducting the assessment. Additionally, the examined

approaches overlook a crucial factor: the incorporation of business analysis to comprehend the operational environment in which the business functions.

Another potential approach for development is to consider the spiral development method. However, even this approach imposes constraints on users by prescribing a specific sequence for conducting various stages of the model. My true aim is to empower users to alter their thinking and approach in real-time, maximizing flexibility. I want them to be able to adjust experiment parameters on-the-fly from any point in the process without needing to start over. In terms of development principles, my goal is to achieve strong cohesion and loose coupling between different steps. Additionally, the model must comprehensively address all security layers within the system, including firewalls, intrusion detection systems, and cybersecurity policies. It must also embody simplicity, robustness, ease of control, adaptability, and effective communication. The proposed model has been named SATAM (Semi-Automatic Threat Assessment Model). Grounded in thorough study and research analysis, a model is seen as a set of steps for task execution, while a methodology comprises tools or research methods that translate management theory into practical application. Both internal and external stakeholders play an active role throughout the assessment process, with specific stakeholder elaboration to be provided later in this thesis.

Each activity consists of multiple processes, many of which can occur concurrently based on available assessment resources. The output of one process can serve as input for another, or the output of one process may influence and alter the input of another, and vice versa. The SATAM model is designed to be an ongoing endeavor once applied to a system, as continuous attention is required to ensure that countermeasures remain relevant and effective throughout the ongoing process. Ultimately, SATAM aims to assist security practitioners in determining the appropriate level and allocation of security measures within the organizational structure of the system. The methodology has been presented in various SCI journals and conferences across Europe and the United States. Different phases of the methodology have been presented at different conferences and within SCI journals. The methodology examines both organizational and technological aspects to construct a comprehensive overview of the threats faced by a company. The activities of the methodology encompass the subsequent processes. The list of activities carried out to design

and implement the model can be assessed in a number of sub-activities, including the following:

Activity 1- Analysis of environment used by source and target machine.

The number of virtual machines deployed on the server is analysed in this activity in order to grasp the state of the art cast-off by any firm. Later, the communication channel will be examined to determine how each component of organization is used to transport information/data among them. Finally, the network's connection to the internet, i.e., the firewall utilized to guarantee security for the enterprise, is examined. The following sub-activities will be carried out for vulnerability identification and threat analysis:

1. Identifying vulnerable network ports using fundamental penetration testing methods.

2. Identifying the road map the threat agent uses to breach the network by executing a collection of protocols.

Activity 2- Research methodologies for identifying the components and technology needed to create a semi-automatic model.

The goal of this activity is to examine and analyse existing technology utilized by a variety of models and methodologies in order to comprehend the state of the art used to accomplish them. To carry out this task, the following sub-activities will occur:

1. The existing model will be studied and analysed in the literature review phase, with the primary goal of identifying the technology employed by them and the roadmap cast-off in order to evaluate the threat agent in an organization.

2. The next step is comprehending the various models' approaches to designing and implementing their model/methodology.

3. Identifying the current model and methods' weaknesses, advantages, and gaps is the final step. Based on the identification, building and constructing the semi-automatic model using the necessary tools and technologies would be possible. The simulated architecture will undergo validation and verification. The specifics of this activity will be discussed in chapters 2 and 3, where relevant work and research techniques are covered in depth.

Activity 3: Create and deploy the model's simulation architecture on the ESXi server.

The component of the model will be designed and implemented on the server using a number of VMs put on it in this activity. Based on the needs and gaps discovered during analysis of the current model and methods. This activity will have the following sub-activities:

1. Analysis of the number of tools for capturing the data stream on the server, i.e., information gathering. In this activity, the tool identification will be determined for the model based on the semi-automatic design requirements.

2. Determine the optimal tool for vulnerability analysis based on the semi-automatic model requirements. In this activity, I will evaluate the vulnerable port identification list of common vulnerabilities exposures (CVEs) linked with the target machine.

3. Using the CVE list, determine the threat agent's environment, attack vectors cast-off by the threat agent, prerequisites inputs, and potential output.

Activity 4: Threat assessment (evaluation)

Numerous experiments will be conducted in this activity to evaluate the model. With the aid of penetration testing phases, the simulation architectural communication channel will first be validated to assess connectivity (e.g., by running a ping command to each component). There are a number of different sub-actions that will be completed for the evaluation, including the following:

1. The PCAP file-based data gathering from the server.

2. Extracting the necessary attributes from PCAP files in order to learn more about the threat agent.

3. Running the extraction-related Python code to provide the model with a semi-automation feature.

Activity 5: Calculating the Threat agent and attributes

With the aid of a Python script, the semi-automatic model in this activity will extract the necessary attributes from the PCAP files and identify the source IP, destination IP, the

protocol used, the active layer, the source port, the location of the threat agent (longitude and latitude), and the internet service provider used by the threat agent. To analyse the calculation of the threat agent attribute, numerous sub-activities are carried out, including:

1. The motivation factor is established using a probabilistic approach in order to pinpoint the threat agent's motivation for infiltrating the network.

2. The opportunity factor is identified using the fundamentals of penetration testing to determine the weak points in the environment that allow threat agents to infiltrate an organization's network.

3. A variety of parameters, including time spent on the network, the highest protocol accessed, source port targets, and the sorts of activities carried out by threat agent groups, determine the capacity factor. The specifics of the traits are covered in the results and discussion section of chapter 4.

Activity 6: Vulnerability assessment

The vulnerable port will be determined in this activity, and the list of associated CVEs will be determined using Kali Linux. The identification of the environments utilized during network penetration, attack pathways, required input, and potential output is analysed using the CVE list.

Activity 7: Mitigation of impact and threats

The impact of the threat agent on the business's assets will be determined in this activity, and mitigation strategies can be adopted or proposed to the company based on the impact and the approach used to enter the network.

A comprehensive discussion and high-level overview of the aforementioned activities and processes can be found in the results section of subsequent chapters. The numerical labeling assigned to both activities and processes serves a purely presentational purpose, aiding in the comprehension of data flow within the methodology. These numerical labels do not indicate any form of prioritization in the execution of activities or processes within the framework.

Depending on the assessor and the available data for assessment, different pathways may be pursued in each cycle of the methodology's execution.

In the initial phase of the framework, the organizational target area is identified and analyzed. This facilitates the identification of various stakeholders involved in different processes. The information gathered up to this point aids in delineating the system's boundaries, which must be safeguarded against cyberattacks. This necessity leads to a subsequent process: identifying active or inactive threat agents that will be targeting assets. With information from other methodological processes, the framework is equipped to carry out asset identification. The culmination of information from these aforementioned processes contributes to the creation of an initial set of security requirements.

In the later stages of the framework, the previously identified threat agents are examined, and their capabilities are assessed. This assessment permits the establishment of a preference structure based on their significance to the organization. Drawing from all preceding activities and processes, I possess adequate information to conduct a vulnerability analysis, culminating in an evaluation of complexity, accounting for agent capabilities. Data gathered from the activities and processes can be harnessed to construct scenarios involving identified threat agents, targeting individual assets or processes by exploiting vulnerable ports. The outcomes of these activities include system models and attack scenarios, which are pivotal in the threat identification process, and a secondary set of security requirements. Stakeholders evaluate the outcomes of each process, computing the impact of each identified threat across the organization's various tiers. Subsequently, a threat statement is generated and presented to the organization's stakeholders for their consideration.

SATAM distinctiveness lies in the interplay among different stages and the diverse steps within the model. There isn't a singular predetermined path for executing the methodology. The model has the flexibility to choose a path based on the constraints of the cybersecurity concern and their knowledge. It's not mandatory for the model to complete all steps to yield meaningful results. The course of action is contingent upon the analyzed system. Generally, simpler systems necessitate fewer steps, though more steps generally yield superior results.

The formal point of entry for the model is the Scope of activities and processes. Just as in experimental practices within the applied sciences, it is crucial to clearly define the

experiment's scope and boundaries. The formal point of culmination for the model is the evaluation stage. Here, the organization receives insights into each threat's impact on the enterprise, along with a shortlist of these threats. The shortlisting criteria consider the threat's importance, the organizational impact upon realization, and its complexity in relation to the system. Additionally, as an expansion of the methodology, a module could be developed to associate each threat with one or more countermeasures following established standards (ISO17799).

A proposed approach for implementing SATAM is outlined as follows:

- **Defining scope and assessment**: The initial step involves comprehensively describing the system's scope. This encompasses detailed information about the system, its environment, and business processes. Additionally, it entails identifying the various stakeholders involved. To aid in scoping, the process incorporates the identification and selection of threat agents.

- **Threat agent identification and attributes**: It focuses on identifying attributes related to threat agents. This process consolidates all variables to pinpoint and assess threats posed to the system. Vulnerabilities are analyzed, and threat agents are evaluated in the context of the system.

- **Scenario construction and system modeling**: Moving on to the next process, it involves constructing one or more scenarios (depending on the identified and filtered threats). The system under consideration is modeled using the details gathered in the initial stage. Models play a pivotal role in this step.

- **Stakeholder evaluation and scenario selection**: In the final process, stakeholders evaluate the outcomes of the experiments conducted. They determine which scenarios warrant further investigation. At this juncture, a comprehensive understanding of the system's potential vulnerabilities and threat impacts starts to emerge.

Upon completion of these activities, the system gains the capability to assess the impact of identified threats on various facets of its operation. This assessment yields a statement based on the prioritized order of threats. It's worth noting that this methodology can be iterated

multiple times. As stakeholders interact with the experiment outcomes and collaborate with model, additional aspects of the system could come to light. New variables might be introduced or excluded as necessary. The frequency of these iterations is flexible and can be adjusted based on user requirements. Each iteration is expected to provide more detailed insights and findings.

The overarching research methodology of the work described in the thesis primarily focuses on conducting a threat assessment of an information environment using a semi-automatic model. Here are the key steps and components of the methodology:

a. **Data collection:** The research process involves collecting data stream or network traffic from the ESXi server at the University of Hertfordshire's cybersecurity laboratory. The Wireshark tool is used to collect the data from the server, as it provides the ability to save the collected data in a .CSV format. Even any other tool can also be used for collecting the data based on the formatted of data required for extraction of information from it.
b. **Threat agent profiling:** The collected data is analysed to extract various attributes of the threat agents present in the information environment. This includes extracting threat agent attributes, source and destination IP addresses, CVE (common vulnerabilities and exposures) lists based on the source IP address and identifying vulnerable ports for the identified CVE list.
c. **Threat assessment phases:** The threat assessment is conducted through several phases implemented by the semi-automatic model. The phases include the extraction of threat agent attributes, source and destination IP addresses, CVE lists, vulnerable ports, and implementation threat agents based on the CVE list from the NIST (National Institute of Standards and Technology) database.
d. **Analysis and implementation of the system:** The study incorporates computer security researchers and cyberpsychology experts to address the research question of near real-time semi-automated threat assessment. The goal is to determine the motivation, opportunity, and capabilities attributes of threat agents and mitigate the threats governments and businesses face.
e. **Architecture of the system:** The system's architecture involves an ESXi server with different security zones (RED, BLUE, and BLACK), VMWARE CD, DNS, DHCP,

and firewall connections. The server stores the data and information of the University of Hertfordshire, and DMZ acts as a defence mechanism to prevent further damage from attackers.

f. **Threat agent identification and selection:** Threat agents are continuously identified and categorized based on their characteristics and nature. Attributes such as capability, opportunity, and motivation are considered for threat agent profiling.

3.8 Analysis and Implementation of the System.

The work described in this thesis has been carried out as part of a more comprehensive research that includes computer security researchers and cyberpsychology experts. As the research question for the "Near Real-Time Semi-Automated Threat Assessment of Information Environment" is CTI (cyber threat intelligence), data-driven threat agent profiling can be used for determining the motivation, opportunity, and capabilities attributes of threat agent under the context of a continuous threat assessment (Erola et al., 2017). The collaboration between computer security researchers and cyberpsychology experts allows for a multidisciplinary approach to understanding and analysing the complex nature of cyber threats. The computer security researchers bring technical expertise in analysing digital vulnerabilities and identifying potential cyber threats, while the cyberpsychology experts contribute insights into the psychological and behavioural aspects of threat actors.

By integrating these different perspectives, the research project seeks to enhance our understanding of the evolving threat landscape and develop effective strategies for mitigating cyber risks. The findings of this research will have practical implications for the development of proactive defence mechanisms and the formulation of targeted threat response strategies.

The threat remains of budding apprehension to governments and businesses organization, and it becomes an acute necessity for practical tools to help mitigate the threat. Modern risk assessment methods or models recognize a need to perform several threat assessments to identify/analyse various threats in the contemporary information environment. Suppose we do an iterative threat assessment for the network. In that case, the new type of threat agents identified in the data will be addressed quickly with the help of profiling, which the practitioners prepare every time while performing the threat assessments. Security concerns

and continuous threat assessments may help generate the paradox of warning to the cyber operations performed in the information environment. This thesis identifies the research gap in semi-automated information environments, consisting of large heterogeneous infrastructures hosting a large amount of data collected from different platforms (Deore and Waghmare, 2016). The different types of platforms mean the type of environment and the conditions the threat agent uses to attack the particular network. To analyse or identify the solution for such an issue of a large amount of data, decision aid tools should provide their understanding toward new traffic captured and critical intelligence feeds of the threats in real-time information environments.

In the modern knowledge-based, socially driven, virtual computing era, threat assessments are hindered by a lack of resources, complexity, and data size. Information environments are large heterogeneous infrastructures, hosting a large amount of data collected from different types of platforms with the help of several tools. A thesis will consider state of the art on threat agent analysis models and methodologies. At the same time, procedural and technical issues will be resolved by applying cyber analytics principles (Legg et al., 2015.)

The steadfastness of the model is to inaugurate a novel approach that will enable us to take advantage of the vast amount of data collected by the large number of platforms designed in order to identify suspicious traffic, malicious intentions, and network attacks in an automated manner.

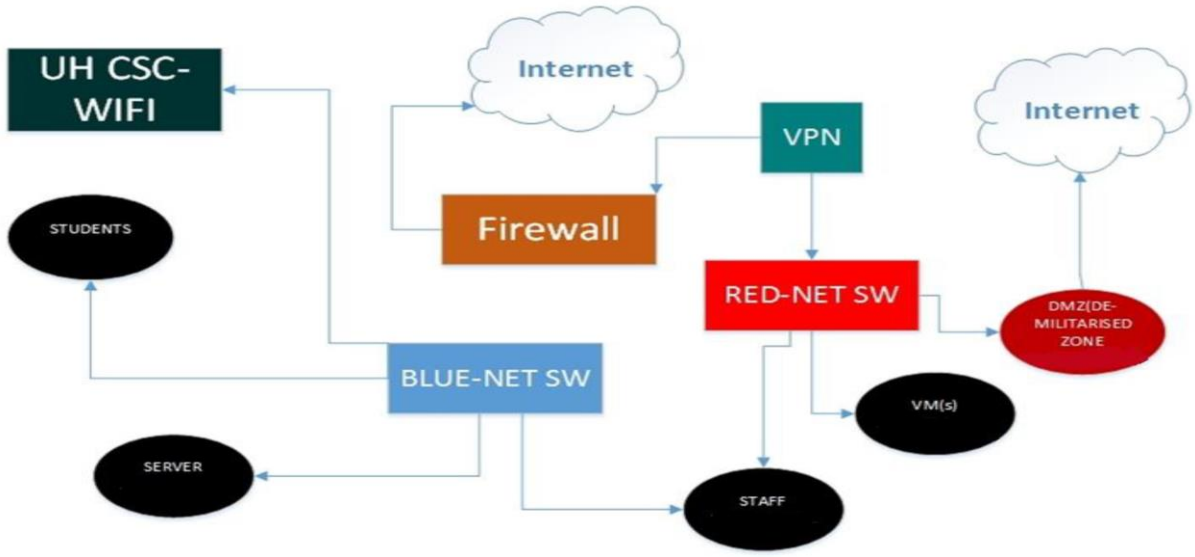


Figure 1 Penetrating Testing Set-up at Cybersecurity Laboratory.

3.9 Identification of threat agents from data stream

The action of gathering information about active and inactive threat agents working inside or outside the business area of the firm is referred to as “threat agent identification and selection.” In line with Summers (Baezner and Robin, 2017), threat agents should be continuously identified because their characteristics are continually changing. When necessary, information from various points of view will be gathered, merged, and threat agents will be named and categorized in accordance with their nature and the enterprise.

- Threat agent capability
- Threat agent opportunity
- Threat agent motivation

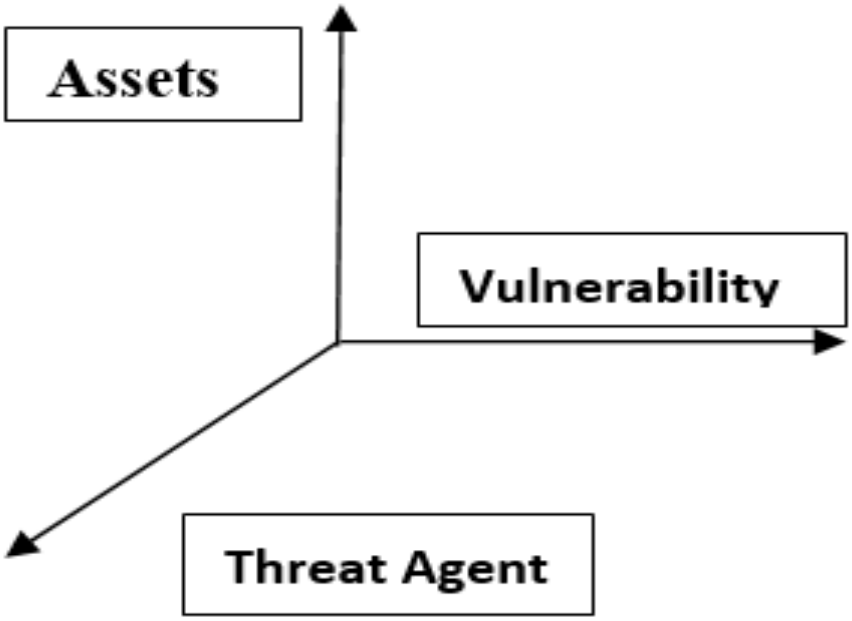


Figure 2. Three-Dimensions of Threat Agents Attributes

3.10 The architecture of systems

The architecture shows that the ESXi server consists of red, blue, and black NET HP-DL380 ESXi VMware CD, DNS, and DHCP, which is further connected to the Blue ESXi security zone and DMZ (demilitarised security zone) and black ESXi connected to 27x juniper srx240 and srx340 firewalls via 27x lab system multiple images of the environment and dedicated interface in red, blue, and black networks. In this server, all the data and information of the University of Hertfordshire is available, and a reliable environment is available for the

attackers installed on VM's. The DMZ's role is to stop the hacker at the threshold point so the attacker groups can control further damage.

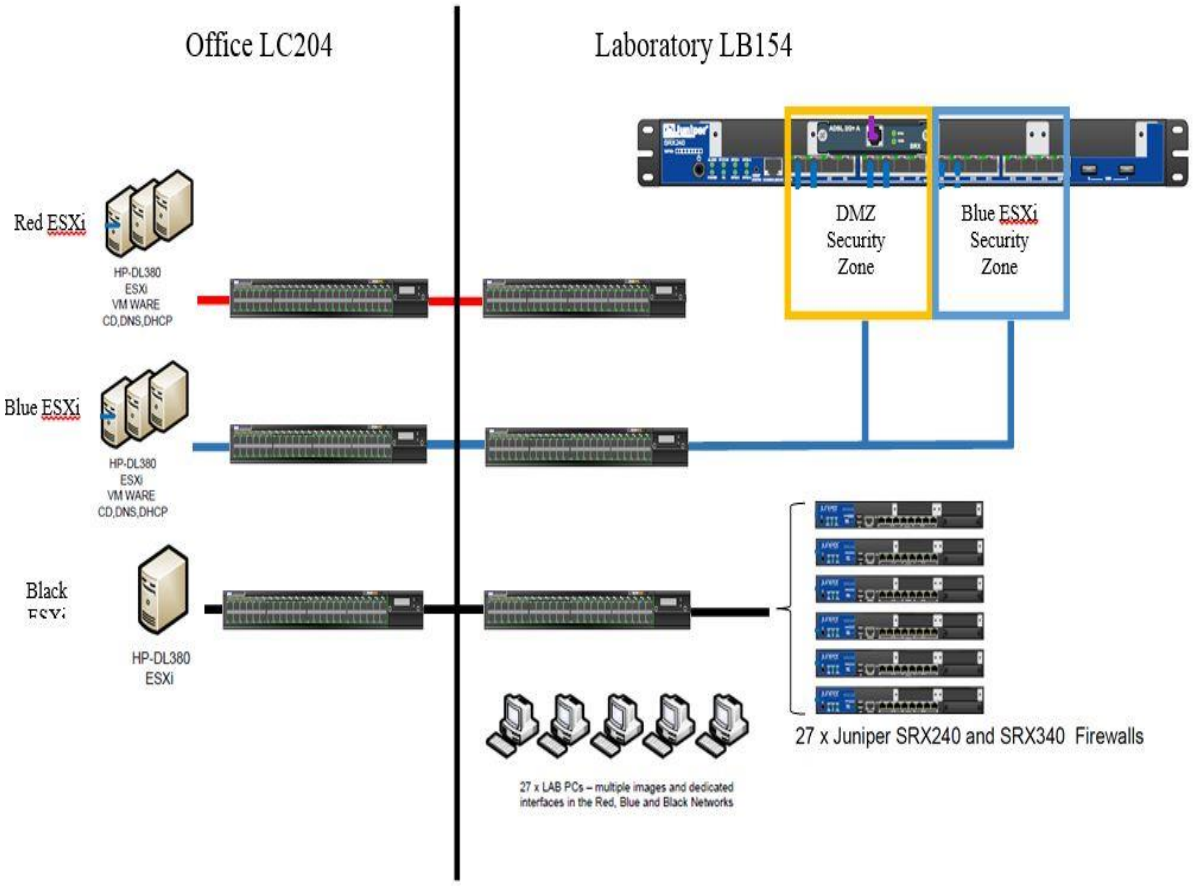


Figure 3 Architecture of System (Abouzakhar, 2015)(Sharma et al., 2022)

The primary purpose of the architecture in above figure is to understand how these attacker groups (i.e., blue teams or adversary attackers) are generating the traffic in the network, increasing the delay time to upload the web page, and extracting useful information from the server such as user credentials, webpages, and accessing the files from the databases.

The data collected from the server is uprooted based on attributes such as source IP address, destination IP address, protocols used, number of ports open, operating on which layer, and location of threat agents. When the model achieves identification of attributes concerning the characteristics identified for the threat agent groups, evaluation of the CVE list starts with the help of various vulnerability scanning tools such as NESSUS and OpenVAS, etc. Later, the cybersecurity practitioners map this CVE list with the NIST

database and identify the vulnerable ports for the particular CVE number. These traditional approaches follow the existing models and methodology to address the vulnerability exploitation of the threat agents identified in the network (Berhe et al., 2021). Because of this, the complexity of threat assessment is tremendously outrageous for the subsisting models. The model displays elements that analyse threat assessment for the detected threat in a semi-automatic network manner, which aids in simplifying the system's complexity.

3.11 Conclusion

The conclusion of Chapter 3 identifies the research question design and implementation strategies with the support of related work, and validation is performed through the use of research methodology. The limitations and shortcomings identified in the present model and procedure inspire the development of a semi-automatic model to extract the essential information for the CTI from the network's collected PCAP files. The required information attributes are the source IP address, the destination IP address, the time spent on the network, the source port, the targeted protocol, the threat agent's latitude, and longitude, and the internet service provider. The procedure of determining attributes will be addressed in Chapter 4 and will demonstrate how to experimentally evaluate required information from semi-automatic PCAP files. Chapter 4 also includes an appraisal of M, O, and C features. The model and research model specification from Chapter 3 will be used to extend the trials.

Chapter-4 Results and Discussions (Ramifications.)

The evaluation of experiments will be explained in this chapter, and the model's execution will be demonstrated in stages. In the first phase of execution, an architecture simulation will be addressed, followed by a demonstration of data stream capture from the ESXi server. Finally, the model's extraction of the necessary information from PCAP files will be discussed.

4.1 Chapter Overview

Identifying the potential cybersecurity threat capability in real-time is a crucial activity. Helpful information about the threat in a network helps cybersecurity practitioners take suitable action to mitigate the risk in a network (Iglesias et al., 2009). The research question raised in Chapter 1 is justified in this chapter. As we identify the problem with the existing model and methodology in the previous section of the chapter, that model cannot connect with the NIST database for vulnerable ports, and the threat assessment of threat agent groups is not achieved in an autonomous manner. The designed model can do it in a semi-automatic way, shown in the following sub-sections and the threat assessment of the threat agents addressed in this chapter.

Elaborating all the information about the potential cybersecurity threats of an organization is typically achieved manually by the existing models and methodology, as discussed in chapter 2. The TAME model conducts a manual threat assessment and vulnerability exploitation tree analysis. TAME (Vidalis and Jones, 2003) identified the capability and opportunity used by threat agent groups to breach the organization's network step by step manually. As a result, the complexity of dealing with the threat agent is not ideal. Chapter 2 is a complete examination of the TAME model.

4.2 Implementation of Tools and Technology for Model

Threat assessment can be automated with the help of tools, techniques, and various real-time models (Xue et al., 2020). The behaviours of threat agents are erratic, and the goals of threat agents change with time or the purpose of the task based on motivation, opportunity, and capability (A Jones, 2002)(Mavroeidis and Bromander, 2017). Profiling is a process that generates a profile for the threat agents based on the historical information extracted from the

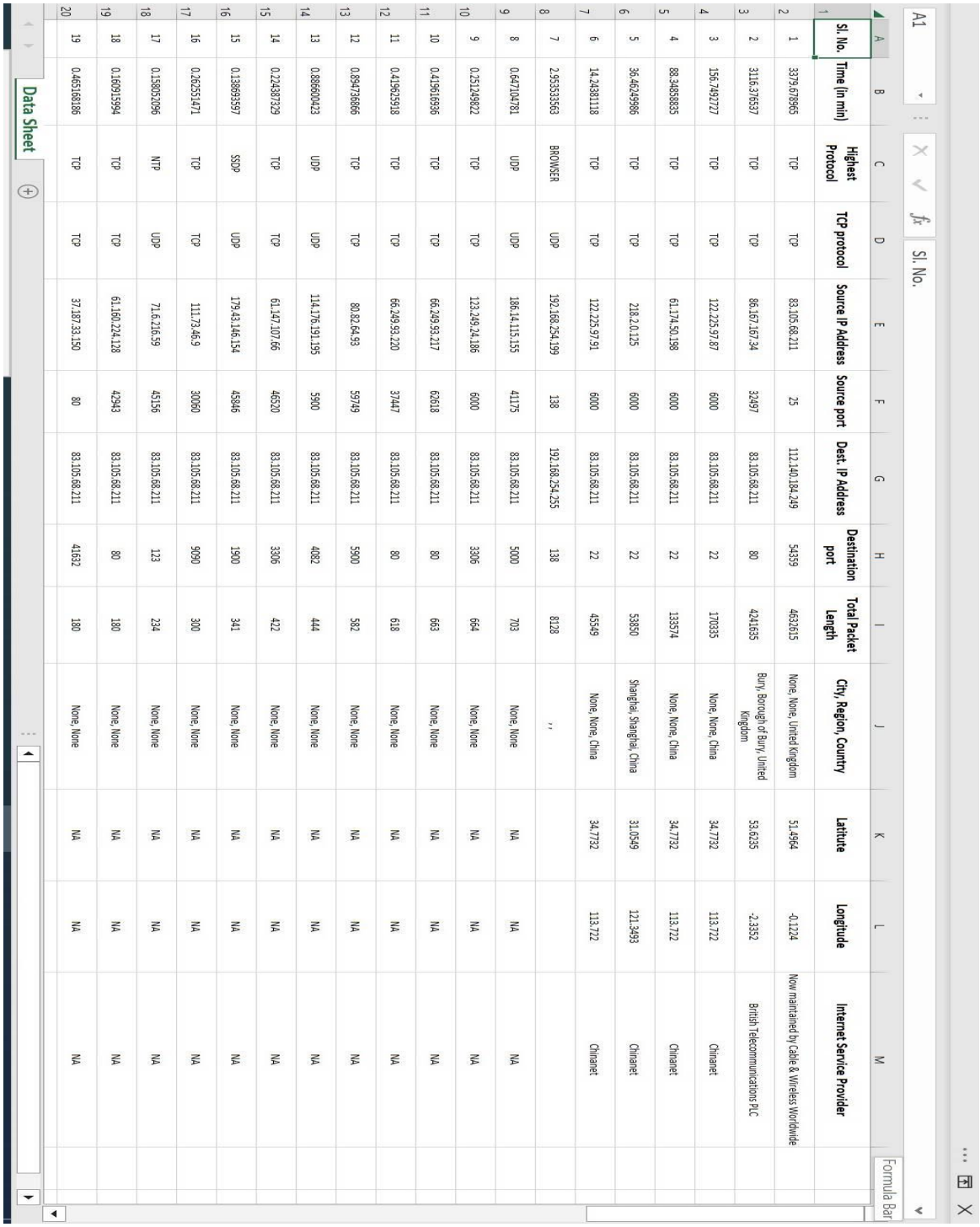
Packet Capture Application Programming Interface files captured in a network with the help of penetration testing phases. The determination of qualities and features of threat agents that will help implement the threat agents' profile can be classified as profiling, according to a literature review analysis of the various models and methodologies. The threat agent profile will assist in identifying the anticipated (future) recognized threat agent in the network. Why do we need to implement profiling of threat agents? Threat profiling is critical to performing an organization's threat assessment. The profile can be populated by having suitable, ample, and precise information about the threat agent, such as behaviour and other useful information including source IP address, destination IP address, number of open ports, number of packets generated, location of the threat agent, and time spend on the network with minimal user intervention (Atote et al., 2016). The user is minimal intervention because the footprints captured by the capturing data tool during threat assessment in the form of PCAP files cannot be altered by the potential threat agent while traversing the network of an organization. The threat agent cannot do the alteration because once they generate the packets in the network, they cannot erase the network's footprint because of the accessing property of the network. This research attempts to recognize the aspects of profiling and deliver solutions. Suppose we have the threat profile for the historically identified threat agents from an organisation's network. In that case, we can use these profiles as references while executing the threat assessment. The data captured from the network can be used effectively and in an optimized manner to address the recent threat agent identified from the network.

It has been accepted that continuous threat assessments do mitigate the risks (Asgari, Haines and Rysavy, 2017). In the modern, socially driven, virtual computing era, threat assessments are hindered by a lack of resources, complexity, and size of data (Azaria et al., 2014)**.** Information environments are large heterogeneous infrastructures, hosting a large amount of data collected from different types of sensors and platforms (Vidalis, Jones and Blyth, 2004). Decision aid tools should provide their understanding of new data and threat assessments to cope with a large amount of data. University computer emergency response team (CMU-CERT) groups determined that there are three key groups of threat agents, i.e., the technology of organization sabotage, compromising with intellectual property, and data stream fraud (Cappelli, Moore and Trzeciak, 2012). In recent years, the growing cases highlighted by internet media revealed that both business and government organizations suffered a similar experience. In contrast, the organisation's internal users have filtrated the priority information

and shared it with the threat agents (Susukailo, Opirskyy and Vasylyshyn, 2020). The threat agents require serious attention from both users and organizations.

