A methodological approach to investigating lateral movement attacks using a threat hunting architecture

T Mokoena

orcid.org 0002-3097-5840

Dissertation accepted in fulfilment of the requirements for the degree *Master of Science in Computer Science* at the North-West University

Supervisor: Dr R Serfontein

Co-supervisor: Prof HA Krüger

Examination: July 2025

Preface

All honour and glory to our Heavenly Father, Lord, and Saviour, without whom none of this would have been possible. Thank you for giving me the strength, courage, and perseverance to complete this study.

I extend my heartfelt gratitude to my supervisor, Dr. Rudi Serfontein, for your unwavering support and guidance throughout this journey. Your critical and constructive feedback has been instrumental in keeping me on track and ensuring the quality of my work. To my co-supervisor, Prof. Hennie Kruger, the voice of reason behind the scenes, thank you for your invaluable insights and meticulous attention to detail. Your ability to highlight the small but significant aspects played a crucial role in shaping this dissertation.

To my family, my loving wife, Sandy Mokoena, thank you for stepping into my role and supporting me so selflessly while I was immersed in writing. To my two amazing and spirited children, Khanya and Katli, your unwavering support and prayers have been my constant source of motivation. Thank you for believing in me and inspiring me to pursue this path.

This dissertation is not just a reflection of my academic journey but also a testament to the love, faith, and support of those around me. To all who stood by me, encouraged me, and made this achievement possible, thank you from the depths of my heart.

Abstract

In this study, the application of hypothesis-driven threat hunting methodologies to detect lateral movement attacks is investigated. Lateral movement attacks, as pivotal components of advanced persistent threats (APTs), enable attackers to stealthily navigate and exploit compromised networks by moving from one compromised system to another within the same network. One approach to detecting such threats is through threat hunting, which involves proactively identifying threats based on known tactics and behaviours. A key focus of this study is the Targeted Hunting integrated Threat Intelligence (TaHiTI) methodology. The primary objective is to investigate the applicability of TaHiTI and assess its potential for improving cybersecurity defences against lateral movement attacks. This is achieved using a simulation-based experimental design that replicates various attack scenarios within a controlled virtual laboratory. Through a structured qualitative approach supported by experimental simulation, this study assesses the applicability of the TaHiTI methodology in detecting lateral movement attacks. The findings highlight the strengths of the methodology in detecting stealthy attacker behaviours and its relevance for practical implementation in cybersecurity operations. Limitations related to simulation-based research are discussed, along with opportunities for future work, including real-world testing and expanded threat modelling. The study contributes to both academic and applied cybersecurity by demonstrating how structured, intelligence-driven hunting strategies can advance the detection of sophisticated intrusions.

Keywords: Lateral movement detection, advanced persistent threats, threat hunting, TaHiTI methodology, cybersecurity methodologies, MITRE ATT&CK framework, simulation-based research, proactive threat detection, continuous innovation, network security

Opsomming

In hierdie studie word die aktiewe opsporing van laterale bewegingsaanvalle ondersoek. Laterale bewegingsaanvalle, as deurslaggewende komponente van gevorderde aanhoudende bedreigings (APT's), stel aanvallers in staat om sluipende netwerke te navigeer en te ontgin deur van een gekompromitteerde stelsel na 'n ander binne dieselfde netwerk te beweeg. Een benadering om laterale bewegingsaanvalle op te spoor is deur gebruik te maak van dreigementjag, wat 'n benadering is waardeur bedreigings opgespoor word deur hul bekende kenmerke te gebruik. Een van hierdie bedreigingjagtegnieke is die Targeted Hunting-geïntegreerde Threat Intelligence (TaHiTI) metodologie. Die primêre doel van hierdie studie is om die TaHiTI-metodologie in 'n beheerde omgewing aan te neem en te valideer. Hierdie studie het ten doel om die toepaslikheid en doeltreffendheid van TaHiTI te ondersoek in die verbetering van kuberveiligheidverdediging teen laterale bewegingsaanvalle, wat bydra tot die begrip van bedreigingjagmetodologieë in kuberveiligheid. Deur 'n simulasie-gebaseerde eksperimentele ontwerp te gebruik, herhaal hierdie studie verskeie laterale bewegingsaanvalscenario's binne 'n beheerde virtuele laboratoriumomgewing. Deur 'n benadering wat kwalitatiewe data-analise insluit, beoordeel hierdie studie die doeltreffendheid van die TaHiTI-metodologie in die opsporing van laterale bewegingsaanvalle. Die bevindinge demonstreer die potensiaal van die TaHiTI-metodologie om laterale bewegingsaktiwiteite proaktief te identifiseer, wat die geskiktheid daarvan vir praktiese toepassings in kuberveiligheid beklemtoon. Terwyl die sterkpunte van die metodologie ten toon gestel word, spreek die studie ook die beperkings aan wat inherent is aan simulasie-gebaseerde navorsing en skets aanwysings vir toekomstige werk, insluitend die behoefte aan werklike toepassingstoetsing en verdere verkenning van laterale bewegingstegnieke. Dit beklemtoon die kritieke rol van voortdurende innovasie en aanpassing in kuberveiligheidspraktyke om tred te hou met die vinnig ontwikkelende bedreigingslandskap. Die bekragtiging van TaHiTI in 'n akademiese omgewing verryk nie net die vakkundige diskoers oor kubersekuriteitsmetodologieë nie, maar stel ook die weg voor vir verdere navorsing en ontwikkeling wat daarop gemik is om kuberveiligheidsverdediging te bevorder.

Sleutelwoorde: Laterale bewegingsopsporing, gevorderde aanhoudende bedreigings, bedreigingjag, TaHiTI-metodologie, kuberveiligheidsmetodologieë, MITER ATT&CK-raamwerk, simulasie-gebaseerde navorsing, proaktiewe bedreigingopsporing, deurlopende innovasie, netwerksekuriteit

TABLE OF CONTENTS

List of abbreviations

APT	Advanced Persistent Threats
C2	Command and Control
EDR	Endpoint Detection and Response
HELK	Hunting ELK (Elasticsearch, Logstash, Kibana)
IOC	Indicator of compromise
MITRE ATT&CK	MITRE Adversarial Tactics, Techniques, and Common Knowledge
NTLM	New Technology Lan Manager
PtH	Pass-the-Hash
RAT	Remote access tool
RDP	Remote desktop protocol
SMB	Server message block
TaHiTI	Targeted Hunting integrated Threat Intelligence
TTP	Tactics, Techniques, and Procedures
WMI	Windows Management Instrumentation

List of figures

List of tables

Chapter 1 Introduction and contextualisation

1.1. Introduction

In today's cybersecurity landscape, lateral movement has emerged as a critical tactic that advanced persistent threats (APTs) employ to navigate compromised networks stealthily. APTs are a type of cyberattack that enables an adversary to infiltrate an organisation's network environment for an extended period of time without detection (Wang *et al.*, 2021; Yan *et al.*, 2019). This kind of attack allows attackers to escalate privileges, access sensitive data, and expand their footholds within the infrastructure of an organisation (Purilock, 2024). Recent analyses underscore the increasing sophistication of lateral movement strategies, particularly in ransomware attacks, where threat actors meticulously traverse networks to maximise their impact (Chacko *et al.*, 2022; Smiliotopoulos *et al.*, 2023).

Lateral movement is a sophisticated cyberattack technique in which attackers navigate deeper into compromised networks to access valuable assets (Lanaerts-Bergmans, 2023). This phase, which accounts for 80% of an attack's timeline, allows attackers to expand their influence on the victim's environment (Cynet, 2024; Zhao *et al.*, 2020). The prolonged nature and complexity of these attacks, coupled with the vast amount of data generated, pose significant challenges for organisations in terms of threat detection and incident response (Hospelhorn, 2020). Current detection methods, which often provide after-the-event analyses, have limited effectiveness in preventing ongoing attacks. The high volume of internal network traffic and false positives further complicate the detection and prevention of lateral movement attacks (Kambourakis *et al.*, 2024).

Traditional security measures often struggle to detect covert activities, as attackers adeptly mimic legitimate user behaviours to evade detection. This challenge has prompted a paradigm shift toward proactive defence mechanisms, notably threat hunting (Bienzobas & Sánchez-Macián, 2023). Threat hunting involves a systematic and continuous search for indicators of compromise within an organisation's network, aiming to identify and mitigate threats before they can inflict significant damage (Pérez-Gomariz *et al.*, 2024). The 2024 SANS Threat Hunting Survey highlights a growing maturity in threat-hunting methodologies, with a significant increase in organisations adopting formal

processes (Fuchs & Lemon, 2024). The prolonged dwell time between an attacker's initial network penetration and their detection exacerbates the threat posed by lateral movement. Attackers can remain undetected for extended periods, significantly increasing their potential for data exfiltration, operational sabotage, and reputational damage. Such extended access not only escalates potential damage but also complicates the response and recovery processes (Rabbani *et al.*, 2024).

The persistence and stealth of lateral movement highlights a critical gap in traditional cybersecurity frameworks, necessitating the development of more advanced detection strategies. Addressing the inherent challenges of detecting lateral movement is essential for organisations to defend against sophisticated threats and mitigate the adverse impacts of cyberattacks. **This study aims to investigate the application of threat hunting methodologies for the effective detection of lateral movement attacks within organisational networks**. By exploring innovative approaches to identify and mitigate these threats, this study seeks to contribute to the development of more robust cybersecurity strategies and improve the protection of critical organisational assets.

1.2. Goals and objectives

The primary objective of this study is to explore how the TaHiTI methodology can be effectively applied to detect lateral movement attacks in a controlled environment. This objective supports the research question and anchors the study in practical implementation and evaluation. In the rapidly evolving field of cybersecurity, lateral movement attacks present a significant challenge to organisational networks. These sophisticated techniques enable APT to stealthily navigate compromised systems, escalate privileges, and access sensitive data (Lanaerts-Bergmans, 2023). To effectively counteract such threats, threat hunting methodologies can be implemented. This section delineates the primary goals and objectives of the study, which are designed to address the central research question: "**How can a threat hunting methodology be effectively applied to detect lateral movement attacks within organisational networks?**" To address this research question, this study aimed to achieve the following objectives:

- **Explore** lateral movement and the techniques employed by APTs. This is accomplished by reviewing the literature in order to identify and categorise the

methods used by APTs to perform lateral movement attacks within networks and develop an understanding of lateral movement strategies.

- **Investigate** approaches to addressing lateral movement attacks by reviewing the literature and identifying various approaches and techniques that can be used, analysing their strengths and limitations, and selecting those approaches or techniques that warrant further investigation.
- **Identify** an effective approach to setting up a virtual environment for simulations based on the needs of the approaches or techniques identified and create a virtual testing environment based on those needs.
- **Validate** the approaches and/or techniques identified by applying them in the virtual environment.
- **Discuss** the findings obtained from the experimental data and make recommendations regarding the validity of the identified approaches and/or frameworks.

By systematically pursuing these objectives, this study aimed to contribute to the field of cybersecurity by improving the understanding of lateral movement attacks and improving the methodologies employed to detect and mitigate such threats. The insights gained from this research are expected to help organisations strengthen their defence mechanisms against sophisticated adversaries.

1.3. Scope of the study

Lateral movement represents a significant threat to networked devices, especially if the attacks remain undetected. As with other threats within cybersecurity, there are a significant number of techniques and approaches that can be employed to address these threats. For this reason, the scope of this study was restricted to investigating a specific subset of these approaches, namely threat hunting, in order to make it manageable within the confines of a single study. As such, other techniques or approaches, regardless of validity, were considered outside the scope of this study. Furthermore, due to the positive impact that detecting these attacks could have on the security of a network, only lateral movement as an attack category was considered. While true that APTs employ other attack strategies that can be even more destructive, reducing the incidence of lateral movement should significantly reduce the impact of APT attacks in general, and therefore

attack categories other than lateral movement were also considered outside the scope of the study. Finally, this study focused specifically on investigating lateral movement detection using threat hunting, and steps that can be taken to mitigate these attacks were therefore not within the scope of this study.

1.4. Ethical considerations

The research proposal was presented to the Faculty of Natural and Agricultural Sciences' Ethics Committee for ethical clearance. The study was approved as a no risk study and the ethics number NWU-00483-21-A9 was issued on 01 March 2021. The following ethical considerations were adhered to during the execution of the study:

- This study does not use data from human or animal participants;
- The study does not use data from either public or private data sets;
- The study does not use confidential or sensitive data, as it is all simulated and not applicable or related to real-world entities; and
- The ethical committee approved it as a no-risk study.

In the event that any other ethical concerns had arisen during the execution of the study, the appropriate ethics committee would have been contacted before proceeding.

1.5. Structure of the study

This study is systematically organised to provide a comprehensive exploration of lateral movement attacks within organisational networks and the application of threat hunting methodologies to detect such threats. The remainder of this study is organised as follows.

i. Chapter 1: Introduction

Chapter 1 sets the stage for investigation into the nuanced realm of lateral movement attacks within cybersecurity. The study is framed by presenting an overview of the research topic, including background, problem statement, research question, goals and objectives, scope, ethical considerations, and structure of the study.

ii. Chapter 2: Advanced persistent threats

Chapter 2 delves deep into advanced persistent threats (APTs), defining them as long-term stealthy cybersecurity attacks designed to penetrate and remain undetected within an organisation's network. The discussion progresses through the stages of APTs, emphasising the importance of lateral movements in allowing attackers to navigate compromised systems and access sensitive information. This chapter also examines existing detection frameworks, such as intrusion detection systems and network anomaly detection, outlining their capabilities and limitations, and laying the groundwork for the importance of the innovative detection strategies discussed in this study.

iii. Chapter 3: Threat hunting

Chapter 3 discusses the evolution, strategies, and methodologies of threat hunting in cybersecurity. The chapter emphasises the proactive nature of threat hunting in identifying hidden threats and discusses how it significantly reduces dwell time and bridge breach detection gaps. The chapter concludes with a detailed examination of the adopted threat hunting methodology adopted in this study because of its comprehensive approach to integrating threat intelligence with proactive hunting practices.

iv. Chapter 4: Research methodology

Chapter 4 outlines the research design, including the methods and procedures employed to achieve the objectives of the study. It details of the development of the threat hunting environment and the validation process for the adopted threat hunting methodology.

v. Chapter 5: Hypothesis-driven threat hunting architecture testing

Chapter 5 presents a rigorous validation process for the adopted threat hunting methodology through experiments conducted in a controlled laboratory environment. By leveraging hypotheses derived from known frameworks, this chapter illustrates the operationalisation of a hypothesis-driven threat hunting model aimed at simulating lateral movement attacks. The detailed narrative of the simulation process, from tool selection to execution and threat hunting, sets the stage for a critical evaluation of the effectiveness of the methodology in an academic setting.

vi. Chapter 6: Results analysis and validation of TaHiTi

In Chapter 6, a detailed analysis of the experimental results obtained in Chapter 5 is presented. This analysis examines lateral movement techniques within the framework of the threat hunting platform and the adopted methodology, offering a granular look at how APT exploit these techniques. The chapter transitions from hypothesis testing to in-depth technical analysis, culminating in a discussion of the significance of advanced threat hunting in identifying and mitigating lateral movement attacks within network environments.

vii. Chapter 7: Summary and conclusion

Chapter 7 synthesises the study findings, reflects on how the research objectives were achieved, and addresses the challenges encountered. This final chapter not only underscores the contributions of the study to both theory and practice, but also proposes avenues for future research, suggesting how subsequent investigations can build on the foundations and insights of this work. This structured approach ensures logical progression of ideas and facilitates a clear understanding of the study. Each chapter builds upon the previous one, culminating in a comprehensive analysis of the detection and mitigation of lateral movement attacks using threat hunting methodologies.

1.6. Chapter summary

This chapter discusses the fundamental aspects of this study. It begins by defining the problem statement and the goals and objectives of the study. The study's scope is then defined. The chapter concludes with a thorough overview of the study's structure, emphasising the main themes for each section and summarising the content of individual chapters.

Chapter 2 Advanced persistent threats

2.1. Introduction

In this study, the use of threat hunting to detect advanced persistent threats (APT) attacks, specifically lateral movement, is investigated in an academic context. Subsequently, an in-depth look at APTs is warranted. This chapter discusses APTs and elaborates on the special forms of lateral movement attacks described in literature. The chapter starts by defining APTs in general, followed by a more in-depth look at lateral movement attacks. Several models and frameworks, such as MITRE ATT&CK and cyber kill chain models, which can be used to detect lateral movement attacks, are also discussed.

2.2. Advanced persistent threats and lateral movement

This section begins with a background on advanced persistent threats (APTs), and then discusses how APTs execute lateral movement attacks and describes the characteristics of APT. This is followed by a discussion of lateral movement, including APT and lateral movement attack lifecycles. Additionally, it discusses the detection frameworks and models that can be used to identify lateral movement attacks.

2.2.1. Advanced persistent threats (APTs)

Advanced persistent threats (APTs) are a type of cyberattack that enables an adversary to infiltrate an organisation's network environment for an extended period of time without detection (Wang *et al.*, 2021; Yan *et al.*, 2019). This attack is carried out by a malicious actor, also known as an adversary, who is responsible for a security incident that can compromise the security of an organisation (Dong *et al.*, 2021). APTs employ various Tactics, Techniques and Procedures (TTPs) to infiltrate, persist within, and move laterally across targeted networks, posing significant challenges to the security of an organisation.

A critical technique in the lateral movement phase is credential dumping, in which attackers extract usernames and passwords from compromised systems using tools such as Mimikatz, enabling them to access additional systems and expand their control (Bi *et*

al., 2023). Furthermore, attackers often use pass-the-hash and pass-the-ticket techniques to authenticate network resources without actual passwords, bypassing standard authentication controls and gaining access to sensitive data and critical systems (Wilkens *et al.*, 2019). Furthermore, remote execution tools such as PsExec, PowerShell, and Windows Management Instrumentation (WMI) are commonly employed by adversaries to execute commands and scripts on remote systems, facilitating control over compromised systems and enabling lateral movement within the network (Mailewa & Rozendaal, 2022). These lateral movement techniques are crucial for APT operations because they allow adversaries to navigate networks stealthily, access high-value targets, and achieve long-term objectives while minimising the risk of detection.

Through these methods, APTs can compromise systems, interrupt services, commit financial fraud, and expose or steal intellectual property (Zheng, 2020). Attacks initiated by APTs can remain undetected for a significant period of time, making it crucial to identify them as they can cause significant harm to organisations and result in substantial financial losses. The SolarWinds attack, for example, went undetected for several months, allowing attackers to compromise systems, interrupt services, commit financial fraud, and expose or steal intellectual property (Quintero-Bonilla & Martín del Rey, 2020).

APT attacks have multiple phases, such as reconnaissance, preliminary compromise, and privilege escalation, and use various attack techniques, including social engineering, malware, and software and system vulnerabilities (Al-Saraireh & Masarweh, 2022). The goal of an attacker is to gain access to the system and obtain valuable information while remaining undetected for as long as possible, which can cause significant damage to the target network. The "lateral movement" phase is the focus of this study, and while other phases of APTs enable adversaries to gain a foothold within a victim's network and establish persistence by escalating the attack level (Dong *et al.*, 2021), these phases are beyond the scope of this study. Adversaries can then use lateral movement attacks to move from one compromised system to another and gain access to the sensitive resources. This allows them to access systems that have not been previously compromised (Al-Saraireh & Masarweh, 2022).

The National Institute of Standards and Technology (NIST, 2011) defines APT as an "adversary with sophisticated levels of expertise and significant resources, enabling it to generate opportunities through the use of multiple attack vectors to achieve its objectives,

which are typically to establish and extend footholds within the information technology infrastructure of organisations for the purpose of continuously exfiltrating information and/or to undermine or impair the organisation's operations". APTs are resourceful, have clear goals and reasons for doing what they do, and possess strong technical skills. A breach in a company's network can remain undetected for an extended period, providing attackers ample time to execute their attacks (Alshamrani *et al.*, 2019).

In addition to the features of APTs, Alshamrani *et al.* (2019) emphasise that adversaries are well-resourced and organised, continually trying to gain access to victims' environments for a long period of time and employing stealthy and evasive attack methods to avoid detection. APT attacks usually target specific organisations or industries and involve extensive reconnaissance. They sneak into their target networks and remain undetected. This, along with their well-organised and well-resourced approach, explains their persistence and use of stealthy and evasive attack techniques. APT-orientated attacks are planned and have a focused approach that follows an attack life cycle consisting of multiple phases (Lehto, 2022; Zou *et al.*, 2020). In this sense, APTs are fierce opponents that are difficult to counter. Intrusion attempts by these adversaries are not constantly reinvented, which means that a model can be used to predict their behaviour (Araujo *et al.*, 2021).

The next section discusses lateral movement in detail in relation to APTs. Lateral movement is a critical phase in the lifecycle of an APT attack, allowing adversaries to traverse the network, access higher value targets, and maintain persistence. Understanding and detecting lateral movement are essential to mitigate the impact of APTs and protect organisational assets.

2.2.2. Lateral movement

This section focuses on lateral movement (LM) and its relation to advanced persistent threats (APT), including its lifecycle, as discussed in Section 2.2.2. It provides a comprehensive overview of LM, examines the detection capabilities proposed by researchers, and concludes with a summary of key points. Nolette and Devry (2020) define lateral movement as a critical step in the network attack process, which encompasses its own kill chain steps. APT attack campaigns involve lateral movement, described in various attack taxonomies, such as the Lockheed Martin cyber kill chain

(Ahmed *et al.*, 2021) and MITRE ATT&CK frameworks (Kinnunen, 2022; Roy *et al.*, 2023). A simplified version of the APT lifecycle campaign is shown in Figure 2-1.

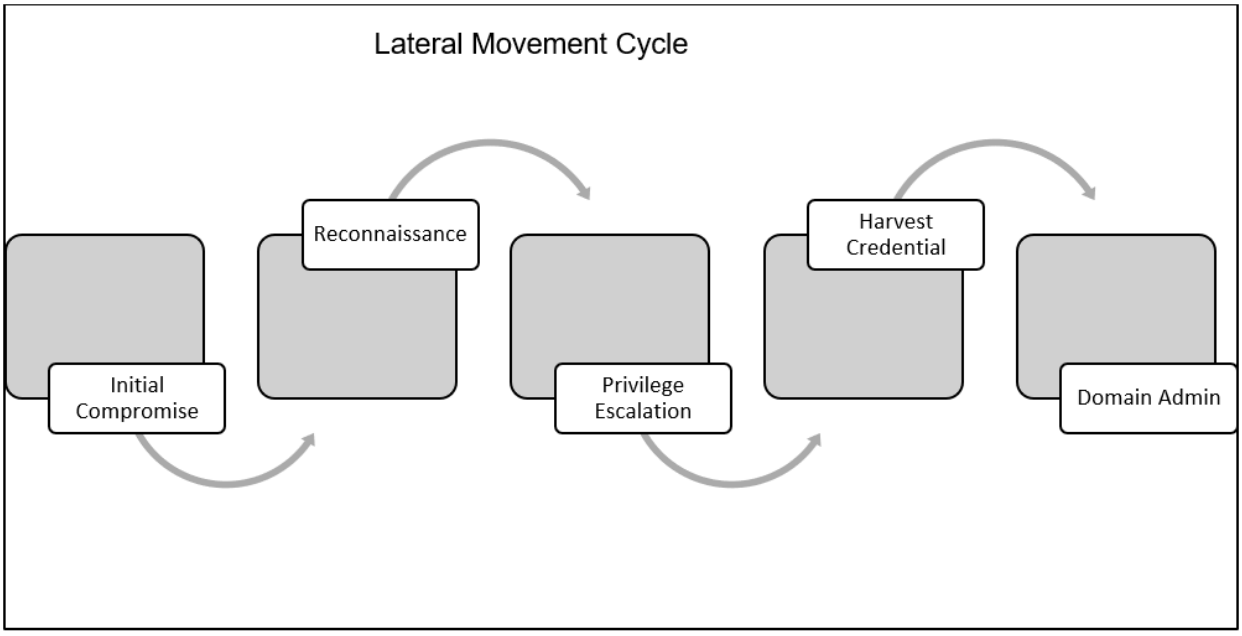


Figure 2-1: APT campaign showing the Lateral Movement cycle (Adapted from: Bowman *et al.*(2020))

Once an adversary has gained initial access through compromised credentials and elevated privileges, they move laterally across the network using these credentials to access other systems until they obtain domain credentials. Typically, they target a user workstation by exploiting system or software vulnerabilities. After gaining initial low-privileged access, they escalate their privileges, allowing them to perform LM by moving from one system to another through the network to achieve their objectives. This makes it imperative to detect these attacks promptly, as attackers can gradually increase their access to critical systems over time. The next section discusses various methods for detecting LM attacks.

2.2.1.1 Lateral movement detection

The MITRE ATT&CK framework lists many lateral movement techniques and describes the detection and mitigation strategies discussed in Section 2.2.1.2 (Georgiadou *et al.*, 2021; Kinnunen, 2022; Sica *et al.*, 2023). The main distinction between lateral movement detection and other intrusion detection methods is that lateral movement occurs after the initial network is compromised. Consequently, lateral movement is typically carried out behind the security controls installed to protect an organisation's network boundaries.

Various studies, such as those conducted by Rajesh *et al.* (2021), have evaluated various lateral movement detection frameworks and architectures, which are summarised in this section.

Mavroeidis and Josang (2018) introduced a data-driven threat classification methodology based on ongoing evaluation and analysis of aggregated system monitor (sysmon) logs. The development of the proposed Cyber Threat Intelligence Ontology (CTIO) was based on the Cyber Threat Intelligence model, which was also published and represents the majority of the first part of this work (Mavroeidis & Bromander, 2017). In the second part of the study, a threat assessment system is proposed that uses CTIO to classify sysmon's event logs into four threat categories: high, medium, low and unknown. Additionally, this threat assessment system is based on a cyber threat intelligence ontology to automatically classify executed software into various threat levels by analysing sysmon logs. By augmenting cyber-defensive capabilities through situational awareness, prediction, and automated actions, the proposed system and approach enhance these capabilities.

Fawaz *et al.* (2016) proposed a lateral movement detection architecture to propagate host-level monitoring from a global network-wide perspective. Detection is based on monitoring inter-process communication at the host level, and the results are aggregated into clusters to form a host communication graph. To identify inter-cluster connections, host communication graphs were evaluated globally. Fawaz *et al.* (2016) contend that monitoring process system calls allows for the detection of lateral movement more effectively than using timing information or port numbers. Although this approach demonstrates that monitoring process network usage can detect lateral movements, no qualification can be given as to whether the movement is malicious.

Rajesh *et al.* (2021) and Jain and Conklin (2018) also used an Elastic Stack (ELK) to analyse enormous log records and detect malicious behaviour. Rajesh *et al.* (2021) implemented a massive log stash data processing pipeline to gather a critical mass of logs, while Jain and Conklin (2018) produced sysmon log events. In both cases, ELK was used to iterate the log files and identify malicious patterns. However, both studies neglected the requirement for a general-purpose rule-based endpoint detection and response (EDR) system because they were closely related to ELK practices.

Sqrrl (2018) proposed a framework for cyber threat hunting for advanced persistent defences (APD) to detect APT attacks proactively. The goal of this framework is to create a defence structure that evolves in response to each attack. Defenders can streamline response times and mitigate the challenge of persistence by cataloguing observations about attacker TTPs, weak points in their defences, and obstructions in the investigative workflow (Sqrrl, 2018). Analysts can present the information collected to their security teams and use these interpretations to improve defensive technologies and consistently refine detection/response techniques. Improving past failures and investing more in effective strategies allow the security team to stay one step ahead of adversaries rather than one step behind them. Intelligence, hunting, and response are the three main cycles in the APD framework (Sqrrl, 2018).

The APD framework is uniquely equipped to detect TTPs, which is an important feature. TTPs are the strongest compromise indicators to detect and prevent APT attacks. With its emphasis on intelligence-driven threat hunting and response, APD is a framework for delving deeper into adversaries' actions by leveraging an understanding of their behaviour (TTPs) to help defences evolve faster than attacks. This study focuses on threat hunting for APT attacks, specifically lateral movement attacks. In summary, an APT gains access to a computer on a network by exploiting a vulnerability (e.g. a code injection attack) or by making use of user errors, such as opening suspicious emails. To expand access, they must maintain persistence while moving laterally to other network resources. This section presents an overview of lateral movement, its detection, and the relevant studies on the topic.

2.2.3. APT attack lifecycle

The cybersecurity industry has long been viewed as a cat-and-mouse game between attackers and defenders, with defenders often trailing behind (Ahmed *et al.*, 2021; Chain, 2015). APTs are designed to stealthily exfiltrate sensitive and valuable information from a network. As a result, most security systems struggle to detect or prevent these types of attacks because of their well-organised and sophisticated nature. One of the most infamous APT attacks is Stuxnet, which targeted Iran's nuclear program and critical physical systems (Utinková, 2021). Ussath *et al.* (2016) analysed 22 different APT incidents and identified common methods used within the different phases of APT attacks. They concluded that credential dumping is a frequent tactic for hackers to move laterally

through a network. This method allows attackers to mask their activities as normal traffic, making detection more challenging and enabling them to circumvent existing security measures. LM attacks, which are part of APT strategies, allow attackers to maintain unauthorised access to a network for extended periods without detection. Social engineering is the most common method used to initiate a compromise between the internal network and perimeter (Bullée *et al.*, 2018).

Once an attacker compromises one computer within the organisation, they gain access to sensitive information through LM, enabling them to move from one computer to the next. The primary goal of LM attacks is often to control the domain controller, which can be either the final objective or a step towards further compromise to access sensitive data. The scenario shown in Figure 2-2 is a typical example of an APT attack involving a local machine. Local machine attacks consist of two stages. During the first stage, attackers take valid credentials of the host and employ them to access the target host or resources on the opposite side of the attack. These attacks occur when an attacker successfully acquires legitimate credentials from a source host and uses them to connect to the target host. Soria-Machado *et al.* (2017) revealed several methods for detecting local machine attacks. According to the study, there is no distinction between genuine connections and connections made using stolen credentials at the protocol level. Techniques, such as pass-the-hash and pass-the-ticket, can also be used (Soria-Machado *et al.*, 2017). A simple indicator of a local machine attack could be the use of a domain administrator's account on a device other than the one it is intended to use.

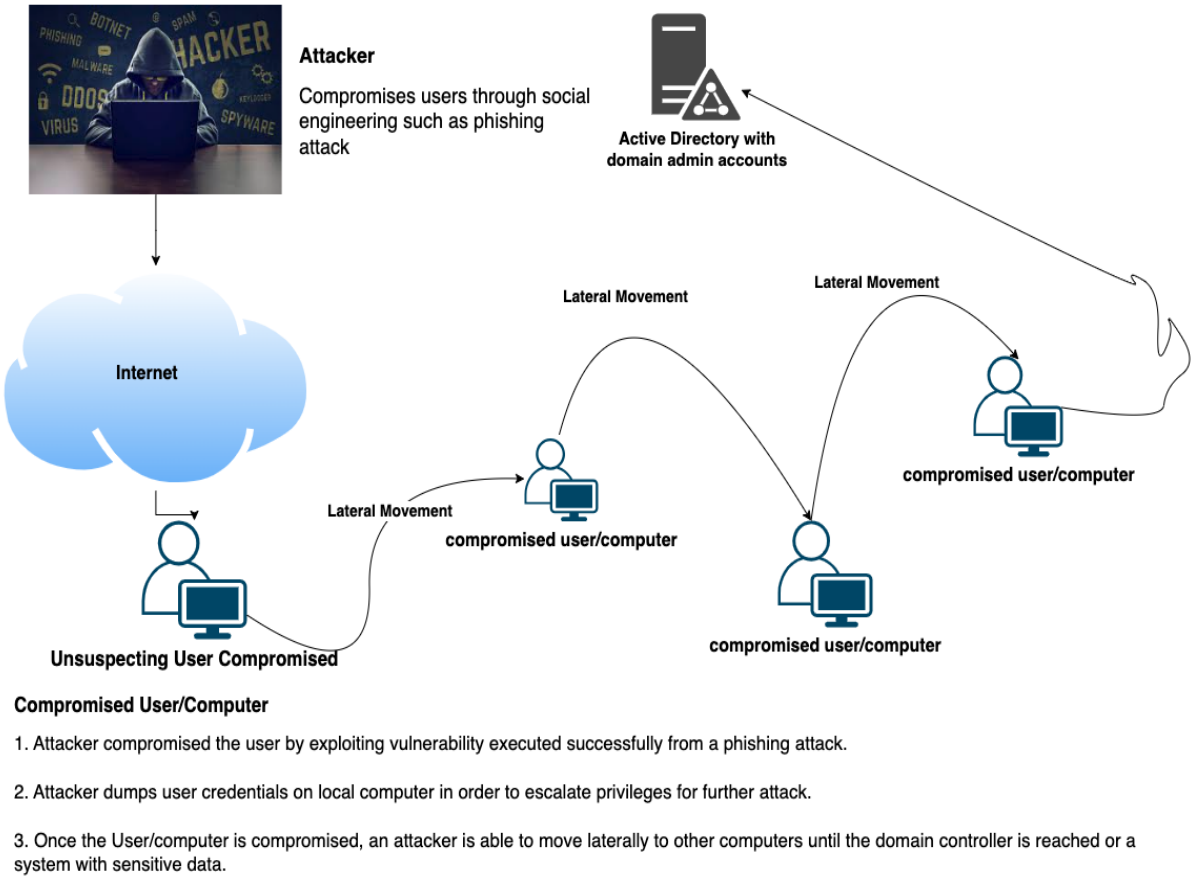


Figure 2-2: Typical lateral movements in APT (Adapted from:Soria-Machado *et al. (*2017)

The literature highlights the sophisticated nature of APT attacks and their ability to remain undetected within networks for extended periods of time. APTs are designed to bypass traditional security measures using well-organised and advanced techniques, making detection challenging (Ahmed *et al.*, 2021). A common method for lateral movement is credential dumping, which allows attackers to access multiple systems using stolen credentials (Ussath *et al.*, 2016). The initiation of APT attacks often involves social engineering to gain access (Bullée *et al.*, 2018). Distinguishing between legitimate and malicious uses of credentials is difficult and requires advanced detection techniques (Soria-Machado *et al.*, 2017). The frameworks and methodologies discussed in the literature aim to address these challenges by improving detection capabilities, situational awareness, and automating the threat response. The objective of examining these frameworks is to understand their effectiveness in detecting and mitigating APT attacks, particularly during the lateral movement phase. This understanding will inform the development and implementation of more robust security measures to protect organisational networks from sophisticated cyber threats.

2.2.4. Attack detection framework and models

Effective detection and prevention of APTs and LM attacks require a continuously updated knowledge base that can be used by detection systems. Analysts employ various frameworks and knowledge bases to determine and analyse the TTPs employed by adversaries, as well as how these techniques correlate and combine to launch effective attacks against the physical and logical infrastructure of individuals or organisations. This section introduces the MITRE, cyber kill chain, Mandiant APT lifecycle and Diamond models.

2.2.1.2 MITRE ATT&CK tactics, techniques, and procedures

The MITRE ATT&CK framework, which represents adversarial tactics, techniques, and common knowledge, was first published in 2013, and is currently the most widely used and respected framework (Georgiadou *et al.*, 2021; Strom *et al.*, 2020). It describes the tactics, techniques, procedures (TTP), and activities that adversaries or attackers may use during various stages of a cyberattack to achieve their goals within the environment of the targeted system (Palacin, 2021). This framework can be used to develop and assist in the construction of a unique TTP based on real-world experience and the analysis of specific adversarial capabilities and behaviours. It includes 14 distinct tactics, each of which encompasses a wide range of potential methods and variations in the methods used by an adversary (Palacin, 2021). The tactics employed by the adversary represent the goal of the actor's behaviour, whereas techniques and sub-techniques describe the actor's behaviour. In TTP, "P" refers to a procedure in which an adversary uses various techniques. The framework comprises fourteen tactics, including reconnaissance, resource development, initial access, execution, persistence, privileged execution, defence evasion, access to credentials, discovery, LM, collection, command and control, exfiltration, and impact. Detailed descriptions of each tactic are provided in Figure 2-2 and Table 2-1. As a result, these tactics are based on a number of techniques ranging from seven to 39 (Kinnunen, 2022; Roy *et al.*, 2023).

Table 2-1: 14 Tactics in the enterprise ATT&CK (Roy *et al.*, 2023)

Tactic	Attacker(s) objective
1. **Reconnaissance**	Gather information that they can use to plan future operations
2. Resource development	Establish resources that they can use to support operations
3. Initial access	Get in the network
4. Execution	Run malicious code
5. Persistence	Maintain their foothold
6. Privilege escalation	Gain higher-level permissions
7. Defence evasion	Avoid being detected
8. Credential access	Steal account names and passwords
9. Discovery	Figure out the victims' environment
10. Lateral movement	Move through your environment
11. Collection	Gather data of interest to their goal.
12. Command and control	Communicate with compromised systems to control them
13. Exfiltration	Steal data
14. Impact	Manipulate, interrupt, or destroy your systems and data

TTPs are used because they can describe the methods and profiles of specific attackers (Kinnunen, 2022; Kryukov *et al.*, 2022; Roy *et al.*, 2023). Tactics are descriptions that form part of the attack lifecycle and detail how adversaries conduct their activities. They represent the "why" of a technique, explaining the reasoning behind an action and its main tactical objective. The ATT&CK matrix consists of 14 tactics with their applicable techniques, however, with the focus on lateral movement attacks. Figure 2.3, highlighted in red, shows the nine techniques used to perform lateral movement attacks by APTs, some of which were used as part of this study.

	Credential Access (17 techniques)	Discovery (32 techniques)	Lateral Movement (9 techniques)	Collection (17 techniques)
1	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services	dversary-in-the-Middle (3)
2	Brute Force (4)	Application Window Discovery	Internal Spearphishing	rchive Collected Data (3)
3	Credentials from Password Stores (6)	Browser Information Discovery	Lateral Tool Transfer	udio Capture
4	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	utomated Collection
5	Forced Authentication	Cloud Service Dashboard	Remote Services (8)	rowser Session Hijacking
6	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	lipboard Data
7	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	ata from Cloud Storage
8	Modify Authentication Process (9)	Container and Resource Discovery	Taint Shared Content	ata from Configuration Repository (2)
9	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (4)	ata from Information Repositories (3)
10	Multi-Factor Authentication Request Generation	Device Driver Discovery		Data from Local System
11		Domain Trust Discovery		Data from Network Shared Drive

Figure 2-3: MITRE ATT&CK and TTPs (Adapted from: Mitre, (2024))

These techniques describe how an APT employs tactics to achieve its goals. For example, an APT employing a lateral movement tactic uses logon scripts, pass-the-hash, and remote file copy techniques, thereby providing a middle ground between the tactics and specific details of the procedures used by adversaries. The procedures describe how adversaries employ a technique to implement this tactic.

2.2.1.3 Cyber kill chain model

APT often infiltrate the infrastructure, conduct operations, and then elude detection according to the MITRE ATT&CK and cyber kill chain frameworks. However, the main distinction between the two frameworks is that the cyber kill chain primarily provides an order of operations for an adversarial attack, without any further details on how to conduct such an attack (Georgiadou *et al.*, 2021). In contrast, MITRE ATT&CK specifies several techniques that an adversary may use to accomplish their objectives (Sica *et al.*, 2023). Tables 2-2 show how the seven phases of the cyber kill chain framework are loosely connected to the 14 tactics of the MITRE framework.

Table 2-2: Cyber kill chain phases (Muckin *et al.*, 2019)

Phases	Cyber kill chain	Description	MITRE ATT&CK
1	**Reconnaissance**	This phase involves conducting research on the target.	**Reconnaissance**
2	**Weaponization**	In this phase, the attacker prepares to attack the vectors and payloads to execute against the identified victim.	**Resource development**

Phases	Cyber kill chain	Description	MITRE ATT&CK
3	**Delivery**	The attack vectors and payloads are then delivered to the identified victim or environment.	**Initial access**
4	**Exploitation**	Exploits the vulnerabilities that are the target of applications or the operating system against the victim. Exploitation can also involve social engineering to directly target a user.	**Execution**
5	**Installation**	The attacker installs malicious payloads, such as a remote access trojan or backdoor, on the victim's system, which allows the attacker to maintain his foothold in the environment even if the compromised system is rebooted as part of the remediation.	**Persistence**
6	**Command and control**	An outbound connection is initiated to a Command & Control (C2) server. The connection allows the attacker to gain direct remote access to the compromised victim system.	**Privilege execution** **Defence evasion** **Credential access** **Discovery** **Lateral movement** **Collection** **Command and control**
7	**Action on objectives**	The attacker then takes action to achieve the original goal, resulting in exfiltration of data.	**Exfiltration** **impact**

In order to carry out a successful cyberattack, an adversary must navigate through seven distinct phases in the cyber kill chain. Successfully completing these stages allows system administrators and blue teams, which are responsible for conducting operational network vulnerability evaluations and providing mitigation techniques to customers who require an independent technical review of their network security posture, to gain a better understanding of the adversary's actions (Sehgal & Thymianis, 2023). This is achieved by establishing an intelligence feedback loop that enables defenders to understand the adversary's actions at specific stages in the cyber kill chain and take action to mitigate the chances of future intrusion success. The seven stages in the cyber-kill chain are reconnaissance, weaponisation, delivery, exploitation, installation, command and control, and actions on objectives (Ahmed *et al.*, 2021).

2.2.1.4 The Mandiant APT attack lifecycle model

APT attackers operate and move laterally throughout the network for data exfiltration according to the threat lifecycle described by Mcwhorter (2014) from Mandiant. It offers distinct examples of the actions and tools that APTs use when attacking a threat hunting target. Figure 2-4 shows the representation of this model. The Mandiant model begins with the initial compromise, which typically involves the victim clicking on a link or attachment in a spear-phishing email that contains malicious code (Mandiant, 2017). This allows the adversary to further attack through the execution of the malicious code that is distributed using a malicious link on the system.

