SEC7001

Cloud and Network Security

Master's Project

Prepared by AUSTIN ORUMWENSE M.Sc. (Hons)

Student ID: 2214630

THE IMPACT OF EMERGING CLOUD SECURITY THREATS: A FOCUS ON ADVANCED PERSISTENT THREATS

School of Arts and Creative Technologies

Supervisor: Dr Mansoor Ihsan

A report submitted in the partial fulfilment for the MSc degree in Cloud and Network Security

University Of Bolton August 2023

DECLARATION

I hereby declare that this project, "The Impact of Emerging Cloud Security Threats: A Focus on Advanced Persistent Threats" is my own work and has not been submitted in any form to any other educational institution. All sources used in this project have been cited and referenced.

ABSTRACT

The rapid advancement in cloud computing technology is in a constant state of evolution with threat actors continuously refining their tactics, exploiting new vulnerabilities, and expanding their scope of influence. This dynamic environment exposes it to a range of emerging cyber-attacks, including Advanced Persistent Threats (APT) impacting both customers and service providers. The need for researchers to understand the gap in the literature regarding APT detection has become crucial. In response to this urgent need, this thesis investigates the impact of Advanced Persistent Threats in cloud environments and proposes effective mitigation strategies. The research aims to comprehensively understand APTs' influence on cloud security, analyse existing approaches, emulate APT adversary plans, simulate attacks using Mitre Caldera, employ Snort for detection and utilize Nessus Vulnerability scanning tool. The study answers critical questions about APTs' exploitation of cloud environments, strengths, and weaknesses of mitigation methods, impacts of successful APT attacks, vulnerabilities in cloud infrastructures, and techniques for detecting APTs.

In synthesis, the research findings underscore the intricate interplay between APT activities and cloud environments, emphasizing the exigency for robust detection and mitigation strategies. The amalgamation of APT simulation, vulnerability assessment, and analysis of detection mechanisms yields invaluable insights into the evolving threat landscape within cloud ecosystems. With organizations increasingly embracing cloud technologies, the lessons derived from this study substantially contribute to the ongoing discourse on fortifying cloud security against persistent and evolving cyber threats.

Keywords: Advanced Persistent Threats (APT), cloud security, emulation, Mitre Caldera, vulnerability scanning, adversary emulation.

ACKNOWLEDGEMENT

I would like to extend my heartfelt appreciation to my thesis supervisor, Dr. Ihsan Mansoor, for his invaluable guidance and unwavering support throughout this journey. I am also grateful to the educators at the Creative Technology Department of the University of Bolton for their insights and mentorship during my master's program; the school provided access to some tools that were instrumental in my research. My colleagues' contributions have also been invaluable, and I extend my gratitude to them for the insightful discussions we shared. A special thank you goes to my mother for her encouragement, prayers, and constant motivation. This accomplishment is dedicated to all of you.

CONTENTS

LIST OF ABBREVIATIONS

APT	Advanced persistent threat
AWS	Amazon Web Services
ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge
C&C/C2	Command and Control
CVE	Common vulnerability and exposures
DNS	Domain Name System
EC2	Elastic Compute Cloud
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICT	Information computer technology
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPS	Intrusion Prevention System
IT	Information technology
OS	Operating System
SDN	Software Defined Networking
SIEM	Security Information and Event Management
TTPs	Tactics, techniques, and procedures
UDP	User Datagram Protocol
URL	Uniform Resource Locator
VM	Virtual Machine
VPN	Virtual Private Network