In response to covid-19 nowadays, organization and business mostly share their files and documents over the internet to run their business. It is now standard practice for users of the organization to have admittance to large repository documents, which are electronically warehoused on distributed file servers. Many organizations offer company laptops and desktops to users for working while using email to organize and schedule/reschedule meetings. Amenities such as video conferencing are used to hold meetings worldwide, and an organisation's users are continuously connected to the internet. The electronic nature of the files and records of an organization on the internet makes it easier for threat agents to attack it. On the advantage side of threat assessment, practitioners of an organization can easily capture the activity logs of the internal threat agent while analysing their captured packets (Wold, Esbensen and Geladi, 1987). However, analysing such activity logs is practically infeasible because of the user's high volume of daily activities.

We present an efficient model for threat detection and analysis based on the conception of anomaly detection. Given the large variety of the data stream in the form of PCAP files (between 2012 and 2019), the model implements the threat agent profiles from the PCAP files and determines the cyber threat intelligence based on evaluation of motivation, opportunity, and capability of threats. With the help of these profiles, comparisons can be populated that show how the current observations fluctuated from the previous observation. To assess the performance of the tactic, the model extracted the required valuable information such as source IP, destination IP, target port, location of target IP etc., from the PCAP files in a semi-automated manner. Output was generated in the form of an Excel sheet consisting of various attributes of threat agents identified next to the real-world information environment. It was found that the system executed expressively soundly for detecting the attacks. The visualization of reports enabled us to identify which attributes help to determine M, O, and C factors for the threat agents.



Sl. No.	Time (in min)	Highest Protocol	TCP protocol	Source IP Address	Source port	Dest. IP Address	Destination port	Total Packet Length	City, Region, Country	Latitute	Longitude	Internet Service Provider
1	3379.678965	TCP	TCP	83.105.68.211	25	112.140.184.249	54359	4652615	None, None, United Kingdom	51.4964	-0.1224	Now maintained by Cable & Wireless Worldwide
2	3116.376537	TCP	TCP	86.167.167.34	32497	83.105.68.211	80	4241635	Bury, Borough of Bury, United Kingdom	53.6235	-2.3352	British Telecommunications PLC
3	156.7492727	TCP	TCP	122.225.97.87	6000	83.105.68.211	22	170335	None, None, China	34.7732	113.722	Chinanet
4	88.34858835	TCP	TCP	61.174.50.198	6000	83.105.68.211	22	133574	None, None, China	34.7732	113.722	Chinanet
5	36.46249886	TCP	TCP	218.2.0.125	6000	83.105.68.211	22	53850	Shanghai, Shanghai, China	31.0549	121.3493	Chinanet
6	14.24381118	TCP	TCP	122.225.97.91	6000	83.105.68.211	22	45549	None, None, China	34.7732	113.722	Chinanet
7	2.953333563	BROWSER	UDP	192.168.254.199	138	192.168.254.255	138	8128	, ,			
8	0.647104781	UDP	UDP	186.14.115.155	41175	83.105.68.211	5000	703	None, None	NA	NA	NA
9	0.251249822	TCP	TCP	123.249.24.186	6000	83.105.68.211	3306	664	None, None	NA	NA	NA
10	0.419616936	TCP	TCP	66.249.93.217	62618	83.105.68.211	80	663	None, None	NA	NA	NA
11	0.419625918	TCP	TCP	66.249.93.220	37447	83.105.68.211	80	618	None, None	NA	NA	NA
12	0.894726866	TCP	TCP	80.82.64.93	59749	83.105.68.211	5900	582	None, None	NA	NA	NA
13	0.886600423	UDP	UDP	114.176.191.195	5900	83.105.68.211	4082	444	None, None	NA	NA	NA
14	0.224387329	TCP	TCP	61.147.107.66	46520	83.105.68.211	3306	422	None, None	NA	NA	NA
15	0.138693357	SSDP	UDP	179.43.146.154	45846	83.105.68.211	1900	341	None, None	NA	NA	NA
16	0.262551471	TCP	TCP	111.73.46.9	30060	83.105.68.211	9090	300	None, None	NA	NA	NA
17	0.158052096	NTP	UDP	71.6.216.59	45156	83.105.68.211	123	234	None, None	NA	NA	NA
18	0.160915994	TCP	TCP	61.160.224.128	42943	83.105.68.211	80	180	None, None	NA	NA	NA
19	0.465168186	TCP	TCP	37.187.33.150	80	83.105.68.211	41632	180	None, None	NA	NA	NA

Figure 4: Extraction of attributes from PCAP files.

The process of extracting usable data from recorded PCAP files is depicted in the image above. A model based on the phase 1 execution was used to help with the extraction. The model will first accept PCAP files as input and produce a potential output in the form of Excel sheets. Given that some PCAP files are incredibly large, one example of the extracted

information was shown in order to better elaborate on the necessary helpful information regarding the identified threat agent groupings. The link below allows a view of all of the PCAP file's detailed information. Threat agent profiling can be carried out using the related IPs and the data collected from the PCAP files. Profiling can be carried out by identifying the environment, attack vectors, and input and output of associated IPs. When the other execution phases are in progress, a detailed demonstration of profiling is visible in another part. However, this thesis illustrates all the threats identified in a network captured during the penetration testing against the University of Hertfordshire ESXi server.

4.3 Evaluation of Motivation, Capability, and Opportunity

The threat assessment of a model is a continuous process for the data stream/PCAP files collected from the network in an information environment. While evaluating the impact of threat agent groups on the organization or the business, determining the value of assets, vulnerability identification, and threat agent's footprint attributes play a prominent role in the calculation (Vidalis and Jones, 2005). The figure below shows the representation of the main characteristics in a three-dimensional matrix. The model must address this while performing threat assessments of the real-time network.

Figure 5 3-D Representation of Threat Assessment.

Country	No. of attacks
US	28.519
Brazil	6.204
UK	5.099
Germany	4.736
Italy	2.738
Canada	2.345

France	2.022
Denmark	2.004
Australia	1.317
South Korea	1.259

Table 5 Digital Attacks (Asgari, Haines and Rysavy, 2017)

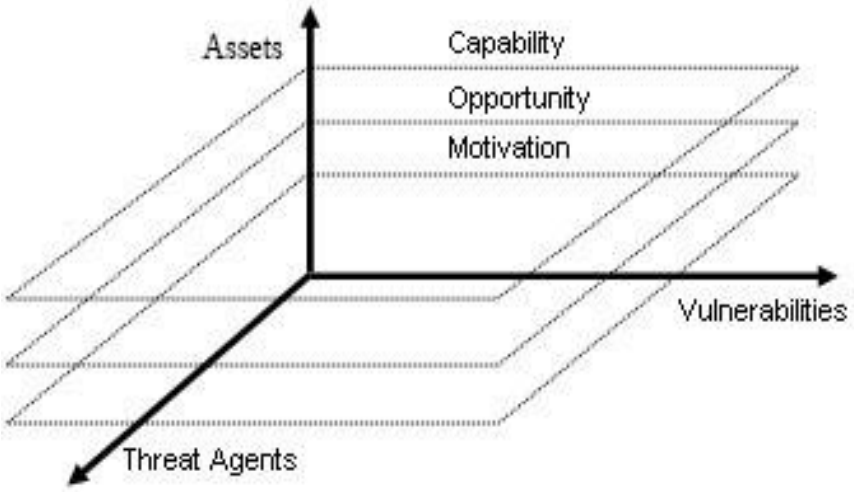


Figure 6 Three-Dimensional Matrix.

"A threat assessment is a statement of threats related to vulnerabilities of company assets and agents, and a statement of believed capabilities that those threat agents possess (Vidalis, Jones and Blyth, 2004)." The function threat can be calculated with the threat agent's motivation, capability, opportunity, and the impact of the successful attacks on an organization of the nation.

$$Threat = "Function\ (Motivation, Capability, Opportunity, and\ Impact)" \quad (1)$$

	Low	**High**
Low	**A** Minimal Effort	**B** Keep informed
High	**C** Keep satisfied	**D** Key players

Figure 7 Power/Interest Matrix(Lessler et al., 2016).

The equation is expressed as breaking down each component of the equation:

- **Motivation:** Refers to the underlying reasons or incentives that drive a potential threat actor to engage in harmful or malicious activities. Motivation can vary widely and may include factors such as financial gain, ideological beliefs, personal grievances, or political motives.
- **Capability:** Represents the resources, skills, knowledge, and tools possessed by a threat actor. It assesses their ability to successfully attack or exploit a vulnerability. Factors such as technical expertise, access to specialised equipment, or organisational support contribute to a threat actor's capability.
- **Opportunity:** Refers to the conditions or circumstances that allow a threat actor to exploit vulnerabilities or launch an attack. It includes factors such as weak security controls, inadequate monitoring, physical access, or loopholes in systems or processes that create openings for malicious activities.
- **Impact:** Assesses the potential consequences or harm that may result from a successful attack or exploitation. It considers the magnitude of damage, financial losses, disruption to operations, compromise of sensitive information, or harm to individuals or assets.

The "function" part of the equation indicates that the threat level is determined by combining these factors using a specific formula or algorithm. The exact function used may vary depending on the specific risk assessment methodology or organization's approach. By evaluating and quantifying each component, the threat equation helps security professionals or risk analysts assess the threat level posed by a particular entity or scenario. This information can then be used to prioritize security measures, allocate resources, and develop appropriate risk mitigation strategies.

Threats	% of Respondents
Denial of service	52%
Website defacement	27%
Viruses	59%
E-Mail interception	39%
Internal fraud	39%

Fraud affecting a third-party service such as a credit card	23%
Theft of confidential information on electronic documents	58%
Threats from disgruntled employees or contractors	43%
Interception of wireless LAN communications	45%

Table 6 Worst Threats to IT Security(Shin and Lowry, 2020).

4.3.1 Motivation

The evaluation of motivation for threats is the problematic part. It could be determined with the help of an analysis of hacktivism branded attacks by groups of assessment models and the network's vulnerability in next-to-real-time semi-automated information environments. Attacker's motivations are constantly changing, as the growing rate of hacktivism attacks by different groups of people shows. It can also be seen in the differences in unique motivations based on each group or the organization or vertical market; some common motivations include (Rubini et al., 1993):

- Profit (direct or indirect)
- Direct grudge
- Fun / reputation
- Further access to partner/connected systems.

$$F\ (X)\ =\ f\ \big(Cap, Opp, Mto, V(VIA)\big)\ Y\ , f\ (Vulnerability) Asset\ , Impact, T \quad (2)$$

The above equation abbreviation shows the meaning of each term where Cap stands for capabilities, Opp is an opportunity of the threat agent, Mto is motivation, and V (and VIA) stands for the value of intangible assets, threat assessments, and time complexity. Three functions are used to form the equation.

1. f(Cap, Opp, Mto, V(VIA)):
    a. Cap: the resources, skills, and knowledge possessed by a threat actor.
    b. Opp: the conditions or circumstances that allow a threat actor to exploit vulnerabilities or launch an attack.

c. Mto: the underlying reasons or incentives that drive a potential threat actor.
d. V(VIA): V(vulnerability, impact, awareness) represents the vulnerability, impact, and awareness factors associated with a particular threat or risk.

f(Cap, Opp, Mto, V(VIA)) is a function that combines these factors in a specific manner and identifies the value of intangible aspects. It can be assumed that it incorporates these variables to determine a value or rating for the threat. Y is a multiplier or weight associated with f(Cap, Opp, Mto, V(VIA)).

2. f(Vulnerability):
    a. Vulnerability refers to weaknesses or flaws in systems, processes, or technologies that could be exploited by threat actors.
    b. f(Vulnerability) is a function that assesses the severity or significance of the vulnerability.
3. Asset:
    a. The asset represents the value or importance of the target or resource that is at risk of being compromised or affected by a threat.
    b. The equation includes the term f(Vulnerability)Asset, which suggests that the impact of the vulnerability on the asset is considered.
4. Impact:
    a. Impact assesses the potential consequences or harm that may result from a successful attack or exploitation. It can include factors such as financial losses, disruption of operations, compromise of sensitive information, or harm to individuals or assets.
5. T: Time complexity
    a. T represents any additional factors or variables that are relevant to the threat assessment but are not explicitly specified in the equation or the total time spent extracting the process.

Overall, the equation combines various factors, such as capability, opportunity, motivation, vulnerability, asset value, and impact, to assess the threat level posed by a particular scenario or entity. The exact functions used to combine and weigh these factors depend on the extraction value, so they may vary depending on the specific risk assessment methodology or context in which the equation is applied. The ultimate output of the threat assessment

performed for the specific organization or business of the country is the sum of the results of each operation. The worth of an organization's assets will be determined when the identified threat agents in the network have their capability, opportunity, and motive assessed in the first function. Then the threat agent IPs are extracted using a model and semi-automatically using Python libraries. With the use of penetration testing principles, the opportunity and capability will be identified. The motivation of the threat agent will be defined following the probabilistic approach and motivational principles. The value of assets evaluation is processed after completing the M, O, and C evaluations. Combining these four parameters can help determine the threat agent's ability to breach the network.

The second function involves vulnerability investigation using Kali Linux tools found in the library. The vulnerability study used OpenVAS and other tools available in the Kali Linux library. The discovered IPs of threat agents were removed from the list of CVEs that were found to be related to the IPs of threat agents. The value of mitigation techniques concerning asset value will be calculated based on examining the CVE model. Finally, linking the list of CVEs with the NIST database was finished to provide a semi-automatic function to the model.

The impact on the network is determined in the third function using threat assessment and vulnerability exploitation analysis. Finally, the last function is T, which stands for time complexity; the entire time the model takes to address all threat assessment functions will be the total time a model uses to handle a threat agent found in the network while analysing a network.

Motivators	**Primary Groupings**
Level 1	Political.
Level 2	Secular.
Level 3	Personal gains.
Level 4	Religion.
Level 5	Terrorism.

Level 6	Curiosity.

Table 7 Threat Agent Motivators(A Jones, 2002).

4.3.2 Capability

The capability of threats could be determined with the analysis of risk assessment models and the network's vulnerability in a next-to-real-time semi-automated information environment (Vidalis and Jones, 2006).

Cyber risk = Threat, Vulnerability, Information Value (3)

The above equation shown is known as the “cyber risk equation” or “risk formula” in the context of cybersecurity. It is used to assess and quantify the level of risk associated with cyber threats and vulnerabilities, taking into account the value of the information at stake. Here is an explanation of each component:

- **Threat:** The threat component refers to potential sources or actors that may exploit vulnerabilities in the information systems or networks. Threats can include malicious hackers, malware, insider threats, or any other entity that poses a risk to the security of digital assets.
- **Vulnerability:** Vulnerability represents weaknesses or gaps in information systems or networks that threats can exploit. These vulnerabilities can arise from misconfigurations, outdated software, inadequate access controls, or other factors that can be exploited to gain unauthorized access or compromise the integrity of your systems.
- **Information value:** The information value component assesses the importance, sensitivity, or criticality of the information assets that owners are seeking to protect. It considers factors such as the confidentiality, integrity, and availability requirements of the information and its strategic or financial value to the organisation.

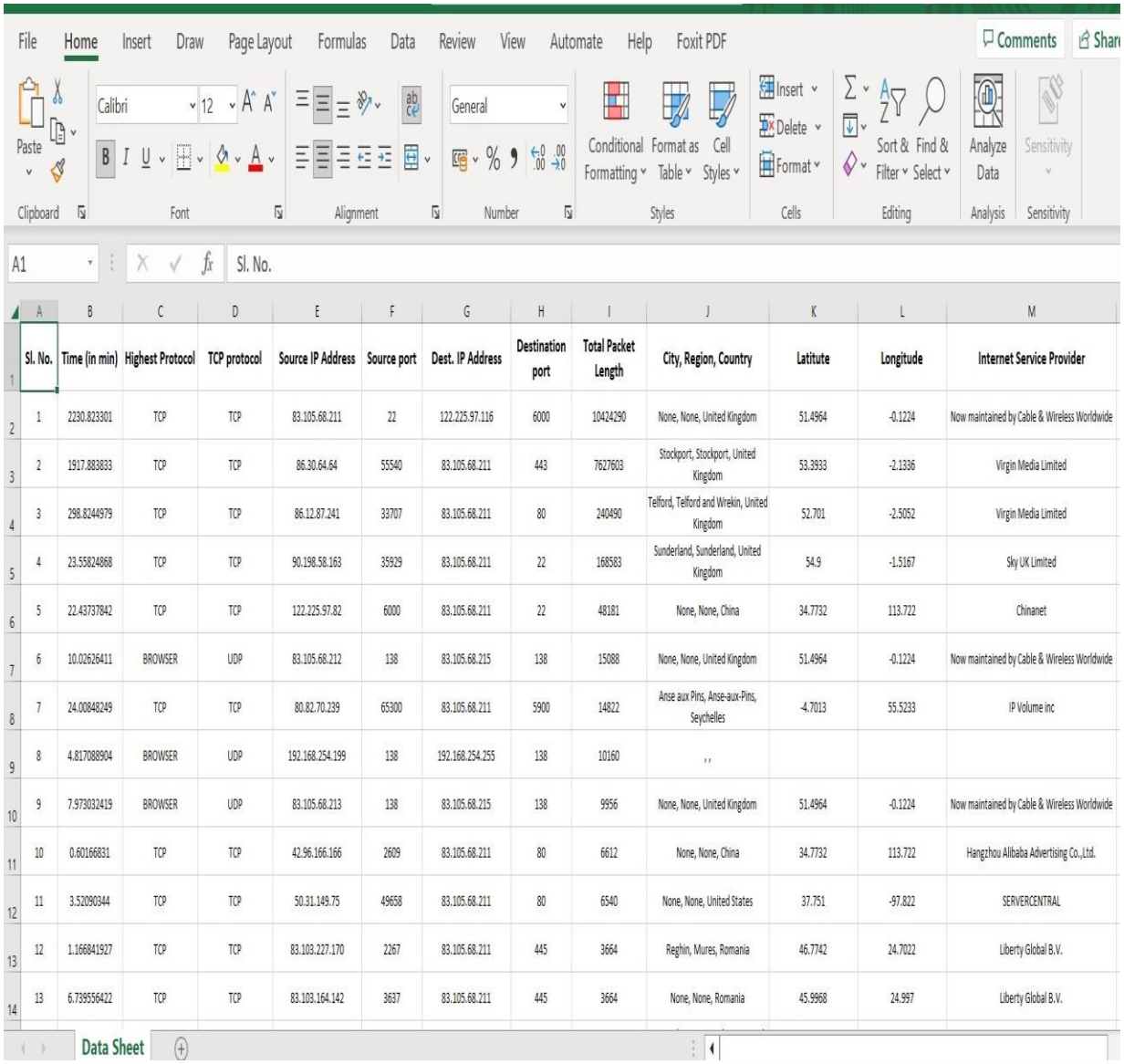
The ‘x’ in the equation represents multiplication, indicating that these three components are multiplied together to calculate the overall cyber risk. The equation estimates the potential impact or likelihood of a cybersecurity incident by multiplying the threat, vulnerability, and information value.

The cyber risk equation highlights the interplay between threats, vulnerabilities, and the value of the information at risk. By understanding and quantifying these factors, organizations can prioritize their cybersecurity efforts, allocate resources effectively, and implement appropriate risk management strategies to mitigate potential threats and vulnerabilities.

It is worth noting that different organizations may have variations of the cyber risk equation, incorporating additional factors or using different mathematical models. The specific equation used can depend on the risk assessment methodology or framework adopted by the organization.

Further investigation is achieved with the help of several Kali Linux tools such as NESSUS, SAINTS, WHISKER, SARA, etc. The initial phase of the automatic version of the threat agent analysis model is to collect the data from the server, which the server's administration has achieved between 2012 and 2019. The simulation architecture (detailed in Chapter 3) aids in capturing all data stream from the server using the Wireshark tool available on Kali Linux libraries. The administration used Wireshark to capture the activity of the threat agent groups on the ESXi server between 2012 and 2019. PCAP files with the data were captured in the cybersecurity laboratory. The model uses the massive dataset of PCAP files as input to extract the user information needed for threat assessment from the files. The model featured input from the server's historical and newly generated data for analysis cost-effectiveness. This data mainly consists of PCAP files, which will be extracted in a semi-automatic manner with the help of a Python tool library available on TensorFlow. The information extracted from these PCAP files has some unique attributes such as - time (in min), highest protocol, TCP protocol, source IP address, destination IP address, source port, destination port, total packet length, city, region, country, latitude, longitude, and internet service provider. While the extraction process is being executed, the large number of PCAP files collected from the server will be converted into many Excel sheets based on the unique attributes. These Excel sheets contain all the useful information available about the threat in the PCAP files, such as time spent on the network, location of their IPs, and environment used by them while penetrating the server, etc.

A large amount of information about the threats can be profiled based on their activities performed on the network or specific environment or protocol used to achieve their goal/task. Now, we use all this information to extract critical threat intelligence from these groups of threats to determine the threats' capability, opportunity, and motivation.



Sl. No.	Time (in min)	Highest Protocol	TCP protocol	Source IP Address	Source port	Dest. IP Address	Destination port	Total Packet Length	City, Region, Country	Latitute	Longitude	Internet Service Provider
1	2230.823301	TCP	TCP	83.105.68.211	22	122.225.97.116	6000	10424290	None, None, United Kingdom	51.4964	-0.1224	Now maintained by Cable & Wireless Worldwide
2	1917.883833	TCP	TCP	86.30.64.64	55540	83.105.68.211	443	7627603	Stockport, Stockport, United Kingdom	53.3933	-2.1336	Virgin Media Limited
3	298.8244979	TCP	TCP	86.12.87.241	33707	83.105.68.211	80	240490	Telford, Telford and Wrekin, United Kingdom	52.701	-2.5052	Virgin Media Limited
4	23.55824868	TCP	TCP	90.198.58.163	35929	83.105.68.211	22	168583	Sunderland, Sunderland, United Kingdom	54.9	-1.5167	Sky UK Limited
5	22.43737842	TCP	TCP	122.225.97.82	6000	83.105.68.211	22	48181	None, None, China	34.7732	113.722	Chinanet
6	10.02626411	BROWSER	UDP	83.105.68.212	138	83.105.68.215	138	15088	None, None, United Kingdom	51.4964	-0.1224	Now maintained by Cable & Wireless Worldwide
7	24.00848249	TCP	TCP	80.82.70.239	65300	83.105.68.211	5900	14822	Anse aux Pins, Anse-aux-Pins, Seychelles	-4.7013	55.5233	IP Volume inc
8	4.817088904	BROWSER	UDP	192.168.254.199	138	192.168.254.255	138	10160	, ,			
9	7.973032419	BROWSER	UDP	83.105.68.213	138	83.105.68.215	138	9956	None, None, United Kingdom	51.4964	-0.1224	Now maintained by Cable & Wireless Worldwide
10	0.60166831	TCP	TCP	42.96.166.166	2609	83.105.68.211	80	6612	None, None, China	34.7732	113.722	Hangzhou Alibaba Advertising Co.,Ltd.
11	3.52090344	TCP	TCP	50.31.149.75	49658	83.105.68.211	80	6540	None, None, United States	37.751	-97.822	SERVERCENTRAL
12	1.166841927	TCP	TCP	83.103.227.170	2267	83.105.68.211	445	3664	Reghin, Mures, Romania	46.7742	24.7022	Liberty Global B.V.
13	6.739556422	TCP	TCP	83.103.164.142	3637	83.105.68.211	445	3664	None, None, Romania	45.9968	24.997	Liberty Global B.V.

Figure 8 Extraction of attributes for threat agent groups.

The CTI can be extracted from the identified threat agent groups using Python script execution in the first phase of the model based on the required attributes determined from the PCAP files. As the model runs the Python script on the massive dataset of PCAP files, the potential output is shown in terms of the number of Excel sheets for each collected file in the below figure. Based on the probabilistic technique, the information acquired from each file can be used to evaluate the threat agent's desire to breach the network. In evaluating motivation for the historical dataset, the model can use prediction approaches for the types of motivation the threat agent receives. However, the approach has a limitation, which is usually between (0.1 and 0.9) probability. According to the mathematical, probabilistic method, the

output is always within the range that can lead to a reasonably accurate prediction of motivation.

Factor	Weighting Value				
	1	2	3	4	5
Adult Population (P)	< 1M	1M – 10M	10M – 50M	50M – 100M	>100M
Literacy Level (L)	<50%	51-65%	66-80%	81-90%	>91%
Internet Access (I)	Very Low	Low	Medium	High	Very High
History of Relevant Activity (H)	None	Intermittent	Occasional	Regular	Regular & Widespread
Technical Expertise (T)	None	Very Limited	Limited	Adequate	High Level
Gross Domestic Product per Capita (G)	<$1K	$1K-$5K	$5K-$10K	$10K-$20K	>$20K
Allied Nation Capability (N)	None	Limited	Medium	High	Very High
Indigenous IW Capability (AA)	None	Limited	Medium	High	Very High
Other Factors (AB)					Religious Fundamentalism, Support of International Terrorism

Figure 9 Evaluation of threat agent group attributes (A Jones, 2002; Vidalis and Jones, 2003; Matthews and Matthews, 2014; Lessler et al., 2016).

This CTI can also be used to identify the new threats in-network and extract all information by taking previously identified CTI as a reference. As in Table 4 motivation of these threats and agent groups will be determined based on their environment or the extraction of the data type executed during the process. Factors are responsible for digging into the server, like financial gain, breaching security and being socially responsible.

Factors.	**Characteristics.**	**Level (weighing value).**

Nation-state.	Population, literacy level, internet access, technical expertise, capability, indigenous, etc.	-Number of populations, >57%, High, moderate, high, high respectively.
Terrorism.	Number of activities, education level, internet access, technical expertise, capability, funding, etc.	<1000, training, excellent access, high, expert, unlimited.
Criminal groups.	Geographic range, Group size, type of crime, technical expertise, etc.	Depending on the country's origin, <10k, industrial and smuggling types, highly trained.
ESA(European space agency).	Members, funding, target type, sponsoring organization, etc.	>30%, Unlimited, international stock markets (Valuable profile of companies), widespread.
Corporate attacks.	Markets, technical expertise, organization size, etc.	Dynamic, static, or volatile markets, high level, <10k.

Table 8 Capability Calculations(A Jones, 2002)(Ani, He and Tiwari, 2019).

4.3.3 Opportunity

Similarly, opportunity can be calculated by checking which ports are open, which protocols have open access, and other factors that help a hacker gain unauthorized access to the server. All this information will lead to the evaluation of the opportunity of the threat agent groups. In the same way the capability of a threat agent will be calculated when we identify all information about the threat agents, what type of environment they are using, which protocol they are targeting, how much time they spend on the network, and what type of knowledge they have about the penetrating the network. With the help of all these attributes, we can determine the capability of the threat agent's groups.

Factor	Weighting Value				
	1	2	3	4	5
Number of Activists (A)	1 - 500	501- 1000	1001 - 5000	5001 - 10000	Over 10000
Education Level (E)	Very Low	Low	Medium	High	Very high
Internet Access (I)	Very Low	Low	Medium	High	Very High
History of Relevant Activity (H)	None	Intermittent	Occasional	Regular	Regular & Widespread
Technical Expertise (T)	None	Very Limited	Limited	Adequate	High Level
Funding (F)	None	Very Limited	Limited	Adequate	Unlimited

Figure 10 Evaluation of factors for opportunity (A Jones, 2002; Vidalis and Jones, 2003; Matthews and Matthews, 2014; Lessler et al., 2016).

The above figure model determines the IP addresses for each threat agent by semi-automatically running multiple scripts to calculate the required attributes. The opportunity can be assessed using the threat agents' identified traits and qualities. A model can detect server information such as which port is open, the sort of environment the target computer uses, the types of services operating on the target machine, and the set of protocols utilized to carry out the process. Agents can use the threat's information to efficiently penetrate the network based on the information obtained by the threat. When the threat agent pulls all the information from the target system, it will identify the vulnerabilities associated with the target machine's environment. Furthermore, threat agent will use this information to enter the network or expand their capability to exponentially increase the impact on the target machine's assets. The extraction of attributes can be used to evaluate the opportunity.

4.4 Tribalizing Algorithms

Many different models are used to perform threat assessment for a network in an informational environment on specialized datasets. Some of the datasets are discussed in earlier chapters. Here, I illustrate all the threats identified in a network captured during the penetration testing against the University of Hertfordshire ESXi server. To provide an overview of the current state-of-the-art approaches used to perform the threat assessment, I group all the identified threats from a network based on their profile maintenance concerning the Python program run against the data stream/PCAP files captured during the experiment. Similarly, the critical threat intelligence (Shin and Lowry, 2020) feed is identified from this

group of threat agents based on their footprints extracted during the analysis phase of the experiment. This overview is further divided into two main categories, traditional extraction of information from the PCAP files and instructive techniques applied on the information extracted from the PCAP files to generate the footprints used by the threat agents during traversing in a network of the server.

The first Python program provides the accuracy and the unique attributes of the threat agents for precision, false-positive rate, Anomaly detection rate, and Fault-measure as originally reported (Chen, Cheng and Hsieh, 2010). Secondly, we calculated the performance of the threat agent followed by our proposed three-dimensional metrics, i.e., motivation, opportunity, and capability. The below figure shows that the input is a large number of heterogeneous PCAP files used, which have been captured during the experiment.

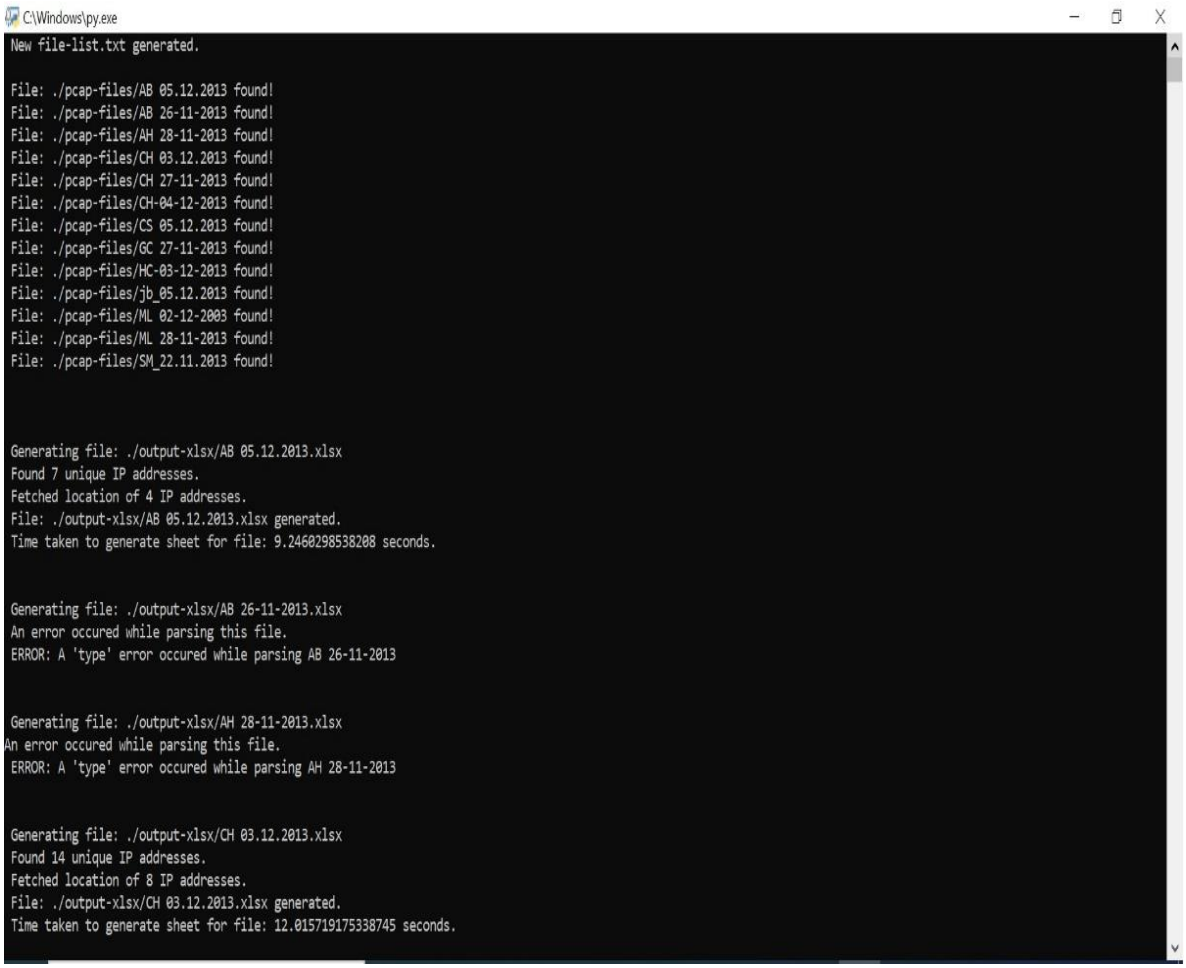


Figure 11. Proposed workflow for raw PCAP file traffic-based feature extraction and experimental results for unique IP addresses with time complexity.