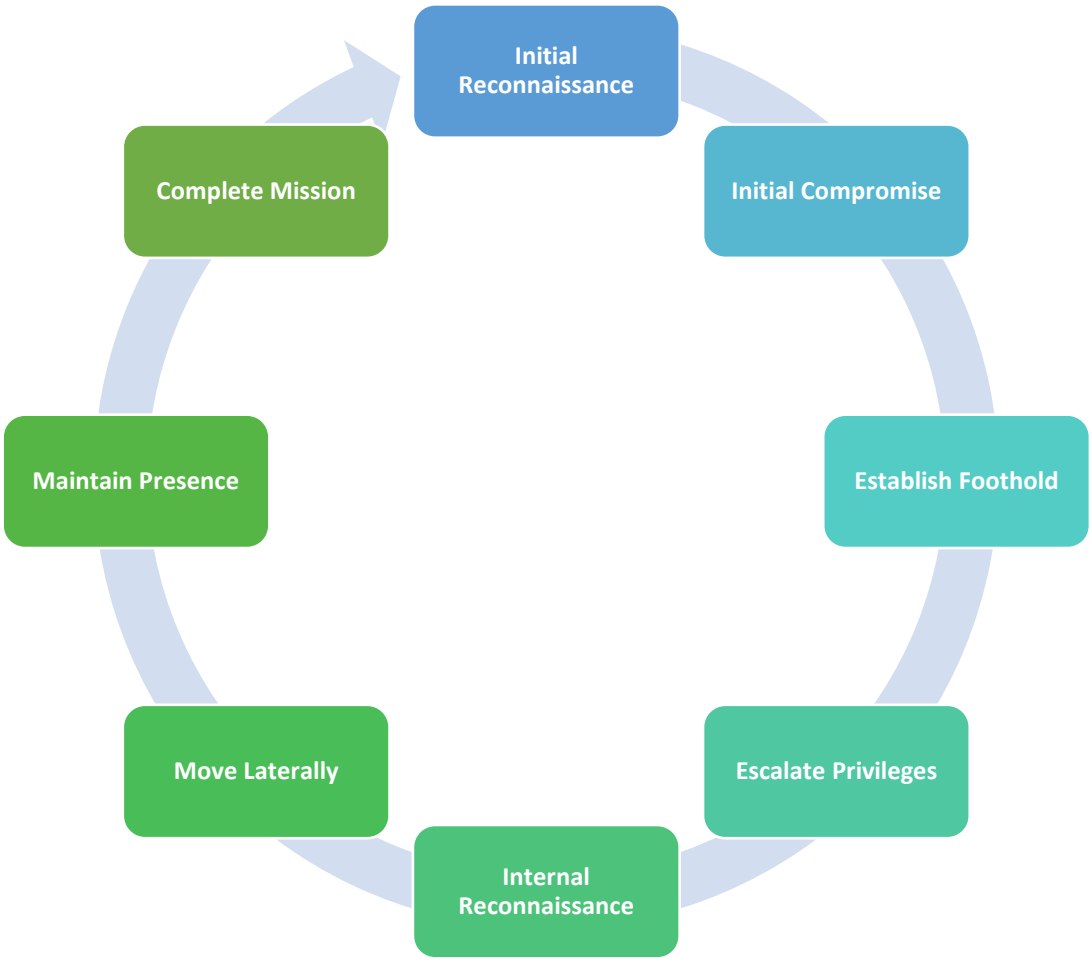


Figure 2-4: Mandiant's lifecycle of advanced persistent threats (Adapted from: Mireles *et al.* (2016))

As shown in Figure 2-4, Mandiant's threat lifecycle outlines the progression from initial compromise through lateral movement to data exfiltration (McWhorter, 2014). This approach contrasts with the Lockheed Martin cyber kill chain framework, which delineates these activities into separate phases: reconnaissance, weaponization, delivery,

exploitation, installation, command and control, and actions on objectives (Hutchins *et al.*, 2011). In Mandiant's model, following the initial compromise, attackers establish a foothold by installing persistent backdoors or downloading additional utilities to maintain control over compromised systems. Subsequent phases include privilege escalation, where attackers obtain elevated access rights, often using tools like Mimikatz to dump credentials. Internal reconnaissance follows, with attackers surveying the target environment using native system utilities to minimize detection. Finally, in the lateral movement phase, attackers leverage legitimate credentials to access additional systems and execute commands remotely using trusted tools such as PowerShell and PsExec (Sadayappan *et al.*, 2024). This lifecycle model emphasizes the importance of understanding attacker behavior at each stage to implement effective detection and response strategies.

2.2.1.5 Diamond model

The adversary, capabilities, infrastructure, and victim vectors are the four most important parts of a threat intelligence study, and are the focus of the diamond model (Ximenes & Mello, 2022). This approach is characterised in the simplest terms as an adversary installing a capability using various attack techniques against a victim. The "adversary" is the group or person who is responsible for an attack by using a "capability" against the "victim". The tools, techniques, and strategies used by an adversary during an attack comprise a capability vector. The infrastructure component of this model encompasses both the logical and physical infrastructures utilised by the adversary to deliver their capability. It can include elements such as networks, IP addresses, domain names, emails, and websites. The victim is the entity or individual that is targeted by the adversary, whether it is an organisation or a person. Finally, an intrusion event can be characterised by the methods and techniques used by the adversary to exploit vulnerabilities in the target over the infrastructure, as shown in Figure 2-5.

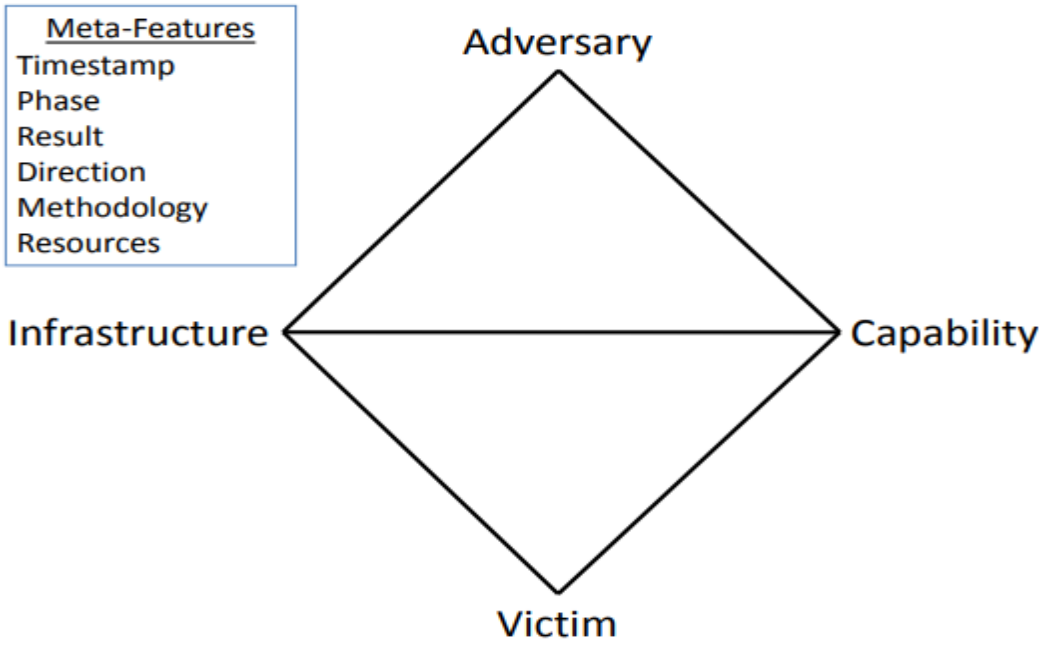


Figure 2-5: The Diamond model framework (Adapted from: Caltagirone *et al.*(2020))

The meta-features shown in the model in Figure 2-5 include timestamp, phase, result, direction, methodology, and resources. These features provide a detailed context for each event and allow for a more nuanced understanding of an adversary's actions and strategies. By examining these connections and features, defenders can gain insight into how adversaries operate, predict future actions, and develop more effective defence strategies (Caltagirone *et al.*, 2020). While there are similarities between the Diamond model and the kill chain framework, this model maps the relationships between the four fundamental aspects of an event rather than representing the TTPs used by adversaries, as does the MITRE ATT&CK framework. Researchers and analysts can use this model to construct and understand the concrete connections between the four vectors and the ways in which these connections influence or are constrained by each other. Analysts' understanding of an adversary's goals and techniques can be improved using this procedure.

2.2.5. APT attacks summary

Cyberattacks, known as APTs, allow attackers to remain hidden in the network of a target organisation for a long period of time. An APT attack uses a methodical kill chain to achieve its objective. To limit the damage that APTs can cause, it is necessary to quickly

detect them. The preceding sections discussed the framework and model. Each model and framework discussed provides unique insights and approaches for addressing cyber threats, and understanding their interactions and applications is crucial for building a robust detection strategy. The MITRE ATT&CK framework provides a comprehensive description of APT TTPs. It categorises the actions of APTs into 14 distinct tactics, ranging from reconnaissance to impact, and maps them to specific techniques. This detailed breakdown helps organisations understand how APTs operate and what methods they might use, making it a powerful tool for improving detection and response capabilities.

The cyber kill chain model outlines the stages APT goes through during an attack, including reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objectives. Although it provides an ordered sequence of events, it lacks the detailed procedural insights offered by MITRE ATT&CK. However, it is useful to understand the general flow of an attack and identify the points of intervention. The Mandiant APT attack lifecycle model provides a detailed look at how APTs conduct their operations, starting from the initial compromise, through privilege escalation and internal reconnaissance, to lateral movement and data exfiltration. It combines several stages into broader phases and emphasises the tools and methods used by attackers. This model is particularly useful for hunting threats and for understanding the progression of APT within a network.

The Diamond model focuses on the relationships between the four core components of a cyberattack which are adversary, capability, infrastructure, and victim. It emphasises understanding these relationships and how they influence each other, thus providing a holistic view of an attack. The Diamond model helps analysts construct and interpret connections between different aspects of an intrusion event, enhancing situational awareness and strategic defence planning. These models and frameworks interact and complement each other in various ways. For example, the MITRE ATT&CK and cyber kill chain models provide detailed techniques for each tactic, whereas the cyber kill chain offers a high-level sequence of attack stages. Together, they offer both granular details and a broad overview, making them powerful tools when used in conjunction. The detailed lifecycle stages of the Mandiant model can be mapped to the tactics and techniques in MITRE ATT&CK, providing a comprehensive understanding of both the methods and sequence of an APTs attack. The Diamond model's focus on relationships and meta-

features provides context that enhances the understanding derived from other frameworks. Analysts can gain deeper insights into the attack patterns described by other models by mapping the adversary's infrastructure, capabilities, and interactions with the victim.

Combining these models provides a multifaceted approach for the detection of attacks, such as lateral movement. The MITRE ATT&CK framework offers detailed insights into specific techniques, and the cyber kill chain outlines the sequence of an attack, while the Mandiant model provides detailed lifecycle stages. The Diamond model highlights the relationships among the key components of an attack. This integrated approach helps build a robust defence strategy, allowing organisations to predict, detect, and respond to APTs more effectively. By leveraging the strengths of each model, defenders can gain a comprehensive understanding of adversarial behaviour and develop more effective countermeasures.

2.3. Related studies on threat hunting methodologies for lateral movement detection

Recent research has increasingly focused on enhancing the detection of lateral movement attacks due to their role in the lifecycle of Advanced Persistent Threats (APTs). Various methodologies have been proposed, ranging from graph-based models to behavioral analysis and machine learning. For instance, Chen *et al.* (2019) presented a graph-theoretic model to increase the cost of lateral movement across enterprise networks by capturing user-machine-application interactions and hardening weak nodes. Similarly, Kushwaha *et al.* (2022) introduced a lightweight method that uses user behavioral analytics and machine learning to detect lateral movement with high precision.

A separate approach by Bai *et al.* (2020) explored the use of supervised machine learning on Remote Desktop Protocol (RDP) logs to classify lateral movement sessions. This approach, focusing on Windows event logs, highlighted the potential of host-level telemetry for effective threat detection. In a more recent development, Zhou *et al.* (2024) proposed LMDetect, a time-aware subgraph classification framework for analysing authentication logs. Their model demonstrated superior detection rates by leveraging both temporal and topological features from log data.

These studies validate the importance of adopting diverse and adaptive methodologies in lateral movement detection and support the rationale behind this research's simulation-based, hypothesis-driven approach. By comparing the performance of the TaHiTI methodology with the insights from these models, this study contributes a practical, intelligence-integrated perspective to the expanding field of proactive threat detection.

2.4. Summary of literature review and gap justification

To confirm the relevance and originality of this study, a structured literature scan was undertaken to determine the extent of academic research on threat hunting methodologies particularly those focused on lateral movement detection and the evaluation of frameworks such as TaHiTI. The review involved a search of academic databases including Google Scholar, IEEE Xplore, Scopus, and SpringerLink. The keywords used included "threat hunting", "hypothesis-driven detection", "TaHiTI methodology", "lateral movement detection", "MITRE ATT&CK threat hunting", and combinations thereof. The initial search yielded approximately 140 results. However, after applying filters to exclude duplicates, non-peer-reviewed articles, general threat intelligence papers, and studies not focused on detection methodologies, fewer than 15 relevant studies remained. Among these, the majority either discussed threat hunting conceptually or focused on specific tooling (e.g., SIEM or EDR), with limited empirical or framework-based evaluation.

For example, Al-Sada *et al.* (2024) conducted a comprehensive analysis of the MITRE ATT&CK framework, extracting and representing statistical insights to provide recommendations for improving security aspects across various digital infrastructures, including enterprise, industrial control systems, and mobile platforms. Their work emphasizes the importance of leveraging ATT&CK's structured knowledge base for threat characterization and risk assessment. Similarly, Mansour (2024) explored the integration of the MITRE ATT&CK framework within public sector organizations, using the SolarWinds compromise as a case study. The research assessed the organization's preparedness against cyberattacks by leveraging specific techniques from the ATT&CK framework, demonstrating how entities can strengthen their security posture through practical application of the framework.

This scarcity of structured, peer-reviewed evaluations highlights a critical gap that this study aims to address. By implementing and testing the TaHiTI methodology in a controlled simulation environment, this research contributes novel empirical findings to an area that has previously been dominated by theoretical discussion and operational guidance. The findings from this study therefore offer academic and practical insights into how hypothesis-driven threat hunting can enhance the detection of lateral movement in organisational networks.

2.5. Chapter summary

APTs are attacks that allow an adversary to gain unauthorised access to an organisation's network environment over an extended period without notice. This chapter provides a comprehensive overview of APTs, including their defining characteristics, various phases of APT attacks, and the attack techniques employed by APTs in the context of lateral movement attacks. Lateral movement represents a crucial stage within the life cycle of APT and encompasses five distinct phases. Additionally, models and frameworks such as the cyber kill chain and MITRE ATT&CK have been extensively examined in the context of threat hunting. The Diamond and Mandiant APT attack lifecycle models are also discussed for their unique perspectives on understanding and mitigating APTs. These models and frameworks collectively offer a multifaceted approach to detect and respond to APTs, highlighting the importance of a robust detection strategy. The following chapter delves into threat hunting, a proactive measure that can be used to detect and identify attacks from lateral movements.

Chapter 3 Threat hunting

3.1. Introduction

Threat hunting is a proactive cybersecurity measure that involves actively searching for signs of malicious activity within an organisation's network. Unlike traditional security measures, which primarily focus on defending against known threats, threat hunting seeks to identify and mitigate threats that have evaded existing security controls (Kulkarni *et al.*, 2023). This approach not only helps in detecting advanced persistent threats (APTs) but also improves the overall security posture by identifying vulnerabilities and potential attack vectors before they can be exploited (Ajmal *et al.*, 2021; Bienzobas & Sánchez-Macián, 2023). The primary goal is to reduce the dwell time, which is the period between an adversary gaining access to an environment and its detection, thereby minimising the potential damage caused by undetected threats (Fatemi, 2019; Kumari *et al.*, 2021). Building on the discussion of APTs in Chapter 2, this chapter focuses on the specific role of threat hunting in detecting lateral movement (LM) within APT attacks. Lateral movement is a critical phase in the life cycle of an APT attack, allowing adversaries to traverse the network, access high-value targets, and maintain persistence (Dong *et al.*, 2021).

In threat hunting, lateral movement refers to the techniques used by adversaries to move from a compromised host to other hosts within a network. This phase involves behaviours, such as unusual log-in patterns, unauthorised access attempts, and the use of legitimate credentials in abnormal contexts (Soria-Machado *et al.*, 2017). By focusing on lateral movement, threat hunters can uncover hidden threats that have bypassed traditional security measures, allowing a faster response to potential breaches (Os *et al.*, 2018). This chapter explores various threat hunting techniques and their application in detecting lateral movement within APT attacks, providing a detailed examination of methodologies that enhance detection capabilities and reduce adversary dwell time.

3.2. Threat hunting background

Threat hunting is a proactive and ongoing tactic used to identify and analyse unnoticed cybersecurity threats that may be present and hidden in networks (Fatemi, 2019; Palacin,

2021). These threats pose a risk to the system and the broader infrastructure if not detected. Typically initiated by APTs who have managed to bypass traditional security measures such as intrusion detection systems (IDSs), intrusion prevention systems (IPSs), antimalware software, and firewalls, these threats can remain undetected for months or years if security controls are insufficient (Araujo *et al.*, 2021). The primary objective of threat hunting is to minimise dwell time, which is the period between when an adversary gains access to an organisation's network and when it is detected (Lee & Lee, 2018).

According to a threat hunting survey by the SANS Institute, as cited by Lee & Lee (2018), dwell time can vary significantly, ranging from a few minutes to several weeks. On average, dwell time is over 90 days, a noticeable decrease from 2013, with improved incident response identified as a crucial factor in this reduction. Introducing new mechanisms or improving existing ones can help identify attackers faster and reduce dwell time. Critical moments during an attack include when an adversary enters the network, is detected through threat hunting, and an incident response operation is performed to recover the network (Os *et al.*, 2018).

Adversaries continuously adapt to new, faster, and more advanced detection methods, developing infiltration and evasion skills to remain undetected. When adversaries bypass the defensive barriers of an organisation, most organisations lack the skills, detection methods, tools, and personnel to prevent APTs from taking control of their network infrastructure (Ponemon, 2019). Therefore, threat intelligence and hunting should play a hands-on role in the organisation's defence strategy in tandem with traditional security procedures and approaches. This strategy allows threat hunters and analysts to detect and analyse the motives, Tactics, Techniques, and Procedures (TTP) that adversaries currently employ, although they should not be relied upon to completely protect the organisation's systems and infrastructure. Once an APT bypasses a standard array of defences, threat hunting plays a critical role (Yamagishi *et al.*, 2022). The hunting process involves manual and machine-assisted techniques, rather than relying solely on automated systems.

3.2.1. Types of threat hunting approaches

This section discusses the types of threat hunting used in various threat hunting approaches.

Structured hunting involves matching adversary tactics, techniques, and procedures (TTP) to attack indicators to recognise patterns of behaviour that can be used to defend against specific strategies and threat vectors employed by malicious actors. This is done to identify and neutralise threats before they can cause damage. These efforts are typically guided by a central hypothesis about a particular TTP and entity and are conducted regularly to provide ongoing assurance and protection. The goal is to produce predictable outcomes that can help uncover adversarial TTPs and support the development of effective content for behavioural threat detection (Bhardwaj *et al.*, 2022).

Unstructured hunting is typically initiated in response to a trigger, such as an indicator of compromise (IOC). Hunters may conduct research as far back as data retention and associated past offences are concerned (Araujo *et al.*, 2021). This method is predominantly data-driven and uses the least-seen principle to identify anomalies in an environment. The least-seen principle focuses on identifying unusual activities or behaviours within the network that are infrequently observed, helping to identify potential security breaches. For example, monitoring login attempts from unusual locations or at odd hours can help identify malicious activities (Ferrag *et al.*, 2020). Unstructured hunting is often performed on an ad hoc basis when time and resources are permitted, which can lead to unpredictable results and investigations that extend beyond the initial scope. However, this approach can effectively detect and identify malware, malicious tools, suspicious networks, and host-based artefacts (Bhardwaj *et al.*, 2022). For example, it may involve analysing logs and network traffic to detect activities that deviate from typical patterns (Bhardwaj *et al.*, 2022).

Entity-driven, also referred to as situational, involves developing a hypothesis derived from an internal risk assessment and a trend/vulnerability analysis, which is specific to the information technology environment of an organisation. Threat hunters can identify entity-oriented leads by examining crowd-sourced attack data and identifying the latest techniques and current cyber threats. They can also search for specific behaviours within the environment (Araujo *et al.*, 2021). It is beneficial for cyber defence analysts to have a thorough understanding of internal risks and critical assets, as well as a long tenure within

the organisation. This can be achieved by maintaining stable teams in the environment for extended periods. An example of this type of hunting might include focusing on high-value targets within an organisation and monitoring for any signs of compromise or unusual activity specific to those assets.

By employing these various types of threat hunting approaches, organisations can improve their ability to detect and mitigate potential threats. Each method offers unique advantages and can be selected based on the specific needs and risk profile of the organisation.

3.3. Threat hunting methodologies and procedures

The threat hunting process involves using multiple parameters and datasets to analyse potential threats, which may yield varying results. There are several approaches to threat hunting, the most prevalent being hypothesis-driven, indicator of compromise (IOC)-based, advanced analytics, and machine-learning methods (Araujo *et al.*, 2021; Taschler, 2023).

The **hypothesis-driven** investigation methodology uses analyses of data collected on novel attacks to determine whether a particular or similar attack has occurred within the environment being investigated. This approach aims to provide threat hunters with updates on attacks and their behaviours, as well as the attacker's unique tactics and approaches for specific attacks. Threat hunters and investigators can develop hypotheses based on TTPs that have been composed and distributed to the community. This hypothesis helps determine whether the same TTPs have been used within the organisation's infrastructure, allowing for a focused and effective investigation based on the known behaviours of active adversaries (Taschler, 2023).

IOC-based investigations are based on indicators of compromise (IOC), which are pieces of forensic evidence indicating that a system may have been breached. These investigations often start with internal threat intelligence data and information collected and analysed by the organisation itself. Threat hunters use these internal data to identify new and emerging threats, utilising IOCs and indicators of attack (IOAs) to uncover hidden malicious activities. IOAs focus on detecting the behaviour and techniques of attackers rather than just the artefacts left behind. Although community research and

announcements of new threats can also initiate a threat hunt, the focus is on using internally gathered intelligence to guide the investigation (Taschler, 2023). It is important to clarify that "community-based research" includes contributions from researchers and practitioners both inside and outside the organisation. Therefore, community sources are not only external; they encompass a collaborative network of experts who contribute to a shared understanding of threat landscapes.

Machine learning and data analysis methodologies filter large amounts of data to identify abnormalities that may signal malicious activity. By analysing data from past events, machine-learning algorithms can help predict the sequence of new threat events based on connections between different parameters and generate trained models for threat prediction. Although threat prediction is not the primary focus of this study, it enhances threat hunting by providing insights that guide the identification of potential lateral movement activities. Integrating this approach with endpoint and server event logs can create a threat-hunting system that uses machine-learning techniques (Berady *et al.*, 2021).

A notable conceptualisation of threat hunting is the hunting loop introduced by Sqrrl (2018). This loop comprises four iterative steps, illustrated in Figure 3-1, that create a continuous cycle in which hunters aim to pursue their objectives efficiently (Hemberg *et al.*, 2024).

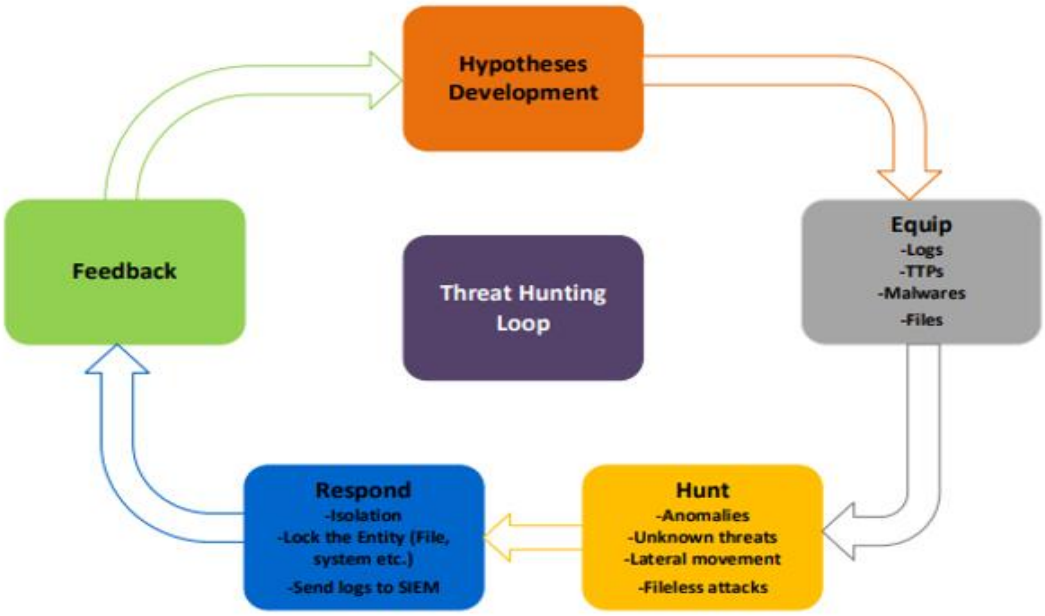


Figure 3-1: Threat hunting loop (Adapted from: Sqrrl, (2018))

The hunting loop has five primary steps (Sqrrl, 2018).

i. Hypothesis development: This process involves formulating a hypothesis regarding potential dangers rooted in a variety of variables, including intelligence briefings, past occurrences, or even intuitive feelings.
ii. Equip: Explore a hypothesis that incorporates tools and techniques, potentially involving data collection, query execution, or visualisation tool use.
iii. Hunt: Identify TTP patterns that support this hypothesis.
iv. Respond: Use advanced analytics to further investigate the hypothesis and identify additional threats.
v. Feedback: Incorporate findings to refine and improve future hunts.

The Hunting Maturity Model (HMM), also introduced by Sqrrl (2018), categorises an organisation's proactive detection capabilities into five levels, ranging from HM0 to HM4, as shown in Figure 3-2.

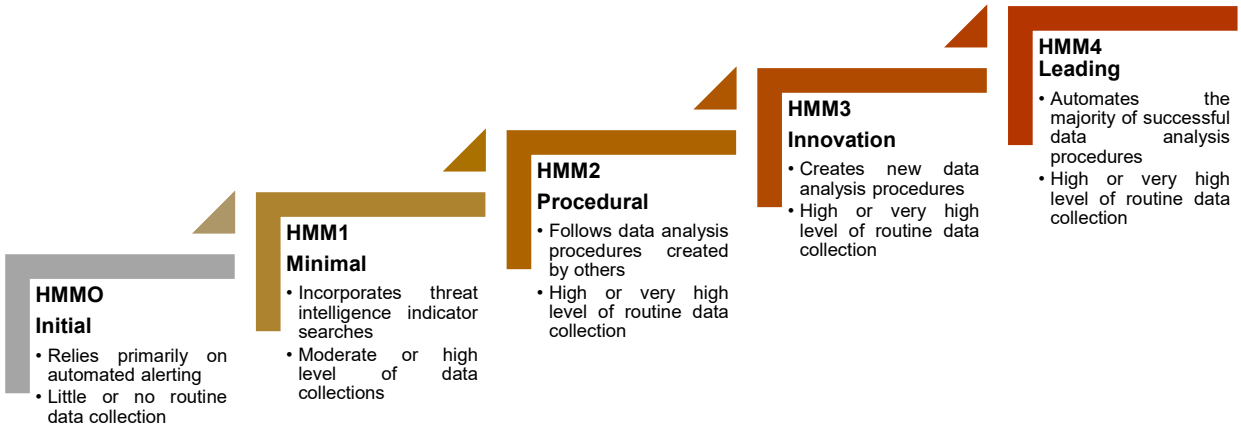


Figure 3-2: Hunting maturity model (Adapted from: Sqrrl (2018))

The Hunting Maturity Model (HMM), introduced by Sqrrl (2018), categorises an organisation's detection maturity from HM0 to HM4. The HMM supports the hunting loop by providing a framework for evaluating and improving an organisation's threat-hunting capabilities. Identifying the level of hunting maturity depends on the quality and quantity of the data collected from the IT environment. The greater the volume and variety of data provided to the analyst, the more accurate the results and the more effective the threat hunter. With the right toolset, including visualisations and analytics, one can determine how to conduct hunts and hunting techniques (Nour *et al.*, 2023).

Integrating the hunting loop and the HMM ensures a structured approach to threat hunting. The iterative nature of the hunting loop, combined with the evaluative framework of the HMM, ensures a continuous improvement in threat detection and response capabilities. This integration allows organisations to establish a robust procedure for conducting threat hunting, which will be detailed further in the experimental chapter. Here is a detailed procedure of how these two frameworks support each other.

i. Hypothesis development (hunting loop) and initial maturity assessment (HMM): Begin by developing a hypothesis about potential threats based on intelligence briefings, past incidents, or expert intuition. At the same time, assess the organisation's current threat hunting maturity level (HM0 to HM4) using the HMM.
ii. Equip (hunting loop) and data collection (HMM): Equip threat hunters with the necessary tools and techniques, including data collection and visualisation tools. At this stage, focus on improving data collection practices to enhance the quality and quantity of data, which directly influences the organisation's maturity level.
iii. Hunt (hunting loop) and procedural development (HMM): Conduct the hunt by identifying TTP patterns that support the hypothesis. Develop and refine procedures based on findings, which helps the organisation move from minimal to procedural maturity.
iv. Respond (hunting loop) and innovation (HMM): Use advanced analytics to further investigate and identify additional threats. Innovate and integrate new tools and techniques to enhance the threat detection and response capabilities.
v. Feedback (hunting loop) and continuous improvement (HMM): Incorporate the findings of the hunt to refine future hypotheses and improve hunting techniques. This feedback loop ensures continuous improvement and helps the organisation to progress to higher maturity levels.

By following this integrated approach, organisations can systematically improve their threat-hunting capabilities, using both the hunting loop and the HMM to establish a robust and iterative process for identifying and mitigating threats.

3.4. Threat hunting data

The success of threat hunting is greatly influenced by the amount and quality of data collected (Fatemi & Ghorbani, 2020). The data collected during threat hunting is usually

in the form of log data, which provides detailed records of activities and events within a network or system. These logs are crucial for identifying and analysing malicious behaviour and patterns. Table 3-1 provides a classification of the various types of event log data collected from endpoint computer systems and servers.

Table 3-1: Types of logs

Type of logs	Brief description
Windows event log	Generates an event log when a hardware or software component is accessed on a Windows operating system (Yamagishi *et al.*, 2022).
Application logs	Created when an event occurs within an application; used by coders to track and understand application behaviour (Fatemi & Ghorbani, 2020).
Directory service logs	Produced by computers configured to respond to security authentication requests in the Windows Server domain (Fatemi & Ghorbani, 2020).
Windows active directory logs	Track changes in user privileges, authentication operations, requests, and other activities (Fatemi & Ghorbani, 2020).
DNS logs	Record activities on a server that matches web addresses to hostnames on the Internet (Boyagane, 2020).
File replication service logs	Record activities on file replications on computers, available only to domain controllers (Sarhan et al., 2021).
Security logs	Record the security events that occur on a computer, including failed logins, password changes, and failed authentication attempts (Boyagane, 2020).
System logs	Record events such as driver errors, sign-ins, and sign-outs when the operating system starts up (Boyagane, 2020).

Network components such as routers, switches, and firewalls create various types of data, and each component maintains a log of its own. As a result, multiple logs are available, such as event logs, which capture information about network usage and traffic. This information includes data on login attempts and events related to the applications. Availability logs record information regarding a system's performance, uptime, and availability (Boyagane, 2020). Server logs document activities that occur on a specific server during a certain period, whereas system logs, also known as syslogs, track data related to the operating system (Das *et al.*, 2020).

Threat logs store information corresponding to a specific security profile within a firewall. Flow data logs record traffic flows at network interfaces when traffic enters or exits, and network traffic is used for such data (Sarhan *et al.*, 2021). Authorisation and access logs

provide information on users and bots that access a certain program or file, whereas change logs compile a list of modifications to a program or file. Finally, resource logs provide information regarding connectivity problems and capacity limits.

In this study, these types of logs are classified as operating system, event, and network logs. Operating system logs include logs generated by the operating system, such as Windows event logs and syslogs. Event logs encompass logs that record specific events within applications and systems, including application and security logs. Network logs cover logs related to network activity and traffic, including DNS and flow data logs. Management of endpoint logs, including security records, is crucial to ensure that records are stored for an appropriate period, according to the needs of the organisation (Boyagane, 2020; Das *et al.*, 2020). A log file records various occurrences in the system, including transactions, errors, and intrusions (Mavroeidis & Josang, 2018).

The Windows event log, found on a Windows operating system (OS), generates an event log when a hardware or software component is accessed. Windows categorises events into six distinct categories: application logs, security logs, setup logs, system logs, forwarded events, and directory service logs (Microsoft, 2021). Application logs are generated to help coders track and comprehend the application's behaviour during development and prior to its release. Directory service logs are produced using a computer configured to respond to security authentication requests in the Windows server domain. These logs track changes in user privileges, authentication operations, requests, and other activities and are known as active directory logs (Fatemi & Ghorbani, 2020).

3.5. Indicators of compromise (IOC)

Threat hunters often need to collect data on potential indicators of compromise (IOC) to determine whether there are malicious activities within organisational information systems. These IOCs serve as a trail of clues left behind by adversaries, allowing hunters to determine whether a malicious attack occurred early in the process or if it is still ongoing (Haber & Rolls, 2020). Some IOCs, which can range from simple metadata to complex malicious code, may even be completely ignored by an adversary during their activities. To determine the probability of a successful incident, threat hunters and analysts examine the collected and informative IOCs to gain a more complete understanding of the situation (Chen *et al.*, 2024).

Similarly, indicators of attack (IOA) are artefacts created by an attacker during an attack that can be used to determine what is currently happening. IOAs focus on the behaviours and tactics used by attackers rather than on the final outcomes. For example, an IOA could be an unusual pattern of login attempts or unexpected changes in system configuration (Bienzobas & Sánchez-Macián, 2023). To gain a near-real-time analysis of a security incident, threat hunters should use IOCs and IOAs simultaneously.

Examples of IOCs include unusual network traffic patterns, such as unexpected outbound connections or high volumes of data being sent to unfamiliar IP addresses (Haber & Rolls, 2020); unexpected file changes, such as modifications to system files or the presence of unknown files (Chen *et al.*, 2024); unauthorised login attempts, including multiple failed login attempts or logins from unusual locations (Haber & Rolls, 2020); and anomalous behaviour in system processes, such as unexpected resource usage or unauthorised application execution (Bienzobas & Sánchez-Macián, 2023). These indicators provide a foundation for threat hunters to detect and analyse potential security incidents. By leveraging IOCs and IOAs, threat hunters can develop a comprehensive understanding of an adversary's actions and improve their ability to respond effectively to threats.

In conclusion, the collection and analysis of IOCs are fundamental to threat hunting. Threat hunters can detect and mitigate potential threats more efficiently by examining various types of indicators. This approach improves the overall security posture of an organisation by providing early warnings of malicious activities and helps prevent significant breaches. The integration of IOCs and IOAs further strengthens the ability to detect both historical and active threats, making them a critical component of modern cybersecurity strategies.

3.6. Threat hunting system

Several threat hunting tools can be used during threat hunting operations. These solutions allow threat hunters to automate the detection and analysis of malicious activities, thereby making the process more efficient and effective. Using these solutions, threat hunters can continuously monitor, detect, and respond to potential threats. This study focuses on the following solutions: Security Information and Event Management (SIEM), Managed Detection and Response (MDR), Security Analytics, Intrusion

Detection Systems (IDS), and Machine Learning in Security. Although other tools are available, these are the primary solutions used in this study.

Security information and event management (SIEM) is a security solution that integrates critical sources and tools to provide directions for the search process and to detect and respond to security threats. SIEM systems collect and analyse log data from various sources within an organisation's IT environment to identify unusual patterns or incidents that suggest a security breach. By aggregating and correlating data from different sources, the SIEM can provide comprehensive network searches and real-time analysis of security events (Palacin, 2021). Security analysts can leverage the SIEM to conduct comprehensive network searches, which helps ensure that the indicators for both attacks and compromises provide clear guidance for tracking threats. To optimise the use of SIEM and manage MDR tools, it is essential that the security environment incorporates as many essential resources and utilities as possible (Palacin, 2021).

Managed detection and response (MDR) is an automated security solution that offers continuous monitoring, threat detection, and incident response capabilities to organisations. Providers of MDR use SIEM, threat intelligence, proactive threat hunting, and incident response tools to identify and respond to security threats. These services can help improve an organisation's security posture by providing 24/7 monitoring, threat detection, and incident response capabilities, allowing organisations to detect and respond to threats more effectively (Ayyagari *et al.*, 2021).

Security analytics is a broader category that uses machine learning and artificial intelligence to analyse security data, providing a more comprehensive understanding of the security posture of an organisation compared to traditional SIEM systems. Security analytics can use data from multiple sources such as network devices and servers to identify patterns and anomalies that can indicate a security threat. Specific tools used for security analytics include Splunk, IBM QRadar, and ArcSight (Chatzilygeroudis *et al.*, 2021).

Intrusion detection systems (IDS) are designed to assist in the detection of APTs in addition to simpler types of cyberattacks. Intrusion detection is the process of monitoring events that occur on a computer system or network and analysing them for signs of possible incidents, such as violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices (Alhajjar *et al.*, 2021;

Mohan, 2015). There are three primary types of intrusion detection systems: network-based (NIDS), host-based (HIDS), and application-based (AIDS) systems. NIDS monitors network traffic, HIDS monitors host activities, and AIDS monitors application-level activities. These systems are relevant to threat hunting because they provide crucial data that can help identify malicious activities within different layers of an IT environment.

Machine learning (ML) is increasingly being used in threat hunting to analyse large amounts of data and identify abnormalities that may signal malicious activities. ML algorithms can predict the sequence of new threat events based on the connections between different parameters and generate trained models for threat prediction (Yamagishi *et al.*, 2022). Although threat prediction is not the primary focus of this study, it improves threat hunting by providing insights that guide the identification of potential lateral movement activities.

This study detects lateral movement attacks through hypothesis-driven analysis of endpoint logs using HELK and contextual interpretation based on threat intelligence, no machine learning techniques were applied. Elasticsearch is a well-known open-source enterprise-level search engine that includes machine learning features. It uses unsupervised learning to identify the characteristic anomalies (Collier & Azarmi, 2019).

Bayesian methods are used to model data where the likelihood of a hypothesis changes as new information becomes available (Berger, 2012). This method is advantageous because it requires only data on normal behaviour for training, which is easily available in large quantities on an enterprise network, making it ideal for security use cases (Ring *et al.*, 2021). Although machine learning is not a silver bullet for security purposes, it is essential to understand its limitations to obtain accurate results (Ghosh *et al.*, 2023).

Table 3-2: Summary of various threat hunting systems

Technology / Method	Description	Functionality / Approach
Security information and event management (SIEM)	A security tool that identifies unusual patterns or incidents that suggest security breaches.	Integrates critical sources and tools to provide directions for the search process, detect and respond to security threats.

Technology / Method	Description	Functionality / Approach
Managed detection and response (MDR)	A security service offering continuous monitoring, threat detection, and incident response capabilities.	Using SIEM, threat intelligence, proactive threat hunting, and incident response tools for 24/7 monitoring and threat detection.
Security analytics	A solution that uses machine learning and artificial intelligence to analyse security data.	Gather data from various sources, such as network devices and servers, to identify patterns and anomalies that indicate security threats.
Intrusion detection systems (IDS)	Systems designed to detect and alert to persistent advanced threats and other cyberattacks.	Includes network-based, host-based, and application-based systems that monitor and analyse activities for malicious activity.
Machine learning in security	A process in which computers learn without explicit programming used in security analysis.	Involves unsupervised, semi-supervised, or supervised learning to analyse data and identify patterns.
Elasticsearch machine learning	An open-source enterprise-grade search engine used for anomaly detection in endpoint logs.	Using unsupervised learning and Bayesian methods to model data and recognise periodicity in the data.

In summary, various tools and methodologies play a crucial role in enhancing threat hunting capabilities. By integrating these tools, security analysts can automate many aspects of threat detection, improve incident response times, and reduce the overall impact of cyber threats on an organisation. Each tool and method provides unique functionalities that, when used together, create a robust defense mechanism against sophisticated cyber threats.

3.7. Threat hunting methodology

Threat hunting is a proactive cybersecurity strategy designed to detect and mitigate threats that may bypass traditional security measures. This approach is becoming increasingly important because of the sophisticated nature of modern cyber threats, such as advanced persistent threats (APTs), which can remain undetected within a network for extended periods. The goal of threat hunting is to reduce dwell time, the period between

an attacker's initial compromise and their detection, thereby minimising potential damage to an organisation. Various approaches exist for threat hunting, each of which has its own strengths and weaknesses. This study focuses on the TaHiTI methodology, a targeted cyber threat hunting approach that integrates threat intelligence.

3.7.1. TaHiTI – Targeted hunting integrating threat intelligence

TaHiTI was investigated in this study because of its effectiveness and increasing adoption in the field of cybersecurity. Previous studies indicate that combining threat intelligence with threat hunting significantly improves the ability to detect APTs and other sophisticated attacks (Os *et al.*, 2018). The Dutch Payment Association developed the TaHiTI methodology to address the limitations of existing security measures and to improve proactive threat detection. The TaHiTI methodology comprises three phases: threat intelligence gathering, threat response, and threat hunting feedback. Threat-intelligence gathering involves collecting information about potential threats, including threat actors, attack vectors, and vulnerabilities. The threat response phase involves responding to identified threats such as mitigating vulnerabilities or blocking malicious traffic. The threat hunting feedback phase involves reviewing the threat-hunting process and making improvements as needed. However, this process is complex and time-consuming.

Threat intelligence gathering is the initial phase that involves gathering information about potential threats from various sources. This information includes details about threat actors, their tactics, techniques, and procedures (TTPs), attack vectors, and system vulnerabilities. Effective threat intelligence gathering is crucial to understanding the threat landscape and preparing for potential attacks (Soria-Machado *et al.*, 2017).

Threat response, at this phase organisations respond to identified threats by taking actions such as mitigating vulnerabilities, blocking malicious traffic, and implementing preventive measures. This phase is critical for minimising the impact of detected threats and preventing future incidents (Os *et al.*, 2018).

Threat hunting feedback is the final phase that involves reviewing the threat-hunting process, analysing the effectiveness of the response, and making necessary

improvements. Continuous feedback and improvement are essential to maintain an effective threat hunting program (Os *et al.*, 2018).

TaHiTI is designed to promote a common understanding of threat hunting and to integrate threat intelligence and threat hunting in an approach based on best practices. According to Os *et al.* (2018), "Threat hunting is a proactive effort to find signs of malicious activity on an organisation's IT infrastructure, both current and historical, that have eluded existing security measures." Several factors contribute to the evasion of security defences, including the use of new or unknown attack techniques, zero-day exploits, and inadequate detection technology. The TaHiTI process consists of six steps, subdivided into three phases: initiation, hunting, and finalisation. The overall process is illustrated in Figure 3-3.