LIST OF APPENDICES

LIST OF TABLES

LIST OF FIGURES

1.0 INTRODUCTION

1.1 Background

Cloud computing is swiftly growing in popularity, driven by a blend of market dynamics and technological advancements. Evolving business landscapes are spurring transformations in company computing infrastructures. The count of enterprise services and applications is consistently rising, with continual additions and retirements of both new and old offerings. The term 'cloud computing' has been subject to various interpretations from both academic and practical perspectives, resulting in divergent definitions. Buyya et al. (2010) view cloud computing as the "fifth utility", comparable to water, gas, electricity, and telephone services. According to this perspective, cloud computing involves convenient and readily accessible computing services, akin to other utility services. However, Kim (2009) challenges this definition, arguing that utility computing is merely a subset of service cloud computing. The National Institute of Standards and Technology (NIST) presents a succinct interpretation, characterizing cloud computing as a framework facilitating widespread, user-friendly, and readily available network entry to a communal reservoir of adaptable computational assets (Mell and Grance, 2011). This study adopts NIST's definition, as it outlines a cloud model with five essential characteristics, three service models, and four deployment models. Different service models cater to various business needs, with three main models being SaaS, PaaS, and IaaS. SaaS, or Software as a Service, offers internet-accessible applications. PaaS, or Platform as a Service, provides a cloud-based platform for users to develop and deliver applications. IaaS, or Infrastructure as a Service, offers on-demand access to infrastructure components such as storage, networks, and servers via the web (Singh et al., 2023). Alongside these models, there are four key actors in cloud computing: cloud providers, consumers, carriers, and auditors.

The high availability and dependability of computing services inside cloud environments have become critical as cloud computing has become the primary means of delivering IT services (Zhang et al., 2019). To prevent service disruptions, it is imperative to proactively identify potential vulnerabilities and establish robust defence mechanisms in advance. Large-scale data centres have become the preferred choice for hosting internet and business applications, with a significant shift from traditional infrastructure. These data centres house enormous clusters of servers and storage systems, and there are even plans to construct facilities that can accommodate over a million servers (Tang et al., 2018). While some data centres are dedicated to running applications for a single company, like the search engine clusters managed by Google, others are operated by service providers who offer storage and computational resources to customers at remarkably low costs due to their extensive scale.

Emerging attacks are threats that have just been discovered or were previously unknown, whereas zero-day attacks exploit flaws that software vendors have not yet addressed (Regi et al., 2022). These sorts of attacks put the cloud confidentiality, integrity, and availability at danger, and they can seriously harm an organization's finances, operations, and reputation. The existing format of traditional security measures like identity, authentication, and authorization is no more sufficient for cloud environments. Cloud service providers today need to protect data stored in the cloud in a similar manner to banks. To safeguard the most valuable financial assets, banks employ a variety of security measures, such as surveillance cameras, armed guards, panic buttons, and inner sanctuaries or vaults (Knapp et al., 2011). Nevertheless, while numerous governmental and commercial entities are shifting towards cloud computing and virtualized environments, some have not yet adopted these technologies due to concerns surrounding security (Charif and Awad, 2014). Current research has also revealed that safeguarding the physical infrastructure of data centres, such as power distribution and cooling systems, is just as crucial as protecting the servers and networks they support (Islam et al., 2018).

The rapid evolution of IT infrastructures, such as cloud computing and virtualization, has presented a significant challenge to conventional cybersecurity measures. In recent times, cyber-attacks have grown increasingly sophisticated, characterized by their high level of targeting and long-term nature. These prolonged attacks, often attributed to state-sponsored efforts, are commonly referred to as Advanced Persistent Threats (APTs) (Khaleefa and Abdulah, 2022). APTs are not singularly sophisticated attacks as initially perceived; rather, they are complex combinations of well-known techniques designed to achieve specific, highly valuable objectives. At present, no individual technology can offer complete protection against APT attacks, and the detection of an attack often occurs when it is already too late to prevent significant damage.

1.2 Advanced Persistent Threats

Over the years, security challenges have evolved from single-node attacks to distributed attacks, significantly impacting various sectors. These detrimental attacks not only disrupt the availability of machines but also jeopardize the confidentiality of data, financial systems, aerospace industry, defence infrastructure, educational technology, and more. In recent times, information security breaches have posed severe risks to individuals, with each successful attack estimated to cost organizations approximately 7.2 million dollars per incident (Diego et al., 2018). Advanced persistent threats have been identified since the early 2000s, with notable instances dating back to 2003. During that time, China-based hackers orchestrated the Titan Rain campaign, aiming to pilfer confidential state secrets from U.S. government entities. The targets of these attacks encompassed military information and involved APT assaults directed at the sophisticated systems of prominent government agencies, including NASA and the FBI. Security analysts attributed the origins of these attacks to the Chinese People's Liberation Army.