The potential output generated with analysis of PCAP files is the unique number of Excel sheets which consist of information about the threat agents such as time (in min), highest protocol, TCP protocol, source IP address, destination IP address, source port, destination port, total packet length, city, region, country, latitude, longitude, and internet service provider. The specific attributes for each experiment run against the PCAP files can be retrieved from- **https://github.com/Gauravsbin/Excell-sheets-of-PCAP-files**. Furthermore, with the help of these unique attribute's help, we can determine the capability and opportunity of the threat agents (Rynes and Bjornard, 2011). Based on the footprints followed by the threat agents during the analysis, the model can determine the motivation factor for attackers. For example, threat agent groups exclusively target machine running Windows XP as their operating system. The motivation element can be inferred, because one specific collection of threat agents targets just the Windows XP environment. Because Windows XP is a more vulnerable environment than other domains such as Linux or Windows 10, evaluating such an information model will predict the motive factor to attack the specific computer deployed on the network.

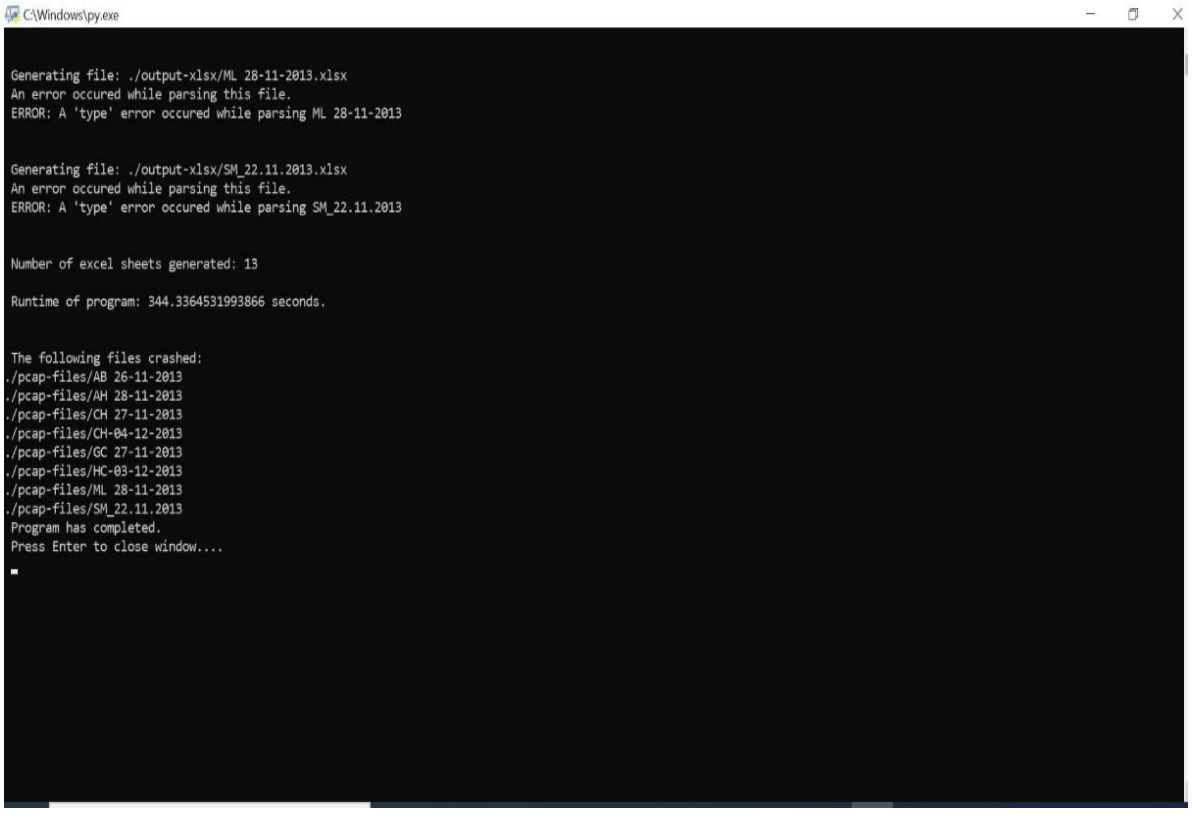
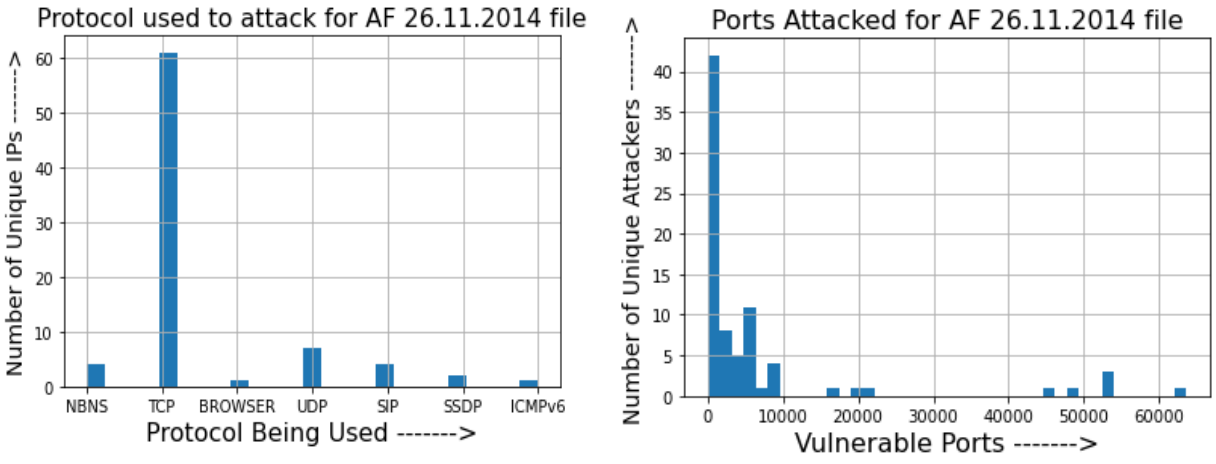


Figure 12. Workflow for raw PCAP file and experimental results for unique IP addresses with time complexity.

A few of the PCAP files, that have been captured during the experiment with the help of the Wireshark tool, have been corrupted as well. At the same time, testing with the python program list of crashed files generated during the experiment is also shown in the above figure. During further confirmation about these files, they were checked manually, and with the help of Wireshark and other analysis tools for PCAP files, no information could be extracted from them. There may be some capture issue, or it might be the connection was lost at the hacker's end during the establishment of the network. The time complexity can also be evaluated with the help of the addition of all time taken by each PCAP file to generate the unique IPs with attributes of information about it. This is the unique feature of this model in comparison with the existing model and methodologies. Existing models, for example, VIM, TAME, and Jones use manual methodologies and techniques to establish the attributes of the threat agent based on the attribute determination of M, O, and C for the threat agents. These existing models do not account for the complexity of dealing with each threat agent. In contrast, the semi-automatic threat agent analysis model considers the complexity of assessing in a semi-automatic manner. This could be happened because the use of semi-automatic approaches for threat assessment of networks next to the real-time informational environment.

4.5 Workflow and Comparative Experiments

In the previous section, the output was generated in the form of Excel sheets with the unique attribute of threat agents in a semi-automatic manner. So, to determine the motivation, opportunity, and capability of threat agent groups, interactive techniques were applied on the output of the previous phase in such a manner as to provide a semi-automatic feature to the



model (Rossebo, Fransen and Luiijf, 2016).

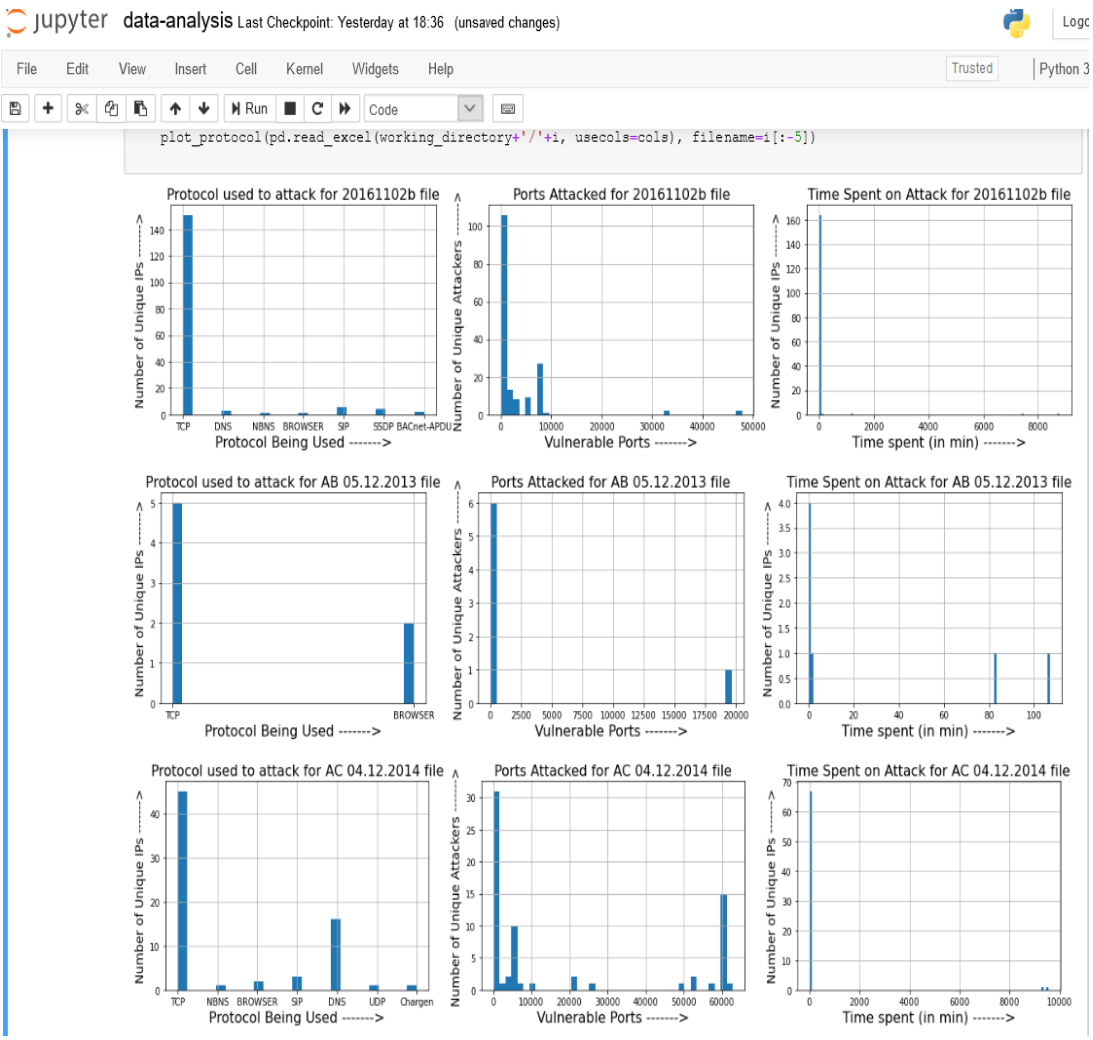


Figure 13 Experimental Results for Each PCAP file, Feature Extraction Strategy, and Network.

This novel approach helps us to optimize the complexity of the threat assessment of a network. This chapter also shows the process of using python libraries on TensorFlow, and deep learning techniques will be examined to identify the unique tuples of data stream/PCAP files. This approach mainly depends on the chronological order of packets in PCAP files.

Here, we first make groups of all the unique IPs extracted from raw PCAP files captured from the network with the help of Wireshark. The grouping of all unique IPs based on their attributes and characteristic features was identified during the analysis and implementation of data stream. Similarly, the potential output generated in the previous phase will be used as

potential input for the second phase of analysis and implementation. Such a process is known as the profiling of threat agents. As in the previous phase, we generated the Excel sheet for each captured PCAP file consisting of useful information as ports open, on which layer they are operating, time spent on the network, and the location of the threat agent, etc.

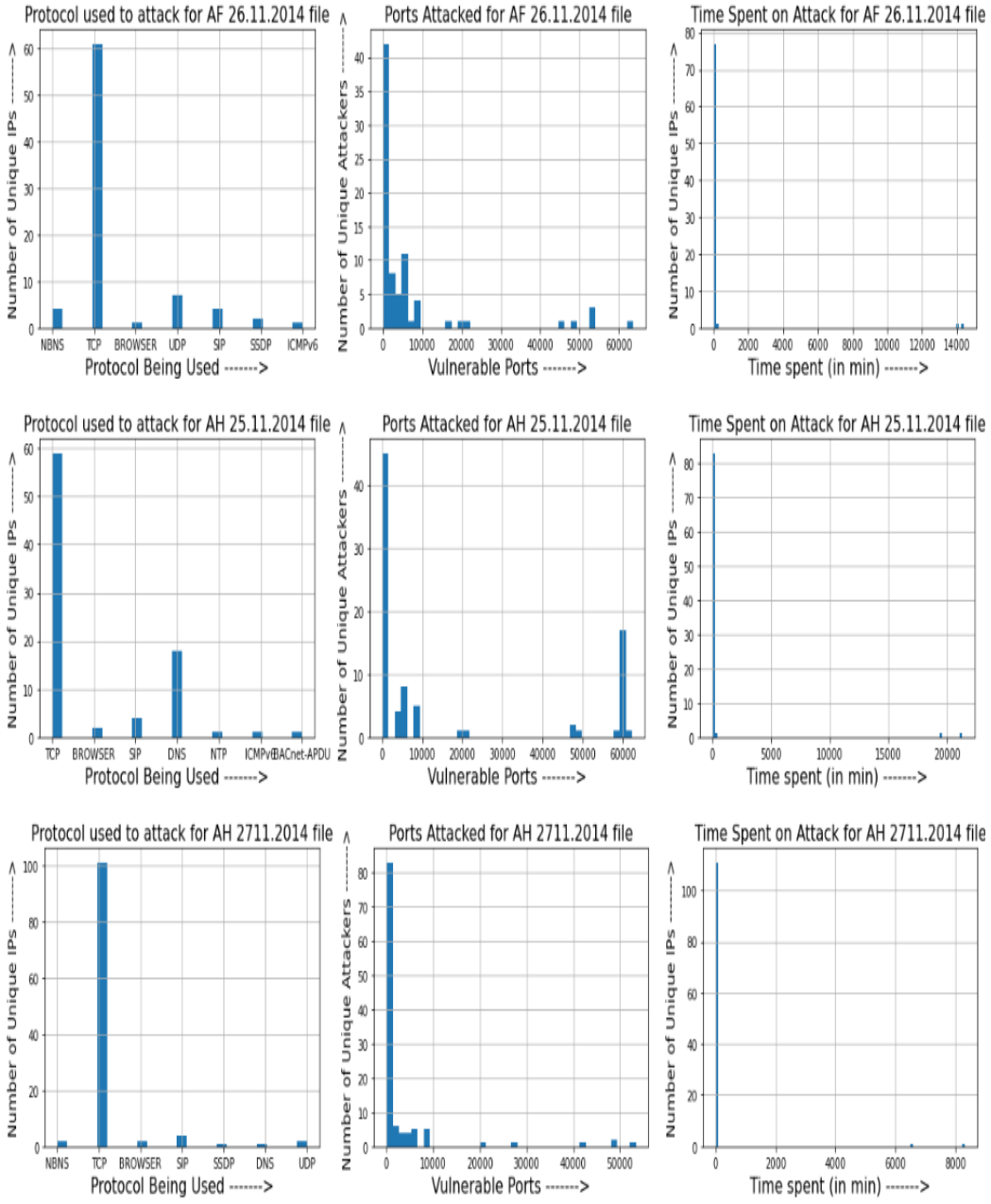


Figure 14 Histogram for each input based on protocol, ports, and time.

Based on this analysis, now make one more IPYNB (Interactive Python Notebook and Jupyter Notebook) file. "Jupyter is a free, open-source, interactive web tool known as a

computational notebook. Researchers can combine software code, computational output, explanatory text, and multimedia resources in a single document. A Jupyter Notebook document is a JSON document, following a versioned schema, containing an ordered list of input/output cells which can contain code, text (using Markdown), mathematics, plots, and rich media, usually ending with the IPYNB extension (Saygili et al., 2018)(Van Veen et al., 2019)(Narkar, Thomson and Fox, 2020)". This file consists of an algorithm performing data clustering of unique IPs found in the Excel sheet of the previous phase. The data clusters of IPs are formed based on the number of IPs facing a particular type of attack.

This particular type of attack is determined based on the number of factors identified during the analysis. The IPYNB file collects all the unique IPs as input. It extracts the information on which layer they are operating, what type of ports and protocols were compromised when the source IPs of end-users were attacked, what information they extracted from the VM's particular environment, and so on. The analysis groups all the threat agents into a particular category depending on their attacking behaviours identified during the analysis.

The above figure shows the Histogram of the bar chart with the help of the IPYNB algorithm for each Excel sheet generated during the first phase. The first bar chart shows protocols used in attacks. That is, on the y-axis, the number of unique IPs and, the x-axis shows, the number of protocols being assessed for them. The second bar chart shows vulnerability ports, i.e., on the y-axis shows is the number of unique IPs, and on the x-axis is the number of ports being assessed for them. The third bar chart shows time spent on the network for an attack on the y-axis, the number of unique IPs on the y-axis, and the x-axis is shown time spent on the network in minutes.

The above histogram for the protocols, ports and time spent on the network will help evaluate the threat agent's three main attributes, motivation, opportunity, and capability. Once we identify the port open during the network's access, we can determine the opportunity for the groups of threat agents used during the penetration of the network. In the same way, the above histogram will help us identify the protocols accessed by the threat agents that will lead to an evaluation of the hacker's potential capability.

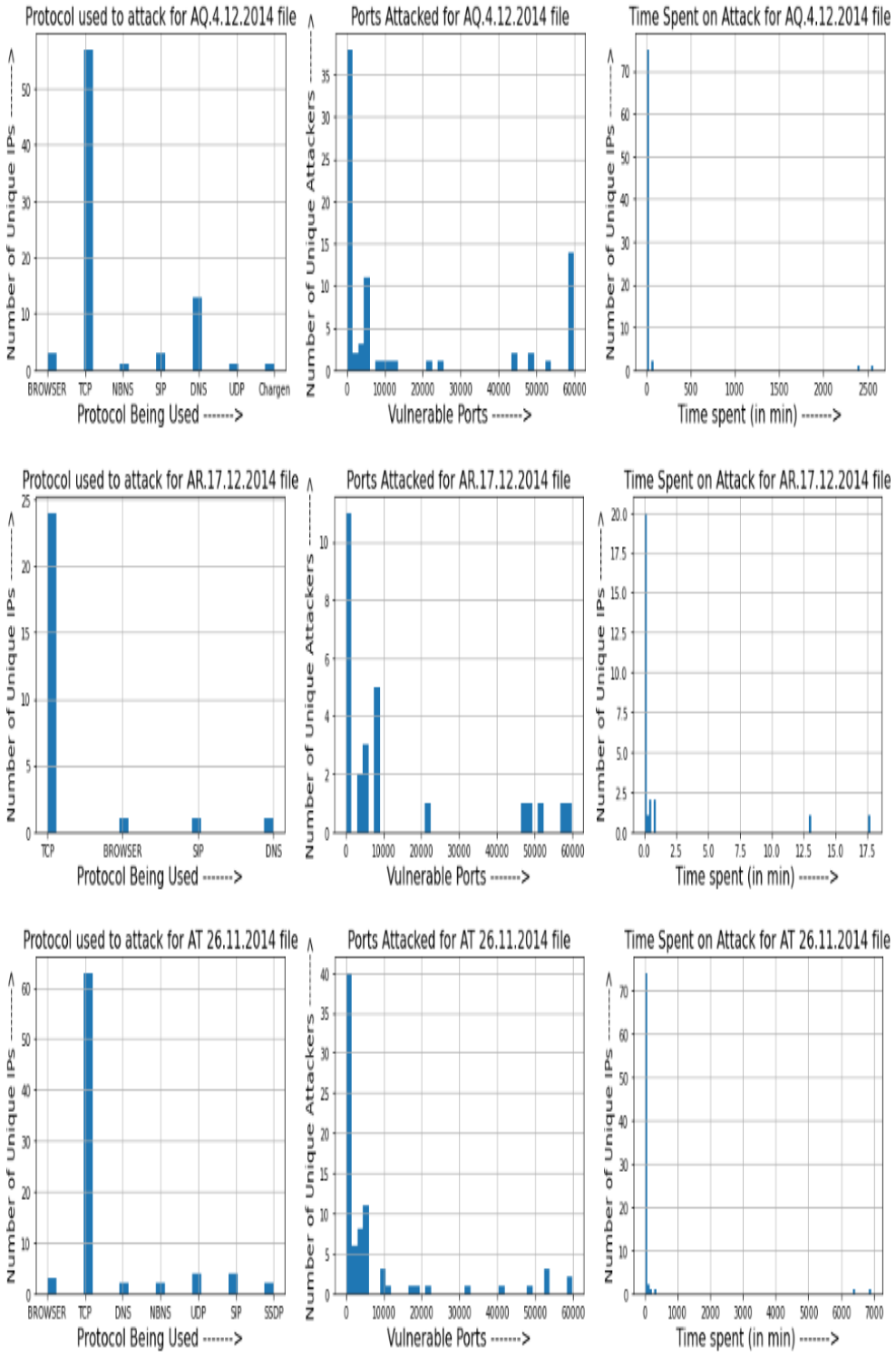


Figure 15 Histogram for each input based on protocol, ports, and time.

Similarly, the above figure shows the histogram of bar charts and analysis of different inputs. The first bar chart shows protocols used in attacking on the y-axis, the number of unique IPs

and on the x-axis, the number of protocols being assessed for them. The same second bar chart shows vulnerability ports, on the y-axis is the number of unique IPs, and on the x-axis is the number of ports being assessed for them. The third bar chart shows time spent on the network for an attack on the y-axis, the number of unique IPs, and the x-axis is time spent on the network in minutes.

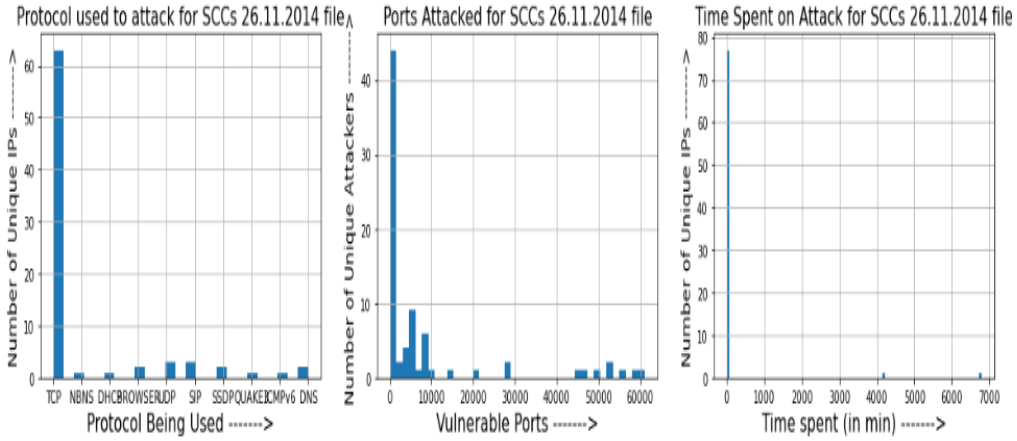


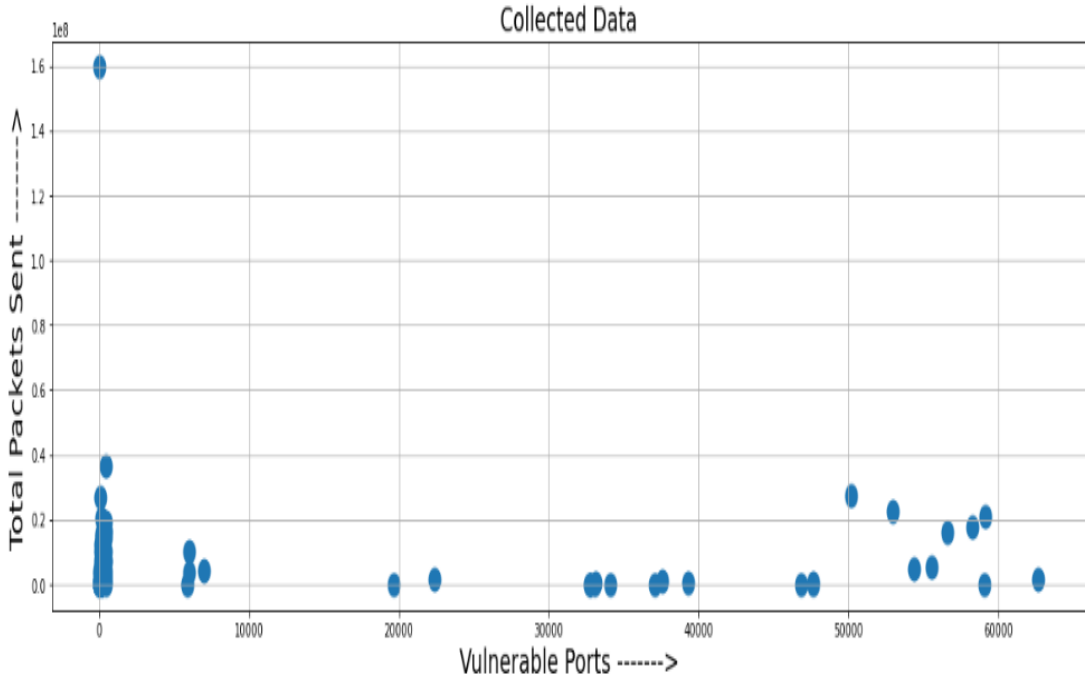
Figure 16 Histogram for each input based on protocol, ports, and time.

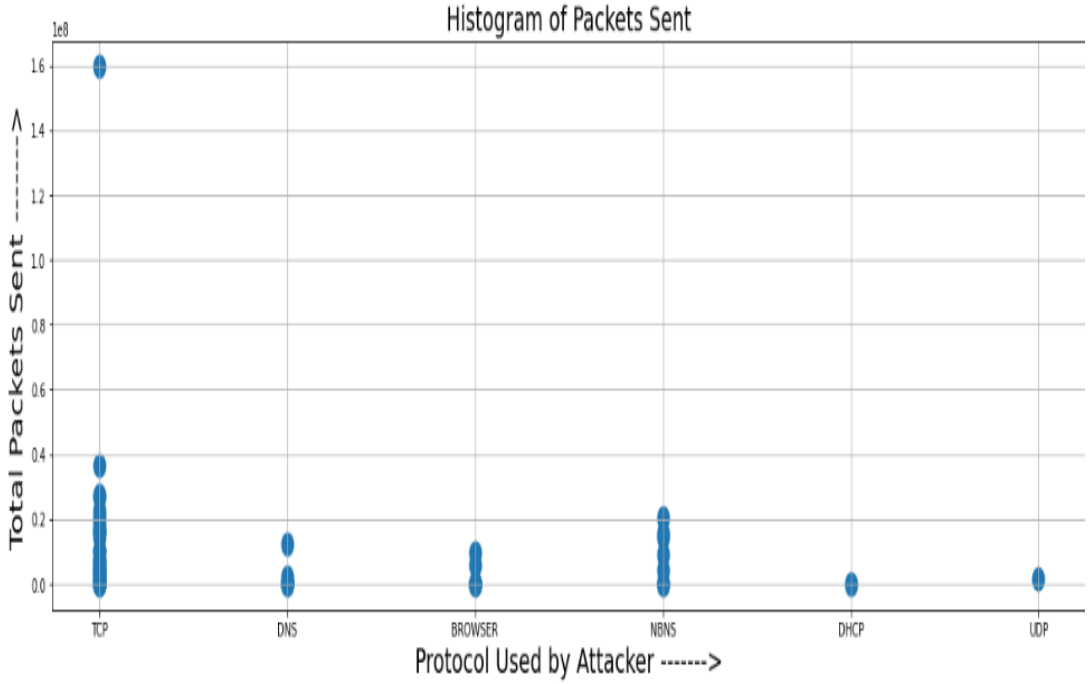
The above figures show two parts to the outputs generated by the. IPYNB file. In the first part, three histograms are generated for every file in the output-Excel sheet, and the second part generates the histogram on the cumulative data of all the files in the folder.