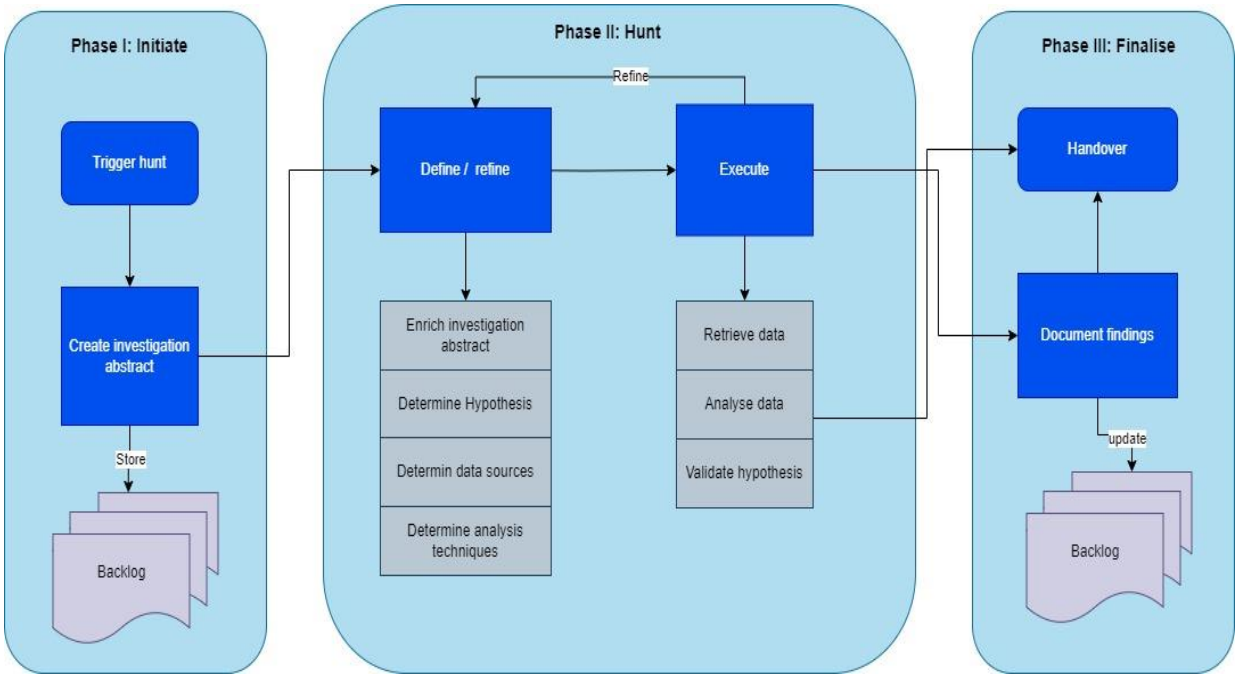


Figure 3-3 TaHiTi process (Os *et al.*, 2018)

During the initiation phase, a hunt is triggered by a preliminary action, such as an alert from a security information and event management (SIEM) system or a new threat intelligence report. This trigger is converted into an investigation summary and added to the hunting backlog. This initial phase involves the hunt trigger and other processes that initiate the threat hunting process. Processes that can potentially trigger the start of the hunt overlap strongly with those that receive investigation output. The feedback loop

contributes to the iterative threat hunting process. When executed effectively, hunting can act as a catalyst to enhance other processes (Lukova-Chuiko *et al.*, 2020).

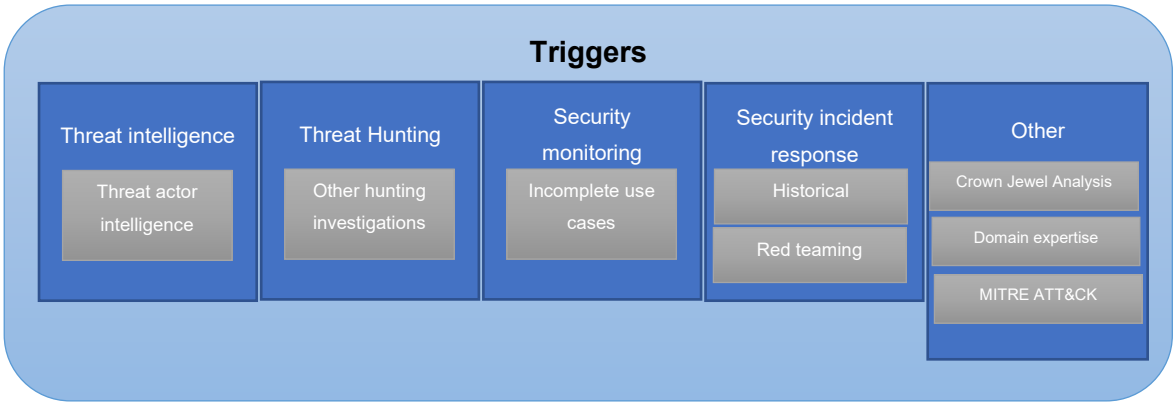


Figure 3-4: Hunting triggers (Os *et al.*, 2018)

Figure 3-4 presents the range of potential triggers that can initiate a threat hunting activity, as adapted from Os *et al*. (2018). These triggers represent key intelligence sources or events that prompt analysts to investigate possible threats. The categories include threat intelligence, which covers insights such as threat actor behaviours and indicators of compromise; ongoing or historical threat hunting investigations, which may identify recurring patterns or gaps requiring deeper analysis; and security monitoring alerts, particularly those derived from incomplete or ambiguous use cases.

Additionally, security incident response outcomes, such as learnings from red team exercises or forensic reviews of past incidents, serve as valuable hunting triggers. The final category, labelled Other, includes strategic planning artefacts like crown jewel analysis, expert domain knowledge, and structured frameworks such as the MITRE ATT&CK matrix. Together, these categories provide a comprehensive foundation for building well-informed, hypothesis-driven hunts and are integral to the initial phase of the TaHiTI methodology. When triggers are received, the hunting team embarks on an abstract investigation. In this context, an abstract investigation refers to a preliminary high-level investigation that provides a general overview of the threat, without delving into specific details. This information is later refined and updated when the hunt is chosen for execution.

The second phase, the hunting phase, involves two main steps: defining and refining the objectives, and executing the search. During the ‘define and refine’ step, the objectives of the hunt are clearly outlined and adjusted as new information comes to light or issues

arise. The scope, data sources, and analytical methods are defined during this phase. The execution step involves physically performing the search, retrieving the data, and performing the analysis (Os *et al.*, 2018).

The final phase, the finalisation phase, includes validating the hypothesis based on the data analysis results, documenting the findings, and making recommendations. Figure 3-5 depicts the various processes triggered by threat hunting investigations, such as response to security incidents, updates to security monitoring, generation and dissemination of threat intelligence, vulnerability management, and other recommendations. Step five involves careful analysis of the results of the execution phase. Documented findings should include the primary results of the search, along with any inferences derived from these results. Recommendations can include suggestions for improvements in preventive measures, such as configuration changes or architectural alterations, and suggestions for improving log keeping by incorporating additional sources and details. Additionally, recommendations can be provided for use in security monitoring and process improvements, such as strengthening vulnerabilities and managing configurations (Os *et al.*, 2018).

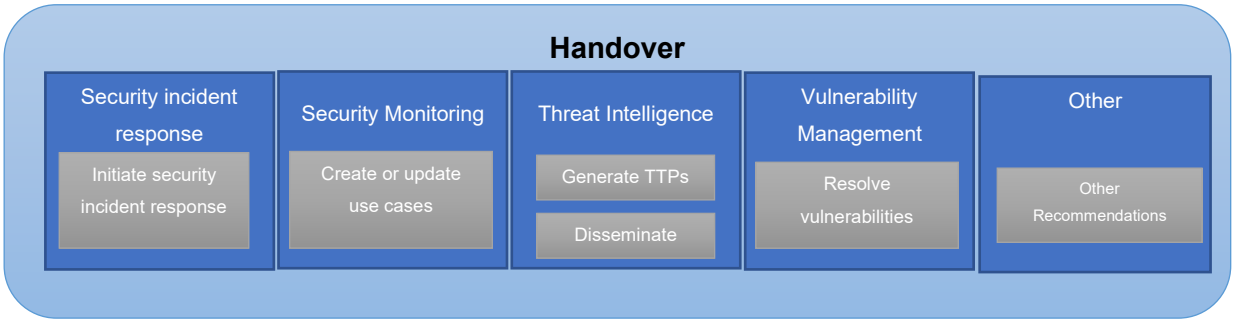


Figure 3-5: Processes triggered by threat hunting investigations (Os *et al.*, 2018)

The document should include a section dedicated to 'lessons learned', which outlines the ways in which the hunt experience has facilitated personal growth and development. Hunters have potentially acquired significant knowledge about certain aspects of infrastructure, which can be considered valuable lessons. These insights can facilitate novel hunting practices and improve the effictiveness of future hunting practices. The finalised report on the hunting investigation should be distributed to the relevant parties involved, including security operations centre managers, risk managers and chief information security officers (Os *et al.*, 2018).

Threat hunting reports contain confidential information. It is important to update the hunting backlog after the hunt is completed. The results of the hunt should be recorded in the system along with details of the hunt implementation and subsequent actions. This information may be useful in determining whether a new investigation of the same hypothesis should be conducted. The final phase involves transferring the task to subsequent procedures. Various procedures can obtain inputs from hunting enquiries, such as security incident responses, security monitoring, threat intelligence, vulnerability management, and other processes (Os *et al.*, 2018).

The TaHiTI methodology is a comprehensive and systematic approach to establish a threat hunting program within a business. This methodology emphasises the importance of incorporating threat intelligence into the process and continuously improving the program based on the results of hunting and profiling. TaHiTI has gained widespread adoption in the field of threat hunting and has proven effective in creating and implementing customised threat hunting programs that meet the specific requirements of an organisation.

In summary, TaHiTI provides a structured and comprehensive method for threat hunting that integrates threat intelligence at its core. This approach is particularly relevant for identifying and mitigating lateral movement attacks, which is the key focus of this study. The integration of threat intelligence allows for a more informed and targeted hunting process, which is crucial for detecting sophisticated threats that can evade conventional security measures. By adopting TaHiTI, this study aims to demonstrate its effectiveness in reducing dwell time, improving incident response, and improving the overall security posture.

3.8. Chapter summary

This chapter provided a comprehensive overview of threat hunting, focusing on its methodologies, procedures, data sources, and tools. Threat hunting is a proactive cybersecurity strategy designed to detect and mitigate threats that bypass the traditional security measures. The background section discussed the importance of threat hunting in minimising the dwell time and enhancing the incident response. It also detailed different types of threat hunting, including structured, unstructured, and entity-driven approaches. The section on methodologies and procedures outlined various approaches to threat

hunting, such as hypothesis-driven, IOC-based, advanced analytics, and machine-learning methods. It also emphasised the iterative nature of the hunting process, supported by frameworks such as the hunting loop and the Hunting Maturity Model (HMM).

The chapter also highlighted the significance of data in threat hunting, detailing different types of logs, such as Windows event logs, application logs, and DNS logs, which are crucial to detecting malicious activities. Indicators of compromise (IOC) were discussed, providing examples of common IOCs and their role in identifying security breaches. Various threat hunting tools, including SIEM, MDR, Security Analytics, IDS, and machine learning, were reviewed for their functionalities and contributions to effective threat detection and response. This study aimed to leverage Elasticsearch's machine-learning capabilities to detect lateral movement attacks, demonstrating the integration of advanced tools in threat hunting. Finally, the TaHiTI methodology was introduced and examined in detail. TaHiTI integrates threat intelligence into the threat hunting process, providing a structured approach that improves the detection and mitigation of sophisticated threats. The phases of the methodology, including threat intelligence gathering, threat response, and feedback, were discussed along with the specific steps involved in the hunting process.

In conclusion, this chapter established a solid foundation for understanding threat hunting and its critical role in modern cybersecurity. Integration of various tools, data sources, and methodologies, particularly the TaHiTI framework, underscores the importance of a comprehensive approach to detecting and mitigating cyber threats. This understanding will inform the development of more robust security measures in subsequent chapters, focusing on practical applications and experimental validations.

Chapter 4 Research methodology

4.1. Introduction

This chapter outlines the research methodology adopted for this study, which aimed to examine how the TaHiTI methodology can be effectively applied to detect lateral movement attacks in a controlled academic setting. The primary objective was to establish a robust and systematic approach to threat hunting, specifically focusing on lateral movement attacks associated with advanced persistent threats (APT). Building on the foundational discussions in previous chapters, this chapter delves into the research methods, approaches, and strategies used in this study. The methodology is aligned with the qualitative nature of this investigation, guided by structured observations, thematic evaluation, and contextual interpretation of threat detection outcomes. It begins with a brief overview of the relevant research methodologies, including positivism, interpretivism, and pragmatism. This study follows a qualitative research philosophy grounded in contextual inquiry and observational analysis, suitable for exploring practical implementation scenarios in threat hunting.

4.2. Research methodologies

Research methodologies provide a structured framework for investigating questions and deriving relevant knowledge. This section explores three primary research philosophies, positivism, interpretivism, and pragmatism, and discusses their relevance and application in this study.

Positivism emphasises objective reality and the use of empirical methods to discover the truth. This philosophy posits that knowledge is best obtained through observable and measurable facts, often utilising quantitative methods such as surveys and experiments to test hypotheses and establish general laws. Positivism is grounded in the belief that reality is objective and can be understood through scientific inquiry (Morgan, 2014; Saunders *et al.*, 2019). While positivism supports empirical analysis, this study applies a contextual, qualitative approach more aligned with interpretivism. It focuses on observational patterns and interpretive log analysis rather than hypothesis testing or

numerical generalisation. Thus, an interpretivist-leaning pragmatic stance is adopted to support practical insights derived from structured simulation.

In contrast, **interpretivism** focuses on the subjective nature of reality, emphasising that knowledge is socially constructed and can only be understood through the meanings and experiences of individuals. This philosophy often employs qualitative methods, such as interviews and observations, to explore the complexities of human interactions and social contexts (Creswell, 2013; Saunders *et al.*, 2019). Although interpretivism provides rich, contextual insights, it is less suited for studies that require objective measurement and analysis, such as this one.

Pragmatism serves as a middle ground between positivism and interpretivism, emphasising practical outcomes and real-world applications. Pragmatists are flexible in their methodological choices and often use a combination of qualitative and quantitative methods to address research questions. This philosophy values both objective and subjective data, focusing on the practical implications of the research findings (Creswell, 2013; Morgan, 2014). Pragmatism is particularly useful in applied research settings where the resolution of specific problems is a primary goal.

The choice of these three philosophies over others, such as critical realism, is because of their direct relevance and applicability to the nature of this study. Critical realism, which focuses on understanding the underlying mechanisms of social phenomena, is not applicable here because of the study's emphasis on observable data and practical outcomes. The selected philosophy for this study, positivism, is well suited to the quasi-experimental nature of the research, focusing on quantitative data to evaluate the effectiveness of TaHiTI in threat hunting. This choice was informed by the need for objective measurement and analysis to validate the study's findings and to contribute to a broader understanding of cybersecurity practices.

4.3. Research strategy

The research strategy for this study is rooted in a data-driven approach and a quasi-experimental method chosen for their alignment with the objectives of the study and the nature of the data. This strategy encompasses the design and execution of experiments

within a controlled environment to evaluate the effectiveness of the TaHiTI. The following sections elaborate on the key components of this research strategy.

4.3.1. Research approach

This study adopts a data-driven, qualitative approach, where structured observations and log-based evidence are analysed to evaluate detection behaviours. The analysis emphasizes behavioural indicators, attack timelines, and hypothesis validation. This approach is crucial for understanding the nuances of TaHiTI's effectiveness in identifying and mitigating such attacks. Data-driven methodologies involve collecting, analysing, and interpreting data to identify patterns, trends, and correlations. Although the environment produced measurable outputs, the primary analysis was qualitative, focusing on log narratives, event correlation, and pattern recognition. Detection artefacts were contextually assessed, rather than statistically modelled (Os *et al.*, 2018).

4.3.2. Quasi-experimental approach

A quasi-experimental design is utilised to assess the impact of TaHiTI on the detection of lateral movement attacks. Unlike true experiments, quasi-experiments do not require random assignments, making them suitable for studies where controlled random sampling is impractical. This design allows for the manipulation of independent variables and observation of their effects on dependent variables in a controlled setting (Rodriguez & Rodriguez, 2019). In this study, the independent variable is the application of the TaHiTI methodology, while the dependent variables include the accuracy of threat detection, the speed of response, and the reduction of false positives. The experimental setup involves a simulated network environment in which attacks are emulated, and the TaHiTI is used to detect and mitigate these threats. This setup ensures that the findings are relevant and applicable to real-world scenarios (Kadan, 2021).

4.3.3. Data collection and analysis

Data collection is a critical aspect of research strategy, which involves the systematic gathering of quantitative data from various sources. These sources include log files, network traffic data, and system alerts, all of which are analysed to identify patterns indicative of lateral movement attacks. Event data was analysed through contextual

review of logs and system activity. No machine learning or statistical methods were applied, instead, detection patterns were interpreted against MITRE ATT&CK references (Abualkas & Bhaskari, 2023). The data analysis process involves several steps, including data cleaning, pre-processing, and visualisation. The analysis focused on qualitative review of system and security logs, guided by the threat hunting hypotheses derived from TaHiTI. The objective was to identify whether TTPs were successfully detected under each monitoring scenario and how detection quality varied with visibility.

The research strategy used in this study is designed to evaluate the effectiveness of TaHiTI in a controlled virtual environment. By employing a quasi-experimental approach and focusing on data-driven methods, this study aims to provide an evaluation of TaHiTI's capabilities in detecting and mitigating lateral movement attacks.

4.4. Application of TaHiTI

This section explores the practical implementation of the TaHiTI methodology, focusing on its structured application in threat hunting. TaHiTI aims to enhance the detection and mitigation of sophisticated cyber threats, particularly those involving lateral movement. While TaHiTI theoretically supports machine learning-based detection, no such techniques were applied in this study. Instead, the implementation relied on rule-based and hypothesis-driven analysis grounded in threat intelligence.

4.4.1. Overview of TaHiTI

TaHiTI was developed to address the limitations of traditional security measures, by proactively identifying attacker techniques through structured threat hunting. It leverages threat intelligence, which includes information about threat actors, their tactics, techniques, and procedures (TTP), and known attack vectors. This comprehensive integration enables a more informed and targeted approach to threat hunting, which is crucial for reducing the adversary dwell time within a network (Os *et al.*, 2018). The theoretical foundation of TaHiTI emphasises a proactive stance in cybersecurity, advocating for the continuous collection and analysis of threat intelligence to stay ahead of potential attackers. This approach is particularly vital in the context of modern cybersecurity, in which adversaries increasingly use sophisticated techniques to avoid detection. Although TaHiTI theoretically supports machine learning-based detection, this

study did not apply ML techniques. Instead, the focus was on rule-based and behaviour-driven analysis derived from threat intelligence.

4.4.2. Operationalisation of TaHiTI

The operationalisation of the TaHiTI in this study involves a structured and systematic approach to threat hunting, divided into three key phases: preparation, execution and hunt, and act and finalise. These phases provide a systematic framework for conducting threat hunts, as illustrated in Figure 4-1.

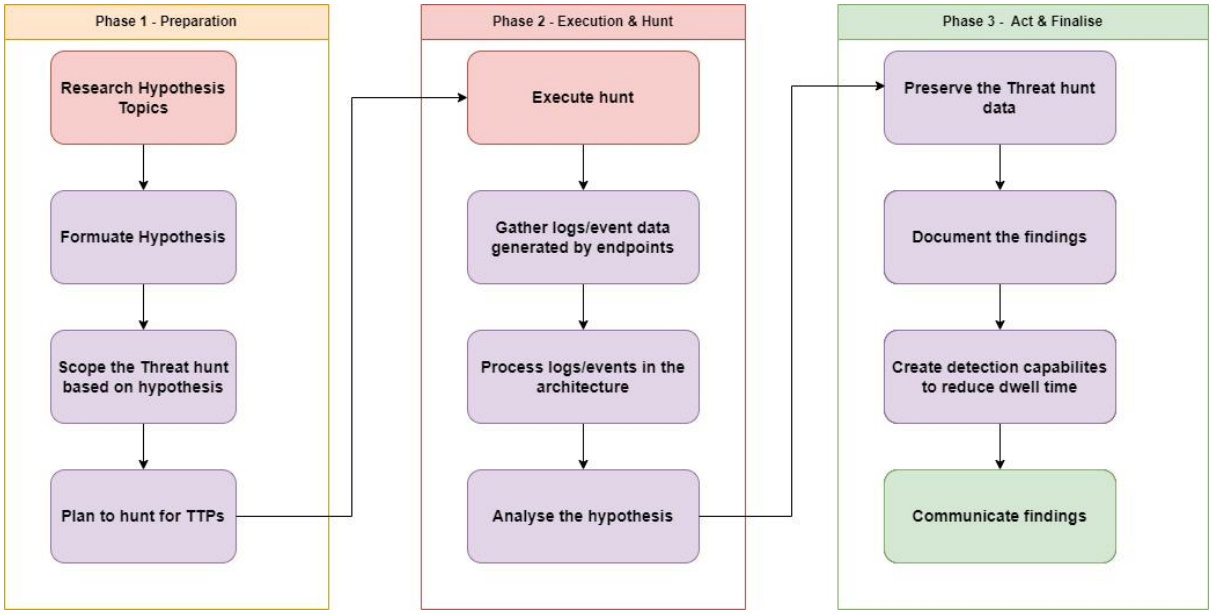


Figure 4-1: Overview of the application of TaHiTI

The **preparation phase** is crucial for laying the groundwork for the threat hunt. This phase involves formulating hypotheses based on comprehensive threat intelligence reports and previous research. A detailed hunting plan is developed, specifying the TTPs to be investigated and the analytical methods to be employed. This phase includes setting up the simulation environment, categorising each technique according to its specific identifier, and establishing a structured framework for the simulations. The preparation phase ensures that the investigation is targeted and aligns with the study's objectives, particularly concerning lateral movement detection.

The **execution phase** involves implementing the threat hunting plan within a controlled environment. This phase begins with the simulation of lateral movement attacks, employing tools like PowerShell, Cobalt Strike, and RAT to replicate real-world adversary

techniques. These simulations are conducted under the assumption of a compromised network state, allowing for a realistic assessment of the TaHiTI methodology. The data-driven threat hunting model, as outlined by Rodriguez and Rodriguez (2019), guides this phase, ensuring alignment with contemporary cybersecurity methodologies. The Hunting ELK (HELK) instance plays a pivotal role in aggregating and analysing data collected during the simulation. This evidence collection process is integrated into the simulation framework, exemplifying a thorough and reflective methodological approach.

In the final phase, the findings from the execution phase are consolidated and documented. This phase involves analysing the collected data, validating the initial hypotheses, and compiling comprehensive reports detailing the detected threats, identified vulnerabilities, and recommended actions. The meticulous documentation of the simulation process and results substantiates the hypothesis-driven approach to threat hunting and contributes significantly to the academic discourse on cybersecurity strategies against lateral movement attacks. The findings are shared with relevant stakeholders, ensuring that the insights gained are utilised to improve ongoing security efforts.

The simulation approach integrates and aligns with the Mitre ATT&CK framework, as detailed in Chapter 3. This integration provides a comprehensive overview of the framework's tactics and enhances the study's methodological rigor. The simulation and hunting processes are meticulously documented, ensuring that the study's findings are robust and reproducible. The evidence collected through the HELK instance is crucial for validating the TaHiTI methodology within an academic setting, laying the groundwork for further analysis and validation in subsequent chapters.

4.4.3. Lateral movement attack techniques and tools

Lateral movement is a critical phase in the life cycle of a cyberattack, particularly in advanced persistent threat (APT) scenarios. Once the initial access is gained, adversaries use lateral movement techniques to navigate through a network, escalate privileges, and access sensitive data. This phase is essential for maintaining persistence and achieving attack objectives, such as data exfiltration or system compromise. The ability to detect and mitigate lateral movement is crucial for effective threat hunting and is a key focus of the TaHiTI. The methods and tools used for lateral movement can vary

widely, depending on the attacker's objectives and the environment. Common techniques include credential dumping, pass-the-hash attacks, remote service exploitation, and abuse of legitimate tools and protocols such as Remote Desktop Protocol (RDP) and Windows Management Instrumentation (WMI).

Credential dumping involves extracting account credentials from the operating system and software on a compromised system. Tools like Mimikatz can be used to dump credentials, allowing attackers to move laterally by impersonating legitimate users (Alvarez, 2020). This technique is particularly dangerous because it can bypass many security measures by using valid credentials.

Pass-the-hash (PtH) is a technique that uses the hash of a user's password to authenticate without knowing the actual password. Attackers can use this method to access other systems in the network, often without triggering standard authentication alerts. This technique is commonly used in conjunction with credential dumping (Strom & Smith, 2023).

In **exploitation of remote services,** attackers often exploit vulnerabilities in remote services to gain unauthorised access to additional systems. Common targets include the remote desktop protocol (RDP) and server message block (SMB) services. Exploiting these services can allow attackers to move laterally within a network, often with elevated privileges (Bai *et al.*, 2019).

With the **abuse of legitimate tools,** attackers frequently use legitimate administrative tools, such as PowerShell, PsExec, and Windows management instrumentation (WMI), to execute commands and scripts across the network. These tools are often already present in the environment, allowing attackers to blend in with regular network traffic and evade detection (Kushwaha *et al.*, 2022; Smiliotopoulos *et al.*, 2024). The use of legitimate tools for malicious purposes poses a significant challenge for traditional security measures, making it a key focus area for threat hunting methodologies like TaHiTI.

Detecting lateral movement requires a combination of network monitoring, endpoint detection, and threat intelligence. Signature-based detection can identify known threats, while behavioural analysis helps uncover new or evolving tactics. Anomaly detection algorithms can highlight unusual activities, such as logins from atypical locations or at

odd times, which may indicate lateral movement attempts (Zhou *et al.*, 2024). The TaHiTI methodology leverages these detection strategies, integrating machine learning models to enhance the detection of anomalous patterns indicative of lateral movement.

In the context of TaHiTI, the focus on lateral movement involves using threat intelligence to identify relevant TTPs and develop detection rules tailored to the organisation's specific threat landscape. The integration of machine learning models can enhance the detection of anomalous patterns indicative of lateral movement. By continuously updating detection capabilities based on new threat intelligence, TaHiTI aims to minimise the dwell time of attackers within the network and reduce the overall risk to the organisation (Os *et al.*, 2018). Understanding and detecting lateral movement is vital for preventing the progression of cyberattacks and reducing the dwell time. TaHiTI offers a structured approach to addressing lateral movement, integrating threat intelligence, and continuously refining detection techniques.

4.4.4. Architect system environment setup

The architect system environment is a crucial component of this study, providing a controlled setup to validate the TaHiTI. The environment simulates a real-world network, allowing for the safe execution of lateral movement attacks and the subsequent analysis of these attacks. The architectural setup consists of three primary components: the attacker environment, the victim environment, and the threat hunt environment.

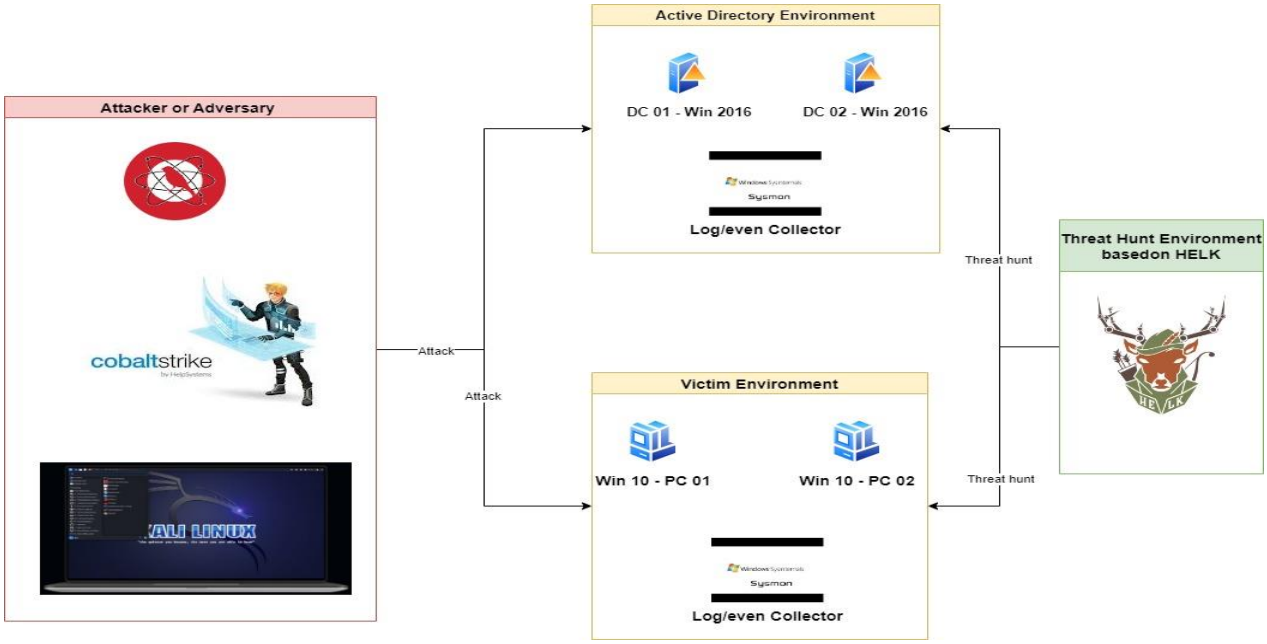


Figure 4-2: Hypothesis-driven architect

Figure 4-2 provides a detailed overview of this setup, illustrating the relationships and interactions between these components.

Attacker environment: This environment is configured with attack tools, including Cobalt Strike, atomic red team and Kali Linux, representing a realistic adversary infrastructure. The attacker initiates lateral movement attacks against the victim environment, simulating real-world attack scenarios. The use of these tools allows for the simulation of sophisticated APT TTPs.

Victim environment: The victim environment includes several endpoint devices running Windows 10 (PC 01 and PC 02) and two domain controllers (DC 01 and DC 02) running Windows Server 2016. These systems are configured to replicate typical corporate network environments. The environment captures log and event data from these systems, using tools such as sysmon and event viewer, which are crucial for detecting lateral movement activities.

Threat hunt environment: This environment is based on the HELK stack, a platform designed for threat hunting and data analytics. The HELK stack is employed to aggregate and analyse the collected data, providing insights into the attack patterns and techniques used. It supports the hypothesis-driven approach by enabling detailed analysis and visualisation of the collected logs and events.

The integration of these components facilitates a seamless workflow for simulating lateral movement attacks and analysing the results. The attacker environment initiates the attacks, while the victim environment collects data through extensive logging and monitoring. The threat hunt environment processes this data, applying the TaHiTI methodology to identify and respond to potential threats. This comprehensive setup ensures that the experiments are conducted in a controlled and secure manner, providing reliable and accurate results.

The architect system environment is meticulously designed to replicate real-world conditions under which lateral movement attacks occur. This setup is crucial for validating the TaHiTI methodology, as it provides a realistic and controlled environment for testing. By simulating a variety of attack scenarios, the study can comprehensively assess TaHiTI's effectiveness in detecting and responding to lateral movement attacks. The findings from this setup are expected to contribute significantly to the academic discourse

on cybersecurity strategies, providing practical insights for improving threat detection and response capabilities. The application of the TaHiTI methodology within this study highlights its potential for effectively detecting and mitigating sophisticated cyber threats, particularly those involving lateral movement. By integrating threat intelligence, advanced tools, and a controlled simulation environment, TaHiTI offers a comprehensive approach for proactive threat hunting. The structured approach, encompassing hypothesis formulation to data analysis, underscores the methodology's practical relevance and efficacy in modern cybersecurity operations. This discussion lays the groundwork for the detailed experimental validation and analysis presented in subsequent chapters, providing valuable insights into TaHiTI's applicability in real-world scenarios.

The following will elaborate on the methodological framework used to validate TaHiTI's effectiveness in a controlled simulation environment. This section will present a detailed overview of the experimental design, from the formulation of hypotheses to the final data analysis, providing a comprehensive examination of TaHiTI's capabilities in identifying and responding to lateral movement attacks.

4.5. Integrated quasi-experimental approach to validating TaHiTI

This section aims to present a comprehensive and methodologically sound framework to evaluate the effectiveness of the TaHiTI threat hunting methodology in a simulated environment. This approach is visually summarised in Figure 4-3, which outlines the key steps from hypothesis formulation to data analysis.

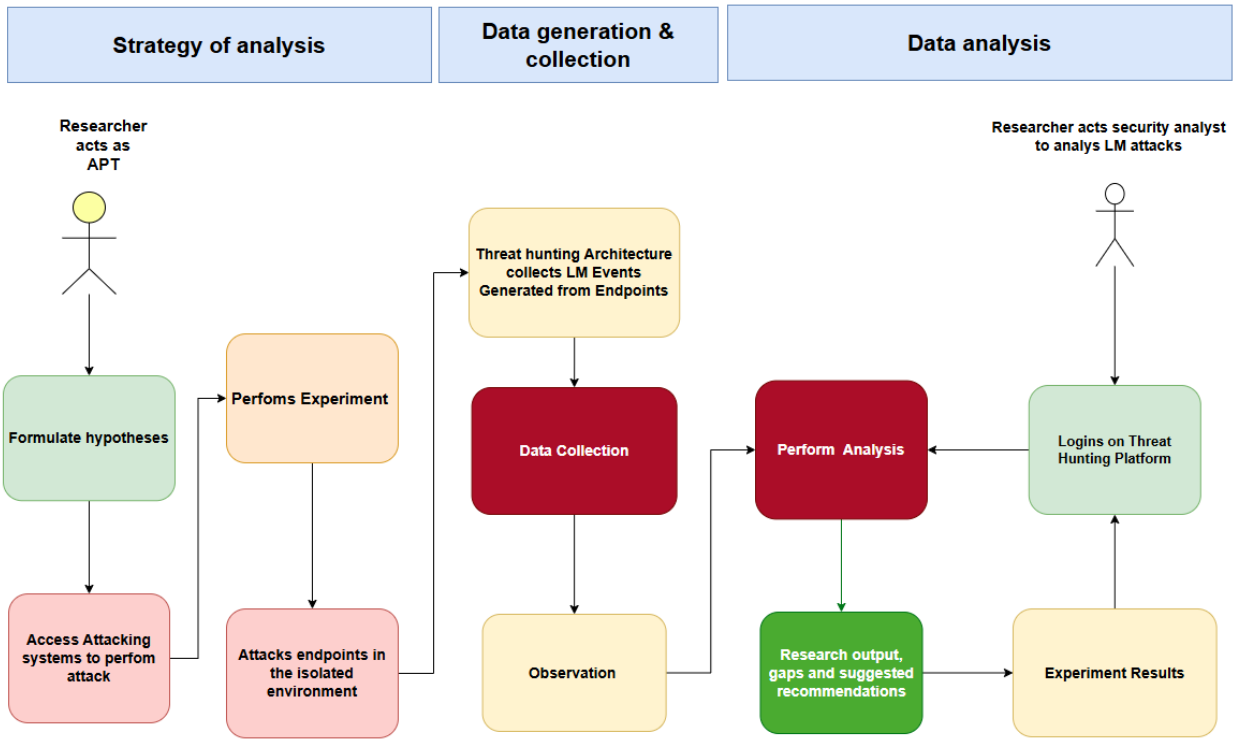


Figure 4-3: Review of research methodology in action

To simulate lateral movement attacks in a controlled environment and validate the effectiveness of the TaHiTI methodology, the following steps were taken.

Simulating lateral movement attacks: The researcher acts as an adversary to simulate realistic lateral movement attacks. This step is crucial for creating authentic scenarios that test TaHiTI's capabilities in identifying and responding to these threats.

Hypothesis formulation and execution: Hypotheses are developed based on existing research and practical insights gained during the simulation. These hypotheses guide the simulated attacks against the endpoints, providing a structured framework for the study.

Data generation, aggregation, and analysis: Data collection is carried out using the sysmon events and aggregated within a HELK framework, with HELK serving as the central analytics platform. While HELK supports advanced analytics, this study limited analysis to rule-based detection and manual event interpretation, consistent with qualitative design principles.

Experimental validation and documentation: The quasi-experimental design allows for a structured validation process. The documentation of results is aligned with TaHiTI

and data-driven principles, providing a detailed account of the study's findings and the validation of the hypotheses.

Integrated approach to analysis and findings: The study synthesises quantitative data to provide a comprehensive understanding of TaHiTI's performance. This integrated approach highlights the strengths and potential improvements of TaHiTi.

Figure 4-3 visually represents this integrated approach, capturing the essence of the research methodology and its application in this study. The illustration provides a clear and detailed roadmap of the processes involved, from the initial hypothesis formulation to the final analysis and documentation of the findings. This section emphasises the importance of a rigorous and structured approach to validating TaHiTI in a controlled environment, and demonstrates its effectiveness and potential for real-world applications, particularly in academia.

4.6. Chapter summary

This chapter presented a comprehensive overview of the research methodologies and strategies employed in this study, with a particular focus on the validation of the TaHiTI methodology. The chapter began by discussing the theoretical underpinnings of research philosophies, such as positivism, interpretivism, and pragmatism, and justified the selection of positivism as the guiding philosophy for this quasi-experimental study. The chapter then outlined the application of the TaHiTI methodology, detailing its operationalisation and the structured process followed for its implementation. Key sections included the overview of lateral movement attack techniques and tools, and the integrated quasi-experimental approach used to validate TaHiTI in a simulated environment. These sections provided a thorough examination of the technical and methodological aspects of the study, emphasising the use of advanced tools and frameworks like HELK for data collection and analysis. Overall, this chapter has laid a solid foundation for understanding the research approach and its practical application in the context of cybersecurity. The findings and methodologies discussed will serve as a critical reference for subsequent chapters, where the experimental results and their implications will be explored in detail. This comprehensive approach not only validates the TaHiTI methodology but also offers valuable insights into the practical aspects of threat hunting, contributing to the field's academic and operational knowledge base.

Chapter 5 Hypothesis-driven threat hunting architecture testing

5.1. Introduction

Building on the methodologies and approaches detailed in Chapter 4, this chapter presents the practical application of the hypothesis-driven threat hunting architecture, focusing on simulating lateral movement attacks to evaluate the effectiveness of TaHiTI. The chapter outlines the experimental setup, tool selection, and data collection methods employed in the study. Simulations replicate real-world attack scenarios within a controlled virtual environment, allowing for rigorous testing of the formulated hypotheses. Detecting lateral movement is critical in the context of advanced persistent threats (APT) because it represents a key phase in which attackers escalate their control within a compromised network. The subsequent sections provide a detailed overview of the tools selected for their relevance to threat hunting, the configuration of the environment for realistic attack execution, and data collection processes supporting comprehensive analysis. This structure aims to validate the efficacy of TaHiTI in detecting lateral movements in an academic context.

5.2. Setup of tools and environment

In preparation for the simulations designed to validate TaHiTI, careful consideration is given to the selection of tools and setting up the environment. Each tool is chosen based on its proven effectiveness in simulating APTs and supporting a robust threat hunting process, which are crucial for evaluating TaHiTI capabilities. The virtual environment is configured to simulate what is considered a typical corporate network, ensuring that the simulations can replicate potential real-world conditions and generate relevant data for analysis. While this approach provides a foundation for testing how well TaHiTI can detect and respond to the complex behaviours exhibited by APTs, it is important to note that real-world networks may differ from this simulated environment. Similar studies, such as those of Lee *et al.* (2021), acknowledge the challenges of creating exact replicas of complex networks and instead focus on building simulations based on common architectures in cybersecurity research. Simulations in cybersecurity, including those discussed by Kavak *et al.* (2021), serve as approximations of real-world conditions,

providing environments where network vulnerabilities and defence strategies can be tested without the variability found in actual corporate networks (Kavak *et al.*, 2021). Additionally, Lee *et al.* (2021) emphasise that while these simulations should reflect typical network environments, they must remain adaptable, as real-world IT infrastructures are dynamic and complex. The following subsections provide a detailed overview of the selected tools and the environmental configuration that underpin these simulations.

5.2.1. Tools

The selection of tools for this study is guided by their established effectiveness in simulating APT scenarios and supporting comprehensive threat hunting processes. These tools fall into three broad categories: simulations, attacks, and detection. Each category serves a specific purpose in replicating APT tactics and allowing a thorough evaluation of TaHiTI for lateral movement detection.

Simulation tools are designed to create realistic controlled environments where adversarial tactics can be accurately mimicked. A common feature of these tools is their ability to replicate APT behaviours consistently and safely. **Cobalt Strike** is central to this category and is known for its effectiveness in red-teaming exercises and adversary simulations. It enables replication of lateral movement, command-and-control (C2) operations, and phishing attacks (Khaver, 2023). **PowerShell** also plays a key role here, often used to automate tasks like system discovery and reconnaissance. Due to its deep integration within Windows systems, PowerShell allows simulation of realistic administrative activities, including those exploited by attackers for lateral movement (Smiliotopoulos *et al.*, 2023).

Attack tools replicate the actions that adversaries might perform once they gain access to a system. A defining feature of these tools is their ability to simulate realistic malicious actions such as dumping credentials and remote access. **Mimikatz** is critical in this category, simulating credential theft and pass-the-hash (PtH) attacks to demonstrate lateral movement within networks (Raj, 2020). Similarly, **Quasar RAT** is used to emulate remote access and persistence tactics. Originally designed for legitimate remote administration, Quasar RAT is often repurposed for malicious use, making it a relevant

tool for the study of lateral movement and remote-control scenarios (Ackerman & Clifford, 2021; Palacin, 2021).

Detection tools are responsible for monitoring, capturing, and analysing malicious activities within the simulated environment. A shared characteristic of these tools is their ability to detect and visualise patterns and anomalies indicative of adversarial activity. The **System monitor (sysmon)** is a key detection tool in this study, capturing critical system activities such as process creation, network connections, and file modifications (Danneman & Hyde, 2021). The detailed logs collected by sysmon are processed using Hunting ELK (HELK), an advanced open-source threat detection platform. HELK integrates Elasticsearch for data storage and search, Logstash for log ingestion and processing, and Kibana for data visualisation and real-time monitoring (Benito *et al.*, 2023). These components work together to enable HELK to identify suspicious activities and detect lateral movement across the simulated network.

Additional tools, such as **Atomic Red Canary** scripts, are used to simulate specific attack techniques mapped to the MITRE ATT&CK framework. These open-source scripts allow cybersecurity teams to replicate known APT behaviours in a controlled and repeatable manner. This helps assess the effectiveness of detection and response tools by simulating attacks such as credential dumping and phishing attempts, aligning closely with real-world attack scenarios (Oakley, 2019).

Finally, **Kali Linux** serves as the primary operating system to run various penetration testing tools. Widely recognised for its suite of utilities tailored to ethical hacking and digital forensics, Kali Linux is the platform of choice for conducting these simulations (Ackerman & Clifford, 2021). While alternatives like Parrot OS could have been used, Kali Linux is selected due to its extensive support and documentation, facilitating smoother simulations. Together, these tools ensure that the virtual environment closely mimics real-world attack scenarios, providing comprehensive data to evaluate the ability of TaHiTI to detect lateral movement. By categorising the tools into simulations, attacks, and detection, this study clearly demonstrates how each tool fits into the overall framework of the simulations, enabling a structured approach to testing TaHiTI.

5.2.2. Environment setup

The environment for this study is designed to replicate a corporate network, providing a controlled environment to simulate lateral movement attacks and to evaluate TaHiTI. Corporate networks generally consist of multiple interconnected systems, including servers, client machines, and network devices, such as routers and firewalls, all configured to support business operations while maintaining security and network integrity (Xu & Russello, 2022). These components are often arranged to create a secure, efficient, and manageable environment. However, this study provides a high-level overview, focusing on the tools and systems used to simulate a typical corporate network environment.

The virtual environment, as shown in Figure 5-1, includes three distinct environments: attacker, victim, and threat hunting, each configured to interact as they would in a real-world scenario. An active directory (AD) environment is also included as a part of the victim environment, as many corporations make use of AD and rely on AD for authentication, access control, and network management, making it a frequent target for adversaries during lateral movement and other network-based attacks. AD environments allow attackers to exploit vulnerabilities within the authentication and directory services, making them ideal for replicating real-world attack scenarios in this study (Khattab, 2020).