According to the explanation provided by the National Institute for Science and Technology, an Advanced Persistent Threat denotes an adversary with abundant resources and extensive proficiency, providing them a notable edge in effectively carrying out successful exploits (NIST, 2017). The adversary employs various attack techniques with the objective of infiltrating the target organization and establishing a foothold. The primary goal of these attacks is to steal and extract sensitive information, paving the way for future incursions and detrimentally impacting the organization's operations or objectives. APTs persistently make repeated attempts over an extended period, emulating the target's defences to remain inconspicuous and effectively accomplish their mission (Wang et al., 2016).

Advanced Persistent Threats pose a significant and escalating security risk to both businesses and government organizations. According to the 2014 State of Endpoint Risk report, APTs ranked as the third most dangerous security threat out of 676 surveyed organizations. The report also highlights that the use of mobile platforms and cloud computing ranked as the top two security risks. Although not proven, it is widely speculated that APTs are often sponsored by nations due to their high level of sophistication, and their initial targets were predominantly military and government agencies. However, the landscape has evolved, and APTs now target a wide range of businesses and government agencies. It is important to note that the primary objective of APTs frequently revolves around the theft of valuable intellectual property. According to Khan & Khan (2019), the main goal of APT attackers revolves around securing economic, political, and strategic benefits through the unauthorized acquisition of information from vital infrastructure and resources. These attackers specifically target certain organizations. Additionally, Rouse (2020) highlights that APTs focus on sectors such as national defence, manufacturing, and the financial industry, where valuable information like intellectual property, military plans, and government data is present.

APTs represent a rapidly expanding threat in the field of information security, posing significant challenges for organizations. These attacks are orchestrated by highly skilled and well-resourced attackers, with a primary focus on extracting sensitive information from private entities. The main objective of APTs is to exfiltrate data to external hosts, involving activities such as data theft and data exfiltration (Singh et al., 2019). Notable instances of APT incidents include the breach of Adobe in 2013, where approximately 9 GB of encrypted password data was stolen, and the Ashley Madison breach in 2015, resulting in the theft of around 40 GB of their database. In contrast to other forms of exploits, Advanced Persistent Threats (APTs) are strategic, continuous, and concealed assaults that are specifically aimed at organizations, rather than random individuals or typical system users. These exceptionally sophisticated attacks are not motivated by immediate benefits; instead, their objective is to secretly infiltrate the targeted organization over a prolonged duration, enabling them to extract sensitive and vital information necessary for accomplishing their goals. APTs showcase adaptability by employing a combination of hardware devices and software tools to elude defensive countermeasures. Employing a methodical approach, APTs frequently rely on social engineering as their primary method for illicitly entering the targeted organization. Although APT attacks commonly make use of Zero-day vulnerabilities referring to undisclosed software vulnerabilities a recent study by Li et al. (2016) discloses that 19% of reported APT cases relied on Zero-day vulnerabilities, 70% exploited existing and well-known vulnerabilities, and 11% utilized vulnerabilities that were not yet recognized.

1.2.1 APT Life Cycle

The life cycle of Advanced Persistent Threats typically comprises six phases, which include spear phishing attacks, reconnaissance, establishing presence, exploration, data extraction, and maintaining persistence. Advanced Persistent Threats (APTs) represent intricate and multi-phase cyber assaults. To effectively penetrate a system, these attacks adhere to a multifaceted procedure encompassing victim targeting, information gathering, approach implementation, vulnerability exploitation, ongoing activity, and the extraction and transfer of data (Hejase et al., 2020). It is widely acknowledged that sophisticated attackers, regardless of their motives, funding, or control, often operate within a defined cycle when targeting their objectives. Figure 1 illustrates the evolution of APTs and highlights the APT Life Cycle (Virvilis et al., 2013).