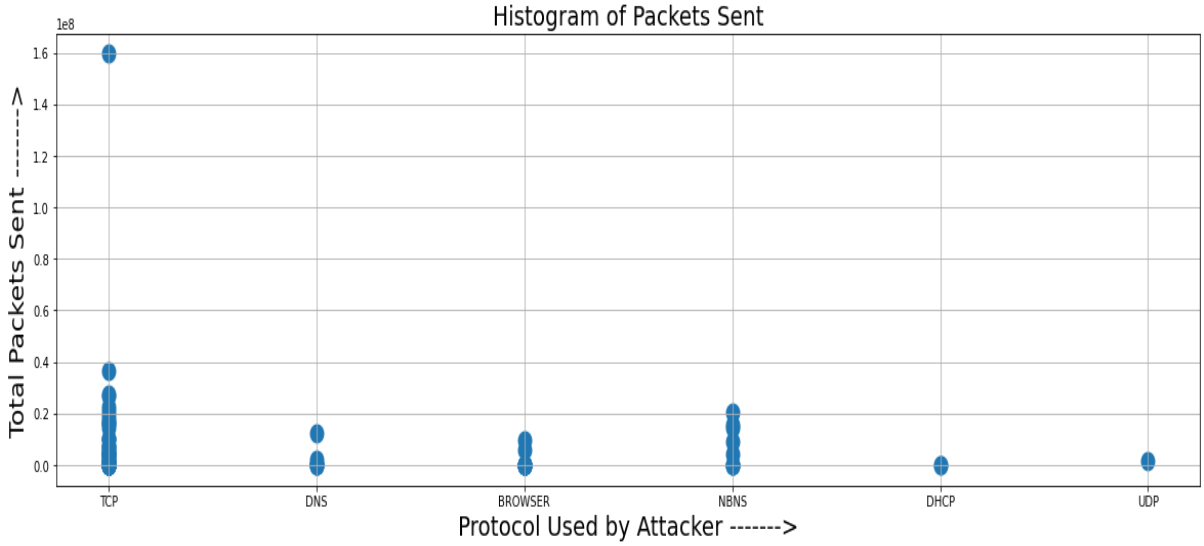
For every file in the output-Excel sheet, three histograms have been generated, and consist of common data on the y-axis (i.e., 'number of unique IPs,) and on the x-axis as follows: -

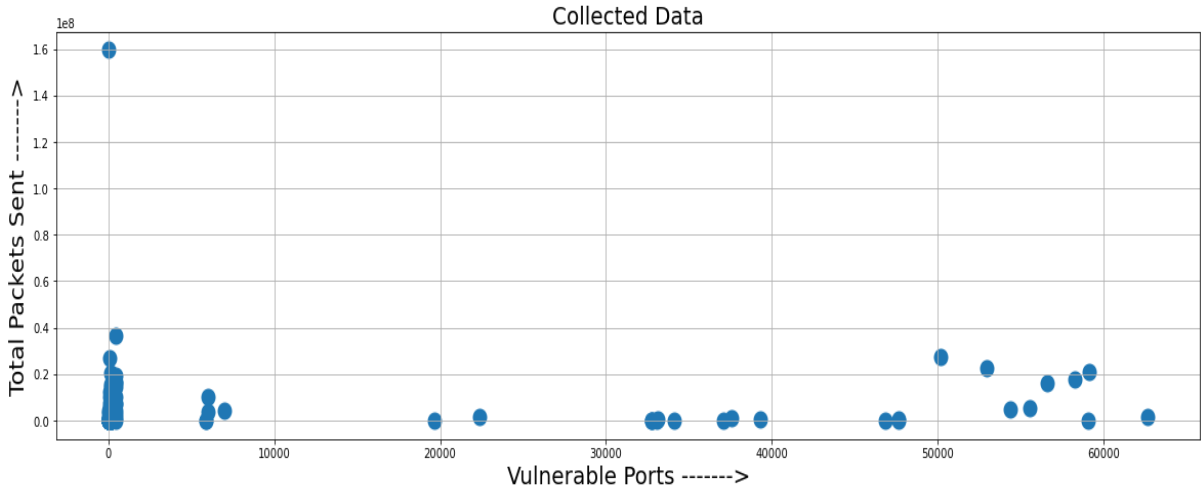
- The first shows us the protocols being used by the attackers.
- The second highlights the vulnerable ports that have been attacked.
- The third shows how long an attacker will usually spend attacking a host.

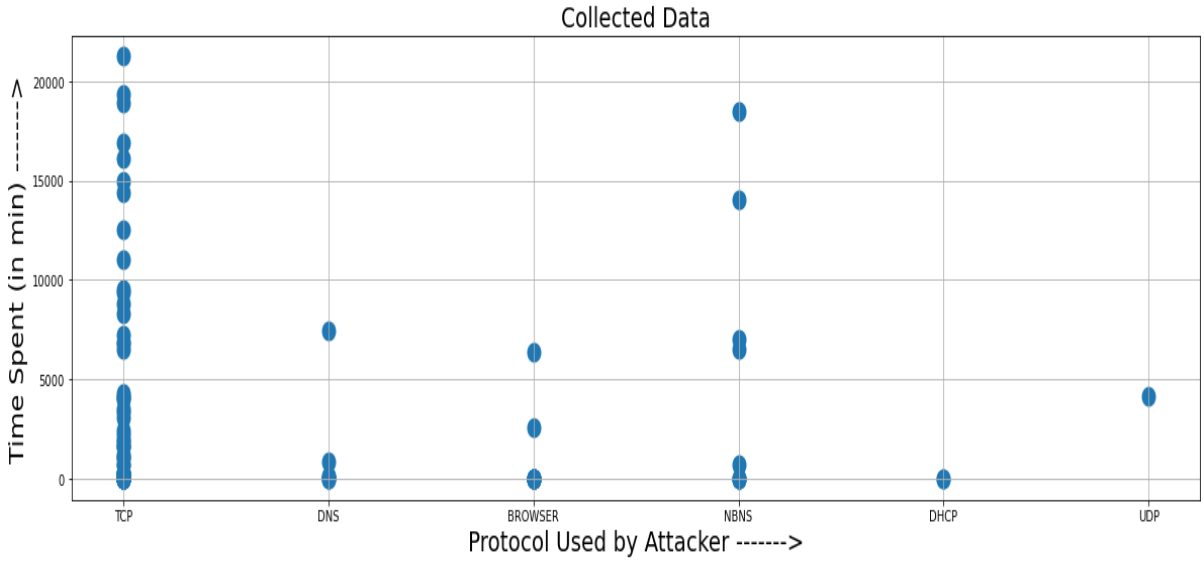
These results will help identify the particular groups of threat agents accessing a specific protocol for network penetration, which leads to determination of the category of the threat agent. For example, in the above figure, the TCP protocol is used by most IPs and the main target is the network layers. So, we can conclude that in this analysis, the threat agents have primarily been DDoS. Four histograms are generated by using data from all the files in the folder.

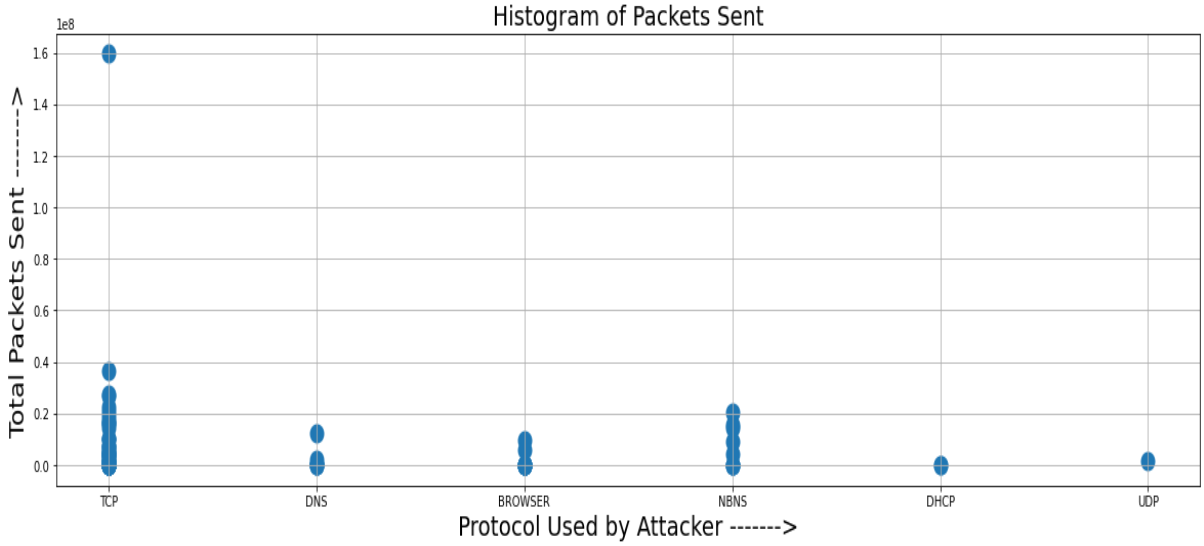

Collected Data
1e8
1.6
1.4
1.2
1.0
0.8
0.6
0.4
0.2
0.0
Total Packets Sent ------->
0
10000
20000
30000
40000
50000
60000
Vulnerable Ports ------>


Histogram of Packets Sent
1e8
1.6
1.4
1.2
1.0
0.8
0.6
0.4
0.2
0.0
Total Packets Sent ------->
TCP
DNS
BROWSER
NBNS
DHCP
UDP
Protocol Used by Attacker ------->


Histogram of Packets Sent
1e8
Total Packets Sent ------->
TCP
DNS
BROWSER
NBNS
DHCP
UDP
Protocol Used by Attacker ------->


Collected Data
1e8
Total Packets Sent ------->
Vulnerable Ports ------->

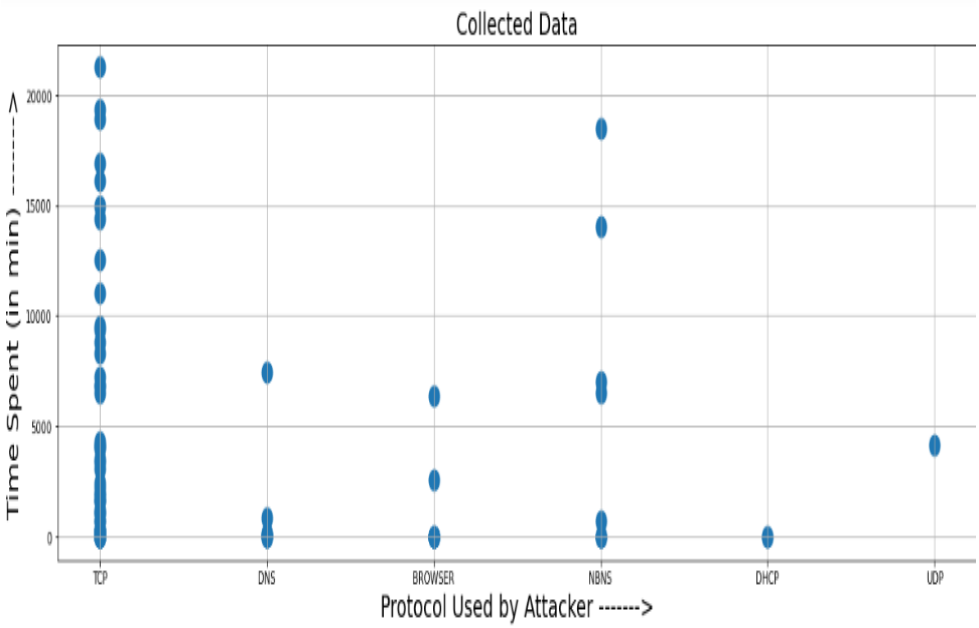

Collected Data
Time Spent (in min) ------->
TCP
DNS
BROWSER
NBNS
DHCP
UDP
Protocol Used by Attacker ------->



In the above figures, these histograms are based on the accumulated data in the potential output produced in the Excel sheets. They are used to represent the number of packets

generated for traffic during penetration testing, protocols, or layers used by threat agents and targeting vulnerable ports to achieve the goal.

- The first histogram is between ‘vulnerable ports’ and ‘total packets sent.’ This data shows how many packets were sent to which port on the host machine.
- The second histogram is between ‘protocol used by attacker’ and ‘total packets sent.’ This data shows the volume of packets for every protocol used to attack the host.



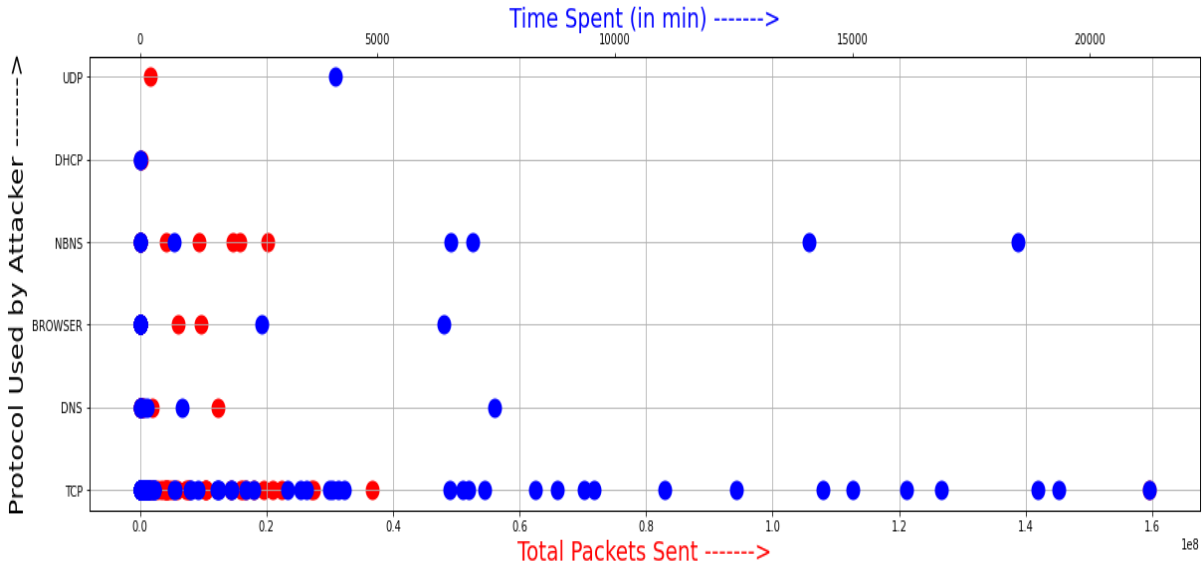


Figure 18 Histogram for Total Packets, Time, Protocol, and Collected Data

The above figure represents the histogram plotting the total data collected from each unique IP, the total time spent on the network, and the protocols used to attack the network.

- The first histogram plots the protocol used by an attacker against the time spent. This data highlights the amount spent by the attacker for every protocol used to attack the host.
- The second histogram shows the protocol used by an attacker on the y-axis with both total number of packets sent (in red) and time spent (in blue) on the x-axis. Even though these have different units, it gives us a statistically relative visual of how the time spent by the attacker varies with the number of packets sent for the same protocols.

4.6 Conclusion

Threats and threat agent's risks are emerging in the threat assessment of a network for an organization and the business of companies, and security risk management practitioners enable a mechanism to explore these risks and enforce their countermeasures based on the threat agent profiling and determining the critical threat intelligence feed to them. This paper presents a semi-automatic model based on the threat assessment of the PCAP files captured by the semi-automatic featured tools during a penetration testing run against the ESXi server of the University of Hertfordshire. The framework captured the data between 2012 and 2019

and illustrated the value of assets stored on the server, and the motivation, opportunity, and capabilities of the threat agents accessing the network. The situational awareness data is also evaluated by this semi-automatic model of threat assessment through exploration of the threat profiles for the historically captured data with the aid tools. Also, I provide the threat prevention practitioners with the idea of using an automatic model for the threat assessment of a network. This research's findings would support decision-makers management and software developer in building threat agent profiling for historical data. Determining critical threat intelligence feeds for the threat agent's groups might help evaluate new threats found in the network. Ultimately, I propose that future research directions work for the threat agent analysis models and methodology.

In future work, we aim to build an automatic-based vulnerability tree analysis security reference model as a security risk management tool to evaluate the security needs of PCAP files or data stream with sequential requirements of the next to the real-time informational environment. The CVE list available on the NIST can be extracted based on the analysis and implementation of PCAP files captured during the penetration testing against the network. These CVE lists will further be extracted based on their information or footprints captured by the design aid tool to generate an output as a vulnerability tree for the analysis of threat agents identified in the situational awareness data of a network. According to my analysis and implementation of threat assessment and study of various models and methodologies. I suggest that if the future model can automatically evaluate both threat assessment and vulnerability assessment for the PCAP files with the help of interactive tools, the complexity will be more effective than the existing model and methodology.

The ESXi server's PCAP file analysis was achieved by the interactive process of TensorFlow, which provides a semi-automatic approach for the threat assessment of the network. In this chapter, the model performs threat assessment for vast amounts of data based on threat agent profiling concerning their unique attributes. In this chapter, model analyses, the target IP address performs the penetration on which layer, protocol, number of packets generated during the penetration and location of the threat agent, etc. Based on all the information retrieved by running the threat assessment on the data collected from the server model, implement the cybersecurity profiles for the identified threat agent in the network. Threat agent profiling will help in the future threat assessment process of the network so that

newly identified threat agents can be mapped with the database created for threat agent profiling. It leads to time complexity optimization for analysing the newly identified threat agent in-network.

Chapter-5 Vulnerability Exploitation Analysis

5.1 Chapter Overview

Analysis and implementation of vulnerabilities is a challenging snag faced by the organization and business of society. However, in the modern information environment of the digital era, there is an obvious need to design a semi-automatic model to analyse and implement the vulnerabilities of the NIST database. Risk management practitioners should develop exposure implementations to provide security to their organization and business for the newly identified threats in live data collected in the future. The national vulnerability database (NIST) (Ralchenko, Kramida and Reader, 2008), which was developed by the US and maintains all acknowledged records of cybercrime and vulnerability registered with it by the various organization of countries worldwide. The vulnerability exploitation registered with the NIST database in 2020 are at nearly 18,000 and approximately 50 CVE lists are being telerecorded daily. It shows that attack an organization are increasing exponentially annually (Strom et al., 2018). Helsinki University Press reported a nearly 43% increase in vulnerability registration from different sources each year (Geerts, 2020). Since the patterns reported of vulnerabilities is very high of other countries are constantly facing threat agents snags in their environment. Various organizations spend lots of money on security practitioners to keep their environment free from risk caused by threat agents. Therefore, the National Infrastructure Advisory Council introduced the CVSS scoring system of vulnerabilities exploitation faced by various organizations. It can be proposed for drafting with NIST, which the security risk management team may use as a reference to address the new threat in an organization’s network.

As shown in fig below, cybercrime and vulnerability exploitation exponentially increase yearly referencing the covid 19, and most organisations' work-from-home trends are rising. Because of this, essential files, documents, and meetings with clients or teams are going online with the help of applications or web browsers. Most of the work is accomplished via VPN (virtual private network) connections, and work-related files are shared with clients and the other team members via VPN or online. Therefore, in 2020, vulnerability exploitation increased at a rate of 8.3%, which can be observed in the histogram (Grother, 1995).

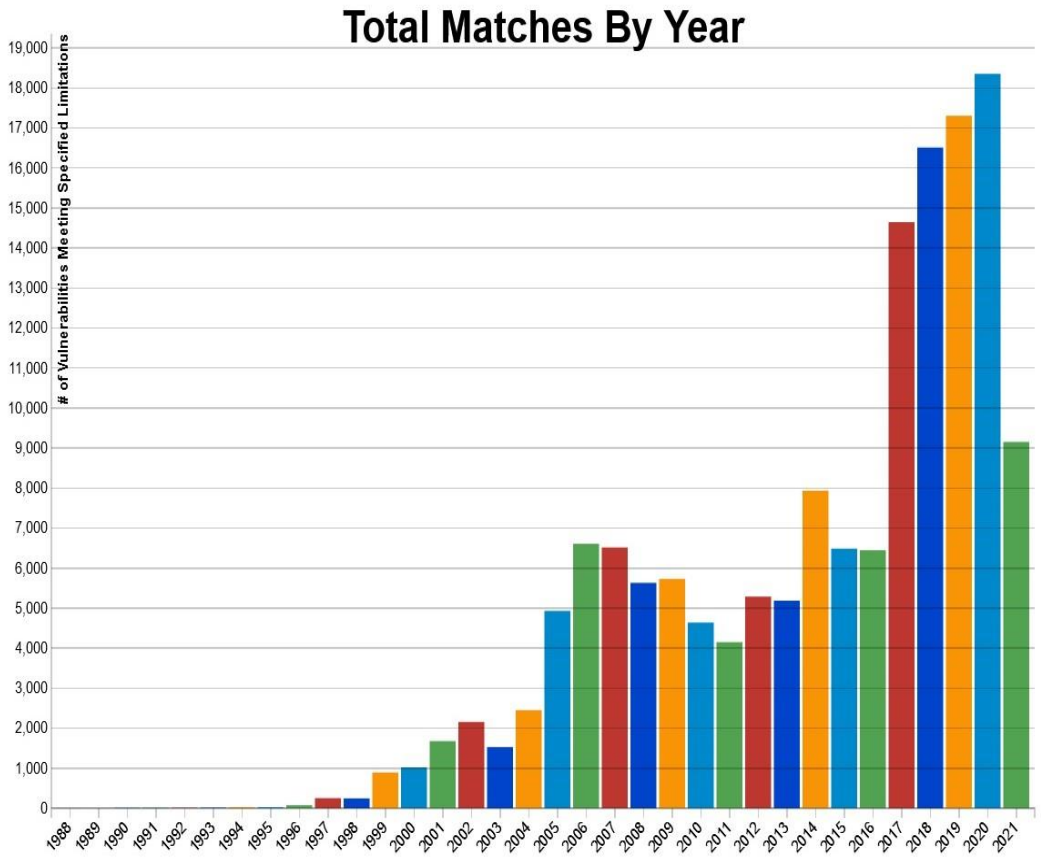


Fig. 19: Vulnerability Exploitation of NIST Database (Sharma et al., 2022)

The CVSS score is widely accepted by vulnerability management tools, but it is only the CVSS score, so we cannot effectively address vulnerability exploitation. To improve the prediction ability of risk management teams, they need more attributes about the vulnerability exploitations in detail. Later they can use them as references to compare with characteristics and features of newly identified threats in the network. To solve a problem, this research introduces a semi-automatic model for vulnerability analysis, which handles all the CVE lists of the vulnerabilities available in the NIST database between the years 1999 and 2021. The semi-automatic model extracts all the information related to the CVE from the database based on the attributes shown in the tables below.

Table 9. Environments and Attack Vectors of Threat Agents.

Environments used by a threat agent to exploit the network	**Attack vectors of threat agents**
Windows 10.	Physical.

Windows 8.	Network.
Linux Kernel Version.	Adjacent.
MY SQL.	Local.
Postgres.	
Apache.	
Apple (Xcode 1.5)	
Samba (2.18.13)	

Table 10. Inputs and Potential Result of Threat Agents.

Pre-Requisites inputs of threat agents	**Potential results of the threat agents**
Credential:	Credential acquisitions
Root privileges:	Privilege escalation
Remote access:	Remote access
Local access:	Denial of services
Network access:	Run arbitrary commands
	Data access
	Data manipulation

In the existing models and methodology for vulnerability exploitation analysis, there is no general solution for addressing the vulnerability exploitation of the CVE list of the NIST database. The need arises for all risk assessment management practitioners to provide a proper solution for vulnerability exploitation. All these models analyse the footprints of the threat agents and the approaches followed by the threat agent for exploiting the system's vulnerability with the help of the vulnerability tools available. So, my work must provide a novel tincture to such a snag with optimized time complexity and system effectiveness. The existing model addresses vulnerability exploitation manually or uses traditional tools such as NESSUS, Netsparker, OpenVAS, Arachni, NMAP, Acunetix, etc. Because of this, the time complexity of the system is very high (Ruiter et al., 2017). To provide an effective solution for optimizing the time complexity, the model uses semi-automatic approaches to address the vulnerability list of the NIST database. The main contribution of this research work is as follows:

- We are implementing a semi-automatic model to analyse the vulnerability exploitation of the NIST database.
- The traditional approaches of vulnerability prioritization depend on the CVSS score. In contrast, our work prioritizes vulnerability with the help of the CVSS score. It includes the other attributes of threat agents including environment, attack vectors, Pre-requisites inputs, and potential outputs.
- This work implements the groups of threat agent lists based on the vulnerability analysis achieved by the model between 1999 and 2021.

5.2 Background of Vulnerability Analysis Work

A standard vulnerability scoring system (CVSS) is characterized based on numerous risk assessment models (Allodi et al., 2017) (Teixeira et al., 2015)**,** is vendor-independent, and is a universal scoring system that can be used for the quantitative measurement of the severity of various software vulnerabilities. Software vulnerabilities have many risks, and CVSS neutralizes these effects depending on the risk (Feutrill et al., 2018). This vulnerability exploitation of software identification depends on several factors, such as the environment, the platform used by the threat agent's groups, the number of inputs used to penetrate the network, the number of identified attack vectors of the threat agents, and the potential outputs of the threat agents. The scores in CVSS are premeditated based on three attributes and equations, namely temporal, environmental, and base. The vulnerabilities alter over time and the temporal attributes provide the information about the same. The information environment an organization's system on the other hand, can provide circumstantial information on an environment and this is delivered by Environmental attributes (Feutrill et al., 2018)**.** Unlike temporal and environmental attributes, the values and scores of base attributes are openly accessible in NVD and signify vulnerability inherent physiognomies.

CVSS has various weaknesses, and the Vulnerability Rating and Scoring System (VRSS), on the contrary, has a better assortment of scores (Munaiah and Meneely, 2016) (Samuel, Aalab and Jaskolka, 2020). One of the many drawbacks of CVSS is that the dissemination of the base score is extremely bimodal, and numerous blends of attributes yield the matching concluding score (Feutrill et al., 2018)**.** The accuracy of these calculated scores is also suspicious (Munaiah and Meneely, 2016) (Alfadel, Costa and Shihab, 2021)**.** Sometimes, the CVSS score found in the NIST database is not determined the same when risk management

practitioners mapped newly identified threat agents in the network. It might have happened because the environment and inputs used by the threat agents changed with time and modernization in the informational settings**.** However, there is no indication that VRSS scores are more illustrative than CVSS scores (Allodi et al., 2018)**.**

Moreover, numerous categories of prejudice (bias) influence the data in vulnerability databases, which overpowers detailed statistical investigation (Ruohonen et al., 2018). There are shreds of evidence in the literature that the CVSS base score, when tested unaided, is unsuitable for targeting vulnerability prioritization (Berhe et al., 2021) (Pendleton et al., 2016)**.** This metric was not enough to elaborate on the information context in which risk management practitioners can deploy their approach to analyse the vulnerability. The probabilistic rate of attack or exploitation iteration is impossible to understand with regards to conditions or the environments used by the threat agent groups that may exist in the early stage of the design phase. It reckons on hypothesizing and theorizing, which does not help identify and incorporate appropriate security of mitigations. In (Allodi, 2017)**,** the authors claimed that using CVSS scores as a random tactic is practical. The cause of such assumptions is that many vulnerabilities with high severity have not been exploited much (Alfadel, Costa and Shihab, 2021)**.**

Security experts have articulated the requirement for temporal data**.** CVSS temporal data provide information that can predict forthcoming exploitations in the black market (Allodi, 2017)**.** Unfortunately, however, this information is not available in NVD (National Vulnerability Database). End users cannot find this information conveniently, because it exists in various forms and limited sizes on vendor sites. In these above-stated circumstances, unconventional methods are indispensable to advance proactive security. It can be effectuated by predicting the vulnerable software components on the development side or expecting how many vulnerabilities will be there in the future (Joh and Malaiya, 2014).

Moreover, deployment is tricky, requiring information about existing vulnerabilities. The authors of CVSS try to advance its extensiveness by providing improved portrayals of vulnerabilities. Every new version of the CVSS standard has presented some more additions and variations in the given set of attributes (Cisar et al., 2016) (Franklin, Wergin and Booth, 2014). However, many additional aspects strongly influence the threat and are not counted with the prevailing methodologies. There is a human agent behind every attack with an

incentive (Jing et al., 2014). I have presumed that considering the attacker's characteristics in the vulnerability polarization may help to progress in system security.

5.3 Semi-Automatic Model (SATAM)

The CVE list deduced from the model's collected data is delineated with the CVE list of the NIST database. After that, prioritization will be achieved based on the CVSS score available in the database and the attributes determined by the vulnerability tree analysis of the semi-automatic model. The model design spawns the CVE list of vulnerability exploitation characteristics available in the NIST database. To modify, such a list model uses the approach of an interactive Python library available on Jupyter notebook and designed the algorithm. The algorithm takes all the NIST databases for the years 1999-2021 as input. It produces the eviscerated data of all CVE lists excluding all the rejected files, corrupt files, and connection lost data files. The eviscerated data becomes the algorithm's input and produces the attributes of the threat agents such environments, pre-requites input, attack vectors, and potentials outputs identified in the database as results. Similarly, the algorithm creates an Excel sheet of all the CVE lists of the NIST database based on the following information about threat agents:

- The threat agent's use of the environment or the system's configuration to exploit the vulnerable ports of the network.
- The inputs and the list of tools used to exploit the vulnerable ports of the network.
- The attack vectors or the footprints used to exploit the network.
- The potential aftermath of a threat agent group's exploitation of an informational environment's network.

The below algorithm is contriving for producing the Eviscerate data from the NIST database.

Algorithm-1:

Step 1: i=0

Step 2: index= []

Step 3: for value in df["Description"]:

Step 4: if "** RESERVED **" in value or "** REJECT **" in value:

Step 5: index. Append(i)

Step 6: print(value)

Step 7: i += 1

Step 8: df. Drop (index, in place=True)

Step 9: print (df. shape)

The algorithm initially downloads the vulnerability database from the internet, and the data can be downloaded in CSV format. When data is downloaded from a website, its size is enormous and it contains unwanted rows and columns. Unwanted rows and columns refer to CVE lists that do not include comprehensive or accurate information in accordance with the model's requirements for treating agent groups. Given the limitations of the database, I created a Python script technique to extract the database based on the model's needs. Initially, set the I increment to zero and start the script. Next, the database is input in CSV format and all the rows and columns with reserved and refuse keywords in their attributes are removed, because these keywords are no longer required to determine information about threat agents. The model then creates CSV format data while removing undesired data from the input source as potential output. The new output will be regarded as input in the following step of the algorithm, which will then generate the output in the form of an Excel sheet based on the environment's needed keywords connected with threat agent groups, attack vectors, prerequisites input, and finally, the potential output.

5.4 Evaluation of Vulnerability Exploitation

The evaluation of vulnerability exploitation can be procured by designing the model's vulnerability tree analysis for the NIST database. The data-flow diagram of tree analysis from root to bottom is shown in the figure below. Here the core consists of all the NIST databases available on the NVD. This root consists of all the registered CVEs listed from various world organizations, including the corrupt, rejected, and no information open CVEs. A vulnerability assessment identifies, classifies, defines, and prioritizes vulnerabilities in computer systems, applications, and network underpinnings and provides assessing the organization with the necessary awareness, knowledge, and risk background to understand the threats to its environment and to retaliate judiciously. The vulnerability tree analysis can be cast-off to evaluate the exploitation of a particular CVE of the threat agent. Asset value represents an organization's assets, and the summation function represents the threat agent's attributes.