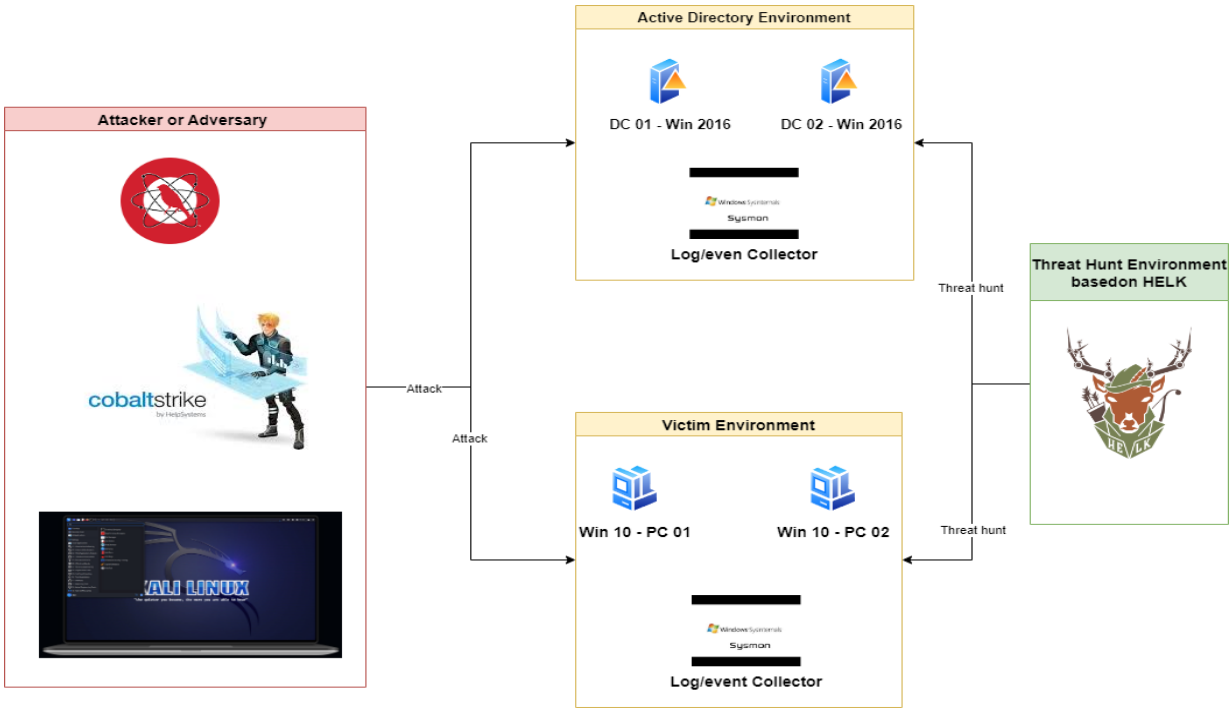


Figure 5-1: Hypothesis-driven architect

Figure 5.1 provides a high-level overview of the environment simulation, detailing the key tools and systems used, rather than focusing on the physical network infrastructure such as routers and firewalls. This study aims to replicate an adversarial scenario and test threat detection on a software level, and, therefore, it is not necessary to fully simulate a physical network. The simulated environment, although seemingly limited in devices, provides the necessary foundation for analysing the effectiveness of TaHiTI, as an effective lateral movement detection method should be able to detect such an attack even if it involves only two victim systems.

The attacker environment, shown to the left in Figure 5-1, uses CobaltStrike and Kali Linux to emulate sophisticated adversarial techniques. Because these tools have been thoroughly discussed in Section 5.2.1, this section focuses on how the attacker environment is configured. It runs on a separate virtual machine within the same network as the victim environment, ensuring local network access, which is crucial to simulate lateral movement and other attack vectors. In a real-world scenario, an APT would first establish a foothold in the network before executing lateral movement attacks. Therefore, it can be assumed, for the purposes of these simulations, that the attacker already has access to the local network before commencing an lateral movement attack. Network connectivity is confirmed by establishing communication channels between the attacker and victim environments, allowing the attacker to interact with the victim system, thereby validating the simulation setup. This configuration realistically mirrors an attacker's access to a local network in a real-world scenario, where penetration occurs within the same network perimeter.

The **victim environment**, depicted in the centre of Figure 5.1, includes a Windows domain controller running Windows Server 2016 and two Windows 10 systems (WIN-LAB and WIN-LAB-02) with IP addresses 192.168.10.49 and 192.168.10.30, respectively. This setup is valid for testing lateral movement detection techniques as it sufficiently simulates the core functionalities of a corporate network without requiring the inclusion of a large number of devices. The systems are configured in a way that is similar to a typical corporate network environment, with critical components such as a domain controller, endpoints, and logging mechanisms such as sysmon included. Although larger corporate networks may include significantly more devices, this minimal setup provides a controlled and representative environment that is sufficient for the purposes of this study.

The threat hunting environment, shown to the right of Figure 5.1, is based on the HELK platform, an open-source system designed for advanced threat detection and response. The HELK environment is configured to process logs and events generated by victim systems, enabling a detailed analysis of attacker behaviour. The attacker environment sends simulated attacks to the victim systems, and the resulting system activities are logged and analysed using HELK. Communication between these three environments ensures that all network components interact as they would in a real-world corporate network, making it a valid simulated setup to use when testing TaHiTI's lateral movement detection capabilities.

5.3. Simulation and hunting

The simulation and hunting processes in this study are designed using predefined techniques from the MITRE ATT&CK framework. Specifically, this study focuses on the lateral movement tactic within the framework, which encompasses several techniques commonly employed by APTs to traverse a network after gaining an initial foothold. Although the MITRE ATT&CK framework lists numerous lateral movement techniques, only five were selected for this study. Selection is based on the relevance of these techniques to common attack vectors in corporate environments, their diversity in terms of attack methods, and their practicality in terms of simulation and detection. The techniques chosen are as follows:

i. **Pass-the-Hash (T1075)**: This technique involves using the hashed credentials of a legitimate user to gain access to other systems within the network, without the need for a plaintext password. This is commonly exploited in corporate environments, where administrative credentials are reused across multiple systems. It was selected because of its prevalence in real-world attacks and the challenges it presents in terms of detection (Mitre, 2024). These challenges include, among others, the reuse of credentials across various systems, which allows attackers to leverage a single compromised hash to access multiple machines without needing to re-compromise each system. This creates difficulty for security systems to distinguish between legitimate administrative activity and malicious lateral movement (Dimov & Tzonev, 2017; Jadeja & Vaghasia, 2018; Oberle *et al.*, 2016).
ii. **Remote desktop protocol (RDP) (T1021.001)**: RDP is a popular protocol used to connect remote systems. Attackers often abuse RDP to gain lateral access once

inside the network. This technique was chosen for its widespread use in corporate settings and the ease with which attackers can leverage it to maintain persistence and expand access (Mitre, 2024). By obtaining remote desktop access, an attacker can control the compromised machine as if physically present, allowing them to execute commands, transfer files, and install malicious software. This access enables the attacker to move laterally across the network, escalate privileges, and maintain a persistent foothold by creating new RDP sessions or adding user accounts with administrative privileges. Moreover, since RDP is commonly used for legitimate administrative purposes, malicious activities using this protocol can blend with normal traffic, making detection more difficult (Ashfaq & Malik, 2022).

iii. **Windows administrator shares (T1077):** Attackers frequently use administrative shares to copy malicious tools and remotely execute commands. This technique is particularly relevant in corporate networks due to its use in file sharing and remote execution within Windows environments, where administrative shares (e.g. C$, ADMIN$) are commonly used for maintenance tasks by system administrators. Attackers often take advantage of these administrative shares to move laterally within a network by disguising malicious tools as legitimate files or processes. By placing these tools in shared locations, attackers increase the likelihood that a legitimate administrator or automated system will unknowingly execute or distribute the malicious software, further compromising the network (Mailewa & Rozendaal, 2022).

iv. **SMB/Windows file sharing (T1021.002)**: The server message block (SMB) is commonly used for file sharing within a network. Attackers exploit SMB vulnerabilities to move laterally between systems. These types of attack generally involve exploiting weak authentication mechanisms or misconfigured file shares to gain unauthorised access, allowing attackers to transfer malicious files, execute remote commands, and gather sensitive information from compromised systems. Attackers can also exploit known vulnerabilities in the SMB protocol, such as the EternalBlue exploit, to propagate malware and gain deeper access to the network (Liu *et al.*, 2022; Sajan, 2024). The inclusion of this technique was motivated by its frequent exploitation in both targeted and opportunistic attacks, particularly in environments where file sharing is essential as is the case with most corporate networks.

v. **Windows Management Instrumentation (WMI) (T1047):** WMI provides administrative capabilities to manage local and remote systems. Attackers can use WMI to execute code and spread it across systems. This technique was chosen

because of its stealthy nature and its ability to bypass traditional detection mechanisms, making it a prime candidate for testing TaHiTI detection capabilities (Nguyen *et al.*, 2024).

These five techniques are each simulated separately to test TaHiTI's effectiveness in detecting lateral movement attacks. While other techniques, such as remote service creation (T1021.004) and token impersonation (T1134) could also have been used for simulations, the selected techniques offer a good representation of the most common LM techniques used in real-world scenarios, while still remaining manageable. These techniques cover a broad spectrum of lateral movement tactics, allowing a comprehensive evaluation of TaHiTI detection capabilities.

5.3.1. Simulation and hunting process

The process for each of the simulations in this study begins with the formulation of hypotheses derived from the MITRE ATT&CK framework. This approach ensures that each simulation remains aligned with the objective of validating TaHiTI's capability to detect lateral movement. Hypotheses are developed to predict specific behaviours and patterns associated with the selected techniques, which can be identified through system logs and network traffic. In order to formulate a hypothesis, a technique is selected from the MITRE ATT&CK framework and its impact on network traffic, system logs, or process execution patterns is predicted. The core assumption of each hypothesis is that the technique produces identifiable anomalies that monitoring tools such as sysmon and HELK can detect. Hypotheses related to lateral movement techniques generally anticipate unusual authentication attempts, command executions, or file transfers that deviate from normal patterns within the network.

For example, **remote system discovery (T1018)** involves an attacker trying to discover other systems within a network. The hypothesis of this technique is that reconnaissance activities will generate distinctive network traffic and system logs, specifically related to system enumeration. The simulation of this attack involves executing PowerShell commands (e.g., net group "domain computers"/domain) to enumerate domain computers. A hypothesis for this attack would state that specific log entries and traffic patterns will reveal the attacker's reconnaissance. The logs, which are captured by sysmon and analysed using HELK, would therefore contain the information necessary to

detect lateral movement. In short, the hypothesis is used to describe how an attack can be inferred from data captured as logs, which in turn makes threat hunting possible. As these attacks are often similar in nature, a general hypothesis can be developed for each technique (Bai *et al.*, 2019; Dong *et al.*, 2021).

Execution of simulations: Each simulation is executed following a structured script designed to replicate the chosen technique. For example, in the remote system discovery (T1018) simulation, PowerShell commands are executed to enumerate domain computers, generating specific logs and network traffic that are subsequently captured and analysed. This approach is consistent with the work of Katano *et al.* (2022), who discuss how the behavioural patterns of devices during lateral movement can be detected through a detailed analysis of logs and network activity. Similarly, other techniques, such as internal spear-phishing (T1534 and T1566.001) and lateral tool transfer (T1570), are simulated using predefined scripts, each of which produces unique behaviours that are recorded and analysed.

Data collection: During each simulation, sysmon is configured on victim systems to continuously monitor and log relevant activities, including process executions, network connections, and system commands. This is consistent with corporate networks, as computers that are part of such networks often have monitoring software installed to help with IT administration. The collected data is then automatically forwarded to HELK, which operates on a dedicated analysis machine. Sysmon is installed on each victim system, while HELK processes the data centrally. The logs are ingested into HELK via Logstash pipelines, ensuring real-time data collection and processing without human intervention. This automation streamlines the collection of detailed system logs and allows for timely analysis of lateral movement activities. Sysmon logs include crucial information to identify signs of compromise, such as unusual process creation or network connections. HELK aggregates these data, providing a comprehensive view of attacks across multiple victim systems.

Data processing in HELK: The data processing phase begins when sysmon logs are collected and ingested into HELK. HELK processes data through its integrated stack, Elasticsearch, Logstash, and Kibana, allowing for a detailed analysis of the system and network activities. During this phase, the data are indexed and queried to identify patterns of lateral movement. Anomalous behaviours such as unexpected file transfers or irregular

command executions are highlighted and visualised through Kibana dashboards. The processed data are analysed to assess how well TaHiTI detects the simulated attacks. The results of this analysis are used to refine the hypotheses and adjust the detection strategies for further simulations. For example, if TaHiTI fails to detect certain behaviours, system configurations or monitoring rules can be adjusted to improve its detection capabilities (Smiliotopoulos *et al.*, 2022). Additionally, detection and visualisation of malicious activities are done using the ELK framework, which integrates Elasticsearch, Logstash, and Kibana for real-time anomaly detection (Muse *et al.*, 2023).

5.3.2. Simulation execution

The simulation execution follows a structured approach that aligns with the objective of the study of validating the TaHiTI's capabilities to detect lateral movement within a corporate network environment. This section outlines the simulation process, from hypothesis formulation to data processing, ensuring a logical flow that matches earlier sections.

The virtual environment used in this study is carefully configured to replicate a typical corporate network. It includes a Windows domain controller and two Windows 10 systems that simulate the core components of a corporate environment. Although the number of devices is limited, this setup is sufficient to capture the essential aspects of lateral movement within a controlled environment. The systems are interconnected, allowing the simulation of real-world attack scenarios such as lateral movement, file transfers, and remote execution of commands. By replicating common attack vectors, the environment provides a valid platform for testing TaHiTI's capabilities. The key stages of the simulation process are outlined as follows:

i. **Formulation of the hypothesis**: For each technique (for example, Remote System Discovery, Pass-the-Hash), a hypothesis is developed based on expected behaviours. For example, the remote system discovery hypothesis (T1018) posits that system enumeration generates distinctive logs including network traffic anomalies and specific system activities (Otomo *et al.*, 2018).
ii. **Execution of the simulation**: The selected technique is simulated by executing predefined scripts that replicate an attack. In the case of remote system discovery, PowerShell commands are executed to enumerate domain computers. Cobalt Strike

is used for more complex attack simulations, such as Pass-the-Hash (T1550.002), where hashed credentials are used to authenticate within the network.

iii. **Data Collection**: During each simulation, sysmon captures relevant system activities while network traffic is monitored for anomalies. The logs are automatically forwarded to HELK, which aggregates and processes data. This step is crucial for ensuring that all critical events are recorded and ready for analysis.

iv. **Data Processing and Analysis**: The collected data is processed in HELK, where they are analysed for patterns and anomalies that align with the hypothesised behaviours. For example, unusual authentication attempts or remote command executions, as seen in the Pass-the-Hash simulation, are flagged and correlated with other system logs to confirm the potential presence of lateral movement.

A simulation concludes with an evaluation of how well TaHiTI detects the simulated lateral movement technique. The detection results are analysed to determine whether TaHiTI successfully identified the anomalies and behaviours described in the hypothesis. For example, in Remote System Discovery simulation, TaHiTI's ability to detect the system enumeration activity and flag the corresponding network traffic patterns is critical for validating its effectiveness. Similarly, in the Pass-the-Hash simulation, TaHiTI's success in detecting anomalous authentication requests is essential to demonstrate its utility in identifying this advanced lateral movement technique.

5.4. Simulation scenarios and results

This section provides a detailed overview of each simulation, focusing on the techniques used, the process followed, and the results obtained. Each simulation is designed to test the effectiveness of TaHiTI in detecting lateral movement based on the hypotheses developed using the MITRE ATT&CK framework.

5.4.1. Simulation 1: Remote system discovery (T1018)

The first simulation focuses on the remote system discovery technique (T1018), a tactic commonly used by APTs to identify other systems within a network. The primary goal of this discovery process is to identify potential targets for lateral movement. The hypothesis formulated for this simulation posits that system enumeration activities, such as the retrieval of domain computers, will generate identifiable network traffic patterns and

system logs that can be detected through a combination of sysmon and HELK. The overall process followed for this simulation is shown in Figure 5-2.

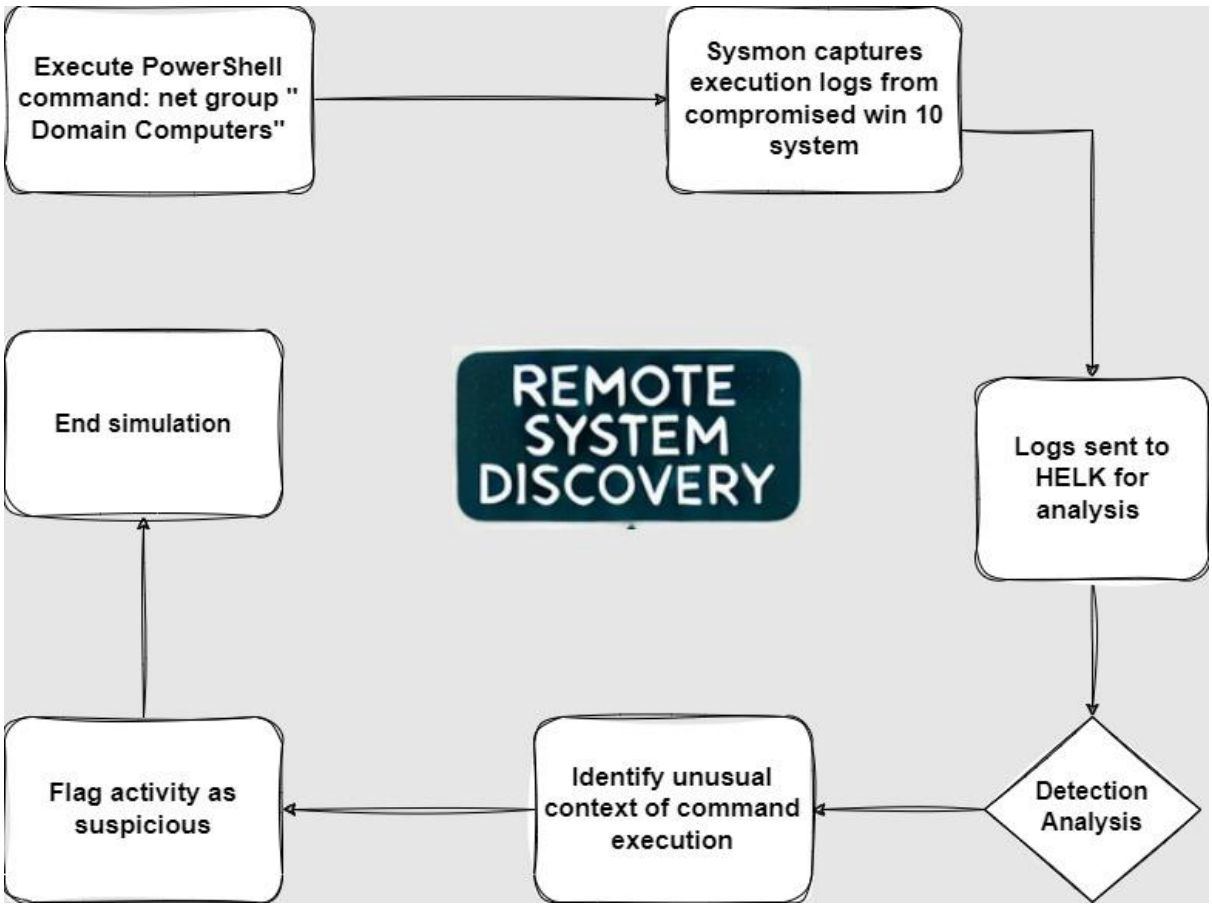


Figure 5-2: Remote system discovery overall process

The simulation is carried out by executing the **net group "Domain Computers" /domain** command via PowerShell on an already compromised Windows 10 machine within the victim environment. This command retrieves a list of all domain computers within the network, simulating a real-world reconnaissance attack aimed at identifying potential targets for lateral movement. It is important to note that only one machine in the victim environment is compromised, as lateral movement attacks would be unnecessary if all systems were already compromised. The aim of this simulation is to demonstrate how attackers move from one compromised machine to other systems in the network. The net.exe process, which is part of the Windows networking utility, is responsible for carrying out network-related commands, such as querying domain information. In this simulation, *net.exe* is used to query domain computers, which then triggers the creation

of the *net1.exe* process. *net1.exe* is a secondary component involved in handling specific networking tasks, often used in enumerating and managing resources on a network.

Sysmon is deployed to log key system activities, such as process creation and network connections, while HELK processes and visualises these logs for further analysis. Figure 5-2 illustrates the sequence of events during the simulation, beginning with the execution of *cmd.exe*, followed by *net.exe*, and culminating in the creation of the *net1.exe* process. This process flow highlights the command execution path typical of a system discovery attack, providing a clear understanding of how such activities unfold in real time. Each process creation event is logged by sysmon, assigned a unique GUID, and sent to HELK for analysis, where anomalous patterns are flagged as potential threats. The detailed step-by-step application of this tactic, including specific commands and outputs, is outlined in Appendix A. Sysmon successfully captures the execution of the **net group "Domain Computers" /domain** command. The process creation event triggered by *net.exe* and the associated network activity are logged and processed by HELK. Analysis of these logs in HELK reveals clear indicators of the system discovery attempt. The execution of a command from a compromised machine, particularly outside typical administrative use cases, is flagged as suspicious because of its unusual context and timing. This activity is flagged as anomalous for several reasons:

i. **Unusual context**: In a standard corporate environment, it is uncommon for regular workstations to request a list of domain computers. Such network-wide queries are typically performed by administrative systems or dedicated IT tools and not by end-user devices.
ii. **Process and timing**: The use of PowerShell and the *net.exe* process for system enumeration from a non-administrative machine is anomalous. Research has shown that malicious actors frequently use built-in administrative tools such as PowerShell for lateral movement and system discovery without triggering conventional antivirus systems (Hendler *et al.*, 2018).

The findings showcase TaHiTI's capability to identify reconnaissance activities such as remote system discovery, which often precedes lateral movement attacks. TaHiTI efficiently distinguishes between standard administrative operations and potentially harmful actions by monitoring and examining the execution of net group commands. HELK's identification of the atypical context and timing underscores TaHiTI's efficacy in

providing early alerts for lateral movement attempts. Although the system successfully marks this activity as suspicious, it is crucial to consider how genuine administrative tasks are managed. For example, network administrators frequently conduct domain-wide queries as part of their regular network updates. If an authorised IT administrator executes the same net group command during planned network maintenance, the system would need to recognise this as legitimate. To differentiate between authorised use and malicious activity, whitelisting or context-based filtering could be employed, such as acknowledging administrative actions performed during standard working hours or from recognised administrative devices, while flagging similar actions outside these parameters for additional scrutiny.

5.4.2. Simulation 2: Internal spear-phishing (T1534 and T1566.001)

The second simulation focuses on the internal spear-phishing technique, identified by the MITRE ATT&CK framework as T1534 and T1566.001. This technique involves an adversary sending phishing emails to internal users within a compromised network to gain further access or to execute additional malicious activities. The hypothesis for this simulation posits that phishing attempts trigger specific anomalies in email communication patterns, user interactions, and system activities, which can be detected through a combination of sysmon and HELK. The simulation employs PowerShell and atomic red canary scripts to simulate an internal spear-phishing attack. The attack is designed to replicate a scenario in which a phishing email containing a malicious Excel file is sent to an internal user. Upon interaction with the attachment, malicious commands are executed, simulating a real-world phishing attack. Sysmon is configured to capture detailed logs of these interactions, focusing on process creation events (sysmon event ID 1), which monitor the launch and execution of the Excel file and subsequent PowerShell commands. The figure illustrates the attack's progression, starting with the initial user interaction with the phishing email, followed by the execution of a malicious Excel file and culminating in the execution of PowerShell commands.

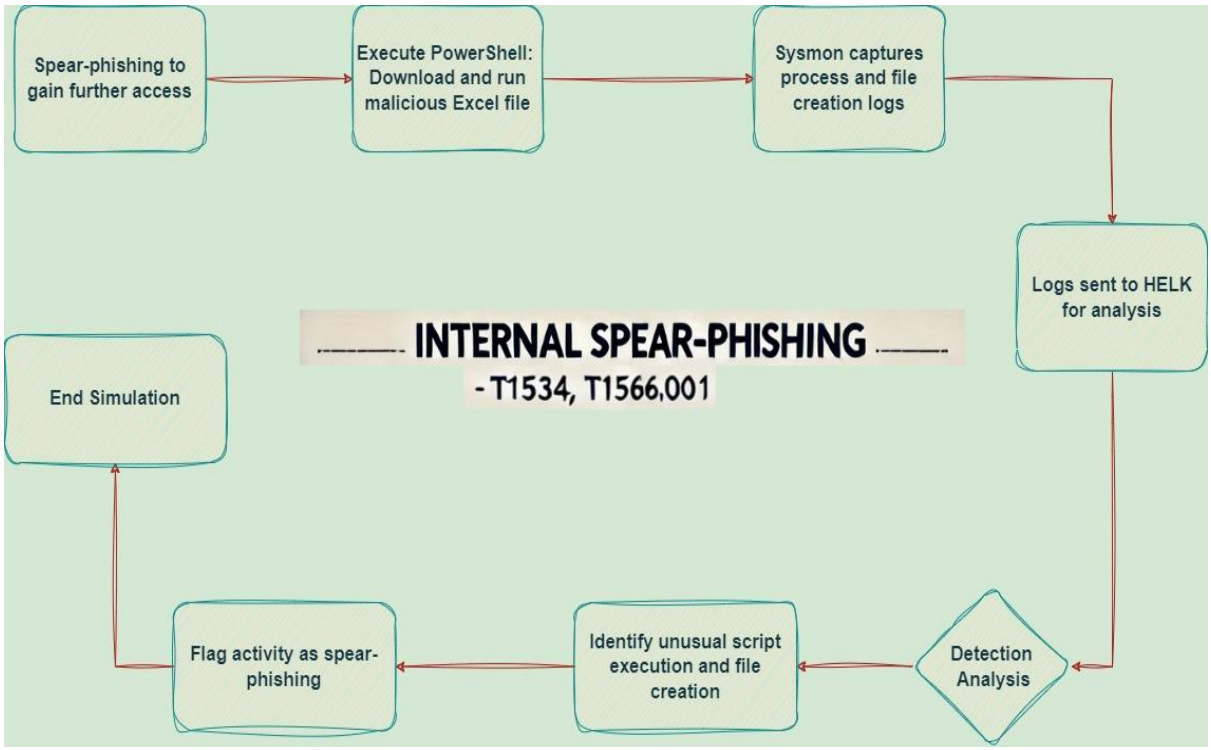


Figure 5-3: Internal spear-phishing overall process

Each step of the attack generates process creation logs, which are captured by sysmon and analysed by HELK. The detailed step-by-step execution of this tactic is provided in Appendix A. The logs show a sequence of activities, including the opening of Excel and the execution of embedded PowerShell scripts. HELK processes these logs and identifies patterns that are consistent with known phishing attacks, such as the execution of macros within Office documents leading to command-line activities. The analysis also reveals distinct patterns commonly associated with phishing, which are flagged by HELK as suspicious because of their deviation from normal user behaviour. Specifically, the following are considered primary indicators of a possible spear phishing attack:

i. **Unusual user behaviour**: The execution of PowerShell commands following the opening of an office document is highly irregular and typically indicative of a phishing attempt.
ii. **Process creation sequence**: The correlation between the Excel process and the subsequent execution of command-line scripts is unusual in standard user workflows, highlighting potential malicious activities.

The simulation demonstrates TaHiTI's capability to detect spear-phishing attempts through a combination of behavioural analysis and detailed process monitoring. By

identifying the unusual sequence of process creation, TaHiTI effectively distinguishes between normal user actions and those characteristic of phishing attacks. This early detection is crucial for preventing further compromise within the network. While the system successfully flags these activities as suspicious, it is important to refine the detection mechanisms to distinguish between malicious and legitimate uses of command-line scripts. For example, authorised scripts executed by IT personnel for maintenance purposes should be recognised as legitimate. Context-based filtering or behavioural baselines can help differentiate between regular administrative actions and atypical user behaviours that signal phishing attempts.

5.4.3. Simulation 3: Pass-the-Hash (PtH) and Window-Management Instrumentation (WMI)

This simulation explores the combined use of the Pass-the-Hash (PtH) technique and Windows Management Instrumentation (WMI) to facilitate lateral movement within a network. PtH allows attackers to authenticate remote systems using captured NT LAN Manager (NTLM) hashes rather than plaintext passwords. NTLM is a suite of Microsoft security protocols that provide authentication, integrity, and confidentiality, commonly used in corporate environments for authentication in networks that are not integrated with Kerberos (Boulila & Dacier, 2023). However, attackers can exploit NTLM by capturing hashed credentials and using them to authenticate without needing the plaintext password, making PtH attacks a significant threat in lateral movement scenarios. WMI, on the other hand, is leveraged to execute commands remotely across multiple Windows systems, further enhancing an attacker’s ability to move laterally without detection. The hypothesis for this simulation posits that PtH combined with WMI generates specific patterns in authentication logs, process creation, and network activity, which can be identified using advanced monitoring tools such as sysmon and HELK. Figure 5-4 provides a comprehensive view of the flow of the simulation, demonstrating how the PtH and WMI techniques are executed in sequence.

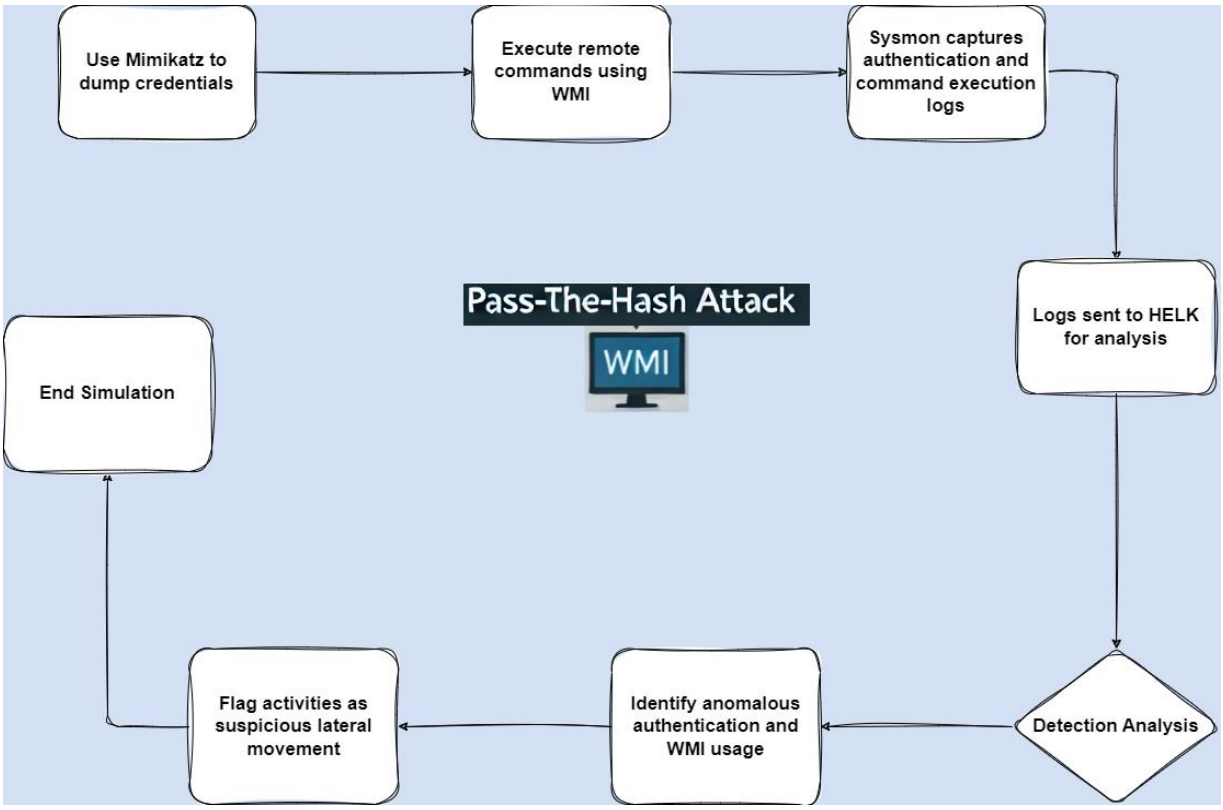


Figure 5-4: PtH and WMI overall process

The process begins with an attacker deploying Cobalt Strike, specifically using its Beacon payload, to establish initial access and maintain persistence in compromised systems. This payload is commonly used in red-teaming and adversarial simulations to simulate command-and-control (C2) channels, allowing the attacker to move laterally and execute further attacks. Mimikatz is then used to extract NTLM hashes from compromised systems, allowing the attacker to authenticate and execute commands without requiring the original plaintext passwords. Mimikatz is a widely used post-exploitation tool designed for credential dumping, making it effective in simulating real-world attacks, as described in the tools section of this study. Finally, WMI commands are executed via PowerShell to facilitate remote operations on the target systems, enabling lateral movement and further compromise without direct interaction. The detailed step-by-step execution of this simulation is available in Appendix A.

Sysmon plays a critical role in capturing the logs of these activities by focusing on process creation events and network connection events. These logs are aggregated and analysed using HELK, which correlates the data to identify patterns consistent with PtH and WMI attacks. The analysis reveals a sequence of processes triggered by PtH authentication

attempts, followed by remote command executions via WMI. HELK's analytical capabilities of HELK enable the detection of subtle, yet critical, signs of lateral movement. PtH and WMI activities are flagged as suspicious based on the following factors:

i. **Unusual authentication attempts**: PtH attacks can be detected by identifying logon attempts that utilise NTLM hashes without preceding password verification, which is a common red flag in lateral movement scenarios.
ii. **Remote command executions**: The execution of commands remotely via WMI, particularly those initiated from non-administrative machines or outside regular operating hours, is identified as an anomaly, signalling potential malicious intent.

This simulation underscores TaHiTI's ability to detect advanced lateral movement techniques that exploit legitimate administrative tools. By continuously monitoring the process creation and authentication logs, TaHiTI can identify when these tools are being used maliciously. The early detection of PtH and WMI activities can significantly disrupt an attacker's ability to move laterally within a network, thereby preventing further compromise. Although the system effectively identifies these activities as suspicious, it remains crucial to differentiate between malicious and legitimate usage of tools, such as WMI. For example, system administrators frequently employ WMI for routine management operations. To minimise false alarms, the implementation of contextual filters and behavioural benchmarks could help distinguish between authorised administrative actions and those that deviate from the typical operational patterns.

5.4.4. Simulation 4: Lateral tool transfer (T1570)

The fourth simulation examines the lateral tool transfer technique, identified by the MITRE ATT&CK framework as T1570. This technique involves an adversary transferring tools or files across a network to facilitate further exploitation and to maintain persistence. The hypothesis for this simulation is that the transfer of unauthorised tools, such as Remote Access Trojans (RATs), generates specific patterns in file creation, process execution, and network activity logs, which can be detected using sysmon and HELK.

The simulation utilises Cobalt Strike to transfer the Quasar RAT from a compromised system (WIN-LAB-02) to another machine within the network (WIN-LAB). The process involves leveraging the credentials obtained in previous simulations to conduct the

transfer, ensuring that the attacker maintains access to the compromised environment. The transferred file Quasar.zip is uploaded, extracted, and executed to enable further lateral movement capabilities. Figure 5-5 illustrates the attack sequence, starting with the tool upload, followed by the file extraction and execution on the target system. The detailed, step-by-step instructions of this simulation are outlined in Appendix A.

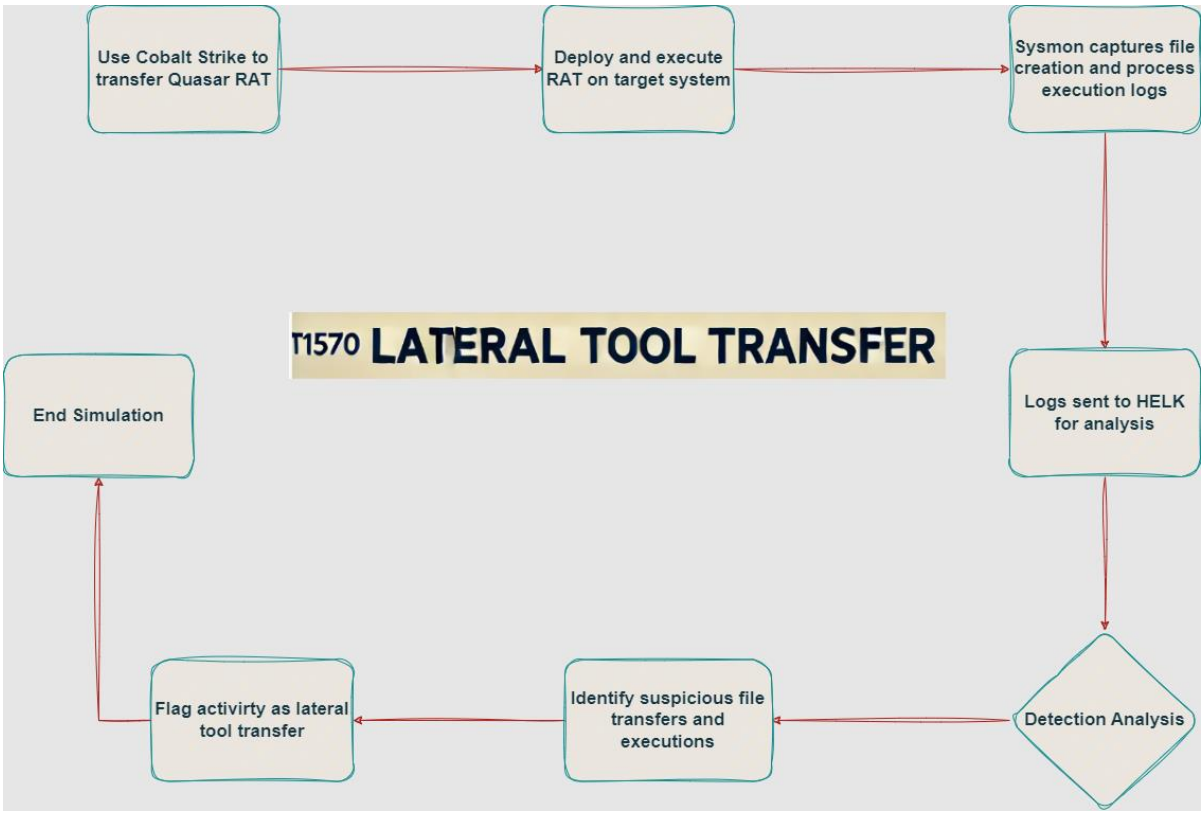


Figure 5-5: Lateral tool transfer overall process

Sysmon captures key events throughout the simulation, specifically focusing on file creation, process creation, and network connection events. These logs are analysed using HELK, which then identifies patterns associated with lateral tool-transfer activities. The analysis reveals distinct indicators of the Quasar RAT transfer, including the creation and execution of transferred files, which are flagged by HELK as potentially malicious because of their unexpected nature and context. The tool transfer activities are flagged as suspicious based on:

i. **Unusual file creation events**: The creation of Quasar.zip on the target system, particularly when linked to previously compromised credentials, is flagged as an anomaly due to its association with known malicious activities.

ii. **Process execution patterns**: The execution of transferred files, especially those initiated from non-standard directories or outside normal operational hours, is identified as suspicious and indicative of lateral movement attempts.

The simulation illustrates TaHiTI's ability to detect lateral tool transfer techniques through detailed monitoring and analysis of file and process creation logs. By identifying abnormal patterns associated with unauthorised tool transfers, TaHiTI differentiates routine administrative activities from potential security threats. This capability is crucial for preventing adversaries from deploying malicious tools that enable further network exploitation. The system successfully flags these activities as suspicious and distinguishing between malicious and legitimate file transfers is essential. System administrators often transfer tools and scripts as part of their regular maintenance tasks. Contextual analysis and whitelisting of authorised tools can help reduce false positives, ensuring that legitimate administrative activities are not unnecessarily flagged, while maintaining robust security against unauthorised tool transfers.

5.4.5. Simulation 5: Remote services (T1021.001)

The final simulation focuses on the Remote Services technique, specifically the use of the Remote Desktop Protocol (RDP) in conjunction with the Quasar remote access trojan (RAT), identified by the MITRE ATT&CK framework as T1021.001. This technique involves an APT leveraging RDP to gain persistent remote access to a target system using a RAT such as Quasar. The hypothesis for this simulation is that HELK will detect unauthorised RDP connections and the subsequent deployment of Quasar RAT, flagging these activities as indicative of lateral movement and remote access by APT. Figure 5-6 depicts the flow of events from the deployment of the Quasar RAT to the establishment of the RDP session and the remote control of the target system.

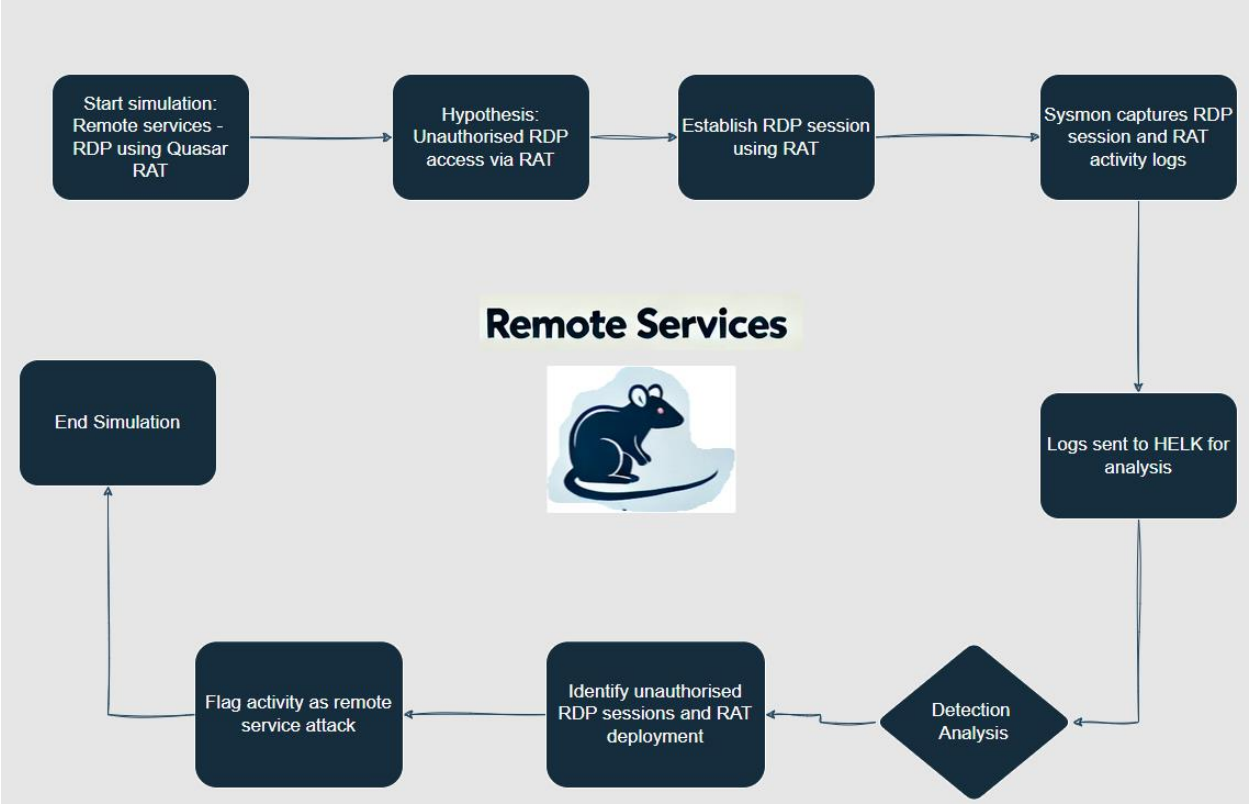


Figure 5-6: Remote services overall process

The simulation begins with the execution of the Quasar RAT on the compromised WIN-LAB system, which was initially breached through a lateral tool transfer attack from the previous simulation. The Quasar RAT runs as a background process in the system, enabling the attacker to establish a remote desktop session. This setup simulates the conditions under which an attacker uses RDP, facilitated by the Quasar RAT, to maintain persistent remote control over a compromised system. The detailed step-by-step application of this tactic is outlined in Appendix A. The sysmon logs capture key activities throughout the simulation, focusing on process creation, network connections, and file creation. HELK analyses these logs to detect the patterns associated with the use of remote services. The analysis identifies critical indicators of a remote services attack, including unauthorised RDP sessions, Quasar RAT deployment, and outbound connections to the attacker's command and control (C2) server. Remote service activities are flagged as suspicious based on the following factors:

i. **Unauthorised RDP session**: Sysmon logs capture the initiation of an RDP session, including details such as the user account used, source and destination IP addresses, and session duration. This session is flagged as suspicious due to the use of

compromised credentials, which are identified using the process described for the simulation discussed in Section 5.4.3.

ii. **Quasar RAT deployment**: The creation of a Quasar RAT executable on the WIN-LAB system is recorded, followed by its execution. HELK correlates these events with RDP sessions, indicating potentially malicious remote access.

iii. **Outbound connection to the C2 server**: HELK detects an outbound connection from the compromised system to the attacker's C2 server, established by Quasar RAT. This connection is flagged as highly suspicious, as it aligns with the known indicators of remote access trojans.