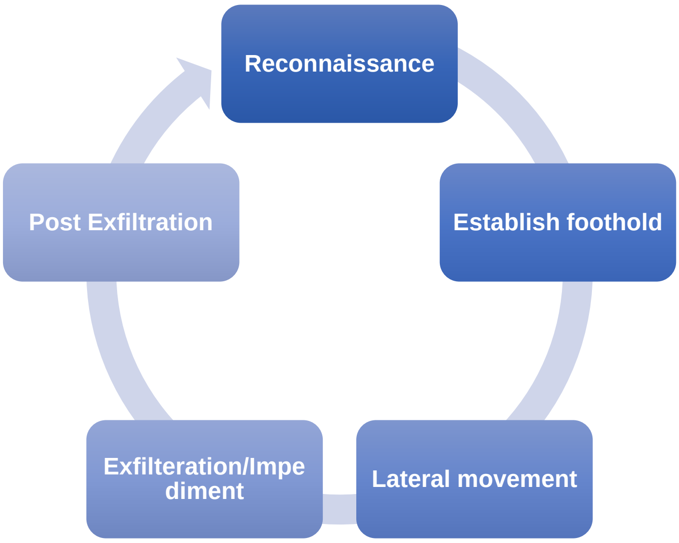


Figure 1 APT Life Cycle

This research will investigate the influence of emerging threats on cloud security by analysing the evolving threat landscape and its consequences. The study aims to identify the various ways APTs impact cloud security and determine suitable strategies for their detection and mitigation. The research will involve a comprehensive review of previous techniques employed for detection, and mitigation, while also exploring effective methods to address these challenges specifically within cloud platforms.

1.3 Problem Statement

The risk of cyber-attacks rises along with the continued reliance on cloud computing. The security, confidentiality, and availability of data in the cloud are seriously threatened by emerging threats and cyberattacks, which can lead to data breaches, service interruptions, and other major repercussions. Large organizations and government agencies have suffered significant data losses due to the inadequacy of traditional mitigation techniques in protecting against Advanced Persistent Threat. Existing methods have proven ineffective in detecting and preventing APT activities across user, application, network, and physical domains. Researchers attribute the success of these attacks to human vulnerability, highlighting the presence of vulnerabilities even when technical mitigation measures are in place, thereby posing continuous threats.

Recent studies emphasize the challenges associated with detecting APTs and underscore the severity of the issue through notable attacks and data breaches affecting esteemed organizations such as RSA security, NASA, FBI, Sony, Citigroup, and Fox Broadcasting, among others (Nicho and Khan, 2014). Despite having traditional security measures in place, these organizations were unable to prevent or detect the attacks. Researchers have extensively investigated this problem, revealing the shortcomings of conventional prevention and detection techniques in effectively countering targeted attacks. Therefore, it is essential to consider how these threats affect cloud security and pinpoint efficient countermeasures.

1.4 Research Aims and Objectives

1.4.1 Aim

This research aims to identify and evaluate the impact of APT in cloud environments and proffer efficient mitigation strategies.

1.4.2 Objectives

The specific objectives of this study are listed below:

I. Investigate the impact of Advanced Persistent Threats on cloud security.

II. Analyse the strengths and weaknesses of the current approaches for addressing APT in cloud environments.

III. Design an operation to emulate an APT adversary plan.

IV. Simulate APT attacks using Mitre Caldera and assess detection capabilities using Snort.

V. Utilise Nessus Vulnerability scanning tool to identify potential vulnerabilities that can be exploited by APT.

VI. Provide recommendations for improving security in cloud environments based on research findings.

1.5 Research Questions

This research will be addressing some questions that are critical in understanding the impact of APTs on cloud environments.