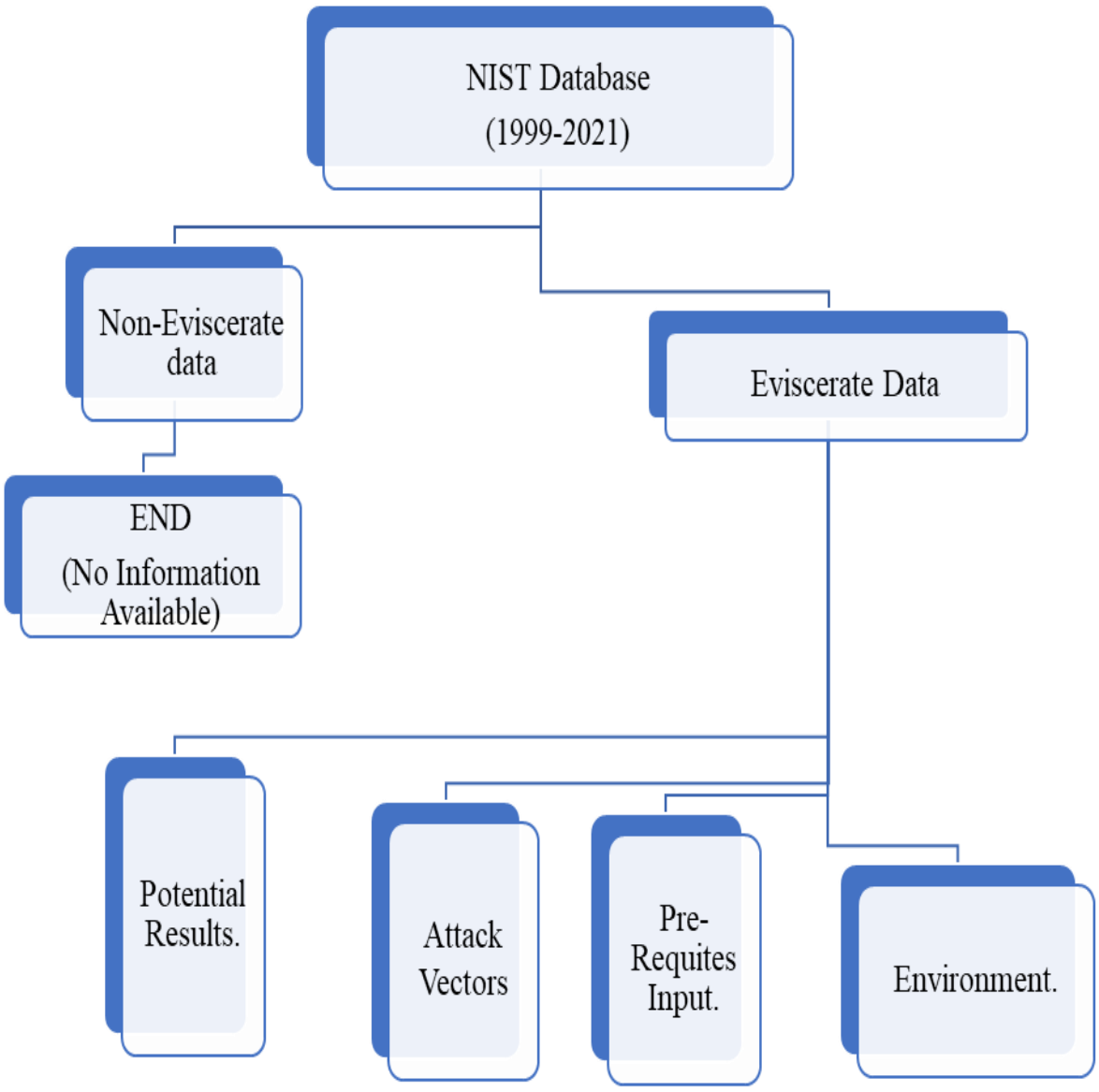


Fig. 20: Vulnerability Tree Analysis.

Vulnerability pertains to the inherent weaknesses present within susceptible ports, whereas the impact signifies the extent to which threat agent groups can influence and affect the network's operational integrity. In the evaluation phase of the vulnerability exploitation for the NIST database, 205,773 vulnerabilities were catalogued from 1999 to 2021. The model ascertains the attack vectors and the potential outputs for all these vulnerabilities in a semi-automatic manner, optimizing complexity compared with subsisting approaches.

Vulnerability Level	Knowledge Level	Incognito
1)	No knowledge of computer level 0	None
2)	Primary education level 1	Not enough
3)	Secondary education level 2	Not enough
4)	High school level 3	Not enough
5)	Intermediate school level 4	Not enough
6)	B-tech in computer science level 4	Script
7)	M-tech in computer science level 5	Amateur
8)	MPhil in computer level 6	Amateur
9)	PhD in computers level 7	Hacker
10)	Postdoc in computer level 8	Good hacker
A)	PhD and post-doc level 9	Better hacker
B)	High knowledge of computer level 10	Best hacker
C)	Criminal record in cyberspace Level expert	Expert/criminal hacker

Table 11: Vulnerability Exploitation Flatten.

The vulnerability tree analysis of exploitation for the NIST database CVE list traverses the threat agent group's source and destination IP address from root to bottom leaves (left and right child) of the trees. The model sways the capability and level of knowledge for these threat agent groups concerning the CVE identified in the database, designs the vulnerability trees, and provides the position of the various CVEs in the tree followed by the top to the bottom approach of traversing. In Table 11, the model's vulnerability levels can be assigned to the identified threat agents in the network, corroborating to CVEs hypothecated to those threat agents in the NIST database. Based on the information available for the CVE in the database, our model can extract the capability, opportunity, motivations, and level of knowledge acquired by threat agents to penetrate an organization's network.

According to "The Basics of Hacking and Penetration Testing by Dr Patrick Engebreston" (Engebretson, 2013), threat agents generally fall into two types. One is enacting penetration testing with permission, white-hat hacking, and the second is performing unethical hacking, black-hat hacking. Concerning hacker studies, our model provides the levels of indexing for

particular threat agents according to their capability, motivation for exploitation, and the knowledge level they used against an organization's vulnerable port. In general, for those hackers who are performing penetration testing as ethical hackers, model assigns them a number or alphabet according to their level of knowledge. On the other hand, the model assigns those performing unethical hacking the letter 'C' in recognition to their level of expertise, which represents a very high priority or major concern for any business of an organization.

5.5 Analysis of NIST Database Vulnerability

This section will discuss the aftermath of the semi-automatic model for vulnerability exploitation analysis of the NIST database. In the previous section, we have described the environment used for data collection from the network. Concerning the characteristics of data stream, our model determined the CVE list for the identified threat agent in a network. Based on the CVE list analysis, risk management practitioners can suggest the priority lists for the vulnerable ports available in the information environment network of an organization. Similarly, our model used an interactive Python library (Tavenard et al., 2020) available on the Jupyter Notebook to optimize the process of manually determining the vulnerable ports from the CVE list available on the NIST database. To aid snags, our model designs an algorithm in such a way that it reads all the registered CVE lists of the NIST database. These lists contain all types of cybersecurity exposures registered with NIST from different world organizations.

These CVEs consist of a list of vulnerable ports from a number of different platforms and environments targeted by the number of threat agent's groups identified in an informational setting. To address the threat agent group's specifications of the system used to penetrate an organization's network, our model implements an algorithm that analyses all the data available on the NIST database from 1999 to 2021 (Smith, Martell and Motekaitis, 2004). The data analysis is carried out in several steps as follows:

1. Initially, the algorithm runs against the NIST database, determines all the data registered with NVD which must include of information about the minimum parameters assigned by the NVD for each CVE to be registered with it.

2. The list of cleaned CVEs is available as an output, consisting of only those CVEs that passed the minimum NVD requirement.
3. The algorithm of the semi-automatic model takes these cleaned CVEs as input and performs the analysis based on the characteristic features available with them.
4. The algorithm carries out the analysis on the CVE list concerning the environment or the platform used by the threat agent groups.
5. The subsequent analysis is carried out based on the input and the resources used by threat agent groups for penetrating the network.
6. The subsequent analysis is based on determining the attack vectors for the threat agent groups.
7. Finally, potential outputs for the threat agent groups are retrieved from the NIST database.

The figure below shows that when the model runs the first phase of an algorithm, we determine 205,763 entities of CVE in the database. After that, the algorithm starts picking the CVE list of data, excluding the rejected, reserved, and corrupt files from it. The semi-automatic model determines that there are 151,833 entities of CVE available in the database between 1999 and 2021 (Smith, Martell and Motekaitis, 2004.) Simultaneously, the next phase of the algorithm is guillotined (executed) and runs arbitrary commands on the CVE list, excluding the file's reject, reverse, and corrupting. Furthermore, the model starts implementing and analysing the number of rows and columns in the cleaned datasets.

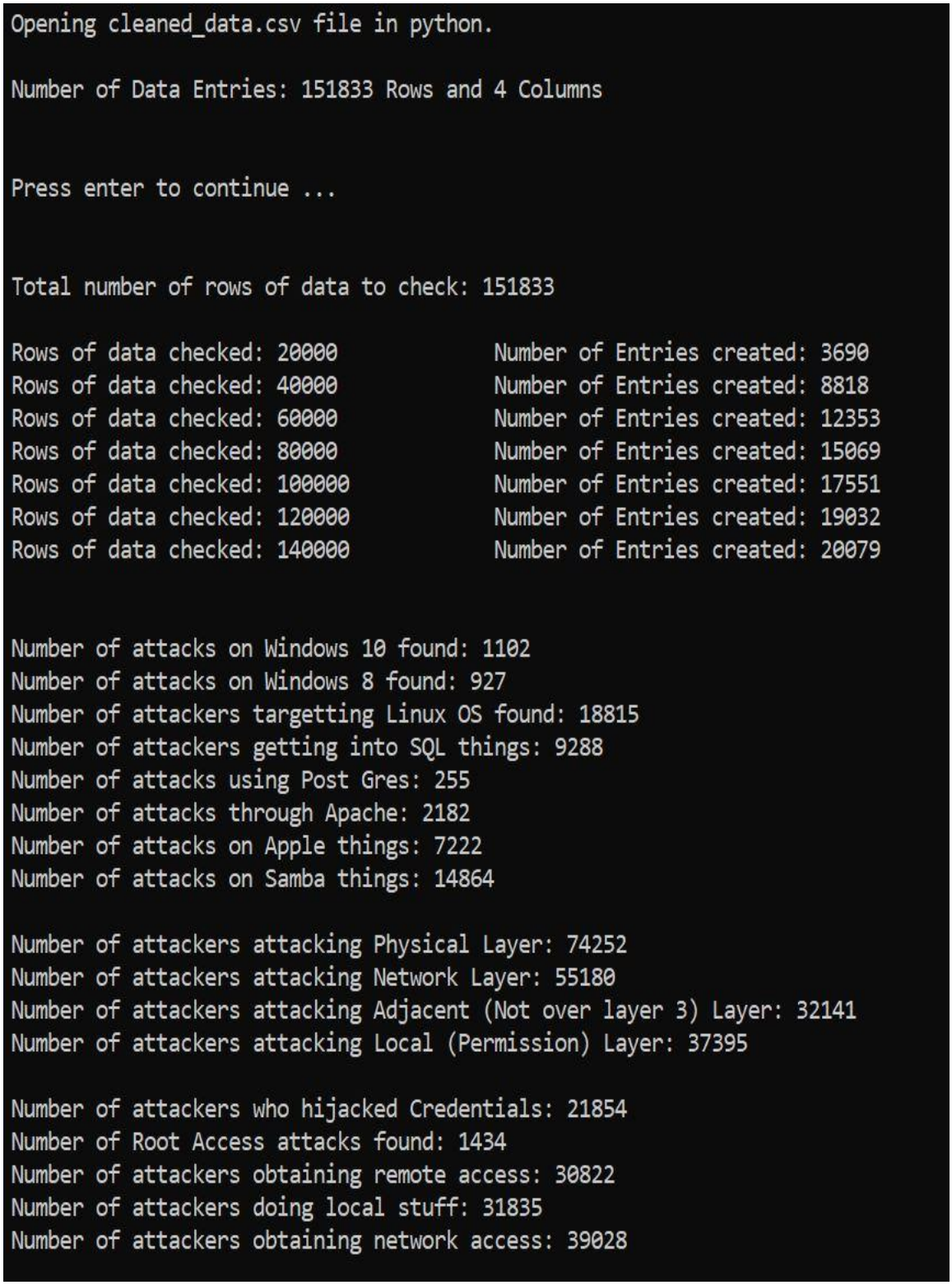


Fig. 21(a): Analysis of Eviscerate Data of NIST.

The first iteration of 2,000 rows executed by the model identified 3,690 entities in the attributes list available for the vulnerability exploitation of the ports. In the same way, the

next iteration of 2,000 rows placed 8,819 entities, the next 2,000 rows found 12,353 entities, and the last iteration determined that 20079 entities were in the outputs.

In the next phase, the semi-automatic model determines the number of attacks executed with the help of different environments or the platforms used by the threat agents. The number of attacks identified on Windows 10 is 1102, Windows 8 is 927, Linux is 18815, SQL is 9,288, postgres is 255, Apache is 2,182, Apple iOS is 7,222, and Samba is 14,864. The model's input and resources in the database can be unyielding by the information (Input) and resources used by these threat agent groups in the database. The risk management team illustrates an organization's network's loopholes or vulnerable ports. In this way, prioritizing vulnerable ports and identifying open ports can be persistent later, which could be cast-off for referencing the opportunity available for the threat agents in a network of an informational environment network.

The model determines the attack vector inputs of threat agent groups such as user credentials, root access, remote access, local access, network access, etc., based on the environment, the information (input), and the resources or tools used by the threat agents to penetrate the network. Identifying attack vector inputs is essential in prioritising the vulnerability identified for a network. Suppose the attack vector input list of the NIST database is already available in a semi-automatic way. In that case, the potential outputs of the attack vectors can be handed down to reference the newly identified threat from the network. In this way, the time complexity of determining a network's vulnerable ports would be low compared with that of conventional approaches followed by a model and methodologies (Sgandurra and Lupu, 2016) (Aufner, 2020). Finally, the last iteration of the algorithm is executed on the NIST database. The model uses identified environments, inputs, and attack vectors for all the CVEs of a clean database as input and determines the potential consequences of outputs for the vulnerability analysis. These potential outputs illustrated the Credential acquisitions, privilege escalation, remote accesses, denials of service, running of arbitrary commands, data access, and data manipulation as the embryonic results of the threat agents determined from the NIST CVE list.

Fig. 21(b): Analysis of Eviscerate Data of NIST

The above figure indicates the identified threat vectors and the potential outputs of threat agent groups from the NIST database. The threat vectors analysis is obtained through the database's model by determining the threat agent group's footprints information in the CVE list. The threat agents used layers such as physical, network, adjacent, and local of the network to attack the particular network of an organization. Once the risk management practitioners list the layers the threat agent groups used to penetrate the network, the model can effectuate the identification of threat agent pigeonholes. Attack vectors are the methods that antagonists use to breach the network level or pervade the particular network of an organization. Attack vectors take many forms, such as man-in-the-middle attacks, malware,

ransomware attacks, compromised credentials, phishing, etc. There are mainly two categories of attack vectors: active and passive (Ullah et al., 2018) (Haber and Hibbert, 2018). Dynamic attack vectors exploit the alteration of the system by generating some system commands that run against the organization, such as untrodden vulnerabilities, man-in-middle attacks, domain hacking, email spoofing, malware, and ransomware. On the other hand, passive attack vectors exploit the system in such a way as to gain unauthorized access to the system, such as phishing, social engineering attacks, and typos squatting attacks.

5.6 Study and Analysis of Vulnerability Databases

The study and analysis of vulnerability databases involves examining extensive data collections describing security vulnerabilities in software, hardware, or other digital systems. These databases typically contain information about vulnerabilities discovered by security researchers, hackers, or other individuals. They often include details about the types of vulnerabilities, the affected systems or software, the severity of the vulnerabilities, and the steps needed to fix or mitigate them.

The purpose of analysing vulnerability databases is to understand the security landscape better and identify patterns or trends that can help improve security practices (Nisioti et al., 2018). Some standard techniques used in the study and analysis of vulnerability databases include the following:

- **Statistical analysis:** This involves using data mining and other statistical techniques to identify patterns in vulnerability data, such as the most common types of vulnerabilities, the most vulnerable software products, or the most frequently exploited vulnerabilities.
- **Threat modelling:** This involves using the data in vulnerability databases to potentially model threats to specific systems or networks. Security professionals can develop more effective security strategies and countermeasures by identifying potential attack vectors and vulnerabilities.
- **Risk assessment:** This involves using vulnerability data to assess the overall risk of specific systems or networks. By combining vulnerability data with information about the value and criticality of the systems being protected, security professionals can prioritize security efforts and allocate resources more effectively.

- **Predictive analytics:** This involves using vulnerability data to predict future trends in security threats and vulnerabilities. By analysing patterns and trends in vulnerability data, security professionals can anticipate emerging threats and develop proactive strategies to mitigate them.

Overall, the study and analysis of vulnerability databases is an essential tool for improving cybersecurity and protecting digital systems from malicious attacks. By leveraging the wealth of data contained in these databases, security professionals can gain insights into the nature of security threats and vulnerabilities and develop more effective strategies to prevent them.

- The UNB ISCX (Internet of Things Security Information Sharing and Analysis Centre) (Nisioti et al., 2018) database is a publicly available dataset containing network traffic data captured from various sources, including IoT devices, desktop computers, and mobile devices. The University of New Brunswick in Canada created the database to support research on network security. In terms of vulnerability analysis of threat agent attributes, the UNB ISCX (Chen et al., 2017) database can be used to analyse the behaviour of attackers and the characteristics of their attacks. The database includes various network traffic data, including packet captures, network flow records, and application logs, which can be used to identify and analyse various types of attacks, such as port scans, malware infections, and DDoS attacks.
    - The UNB ISCX database includes a range of attributes that can be used to analyse threat agents, including their IP addresses, the protocols and ports used in their attacks, the types of attacks they carry out, and the payloads of their attacks (Saad et al., 2011). By analysing this data, researchers can gain insights into the behaviour of attackers and the tactics they use to exploit vulnerabilities in software and networks.
- CAIDA (Cooperative Association for Internet Data Analysis) (Walsworth et al., 2015) is a research organization that focuses on studying and analysing data related to the internet, with a particular focus on network security and stability. CAIDA has developed several databases that can be used for vulnerability analysis, including the Spoofer, the UCSD Network Telescope, and the Darknet Dataset. The Spoofer is a database that tracks Internet Protocol (IP) address spoofing, which is a technique used by attackers to conceal their identity by falsifying the source IP address of a packet. The Spoofer collects data on IP address spoofing incidents and provides information

on the sources of the spoofed packets, the types of spoofing techniques used, and other relevant attributes.

    - The Darknet Dataset is a collection of data on IP addresses that are not intended for public use, such as those assigned to private networks or not in active service. The dataset identifies and analyses malicious activity directed at these IP addresses, such as attempts to scan for or exploit known vulnerabilities. By providing information on the sources of malicious traffic, the types of spoofing techniques used, and the behaviour of threat agents, these databases can help identify network vulnerabilities and develop strategies for defending against cyber threats.

- The MAWI (Measurement and Analysis on the WIDE Internet) (Cho, Mitsuya and Kato, 2001) database is a publicly available repository of network traffic data collected from various sources worldwide. The database contains large volumes of raw network traffic data, which can be used for various research and analysis purposes, including vulnerability analysis of threat agent attributes. The MAWI database can be used to study various attributes of threat agents, such as their behaviour, tactics, and tools. For example, by analysing network traffic data in the MAWI database, researchers can identify patterns of activity associated with known threat actors or malware families. They can also study the characteristics of network traffic associated with specific types of attacks, such as DDoS attacks or phishing campaigns. One way to perform vulnerability analysis of threat agent attributes using the MAWI database is to use machine learning techniques to identify anomalous network traffic patterns. By training machine learning models on large volumes of network traffic data from the MAWI database, researchers can develop algorithms that can automatically detect and classify suspicious network activity, which can be indicative of a potential vulnerability or threat.
- LBNL (Lawrence Berkeley National Laboratory) (Paxson, 2005) database is research that focuses on analysing the attributes of threat agents in order to identify potential vulnerabilities in critical infrastructure. The database is designed to collect and analyse information about threat agents, including their motivations, capabilities, and resources. The LBNL database aims to provide a comprehensive understanding of the threat landscape, which can help organizations identify and prioritize their security

measures. By understanding the attributes of threat agents, organizations can better anticipate potential attacks and take proactive steps to mitigate the risks. The LBNL database is a valuable resource for vulnerability analysis, as it provides a detailed understanding of the motivations and capabilities of potential attackers. By using the database to identify vulnerabilities in critical infrastructure, organizations can take steps to mitigate the risks and protect against cyberattacks.

- UNIBS (University of Brescia) (Elbaz, Rilling and Morin, 2018) database is a database that is used for vulnerability analysis of threat agent attributes. The database contains information about different types of threat agents, including their attributes, behaviours, and attack methods. It is designed to help security professionals and researchers analyse and identify vulnerabilities in computer systems, networks, and other digital assets. The UNIBS database includes several categories of threat agent attributes, such as the following:
    - Technical attributes: These include information about the technical capabilities of the threat agent, such as the operating system, hardware, and software tools used to carry out attacks.
    - Operational attributes: These include information about the operational characteristics of the threat agent, such as the size and structure of the organisation or group that the threat agent belongs to, as well as their strategies and tactics for carrying out attacks.
    - Behavioural attributes: These include information about the behaviour of the threat agent, such as their motivations, goals, and decision-making processes.
    - The UNIBS database is designed to be combined with other vulnerability assessment tools and techniques, such as risk assessment, penetration testing, and threat modelling.
    - The DARPA (Haines et al., 2001) database that is relevant to the vulnerability analysis of threat agents' attributes is the Cyber-Insider Threat (CINDER) database. The CINDER database is designed to support research on insider threats to computer networks, which are threats that come from individuals within an organization who have authorised access to the network. The CINDER database includes data on a variety of attributes related to insider threats, including the following:

- User behaviour: The database includes data on user activity on the network, including login times, file access, and network traffic.
- Network activity: The database includes data on network traffic and communication patterns, including data transfers, email activity, and web browsing.
- Endpoint activity: The database includes data on activity on individual endpoints, such as laptops and desktops, including file access, software installations, and system logs.
- Contextual information: The database includes contextual information about users and their activities, including job roles, security clearances, and past incidents.

- Researchers can use the CINDER database to develop models and algorithms to identify insider threats and predict future incidents. The database is intended to be used to develop new technologies and techniques for detecting and preventing insider threats, ultimately improving computer network security.
- The KDD99 dataset (Cup, 2007) is a well-known dataset used in the field of intrusion detection and vulnerability analysis. It was developed by the Knowledge Discovery and Data Mining (KDD) process and was used as part of the Third International Knowledge Discovery and Data Mining Tools Competition in 1999. The dataset contains network traffic data collected from a simulated military network and is commonly used to evaluate the performance of intrusion detection systems. In the context of threat agent attributes, the KDD99 dataset includes information about various attributes of network traffic that can be used to identify potential threats, such as:
  - Protocol type: This attribute specifies the protocol used in the network traffic, such as TCP, UDP, or ICMP.
  - Service: This attribute specifies the type of service used in the network traffic, such as FTP, HTTP, or Telnet.
  - Source and destination address: These attributes specify the IP addresses of the source and destination hosts involved in the network traffic.
  - Duration: This attribute specifies the duration of the network traffic.

- Flags: This attribute specifies the flags used in the network traffic, such as SYN, FIN, or RST.
- Number of packets and bytes: These attributes specify the number of packets and bytes involved in the network traffic.

By analysing these attributes, intrusion detection systems can identify potential threats and vulnerabilities in the network and take appropriate action to prevent or mitigate attacks. The KDD99 dataset has been widely used in intrusion detection and vulnerability analysis research and has helped improve these systems' accuracy and effectiveness.

- DEFCON (defence readiness condition) (Lim, Baumgarten and Colton, 2010) is a term used by the US Department of Defence to describe the level of readiness of the US military in the face of a threat. The term is also used in the cybersecurity community to describe a series of annual hacking conferences held in Las Vegas, Nevada. There is no specific “DEFCON database” in the context of vulnerability analysis of threat agent attributes. However, at the DEFCON conferences, researchers and security professionals often share information about vulnerabilities and threat actors and discuss strategies for identifying and mitigating cyber threats. These discussions can include information about the attributes of threat agents, such as their motivations, capabilities, and tactics. The DEFCON conferences have also been used as a venue for competitions, and challenges focused on vulnerability analysis and exploitation. For example, the “capture the flag” (CTF) contest at DEFCON involves teams competing against each other to identify and exploit vulnerabilities in a simulated network environment. Overall, while there is no specific database associated with DEFCON in the context of vulnerability analysis, the conference serves as a platform for sharing information, discussing best practices, and developing new approaches to identifying and mitigating cyber threats (Nisioti et al., 2018).

	A	B	C	D	E
1		Environments	Attack Vectors	Pre-Requisites	Potential Results
2		1. Windows 10	1. Physical	1. Credentials	1. Credential Acquisition
3		2. Window 8	2. Network	2. Root Previledge	2. Priviledge Escalation
4		3. Linux Kernal version	3. Adjacent (Not over layer 3	3. Remote Access	3. Remote Access
5		4. My SQL	4. Local (Permission)	4. Local Access	4. Denial of Service
6		5. Post Gres		5. Network Access	5. Run Arbitrary Command:
7		6. Apache			6. Data Access
8		7. Apple (Xcode 1.5)			7. Data Manipulation
9		8. Samba (2.18.13)			
10	CVE ID	Environments	Attack Vectors	Input Pre-Requisites	Output Results
11	CVE-1999-0002	3	2, 3	2	2
12	CVE-1999-0032	3	1, 4	4	5
13	CVE-1999-0070	6	1	5	6
14	CVE-1999-0123	3	1	4, 5	6
15	CVE-1999-0137	3	1, 2, 3	2, 4	2
16	CVE-1999-0179	8	1, 4	5	5, 6
17	CVE-1999-0182	8	2, 3	2	2
18	CVE-1999-0183	3	1	5	6
19	CVE-1999-0242	3	1	5	6
20	CVE-1999-0243	3	2, 3	2	2
21	CVE-1999-0262	3	1, 2, 3, 4	3	3, 5
22	CVE-1999-0289	6	1	5	6
23	CVE-1999-0298	3	1	4, 5	6
24	CVE-1999-0316	3	1, 2, 3	2, 4	2
25	CVE-1999-0317	3	1, 2, 3	2, 4	2
26	CVE-1999-0330	3	1, 2, 3	2, 4	2
27	CVE-1999-0340	3	1, 2, 3	2, 4	2
28	CVE-1999-0341	3	1, 2, 3	2, 4	2
29	CVE-1999-0342	3	1, 2, 3	2, 4, 5	2, 6
30	CVE-1999-0373	3, 8	1, 4	4	5
31	CVE-1999-0381	3	1, 2, 3	2, 4	2
32	CVE-1999-0385	8	1, 2, 3, 4	3	3, 4, 5
33	CVE-1999-0400	3	1, 2	5	4, 6
34	CVE-1999-0401	3	1	4, 5	6
35	CVE-1999-0402	3, 8	1	5	6
36	CVE-1999-0403	3	1, 2	4	4
37	CVE-1999-0409	3	1, 2, 3	2, 4	2
38	CVE-1999-0421	3	2, 3	2, 5	2
39	CVE-1999-0439	3, 8	1, 2, 3, 4	3, 4, 5	3, 5, 6
40	CVE-1999-0451	3	1, 2	4	4
41	CVE-1999-0459	3	1, 2	4	4
42	CVE-1999-0460	3	1, 2	4	4
43	CVE-1999-0462	3	1, 2, 3	2, 4, 5	2, 6
44	CVE-1999-0491	3	1, 4	4	5
45	CVE-1999-0661	3	1	5	6
46	CVE-1999-0678	3, 6, 8	1	5	6
47	CVE-1999-0712	3	1	5	6
48	CVE-1999-0730	3, 8	1	4, 5	6
49	CVE-1999-0732	3, 8	1	4, 5	6
50	CVE-1999-0743	3, 8	1	4, 5	6
51	CVE-1999-0754	3	1	4, 5	6
52	CVE-1999-0793	7	1	5	6

Fig. 22: Generation of Excels sheets with attributes of threat agents.

The above figure shows the sample of the Excel sheet generated by our proposed model and consists of the list of all the CVEs. The algorithm determines the attributes of the threat agent's groups concerning the environments, pre-requites input, attack vectors, and potential output. As the number of CVE lists is very prodigious, the outcome is also generated in prodigious size and can be seen at **https://github.com/Gauravsbin/Exploitation-of-Vulnerability-for-NIST-Database-1999-2021-.** The semi-automatic model collects the DataStream or PCAP files from the University of Hertfordshire ESXi server. The PCAP files are captured by the number of virtual machines installed on the system to follow the activities

performed by the threat agents in a network of the informational environment (Sharma, Vidalis, Menon, Anand and Kumar, 2021). In the first phase, a semi-automatic model extracts valuable information about the threat agents from the PCAP files. Simultaneously, extracting critical intelligence feeds from the identified threat agent groups in a network and designs the profiles for the threat agent groups. The list of IP addresses the threat agents use to attack the target machine is devised. Concerning the IP address of the threat agent, the associated list of CVEs can be indefatigable (interpreted) by mapping activities executed by the threat agent on a network with the NIST database.

The contribution based on the above figure is that, as stated in the thesis, the model is semi-automatic; when the required information is directly available in the Excel sheet, the threat agent practitioners can obtain the necessary information about the threat agent by running the Ctrl+F command on the Excel sheet. Based on this, they will receive all information, such as the type of environment the threat agent uses to penetrate the network, which attack vectors were used, what information was extracted from the target machine, and so on. With this information, cybersecurity practitioners can recommend mitigation techniques for organisations to save their environment from cyberattacks. The only constraint of this excel sheet is that the output accuracy ranges from 80% to 90% based on identifying related CVEs with threat agents.

In the above figure, the SATAM model analyses all the identified threat agents from the PCAP files captured from the network of the ESXi server and maps them with the CVE list of the NIST database. In this table, when a model performs the vulnerability analysis on the identified CVE list of the NIST database, the outcomes are generated with the following characteristics of the threat agent: environment used by the threat agents, attack vectors used by the threat agent, pre-requisites inputs followed by the threat agents, and the potential outcomes or results of the penetration performed by the threat agents. When the SATAM model provides such information for all the NIST databases, it will help index the identified threat agent capability and the opportunity pursued by them during the network penetration. The SATAM model performs the vulnerability analysis of the identified threat agents and will help threat assessment practitioners to determine the critical threat intelligence feeds to the groups of threat agents. When cybersecurity practitioners have CTI information(with them) for past threat assessments achieved for an organization, it will be easy and efficient to

use such information to address the newly identified threat gents in a network. The vulnerability analysis will help design a vulnerability tree analysis for an organization's network used at its workplace.

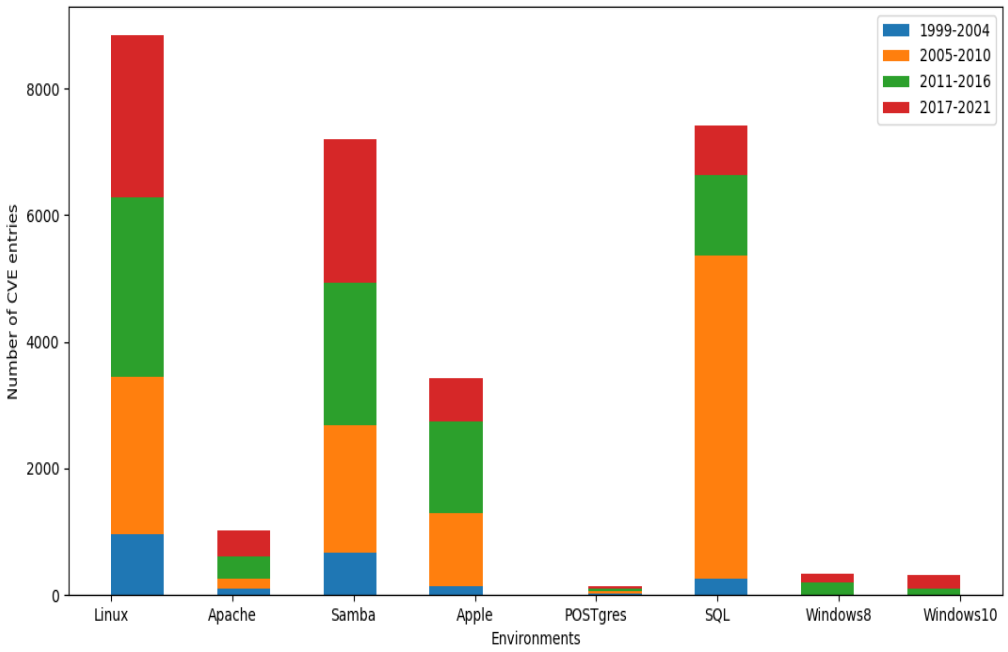


Fig. 23: Environments used by a threat agent to exploit the network.