This simulation demonstrates TaHiTI's effectiveness in detecting complex remote service-based attacks. By correlating remote login events, process creation logs, and network activity, HELK provides a comprehensive view of the attack, effectively identifying the unauthorised RDP session and the subsequent deployment of the Quasar RAT. The analysis confirms HELK's ability to detect remote service techniques that adversaries use to maintain persistence and control over compromised systems. This capability is crucial for preventing further lateral movement and mitigating the risks associated with such sophisticated attacks. HELK effectively flags these activities as suspicious; however, distinguishing between legitimate and malicious RDP use still remains a challenge. RDP is frequently used by IT professionals for legitimate remote administrations. To reduce false positives, context-aware filtering, behavioural analysis, and whitelisting of known authorised remote connections can help differentiate between legitimate administrative actions and unauthorised remote access attempts.

5.5. Chapter summary

Chapter 5 explores the practical application of the TaHiTI framework through a series of controlled simulations aimed at evaluating its effectiveness in detecting lateral movement techniques within a simulated network environment. The chapter begins with an overview of tool selection and environment setup, both of which are carefully done to replicate real-world conditions. Tools such as Cobalt Strike, PowerShell, Quasar RAT, and sysmon are used for their proven ability to simulate advanced persistent threat (APT) tactics and generate actionable data for analysis. The core of the chapter focuses on the execution of five distinct simulations, each aligned with a specific technique from the MITRE

ATT&CK framework. These simulations are designed to rigorously test the ability of TaHiTI to detect and respond to various lateral movement strategies. The data generated from each simulation are aggregated and analysed using the HELK platform, which is instrumental in detecting patterns, anomalies and indicators of adversarial behaviour.

Through these structured simulations, this study demonstrates that a methodical approach to threat hunting, supported by robust tools and sophisticated data analysis, is effective in detecting complex attack vectors. Each simulation validated the hypothesis that TaHiTI, when integrated with HELK, can help to successfully identify lateral movement tactics. In the next chapter, the results of the simulations are evaluated and discussed within the context of the original TaHiTI threat hunting methodology.

Chapter 6 Results analysis and validation of TaHiTI

6.1. Introduction

This chapter presents a detailed analysis of the simulations discussed in Chapter 5 designed to evaluate the effectiveness of TaHiTI in detecting lateral movement attacks within a controlled virtual environment. The primary objective was to illustrate how TaHiTI's structured approach enables advanced threat detection capabilities compared to no monitoring and basic monitoring methods. To achieve this, each simulation was conducted across three monitoring levels: no monitoring, basic monitoring, and TaHiTI-enabled setup. This comparative approach clearly demonstrates TaHiTI's added value in identifying sophisticated lateral movement tactics.

The chosen simulations correspond to lateral movement techniques commonly identified in the MITRE ATT&CK framework. These include Remote system discovery, Internal spear-phishing, Pass-the-Hash (PtH) attacks, Lateral tool transfers, and Remote service abuse. These techniques represent common methods employed by advanced persistent threats (APTs) to move laterally within networks while evading detection. Each simulation focuses on the specific challenges of differentiating between benign and malicious activities within an organisational network. This chapter shows how moving from no monitoring to TaHiTI-enabled monitoring enhances detection accuracy, reduces false positives, and speeds up the recognition of lateral movement thanks to TaHiTI's structured, hypothesis-driven approach.

In each simulation, the phases of Initiate, Hunt, and Finalise guide the threat hunting process. 'Initiate' establishes a baseline of normal activities, 'hunt' targets deviations indicating potential threats, and 'finalise' consolidates findings to confirm or refute malicious activity. This chapter offers insights into the practical benefits of TaHiTI, reinforcing its necessity in dynamic cybersecurity environments by systematically highlighting detection gaps in unstructured monitoring approaches.

6.2. Analysis approach overview

The analysis of the simulations follows TaHiTI's three primary phases, namely Initiate, Hunt, and Finalise. During the Initiate phase, hypotheses are formulated for each

simulation, with specific indicators of compromise (IOCs) identified based on typical patterns for each lateral movement technique. This phase establishes the foundational assessment and observational tracking required for subsequent threat hunting analysis to observe expected behaviours in each scenario, simulating both legitimate and malicious activities within a corporate network environment. The Hunt phase involves executing the simulation and actively monitoring patterns consistent with the anticipated attack vectors. Simulation data are gathered from three distinct setups: no monitoring, basic monitoring, and the structured application of TaHiTI, to assess detection capabilities under varying levels of oversight. Lastly, in the Finalise phase, data is systematically analysed to identify deviations from baseline activities, which are essential for early threat detection, and the findings are documented to highlight TaHiTI's detection accuracy and efficiency. Each simulation is conducted under three distinct monitoring conditions or tiers to provide a rigorous comparative analysis:

- **No monitoring:** This condition operates without active monitoring or alert systems. This level provides a reference for understanding how lateral movement activities progress undetected in the absence of monitoring tools. Observations from this phase underscore the potential risks inherent in unmonitored environments.
- **Basic monitoring**: At this level, basic monitoring tools capture system and network events, simulating a typical environment with standard security practices in place. While this setup offers partial visibility into system actions, it lacks the structured analytic depth required to distinguish between benign and malicious activities reliably.
- **TaHiTI-enabled detection**: This final level leverages the TaHiTI methodology, which introduces a structured, hypothesis-driven approach to threat detection. Using the Initiate, Hunt, and Finalise phases, TaHiTI's systematic process facilitates the proactive identification of lateral movement techniques by establishing behavioural benchmarks.

Each simulation is conducted across these three tiers, progressing from unmonitored activities to advanced, structured threat detection under TaHiTI. The same activities are performed in all three simulation types, which allows for a direct comparison of the impact the various monitoring approaches has on the outcomes. By comparing these outcomes across different monitoring levels, the analysis demonstrates TaHiTI's strengths in pinpointing lateral movement attempts that might otherwise go unnoticed. This approach

not only provides a clear framework for evaluating the effectiveness of TaHiTI but also reinforces the necessity of structured threat detection methodologies in dynamic network environments.

6.3. Simulations analysis

This section presents a detailed analysis of the simulations conducted to evaluate the effectiveness of TaHiTI for detecting various lateral movement techniques. Each simulation corresponds to a specific tactic outlined in the MITRE ATT&CK framework, encompassing activities such as remote system discovery, internal spear-phishing, PtH combined with WMI, lateral tool transfers, and remote service abuse. For each simulation, the findings are discussed across three tiers of monitoring: no monitoring, basic monitoring, and TaHiTI-enabled detection (structured approach). By sequentially examining each simulation and assessing it at these monitoring levels, this section illustrates TaHiTI's role in differentiating benign activities from potential security threats. The analysis showcases specific examples of logged events, detailing how TaHiTI's methodology helps address ambiguities in traditional monitoring to reduce false positives and improve response times. Appendix A contains numerous screenshots of some data collected during the simulations.

6.3.1. Analysis of simulation 1: Remote system discovery

The objective of the first simulation is to test TaHiTI's ability to detect remote system discovery activities, a reconnaissance technique commonly used by attackers to identify network resources. This simulation evaluates the effectiveness of TaHiTI in distinguishing between benign administrative network scans and reconnaissance activities associated with lateral movement attacks.

In the non-monitoring stage, remote system discovery activities go completely undetected. The simulation involves executing the *net group "Domain Computers" /domain* command using PowerShell on a compromised machine. Sysmon records this activity as a typical process creation log (Event ID 1) under routine conditions. However, without a monitoring system in place, no alerts are generated and these reconnaissance actions remain indistinguishable from benign system interactions. This baseline scenario

highlights the risk that attackers can perform reconnaissance without monitoring, emphasising the need for proactive threat detection.

During the basic monitoring stage, slight improvements are observed. When executing remote system discovery commands, process creation logs (Event ID 1) are occasionally flagged as isolated events. For example, PowerShell commands are associated with *cmd.exe* and *net.exe* trigger entries, but they lack the analytic depth to link them back to potential reconnaissance. Network connections to the domain controller, captured by Event ID 3, sporadically appear in the logs; however, no context ties these interactions to any malicious activity. Limited visibility fails to provide actionable insights, as benign administrative scans appear similar to potential attacks. This stage underscores the challenges of relying solely on isolated event logs, in which critical activities blend into typical network noise. Figure A-12 in Appendix A shows sysmon logs, particularly Event ID 1 for process creation and Event ID 3 for network connections, and capture calls for *cmd.exe* and *net.exe.* HELK is later used to aggregate and analyse these logs within the TaHiTI process.

When following the TaHiTI methodology, threat hunting activities are structured to focus on identifying deviations in established behavioural patterns. During the ‘Initiate’ phase, a behavioural baseline for administrative tasks, such as network discovery and defining expected command sequences and patterns, is established. In the ‘Hunt’ phase, the process flow from *cmd.exe* to *net.exe* is flagged as atypical based on the observed deviations from no monitoring. For instance, Event ID 1 (process creation) and Event ID 3 (network connection) are correlated to identify an anomalous sequence indicative of a reconnaissance attempt. This structure enables TaHiTI to connect these log events and distinguish them from legitimate admin tasks, marking the event as high-risk due to atypical command patterns and non-standard timestamps. (see Figure A-12 Appendix A)

This simulation illustrates how TaHiTI’s structured methodology enhances threat detection by distinguishing between legitimate and malicious behaviours through pattern recognition. Without this framework, standard system monitoring struggles to accurately detect reconnaissance activities, often mistaking them for routine actions. The correlation of log events, such as process and network connection logs, enables precise detection, thereby confirming its effectiveness against stealthy reconnaissance attacks. These findings reinforce the necessity of a structured approach such as TaHiTI, which

proactively identifies threats by observing deviations in known behaviours. Table 6-1 provides a summary of detection capabilities across no monitoring, basic monitoring, and TaHiTI-enabled stages, showing a marked improvement in recognising reconnaissance behaviours when each new level of monitoring is deployed.

Table 6-1: Summary of detection for remote system discovery

Technique	Activity	No monitoring	Basic monitoring	TaHiTI-enabled detection
Remote System Discovery	Execution of net group "Domain Computers"	Not detected	Occasional alerts	Consistently flagged as reconnaissance
	Process Creation (*cmd.exe, net.exe*)	No alerts	Limited, sporadic alerts, indistinguishable from admin tasks	Patterns identified in sequence
	Network Connection to Domain Controller	Overlooked, unmonitored	Minor alerts, lacks baseline context	Flagged as atypical activity

Unlike the no-monitoring and basic monitoring setups, which fail to contextualise remote system discovery actions, TaHiTI consistently detects patterns indicative of malicious discovery attempts. This finding aligns with research by Kushwaha *et al.* (2022) and Kapoor *et al.* (2021), which highlights the efficacy of structured methodologies in detecting reconnaissance within APT campaigns. By establishing behavioural baselines, TaHiTI distinguishes between legitimate administrative actions and unauthorised reconnaissance, thus reinforcing its value in proactive threat detection. Building on these insights, the next simulation explores TaHiTI's approach to detecting social engineering techniques, specifically through internal spear-phishing detection.

6.3.2. Analysis of simulation 2: Internal spear phishing

The second simulation evaluates TaHiTI's ability to detect and differentiate internal spear-phishing activities from regular user interactions. This simulation specifically targets the MITRE ATT&CK technique T1534, which is internal spear phishing, and T1566.001, which is spear phishing with an attachment. These methods are often used to gain

network access by tricking users into engaging with malicious attachments, leading to actions such as command execution and credential theft. The simulation aims to demonstrate how effectively the framework helps to identify spear-phishing attempts among typical email-based activities, particularly in environments with a high frequency of document handling and email communication.

In environments without monitoring mechanisms, spear-phishing activities remain indistinguishable from normal user behaviour. For example, users can open simulated phishing emails containing malicious Excel attachments. Although this action triggers process creation logs that are *Excel.exe* for executing embedded commands, no alerts are generated. Without any alerting mechanism, these logs remain unflagged, as shown in Appendix A, Simulation 2. The absence of monitoring renders the system vulnerable, allowing attackers to execute commands from attachments with no visible indicators of compromise. This lack of detection highlights a significant risk in unmonitored environments where sophisticated phishing attacks are difficult to identify.

With basic monitoring in place, user activities involving email attachments are intermittently observed. For example, when users open malicious Excel attachments, basic monitoring captures isolated events such as the initiation of PowerShell commands (Event ID 4688) within Excel. However, these alerts lack context and do not connect back to the email source, making it challenging to flag them reliably as a phishing attempt. Appendix A, Figure A-15 illustrates a sample log from HELK, where the PowerShell process is logged, but without sufficient linkage to the initiating email activity. The scattered nature of these alerts makes it challenging to distinguish spear-phishing attempts from normal email interactions, resulting in sporadic and inconsistent detection that often misses the full attack chain. Furthermore, some network traffic related to command and control (C2) connections is sporadically flagged, but remains ambiguous without correlation to the original spear-phishing trigger. This inconsistency highlights the limitations of basic monitoring, as legitimate and malicious interactions often appear similar without an advanced analytical framework.

Upon initiating TaHiTI's structured process, the detection accuracy improves significantly. During the 'Initiate' phase, no monitoring of behavioural patterns for users' email and document interactions, which become critical in the following phases, is established. In the 'Hunt' phase, TaHiTI specifically monitors user engagement with email attachments

and notes deviations from typical patterns, such as immediate PowerShell execution upon opening an Excel file. This phase's structured analysis pinpoints anomalies by focusing on event sequences, including process initiation and network connections that follow email interactions. For instance, the execution of PowerShell commands after opening a document is flagged as suspicious because of its deviation from normal user behaviour. Appendix A, Figure A-18 displays how TaHiTI correlates with these interactions, revealing an abnormal sequence that deviates from standard email behaviours. In the 'Finalise' phase, these observations are consolidated, identifying this potential spear-phishing attempt as a high-risk event. This simulation demonstrates the advantage of TaHiTI in differentiating spear-phishing attempts from benign document interactions by leveraging a structured and context-aware approach. Table 6-2 provides a comparative summary of detection outcomes across monitoring levels for remote system discovery.

Table 6-2: Internal spear phishing detection analysis across monitoring levels

Technique	Activity	No Monitoring	Basic Monitoring	TaHiTI-Enabled Detection
Internal spear phishing	Malicious email receipt	Not detected	Overlooked as regular email	Detected as anomalous based on sender patterns
	Attachment execution (malicious Excel file)	No alerts	Limited visibility	Detected due to atypical sequence of events
	Process creation (Excel.exe, PowerShell)	No alerts; blends in	Occasional, isolated alerts	Correlated to reveal phishing activity patterns
	Network connection (C2)	Unmonitored	Basic alerts without context	Flagged as high-risk due to unusual IP connections

This simulation highlights TaHiTI's ability to identify spear-phishing indicators that are otherwise obscured by normal user activities, such as frequent email interactions and document handling. Without TaHiTI, detecting spear-phishing remains challenging because these activities appear similar to regular user actions. While basic monitoring sporadically identifies anomalies, it lacks the necessary context to flag spear-phishing

attempts consistently. TaHiTI's structured methodology, focusing on deviations from established behaviour patterns, enables precise detection of internal spear-phishing attempts, addressing the detection challenges highlighted in research by Bhadane and Mane (2019). The next simulation investigates how TaHiTI handles advanced lateral movement tactics, including credential misuse and command execution in network segments.

6.3.3. Analysis of simulation 3: Pass-the-Hash (PtH) and Windows Management Instrumentation (WMI)

TaHiTI's capacity to detect sophisticated credential and remote execution techniques, specifically PtH and WMI abuse methods, is investigated in the third simulation. PtH allows attackers to authenticate within a network using NT LAN Manager (NTLM) hashes without knowing the actual password, whereas WMI enables remote command execution, aiding in lateral movement. NTLM is a suite of Microsoft security protocols that provides authentication, integrity, and confidentiality and is commonly used in corporate environments for authentication in networks that are not integrated with Kerberos (Boulila & Dacier, 2023). This simulation demonstrates how effectively TaHiTI detects and distinguishes these stealthy techniques from legitimate administrative actions, providing early detection capabilities in environments in which such tactics might otherwise evade basic monitoring systems.

In the non-monitoring environment, PtH and WMI actions remain completely unmonitored, enabling attackers to conduct credential-based lateral movements without hindrance. For instance, the simulation includes executing commands via WMI on a compromised machine (WIN-LAB), utilising extracted NTLM hashes to access other networked systems without a password. Since there is no monitoring or alert system, activities such as these blend into routine administrative tasks. No alerts or flags indicate unauthorised credential use or remote command execution, underscoring the risks inherent in environments lacking proactive detection capabilities (see Appendix A, Simulation 3).

Basic monitoring provides limited insight into PtH and WMI-related activities. For example, while executing remote commands on WIN-LAB using WMI, basic monitoring sporadically flags Event ID 4688 (which indicates process creation using WMI command

execution) as suspicious. Additionally, authentication events associated with NTLM hashes occasionally trigger minor alerts under Event ID 4624 (successful login). However, these alerts lack sufficient context to correlate credential anomalies directly with PtH or WMI abuse. For example, Event ID 4688 may be flagged because of the WMI's remote execution, but without a clear link to malicious activities, this event appears similar to legitimate administrative sessions. Appendix A, Figure A-22, illustrates a sample log entry in which an unauthorised credential usage event is flagged. Consequently, while individual alerts appear, they do not consistently signal potential attacks because of the absence of structured analysis and contextual correlations.

With TaHiTI in use, the detection becomes far more robust. During the 'Initiate' phase, TaHiTI establishes a normal baseline for credential usage, specifically monitoring for unusual patterns in authentication attempts and remote command executions. For example, TaHiTI differentiates between legitimate and suspicious WMI activities by noting deviations from established login patterns and execution behaviours. In the 'Hunt' phase, TaHiTI tracks anomalies in credential and WMI use, such as NTLM hash-based authentications that deviate from standard password logins. When NTLM hashes are used across systems within short intervals, TaHiTI flags these sequences as suspicious, based on their frequency and atypical credential usage patterns. This structured detection identifies PtH attempts and highlights command executions linked to unauthorised credentials. Appendix A, Figure A-25, provides an example log showing TaHiTI's identification of unusual process chains stemming from hash-based authentication, which it flags as suspicious.

The 'Finalise' phase consolidates these observations, generating a high-confidence alert indicating PtH and WMI abuse due to unusual patterns in credential use and remote command execution. TaHiTI's correlation between credential-based authentication and remote WMI actions provides clear evidence of lateral movement, allowing timely detection and intervention. Table 6-3 summarises the findings across no monitoring, basic monitoring, and TaHiTI-enabled detection levels for PtH and WMI-based lateral movement.

Table 6-3: PtH and WMI detection analysis across monitoring levels

Technique	Activity	No monitoring	Basic monitoring	TaHiTI-enabled detection
Pass-the-Hash (PtH)	Credential Dumping	Undetected, blends with admin	Rarely flagged; logs buried in admin activities	Detected as suspicious due to anomalous credential patterns
	Authentication Using Hash	No visibility	Intermittent alerts, lacks event correlation	Consistently flagged as atypical authentication method
Windows Management Instrumentation (WMI)	Remote Command Execution	Overlooked as routine admin activity	Occasional alerts, indistinct from legitimate admin commands	Detected as anomalous due to abnormal WMI patterns
	Network Activity Linked to WMI	Not flagged	Limited alerts without correlation	Consistently identified as malicious due to unusual IP usage

This simulation illustrates TaHiTI's efficacy in detecting stealthy lateral movement techniques, such as PtH and WMI abuse, which often bypass traditional monitoring systems. Without TaHiTI, these actions are either missed entirely or flagged inconsistently, as they closely mimic legitimate administrative tasks. Basic monitoring occasionally identifies individual anomalies; however, without contextual linkage, it fails to recognise these actions as lateral movement attempts. TaHiTI's structured methodology enables precise detection by focusing on atypical credential use and command execution patterns, underscoring the value of the system in securing corporate networks against sophisticated threats.

This simulation aligns with findings by Elgohary and Abdelbaki (2022), who underscore the importance of Windows API monitoring in detecting lateral movements involving credential tools such as Mimikatz. These results further reinforce the value of TaHiTI's structured approach, particularly in distinguishing between standard administrative actions and lateral movement tactics that exploit legitimate tools for malicious purposes. This validation confirms the role of TaHiTI as a critical asset in network security, enhancing its applicability in complex cybersecurity scenarios. Transitioning from this simulation, the next analysis explores TaHiTI's ability to detect lateral tool transfers,

particularly focusing on unauthorised file transfers and the persistence of remote access tools (RATs) such as Quasar within the network.

6.3.4. Analysis of simulation 4: Lateral tool transfer

With the fourth simulation, TaHiTI's effectiveness in detecting lateral tool transfers within a network, specifically the movement and deployment of remote access tools (RATs) such as Quasar, is evaluated. This simulation focuses on the MITRE ATT&CK technique T1570, examining how effectively TaHiTI distinguishes malicious file transfers and process executions from routine network activities. The objective is to detect unauthorised file transfers, particularly those associated with RAT deployment, which attackers often use to maintain persistence and remote access.

When no monitoring is considered, lateral tool transfers remain entirely unmonitored. For instance, the attacker transfers the Quasar RAT in a compressed Quasar.zip file from one compromised machine (WIN-LAB-02) to another target system within the network (WIN-LAB) without triggering any alerts. The lack of monitoring allows file creation, extraction, and RAT deployment processes to proceed undetected seamlessly blending with legitimate network file transfers. This unmonitored environment underscores the risk posed by RATs, which attackers can use for remote control and persistence if detection mechanisms are absent (see Appendix A, Simulation 4).

With basic monitoring enabled, limited visibility into file creation and network traffic is established. For example, sysmon's Event ID 11 (file creation) flags the presence of the Quasar.zip file on WIN-LAB when it is copied from WIN-LAB-02. Similarly, Event ID 3 (network connection) logs the outbound connection attempts made by the RAT onto a command and control (C2) server. However, these events are isolated and lack contextual analysis, making it challenging to identify them as unauthorised. For instance, while Event ID 11 highlights file creation, basic monitoring does not correlate with the deployment of Quasar, as these activities can mimic typical administrative file transfers. RATs such as Quasar are commonly used for legitimate administrative tasks, such as remote troubleshooting and system maintenance, further complicating the identification of malicious intent when only isolated logs are reviewed without a deeper context (Ibrahim & Thanoon, 2022). Appendix A, Figure A-27, includes a sample log entry in which file

creation events are noted. Consequently, alerts remain inconsistent and insufficient to distinguish lateral tool transfer as a high-risk event.

The structured approach of TaHiTI provides comprehensive detection capabilities. During the ‘Initiate’ phase, TaHiTI establishes a baseline for typical file transfers and process executions within the network. This baseline allows TaHiTI to differentiate legitimate administrative tasks from potentially malicious lateral tool transfers by focusing on anomalies related to unauthorised file paths and unusual timing patterns. In the ‘Hunt’ phase, TaHiTI continuously monitors deviations from standard behaviour, such as unexpected file creation associated with Quasar.zip and RAT’s process creation following file extraction. For example, sysmon Event ID 1 (process creation) captures the initiation of Quasar.exe after the compressed file is extracted, thus triggering further analysis. TaHiTI also detects the RAT’s network traffic (captured in Event ID 3) as anomalous due to connections to non-standard IP addresses. This correlation of file, process, and network events enables robust identification of lateral tool transfers, clearly marking the deployment of Quasar as suspicious. During the ‘Finalise’ phase, TaHiTI consolidates these findings, flagging the entire sequence of events from file transfer to process creation and network connection as a high-risk lateral tool transfer. By correlating the initial transfer of Quasar.zip with subsequent process creation and C2 traffic, TaHiTI distinguishes this activity as suspicious, alerting the system to potential RAT-based persistence. Table 6-4 presents a comparison across no-monitoring, basic monitoring, and TaHiTI-enabled detection of lateral tool transfer activities.

Table 6-4: Lateral tool transfer detection analysis across monitoring levels

Technique	Activity	No monitoring	Basic monitoring	TaHiTI-enabled detection
Lateral tool transfer	File Creation for Tool Transfer	Not flagged; appears routine	Occasionally detected without context	Flagged due to atypical file paths and timing
	Execution of Remote Access Tool (RAT)	Overlooked; mimics admin actions	Rarely noted; lacks correlation	Identified as suspicious due to specific RAT patterns
Network Activity from RAT	Outbound C2 Communication	Undetected, appears routine	Basic alerts on outbound connections, lacks correlation	Consistently flagged; identifies patterns linked to RAT activity

Technique	Activity	No monitoring	Basic monitoring	TaHiTI-enabled detection
Process Activity	Process Spawned by RAT	Not visible	Minimal alerts, no RAT origin context	Detected and correlated with tool transfer

This simulation underscores TaHiTI's structured approach to detecting lateral tool transfers that would otherwise evade traditional monitoring systems. Without TaHiTI, RAT-related activities blend into routine file transfers and network communication, allowing attackers to establish remote access without raising suspicion. Basic monitoring occasionally flags events, but fails to correlate them into a recognisable threat pattern. TaHiTI's ability to correlate file creation, process initiation, and network connection logs provides a comprehensive view, facilitating the early detection of unauthorised tool transfers. These findings align with those of Palacin (2021) and Tiwary (2023), who highlight the importance of monitoring sysmon logs for the effective detection of lateral tool transfers. Additionally, Smiliotopoulos *et al.* (2022) and Ibrahim and Thanoon (2022) underline the persistent threat posed by RATs, validating TaHiTI's utility in differentiating benign from malicious transfers. The structured approach proves crucial for early detection, showcasing TaHiTI's role as an effective monitoring solution for lateral tool transfer attacks. The final simulation further explores TaHiTI's ability to detect unauthorised remote services, focusing on RDP connections facilitated by Quasar RAT.

6.3.5. Analysis of Simulation 5: Remote services using Quasar RAT

The penultimate simulation investigates TaHiTI's utility in identifying unauthorised remote access established through remote desktop protocol (RDP) connections controlled by the Quasar remote access tool (RAT). This simulation targets the MITRE ATT&CK technique T1021.001 (remote services), and aims to distinguish legitimate RDP activity from malicious connections that attackers may use for lateral movement and persistence. The objective is to assess how effectively TaHiTI can detect RAT-based remote access attempts that closely mimic authorised administrative actions within the network.

In the non-monitoring environment, remote services facilitated by the Quasar RAT proceed without any alerts or detections. For instance, the attacker uses the Quasar RAT to initiate an RDP session from WIN-LAB-02 to WIN-LAB, maintaining control over WIN-

LAB through the RAT without generating any logs that could indicate malicious activity. This lack of visibility enables an attacker to execute commands remotely and is completely undetected. The absence of monitoring in this phase underscores a key vulnerability: unauthorised remote access can be maintained without raising suspicion, even when attackers are actively executing commands on compromised systems (see Appendix A, Simulation 5).

With basic monitoring enabled, limited insights into remote service activity become available, although they are not sufficient to identify this as malicious. Sysmon's Event ID 1 (process creation) logs the initiation of RDP sessions and Event ID 3 (network connection) captures the outbound traffic associated with the RDP activity of the Quasar RAT. However, due to the lack of correlation between these events and specific RAT patterns, alerts remain sporadic and isolated. For example, Event ID 3 flags outbound connections from WIN-LAB-02 to WIN-LAB, but lacks the context to associate this with unauthorised RAT-driven RDP connections. This limitation means that, while unusual outbound traffic may occasionally be flagged, it fails to conclusively identify RAT-based persistence as suspicious. Thus, basic monitoring provides only superficial visibility of RDP connections, leaving RAT-facilitated activities uncorrelated and largely undetected. (see Appendix A, Figure A-32).

TaHiTI's structured approach, in contrast, enables a detailed and contextualised analysis of remote services. During the 'Initiate' phase, TaHiTI establishes patterns for legitimate RDP sessions, including usual timings, IP addresses, and process behaviours associated with authorised administrative actions. This no monitoring understanding allows TaHiTI to differentiate legitimate RDP usages from suspicious RAT-driven connections. In the 'Hunt' phase, TaHiTI actively monitors deviations from the established RDP patterns. For instance, TaHiTI detects an unusual RDP session initiated by Quasar RAT from WIN-LAB-02 to WIN-LAB. Sysmon Event ID 1 (process creation) captures the RDP session launch, while Event ID 3 (network connection) logs reveal outbound traffic towards a non-standard IP address, typically associated with C2 activities. TaHiTI correlates these specific processes and network events to the presence of an anomalous remote access session, marking it as high-risk due to its deviation from typical RDP behaviour.

During the 'Finalise' phase, TaHiTI consolidates the findings, flagging the unauthorised RAT-driven RDP session as a critical threat. By correlating process creation and network

activity data, TaHiTI identifies the Quasar RAT's persistence mechanism through RDP, thus distinguishing it from legitimate administrative RDP sessions. This end-to-end analysis not only provides visibility into the RAT's activities but also highlights the patterns that differentiate RAT-based remote services from normal network management operations (see Appendix A, Figure A-34).

Table 6-5 presents a comparative analysis of detection levels across baseline, basic monitoring, and TaHiTI-enabled environments for RDP activities linked to the Quasar RAT.

Table 6-5: Remote services detection analysis across monitoring levels

Technique	Activity	No Monitoring	Basic Monitoring	TaHiTI-Enabled Detection
Remote services	RDP Session Initiation	Unmonitored; viewed as routine	Sporadic alerts without context	Identified as unauthorised based on RAT patterns
	RAT-Driven RDP Persistence	Overlooked; mimics admin actions	Rarely flagged, lacks correlation	Detected due to RAT-specific behaviour patterns
Network activity from RAT	Outbound RAT-controlled RDP connections	Unobserved; routine traffic	Basic alerts on outbound connections, no correlation	Consistently identified as unauthorised; recognises RAT-linked IP connections
Process execution	RAT-Induced processes and commands	Not visible	Minimal alerts, isolated process events	Detected with context; links processes to unauthorised RDP sessions

This simulation supports the validity of TaHiTI's structured approach for identifying unauthorised remote services, particularly RAT-driven RDP connections that would otherwise bypass standard monitoring. In the absence of TaHiTI, remote access via Quasar RAT remains indistinguishable from legitimate administrative tasks, allowing attackers to maintain persistent control over compromised systems. Basic monitoring offers limited visibility, but lacks a correlation between events, which leads to RAT-associated activities not being flagged effectively. However, TaHiTI can correlate RDP session initiation, network traffic, and process execution logs to reveal the malicious nature of the remote access session. This simulation demonstrates the critical value of

TaHiTI in distinguishing between authorised and unauthorised remote access and enhancing network security by detecting sophisticated persistence mechanisms.

This simulation also corroborates the findings of Bai *et al.* (2019) and Ashfaq and Malik (2022), who discuss the challenges inherent in detecting RDP-based lateral movement due to encrypted communications and legitimate credentials. These studies underscore the need for continuous monitoring and sophisticated analysis techniques, both of which are provided by TaHiTI. By highlighting deviations from established baselines, TaHiTI demonstrates its capability to detect complex remote service attacks, further validating its utility. Building on the detailed findings from each simulation, the next section presents a comparative analysis that synthesises these insights, highlighting TaHiTI's critical role in enhancing the detection of lateral movements.

6.4. Comparative analysis and summary of findings

In this section, the findings from the five simulations presented in this chapter are considered by comparing non-monitoring, basic monitoring, and TaHiTI-enabled monitoring approaches. Each simulation underscores the critical enhancements that TaHiTI introduces in detecting lateral movement techniques from identifying reconnaissance behaviours to differentiating unauthorised remote access from legitimate administrative actions. The comparative insights illustrate TaHiTI’s impact on threat detection accuracy, particularly in reducing false positives and providing a comprehensive context for complex threat behaviours.

In the **no-monitoring simulations**, none of the lateral movement activities raised alerts. Whether attackers conduct network discovery, spear-phishing, or established persistent remote sessions, these actions blend seamlessly with regular user activities, highlighting the vulnerabilities of unmonitored environments. The absence of monitoring means that the simulated attacker could execute these tactics undetected, posing significant risks to the security of the system.

Basic monitoring, incorporating standard logging and event capture tools, such as sysmon, introduced minimal detection improvements. This setup occasionally flags anomalous events, such as PowerShell executions or unexpected network connections. However, without correlating these events with specific threat behaviours or

distinguishing benign from malicious actions, the detection remains unreliable. For instance, while certain process creation events or network connections are flagged, they lack the context to identify them as components of an attack chain, leading to inconsistent and often inconclusive alerts. Basic monitoring failed to provide a structured response, especially in more complex techniques, such as PtH and WMI abuse, where malicious activities closely mimic legitimate tasks.

With **TaHiTI-enabled detection**, the structured methodology that consists of the Initiate, Hunt, and Finalise phases made detailed, context-aware monitoring possible, thereby enhancing the detection capabilities of the monitoring system. In each simulation, TaHiTI differentiated malicious activities from benign actions by leveraging baselines and correlating event patterns. For example, in the spear-phishing simulation, TaHiTI tracked a typical sequence from email receipt to command execution, pinpointing suspicious behaviours that would otherwise be misinterpreted as routine email actions. The consistent ability of the framework to detect nuanced deviations from established baselines across all simulations underscores its effectiveness in detecting advanced lateral movement tactics.

This comparative analysis highlights three central findings regarding the effectiveness of TaHiTI in lateral movement detection. Firstly, TaHiTI consistently identified nuanced indicators of compromise overlooked by basic monitoring, particularly in scenarios involving multistage attacks. This is evident in the remote services simulation, where TaHiTI identified unusual RDP sessions linked to Quasar RAT in which standard monitoring systems flagged sporadically without context.

Secondly, basic monitoring systems frequently generate false positives due to a lack of contextual awareness, which often results in alert fatigue and inefficiency. TaHiTI mitigated this by correlating activities such as email-triggered PowerShell executions with established behavioural baselines, thereby reducing unnecessary alerts and focusing attention on genuine threats.

Finally, TaHiTI’s hypothesis-driven approach allows it to recognise multistage attack patterns and identify the relationships between seemingly discrete actions. In the lateral tool transfer simulation, TaHiTI connected file creation with process execution and outbound network activity, thus recognising the full scope of Quasar RAT deployment.

This correlation capability underscores the advantage of TaHiTI in detecting and responding to complex attack tactics.

Table 6-6, summarises the findings across all simulations, contrasting the detection efficacy of the no monitoring, basic monitoring, and TaHiTI-enabled setups. This summary provides a consolidated view of TaHiTI's contributions to threat detection.

Table 6-6: Comparative analysis summary

Simulation technique	Event/Activity	No monitoring	Basic monitoring	TaHiTI-enabled detection
Remote System Discovery	Network Enumeration execution of "net group 'Domain Computers'"	Undetected	Sporadically flagged, lacks context	Consistently detected; recognised as reconnaissance behaviour
Internal Spear Phishing	Malicious Attachment Execution	Undetected	Occasional isolated alerts	Identified as spear-phishing via atypical email-to-command patterns
PtH & WMI	Credential Use and Command Execution of WMI	Not visible	Inconsistent alerts, no pattern	Detected with correlation of credentials and WMI activity
Lateral Tool Transfer	RAT File Transfer	Undetected	Rarely flagged, no tool correlation	Consistently identified as lateral tool transfer through file patterns
Remote Services with RAT	RDP Sessions initiated by RAT	Undetected	Basic alerts on RDP sessions	Flagged as high-risk with correlation to RAT presence

This comparative analysis validates the role of TaHiTI as a critical enhancement to traditional monitoring. Baseline setups expose networks to high risks, with attackers being able to conduct lateral movement activities undetected. Basic monitoring is a clear improvement as it introduces event-level visibility, but it still falls short of recognising complex behaviours or correlating events within an attack sequence, which leads to gaps in detection.

The structured phases of TaHiTI directly address these limitations. The ‘Initiate’ phase establishes patterns of expected user and administrative behaviours, providing a baseline against which deviations are measured. The ‘Hunt’ phase then actively seeks anomalies in these patterns by applying a detailed context to detect malicious behaviours. Finally, the ‘Finalise’ phase consolidates and correlates alerts to draw connections across seemingly isolated events, effectively reducing false positives and enhancing detection precision. Through these structured phases, TaHiTI demonstrates its effectiveness in proactively detecting and mitigating lateral movement attacks that would otherwise remain hidden within regular network activities.

The comparative analysis confirms that TaHiTI not only improves detection rates but also provides critical contextual insights that elevate threat-hunting strategies beyond standard monitoring capabilities. This analysis highlights TaHiTI’s structured approach as essential for identifying and responding to complex lateral movement techniques in real-time, affirming its role as a powerful tool for advancing cybersecurity frameworks.

6.5. Chapter summary

This chapter presents an analysis of the effectiveness of the TaHiTI methodology for detecting lateral movement techniques in a simulated environment. Through a series of five simulations, TaHiTI’s structured, phased approach, which comprises the Initiate, Hunt, and Finalise stages, is compared to approaches that feature no monitoring, as well as approaches that involve traditional monitoring. The TaHiTI-enabled simulations demonstrate improvements in detection reliability and accuracy across all of the examined scenarios, highlighting its worth as a threat hunting framework. In the next, and final, chapter, the conclusion of this study is presented.

Chapter 7 Summary and conclusion

7.1. Introduction

This study investigates the critical challenge of lateral movement attacks within organisational networks, focusing on the application of a structured threat hunting methodology to improve detection efforts. Lateral movement, a key tactic used by APTs, enables attackers to navigate compromised systems, increase privileges, and access sensitive data while avoiding detection. These attacks, which are often undetected for long periods, pose significant risks to data integrity, operational stability, and organisational reputation. In this study, the Threat Hunting and Intelligence-Driven Investigation (TaHiTI) methodology was applied within a controlled virtual environment in order to examine the effectiveness of proactive threat hunting in identifying lateral movement activities. Simulations were carried out using the HELK platform, replicating real-world attack scenarios to test and validate the methodology. Key findings of the study highlight the critical role of hypothesis-driven threat hunting in reducing attacker dwell time and thereby potentially mitigating the impact of lateral movement attacks. The study demonstrates how integrating threat intelligence into a structured threat hunting framework improves the ability to detect APTs and lateral movement activities.

7.2. Summary of the study

This study provides a comprehensive exploration of lateral movement attacks within cybersecurity, emphasising the application of TaHiTI methodology to enhance detection and mitigation efforts. Lateral movement attacks, a critical phase in the lifecycle of APTs, pose significant challenges due to their stealthy and prolonged nature. The study was structured to systematically investigate these challenges, focusing on the detection and proactive response to activities of lateral movement within organisational networks.

The study is organised into seven chapters, each of which contributes to overarching research objectives. Chapter 1 introduces the study and presents its research problems, objectives, and structure. The criticality of lateral movement in cyberattacks is highlighted, and its prevalence and the need for advanced detection methodologies is noted. The central research question, **"How can a threat hunting methodology be effectively**

applied to detect lateral movement attacks within organisational networks?", is introduced and forms the foundation of the study.

Chapters 2 and 3 provide a theoretical framework for the remainder of the study. Chapter 2 examines advanced persistent threats with a focus on the tactics, techniques, and procedures (TTPs) that allow lateral movement. This chapter underscores the role of lateral movement in allowing attackers to traverse networks and access critical resources. Chapter 3 expands on this by exploring threat hunting as a proactive cybersecurity measure. The chapter details the evolution of threat hunting methodologies, emphasising the importance of reducing attacker dwell time and highlighting the integration of threat intelligence within structured hunting strategies.

Chapter 4 describes the research methodology, detailing the design and configuration of a controlled laboratory environment to simulate lateral movement attacks. This chapter outlines the use of a hypothesis-driven approach to threat hunting utilising the TaHiTI methodology as a framework to detect and mitigate lateral movement activities.

Chapters 5 and 6 focus on the setup, implementation and analysis of simulations aimed at investigating the validity of TaHiTI. Chapter 5 describes the execution of various lateral movement techniques within a simulated environment and tests the effectiveness of TaHiTI in identifying attack scenarios. Tools such as PowerShell, Cobalt Strike, and Quasar RAT are utilised, with data collected and analysed using the HELK platform. Chapter 6 presents an in-depth analysis of the simulation results, demonstrating the strengths of a hypothesis-driven threat hunting framework. The findings validate the TaHiTI methodology as an effective approach for proactively detecting lateral movement attacks, enhancing detection accuracy, and reducing false positives. This chapter synthesises the key findings of the study, reflecting on the achievement of its objectives and setting the stage for further exploration. By addressing the complexities of lateral movement attacks, this study provides both theoretical and practical contributions to the field of cybersecurity. The structured approach adopted highlights the critical role of hypothesis-driven threat hunting in reducing dwell time and potentially helping to mitigate advanced threats. The next section focuses on the specific objectives of this study and details its impact on both theoretical understanding and practical applications in the domain of cybersecurity.

7.3. Contribution

As stated in Chapter 1, the primary goal of this study is to investigate how a threat hunting methodology can be effectively applied to detect lateral movement attacks within organisational networks. To achieve this main goal, a number of research objectives are introduced in Chapter 1. The manner in which these research objectives are achieved in this study is as follows:

Explore lateral movement and the techniques employed by APTs. This objective was addressed in Chapter 2, which conducted a detailed review of the literature to identify and categorise the methods used by advanced persistent threats (APTs) for lateral movement. The chapter provided a thorough analysis of lateral movement techniques, including reconnaissance, credential abuse, and remote execution, among others, as outlined in the MITRE ATT&CK framework. By developing an understanding of these strategies, this research created a robust foundation for simulating these techniques in subsequent chapters. The categorisation of APT tactics and techniques informed the hypothesis formulation and simulation design used in validating the TaHiTI methodology.

Investigate approaches to address lateral movement attacks. In Chapter 3, various approaches and techniques for detecting lateral movement attacks were investigated. These included a critical analysis of traditional detection methods, such as signature-based and behavioural analysis, and their limitations in identifying stealthy APT activities. The chapter also reviewed advanced detection techniques, including anomaly detection and the integration of threat intelligence. The strengths and weaknesses of these methods were highlighted, with a focus on identifying gaps that could be addressed by hypothesis-driven threat hunting. This analysis reinforced the need for a structured framework like TaHiTI, which combines proactive monitoring and systematic detection to address these gaps.