In the above figure, the semi-automatic threat assessment (platform) model groups the identified threat agent considering the environment cast off by hackers. The CVE list of the NIST database consists of practical information about the threat agents, such as the type of platform used to attack the network, the script run by the threat agents, the level of knowledge or skills acquired by the threat agents, and the capability of attackers. The identification of attributes is accomplished by the model and by mapping them with the associated CVE list of the NIST database. The operating system used by the hackers to attack the network is evaluated by the model and with the help of the interactive library of Python available on the Jupyter Notebook. Furthermore, the model plots a histogram of the number of CVE entities against the operating system used by the attackers to execute attacks against an organization's network.

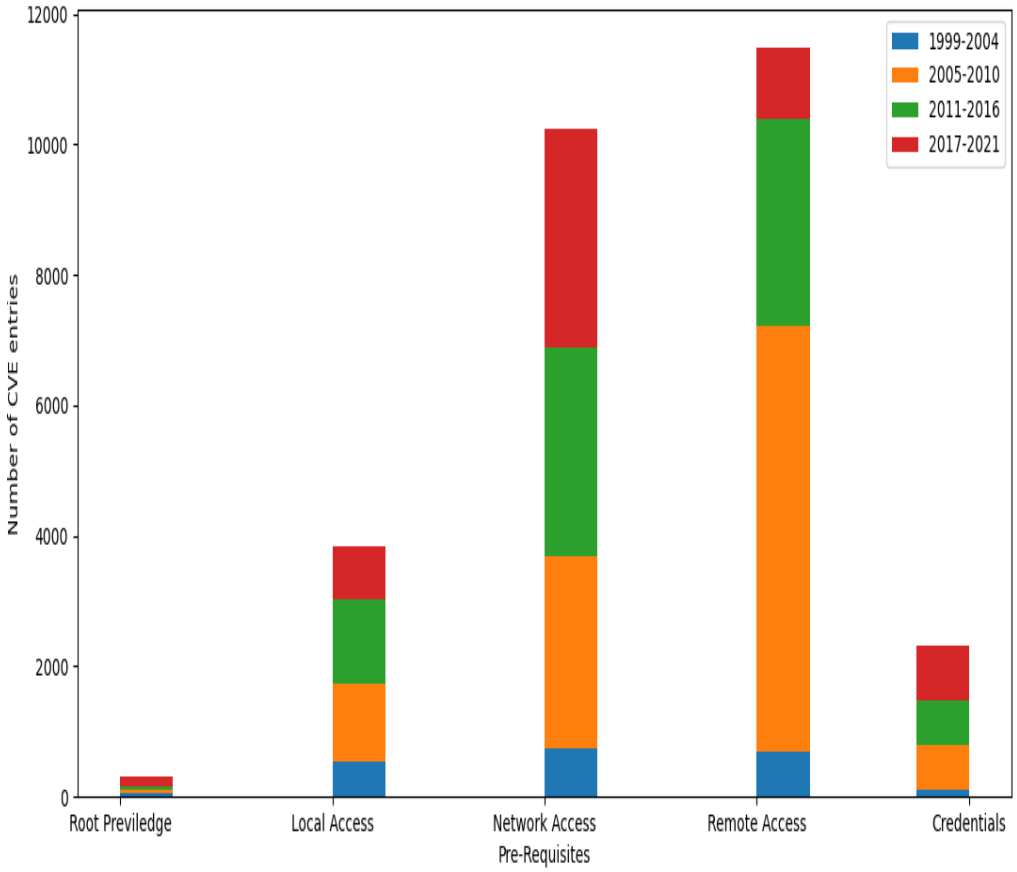


Fig.24: Pre-Requisites inputs of threat agents.

In the above figure, the model plots a histogram of the number of CVE entries against the pre-requisites inputs the threat agent groups cast off. The semi-automatic model evaluates the pre-requisites inputs the threat agents use to execute codes, scripts, or malicious activities against an organization's network. The model mapped the CVE list of source IP addresses from the captured packets of data stream with the CVE list of the NIST database based on the identified inputs of the threat agents. The groups of threat agents associated with the particular type of input used during the execution attacks against the network between 1999-2021 are shown in the histogram.

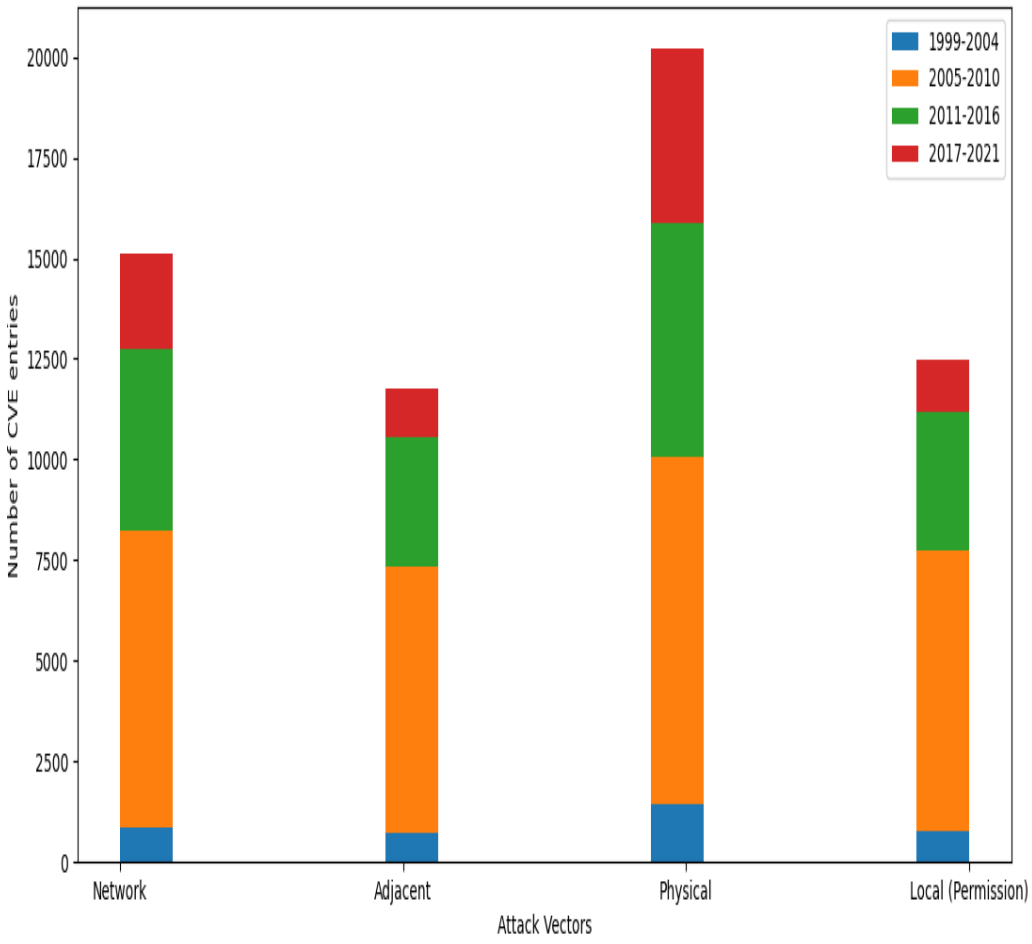


Fig. 25: Attack vectors of threat agents.

In the above figure, the semi-automatic threat agent analysis model plots a histogram of threat agent's attack vectors cast-off to execute the attacks against the University of Hertfordshire server and the number of CVE list entries associated with the NIST database between 1999-2021. The above histogram shows the groups of threat agents operating on each layer and execution of the target machine was achieved.

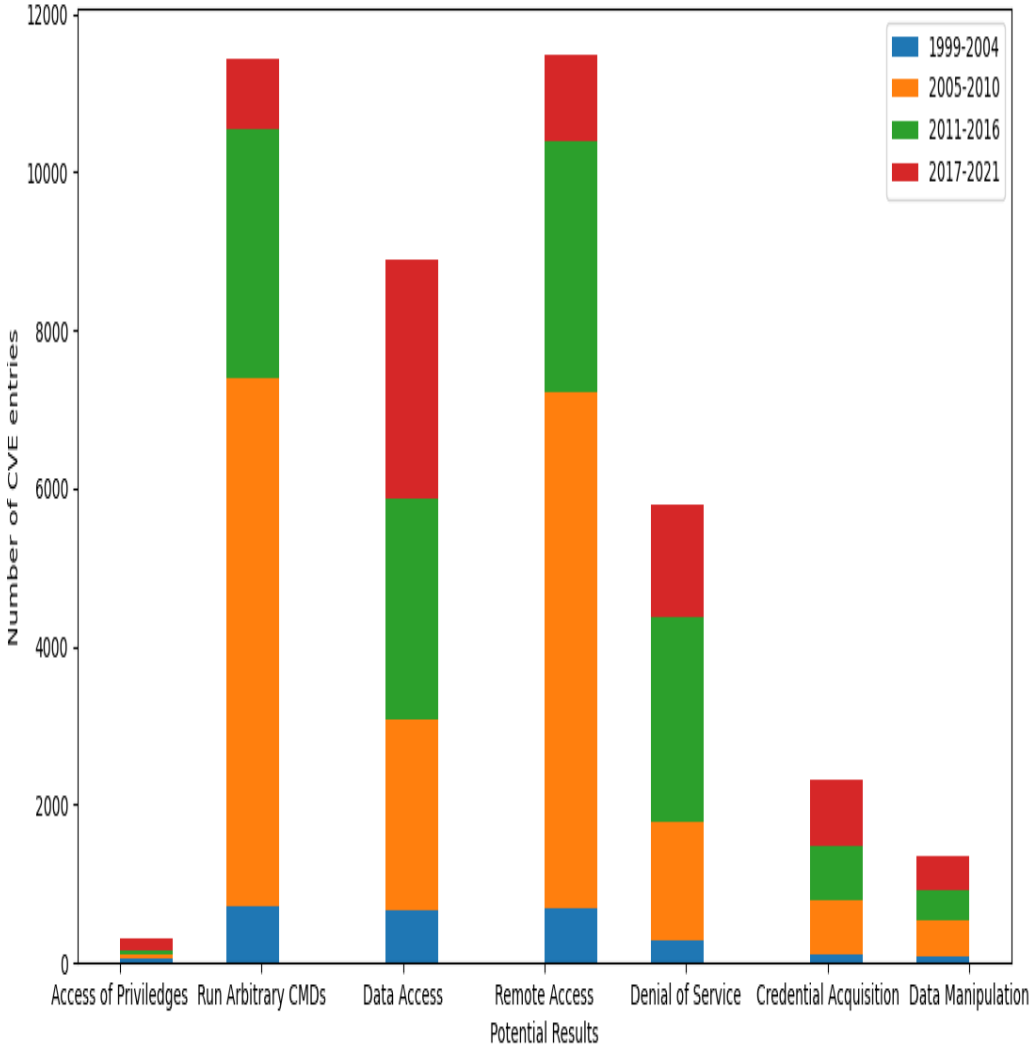


Fig.26: Potential results of the threat agents.

In the above figure, the histogram created by the threat agent analysis model shows the number of CVE entries on the NIST database and the potential outputs of the threat agent groups. The activities performed by the group of CVEs associated with the threat agents groups determined in the PCAP files from the server are shown in the histogram, such as access of privileges, run arbitrary commands, data access, data manipulation, and credential acquisitions. The existing model and methodology follow the evaluation process for the environments or platform, inputs of threat agents, attack vectors, and potential results

manually used by the threat agents due to the manual process of identification of attributes for vulnerability exploitation. The time complexity increased, and simultaneously the performance of the existing model and methodology is declined. While the semi-automatic model already evaluates the attributes of threat agents available in the CVE list of the NIST database. The list of features our model generates is in the form of Excel sheets. Identifying threat agents in a network and the associated list of CVEs is dextrous. The mapping of the identified CVEs to the Excel sheet of results helps evaluate the organization's vulnerable port. Because of the automated process of identifying attributes of threat agents, the process's time complexity is reinforced. The results of the vulnerability exploitation of the NIST database would be used for commercial purposes by other existing models and methodologies. When the exiting model identifies the associated list of CVEs, they can check for the attributes from the Excel sheet by clicking on Ctrl+F and placing the CVE number for the search. The associated results with the particular CVE can be tenacious.

5.7 Conclusion

The main focus of the research is to provide proactive security to networks. Similarly, the identified pivotal vulnerable ports must be prioritized or addressed first meaningfully. Vulnerability exploitation risks materialize in the vulnerability analysis for the threat agent groups available in an organization's network and the company's business. The risk management team should apply the prioritization policy to the vulnerable ports in a meaningful manner and optimize time complexity. Moreover, this work lodges a semi-automatic evaluation model for exploiting a vulnerability in the NIST database as a CVE list. The analysis and implementation of all the CVE lists effectuate the CVSS score and the attributes of the threat agent groups used while exploiting the vulnerable ports of a network. This approach helps potential results be more accurate, precise, practical, or meaningful. While an organization's network in an informational environment is being analysed, the time complexity is optimized using the semi-automatic model approach. In the future, our research would suggest that the model work for both vulnerability analysis and calculation of threat agent attributes simultaneously with optimized time and area complexity.

Chapter – 6 Summary and Conclusion

6.1 Chapter Overview

Chapter 6 is the concluding chapter of this thesis. It begins by presenting the problems and constraints encountered during the lifetime of this research. The future development of the model is shown in the last part of this chapter. The limitations, dissemination plan and exploitation plan for developing the model are described in the later section. Finally, the chapter concludes by discussing the research breakthroughs of the semi-automatic model for threat assessment described in the thesis.

6.2 Conclusion

This research addressed the need for an efficient and precise model to deal effectively with threats in the near-real-time modern computing informational environment. It was hypothesized that security practitioners should focus on the groups of threat agents and hazards present in an organization's network system. The ESXi server network at the University of Hertfordshire was used as a testing ground to validate this claim.

The thesis's primary objective was to develop a semi-automatic model for conducting threat assessments on the University of Hertfordshire's network (ESXi server). The specific objectives of the project were as follows:

- **Research objective:** Analyse the modern information environment and identify key characteristics and attributes that must be included and measured in a comprehensive threat assessment model. This involved conducting a state-of-the-art analysis of existing threat assessment models and methodologies to identify their strengths and limitations. The objective was to gather insights and identify the essential elements that should be incorporated into the developed model.
- **Development objective:** Design and implement a robust threat agent analysis model to effectively address the unique challenges and threats in a modern informational environment network. This objective included developing algorithms, methodologies, and frameworks for identifying, modifying, and treating different threat agents within the network. The model's development aimed to ensure scalability, efficiency, and accuracy in threat assessment processes. Additionally, a key focus was to create a

dissemination strategy to promote the model's adoption and facilitate its integration into organization's existing cybersecurity frameworks.

- **Evaluation objective:** Implement and evaluate the developed model by conducting a series of experiments and assessments using software tools and hardware specifically designed for modern informational environment networks. The objective was to validate the model's effectiveness in accurately identifying and assessing threat agents within the network. Evaluation techniques included quantitative, qualitative, hybrid, and knowledge-based approaches to measure the model's performance, reliability, and applicability. The results and findings of these evaluations would be documented and published in various SCI journals, contributing to the broader scientific community's understanding of threat assessment in near-real-time informational environments.

By expanding on the objectives, the project aimed to provide a comprehensive analysis of the modern information environment, design and implement an advanced threat agent analysis model, and evaluate its performance through rigorous experiments and assessments. This holistic approach would ensure that the developed model effectively addressed threat assessment's unique challenges and requirements in near-real-time informational environments and contributed to the field's scientific knowledge and advancements. Chapter 2 of the thesis focused on meeting the first research objective by examining existing models and methodologies. It explored the tactics used by cybersecurity practitioners to address threat agents on various network platforms. The strengths and weaknesses of current technology and threat agent analysis models were analysed to comprehensively understand their methodologies. The chapter also covered concepts related to organizational risk, vulnerability exploitation, and threat assessment.

Chapter 3 addressed the second development objective by discussing the requirements for software and hardware tools and the steps involved in creating and implementing the model. This chapter followed the research approach and included relevant work in the field. Chapters 4 and 5 involved the evaluation of threat assessments and vulnerability analysis of the data stream, achieved through the implementation of the developed model. The findings and outcomes of these evaluations were documented in the corresponding chapters. While the thesis considers the research's success in breaking scientific barriers in the domain of threat assessment for near-real-time informational environments, acknowledges that complete

security is unattainable. Regardless of the resources allocated to asset protection, the author recognizes that nobody truly understands the state of the art of threat assessment and vulnerability exploitation of the model. The realization that “nothing can be 100% secure” serves as a reminder that threat assessment is not solely about preserving assets and systems but also about empowering cybersecurity practitioners and protecting them from accusations of negligence. This research addressed the need for an efficient and precise model for conducting threat assessments in a near-real-time modern computing informational environment. The research hypothesized that security practitioners should focus on the groups of threat agents and hazards present in an organization’s network system. The study validated this hypothesis by conducting threat assessments on the ESXi server network at the University of Hertfordshire.

The research successfully developed a semi-automatic model capable of analysing and treating threat agents in the network. The specific objectives included researching the characteristics and attributes necessary for a comprehensive threat assessment model, designing and implementing the threat agent analysis model, and evaluating its performance using various techniques. The results of the evaluations were intended to be published in recognized scientific journals. The thesis structure reflected the accomplishment of these objectives, with Chapter 2 reviewing existing models and methodologies and Chapter 3 focusing on the requirements and implementation of the developed model. Chapters 4 and 5 documented the evaluation of threat assessments and vulnerability analysis of the data stream, showcasing the model’s effectiveness. While the research contributed to the field of threat assessment in near-real-time informational environments, it was acknowledged that complete security is unattainable. Despite resource allocation for asset protection, nobody truly understands state of the art in threat assessment and vulnerability exploitation of the model. The study emphasizes that threat assessment is not solely about preserving assets and systems but also about empowering cybersecurity practitioners and protecting them from accusations of negligence.

Overall, this research provides insights into the development and evaluation of a semi-automatic model for threat assessment in the network, contributing to the advancement of threat assessment methodologies in dynamic and chaotic organizational networks.

6.3 Limitation of the Semi-Automatic model

The following are the limitations connected with the semi-automatic model:

- **Limited automation and manual intervention:** The semi-automatic model, as indicated by its name, relies on a combination of automated processes and manual tasks to handle threat assessments. While automation is present in certain aspects, the model still requires human intervention for certain critical tasks. This reliance on manual intervention limits the overall level of automation and introduces potential delays or inefficiencies in the threat assessment process.
- **Challenges within addressing new threats:** The model's vulnerability accuracy is reported to be between 70% and 80%, indicating a relatively high level of accuracy in identifying known vulnerabilities. However, in the event of a new or emerging threat, the model may face limitations in effectively addressing the organization's security concerns. As new threats require novel mitigation strategies, the model may need to rely on manual techniques and expert knowledge to handle these unique security challenges.
- **Probabilistic approach limitations:** The model utilizes a probabilistic technique for the motivation factor, which assigns probabilities ranging from 0.1 to 0.9. While this approach provides a certain level of flexibility and adaptability, it introduces inherent uncertainty into the model's predictions. The accuracy of the model's motivation factor is dependent on the quality of the underlying probabilistic model, which may result in varying levels of accuracy and potentially impact the reliability of the overall threat assessments.
- **Subjectivity in attribute evaluation:** The model's attribute evaluation process is performed manually, indicating that human judgement and expertise are involved in assessing certain attributes relevant to the threat assessment. This manual approach introduces subjectivity and potential biases into the evaluation process, which can affect the overall accuracy and objectivity of the results. The consistency and reliability of the attribute evaluation depend heavily on the expertise and experience of the individuals performing the manual assessments.
- **Lack of real-time updates:** The semi-automatic model may face limitations in providing real-time updates on emerging threats or vulnerabilities. Because manual tasks are involved in the threat assessment process, the model's ability to promptly incorporate and respond to the ever-changing threat landscape may be hindered. This delay in updating the model with the latest threat intelligence and mitigation strategies

could potentially leave the organization exposed to new risks before appropriate countermeasures can be implemented.

- **Scalability challenges:** The model's scalability may pose a limitation because of the involvement of manual tasks. As the volume and complexity of threat data increase, the effectiveness and efficiency of the model in handling larger datasets and numerous assessments may become constrained. The reliance on manual intervention for certain tasks may limit the model's ability to scale and handle the growing demands of threat assessment in larger organizations or complex network environments.

Despite its benefits, the semi-automatic model does come with certain limitations. First, while the model incorporates automation, it still requires manual intervention for critical tasks, limiting the overall level of automation and potentially introducing delays in the threat assessment process. Additionally, the model's vulnerability accuracy, ranging between 70% and 80%, implies that it may face challenges in effectively addressing new or emerging threats that require unique mitigation strategies beyond its existing knowledge base. Moreover, the probabilistic approach used for the motivation factor introduces uncertainty, and the accuracy of this factor can vary from 0.1 to 0.9. The manual attribute evaluation process introduces subjectivity and potential biases into the assessment, affecting the overall accuracy and objectivity of the results. Finally, the model's scalability may be constrained because of the involvement of manual tasks, limiting its ability to handle larger datasets and numerous assessments, particularly in dynamic and rapidly evolving threat environments.

6.4 Dissemination plan

The thesis will describe in the dissemination plan what objectives were decided or recognized to apply the semi-automatic model alongside the real-time information environment and will include the list of completed goals and plans for the exploitation part, to be followed by the following team. A semi-automatic model for the near-real-time informational environment was successfully developed and implemented. As defined in the development objectives in chapter 1, the fundamental aspects of the semi-automatic threat agent analysis model have been successfully achieved. The semi-automatic threat assessment and vulnerability exploitation models' functions are illustrated in chapters 4 and 5 respectively.

Dissemination is a continuous process of project-wide marketing and awareness-building. An organized document (such as a dissemination strategy) that guides the entire consortium

should be used to design and coordinate this process at the project's outset. Publication of programme or policy papers is a common form of dissemination. Findings from the experiment will be published in SCI journals and conference publications. Dissemination transmits results and best practices among peers, industrial stakeholders, and policymakers. The primary goals are to maximize distribution of project results to a diverse range of researchers and engineers within key cybersecurity organizations and projects. These dissemination actions are viewed as vital before and during the result's exploitation. It should also be mentioned that cybersecurity practitioners, including cyber domain specialists, are an essential focus for this dissemination endeavour.

The semi-automatic model dissemination plan begins with information collecting regarding the existing model and methodology. The initial phase of the model saw the study's completion and the model's discovery. The data collected from the server was identified in the following phase. A comparison of suitable tools was performed based on the information required to address the recognized threat agent in an environment. The extraction of CTI and the construction of profiles for threat agent groups are done automatically using Python library source codes. Based on the threat assessment findings, a list of CVEs connected with the target IP address is collected to determine the environment, input attack vectors, and the potential outputs of the identified threat agents. A dissemination plan is critical to any project, because it outlines how the project outcomes will be shared with stakeholders and the wider community. The dissemination plan for the SATAM is as follows:

1. **Stakeholder engagement:** The first step is identifying and engaging with the project's key stakeholders, such as law enforcement agencies, security personnel, government organizations, and other relevant authorities. Stakeholders should be kept informed of project developments and invited to provide feedback on the SATAM model throughout the project.
2. **Journal/conference presentations:** Journals and conferences are an excellent opportunity to showcase the SATAM model to a broader audience. Presentations should highlight the benefits of the SATAM model and how it can help stakeholders identify and mitigate potential threats.
3. **Publications:** Academic publications are another avenue for disseminating the SATAM model's outcomes. The thesis aims to publish their findings in peer-reviewed

journals to establish the validity of the SATAM model and its effectiveness in identifying and assessing potential threats.

4. **Demonstrations and pilot projects:** Demonstrations and pilot projects can be used to showcase the SATAM model's effectiveness in identifying and assessing potential threats.

The SATAM dissemination plan should include stakeholder engagement, conference presentations, publications, webinars and workshops, a project website and social media, and demonstrations and pilot projects. These activities should be integrated into a comprehensive dissemination strategy to ensure that the SATAM model's outcomes reach the broadest possible audience and that stakeholders are kept informed throughout the process.

6.5 Exploitation Plan

The exploitation strategy primarily addresses the model's progress regarding the future perfectiveness and the semi-automatic model's continuous process. The project's next stage is to create a single API (application programming interface) to connect the cybersecurity profiles with the NIST database, which will be available online. Because of this feature, the model will be upgraded from semi-automatic to entirely automatic. It will also improvise the efficiency of the model's complexity regarding time and area.

The plan documents the activities to be carried out in order to improve the successful exploitation of project results in terms of industrial development/creation of products or processes and market placement. An exploit is a piece of code that exploits a software vulnerability or security weakness. It is written as a proof-of-concept threat by security researchers or hostile actors for use in their operations. The plan must include the following critical elements: clear objectives and strategies, stakeholders, key messages, communication channels and tools, all planned communication, distribution, and exploitation activities, and a list of expected results.

Exploiting the SATAM model would require a well-defined plan that outlines the steps needed to operationalize the model in real-world scenarios. Here is an exploitation plan for the SATAM model:

1. **Define objectives:** The first step is to define the objectives of the SATAM model. These objectives may include identifying potential threats, prioritizing potential threats based on their severity and likelihood, and providing decision-makers with the necessary insights to take proactive measures to mitigate potential threats.
2. **Identify data sources:** The next step is identifying the data sources required to feed the SATAM model. These sources may include internal data such as incident reports, security logs, and surveillance footage, as well as external data sources such as news feeds, social media, and government threat assessments. The data must be collected, organized, and integrated into a centralized database to allow for efficient analysis.
3. **Develop SATAM model:** The SATAM model should be developed and customized to suit the specific objectives and data sources identified. The model may include machine learning algorithms, natural language processing tools, and statistical models. The model should be tested and validated against real-world scenarios to ensure its accuracy and effectiveness.
4. **Deploy SATAM model:** The SATAM model should be deployed in a real-world scenario, and the data collected should be fed into the model. The model should analyse the data and generate insights that can assist decision-makers in identifying and assessing potential threats.
5. **Use insights to make decisions:** Decision-makers should use the insights generated by the SATAM model to make informed decisions and take proactive measures to mitigate potential threats. The model should be regularly updated and refined based on the feedback received from decision-makers and other stakeholders.
6. **Monitor and evaluate results:** The results of the SATAM model should be monitored and evaluated to assess its effectiveness in identifying and assessing potential threats. The model should be regularly refined and updated based on feedback to improve its accuracy and effectiveness.
7. **Ensure data security and privacy:** Finally, it is essential to ensure the security and privacy of the data being used. This may include implementing access controls, data encryption, and other security measures to protect against unauthorized access or data breaches. Maintaining compliance with relevant laws and regulations regarding data privacy and security is essential.

Exploiting the SATAM model requires a well-defined plan outlining the steps needed to operationalize the model in real-world scenarios. The plan should include defining objectives, identifying data sources, developing the SATAM model, deploying the model, using insights to make decisions, monitoring and evaluating results, and ensuring data security and privacy.

The next step is to employ VLSI technology to assess the area complexity of existing models and methodologies and compare them to our proposed model to demonstrate its efficiency with facts. An appropriate database will be used to address the historical data collected from the server. As a result, the efficiency in managing the cybersecurity profile of the detected threat agents from the target IP addresses will be attained.

6.6 Future Scope

The proposed model must comprehend how the firm uses e-commerce and be capable of tackling the multidimensional matrix of information security. The future model will consider the spiral development approach, the operational approach (functional level strategy leads to operational process, which means analysing the threat from situational awareness data and comparing it with historical data, which helps to improve the effectiveness or efficiency to identify the hazards in a network) and operating in a distributed manner while performing threat analysis. A database including threat agent profiles and vital intelligence feeds is required to help evaluate newly found threats in a network. It can also automatically assess network threats' motivation, opportunity, and capabilities. As a result, complexity will be more efficient. The SATAM has immense potential for future development and application in a wide range of industries and sectors. Here are some possible future scope areas for the SATAM model:

- **Increased automation:** Currently, the SATAM model requires human input for some aspects of threat assessment. In the future, the model could be enhanced with increased automation to reduce the need for human input, thereby increasing efficiency and accuracy.
- **Integration with advanced technologies**: Advanced technologies such as AI, big data analytics, and the Internet of Things can be integrated with SATAM to improve the model’s accuracy and effectiveness.

- **Industry-specific customization:** SATAM can be customized for different industries, such as transportation, healthcare, finance, and retail. Industry-specific customizations can help optimize the model's features to meet each industry's specific needs and requirements.
- **Real-time threat assessment:** With the integration of real-time data feeds, SATAM can provide a real-time threat assessment, allowing organizations to identify and mitigate potential threats in real-time, thereby minimizing damage and improving response times.
- **Cybersecurity:** SATAM can be used to improve cybersecurity by monitoring and detecting potential threats to computer networks, data breaches, and other cybersecurity threats.
- **Predictive analytics:** SATAM can be enhanced with predictive analytics, enabling it to identify and forecast potential threats and allowing organizations to take proactive measures to prevent and mitigate potential threats.

In summary, the SATAM model has immense potential for future development and application in a wide range of industries and sectors. As technology advances, the SATAM model can be enhanced with increased automation, integration with advanced technologies, industry-specific customizations, real-time threat assessment, cybersecurity, and predictive analytics, making it a valuable tool for organizations to identify and mitigate potential threats.

References:

Abouzakhar, N. (2015) 'ECCWS2015-Proceedings of the 14th European Conference on Cyber Warfare and Security 2015: ECCWS 2015', in. Academic Conferences Limited.

Abu, M. S. et al. (2018) 'Cyber threat intelligence–issue and challenges', Indonesian Journal of Electrical Engineering and Computer Science, 10(1), pp. 371–379.

Addison, S. (2002) 'Introduction to security risk analysis and the cobra approach', C & A security system report (Online serial). Available: www. security-risk-analysis. com.

Alberts, C. J., Dorofee, A. J. and Allen, J. H. (2001) OCTAVE Catalog of Practices, Version 2.0. Carnegie-Mellon Univ Pittsburgh Pa Software Engineering Inst.

Alfadel, M., Costa, D. E. and Shihab, E. (2021) 'Empirical Analysis of Security Vulnerabilities in Python Packages', in 2021 IEEE International Conference on Software Analysis, Evolution and Reengineering (SANER). IEEE, pp. 446–457.

Allodi, L. (2017) 'Economic factors of vulnerability trade and exploitation', in Proceedings of the 2017 ACM SIGSAC conference on computer and communications security, pp. 1483–1499.

Allodi, L. et al. (2017) 'Estimating the assessment difficulty of CVSS environmental metrics: an experiment', in International Conference on Future Data and Security Engineering. Springer, pp. 23–39.

Allodi, L. et al. (2018) 'The effect of security education and expertise on security assessments: The case of software vulnerabilities', arXiv preprint arXiv:1808.06547.

Alomar, N. et al. (2020) '" You've Got Your Nice List of Bugs, Now What?" Vulnerability Discovery and Management Processes in the Wild', in Sixteenth Symposium on Usable Privacy and Security ({SOUPS} 2020), pp. 319–339.

Ambusaidi, M. A. et al. (2016) 'Building an intrusion detection system using a filter-based feature selection algorithm', IEEE transactions on computers, 65(10), pp. 2986–2998.

Ani, U. D., He, H. and Tiwari, A. (2019) 'Human factor security: evaluating the cybersecurity capacity of the industrial workforce', Journal of Systems and Information Technology.

Araki, H. et al. (1996) 'Development of rear-end collision avoidance system', in Proceedings of Conference on Intelligent Vehicles. IEEE, pp. 224–229.

Archer, E. M. (2014) 'Crossing the rubicon: Understanding cyber terrorism in the european

context', The European Legacy, 19(5), pp. 606–621.

Asgari, H., Haines, S. and Rysavy, O. (2017) 'Identification of threats and security risk assessments for recursive Internet architecture', IEEE Systems Journal, 12(3), pp. 2437–2448.

Atote, B. S. et al. (2016) 'Inferring emotional state of a user by user profiling', in 2016 2nd International Conference on Contemporary Computing and Informatics (IC3I). IEEE, pp. 530–535.

Aufner, P. (2020) 'The IoT security gap: a look down into the valley between threat models and their implementation', International Journal of Information Security, 19(1), pp. 3–14.

Azaria, A. et al. (2014) 'Behavioral analysis of insider threat: A survey and bootstrapped prediction in imbalanced data', IEEE Transactions on Computational Social Systems, 1(2), pp. 135–155.

Baezner, M. and Robin, P. (2017) Stuxnet. ETH Zurich.

Bagstad, K. J. et al. (2011) 'ARIES–ARtificial Intelligence for Ecosystem Services: a guide to models and data, version 1.0', ARIES report series, 1.

Baker, Z. K. and Prasanna, V. K. (2004) 'Time and area efficient pattern matching on FPGAs', in Proceedings of the 2004 ACM/SIGDA 12th international symposium on Field programmable gate arrays, pp. 223–232.

Berhe, S. et al. (2021) 'Leveraging UML for Access Control Engineering in a Collaboration on Duty and Adaptive Workflow Model that Extends NIST RBAC', in Research Anthology on Recent Trends, Tools, and Implications of Computer Programming. IGI Global, pp. 916–939.

Bishop, M. et al. (2014) 'Insider threat identification by process analysis', in 2014 IEEE Security and Privacy Workshops. IEEE, pp. 251–264.

Bloom, B. H. (1970) 'Space/time trade-offs in hash coding with allowable errors', Communications of the ACM, 13(7), pp. 422–426.

Blyth, A. J. C. and Kovacich, L. (2001) 'Information Assurance: Computer Communications & Networks. UK'. Springer-Verley.

Boban, M. (2010) 'Building eGovernment model on the principles of new economy trends and international standards considering protection of citizen privacy and personal data', E-Society Journal Research and Applications, 1(2), pp. 1–15.

Bose, J. S. C. et al. (2017) 'Development and designing of fire fighter robotics using cyber

security', in 2017 2nd International Conference on Anti-Cyber Crimes (ICACC). IEEE, pp. 118–122.

Bruzzese, R. (2019) 'An Analisys of Application Logs with Splunk: developing an App for the synthetic analysis of data and security incidents', arXiv preprint arXiv:1912.11283.

Cao, J. et al. (2013) 'A survey on security aspects for LTE and LTE-A networks', IEEE communications surveys & tutorials, 16(1), pp. 283–302.

Cappelli, D. M., Moore, A. P. and Trzeciak, R. F. (2012) The CERT guide to insider threats: how to prevent, detect, and respond to information technology crimes (Theft, Sabotage, Fraud). Addison-Wesley.

Chen, M. et al. (2017) 'Machine learning for wireless networks with artificial intelligence: A tutorial on neural networks', arXiv preprint arXiv:1710.02913, 9.

Chen, R.-C., Cheng, K.-F. and Hsieh, C.-F. (2010) 'Using rough set and support vector machine for network intrusion detection', arXiv preprint arXiv:1004.0567.

Cho, K., Mitsuya, K. and Kato, A. (2001) 'Traffic data repository at the wide project', in Proceedings of USENIX 2000 Annual Technical Conference: FREENIX Track, San Diego, CA (June 2000) Xu, J., Fan, J., Ammar, MH, Moon, SB: On the design and performance of prefix-preserving IP traffic trace anonymization. In: SIGCOMM IMW.

Cisar, P. et al. (2016) 'Scoring system as a method of improving IT vulnerability status', Annals of the Faculty of Engineering Hunedoara, 14(3), p. 207.

Clancy, T. C. (2011) 'Efficient OFDM denial: Pilot jamming and pilot nulling', in 2011 IEEE International Conference on Communications (ICC). IEEE, pp. 1–5.

Cup, K. D. D. (2007) 'Data. Knowledge Discovery in Databases DARPA Archive'.

Damnjanovic, A. et al. (2011) 'A survey on 3gpp heterogeneous networks. Wireless Comm'. IEEE.

Deore, U. D. and Waghmare, V. (2016) 'Cyber security automation for controlling distributed data', in 2016 International Conference on Information Communication and Embedded Systems (ICICES). IEEE, pp. 1–4.

Dharmapurikar, S. and Lockwood, J. W. (2006) 'Fast and scalable pattern matching for network intrusion detection systems', IEEE Journal on Selected Areas in communications, 24(10), pp. 1781–1792.

Elbaz, C., Rilling, L. and Morin, C. (2018) 'Reactive and Adaptive Security Monitoring in Cloud Computing', in 2018 IEEE 3rd International Workshops on Foundations and

Applications of Self* Systems (FAS* W). IEEE, pp. 5–7.
Engebretson, P. (2013) 'The Basics of Hacking and Penetration Testing'. Waltham: Elsevier Hadnagy.
Erola, A. et al. (2017) 'RicherPicture: Semi-automated cyber defence using context-aware data analytics', in 2017 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA). IEEE, pp. 1–8.
Feutrill, A. et al. (2018) 'The effect of common vulnerability scoring system metrics on vulnerability exploit delay', in 2018 Sixth International Symposium on Computing and Networking (CANDAR). IEEE, pp. 1–10.
Franklin, J., Wergin, C. and Booth, H. (2014) 'CVSS implementation guidance', National Institute of Standards and Technology, NISTIR-7946.
Fresner, J. et al. (2017) 'Energy efficiency in small and medium enterprises: Lessons learned from 280 energy audits across Europe', Journal of Cleaner Production, 142, pp. 1650–1660.
Gamble, E. et al. (2020) 'Problems with crisis intervention: When the government wants to restrain big banks but punishes small businesses instead', Journal of Business Venturing Insights, 14, p. e00185.
Geerts, E. (2020) 'Book Review: Vulnerable Futures, Transformative Pasts: On Vulnerability, Temporality, and Ethics by Miri Rozmarin, Peter Lang, 2017, 194 pages. ISBN 978-1-78707-392-0 (ePub)(also available in print, ePDF and mobi)'. Helsinki University Press.
Gelso, E. R. and Sjoberg, J. (2017) 'Consistent threat assessment in rear-end near-crashes using BTN and TTB metrics, road information and naturalistic traffic data', IEEE Intelligent Transportation Systems Magazine, 9(1), pp. 74–89.
Ghanem, K. et al. (2012) 'Reducing ping-pong Handover effects in intra EUTRA networks', in 2012 8th International Symposium on Communication Systems, Networks & Digital Signal Processing (CSNDSP). IEEE, pp. 1–5.
Goel, S., Pon, D. and Menzies, J. (2006) 'Managing information security: Demystifying the audit process for security officers', Journal of Information System Security, 2(2), pp. 25–45.
Gollmann, D. (2010) 'Computer security', Wiley Interdisciplinary Reviews: Computational Statistics, 2(5), pp. 544–554.
Grother, P. J. (1995) 'NIST special database 19', Handprinted forms and characters database, National Institute of Standards and Technology, p. 10.

Haber, M. J. and Hibbert, B. (2018) Asset Attack Vectors: Building Effective Vulnerability Management Strategies to Protect Organizations. Apress.

Haines, J. W. et al. (2001) 1999 DARPA intrusion detection evaluation: Design and procedures. MASSACHUSETTS INST OF TECH LEXINGTON LINCOLN LAB.

Icove, D., Seger, K. and VonStorch, W. (1996) 'Computer Crime: A Crimefighter's Handbook', Computer Fraud & Security, 6(1996), pp. 15–18.

Iglesias, J. A. et al. (2009) 'Modelling evolving user behaviours', in 2009 IEEE Workshop on Evolving and Self-Developing Intelligent Systems. IEEE, pp. 16–23.

Ingoldsby, T. R. (2010) 'Attack tree-based threat risk analysis', Amenaza Technologies Limited, pp. 3–9.

Jing, Y. et al. (2014) 'Riskmon: Continuous and automated risk assessment of mobile applications', in Proceedings of the 4th ACM Conference on Data and Application Security and Privacy, pp. 99–110.

Joh, H. and Malaiya, Y. K. (2014) 'Modeling skewness in vulnerability discovery', Quality and Reliability Engineering International, 30(8), pp. 1445–1459.

Jones, A (2002) 'Identification of a Method for the Calculation of the Capability of Threat Agents in an Information Environment', School of Computing. Pontypridd, University of Glamorgan: 0-134.

Jones, Andy (2002) 'Protecting the Critical National Infrastructure-Developing a Method for the Measurement of Threat Agents in an Information Environment', Information Security Technical Report, 2(7), pp. 22–36.

Kabay, M. E. (1996) 'Enterprise Security: Protecting Information Assets'. McGraw-Hill.

Kaufman, L. M. (2009) 'Data security in the world of cloud computing', IEEE Security & Privacy, 7(4), pp. 61–64.

Khandekar, A. et al. (2010) 'LTE-advanced: Heterogeneous networks', in 2010 European wireless conference (EW). IEEE, pp. 978–982.

Kothari, C. R. (2004) Research methodology: Methods and techniques. New Age International.

Lee, J.-H. et al. (2015) 'A study of the radio resource control connection re-establishment procedure on the UE side in 3GPP', in 2015 17th International Conference on Advanced Communication Technology (ICACT). IEEE, pp. 260–262.

Legg, P. A. et al. (2013) 'Towards a conceptual model and reasoning structure for insider

threat detection', Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 4(4), pp. 20–37.

Legg, P. A. et al. (2015) 'Automated insider threat detection system using user and role-based profile assessment', IEEE Systems Journal, 11(2), pp. 503–512.

Leitch, M. M. (2012) Intelligent internal control and risk management: designing high-performance risk control systems. Gower Publishing, Ltd.

Lessler, J. et al. (2016) 'Assessing the global threat from Zika virus', Science, 353(6300).

Leyland, P. and Brooks, P. (1996) 'Report of the UKERNA Secure Email Project'.

Li, Q. and Trappe, W. (2007) 'Detecting spoofing and anomalous traffic in wireless networks via forge-resistant relationships', IEEE Transactions on Information Forensics and Security, 2(4), pp. 793–808.

Lichtman, M. et al. (2013) 'Vulnerability of LTE to hostile interference', in 2013 IEEE Global Conference on Signal and Information Processing. Ieee, pp. 285–288.

Lichtman, M. et al. (2016) 'LTE/LTE-A jamming, spoofing, and sniffing: threat assessment and mitigation', IEEE Communications Magazine, 54(4), pp. 54–61.

Lim, C.-U., Baumgarten, R. and Colton, S. (2010) 'Evolving behaviour trees for the commercial game DEFCON', in Applications of Evolutionary Computation: EvoApplicatons 2010: EvoCOMPLEX, EvoGAMES, EvoIASP, EvoINTELLIGENCE, EvoNUM, and EvoSTOC, Istanbul, Turkey, April 7-9, 2010, Proceedings, Part I. Springer Berlin Heidelberg, pp. 100–110.

Longhurst, G. J. et al. (2020) 'Strength, weakness, opportunity, threat (SWOT) analysis of the adaptations to anatomical education in the United Kingdom and Republic of Ireland in response to the Covid-19 pandemic', Anatomical sciences education, 13(3), pp. 301–311.

Maheshwari, V. and Prasanna, M. (2016) 'Integrating risk assessment and threat modeling within SDLC process', in 2016 International Conference on Inventive Computation Technologies (ICICT). IEEE, pp. 1–5.

Mahmud, S. M. H. et al. (2018) 'CSV-ANNOTATE: Generate annotated tables from CSV file', in 2018 International Conference on Artificial Intelligence and Big Data (ICAIBD). IEEE, pp. 71–75.

Maier, M. W. (1998) 'Architecting principles for systems-of-systems', Systems Engineering: The Journal of the International Council on Systems Engineering, 1(4), pp. 267–284.

Marcellino, W. et al. (2017) Monitoring social media: Lessons for future department of

defense social media analysis in support of information operations. RAND NATIONAL DEFENSE RESEARCH INST SANTA MONICA CA.

Matthews, P. H. and Matthews, P. H. (2014) The concise Oxford dictionary of linguistics. Oxford University Press.

Mavroeidis, V. and Bromander, S. (2017) 'Cyber threat intelligence model: an evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence', in 2017 European Intelligence and Security Informatics Conference (EISIC). IEEE, pp. 91–98.

Morakis, E., Vidalis, S. and Blyth, A. (2003) 'A framework for representing and analysing cyber attacks using object oriented hierarchy trees', in Proceedings of the 2nd European Conference On Information Warfare And Security (ECIW).

Morikawa, I. and Yamaoka, Y. (2011) 'Threat tree templates to ease difficulties in threat modeling', in 2011 14th International Conference on Network-Based Information Systems. IEEE, pp. 673–678.

Mosca, M. (2018) 'Cybersecurity in an era with quantum computers: Will we be ready?', IEEE Security & Privacy, 16(5), pp. 38–41.

Munaiah, N. and Meneely, A. (2016) 'Vulnerability severity scoring and bounties: Why the disconnect?', in Proceedings of the 2nd International Workshop on Software Analytics, pp. 8–14.

Narkar, S., Thomson, B. L. and Fox, P. A. (2020) 'Designing for 2030: The Impact and Potential of Virtual Laboratories', in AGU Fall Meeting Abstracts, pp. IN003-03.

Nisioti, A. et al. (2018) 'From intrusion detection to attacker attribution: A comprehensive survey of unsupervised methods', IEEE Communications Surveys & Tutorials, 20(4), pp. 3369–3388.

Oreku, G. S. and Mtenzi, F. J. (2017) 'Cybercrime: Concerns, Challenges and Opportunities', in Information Fusion for Cyber-Security Analytics. Springer, pp. 129–153.

Pan, S., Morris, T. and Adhikari, U. (2015) 'Developing a hybrid intrusion detection system using data mining for power systems', IEEE Transactions on Smart Grid, 6(6), pp. 3104–3113.

Pandelică, I. (2020) 'The Phenomenon of Cyber Crime', International Journal of Information Security and Cybercrime (IJISC), 9(1), pp. 29–36.

Patel, C. S., Stuber, G. L. and Pratt, T. G. (2004) 'Analysis of OFDM/MC-CDMA under channel estimation and jamming', in 2004 IEEE Wireless Communications and Networking

Conference (IEEE Cat. No. 04TH8733). IEEE, pp. 954–958.

Paxson, V. (2005) ‘LBNL Enterprise Trace Repository’.

Pendleton, M. et al. (2016) ‘A survey on systems security metrics’, ACM Computing Surveys (CSUR), 49(4), pp. 1–35.

Pfleeger, C. P. (2009) Security in computing. Pearson Education India.

Pilgermann, M., Blyth, A. and Vidalis, S. (2006) ‘Inter-organisational intrusion detection using knowledge grid technology’, Information management & computer security.

Polychronopoulos, A. et al. (2007) ‘Sensor fusion for predicting vehicles’ path for collision avoidance systems’, IEEE Transactions on Intelligent Transportation Systems, 8(3), pp. 549–562.

Pontarelli, S., Bianchi, G. and Teofili, S. (2012) ‘Traffic-aware design of a high-speed FPGA network intrusion detection system’, IEEE Transactions on Computers, 62(11), pp. 2322–2334.

Puketza, N. J. et al. (1996) ‘A methodology for testing intrusion detection systems’, IEEE Transactions on Software Engineering, 22(10), pp. 719–729.

Ralchenko, Y., Kramida, A. E. and Reader, J. (2008) ‘NIST atomic spectra database’, National Institute of Standards and Technology, Gaithersburg, MD.

Rao, R. M. et al. (2017) ‘LTE PHY layer vulnerability analysis and testing using open-source SDR tools’, in MILCOM 2017-2017 IEEE Military Communications Conference (MILCOM). IEEE, pp. 744–749.

Rossebo, J. E. Y., Fransen, F. and Luiijf, E. (2016) ‘Including threat actor capability and motivation in risk assessment for Smart GRIDs’, in 2016 Joint Workshop on Cyber-Physical Security and Resilience in Smart Grids (CPSR-SG). IEEE, pp. 1–7.

van Royen, M. E. et al. (2008) ‘Fluorescence recovery after photobleaching (FRAP) to study nuclear protein dynamics in living cells’, in The nucleus. Springer, pp. 363–385.

Rubini, R. et al. (1993) ‘Power spectrum analysis of cardiovascular variability monitored by telemetry in conscious unrestrained rats’, Journal of the autonomic nervous system, 45(3), pp. 181–190.

Rughani, P. H. (2017) ‘ARTIFICIAL INTELLIGENCE BASED DIGITAL FORENSICS FRAMEWORK.’, International Journal of Advanced Research in Computer Science, 8(8).

Ruiter, M. C. de et al. (2017) ‘A comparison of flood and earthquake vulnerability assessment indicators’, Natural Hazards and Earth System Sciences, 17(7), pp. 1231–1251.

Ruohonen, J. et al. (2018) ‘A case study on software vulnerability coordination’, Information and Software Technology, 103, pp. 239–257.
Rynes, A. and Bjornard, T. (2011) Intent, capability and opportunity: A holistic approach to addressing proliferation as a risk management issue. Idaho National Laboratory (INL).
Saad, S. et al. (2011) ‘Detecting P2P botnets through network behavior analysis and machine learning’, in 2011 Ninth annual international conference on privacy, security and trust. IEEE, pp. 174–180.
Salim, M. M., Rathore, S. and Park, J. H. (2020) ‘Distributed denial of service attacks and its defenses in IoT: a survey’, The Journal of Supercomputing, 76(7), pp. 5320–5363.
Samuel, J., Aalab, K. and Jaskolka, J. (2020) ‘Evaluating the soundness of security metrics from vulnerability scoring frameworks’, in 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). IEEE, pp. 442–449.
Saunders, J. H. (2002) ‘Simulation approaches in information security education’, in Proc. 6th National Colloquium for Information System Security Education, Redmond, WA.
Saygili, G. et al. (2018) ‘Cloud-based tools for the probabilistic assessment of the seismic performance of slopes’, in Geotechnical Earthquake Engineering and Soil Dynamics V: Slope Stability and Landslides, Laboratory Testing, and In Situ Testing. American Society of Civil Engineers Reston, VA, pp. 19–26.
Scholand, T. et al. (2007) ‘MIMO Successive Interference Cancellation for UTRA LTE’, in 12th International OFDM-Workshop 2007, pp. 29–30.
Schwarz, K. and Creutzburg, R. (2021) ‘Design of Professional Laboratory Exercises for Effective State-of-the-Art OSINT Investigation Tools-Part 1: RiskIQ Passive-Total’, Electronic imaging, 2021(3), pp. 41–43.
Sesia, S., Toufik, I. and Baker, M. (2011) LTE-the UMTS long term evolution: from theory to practice. John Wiley & Sons.
Sgandurra, D. and Lupu, E. (2016) ‘Evolution of attacks, threat models, and solutions for virtualized systems’, ACM Computing Surveys (CSUR), 48(3), pp. 1–38.
Sharma, G., Vidalis, S., Anand, N., et al. (2021) ‘A Survey on Layer-Wise Security Attacks in IoT: Attacks, Countermeasures, and Open-Issues’, Electronics, 10(19), p. 2365.
Sharma, G., Vidalis, S., Menon, C., Anand, N. and Kumar, S. (2021) ‘Analysis and Implementation of Threat Agents Profiles in Semi-Automated Manner for a Network Traffic

in Real-Time Information Environment', Electronics, 10(15), p. 1849.
Sharma, G., Vidalis, S., Menon, C., Anand, N. and Pourmoafi, S. (2021) 'Study and Analysis of Threat Assessment Model and Methodology in Real-Time Informational Environment', in 2021 IEEE Bombay Section Signature Conference (IBSSC). IEEE, pp. 1–6.
Sharma, G. et al. (2022) 'Analysis and implementation of semi-automatic model for vulnerability exploitations of threat agents in NIST databases', Multimedia Tools and Applications, pp. 1–21.
Shin, B. and Lowry, P. B. (2020) 'A review and theoretical explanation of the 'Cyberthreat-Intelligence (CTI) capability'that needs to be fostered in information security practitioners and how this can be accomplished', Computers & Security, 92, p. 101761.
Shin, M., Dorbala, S. and Jang, D. (2013) 'Threat Modeling for Security Failure-Tolerant Requirements', in 2013 International Conference on Social Computing. IEEE, pp. 594–599.
Smith, R. M., Martell, A. E. and Motekaitis, R. J. (2004) 'NIST standard reference database 46', NIST Critically Selected Stability Constants of Metal Complexes Database Ver, 2.
Sogbesan, A. et al. (2012) 'Collusion threat profile analysis: Review and analysis of MERIT model', in World Congress on Internet Security (WorldCIS-2012). IEEE, pp. 212–217.
Strom, B. E. et al. (2018) 'Mitre att&ck: Design and philosophy', Technical report.
Summers, R. C. (1997) Secure computing: threats and safeguards. McGraw-Hill, Inc.
Susukailo, V., Opirskyy, I. and Vasylyshyn, S. (2020) 'Analysis of the attack vectors used by threat actors during the pandemic', in 2020 IEEE 15th International Conference on Computer Sciences and Information Technologies (CSIT). IEEE, pp. 261–264.
Teixeira, A. et al. (2015) 'Secure control systems: A quantitative risk management approach', IEEE Control Systems Magazine, 35(1), pp. 24–45.
Tevis, J.-E. J. and Hamilton Jr, J. A. (2006) 'Static analysis of anomalies and security vulnerabilities in executable files', in Proceedings of the 44th annual Southeast regional conference, pp. 560–565.
Ullah, F. et al. (2018) 'Data exfiltration: A review of external attack vectors and countermeasures', Journal of Network and Computer Applications, 101, pp. 18–54.
Van Veen, H. J. et al. (2019) 'Kepler Mapper: A flexible Python implementation of the Mapper algorithm.', Journal of Open Source Software, 4(42), p. 1315.
Vidalis, S. and Jones, A. (2003) 'Using vulnerability trees for decision making in threat assessment', University of Glamorgan, School of Computing, Tech. Rep. CS-03-2.

Vidalis, S. and Jones, A. (2005) ‘Analyzing Threat Agents and Their Attributes.’, in ECIW, pp. 369–380.

Vidalis, S. and Jones, A. (2006) ‘Threat Agents: what InfoSec officers need to know’, Mediterranean Journal of Computers and Security.

Vidalis, S., Jones, A. and Blyth, A. (2004) ‘Assessing cyber-threats in the information environment’, Network Security, 2004(11), pp. 10–16.

Walsworth, C. et al. (2015) ‘The caida ucsd anonymized internet traces 2012,”’.

Wold, S., Esbensen, K. and Geladi, P. (1987) ‘Principal component analysis’, Chemometrics and intelligent laboratory systems, 2(1–3), pp. 37–52.

Xu, H. et al. (2011) ‘The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing’, Decision support systems, 51(1), pp. 42–52.

Xue, M. et al. (2020) ‘Machine learning security: Threats, countermeasures, and evaluations’, IEEE Access, 8, pp. 74720–74742.

Yu, H. and Zhang, X. (2017) ‘Research on the Application of IoT in E-Commerce’, in 2017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC). IEEE, pp. 434–436.

Appendix-I.

Threat Assessment Model analysis for publicly available datasets.

1. Introduction

In this thesis, I analyse the threat assessment model applied to three different datasets files obtained from various sources. The PCAP files are captured network data that allow us to study network traffic, detect anomalies, and assess potential threats. The three sources of the dataset's files are:

1. USA Organization (File 1) (**Can be seen in GitHub Link shown in chapter 4)**
2. Sweden Army Network (File 2) (**Can be seen in GitHub Link shown in chapter 4)**
3. PETRAS Project of Railway Threat Assessment (File 3)

I will utilise the threat assessment model (SATAM) to process each dataset and generate outputs, which will be presented in Excel sheets for further analysis.

2. Data Sources

The datasets for analysis can be accessed from the following link: www.netresec.com (Provide the link where the files are available).

3. Data Download

Two dataset files were downloaded for this analysis, one from the USA Organization and the other from the Sweden Army Network organisation.

a) File 1 (snort.log.1425568941 Sweden army files): Datasets from the USA Organization.
b) File 2 (USA .pcap files captured with snort): Datasets from the Sweden Army Network.
c) File 3 cannot be available publicly because it's the property of East Midland Railway and the PETRAS community. When I worked for them, I utilised SATAM to analyse datasets captured from the railway network. So, one test dataset output generated from the captured dataset is shown below to prove that the model can work on any datasets captured from any organisation and perform the threat assessment accordingly.

4. Threat Assessment Model

The threat assessment model used in this analysis is designed to identify potential security threats, detect anomalies, and assess the overall network security. It employs various algorithms and heuristics to process the datasets and extract relevant information for analysis.

5. Analysis Process

The several datasets, along with File 3 (PETRAS Project of Railway), were processed through the threat assessment model. The model analyses the network patterns, identifies suspicious activities, and generates output metrics for each PCAP file from the dataset pool.

6. Output Generated

The threat assessment model generated outputs for each of the three sources of datasets. These outputs are organised and presented in separate Excel sheets:

1. Excel Sheet 1 (US .pcap files captured with snort): Contains the analysis results of the PCAP file from the USA Organization.
2. Excel Sheet 2 (snort.log.1425568941 Sweden army files): Contains the analysis results of the PCAP file from the Sweden Army Network.
3. Excel Sheet 3 (test.pcap files of PETRAS Railway Project): Contains the analysis results of the PCAP file from the PETRAS Project of Railway.

Each Excel sheet includes various metrics, such as:

- Number of packets analysed.
- Identified threats and their severity levels.
- Traffic anomalies detected.
- Suspicious IP addresses or domains.
- Protocol usage distribution.
- Summary of network statistics.

7. Conclusion

The threat assessment model analysis of the three dataset files from different sources provides valuable insights into their network security. By studying the outputs in the Excel sheets, potential threats and anomalies can be identified, and necessary measures can be taken to improve the security posture of the respective organisations. Overall, this analysis demonstrates the effectiveness of the threat assessment model in assessing networks based on datasets captured from the organisation.

Appendix-II.

```
<?xml version="1.0"?>
<?mso-application progid="Excel.Sheet"?>
<Workbook xmlns="urn:schemas-microsoft-com:office:spreadsheet"
 xmlns:o="urn:schemas-microsoft-com:office:office"
 xmlns:x="urn:schemas-microsoft-com:office:excel"
 xmlns:ss="urn:schemas-microsoft-com:office:spreadsheet"
 xmlns:html="http://www.w3.org/TR/REC-html40">
 <DocumentProperties xmlns="urn:schemas-microsoft-com:office:office">
  <LastAuthor>Gaurav Sharma</LastAuthor>
  <Created>2021-11-17T13:49:08Z</Created>
  <LastSaved>2021-11-17T13:49:08Z</LastSaved>
  <Version>16.00</Version>
 </DocumentProperties>
 <OfficeDocumentSettings xmlns="urn:schemas-microsoft-com:office:office">
  <AllowPNG/>
 </OfficeDocumentSettings>
 <ExcelWorkbook xmlns="urn:schemas-microsoft-com:office:excel">
  <WindowHeight>9660</WindowHeight>
  <WindowWidth>16100</WindowWidth>
  <WindowTopX>240</WindowTopX>
  <WindowTopY>20</WindowTopY>
  <ProtectStructure>False</ProtectStructure>
  <ProtectWindows>False</ProtectWindows>
 </ExcelWorkbook>
 <Styles>
  <Style ss:ID="Default" ss:Name="Normal">
   <Alignment ss:Vertical="Bottom"/>
   <Borders/>
```

```
 <Font ss:FontName="Calibri" x:Family="Swiss" ss:Size="11" ss:Color="#000000"/>
 <Interior/>
 <NumberFormat/>
 <Protection/>
</Style>
<Style ss:ID="s16">
 <Alignment ss:Horizontal="Center" ss:Vertical="Center" ss:WrapText="1"/>
 <Font ss:FontName="Calibri" x:Family="Swiss" ss:Size="12" ss:Color="#000000"
  ss:Bold="1"/>
</Style>
<Style ss:ID="s17">
 <Alignment ss:Horizontal="Center" ss:Vertical="Center" ss:WrapText="1"/>
 <Font ss:FontName="Calibri" x:Family="Swiss" ss:Color="#000000"/>
</Style>
</Styles>
<Worksheet ss:Name="Data Sheet">
 <Table ss:ExpandedColumnCount="13" ss:ExpandedRowCount="30" x:FullColumns="1"
  x:FullRows="1" ss:DefaultRowHeight="14.5">
 <Column ss:AutoFitWidth="0" ss:Width="42.5"/>
 <Column ss:AutoFitWidth="0" ss:Width="75.5"/>
 <Column ss:AutoFitWidth="0" ss:Width="86.5" ss:Span="1"/>
 <Column ss:Index="5" ss:AutoFitWidth="0" ss:Width="103"/>
 <Column ss:AutoFitWidth="0" ss:Width="70"/>
 <Column ss:AutoFitWidth="0" ss:Width="103"/>
 <Column ss:AutoFitWidth="0" ss:Width="70"/>
 <Column ss:AutoFitWidth="0" ss:Width="86.5"/>
 <Column ss:AutoFitWidth="0" ss:Width="141.5"/>
 <Column ss:AutoFitWidth="0" ss:Width="103" ss:Span="1"/>
 <Column ss:Index="13" ss:AutoFitWidth="0" ss:Width="196.5"/>
```