Identify an effective approach to setting up a virtual environment for simulations. In Chapter 4, the study established a virtual testing environment to simulate lateral movement attacks. The environment incorporated tools such as sysmon for event logging and HELK for data aggregation and analysis. This setup was tailored to meet the needs of the approaches and techniques identified in the earlier chapters, ensuring that the environment could effectively simulate real-world attack scenarios. The virtual

environment provided a controlled setting for testing the hypothesis-driven TaHiTI methodology, ensuring the repeatability and reliability of the experiments.

Validate the approaches and/or techniques identified by applying them in the virtual environment. This objective was addressed in Chapters 5 and 6, where five lateral movement techniques were simulated and analysed. The simulations tested the effectiveness of TaHiTI in detecting techniques such as internal spear-phishing, Pass-the-Hash (PtH), and remote services abuse. The findings demonstrated that TaHiTI's structured methodology outperformed baseline and basic monitoring setups by systematically identifying anomalous patterns and correlating events indicative of lateral movement. By integrating the phases of Initiate, Hunt, and Finalise, TaHiTI enabled a proactive approach to threat detection, which was validated through detailed comparisons and specific examples from the simulations.

Discuss the findings obtained from the experimental data and make recommendations. In Chapter 6, the findings from the simulations were critically analysed to assess the validity of the TaHiTI methodology. Comparative analysis highlighted the improvements in detection consistency when using TaHiTI. These findings informed a set of practical recommendations for implementing TaHiTI in real-world environments. To enhance clarity and accessibility, these recommendations are now presented in a dedicated section (Section 7.4), which outlines how organisations can incorporate TaHiTI into their operational workflows. Emphasis is placed on hypothesis formulation, use of threat intelligence, prioritisation of TTPs, and integration with existing tools. The study concludes with suggestions for future research, including further exploration of detection strategies for emerging techniques and the refinement of TaHiTI for broader enterprise use.

This study contributes to the field of cybersecurity by demonstrating the effectiveness of TaHiTI as a hypothesis-driven threat hunting methodology. The study not only validates TaHiTI in a controlled setting but also highlights its applicability in real-world scenarios. By integrating structured hunting phases with tools such as HELK and sysmon, the study provides a replicable framework for detecting lateral movement attacks. In addition, the study reinforces the importance of hypothesis-driven hunting, which allows organisations to identify and mitigate threats that would otherwise blend into regular network activities.

These contributions are pivotal in advancing threat detection methodologies, providing practical insights for both academia and industry.

7.4. Significance of findings and comparison with existing literature

The findings of this study underscore the potential of hypothesis-driven threat hunting, particularly the TaHiTI methodology, in proactively identifying lateral movement techniques. This structured approach proved effective in emulating realistic adversary behaviors, correlating strongly with known TTPs defined in the MITRE ATT&CK framework (Berady *et al.,* 2021). From a practical perspective, the study demonstrated that it is possible to adopt TaHiTI's hypothesis generation and iterative refinement model to guide the deployment of detection rules within SOCs. This aligns with research advocating automation in threat hunting for ICS and enterprise networks, where MITRE ATT&CK-informed detection significantly enhanced responsiveness (Arafune *et al.,* 2022).

On a theoretical level, this study contributes to threat hunting literature by validating the application of structured threat hunting methodologies in controlled, repeatable simulations—bridging a research gap highlighted in machine learning-based hunting literature (Chen *et al.*, 2022). Methodologically, the study supports the assertion that combining human-driven hypothesis testing with simulation-based experimentation yields richer detection insights than baseline or no-monitoring strategies. These results reflect the broader consensus that ATT&CK-driven and hypothesis-guided techniques can improve early-phase detection accuracy (Jadidi & Lu, 2021). Future work should focus on real-world deployments and refining hunting hypothesis generation through continuous feedback loops, as encouraged by frameworks integrating Bayesian reasoning and machine-assisted correlation engines (Kim *et al.*, 2023).

7.5. Recommendations for implementing TaHiTI in real-world environments

This section presents practical recommendations for applying the TaHiTI methodology within enterprise environments, based on the findings of the experimental simulations conducted in this study. While the research was carried out in a controlled virtual setup,

the results demonstrated TaHiTI's potential to enhance threat detection, particularly in relation to lateral movement attacks. The following recommendations are intended to support cybersecurity teams in operationalising TaHiTI effectively within real-world contexts.

Firstly, it is recommended that organisations adopt a targeted approach to hypothesis development by focusing on adversary techniques that pose the greatest risk to their environment. This includes prioritising techniques such as credential dumping, Pass-the-Hash, and remote service abuse, which were found to be particularly effective in bypassing standard detection mechanisms. Drawing from existing frameworks such as MITRE ATT&CK, security teams can structure their threat hunting efforts around relevant tactics, techniques, and procedures (TTPs), ensuring that hypotheses are grounded in known adversarial behaviours (MITRE, 2024).

Secondly, the implementation of TaHiTI should be closely integrated with threat intelligence processes. Threat intelligence should inform the formulation of hypotheses and guide the selection of log sources and visibility points. This integration ensures that hunting efforts remain adaptive and focused on current threats. As Gomez et al. (2022) suggest, aligning detection priorities with real-time intelligence significantly increases the relevance and effectiveness of threat hunting activities.

Thirdly, establishing the right telemetry and logging infrastructure is essential. While comprehensive visibility may not be immediately attainable for all organisations, it is critical to ensure that essential data sources are in place. These should include endpoint telemetry such as Windows Event Logs and Sysmon, as well as network-level logs. In this study, the HELK platform proved effective in aggregating such data and enabling meaningful analysis. According to Lee et al. (2021), ensuring consistent and structured data collection is a foundational requirement for any successful threat hunting programme.

Fourthly, organisations are encouraged to embed TaHiTI into their existing security operations, rather than treating it as an isolated process. Threat hunting should complement and enhance routine activities within security operations centres (SOCs). The structured process phases used in this study, Initiate, Hunt, and Finalise, can be adapted to suit different operational models. By integrating TaHiTI with SIEM tools, case

management platforms, and response workflows, teams can accelerate incident detection and response capabilities.

Finally, it is recommended that organisations institutionalise a learning process by documenting each hunt, whether successful or not. Every iteration contributes to the maturity of the hunting programme and provides an opportunity to refine hypotheses and improve detection logic. Sharing findings within the security team supports knowledge retention and promotes continuous improvement, as also emphasised in the maturity models proposed by the SANS Institute (SANS, 2021).

In summary, the application of TaHiTI in real-world environments requires a strategic and structured approach. By focusing on relevant TTPs, integrating threat intelligence, establishing the right data infrastructure, embedding the methodology into operational workflows, and continuously learning from each hunt, organisations can significantly enhance their threat detection capabilities. The recommendations presented here are grounded in both the experimental results of this study and prevailing best practices, providing a pathway for operationalising hypothesis-driven threat hunting.

7.6. Limitations and future work

This section outlines the limitations of the study, reflects on the challenges encountered during its execution, and provides recommendations for future studies. These insights are intended to ensure transparency and pave the way for the advancement of cybersecurity methodology. The study was carried out within a controlled laboratory environment, which, although suitable for validating the TaHiTI methodology, does not fully replicate the complexity of real-world organisational networks. Focusing on specific lateral movement techniques and predefined attack scenarios limits the range of adversarial tactics analysed. Additionally, reliance on synthetic data, due to restricted access to real-world datasets and the lack of access to functioning corporate networks, may not fully capture the variability and unpredictability of live environments.

Resource constraints also present another significant limitation. The laboratory environment lacked adequate backup mechanisms due to limited backup storage resources to be able to perform regular backups, which at the time of setting up the assumption was that it will be a quick rebuilt if needed. This process was time-consuming

and required significant effort, restricting the ability to run simulations on a larger scale or for extended durations. The study process was marked by several personal and logistical challenges. The global COVID-19 pandemic disrupted access to resources and added mental and emotional stress. The loss of a close family member during this period made it particularly difficult to focus on the study, resulting in delays in critical phases. Furthermore, the technical challenges faced during lab reconfiguration further extended the study timeline, as the absence of sufficient backup systems required the reconstruction of the environment from the ground up whenever problems arose.

Future studies could incorporate real-world datasets to validate the TaHiTI methodology under dynamic and more complex conditions. Expanding the scope to include a wider range of lateral movement techniques and integrating endpoint- and network-level monitoring could also provide a more comprehensive detection framework. Using cloud-based infrastructure or other scalable solutions would help overcome resource constraints, allowing more extensive and long-term simulations. Furthermore, refining the methodology to address emerging threats, such as AI-driven attack strategies, would improve its applicability to rapidly evolving cybersecurity landscapes. This study acknowledges its limitations, and the challenges encountered during its execution, but provides a valuable foundation for advancing proactive cybersecurity methodologies. The proposed future work outlines actionable steps to build on these findings, contributing to the development of more resilient and effective approaches for mitigating lateral movement attacks.

7.7. Chapter summary

This chapter concludes the study. It commences with a summary of the study and examines each section and chapter. The initial objectives are revisited, and their fulfilment discussed. Subsequently, the study's contributions are outlined, followed by a concise examination of its limitations and potential areas for future investigation.

References

Abualkas, Y.M.A. & Bhaskari, D.L. 2023. Methodologies for Predicting Cybersecurity Incidents. *Indian Journal of Cryptography and Network Security*. 3(1):1–8.

Ackerman, G. & Clifford, D. 2021. Red Teaming and Crisis Preparedness. In: *Oxford Research Encyclopedia of Politics*. Oxford University Press.

Ahmed, Y., Taufiq, A. & Md Arafatur, R. 2021. A cyber kill chain approach for detecting advanced persistent threats. *Computers, Materials and Continua*. 67(2):2497–2513.

Ajmal, A.B., Shah, M.A., Maple, C., Asghar, M.N. & Islam, S.U. 2021. Offensive Security: Towards Proactive Threat Hunting via Adversary Emulation. *IEEE Access*. 9:126023–126033.

Alhajjar, E., Maxwell, P. & Bastian, N. 2021. Adversarial machine learning in network intrusion detection systems. *Expert Systems with Applications*. 186:115782.

Al-Saraireh, J. & Masarweh, A. 2022. A novel approach for detecting advanced persistent threats. *Egyptian Informatics Journal*. 23(4):45–55.

Alshamrani, A., Myneni, S., Chowdhary, A. & Huang, D. 2019. A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities. *IEEE Communications Surveys & Tutorials*. 21(2):1851–1877.

Araujo, F., Ayoade, G., Al-Naami, K., Gao, Y., Hamlen, K.W. & Khan, L. 2021. Crook-sourced intrusion detection as a service. *Journal of Information Security and Applications*. 61:102880.

Ashfaq, T. & Malik, M. 2022. The Forensics Artifacts on Remote Desktop Protocol and Service: Talha Ashfaq, Muhammad Shairoze Malik. *International Journal for Electronic Crime Investigation*. 6(3):15–21.

Atomic Red. 2024. *Phishing: Spearphishing Attachment*. *Atomic Red Team*. https://atomicredteam.io/initial-access/T1566.001/ Date of access: 09 May 2024.

Ayyagari, M.R., Kesswani, N., Kumar, M. & Kumar, K. 2021. Intrusion detection techniques in network environment: A systematic review. *Wireless Networks*. 27:1269–1285.

Bai, I., Bian, H., Salahuddin, M., Daya, A.A., Limam, N. & Boutaba, A. 2020. DP-based Lateral Movement detection using Machine Learning. https://www.semanticscholar.org/paper/RDP-based-Lateral-Movement-detection-using-Machine-Bai-Bian/a78beef2be0161a012557ff25fc4a605a313eea1.

Bai, T., Bian, H., Daya, A.A., Salahuddin, M.A., Limam, N. & Boutaba, R. 2019. A Machine Learning Approach for RDP-based Lateral Movement Detection. In: *2019 IEEE 44th Conference on Local Computer Networks (LCN)*. IEEE Conference on Local Computer Networks (LCN). pp. 242–245.

Benito, R., Shaffer, A. & Singh, G. 2023. An Automated Post-Exploitation Model for Cyber Red Teaming. *International Conference on Cyber Warfare and Security*. 18(1):25–34.

Berady, A., Jaume, M., Tong, V.V.T. & Guette, G. 2021. From TTP to IoC: Advanced Persistent Graphs for Threat Hunting. *IEEE Transactions on Network and Service Management*. 18(2):1321–1333.

Berger, J. 2012. *Lecture 2: Bayesian Hypothesis Testing*. Duke University. https://cbms-mum.soe.ucsc.edu/lecture2.pdf Date of access: 25 Nov. 2023.

Bhardwaj, A., Kaushik, K., Alomari, A., Alsirhani, A., Alshahrani, M.M. & Bharany, S. 2022. BTH: Behavior-Based Structured Threat Hunting Framework to Analyze and Detect Advanced Adversaries. *Electronics*. 11(19):2992.

Bi, J., He, S., Luo, F., Meng, W., Ji, L. & Huang, D.-W. 2023. Defense of advanced persistent threat on industrial internet of things with lateral movement modeling. *IEEE Transactions on Industrial Informatics*. 19(9):9619–9630.

Bienzobas, Á., & Sánchez-Macián, A., 2023. Threat Trekker: An Approach to Cyber Threat Hunting. ArXiv, abs/2310.04197. https://doi.org/10.48550/arXiv.2310.04197.Boulila, E. & Dacier, M. 2023. WPAD: Waiting patiently for an announced disaster. *ACM Computing Surveys*. 55(10):1–29.

Bowman, B., Laprade, C., Ji, Y. & Huang, H.H. 2020. Detecting Lateral Movement in Enterprise Computer Networks with Unsupervised Graph AI. In: *23rd International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2020)*. San Sebastian: USENIX Association. pp. 257–268. https://www.usenix.org/conference/raid2020/presentation/bowman.

Boyagane, I. 2020. *Understand your Computer System using Logs*. *Medium*. https://towardsdatascience.com/understand-your-computer-system-using-logs-98139d0b5de1 Date of access: 04 May 2023.

Bullée, J.H., Montoya, L., Pieters, W., Junger, M. & Hartel, P. 2018. On the anatomy of social engineering attacks—A literature-based dissection of successful attacks. *Journal of investigative psychology and offender profiling*. 15(1):20–45.

Caltagirone, S., Pendergast, A. & Betz, C. 2020. *The Diamond Model of Intrusion Analysis*. (Technical Report ADA586960). Center for Cyber Threat Intelligence and Threat Research: Threat Intel Academy. https://www.threatintel.academy/wp-content/uploads/2020/07/diamond-model.pdf Date of access: 02 Aug. 2023.

Canary. 2024. *Atomic Red Team*. *T1018*. https://atomicredteam.io/discovery/T1018/. Date of access: 03 May 2024.

Chacko, A.A., Edwin, B. & Thanka, M.R. 2022. Detecting the Lateral Movement in Cyberattack at the Early Stage Using Machine Learning Techniques. In: J.D. Peter, S.L. Fernandes, & A.H. Alavi, eds. Vol. 905. (Lecture Notes in Electrical Engineering). *Disruptive Technologies for Big Data and Cloud Applications*. Singapore: Springer Nature Singapore. pp. 581–588.

Chain, A.C.K. 2015. *Applying Cyber Kill Chain Methodology to Network Defense*. Lockheed Martin. https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf Date of access: 23 Nov. 2022.

Chatzilygeroudis, K., Hatzilygeroudis, I. & Perikos, I. 2021. Machine Learning Basics. In: P. Eslambolchilar, A. Komninos, & M. Dunlop, eds. 1st ed. *Intelligent Computing for Interactive System Design*. New York, NY, USA: ACM. pp. 143–193.

Chen, C.-K., Lin, S.-C., Huang, S.-C., Chu, Y.-T., Lei, C.-L. & Huang, C.-Y. 2022. Building Machine Learning-based Threat Hunting System from Scratch. *Digital Threats: Research and Practice*. 3(3):1–21.

Chen, P.-Y., Choudhury, S., Rodriguez, L., Hero, A. & Ray, I. 2019. Toward Cyber-Resiliency Metrics for Action Recommendations Against Lateral Movement Attacks. *Advances in Information Security*.

Chen, S.-S., Hwang, R.-H., Ali, A., Lin, Y.-D., Wei, Y.-C. & Pai, T.-W. 2024. Improving quality of indicators of compromise using STIX graphs. *Computers & Security*. 144:103972.

Collier, R. & Azarmi, B. 2019. *Machine Learning with the Elastic Stack: Expert techniques to integrate machine learning with distributed search and analytics*. Packt Publishing Ltd.

Creswell, J.W. 2013. *Research Design: Qualitative, quantitative, and mixed methods approaches*. 4th ed. 2455 Teller road, Thousand Oaks, California 91320: SAGE, Inc.

Cynet. 2024. Lateral movement: Challenges, APT, and Automation. https://www.cynet.com/network-attacks/lateral-movement-challenges-apt-and-automation/? Date of access: 05 Dec. 2024.

Danneman, N. & Hyde, J.T. 2021. Predicting Adversary Lateral Movement Patterns with Deep Learning. *ArXiv*. abs/2104.13195. https://api.semanticscholar.org/CorpusID:233407980.

Das, D., Schiewe, M., Brighton, E., Fuller, M., Cerny, T., … Tisnovsky, P. 2020. Failure prediction by utilizing log analysis: A systematic mapping study. In: *Proceedings of the International Conference on Research in Adaptive and Convergent Systems*. pp. 188–195.

Dimov, D. & Tzonev, Y. 2017. Pass-the-Hash: One of the Most Prevalent Yet Underrated Attacks for Credentials Theft and Reuse. In: *Proceedings of the 18th International Conference on Computer Systems and Technologies*. Ruse Bulgaria: ACM. pp. 149–154.

Dong, C., Chen, Y., Zhang, Y., Liu, Y., Lu, Z., … Liu, B. 2021. BEDIM: Lateral Movement Detection In Enterprise Network Through Behavior Deviation Measurement. In: *2021 IEEE 23rd Int Conf on High Performance Computing & Communications; 7th Int Conf on Data Science & Systems; 19th Int Conf on Smart City; 7th Int Conf on Dependability in Sensor, Cloud & Big Data Systems & Application (HPCC/DSS/SmartCity/DependSys)*. Haikou, Hainan, China: IEEE. pp. 391–398.

Elgohary, N. & Abdelbaki, N. 2022. Detecting Mimikatz in Lateral Movements Using Windows API Call Sequence Analysis. In: *2022 4th Novel Intelligent and Leading Emerging Sciences Conference (NILES)*. Giza, Egypt: IEEE. pp. 306–310.

Fatemi, M.R. 2019. Threat-hunting in Windows environment using host-based log data. University of New Brunswick. (Master's). https://unbscholar.dspace.lib.unb.ca/server/api/core/bitstreams/d8fe89b9-7948-4107-9914-cec057f1d273/content Date of access: 05 Mar. 2023.

Fatemi, M.R. & Ghorbani, A.A. 2020. Threat hunting in windows using big security log data. In: *Security, privacy, and forensics issues in big data*. IGI Global. pp. 168–188.

Fawaz, A., Bohara, A., Cheh, C. & Sanders, W.H. 2016. Lateral Movement Detection Using Distributed Data Fusion. In: *2016 IEEE 35th Symposium on Reliable Distributed Systems (SRDS)*. IEEE Symposium on Reliable Distributed Systems. pp. 21–30.

Ferrag, M.A., Maglaras, L., Moschoyiannis, S. & Janicke, H. 2020. Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security and Applications*. 50:102419.

Fuchs, M. & Lemon, J. 2024. *SANS 2024 Threat Hunting Survey: Hunting for Normal Within Chaos*. (Survey). SANS Institute. https://sansorg.egnyte.com/dl/DWUAsHzUUh Date of access: 20 Nov. 2024.

Georgiadou, A., Mouzakitis, S. & Askounis, D. 2021. Assessing MITRE ATT&CK Risk Using a Cyber-Security Culture Framework. *Sensors*. 21(9):3267.

Ghosh, P., Kiran, S., Mahalakshmi, J. & Basha, S.K.A.H. 2023. *Understanding Machine Learning*. India: Academic guru publishing house.

Haber, M.J. & Rolls, D. 2020. Indicators of Compromise. In: Identity Attack Vectors. In: *Identity Attack Vectors*. Berkeley, CA: Apress. pp. 103–105.

Hemberg, E., Turner, M.J., Rutar, N. & O'reilly, U.-M. 2024. Enhancements to Threat, Vulnerability, and Mitigation Knowledge for Cyber Analytics, Hunting, and Simulations. *Digital Threats: Research and Practice*. 5(1):1–33.

Hendler, D., Kels, S. & Rubin, A. 2018. Detecting Malicious PowerShell Commands using Deep Neural Networks. In: *Proceedings of the 2018 on Asia Conference on Computer and Communications Security*. Incheon Republic of Korea: ACM. pp. 187–197.

Hutchins, E., Cloppert, M. & Amin, R. 2011. Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. *Leading Issues in Information Warfare & Security Research*. 1.

Ibrahim, M.R. & Thanoon, K. 2022. Quasar Remote Access Trojan feature extraction depending on Ethical Hacking. *Technium: Romanian Journal of Applied Sciences and Technology*. 4(1):58–75.

Jadeja, N. & Vaghasia, M. 2018. Analysis and Impact of Different Mechanisms of Defending Pass-the-Hash Attacks. In: M.U. Bokhari, N. Agrawal, & D. Saini, eds. Vol. 729. (Advances in Intelligent Systems and Computing). *Cyber Security*. Singapore: Springer Singapore. pp. 179–191.

Jain, U. & Conklin, Wm.A. 2018. Lateral movement detection using Elk stack. Published ETD Collection: University of Houston. (Dissertation). http://hdl.handle.net/10657/3109 Date of access: 15 Nov. 2023.

Kadan, Ö.F. 2021. The effects of creative drama on achievement and motivation levels of the 7th graders in english language classes. *Participatory Educational Research*. 8(3):88–104.

Kambourakis, G., Kolias, C., Gritzalis, S. & Smiliotopoulos, C. 2024. Exploring the boundaries of lateral movement detection through unsupervised learning. pp. 39.

Katano, Y., Kozai, Y., Okada, S. & Mitsunaga, T. 2022. Prediction of infected devices using the quantification theory type 3 based on MITRE ATT&CK Technique. In: *2022 IEEE International Conference on Computing (ICOCO)*. Kota Kinabalu, Malaysia: IEEE. pp. 198–203.

Kavak, H., Padilla, J.J., Vernon-Bido, D., Diallo, S.Y., Gore, R. & Shetty, S. 2021. Simulation for cybersecurity: State of the art and future directions. *Journal of Cybersecurity*. 7(1):tyab005.

Khattab, O. 2020. Conducting empirical research study: How to effectively and securely use the vital features of the Active Directory network server. *International Journal of Advanced Trends in Computer Science and Engineering*. 9(1):87–90.

Khaver, A.V. 2023. Principles of operation and detection on the target system of the dual purpose tool Cobalt Strike. *Modern Information Security*. 54(2).

Kim, Y., Lee, I., Kwon, H., Lee, K. & Yoon, J. 2023. BAN: Predicting APT Attack Based on Bayesian Network With MITRE ATT&CK Framework. *IEEE Access*. 11:91949–91968.

Kinnunen, J. 2022. Threat Detection Gap Analysis Using MITRE ATT&CK Framework. JAMK University of Applied Sciences. (Dissertation). https://urn.fi/URN:NBN:fi:amk-202204125027 Date of access: 05 Sep. 2023.

Kryukov, R., Zima, V., Fedorchenko, E., Novikova, E. & Kotenko, I. 2022. Mapping the Security Events to the MITRE ATT &CK Attack Patterns to Forecast Attack Propagation. In: *Attacks and Defenses for the Internet-of-Things: 5th International Workshop, ADIoT 2022, Copenhagen, Denmark, September 30, 2022, Revised Selected Papers*. Springer. pp. 165–176.

Kulkarni, M.S., Ashit, D.H. & Chetan, C.N. 2023. A Proactive Approach to Advanced Cyber Threat Hunting. In: *2023 7th International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS)*. IEEE. pp. 1–6.

Kumari, S., Tyagi, A.K. & Rekha, G. 2021. Applications of Blockchain Technologies in Digital Forensics and Threat Hunting. In: 1st ed. *Recent Trends in Blockchain for Information Systems Security and Privacy*. Boca Raton: CRC Press. pp. 159–173.

Kushwaha, D., Nandakumar, D., Kakkar, A., Gupta, S., Choi, K., Nehila, J. 2022. Lateral movement detection using user behavioral analysis. *ArXiv*. abs/2208.13524. https://api.semanticscholar.org/CorpusID:251903630.

Lanaerts-Bergmans, B. 2023. Lateral Movement. https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/lateral-movement/? Date of access: 05 Dec. 2024.

Lee, R.M. & Lee, R.T. 2018. Sans 2018 threat hunting survey results. *SANS Institute Reading Room*.

Lee, D., Kim, D., Ahn, M.K., Jang, W. & Lee, W. 2021. Cy-Through: Toward a Cybersecurity Simulation for Supporting Live, Virtual, and Constructive Interoperability. *IEEE Access*. 9:10041–10053.

Lehto, M. 2022. APT Cyber-attack Modelling: Building a General Model. *International Conference on Cyber Warfare and Security*. 17(1):121–129.

Liu, Z., Chen, C., Zhang, L.Y. & Gao, S. 2022. Working Mechanism of Eternalblue and Its Application in Ransomworm. In: X. Chen, J. Shen, & W. Susilo, eds. Vol. 13547. (Lecture Notes in Computer Science). *Cyberspace Safety and Security*. Cham: Springer International Publishing. pp. 178–191.

Lukova-Chuiko, N., Fesenko, A., Papirna, H. & Gnatyuk, S. 2020. Threat Hunting as a Method of Protection Against Cyber Threats. In: *International Conference "Information Technology and Interactions"*.

Mailewa, A. & Rozendaal, K. 2022. A Novel Method for Moving Laterally and Discovering Malicious Lateral Movements in Windows Operating Systems: A Case Study. *Advances in Technology*. (August, 25):291–321.

Mark N.K. Saunders Adrian Thornhill, P.L. 2019. *Research Methods for Business Students*. Pearson.

Mavroeidis, V. & Josang, A. 2018. Data-Driven Threat Hunting Using Sysmon. In: (ICCSP 2018). *Proceedings of the 2nd International Conference on Cryptography, Security and Privacy*. New York, NY, USA: Association for Computing Machinery. pp. 82–88.

Mavroeidis V. & 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)*. pp. 91–98.

Mcwhorter, D. 2014. *APT1: Exposing One of China's Cyber Espionage Units*. Mandiant (Firm). https://www.nationalcyberwatch.org/resource/apt1-exposing-one-of-chinas-cyber-espionage-units-2/ Date of access: 20 Feb. 2024.

Microsoft. 2021. *Event Types*. Vol. 2022. *About Logging*. https://docs.microsoft.com/en-us/windows/win32/eventlog/event-types Date of access: 20 Nov. 2023.

Mireles, J.D., Cho, J.-H. & Xu, S. 2016. Extracting attack narratives from traffic datasets. In: *2016 International Conference on Cyber Conflict (CyCon U.S.)*. pp. 1–6.

Mitre. 2024. *Matrix - Enterprise | MITRE ATT&CK*. *Mitre Coporation*. https://attack.mitre.org/matrices/enterprise/ Date of access: 09 Jul. 2024.

Mohan, V. 2015. Intrusion detection system - A Study. *International Journal of Security, Privacy and Trust Management (IJSPTM)*. 4(1):15.

Morgan, D.L. 2014. *Integrating Qualitative and Quantitative Methods: A Pragmatic Approach*. 1 Oliver's Yard, 55 City Road London EC1Y 1SP: SAGE Publications, Inc.

Muckin, M., Fitch, S.C. & Corporation, L.M. 2019. A Threat-Driven Approach to Cyber Security. *Lockheed Martin*. 45.

Muse, P., S, M.S. & Stanly, H. 2023. Online Log Analysis(OLA) for Malicious User Activities. In: *2023 2nd International Conference on Paradigm Shifts in Communications Embedded Systems, Machine Learning and Signal Processing (PCEMS)*. Nagpur, India: IEEE. pp. 1–6.

Nguyen, T.-G., Nguyen, T.-N., Vu, D.-K., Bui, N.-L., Nguyen, V.-H., Ngo, T.-S. 2024. Detecting Fileless Malware on Windows with ATT&CK: A Practical Approach. In: *2024 International Conference on Electrical, Computer and Energy Technologies (ICECET*. Sydney, Australia: IEEE. pp. 1–6.

NIST. 2011. *Managing information security risk: Organization, mission, and information system view*. (NIST SP 800-39). Gaithersburg, MD: National Institute of Standards and Technology.

Nolette, R. & Devry, J. 2020. https://www.cybersecurity-insiders.com/situational-awareness-driven-threat-hunting/.

Nour, B., Pourzandi, M. & Debbabi, M. 2023. A Survey on Threat Hunting in Enterprise Networks. *IEEE Communications Surveys & Tutorials*. 25:2299–2324.

Oakley, J.G. 2019. Counter-APT Red Teaming. In: *Professional Red Teaming*. Berkeley, CA: Apress. pp. 117–128.

Oberle, A., Larbig, P., Marx, R., Weber, F.G., Scheuermann, D., Thomas, F. 2016. Preventing Pass-the-Hash and Similar Impersonation Attacks in Enterprise Infrastructures. In: *2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA)*. Crans-Montana, Switzerland: IEEE. pp. 800–807.

Os, R.V., Bakker, M., Bouman, R., Leeuwen, M.D. van, Mentges, W. & Piers, A. 2018. https://www.betaalvereniging.nl/en/safety/tahiti/ Date of access: 09 Aug. 2022.

Otomo, K., Kobayashi, S., Fukuda, K. & Esaki, H. 2018. Finding Anomalies in Network System Logs with Latent Variables. In: *Proceedings of the 2018 Workshop on Big Data Analytics and Machine Learning for Data Communication Networks*. Budapest Hungary: ACM. pp. 8–14.

Palacin, V. 2021. *Practical Threat Intelligence and Data-Driven Threat Hunting: A Hands-on Guide to Threat Hunting with the ATT&CK"! Framework and Open Source Tools*. Packt Publishing Limited.

Pérez-Gomariz, M., Cerdán-Cartagena, F. & García, J. 2024. Lm-Hunter: An Nlp-Powered Graph Method for Detecting Adversary Lateral Movements in Apt Cyber-Attacks at Scale. In: Elsevier. pp. 26.

Ponemon. 2019. *Improving the Effectiveness of the Security Operations Center*. Ponemon Institute LLC. https://www.devo.com/wp-content/uploads/2019/07/2019-Devo-Ponemon-Study-Final.pdf Date of access: 25 Nov. 2023.

Purilock. 2024. Lateral Movement. https://plurilock.com/deep-dive/lateral-movement/? Date of access: 05 Dec. 2024.

Quintero-Bonilla, S. & Martín del Rey, A. 2020. A New Proposal on the Advanced Persistent Threat: A Survey. *Applied Sciences*. 10(11):3874.

Rabbani, M., Rashidi, L. & Ghorbani, A.A. 2024. A Graph Learning-Based Approach for Lateral Movement Detection. *IEEE Transactions on Network and Service Management*. 21(5):5361–5373.

Raj. 2020. *Lateral Movement: Pass the Hash Attack*. *Hacking Articles*. https://www.hackingarticles.in/lateral-movement-pass-the-hash-attack/ Date of access: 03 May 2024.

Rajesh, P., Ismail, M., Alam, M., Tahernezhadi, M., & Monika A. 2021. Network Forensics Investigation in Virtual Data Centers using ELK. *2021 International Symposium on Electrical, Electronics and Information Engineering*. 175–179.

Ring, M., Schlör, D., Wunderlich, S., Landes, D. & Hotho, A. 2021. Malware detection on windows audit logs using LSTMs. *Computers & Security*. 109:102389.

Rodriguez, R. & Rodriguez, J.L. 2019. https://www.insomnihack.ch/conference-2019/#201920.

Roy, S., Panaousis, E., Noakes, C., Laszka, A., Panda, S. & Loukas, G. 2023. SoK: The MITRE ATT&CK Framework in Research and Practice. In: arXiv. pp. 16.

Sadayappan, B., Riddle, Z., Nuce, J., Shilko, J. & Kennely, J. 2024. Ransomware Rebounds: Extortion Threat Surges in 2023, Attackers Rely on Publicly Available and Legitimate Tools. *Threat Intelligence*. https://cloud.google.com/topics/threat-intelligence/ransomware-attacks-surge-rely-on-public-legitimate-tools? Date of access: 20 Aug. 2024.

Sajan, D.P.P. 2024. A Comprehensive Analysis of WannaCry Ransomware. *Interantional journal of scientific research in engineering and management*. 08(008):1–5.

Sarhan, M., Layeghy, S., Moustafa, N. & Portmann, M. 2021. Netflow datasets for machine learning-based network intrusion detection systems. In: *Big Data Technologies and Applications: 10th EAI International Conference, BDTA 2020, and 13th EAI International Conference on Wireless Internet, WiCON 2020, Virtual Event, December 11, 2020, Proceedings 10*. Springer. pp. 117–135.

Saunders, M., Lewis, P., Thornhill, A. & Bristow, A. 2019. “Research Methods for Business Students” Chapter 4: Understanding research philosophy and approaches to theory development. In: *Research Methods for Business Students*. Harlow CM17 9NA, United Kingdom: Pearson. pp. 128–171.

Sehgal, K. & Thymianis, N. 2023. *Cybersecurity Blue Team Strategies: Uncover the secrets of blue teams to combat cyber threats in your organization*. Packt Publishing. http://ieeexplore.ieee.org/document/10162645.

Sica, S., Jornet, A., Lichters, A., Mashinchi, A., Kimura, A. & Homewood, A. 2023. *Mitre ATT&CK Matrix*. *v14.1 MITRE - CTI*. https://attack.mitre.org/ Date of access: 02 Jul. 2023.

Smiliotopoulos, C., Kambourakis, G. & Barbatsalou, K. 2023. On the detection of lateral movement through supervised machine learning and an open-source tool to create turnkey datasets from Sysmon logs. *International Journal of Information Security*. 22(6):1893–1919.

Smiliotopoulos, C., Barmpatsalou, K. & Kambourakis, G. 2022. Revisiting the Detection of Lateral Movement through Sysmon. *Applied Sciences*. 12(15):7746.

Smiliotopoulos, C., Kambourakis, G. & Kolias, C. 2024. Detecting lateral movement: A systematic survey. *Heliyon*. 10(4):e26317.

Soria-Machado, M., Abolins, D., Boldea, C. & Socha, K. 2017. Detecting lateral movements in windows infrastructure. *CERT-EU Security Whitepaper*. 12–17.

Sqrrl. 2018. *A Framework for Cyber Threat Hunting*. MA: Cambridge. https://www.threathunting.net/files/framework-for-threat-hunting-whitepaper.pdf Date of access: 18 Feb. 2022.

Strom, B. & Smith, T. 2023. *Pass the Hash*. *Use Alternate Authentication*. https://attack.mitre.org/techniques/T1550/002/ Date of access: 02 May 2024.

Strom, B., Applebaum, A., Miller, D., Nickels, K., Pennington, A., Corporation, M. 2020. *MITRE ATT&CK: Design and Philosophy*. McLean, VA: MITRE. https://www.mitre.org/sites/default/files/2021-11/prs-19-01075-28-mitre-attack-design-and-philosophy.pdf Date of access: 16 May 2023.

Taschler, S. 2023. *What Is Cyber Threat Hunting? CrowdStrike*. https://www.crowdstrike.com/cybersecurity-101/threat-hunting/ Date of access: 20 Nov. 2023.

Tiwary, S. 2023. *Lateral Tool Transfer*. *Lateral Movement - Tool Transfer*. https://attack.mitre.org/techniques/T1570/ Date of access: 03 Mar. 2024.

Ussath, M., Jaeger, D., Feng, C. & Meinel, C. 2016. Advanced persistent threats: Behind the scenes. In: *2016 Annual Conference on Information Science and Systems (CISS)*. Princeton, NJ, USA: IEEE. pp. 181–186.

Utinková, H. 2021. Cyber Attacks against Iran as Instruments of Hybrid Warfare. Faculty of Social Sciences: CHARLES UNIVERSITY. (Dissertation). http://hdl.handle.net/20.500.11956/127643 Date of access: 05 Feb. 2023.

Wang, G., Cui, Y., Wang, J., Wu, L. & Hu, G. 2021. A Novel Method for Detecting Advanced Persistent Threat Attack based on Belief Rule Base. *Applied Sciences*. 11(21):9899.

Wilkens, F., Haas, S., Kaaser, D., Kling, P. & Fischer, M. 2019. Towards Efficient Reconstruction of Attacker Lateral Movement. In: *Proceedings of the 14th International Conference on Availability, Reliability and Security*. New York, NY, USA: ACM. pp. 1–9.

Ximenes, P. & Mello, P. 2022. Applying the Diamond Model of Intrusion Analysis: Brazil's Operation "Car Wash" Cyberattack. In: *2022 International Symposium on Networks, Computers and Communications (ISNCC)*. IEEE. pp. 1–6.

Xu, J. & Russello, G. 2022. Automated Security-focused Network Configuration Management: State of the Art, Challenges, and Future Directions. In: *2022 9th International Conference on Dependable Systems and their Applications (DSA)*. IEEE. pp. 409–420.

Yamagishi, R., Katayama, T., Kawaguchi, N. & Shigemoto, T. 2022. HOUND: Log Analysis Support for Threat Hunting by Log Visualization. In: *2022 12th International Congress on Advanced Applied Informatics (IIAI-AAI)*. IEEE. pp. 653–656.

Yan, D., Liu, F. & Jia, K. 2019. Modeling an Information-Based Advanced Persistent Threat Attack on the Internal Network. In: Shanghai, China: IEEE.

Zhao, S., Wei, R., Cai, L., Yu, A. & Meng, D. 2020. CTLMD: Continuous-Temporal Lateral Movement Detection Using Graph Embedding. In: J. Zhou, X. Luo, Q. Shen, & Z. Xu, eds. Vol. 11999. (Lecture Notes in Computer Science). *Information and Communications Security*. Cham: Springer International Publishing. pp. 181–196.

Zheng, P. 2020. Dynamic Fraud Detection via Sequential Modeling. Fayetteville: University of Arkansas. (Dissertation). https://scholarworks.uark.edu/etd/3633 Date of access: 07 Mar. 2024.

Zhou, J., Yao, J., Chen, X., Yu, S., Xuan, Q. & Yang, X. 2024. Lateral Movement Detection via Time-aware Subgraph Classification on Authentication Logs. *ArXiv*. 12.

Zou, Q., Sun, X., Liu, P. & Singhal, A. 2020. An Approach for Detection of Advanced Persistent Threat Attacks. *Computer*. 53(12):92–96.

Chapter 8 Annexure: Detailed simulations

1. Simulation 1: Remote system discovery (T1018)

The simulation execution phase involves specific commands designed to identify domain computers, particularly using **atomic test #2 (remote system discovery) domain computers of the net group** command in PowerShell (Canary, 2024). The execution of the script is summarised in Table 8-1, and the results are analysed in relation to the victim machine's response.

Table 8-1: Attack script executed (Canary, 2024)

Attack script executed
net group "Domain Computers" /domain

The attacker initiates the command prompt and runs atomic test 2 on the compromised victim machine, executing the command highlighted in the attack scripts, as shown in Figure 8-1.

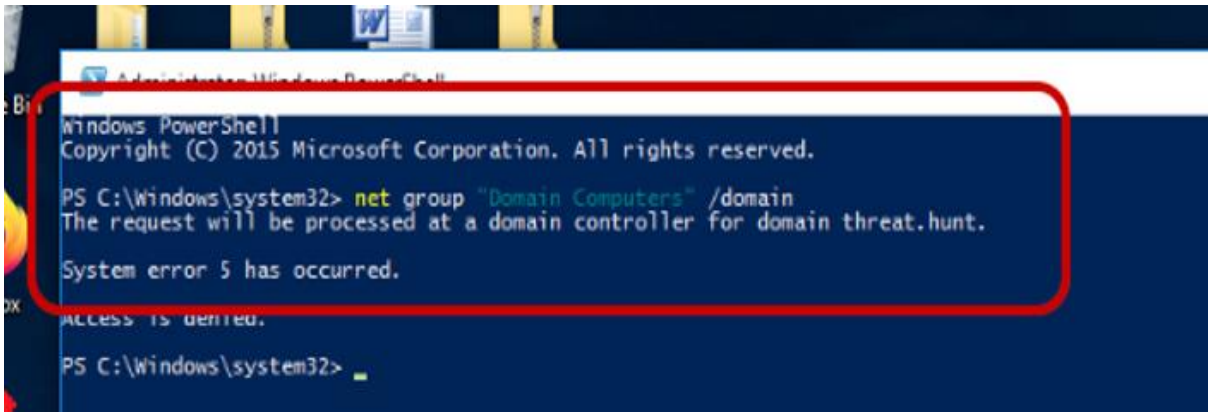


Figure 8-1: Execution of the target machine (Research data)

The hunting phase commences with an investigation of cmd.exe calls and net commands, which are vital for network configuration management. This process, documented through HELK, seeks to identify activities indicative of lateral movements. The analytical approach adopted in this study aligns with the data-driven threat hunting methodology advocated by Rodriguez et al. (2019), emphasising systematic detection and documentation of adversarial tactics. The net group command adds, deletes, and manages global groups on servers. In HELK, the analyst searches for this activity, as illustrated in Figure 8-2,

which indicates that the domain command "net1 group domain computers" is executed with the process name net1.exe and the parent process name net.exe.

event_id	process_parent_guid	CommandLine	process_name	process_parent_name
1	6FE97F59-D7E7-64E3-7303-000000000000	c:\windows\system32**net1** group "domain computers" /domain	**net1.exe**	**net.exe**
1	00000000-0000-0000-0000-000000000000	"c:\windows\system32**net.exe**" group "domain computers" /domain	**net.exe**	-

Figure 8-2: Hunting for domain computers listing (Research data)

The results indicated that sysmon successfully captured the execution of the net group "Domain Computers" /domain command. The process creation event and network activity were logged, and HELK visualized these events, as shown in Figure 1-2. The data collected provided clear indicators of the system discovery attempt, which were flagged as suspicious activity. This simulation effectively illustrated the capability to detect reconnaissance activities, which are precursors to lateral movement using TaHiTI approach. By capturing and analysing the execution of the net group command, the study reinforced the effectiveness of the TaHiTI approach in detecting lateral movement attacks.

2. Simulation 2: Internal spear-phishing

The second simulation focused on the internal spear-phishing technique, identified by the MITRE ATT&CK framework as T1534 and T1566.001. This technique involves an adversary sending phishing emails to internal users within a compromised network to gain further access or to execute additional malicious activities. The hypothesis for this simulation posited that such phishing attempts would trigger specific anomalies in email communication patterns and user interactions, which could be detected.The simulation utilised PowerShell, as the primary tool to execute an atomic red team script simulating an internal spear-phishing attack. This choice reflects the efficiency of PowerShell in replicating real-world APT actions within a controlled network environment. The attack script, outlined in Table A-2, simulates a phishing scenario by downloading and executing a malicious attachment. This scenario demonstrates the potential for harmful payload

delivery and underscores the critical need to detect deceptive tactics as part of a comprehensive threat hunting strategy.

Table 8-2: Internal spear phishing attack script (Atomic Red, 2024)

Attack script executed
$url = 'https://github.com/redcanaryco/atomic-red-team/raw/master/atomics/T1566.001/bin/PhishingAttachment.xlsm' [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12 Invoke-WebRequest -Uri $url -OutFile $env:TEMP\PhishingAttachment.xlsm

The script was executed on the victim's machine to simulate a real phishing attack. It downloads and saves the "**PhishingAttachment.xlsm**" file, setting the security protocol to TLS 1.2, as shown in Figure 8-3. The execution of the target phishing script is demonstrated, highlighting the attack vector.

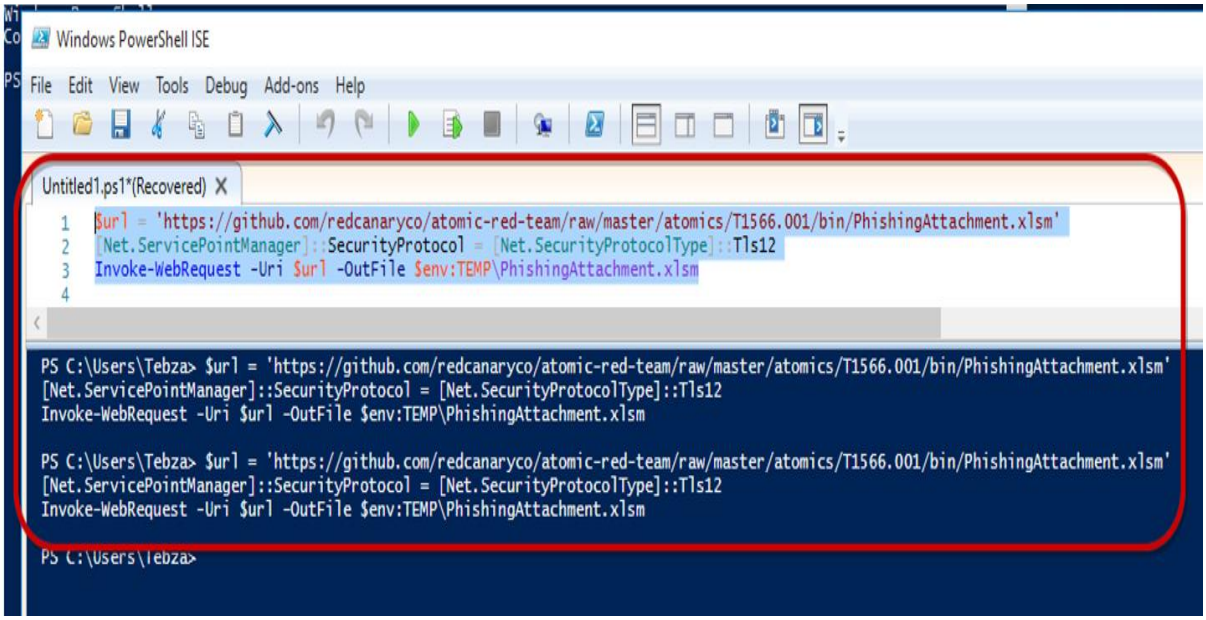


Figure 8-3: Execution of the target phishing script (Research data)

The analysis phase involves monitoring the sysmon logs for events that indicate the execution of spear-phishing emails and scripts. This includes examining file creation events for the "**PhishingAttachment.xlsm**" file, and network connection events related to its download. The detection query for **event ID 3**, as shown in Figure 8-4, enabled the identification of internal spear-phishing activities, highlighting the efficacy of the hypothesis-driven threat hunting architecture.

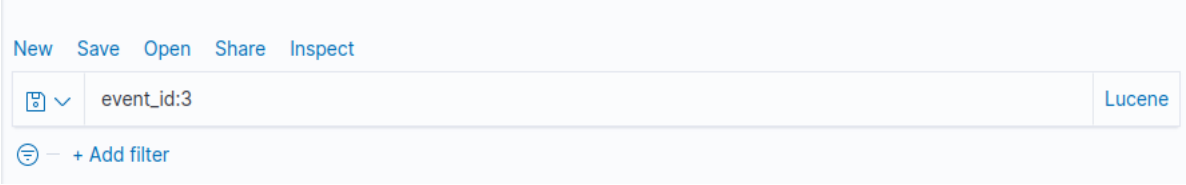


Figure 8-4: Sample query field (Research data)

Figure A-5 showcases the executed query within the hunting architecture, aiding the analyst in identifying the relevant events. The resultant events, as seen in Figure A-6, demonstrate the filtering process within the threat hunting platform, focusing on pertinent event IDs.

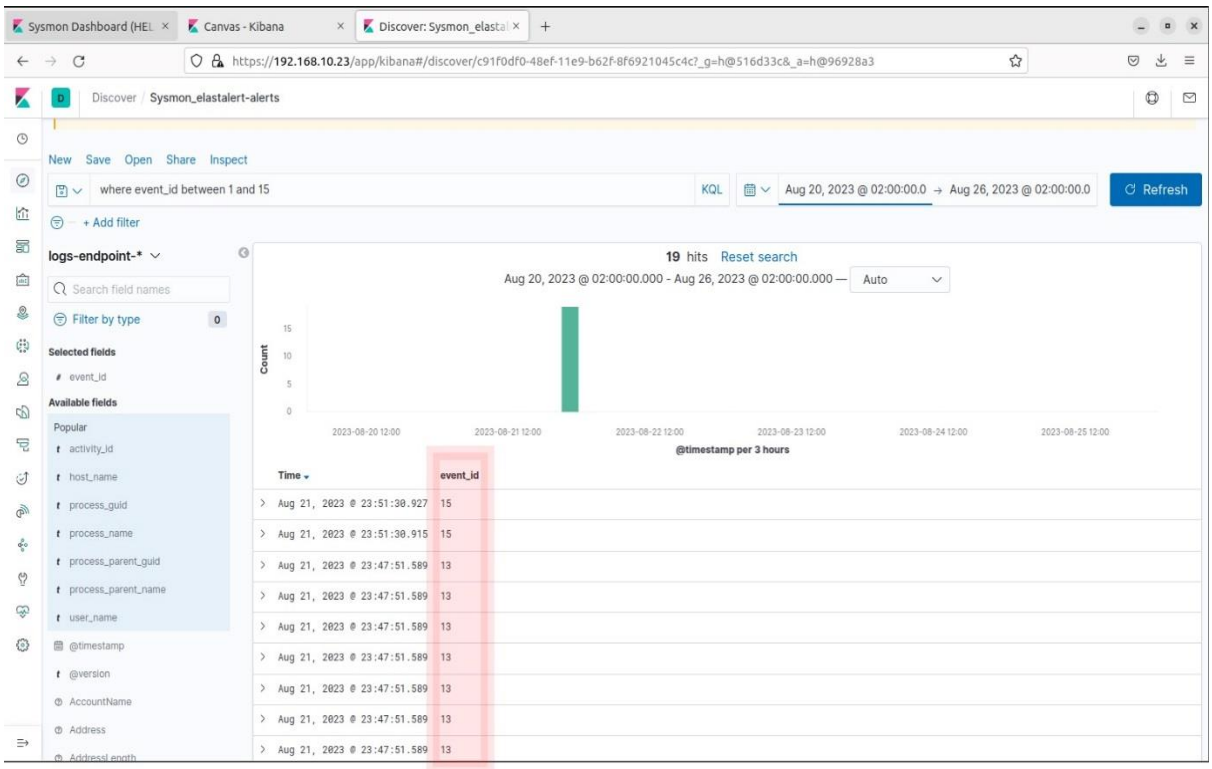


Figure 8-5: Filter in the threat hunt architect (Research data)

The logs further indicate the creation of a file using the PowerShell script. Although the identity of the user executing the macro is known, this detail is not particularly valuable. The key objective is to generate a rule that detects an Excel macro that attempts to access the internet. Figure A-7 illustrates the filtered results based on process IDs, potentially identifying the processes triggered by the phishing script.

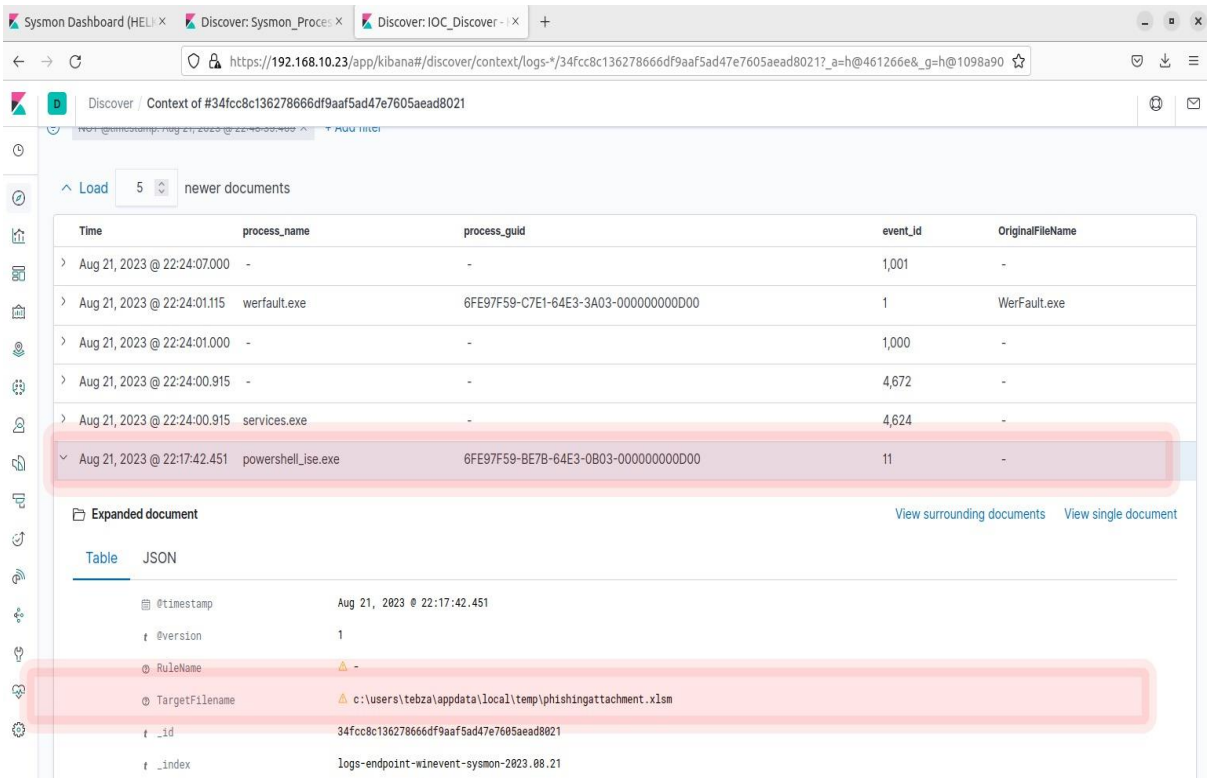


Figure 8-6: Filtered results by process ID 11 and process ID 6064 (process creation) (Research data)

Next, the analyst scrolled through the events until Excel.exe as **the Original FileName,** could be observed. This interesting information is collected from a log file that corresponds to the logs generated when a user downloads and opens an Excel file. By expanding any log, the analyst can observe all information related to the event, either as a JSON or as a table. In Figure A-7, several fields indicate that the document in question was a Microsoft Excel file. Therefore, if the attacker masquerades as a file, changing the executable name, the analyst can use other fields to identify the type of file that is executed. This will be useful when looking for disguised PowerShell or CMD command execution.

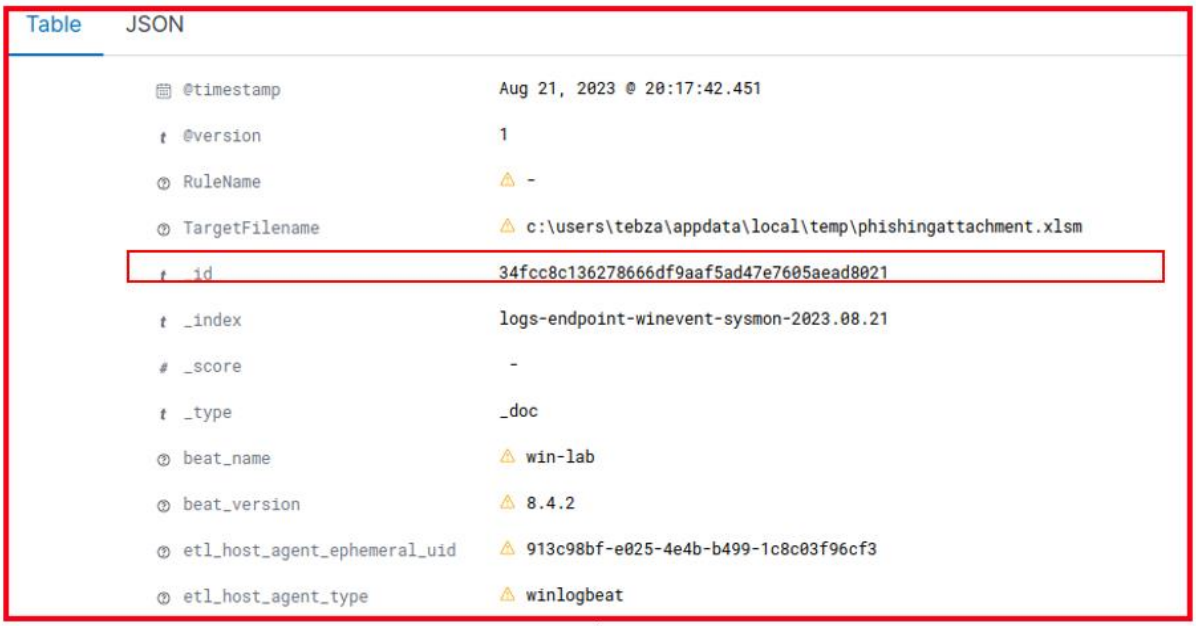


Figure 8-7: Excel process creation log entry - downloaded files (Research data)

Figure A-8 provides a closer look at the downloaded file, **targetFilename "PhishingAttachment.xlsm,"** on the victim machine**.**

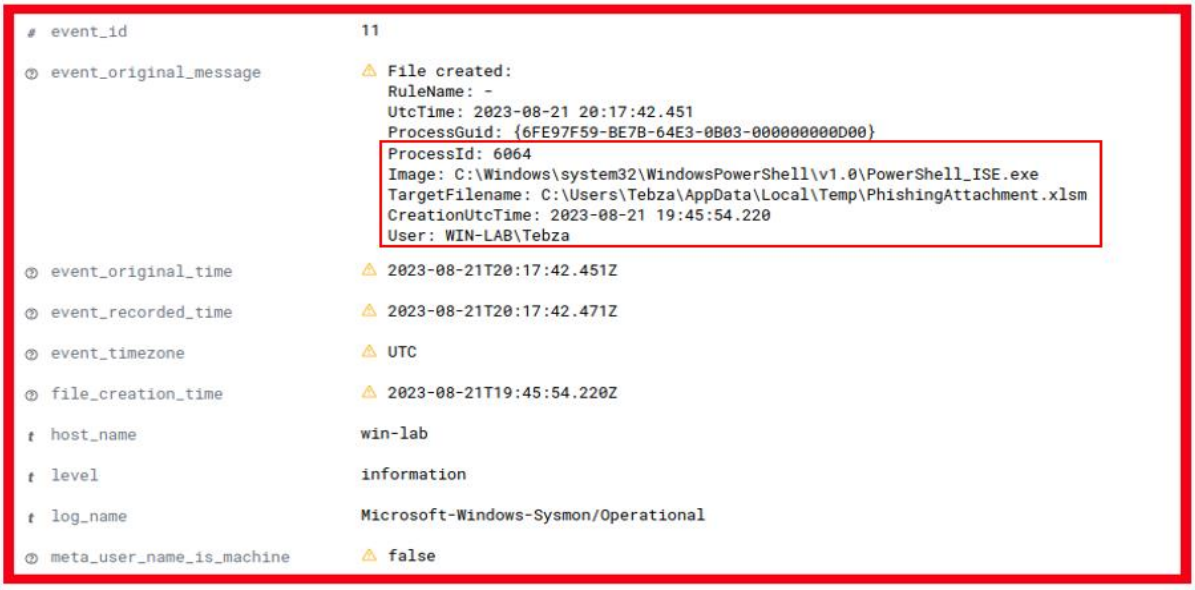


Figure 8-8: Excel process creation log entry – process executed and filed downloaded (Research data)

Figure A-8 expands upon Figure A-9 by further detailing the execution process of the Excel file and its download. Including details such as timestamps, initiating processes, and file paths would be beneficial for completeness. Figure A-9 indicates that for the file created in the background on the victim machine, the analyst is also able to run **FileCreate** queries if required to observe further attacks. Similar to previous figures but

focused on a different aspect of Excel process creation, such as file creation in the background. It is crucial to ensure that Figure A-9 highlights the steps taken by the threat hunting platform to capture and analyse these entries.

t	opcode	Info
t	process_guid	6FE97F59-BE7B-64E3-0B03-000000000D00
#	process_id	6,064
t	process_name	powershell_ise.exe
t	process_path	c:\windows\system32\windowspowershell\v1.0\powershell_ise.exe
t	provider_guid	5770385F-C22A-43E0-BF4C-06F5698FFBD9
t	record_number	10706
t	source_name	Microsoft-Windows-Sysmon
t	task	File created (rule: FileCreate)
#	thread_id	1,904

Figure 8-9: Excel process creation log entry (Research data)

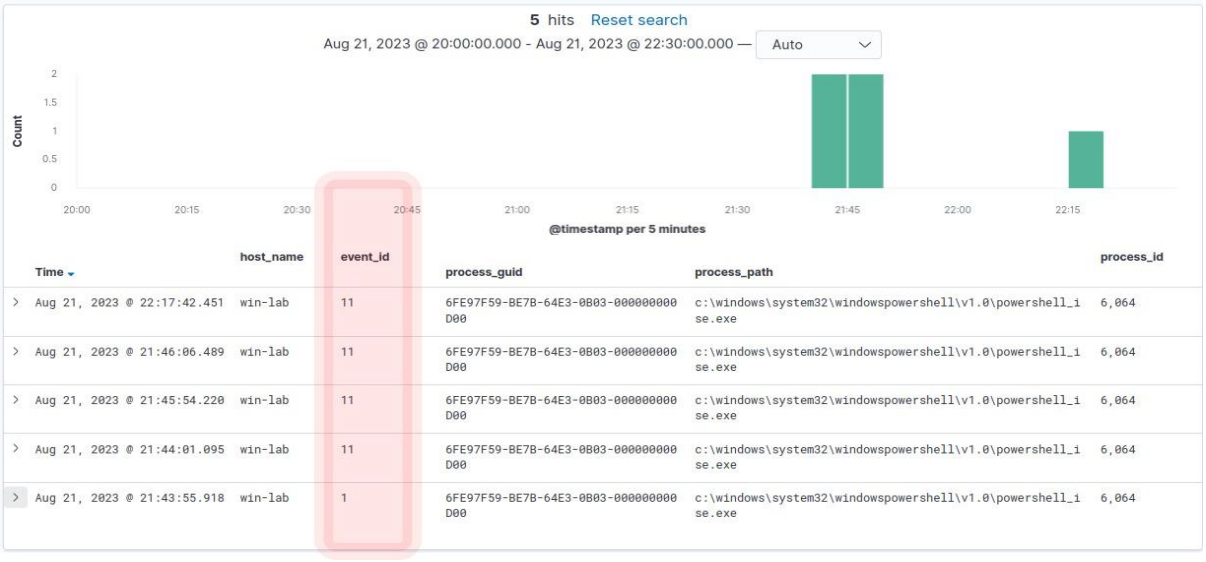
Figure A-10 provides information on the user and computer on which the malicious Excel file was executed. It shows the **FileCreate** process, the victim with the affected **computername,** and the user who is logged on.

t	source_name	Microsoft-Windows-Sysmon
t	task	File created (rule: FileCreate)
#	thread_id	1,904
t	type	wineventlog
ⓘ	user_account	⚠ win-lab\tebza
t	user_domain	win-lab
t	user_name	tebza
#	version	2

Figure 8-10: Excel process creation log entry – computer name and user logged in (Research data)

The analyst now has to narrow down the list of events to observe using different filters to identify malicious documents connected to the Internet. The analyst used a filter to select all logs with an **event_id** value of 11, as shown in Figure 8-11. This process, aligned with

sysmon event ID 11, identifies file creation events. Figure 8-11 is similar to Figure 8-5, but may focus on a different set of criteria for filtering or a subsequent step in the analysis.



Time	host_name	event_id	process_guid	process_path	process_id
Aug 21, 2023 @ 22:17:42.451	win-lab	11	6FE97F59-BE7B-64E3-0B03-000000000D00	c:\windows\system32\windowspowershell\v1.0\powershell_ise.exe	6,064
Aug 21, 2023 @ 21:46:06.489	win-lab	11	6FE97F59-BE7B-64E3-0B03-000000000D00	c:\windows\system32\windowspowershell\v1.0\powershell_ise.exe	6,064
Aug 21, 2023 @ 21:45:54.220	win-lab	11	6FE97F59-BE7B-64E3-0B03-000000000D00	c:\windows\system32\windowspowershell\v1.0\powershell_ise.exe	6,064
Aug 21, 2023 @ 21:44:01.095	win-lab	11	6FE97F59-BE7B-64E3-0B03-000000000D00	c:\windows\system32\windowspowershell\v1.0\powershell_ise.exe	6,064
Aug 21, 2023 @ 21:43:55.918	win-lab	1	6FE97F59-BE7B-64E3-0B03-000000000D00	c:\windows\system32\windowspowershell\v1.0\powershell_ise.exe	6,064

Figure 8-11: Filtering results by process ID (Research data)

Thus far, the analysis has identified the GUID of this PowerShell instance, **6FE97F59-CE85-64E3-5D02-000000000D0**, and the name of the suspicious file, **PhishingAttachment.xlsm**. There is no indication that the file has been opened or the macro has been executed, ensuring that the victim remains uncompromised. Figure 8-12 summarises the overall log data related to spear-phishing attacks.

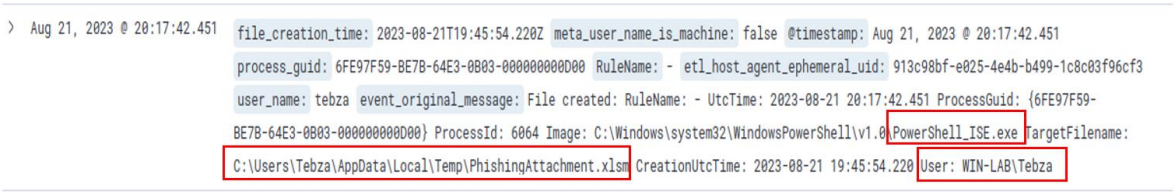


Figure 8-12: Overall log (Research data)

The logs in Figure 8-12 confirm the use of PowerShell to execute and download the "**PhishingAttachment.xlsm**" file, affecting a user named "**Tebza**" on a computer with the hostname **WIN-LAB**. This internal spear-phishing lateral movement attack illustrates the use of a PowerShell script to download a malicious Excel file, demonstrating the capability of lateral movement by maintaining an attacker's foothold on a victim machine.

3. Simulation 3: Pass-the-Hash (PtH) and Windows Management Instrumentation (WMI)

The third simulation focused on the Pass-the-Hash (PtH) technique ID T1550.002 and Windows Mmanagement Instrumentation (WMI) T1047. These techniques are commonly used together in lateral movement within a network. PtH allows attackers to authenticate to remote systems using a captured NTLM hash without needing the plaintext password, while WMI is often leveraged to execute commands remotely across multiple machines. The hypothesis for this simulation was that HELK would detect anomalies in authentication logs and remote command executions, flagging them as suspicious activities indicative of lateral movement.

Table 8-3: PtH and WMI simulation tool

Tool	Name
Cobaltstrike	Offensive tool
Mimikatz	Offensive tool

The simulation began with the execution of these tools, targeting the compromised systems **WIN-LAB-02** and **WINDC02**, as shown in Figure A-13. The attack utilised beacons from the PowerShell command line tools to establish connections back to the attacker's machine, as shown in Figure A-14. This process also involved dumping credentials from compromised systems, leveraging Mimikatz to obtain hashes.

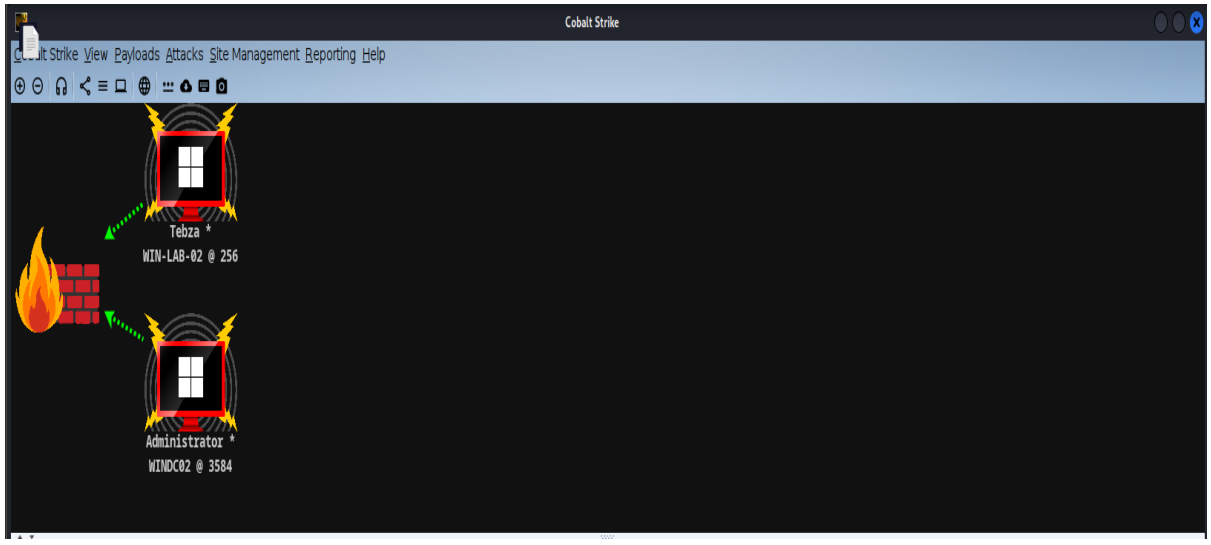


Figure 8-13: Compromised computers (Research data)

The compromised systems are connected back to the attacker machine using beacons from the PowerShell command line tool, as shown in Figure A-14 and Figure A-15. The computers **WINDC02** and **WIN-LAB-02** with beacons connect to the attacker's command and control system.

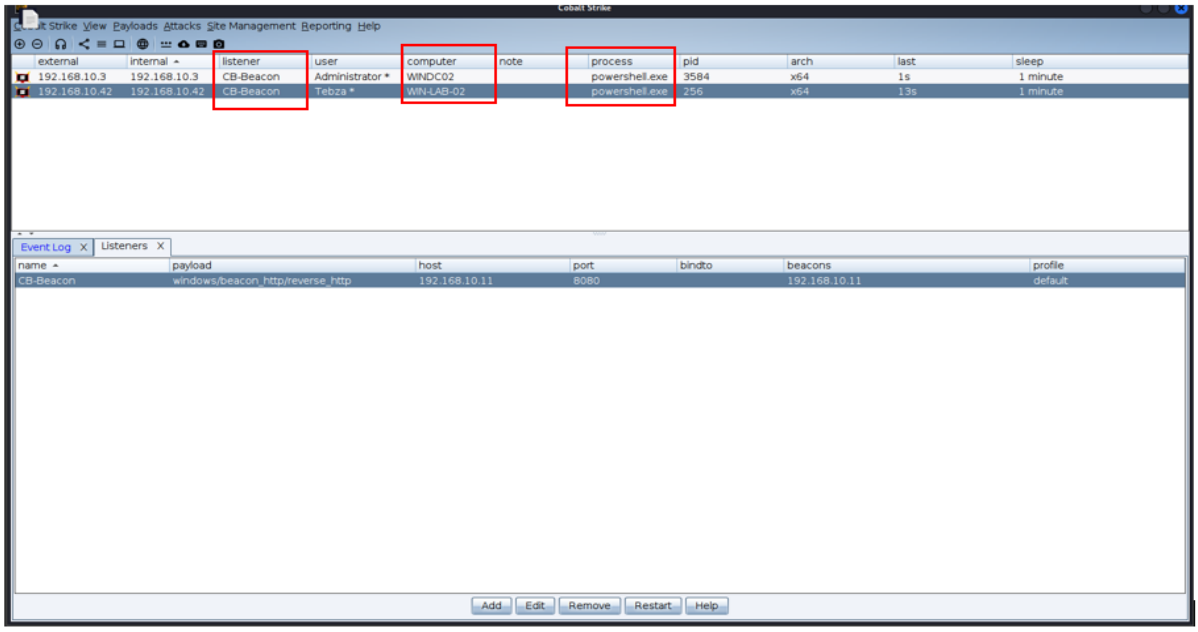


Figure 8-14: Beacon connected (Research data)

Following the establishment of the beacon, credentials were dumped from **the WINDC02** and **WIN-LAB-02** in Figure A-16. A command hashdump was employed to extract credentials, revealing accounts with accessible hashes.

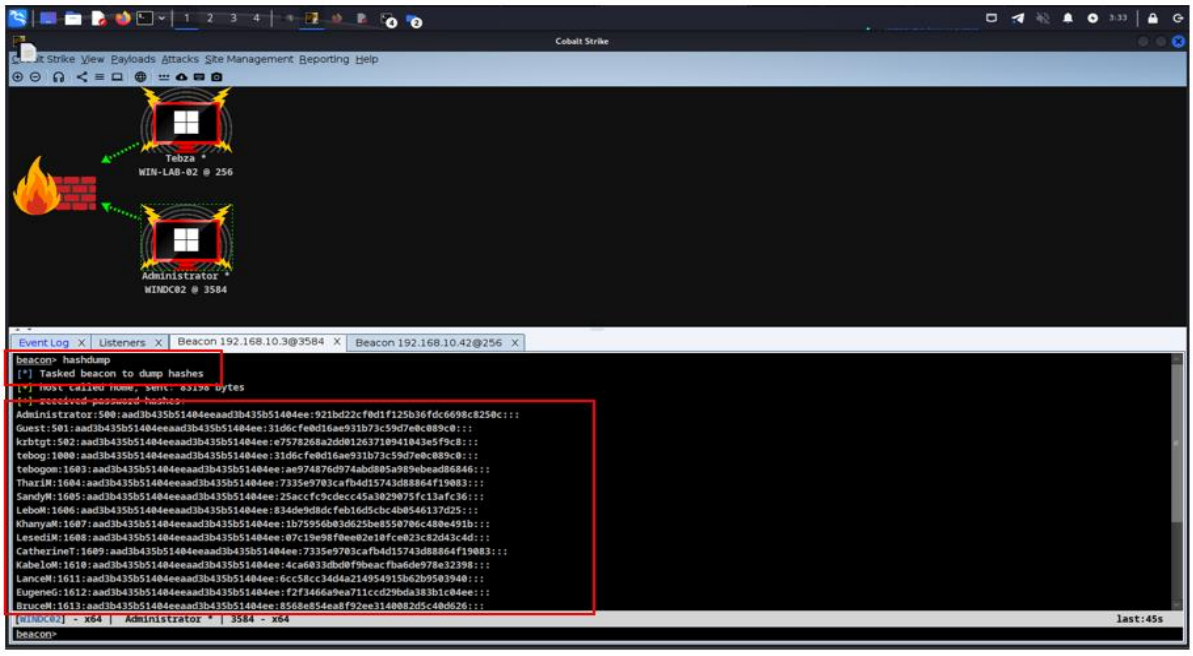


Figure 8-15: Credential dump WINDC02 (Research data)

Dumping of credentials from the second compromised system **WIN-LAB-02**, as shown in Figure A-16 and A-17, showing accounts whose credentials have been dumped using the same **hash-dump** command.

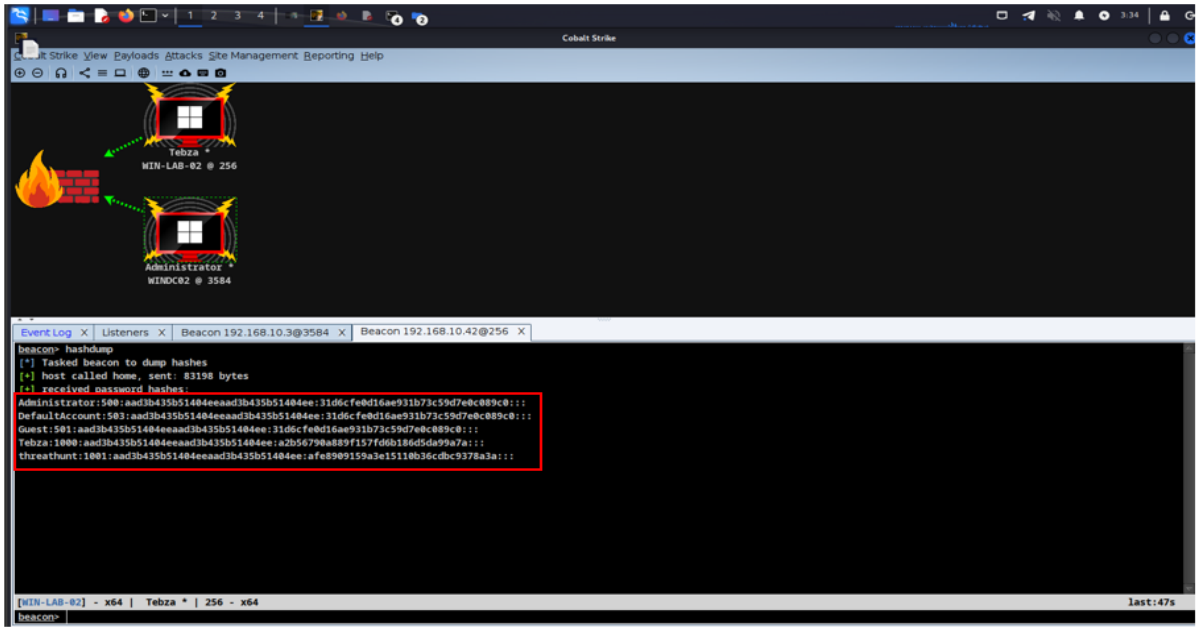


Figure 8-16: Credential dump WIN-LAB-02 (Research data)

The "**getuid**" command confirmed the logged-in users, identifying the **administrator** on **WINDC02** (Figure A-17) and the user **Tebza** on **WIN-LAB-02** (Figure A-18). The attacker verifies the presence of administrative privileges, which are essential for executing further commands and maintaining control over compromised systems.

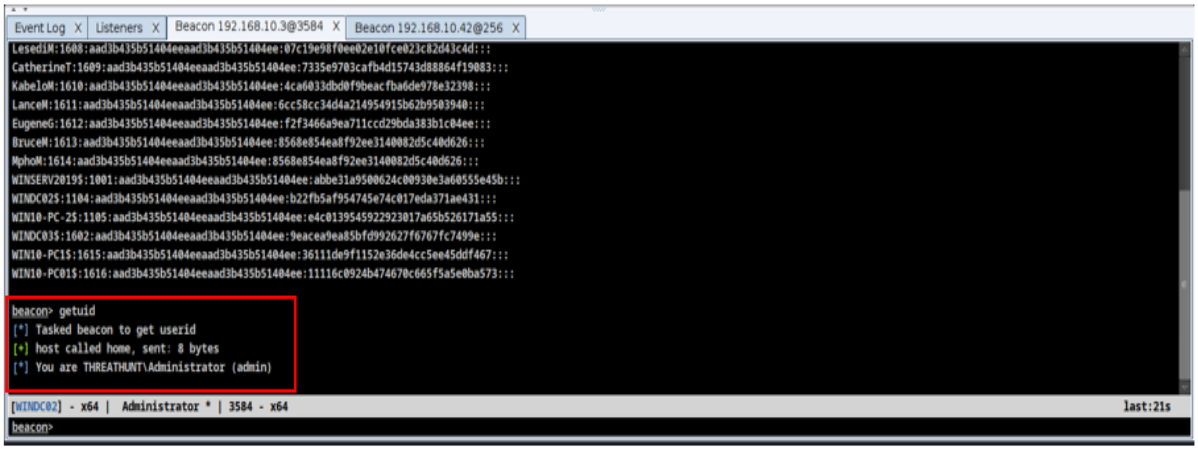


Figure 8-17: GetUID WINDC02 (Research data)

Logged on user "**Tebza**" on, **"WIN-LAB-02"**, as shown in Figure A-18, which also indicates that the attacker is also an administrator of the compromised system on which the attacker is logged in.

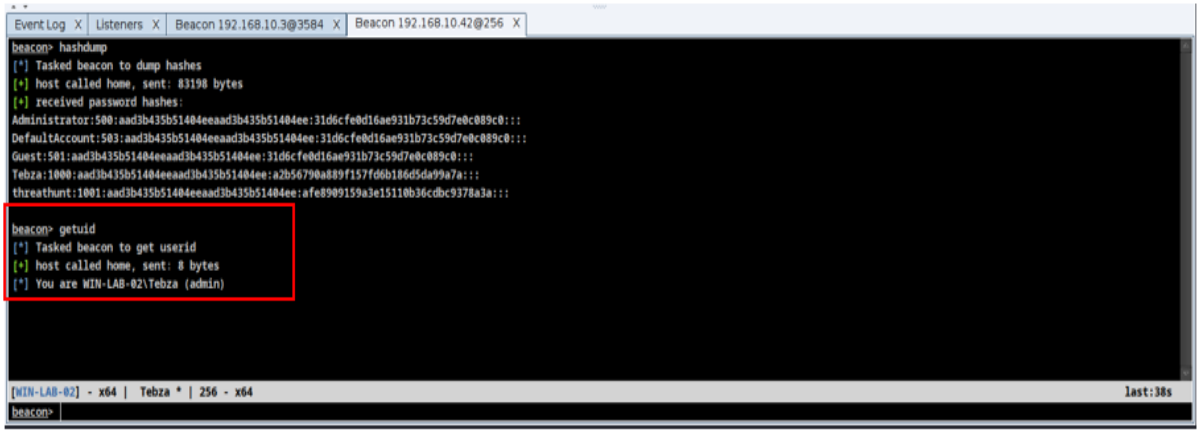


Figure 8-18: GetUID WIN-LAB-02 (Research data)

The consolidated view of the dumped credentials from both compromised systems is illustrated in Figure A-19. This aggregation of credentials provided the attacker with a comprehensive list for potential use in lateral movement.

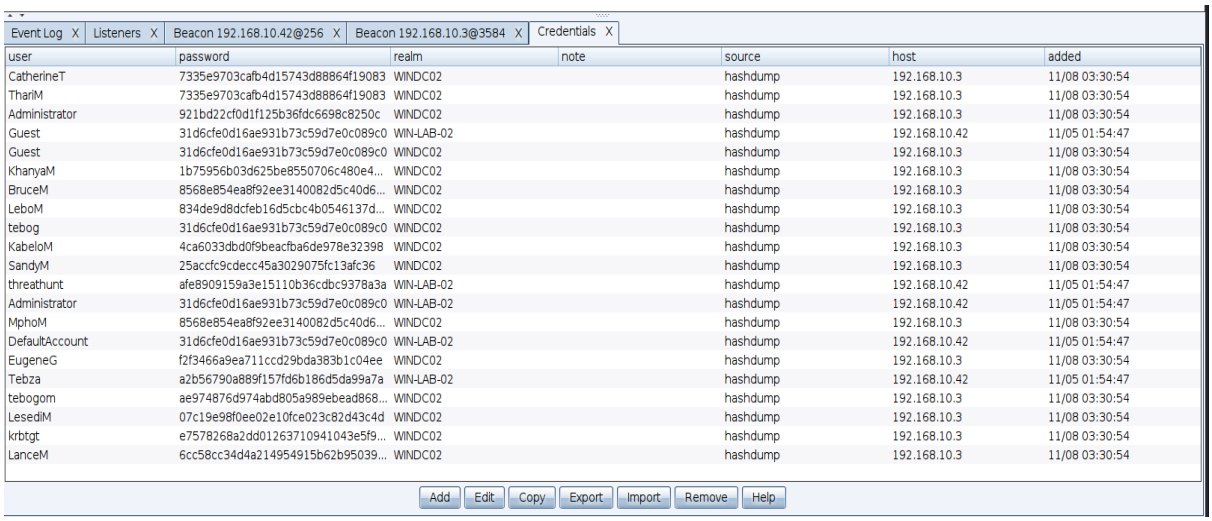


Figure 8-19: Consolidated view of dumped credentials from both compromised systems (Research data)

The attacker then attempts to move laterally on the network by accessing a share on another computer on the network. Figure A-20 shows that the attacker first attempts to access the share with the credentials of the user, who is currently logged in and presented with denied access. This indicates that the credentials of the currently logged-in user on the **WIN-LAB-02** system do not have sufficient access to move laterally. The next step is to use other credentials from the list of dumped credentials. This can be accomplished through a PtH attack.

Figure 8-20: Attempting to access shares (Research data)

The attacker attempted PtH using the **mimikatz** tool by executing the command **mimikatz sekurlsa:: pth /user:Tebza /domain:threat.hunt /ntlm:** (hash dump from credentials acquired earlier), as shown in Figure A-21.

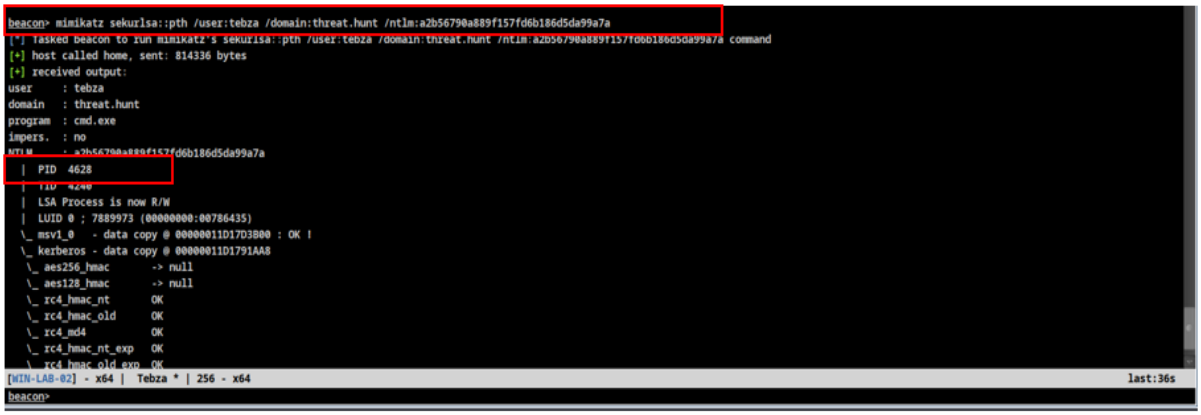


Figure 8-21: PtH technique (Research data)

The next step is to steal a token to mimic another user, which is accomplished by executing the **steal_token** command using PID 4628, as shown in Figure A-22 on the compromised system. The steal_token command is executed using **steal _token 4628**, as shown in Figure A-22.

Figure 8-22: Steal token (Research data)

In Figure A-23, a token is stolen, which impersonates the user on another machine with administrative privileges. This token is used to execute a **WMIC shell** to deploy a beacon that allows the attacker to move laterally. Figure A-24 shows the execution of the shell-wmic command, which indicates the successful establishment of remote access.