<Row ss:AutoFitHeight="0" ss:Height="42">
<Cell ss:StyleID="s16"><Data ss:Type="String">Sl. No.</Data></Cell>
<Cell ss:StyleID="s16"><Data ss:Type="String">Time (in min)</Data></Cell>
<Cell ss:StyleID="s16"><Data ss:Type="String">Highest Protocol</Data></Cell>
<Cell ss:StyleID="s16"><Data ss:Type="String">protocol</Data></Cell>
<Cell ss:StyleID="s16"><Data ss:Type="String">Source IP Address</Data></Cell>
<Cell ss:StyleID="s16"><Data ss:Type="String">Source port</Data></Cell>
<Cell ss:StyleID="s16"><Data ss:Type="String">Dest. IP Address</Data></Cell>
<Cell ss:StyleID="s16"><Data ss:Type="String">Destination port</Data></Cell>
<Cell ss:StyleID="s16"><Data ss:Type="String">Total Packet Length</Data></Cell>
<Cell ss:StyleID="s16"><Data ss:Type="String">City, Region, Country</Data></Cell>
<Cell ss:StyleID="s16"><Data ss:Type="String">Latitute</Data></Cell>
<Cell ss:StyleID="s16"><Data ss:Type="String">Longitude</Data></Cell>
<Cell ss:StyleID="s16"><Data ss:Type="String">Internet Service Provider</Data></Cell>
</Row>
<Row ss:AutoFitHeight="0" ss:Height="30">
<Cell ss:StyleID="s17"><Data ss:Type="Number">1</Data></Cell>
<Cell ss:StyleID="s17"><Data ss:Type="Number">156.85316666051651</Data></Cell>
<Cell ss:StyleID="s17"><Data ss:Type="String">TCP</Data></Cell>
<Cell ss:StyleID="s17"><Data ss:Type="String">TCP</Data></Cell>
<Cell ss:StyleID="s17"><Data ss:Type="String">130.236.100.79</Data></Cell>
<Cell ss:StyleID="s17"><Data ss:Type="Number">80</Data></Cell>
<Cell ss:StyleID="s17"><Data ss:Type="String">192.168.0.2</Data></Cell>
<Cell ss:StyleID="s17"><Data ss:Type="Number">34485</Data></Cell>
<Cell ss:StyleID="s17"><Data ss:Type="Number">143300932</Data></Cell>
<Cell ss:StyleID="s17"><Data ss:Type="String">Linköping, Östergötland, Sweden</Data></Cell>
<Cell ss:StyleID="s17"><Data ss:Type="String">NA</Data></Cell>
<Cell ss:StyleID="s17"><Data ss:Type="String">NA</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="String">Linkopings universitet</Data></Cell>
</Row>
<Row ss:AutoFitHeight="0" ss:Height="30">
<Cell ss:StyleID="s17"><Data ss:Type="Number">2</Data></Cell>
<Cell ss:StyleID="s17"><Data ss:Type="Number">124.71937267825</Data></Cell>
<Cell ss:StyleID="s17"><Data ss:Type="String">TCP</Data></Cell>
<Cell ss:StyleID="s17"><Data ss:Type="String">TCP</Data></Cell>
<Cell ss:StyleID="s17"><Data ss:Type="String">192.168.0.2</Data></Cell>
<Cell ss:StyleID="s17"><Data ss:Type="Number">34485</Data></Cell>
<Cell ss:StyleID="s17"><Data ss:Type="String">130.236.100.79</Data></Cell>
<Cell ss:StyleID="s17"><Data ss:Type="Number">80</Data></Cell>
<Cell ss:StyleID="s17"><Data ss:Type="Number">3824752</Data></Cell>
<Cell ss:StyleID="s17"><Data ss:Type="String">None, None</Data></Cell>
<Cell ss:StyleID="s17"><Data ss:Type="String">NA</Data></Cell>
<Cell ss:StyleID="s17"><Data ss:Type="String">NA</Data></Cell>
<Cell ss:StyleID="s17"><Data ss:Type="String">NA</Data></Cell>
</Row>
<Row ss:AutoFitHeight="0" ss:Height="30">
<Cell ss:StyleID="s17"><Data ss:Type="Number">3</Data></Cell>
<Cell ss:StyleID="s17"><Data ss:Type="Number">93.27368949451666</Data></Cell>
<Cell ss:StyleID="s17"><Data ss:Type="String">TCP</Data></Cell>
<Cell ss:StyleID="s17"><Data ss:Type="String">TCP</Data></Cell>
<Cell ss:StyleID="s17"><Data ss:Type="String">80.239.174.89</Data></Cell>
<Cell ss:StyleID="s17"><Data ss:Type="Number">443</Data></Cell>
<Cell ss:StyleID="s17"><Data ss:Type="String">192.168.0.51</Data></Cell>
<Cell ss:StyleID="s17"><Data ss:Type="Number">47993</Data></Cell>
<Cell ss:StyleID="s17"><Data ss:Type="Number">3734923</Data></Cell>
<Cell ss:StyleID="s17"><Data ss:Type="String">Uppsala, Uppsala County, Sweden</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="Number">59.8551</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="Number">17.6343</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="String">Telia Company AB</Data></Cell>

</Row>

<Row ss:AutoFitHeight="0" ss:Height="30">

<Cell ss:StyleID="s17"><Data ss:Type="Number">4</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="Number">6.3001568960499936</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="String">TCP</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="String">TCP</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="String">213.155.151.150</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="Number">80</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="String">192.168.0.2</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="Number">38926</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="Number">2289445</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="String">Warsaw, Mazovia, Poland</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="Number">52.255800000000001</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="Number">20.935400000000001</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="String">Telia Company AB</Data></Cell>

</Row>

<Row ss:AutoFitHeight="0" ss:Height="30">

<Cell ss:StyleID="s17"><Data ss:Type="Number">5</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="Number">56.286186074500073</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="String">TCP</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="String">TCP</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="String">213.155.151.155</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="Number">80</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="String">192.168.0.2</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="Number">34561</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="Number">2266759</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="String">Warsaw, Mazovia, Poland</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="Number">52.255800000000001</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="Number">20.935400000000001</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="String">Telia Company AB</Data></Cell>

</Row>

<Row ss:AutoFitHeight="0" ss:Height="30">

<Cell ss:StyleID="s17"><Data ss:Type="Number">6</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="Number">1.2280404683333331E-2</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="String">TCP</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="String">TCP</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="String">85.12.30.227</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="Number">80</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="String">192.168.0.2</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="Number">60921</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="Number">1155472</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="String">Newark, New Jersey, United States</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="Number">40.733699999999999</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="Number">-74.193899999999999</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="String">Base IP B.V.</Data></Cell>

</Row>

<Row ss:AutoFitHeight="0" ss:Height="30">

<Cell ss:StyleID="s17"><Data ss:Type="Number">7</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="Number">60.28063377993324</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="String">TLSv1.2</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="String">TCP</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="String">192.168.0.51</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="Number">56864</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="String">80.239.174.117</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="Number">443</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="Number">241555</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="String">None, None</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="String">NA</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="String">NA</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="String">NA</Data></Cell>

</Row>

<Row ss:AutoFitHeight="0" ss:Height="30">

<Cell ss:StyleID="s17"><Data ss:Type="Number">8</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="Number">1.320390166666667E-2</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="String">TCP</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="String">TCP</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="String">213.155.151.184</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="Number">80</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="String">192.168.0.2</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="Number">49752</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="Number">135125</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="String">Warsaw, Mazovia, Poland</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="Number">52.255800000000001</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="Number">20.935400000000001</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="String">Telia Company AB</Data></Cell>

</Row>

<Row ss:AutoFitHeight="0" ss:Height="30">

<Cell ss:StyleID="s17"><Data ss:Type="Number">27</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="Number">1.130197178333333E-2</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="String">TCP</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="String">TCP</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="String">80.239.174.117</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="Number">443</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="String">192.168.0.51</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="Number">56864</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="Number">521</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="String">None, None</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="String">NA</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="String">NA</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="String">NA</Data></Cell>

</Row>

<Row ss:AutoFitHeight="0" ss:Height="30">

<Cell ss:StyleID="s17"><Data ss:Type="Number">28</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="Number">1.1698545483333329E-2</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="String">TCP</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="String">TCP</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="String">80.239.174.91</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="Number">443</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="String">192.168.0.51</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="Number">34266</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="Number">521</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="String">None, None</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="String">NA</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="String">NA</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="String">NA</Data></Cell>

</Row>

<Row ss:AutoFitHeight="0" ss:Height="30">

<Cell ss:StyleID="s17"><Data ss:Type="Number">29</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="Number">3.8524137499999999E-3</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="String">TCP</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="String">TCP</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="String">74.125.205.95</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="Number">80</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="String">192.168.0.2</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="Number">35938</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="Number">132</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="String">None, None</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="String">NA</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="String">NA</Data></Cell>

<Cell ss:StyleID="s17"><Data ss:Type="String">NA</Data></Cell>

</Row>

</Table>

<WorksheetOptions xmlns="urn:schemas-microsoft-com:office:excel">

<PageSetup>

<Header x:Margin="0.3"/>

<Footer x:Margin="0.3"/>

<PageMargins x:Bottom="0.75" x:Left="0.7" x:Right="0.7" x:Top="0.75"/>

</PageSetup>

<Selected/>

<ProtectObjects>False</ProtectObjects>

<ProtectScenarios>False</ProtectScenarios>

</WorksheetOptions>

</Worksheet>

</Workbook>

Appendix-III.

```
<?xml version="1.0"?>
<?mso-application progid="Excel.Sheet"?>
<Workbook xmlns="urn:schemas-microsoft-com:office:spreadsheet"
 xmlns:o="urn:schemas-microsoft-com:office:office"
 xmlns:x="urn:schemas-microsoft-com:office:excel"
 xmlns:ss="urn:schemas-microsoft-com:office:spreadsheet"
 xmlns:html="http://www.w3.org/TR/REC-html40">
 <DocumentProperties xmlns="urn:schemas-microsoft-com:office:office">
  <LastAuthor>Gaurav Sharma</LastAuthor>
  <Created>2021-10-12T14:14:05Z</Created>
  <LastSaved>2021-10-12T14:14:05Z</LastSaved>
  <Version>16.00</Version>
 </DocumentProperties>
 <OfficeDocumentSettings xmlns="urn:schemas-microsoft-com:office:office">
  <AllowPNG/>
 </OfficeDocumentSettings>
 <ExcelWorkbook xmlns="urn:schemas-microsoft-com:office:excel">
  <WindowHeight>9660</WindowHeight>
  <WindowWidth>16100</WindowWidth>
  <WindowTopX>240</WindowTopX>
  <WindowTopY>20</WindowTopY>
  <ProtectStructure>False</ProtectStructure>
  <ProtectWindows>False</ProtectWindows>
 </ExcelWorkbook>
 <Styles>
  <Style ss:ID="Default" ss:Name="Normal">
   <Alignment ss:Vertical="Bottom"/>
   <Borders/>
```

```
 <Font ss:FontName="Calibri" x:Family="Swiss" ss:Size="11" ss:Color="#000000"/>
 <Interior/>
 <NumberFormat/>
 <Protection/>
</Style>
<Style ss:ID="s16">
 <Font ss:FontName="Calibri" x:Family="Swiss" ss:Size="16" ss:Color="#000000"/>
</Style>
<Style ss:ID="s17">
 <Font ss:FontName="Calibri" x:Family="Swiss" ss:Size="11" ss:Color="#000000"/>
</Style>
<Style ss:ID="s18">
 <Alignment ss:Horizontal="Center" ss:Vertical="Bottom"/>
 <Borders>
  <Border ss:Position="Bottom" ss:LineStyle="Continuous" ss:Weight="1"
   ss:Color="#4893D9"/>
  <Border ss:Position="Left" ss:LineStyle="Continuous" ss:Weight="1"
   ss:Color="#4893D9"/>
  <Border ss:Position="Right" ss:LineStyle="Continuous" ss:Weight="1"
   ss:Color="#4893D9"/>
  <Border ss:Position="Top" ss:LineStyle="Continuous" ss:Weight="1"
   ss:Color="#4893D9"/>
 </Borders>
 <Font ss:FontName="Calibri" x:Family="Swiss" ss:Size="12" ss:Color="#FFFFFF"
  ss:Bold="1"/>
 <Interior ss:Color="#4893D9" ss:Pattern="Solid"/>
</Style>
<Style ss:ID="s19">
 <Alignment ss:Horizontal="Center" ss:Vertical="Bottom"/>
```

```
 <Borders>
  <Border ss:Position="Bottom" ss:LineStyle="Continuous" ss:Weight="1"
   ss:Color="#8BC2F4"/>
  <Border ss:Position="Left" ss:LineStyle="Continuous" ss:Weight="1"
   ss:Color="#8BC2F4"/>
  <Border ss:Position="Right" ss:LineStyle="Continuous" ss:Weight="1"
   ss:Color="#8BC2F4"/>
  <Border ss:Position="Top" ss:LineStyle="Continuous" ss:Weight="1"
   ss:Color="#8BC2F4"/>
 </Borders>
 <Font ss:FontName="Calibri" x:Family="Swiss" ss:Size="11" ss:Color="#000000"/>
 <NumberFormat ss:Format="@"/>
</Style>
<Style ss:ID="s20">
 <Alignment ss:Horizontal="Center" ss:Vertical="Bottom"/>
 <Borders>
  <Border ss:Position="Bottom" ss:LineStyle="Continuous" ss:Weight="1"
   ss:Color="#8BC2F4"/>
  <Border ss:Position="Left" ss:LineStyle="Continuous" ss:Weight="1"
   ss:Color="#8BC2F4"/>
  <Border ss:Position="Right" ss:LineStyle="Continuous" ss:Weight="1"
   ss:Color="#8BC2F4"/>
  <Border ss:Position="Top" ss:LineStyle="Continuous" ss:Weight="1"
   ss:Color="#8BC2F4"/>
 </Borders>
 <Font ss:FontName="Calibri" x:Family="Swiss" ss:Size="11" ss:Color="#000000"/>
 <Interior ss:Color="#E4F2FF" ss:Pattern="Solid"/>
 <NumberFormat ss:Format="@"/>
</Style>
```

```
 </Styles>
 <Worksheet ss:Name="Sheet1">
  <Table ss:ExpandedColumnCount="5" ss:ExpandedRowCount="20696"
x:FullColumns="1"
   x:FullRows="1" ss:DefaultRowHeight="14.5">
   <Column ss:AutoFitWidth="0" ss:Width="136"/>
   <Column ss:AutoFitWidth="0" ss:Width="147" ss:Span="3"/>
   <Row ss:Height="21">
    <Cell ss:StyleID="s16"/>
    <Cell ss:StyleID="s16"><Data ss:Type="String">Environments</Data></Cell>
    <Cell ss:StyleID="s16"><Data ss:Type="String">Attack Vectors</Data></Cell>
    <Cell ss:StyleID="s16"><Data ss:Type="String">Pre-Requisites</Data></Cell>
    <Cell ss:StyleID="s16"><Data ss:Type="String">Potential Results</Data></Cell>
   </Row>
   <Row>
    <Cell ss:Index="2" ss:StyleID="s17"><Data ss:Type="String">1. Windows
10</Data></Cell>
    <Cell ss:StyleID="s17"><Data ss:Type="String">1. Physical</Data></Cell>
    <Cell ss:StyleID="s17"><Data ss:Type="String">1. Credentials</Data></Cell>
    <Cell ss:StyleID="s17"><Data ss:Type="String">1. Credential
Acquisition</Data></Cell>
   </Row>
   <Row>
    <Cell ss:Index="2" ss:StyleID="s17"><Data ss:Type="String">2. Window
8</Data></Cell>
    <Cell ss:StyleID="s17"><Data ss:Type="String">2. Network</Data></Cell>
    <Cell ss:StyleID="s17"><Data ss:Type="String">2. Root Previledge</Data></Cell>
    <Cell ss:StyleID="s17"><Data ss:Type="String">2. Priviledge Escalation</Data></Cell>
   </Row>
<Row>
```

<Cell ss:StyleID="s19"><Data ss:Type="String">CVE-2021-3278</Data></Cell>
<Cell ss:StyleID="s19"><Data ss:Type="String"> 4</Data></Cell>
<Cell ss:StyleID="s19"><Data ss:Type="String"> 1</Data></Cell>
<Cell ss:StyleID="s19"><Data ss:Type="String"> 1, 4, 5</Data></Cell>
<Cell ss:StyleID="s19"><Data ss:Type="String"> 1</Data></Cell>
</Row>
<Row>
<Cell ss:StyleID="s20"><Data ss:Type="String">CVE-2021-3347</Data></Cell>
<Cell ss:StyleID="s20"><Data ss:Type="String"> 3, 8</Data></Cell>
<Cell ss:StyleID="s20"><Data ss:Type="String"> 1, 4</Data></Cell>
<Cell ss:StyleID="s20"><Data ss:Type="String"> 4</Data></Cell>
<Cell ss:StyleID="s20"><Data ss:Type="String"> 5</Data></Cell>
</Row>
<Row>
<Cell ss:StyleID="s19"><Data ss:Type="String">CVE-2021-3411</Data></Cell>
<Cell ss:StyleID="s19"><Data ss:Type="String"> 3</Data></Cell>
<Cell ss:StyleID="s19"><Data ss:Type="String"> 1</Data></Cell>
<Cell ss:StyleID="s19"><Data ss:Type="String"> 5</Data></Cell>
<Cell ss:StyleID="s19"><Data ss:Type="String"> 6</Data></Cell>
</Row>
<Row>
<Cell ss:StyleID="s20"><Data ss:Type="String">CVE-2021-3416</Data></Cell>
<Cell ss:StyleID="s20"><Data ss:Type="String"> 3, 8</Data></Cell>
<Cell ss:StyleID="s20"><Data ss:Type="String"> 2</Data></Cell>
<Cell ss:StyleID="s20"><Data ss:Type="String"> 5</Data></Cell>
<Cell ss:StyleID="s20"><Data ss:Type="String"> 4</Data></Cell>
</Row>
<Row>
<Cell ss:StyleID="s19"><Data ss:Type="String">CVE-2021-3444</Data></Cell>

```
  <Cell ss:StyleID="s19"><Data ss:Type="String"> 3</Data></Cell>
  <Cell ss:StyleID="s19"><Data ss:Type="String"> 1</Data></Cell>
  <Cell ss:StyleID="s19"><Data ss:Type="String"> 4, 5</Data></Cell>
  <Cell ss:StyleID="s19"><Data ss:Type="String"> 6</Data></Cell>
 </Row>
 <Row>
  <Cell ss:StyleID="s20"><Data ss:Type="String">CVE-2021-3449</Data></Cell>
  <Cell ss:StyleID="s20"><Data ss:Type="String"> 3, 8</Data></Cell>
  <Cell ss:StyleID="s20"><Data ss:Type="String"> 2</Data></Cell>
  <Cell ss:StyleID="s20"><Data ss:Type="String"> 5</Data></Cell>
  <Cell ss:StyleID="s20"><Data ss:Type="String"> 4</Data></Cell>
 </Row>
</Table>
<WorksheetOptions xmlns="urn:schemas-microsoft-com:office:excel">
 <PageSetup>
  <Header x:Margin="0.3"/>
  <Footer x:Margin="0.3"/>
  <PageMargins x:Bottom="0.75" x:Left="0.7" x:Right="0.7" x:Top="0.75"/>
 </PageSetup>
 <Selected/>
 <ProtectObjects>False</ProtectObjects>
 <ProtectScenarios>False</ProtectScenarios>
</WorksheetOptions>
</Worksheet>
</Workbook>
```

Appendix-IV.

```
<html xmlns:v="urn:schemas-microsoft-com:vml"
xmlns:o="urn:schemas-microsoft-com:office:office"
xmlns:x="urn:schemas-microsoft-com:office:excel"
xmlns="http://www.w3.org/TR/REC-html40">
<head>
<meta name="Excel Workbook Frameset">
<meta http-equiv=Content-Type content="text/html; charset=windows-1252">
<meta name=ProgId content=Excel.Sheet>
<meta name=Generator content="Microsoft Excel 15">
<link rel=File-List href="Output%20not%20all%20box_files/filelist.xml">
<![if !supportTabStrip]>
<link id="shLink" href="Output%20not%20all%20box_files/sheet001.htm">
<link id="shLink">
<script language="JavaScript">
<!--
 var c_lTabs=1;
 var c_rgszSh=new Array(c_lTabs);
 c_rgszSh[0] = "Sheet1";
 var c_rgszClr=new Array(8);
 c_rgszClr[0]="window";
 c_rgszClr[1]="buttonface";
 c_rgszClr[2]="windowframe";
 c_rgszClr[3]="windowtext";
 c_rgszClr[4]="threedlightshadow";
 c_rgszClr[5]="threedhighlight";
 c_rgszClr[6]="threeddarkshadow";
 c_rgszClr[7]="threedshadow";
 var g_iShCur;
 var g_rglTabX=new Array(c_lTabs);
function fnGetIEVer()
{
```

```
 var ua=window.navigator.userAgent
 var msie=ua.indexOf("MSIE")
 if (msie>0 && window.navigator.platform=="Win32")
  return parseInt(ua.substring(msie+5,ua.indexOf(".", msie)));
 else
  return 0;
}
function fnBuildFrameset()
{
 var szHTML="<frameset rows=\"*,18\" border=0 width=0 frameborder=no
framespacing=0>"+
  "<frame src=\""+document.all.item("shLink")[0].href+"\" name=\"frSheet\" noresize>"+
  "<frameset cols=\"54,*\" border=0 width=0 frameborder=no framespacing=0>"+
  "<frame src=\"\" name=\"frScroll\" marginwidth=0 marginheight=0 scrolling=no>"+
  "<frame src=\"\" name=\"frTabs\" marginwidth=0 marginheight=0 scrolling=no>"+
  "</frameset></frameset><plaintext>";
 with (document) {
  open("text/html","replace");
  write(szHTML);
  close();
 }
 fnBuildTabStrip();
}
function fnBuildTabStrip()
{
 var szHTML=
  "<html><head><style>.clScroll {font:8pt Courier
New;color:"+c_rgszClr[6]+";cursor:default;line-height:10pt;}"+
  ".clScroll2 {font:10pt Arial;color:"+c_rgszClr[6]+";cursor:default;line-
height:11pt;}</style></head>"+
```

```
  "<body onclick=\"event.returnValue=false;\" ondragstart=\"event.returnValue=false;\"
onselectstart=\"event.returnValue=false;\" bgcolor="+c_rgszClr[4]+" topmargin=0
leftmargin=0><table cellpadding=0 cellspacing=0 width=100%>"+
  "<tr><td colspan=6 height=1 bgcolor="+c_rgszClr[2]+"></td></tr>"+
  "<tr><td style=\"font:1pt\"> <td>"+
  "<td valign=top id=tdScroll class=\"clScroll\" onclick=\"parent.fnFastScrollTabs(0);\"
onmouseover=\"parent.fnMouseOverScroll(0);\"
onmouseout=\"parent.fnMouseOutScroll(0);\"><a>&#171;</a></td>"+
  "<td valign=top id=tdScroll class=\"clScroll2\" onclick=\"parent.fnScrollTabs(0);\"
ondblclick=\"parent.fnScrollTabs(0);\" onmouseover=\"parent.fnMouseOverScroll(1);\"
onmouseout=\"parent.fnMouseOutScroll(1);\"><a>&lt</a></td>"+
  "<td valign=top id=tdScroll class=\"clScroll2\" onclick=\"parent.fnScrollTabs(1);\"
ondblclick=\"parent.fnScrollTabs(1);\" onmouseover=\"parent.fnMouseOverScroll(2);\"
onmouseout=\"parent.fnMouseOutScroll(2);\"><a>&gt</a></td>"+
  "<td valign=top id=tdScroll class=\"clScroll\" onclick=\"parent.fnFastScrollTabs(1);\"
onmouseover=\"parent.fnMouseOverScroll(3);\"
onmouseout=\"parent.fnMouseOutScroll(3);\"><a>&#187;</a></td>"+
  "<td style=\"font:1pt\"> <td></tr></table></body></html>";
 with (frames['frScroll'].document) {
  open("text/html","replace");
  write(szHTML);
  close();
 }
 szHTML =
  "<html><head>"+
  "<style>A:link,A:visited,A:active {text-decoration:none;"+"color:"+c_rgszClr[3]+";}"+
  ".clTab {cursor:hand;background:"+c_rgszClr[1]+";font:9pt Arial;padding-
left:3px;padding-right:3px;text-align:center;}"+
  ".clBorder {background:"+c_rgszClr[2]+";font:1pt;}"+
  "</style></head><body onload=\"parent.fnInit();\"
onselectstart=\"event.returnValue=false;\" ondragstart=\"event.returnValue=false;\"
bgcolor="+c_rgszClr[4]+
```

```
 " topmargin=0 leftmargin=0><table id=tbTabs cellpadding=0 cellspacing=0>";
 var iCellCount=(c_lTabs+1)*2;
 var i;
 for (i=0;i<iCellCount;i+=2)
  szHTML+="<col width=1><col>";
 var iRow;
 for (iRow=0;iRow<6;iRow++) {
  szHTML+="<tr>";
  if (iRow==5)
   szHTML+="<td colspan="+iCellCount+"></td>";
  else {
   if (iRow==0) {
    for(i=0;i<iCellCount;i++)
     szHTML+="<td height=1 class=\"clBorder\"></td>";
   } else if (iRow==1) {
    for(i=0;i<c_lTabs;i++) {
     szHTML+="<td height=1 nowrap class=\"clBorder\"> </td>";
     szHTML+=
      "<td id=tdTab height=1 nowrap class=\"clTab\"
onmouseover=\"parent.fnMouseOverTab("+i+");\"
onmouseout=\"parent.fnMouseOutTab("+i+");\">"+
      "<a href=\""+document.all.item("shLink")[i].href+"\" target=\"frSheet\"
id=aTab> "+c_rgszSh[i]+" </a></td>";
    }
    szHTML+="<td id=tdTab height=1 nowrap class=\"clBorder\"><a
id=aTab> </a></td><td width=100%></td>";
   } else if (iRow==2) {
    for (i=0;i<c_lTabs;i++)
     szHTML+="<td height=1></td><td height=1 class=\"clBorder\"></td>";
    szHTML+="<td height=1></td><td height=1></td>";
   } else if (iRow==3) {
    for (i=0;i<iCellCount;i++)
```

```
    szHTML+="<td height=1></td>";
   } else if (iRow==4) {
    for (i=0;i<c_lTabs;i++)
     szHTML+="<td height=1 width=1></td><td height=1></td>";
    szHTML+="<td height=1 width=1></td><td></td>";
   }
  }
  szHTML+="</tr>";
 }
 szHTML+="</table></body></html>";
 with (frames['frTabs'].document) {
  open("text/html","replace");
  charset=document.charset;
  write(szHTML);
  close();
 }
}
function fnInit()
{
 g_rglTabX[0]=0;
 var i;
 for (i=1;i<=c_lTabs;i++)
  with (frames['frTabs'].document.all.tbTabs.rows[1].cells[fnTabToCol(i-1)])
   g_rglTabX[i]=offsetLeft+offsetWidth-6;
}
function fnTabToCol(iTab)
{
 return 2*iTab+1;
}
function fnNextTab(fDir)
{
 var iNextTab=-1;
```

```
 var i;
 with (frames['frTabs'].document.body) {
  if (fDir==0) {
   if (scrollLeft>0) {
    for (i=0;i<c_lTabs&&g_rglTabX[i]<scrollLeft;i++);
    if (i<c_lTabs)
     iNextTab=i-1;
   }
  } else {
   if (g_rglTabX[c_lTabs]+6>offsetWidth+scrollLeft) {
    for (i=0;i<c_lTabs&&g_rglTabX[i]<=scrollLeft;i++);
    if (i<c_lTabs)
     iNextTab=i;
   }
  }
 }
 return iNextTab;
}
function fnScrollTabs(fDir)
{
 var iNextTab=fnNextTab(fDir);
 if (iNextTab>=0) {
  frames['frTabs'].scroll(g_rglTabX[iNextTab],0);
  return true;
 } else
  return false;
}
function fnFastScrollTabs(fDir)
{
 if (c_lTabs>16)
  frames['frTabs'].scroll(g_rglTabX[fDir?c_lTabs-1:0],0);
 else
```

```
  if (fnScrollTabs(fDir)>0) window.setTimeout("fnFastScrollTabs("+fDir+");",5);
}
function fnSetTabProps(iTab,fActive)
{
 var iCol=fnTabToCol(iTab);
 var i;
 if (iTab>=0) {
  with (frames['frTabs'].document.all) {
   with (tbTabs) {
    for (i=0;i<=4;i++) {
     with (rows[i]) {
      if (i==0)
       cells[iCol].style.background=c_rgszClr[fActive?0:2];
      else if (i>0 && i<4) {
       if (fActive) {
        cells[iCol-1].style.background=c_rgszClr[2];
        cells[iCol].style.background=c_rgszClr[0];
        cells[iCol+1].style.background=c_rgszClr[2];
       } else {
        if (i==1) {
         cells[iCol-1].style.background=c_rgszClr[2];
         cells[iCol].style.background=c_rgszClr[1];
         cells[iCol+1].style.background=c_rgszClr[2];
        } else {
         cells[iCol-1].style.background=c_rgszClr[4];
         cells[iCol].style.background=c_rgszClr[(i==2)?2:4];
         cells[iCol+1].style.background=c_rgszClr[4];
        }
       }
      } else
       cells[iCol].style.background=c_rgszClr[fActive?2:4];
     }
```

```
    }
   }
   with (aTab[iTab].style) {
    cursor=(fActive?"default":"hand");
    color=c_rgszClr[3];
   }
  }
 }
}

function fnMouseOverScroll(iCtl)
{
 frames['frScroll'].document.all.tdScroll[iCtl].style.color=c_rgszClr[7];
}
function fnMouseOutScroll(iCtl)
{
 frames['frScroll'].document.all.tdScroll[iCtl].style.color=c_rgszClr[6];
}
function fnMouseOverTab(iTab)
{
 if (iTab!=g_iShCur) {
  var iCol=fnTabToCol(iTab);
  with (frames['frTabs'].document.all) {
   tdTab[iTab].style.background=c_rgszClr[5];
  }
 }
}
function fnMouseOutTab(iTab)
{
 if (iTab>=0) {
  var elFrom=frames['frTabs'].event.srcElement;
  var elTo=frames['frTabs'].event.toElement;
```

```
  if ((!elTo) ||
   (elFrom.tagName==elTo.tagName) ||
   (elTo.tagName=="A" && elTo.parentElement!=elFrom) ||
   (elFrom.tagName=="A" && elFrom.parentElement!=elTo)) {
   if (iTab!=g_iShCur) {
    with (frames['frTabs'].document.all) {
     tdTab[iTab].style.background=c_rgszClr[1];
    }
   }
  }
 }
}
function fnSetActiveSheet(iSh)
{
 if (iSh!=g_iShCur) {
  fnSetTabProps(g_iShCur,false);
  fnSetTabProps(iSh,true);
  g_iShCur=iSh;
 }
}
 window.g_iIEVer=fnGetIEVer();
 if (window.g_iIEVer>=4)
  fnBuildFrameset();
//-->
</script>
<![endif]><!--[if gte mso 9]><xml>
 <x:ExcelWorkbook>
  <x:ExcelWorksheets>
   <x:ExcelWorksheet>
    <x:Name>Sheet1</x:Name>
    <x:WorksheetSource HRef="Output%20not%20all%20box_files/sheet001.htm"/>
   </x:ExcelWorksheet>
```

```
  </x:ExcelWorksheets>
  <x:Stylesheet HRef="Output%20not%20all%20box_files/stylesheet.css"/>
  <x:WindowHeight>10420</x:WindowHeight>
  <x:WindowWidth>19420</x:WindowWidth>
  <x:WindowTopX>32767</x:WindowTopX>
  <x:WindowTopY>32767</x:WindowTopY>
  <x:ProtectStructure>False</x:ProtectStructure>
  <x:ProtectWindows>False</x:ProtectWindows>
 </x:ExcelWorkbook>
</xml><![endif]-->
</head>
<frameset rows="*,39" border=0 width=0 frameborder=no framespacing=0>
 <frame src="Output%20not%20all%20box_files/sheet001.htm" name="frSheet">
 <frame src="Output%20not%20all%20box_files/tabstrip.htm" name="frTabs"
marginwidth=0 marginheight=0>
 <noframes>
  <body>
   <p>This page uses frames, but your browser doesn't support them.</p>
  </body>
 </noframes>
</frameset>
</html>
```


Biography.

Gaurav received his bachelor's degree in computer science from Gautama Buddha University, Lucknow, India, in 2010 and his master's degree in VLSI and CAD systems from Thapar University Punjab, India, in 2012. He worked as Research Assistant in a Modular threat assessment project by Innovative United Kingdom (IUK). He also worked as a post-doctoral fellow at De-Montfort University. He is currently working as a Research Engineer at the Nuclear AMRC Sheffield University and pursuing a PhD in the cybersecurity research group at the University of Hertfordshire Hatfield, UK-School of computer science. He focuses on Real-Time Semi-Automated Threat Assessments in Informational Environment. His research areas include Cloud Computing, the Internet of Things, Cybersecurity, Cryptography, and Security in Wireless Sensor Networks.