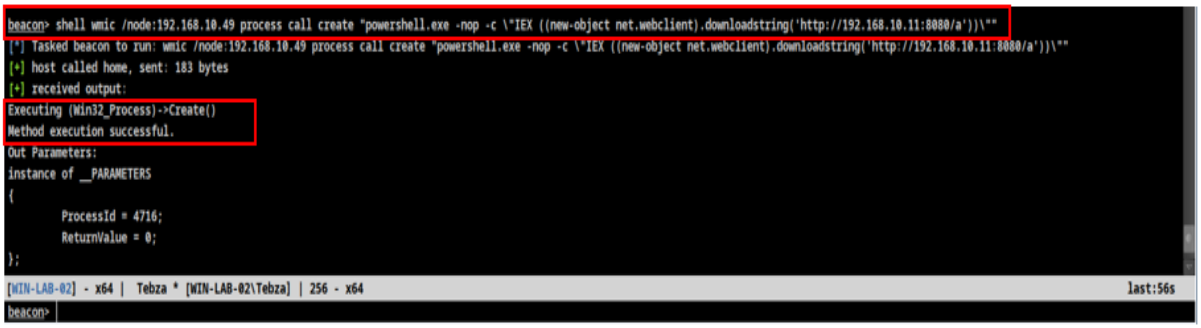


Figure 8-23: WMIC remote access (Research data)

With the remote access established in Figure A-24, indicates that a new system with the computer name **WIN-LAB** is compromised, indicating the successful execution of the lateral movement attack.

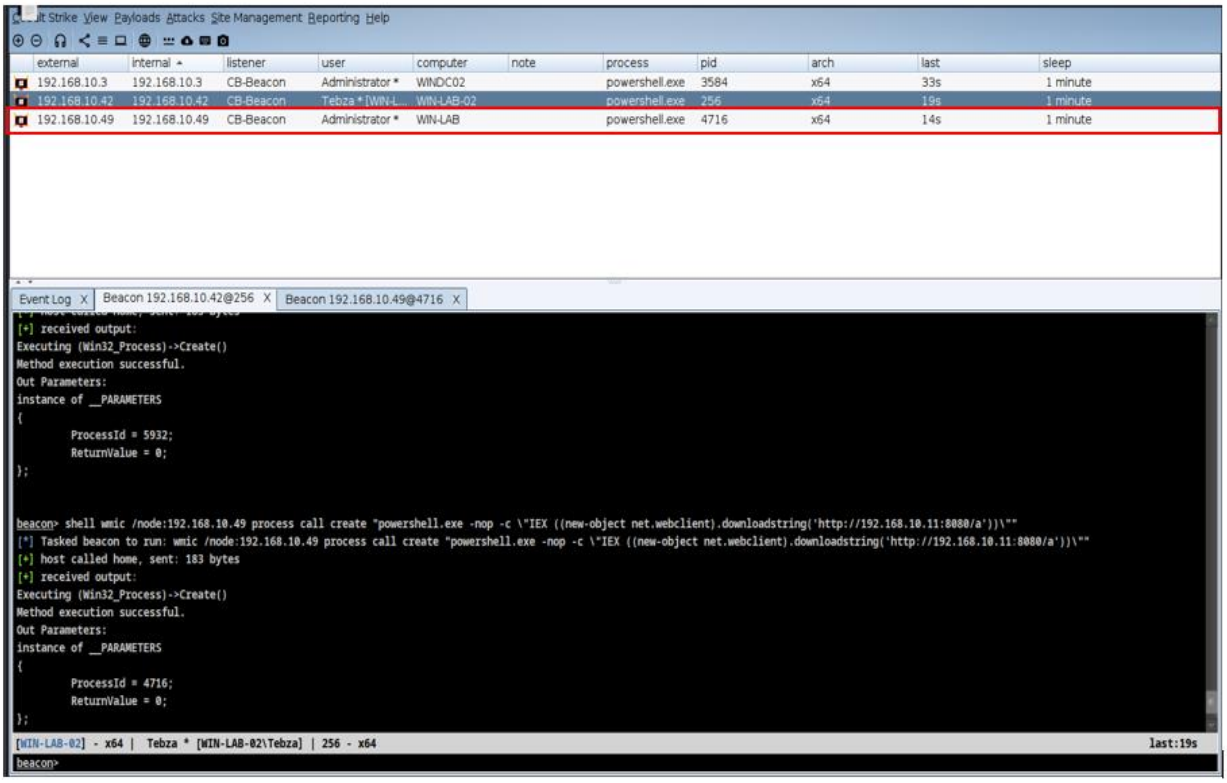


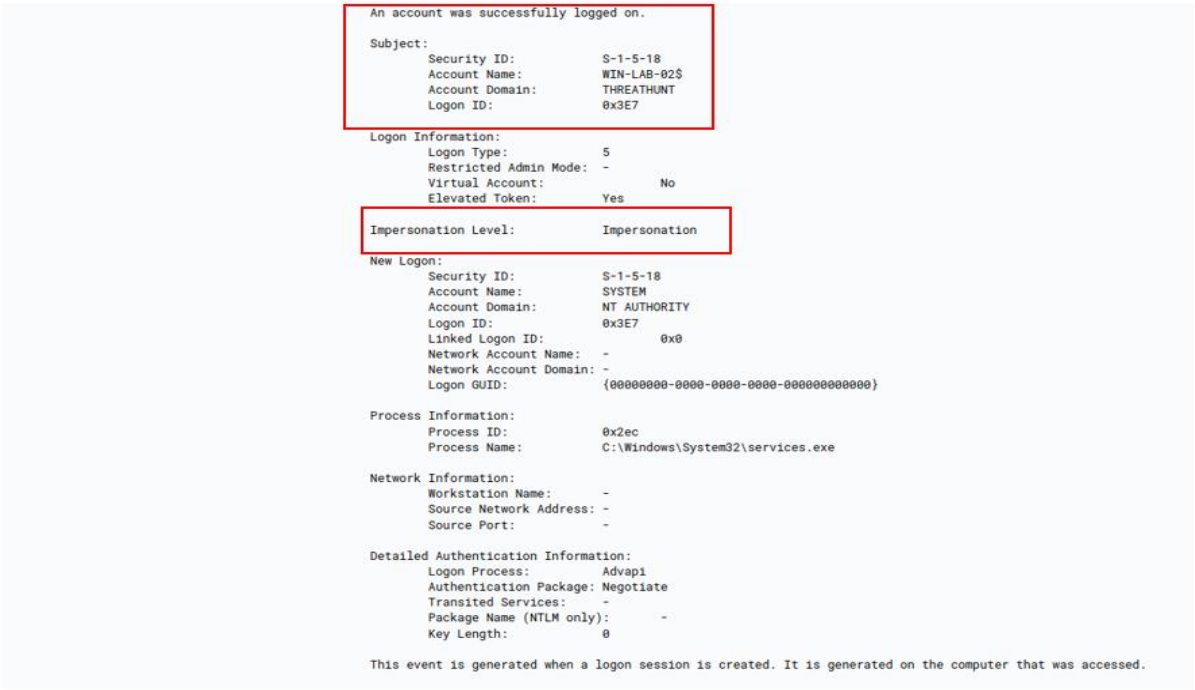
Figure 8-24: New compromised system (Research data)

On HELK, sysmon logs were monitored for indicators of PtH activity, including Event ID 4624 (logon event) and Event ID 4648. The analyst observes sysmon events related to WMI, such as process creation with WMI command-line syntax (Event ID 1) as well as process creation logs related to WMI usage, correlating them with authentication logs to trace potential lateral movements as shown in Figure A-25. The WMI execution logs corroborated these findings with specific indicators of remote access established using

stolen credentials. These events can also be viewed by executing the **event_id:3** query from the hunting platform, as shown in Figure A-26 as a starting point, based on the analysis to be performed.

Figure 8-25: Event query (Research data)

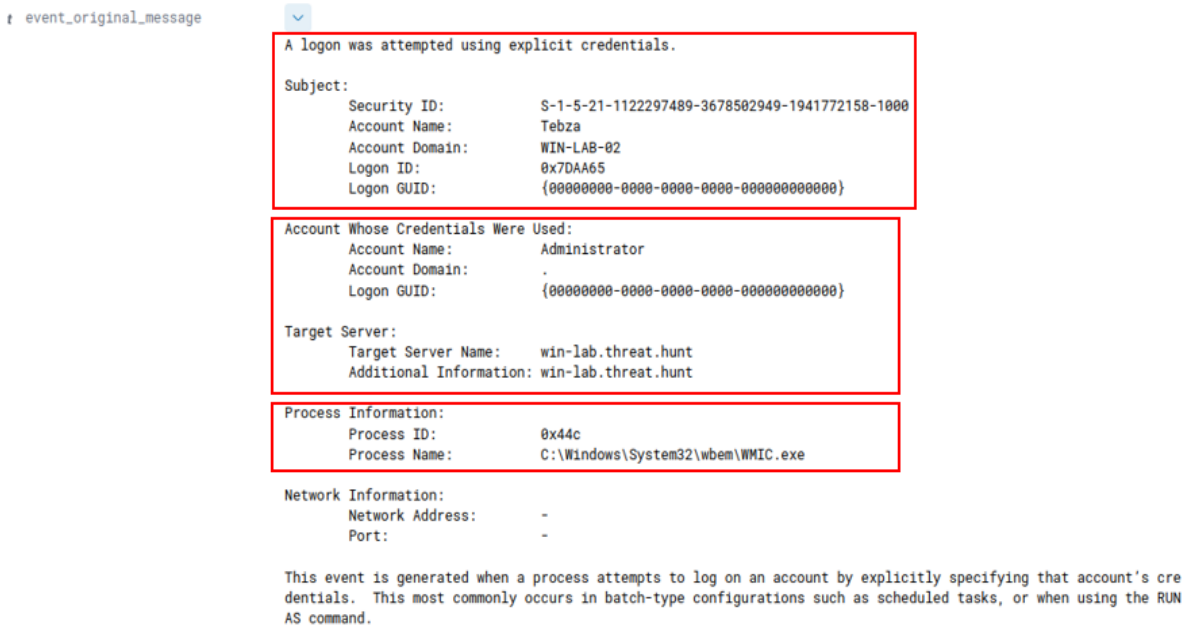
In addition to remote connections, the analyst performed other analyses on the hunting platform to determine any further compromise of the system and was able to find a remote login event using the administrator account from the impersonation attack, as indicated in Figure A-26. The events shown in Figure A-26 were generated when a login session was created. The subject fields indicate the account of the local system that requested a log-in. This is typically a service or a local process. The logon type field indicates the type of logon that occurred, with type 2 being an interactive logon and type 3 being a network logon. The impersonation-level field indicates the extent to which a process in the logon session is impersonated. Impersonation is performed using the initially compromised **WIN-LAB-02** system on the **WIN-LAB** system, as shown in Figure A-26.



```
An account was successfully logged on.

Subject:
        Security ID:            S-1-5-18
        Account Name:           WIN-LAB-02$
        Account Domain:         THREATHUNT
        Logon ID:               0x3E7

Logon Information:
        Logon Type:             5
        Restricted Admin Mode:  -
        Virtual Account:                No
        Elevated Token:         Yes

Impersonation Level:            Impersonation

New Logon:
        Security ID:            S-1-5-18
        Account Name:           SYSTEM
        Account Domain:         NT AUTHORITY
        Logon ID:               0x3E7
        Linked Logon ID:                0x0
        Network Account Name:   -
        Network Account Domain: -
        Logon GUID:             {00000000-0000-0000-0000-000000000000}

Process Information:
        Process ID:             0x2ec
        Process Name:           C:\Windows\System32\services.exe

Network Information:
        Workstation Name:       -
        Source Network Address: -
        Source Port:            -

Detailed Authentication Information:
        Logon Process:          Advapi
        Authentication Package: Negotiate
        Transited Services:     -
        Package Name (NTLM only):       -
        Key Length:             0

This event is generated when a logon session is created. It is generated on the computer that was accessed.
```

Figure 8-26: Remote login and impersonation (Research data)

As the analyst performed the analysis, further compromise indicators indicated that the WMI was processed and executed remotely using explicit credentials, which are the administrators in this case, as shown in Figure A-27. Impersonation is executed and the attacker moves laterally from **WIN-LAB-02 to WIN-LAB.**



```
t  event_original_message

A logon was attempted using explicit credentials.

Subject:
        Security ID:            S-1-5-21-1122297489-3678502949-1941772158-1000
        Account Name:           Tebza
        Account Domain:         WIN-LAB-02
        Logon ID:               0x7DAA65
        Logon GUID:             {00000000-0000-0000-0000-000000000000}

Account Whose Credentials Were Used:
        Account Name:           Administrator
        Account Domain:         .
        Logon GUID:             {00000000-0000-0000-0000-000000000000}

Target Server:
        Target Server Name:     win-lab.threat.hunt
        Additional Information: win-lab.threat.hunt

Process Information:
        Process ID:             0x44c
        Process Name:           C:\Windows\System32\wbem\WMIC.exe

Network Information:
        Network Address:        -
        Port:                   -

This event is generated when a process attempts to log on an account by explicitly specifying that account's cre
dentials.  This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUN
AS command.
```

Figure 8-27: WMI usage (Research data)

The analyst then found another indicator that indicated that the attacker, once lateral movement was achieved, was able to remotely implant a beacon, as shown in Figure A-28, which allows the **WIN-LAB** machine to establish a connection back to the attacker's main machine with **IP 192.168.10.11**, as shown in Figure A-28.

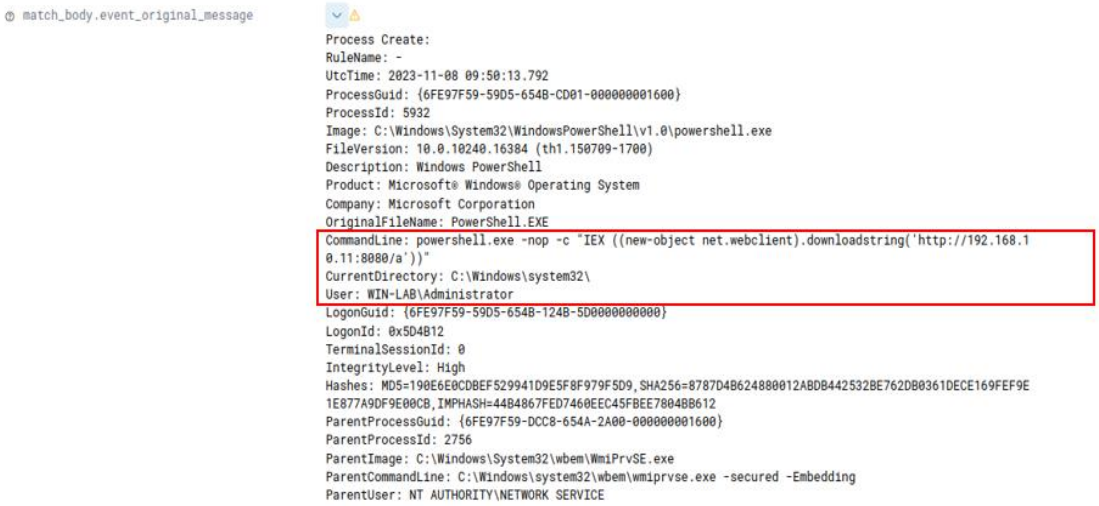


Figure 8-28: Beacon deployment (Research data)

Figure A-29 provides the analyst with a screenshot from the hunting platform that indicates the connection established from the attacker's system with the **IP address 192.168.10.11** to the victim's system with the name **WIN-LAB.**

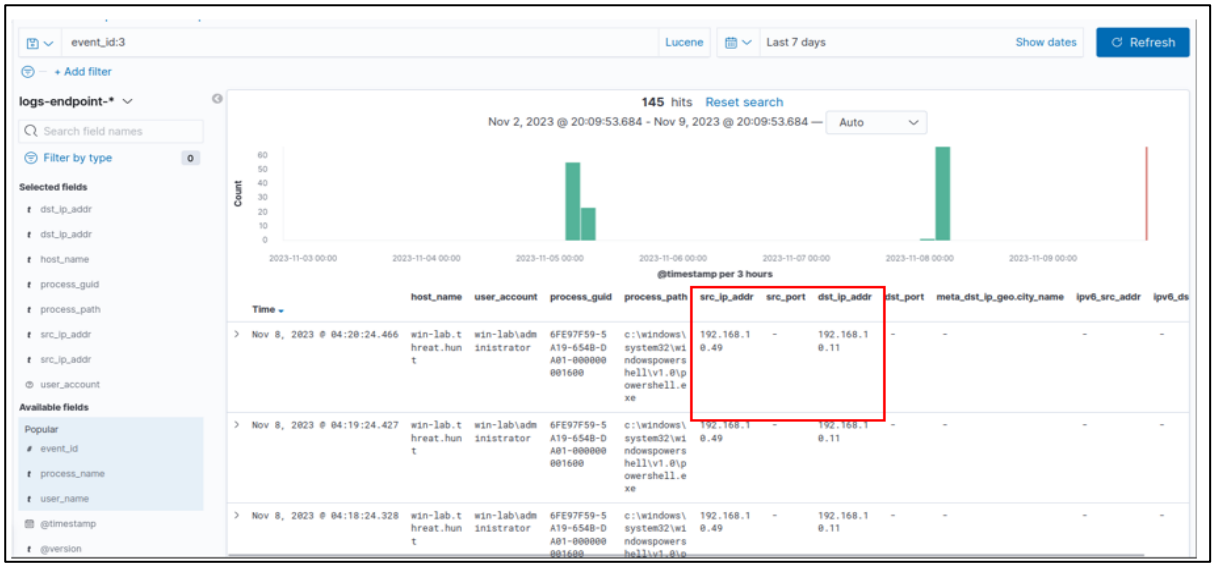


Figure 8-29: Remote connections (Research data)

Figure A-29 provides the analyst with IP address confirmation of connectivity between victim and attacker. Figure A-30 provides an overview of all impersonation events on the compromised host from a lateral movement attack. The categorisation of the impersonation levels in Figure 1-30 is as follows: "%% 1833" means impersonation, "%%1834" indicates delegation, and "%%1841" stands for access denied. These actions were observed during the lateral movement attack simulations.

Time	TargetFilename	host_name	process_name	event_id	ImpersonationLevel	process_path
Nov 8, 2023 @ 10:55:52.943	-	win-lab.threat.hunt	-	4,624	%%1833	-
Nov 8, 2023 @ 10:55:52.943	-	win-lab.threat.hunt	-	4,672	-	-
Nov 8, 2023 @ 10:54:02.467	-	win-lab.threat.hunt	-	4,634	-	-
Nov 8, 2023 @ 10:53:52.495	-	win-lab.threat.hunt	-	4,634	-	-
Nov 8, 2023 @ 10:53:52.495	-	win-lab.threat.hunt	-	4,634	-	-
Nov 8, 2023 @ 10:53:52.471	-	win-lab.threat.hunt	-	4,624	%%1833	-
Nov 8, 2023 @ 10:53:52.471	-	win-lab.threat.hunt	-	4,672	-	-
Nov 8, 2023 @ 10:53:52.464	-	win-lab.threat.hunt	-	4,624	%%1833	-
Nov 8, 2023 @ 10:53:52.464	-	win-lab.threat.hunt	-	4,672	-	-
Nov 8, 2023 @ 10:53:52.455	-	win-lab.threat.hunt	-	4,624	%%1833	-

Figure 8-30: Overview of impersonation events (Research data)

The analyst then observed all other events that were generated from the compromise, which indicated network connections, the execution of PowerShell from network connections, and the spawning of the WMI, as shown in Figure A-31.

Nov 8, 2023 @ 10:00:08.503	1f21ec3f-810d-4b0e-8045-322202e22b4b_0 PowerShell Network Connections	win-lab.threat.hunt	10	6FE97F59-5A19-654B-DA01-0000 00001600	win-lab\administrator
Nov 8, 2023 @ 10:00:08.270	1f21ec3f-810d-4b0e-8045-322202e22b4b_0 PowerShell Network Connections	win-lab.threat.hunt	10	6FE97F59-5A19-654B-DA01-0000 00001600	win-lab\administrator
Nov 8, 2023 @ 10:00:07.899	1f21ec3f-810d-4b0e-8045-322202e22b4b_0 PowerShell Network Connections	win-lab.threat.hunt	10	6FE97F59-5A19-654B-DA01-0000 00001600	win-lab\administrator
Nov 8, 2023 @ 10:00:07.738	1f21ec3f-810d-4b0e-8045-322202e22b4b_0 PowerShell Network Connections	win-lab.threat.hunt	10	6FE97F59-5A19-654B-DA01-0000 00001600	win-lab\administrator
Nov 8, 2023 @ 10:00:07.523	1f21ec3f-810d-4b0e-8045-322202e22b4b_0 PowerShell Network Connections	win-lab.threat.hunt	10	6FE97F59-5A19-654B-DA01-0000 00001600	win-lab\administrator
Nov 8, 2023 @ 10:00:07.215	1f21ec3f-810d-4b0e-8045-322202e22b4b_0 PowerShell Network Connections	win-lab.threat.hunt	10	6FE97F59-5A19-654B-DA01-0000 00001600	win-lab\administrator
Nov 8, 2023 @ 09:56:38.538	Sysmon_f4bbd493-b796-416e-bbf2-121235348529_0 Non Interactive PowerShell	win-lab.threat.hunt	2	6FE97F59-5A19-654B-DA01-0000 00001600	win-lab\administrator
Nov 8, 2023 @ 09:56:38.365	Sysmon_f4bbd493-b796-416e-bbf2-121235348529_0 Non Interactive PowerShell	win-lab.threat.hunt	2	6FE97F59-59D5-654B-CD01-0000 00001600	win-lab\administrator
Nov 8, 2023 @ 09:54:40.398	Sysmon_692f0bec-83ba-4d04-af7e-e884a96059b6_0 WMI Spawning Windows PowerShell	win-lab.threat.hunt	2	6FE97F59-5A19-654B-DA01-0000 00001600	win-lab\administrator
Nov 8, 2023 @ 09:54:39.964	Sysmon_692f0bec-83ba-4d04-af7e-e884a96059b6_0 WMI Spawning Windows PowerShell	win-lab.threat.hunt	2	6FE97F59-59D5-654B-CD01-0000 00001600	win-lab\administrator

Figure 8-31: Overview of other attack activities (Research data)

In summary, Windows uses access tokens to determine the ownership of the running process. The attacker manipulated the access tokens to make a running process appear as if it belonged to someone other than the user who started the process. The attacker uses access tokens to operate in a different user or system security context to perform the actions for which the event was detected on the hunting platform. The attacker was able to move laterally from the initially compromised **WIN-LAB-02** system to **WIN-LAB**. Once the attacker moved laterally, it was able to implant a beacon that enabled a remote connection back to the attacker machine, allowing the attacker to carry out further attacks.

4. Simulation 4: Lateral tool transfer

The fourth simulation focused on the lateral tool transfer technique, identified by the MITRE ATT&CK framework as T1570. This technique involves an adversary moving tools or files across the network to facilitate further exploitation and maintain persistence. The hypothesis for this simulation was that HELK would detect unusual file transfers and associated process creation events indicative of lateral tool transfer activities within the network. The setup for this simulation involved the attacker using **Cobalt strike** to transfer tools from a compromised machine (WIN-LAB-02) to another machine within the network (WIN-LAB). The tools transferred included a remote access trojan (RAT) and additional scripts designed to maintain access and further compromise the target system. The use of Cobalt Strike, as described in Table A-4, provided a realistic environment for observing the attack vector.

Table 8-4: Lateral tool transfer simulation tool

Tool	Name
Cobaltstrike	Offensive Tool

The execution of this attack continued from the previous lateral movement, transitioning from **the WIN-LAB-02** to the **WIN-LAB** system. With an established foothold, the attacker uploaded a file named "**Quasar.zip"** a remote access tool allowing persistent access and further lateral movement capabilities. Figure A-32 depicts the upload process, where the attacker executes the command to transfer the file from the attacker machine to the C-drive of the compromised system.

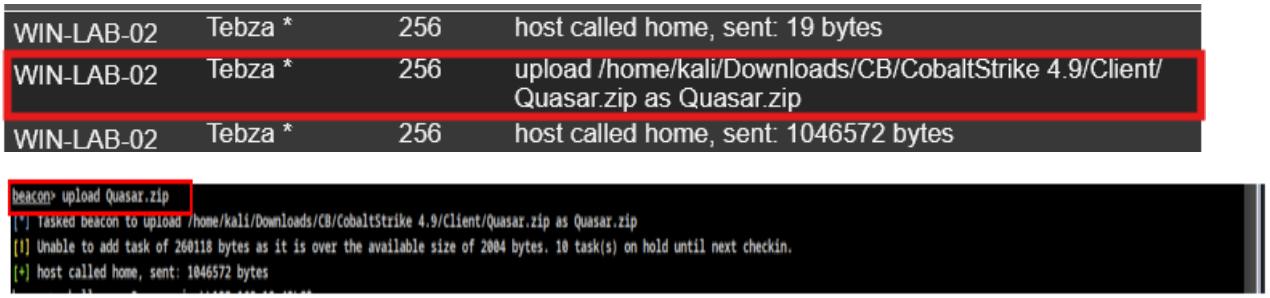


Figure 8-32: File upload attack (Research data)

The attacker then copies the file from the attacker machine to the victim or compromised system to the c drive of the system, which is achieved with the **command "shell copy Quasar.zip \\192.168.10.49\C$"** command, as shown in Figure A-33, demonstrating the execution of lateral transfer.

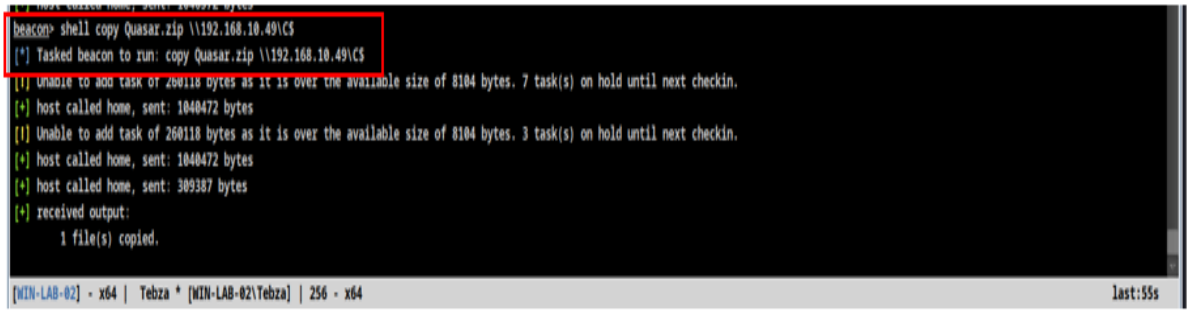


Figure 8-33: Lateral transfer execution (Research data)

The successful copy of the **Quasar.zip** file is shown in Figure A-34 and Figure A-35, indicating that the attacker is capable of extracting the file and running it on the local machine and vice versa.

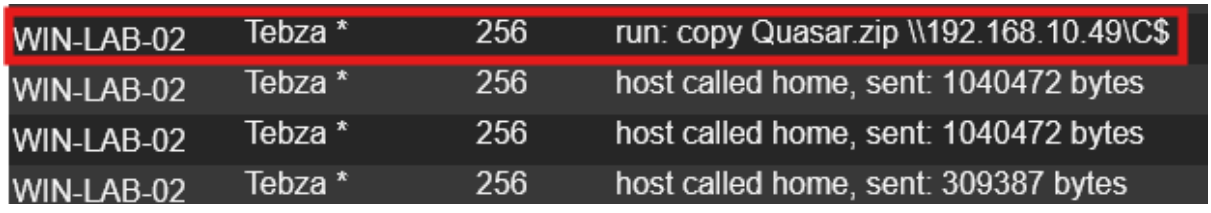


Figure 8-34: Quasar file copy (Research data)

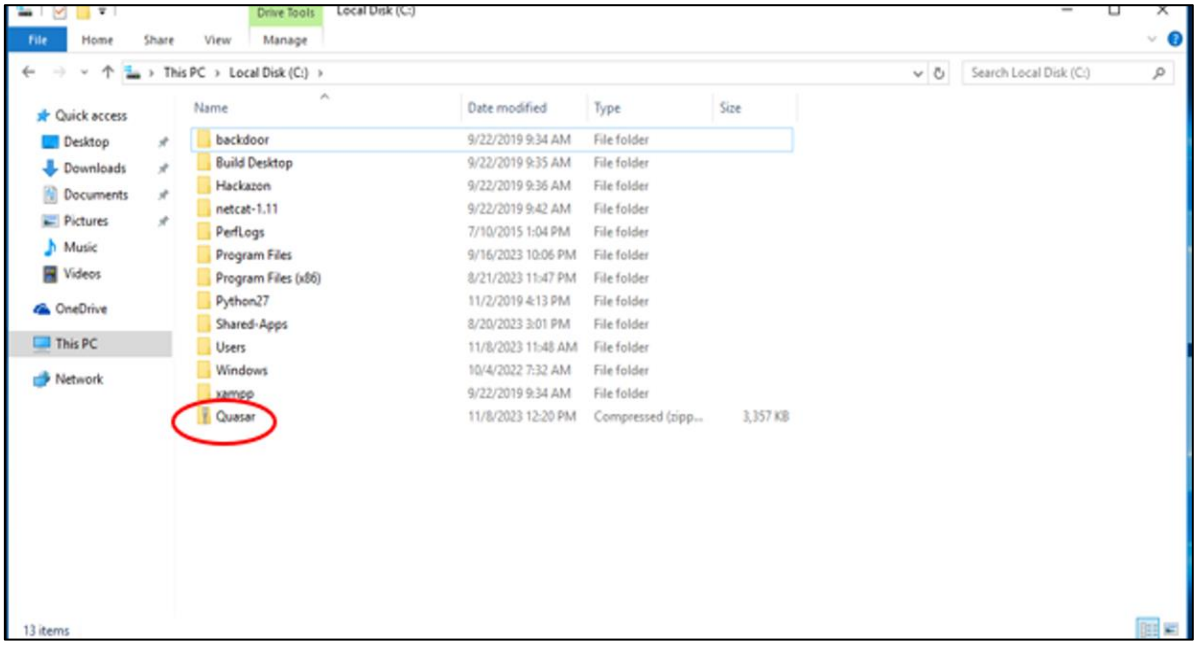


Figure 8-35: Quasar remote access tool (Research data)

In HELK, the analyst monitored sysmon events, particularly focusing on file creation (Event ID 11), process creation (Event ID 1), and network connections (Event ID 3). These events were crucial in identifying and analysing the lateral tool transfer activity. Figure A-36 shows the execution logs, revealing the activities associated with file transfers.

Figure 8-36: Overview of activities (Research data)

Figure A-37 shows all executions performed using a file copy. Because the connection between the compromised machine is encrypted, the compromised system was unable to generate the copy event specifically; however, it was able to indicate that from the WMI process from the earlier execution, suspicious activity was detected.

Figure 8-37: Further activities in the compromised system (Research data)

Figure A-37 shows other processes, including the execution of the local system file with a copy attack from the attacker machine on the compromised system. In summary, the simulation demonstrated the attacker's ability to transfer a file named **Quasar.zip** from the attacker's machine to the compromised system, as shown in the figures and activities detected on the hunt platform. This exercise underlines the importance of monitoring and analysing file transfer activities within a network to detect and prevent lateral movements..

5. Simulation 5: Remote services

The final simulation focused on the remote services technique, specifically the use of remote desktop protocol (RDP) in conjunction with the Quasar remote access trojan (RAT), identified by the MITRE ATT&CK framework as T1021.001. This technique involves an APT leveraging RDP to gain persistent remote access to a target system using a RAT like Quasar. The hypothesis for this simulation was that HELK would detect unauthorised RDP connections and the subsequent deployment of Quasar RAT, flagging these activities as indicative of lateral movement and remote access by an adversary.

The Quasar RAT, detailed in Table A-5, was employed to simulate the remote service technique. Quasar RAT is a known remote access tool that provides extensive control over compromised systems, making it an ideal choice for this simulation.

Table 8-5: Remote services simulation tool

Tool	Name
Quasar rat	Remote access tool

The simulation commenced with the installation and configuration of **the Quasar RAT** on the compromised **WIN-LAB** system, which was initially breached via a lateral file transfer attack. The quasar client is executed on the victim system once the client is ready for the victim system. Following the execution of the Quasar client, it began running in the background, as shown in Figure A-38.

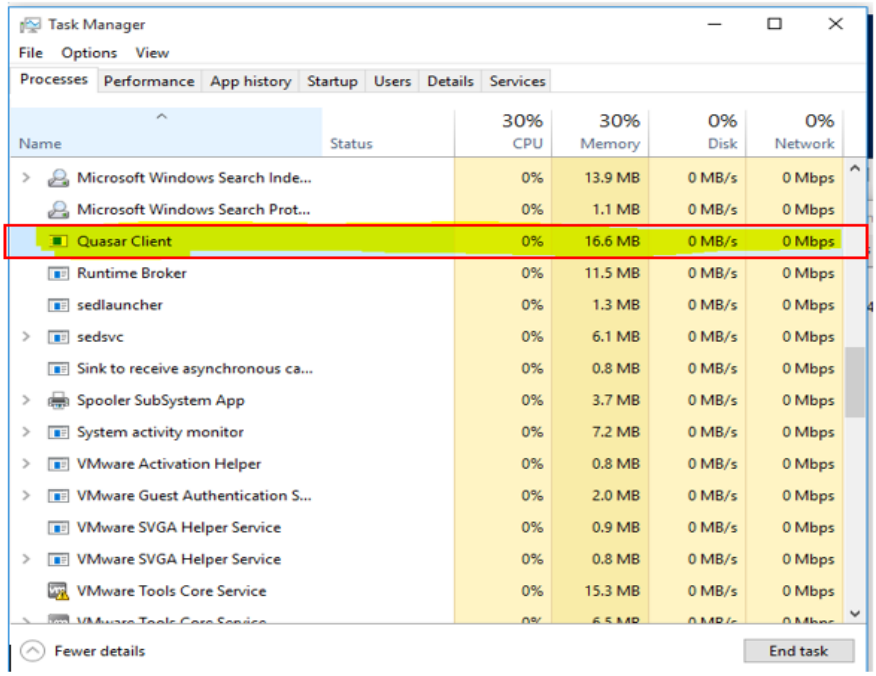


Figure 8-38: Quasar client process running as viewed in the task manager (Research data)

A remote connection was established between the attacker's machine and the compromised **WIN-LAB** system, as shown in Figure A-39. This connection allows the attacker to control the victim system remotely.

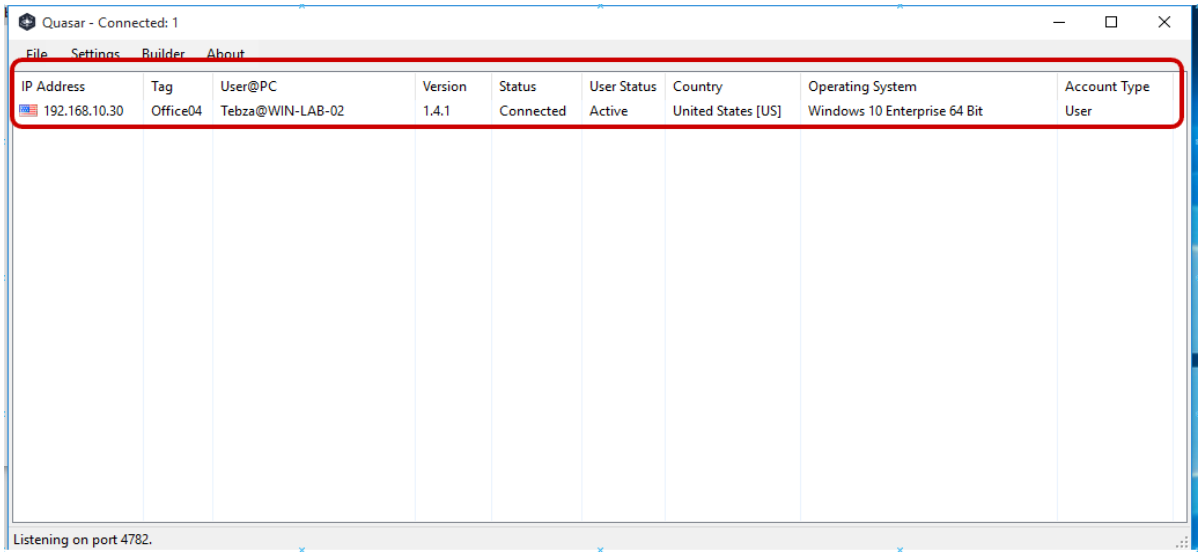


Figure 8-39: Exploring the quasar connection (Research data)

The remote desktop session, shown in Figure A-39, illustrates the attacker's control over the victim system, indicating the use of the Quasar RAT to facilitate remote access. The attacking machine with **IP:192.168.10.30**, is connected to the victim system **WIN-LAB**

with the compromised user '**Tebza**' from the **WIN-LAB-02** system as shown in Figure A-40.

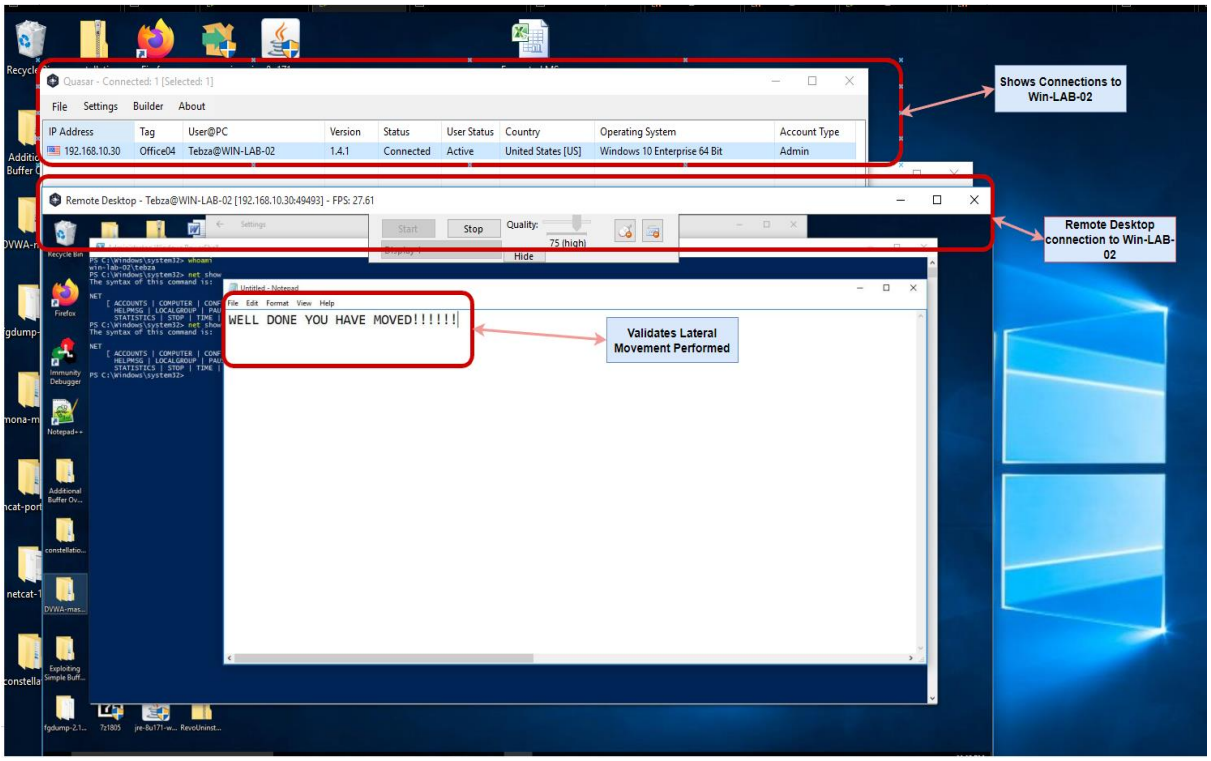


Figure 8-40: Remote desktop session on the victim system (Research data)

The analyst's threat hunt is conducted by monitoring the logs forwarded from the victim machine for events related to RDP connections, file transfers, and command executions. Investigation of sysmon events such as process creation with event ID 1, network connections with event ID 3, and file creation with event ID 11: The threat hunt involved monitoring logs forwarded from the victim machine for events related to RDP connections, file transfers, and command executions. Key sysmon events, such as process creation (Event ID 1), network connections (Event ID 3), and file creation (Event ID 11), were scrutinised. The forwarded events depicted in Figure A-41, provide a comprehensive overview of the activities monitored by analysts.

	Time	host_name	process_name	@timestamp per 3 hours activity_id
>	Aug 21, 2023 @ 22:06:20.448	win-lab	gup.exe	-
>	Aug 21, 2023 @ 22:06:19.993	win-lab	svchost.exe	-
>	Aug 21, 2023 @ 22:06:19.837	win-lab	notepad++.exe	-
>	Aug 21, 2023 @ 22:03:08.433	win-lab	-	-
>	Aug 21, 2023 @ 22:01:27.818	win-lab	taskmgr.exe	-
>	Aug 21, 2023 @ 22:01:27.190	win-lab	taskmgr.exe	-
>	Aug 21, 2023 @ 22:00:00.318	win-lab	svchost.exe	-
>	Aug 21, 2023 @ 22:00:00.292	win-lab	schtasks.exe	-
>	Aug 21, 2023 @ 22:00:00.242	win-lab	schtasks.exe	-
>	Aug 21, 2023 @ 21:59:30.662	win-lab	quasar.exe	-
>	Aug 21, 2023 @ 21:59:30.662	win-lab	quasar.exe	-
>	Aug 21, 2023 @ 21:59:30.646	win-lab	quasar.exe	-
>	Aug 21, 2023 @ 21:59:30.646	win-lab	quasar.exe	-
>	Aug 21, 2023 @ 21:59:21.750	win-lab	-	{994784F5-D364-0000-0F85-479964D3D901}
>	Aug 21, 2023 @ 21:59:21.748	win-lab	-	{994784F5-D364-0000-0F85-479964D3D901}
>	Aug 21, 2023 @ 21:59:21.210	win-lab	client-built.exe	-
>	Aug 21, 2023 @ 21:59:20.241	win-lab	svchost.exe	-
>	Aug 21, 2023 @ 21:59:20.227	win-lab	client-built.exe	-

Figure 8-41: Forwarded events from the victim machine (Research data)

In summary, the simulation demonstrated how attackers could use RDP connections facilitated by the Quasar RAT to control the machines within a network. This simulation highlights the importance of monitoring and analysing such activities to detect lateral movement attacks. Through a careful investigation of the HELK platform, analysts can identify anomalies and patterns in the data, validating the hypothesis that RDP can be exploited for lateral movement. This study successfully conducted five simulations of lateral movement attacks, each revealing potential threats and detection capabilities within a controlled laboratory environment.

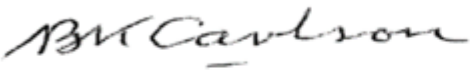
Chapter 9 Annexure: Confirmation of language editing

8 Nahoon Valley Place
Nahoon Valley
East London
5241
2 March 2025

TO WHOM IT MAY CONCERN

I hereby confirm that I have edited the following thesis using the Windows 'Tracking' system to reflect my comments and suggested corrections for the student to action and produce a clean copy.

A methodological approach to investigating lateral movement attacks using a threat hunting architecture by T Mokoena, a dissertation submitted in fulfilment of the requirements for the degree Master of Science in Computer Science at the North-West University.



Brian Carlson (B.A., M.Ed.)
Professional Editor

Email: bcarlson521@gmail.com
Cell: 0834596647

Disclaimer: Although I have made comments and suggested corrections, the responsibility for the quality of the final document lies with the **student** in the first instance and not with myself as the editor.