I. What are advanced persistent threats and how do they exploit cloud environments?
II. What are the strengths and weaknesses of current methods for mitigating APTs?
III. What is the impact and consequences of a successful APT attack.
IV. What are the vulnerabilities and potential attack vectors in cloud infrastructures that make them susceptible to APT attacks?
V. What techniques can be incorporated to effectively improve the cloud security posture against APT attacks.

1.6 Significance of The Study

The fundamental relevance and rationale for this study are its capacity to address the urgent need for understanding the rapidly evolving environment of emerging threats in cloud security. This research will allow for a comprehensive assessment of the risks posed by APT. As technology advances, new vulnerabilities and attack vectors emerge, making it essential to stay ahead of potential security breaches. By examining the impact of APT on cloud security, we can provide insights into the nature, scope, and severity of these threats, enabling organizations to develop targeted strategies and measures to mitigate them effectively. In addition, this research plays a crucial role in developing effective countermeasures and improving overall security posture.

By studying the impact of APT on the cloud environment, we can identify patterns, trends, and attack techniques used by adversaries. This knowledge is instrumental in designing and implementing advanced security solutions, such as intrusion detection systems, threat intelligence platforms, and incident response strategies, specifically tailored to mitigate the identified threats. The dissemination of research outcomes also fosters collaboration and knowledge sharing within the cloud computing community, enabling organizations to collectively enhance their security practices and effectively respond to emerging threats.

1.7 Scope and Limitation of the Study

The scope of this research involves investigating the impact of a successful APT attack on a cloud environment, this will be achieved using Mitre Caldera and Nessus. The research will focus on understanding the strengths and weaknesses of existing approaches, conducting APT attack simulations, assess detection using snort IDS, and utilizing vulnerability scanning to assess the security posture of the cloud infrastructure. This includes investigating the consequences of security breaches, evaluating existing security measures, and proposing efficient mitigation strategies.

In terms of limitations, the findings presented in this study should be interpreted within the specific context of the cloud environments, methodologies, and tools employed. It is important to acknowledge that due to time constraints, this research may not have thoroughly examined all dimensions of Advanced Persistent Threats and their implications for cloud security. Furthermore, while the simulation will be conducted using tools such as Caldera, Snort and Nessus, it is crucial to recognize that these simulations may not fully capture all the intricacies of real-world APT attacks.

1.8 Thesis Organisation

This thesis is categorised into 6 chapters:

- Chapter 2 delves into an extensive literature review on APT in cloud security. It encompasses an analysis of existing literature on the theories surrounding APT in cloud environments, their impact, and the current mitigation strategies employed in this domain. The literature review is organized thematically, effectively presenting the research according to different types of threats and corresponding strategies.
- Chapter 3 focuses on the methodology employed in this study. It includes a detailed description of the approach used to examine the characteristics and impacts of APT, reviewing the tools and techniques for simulated APT attacks and vulnerability scanning. The chapter provides insights into the methodologies employed to review and analyse these threats.

- Chapter 4 entails the implementation stage, conducting the experiment, implementing an operation, and implementing a detection mechanism.
- Chapter 5 focuses on results from the simulation and experiment conducted. The chapter presents a comprehensive review of the findings obtained through this analysis, giving detailed discussion from all aspects of the implementation.
- Chapter 6 Conclusion, recommendation and future work will show the main contribution to knowledge and how significant this contribution is to the field of cyber security and conclude the findings from this study stating how the main project objectives were met.

2.0 LITERATURE REVIEW

This section delves into an extensive review of literature on emerging threats in cloud security with a focus on Advanced persistent threats. It encompasses an analysis of existing literature on the theories surrounding APT in the cloud, their impact, and the current mitigation strategies employed in this domain. The literature review is organized thematically, effectively presenting the research to discuss cloud security threats in general and outlining the existing literature on APTs and their current mitigation strategies. Researchers have recently investigated the different ways in which emerging threats can affect the security of cloud computing. According to Tatam et al. (2021), various factors can contribute to the emergence of these threats, including limited budgetary resources, inadequate staffing and training for security-related tasks, low user awareness, insufficient compliance monitoring, inadequate security policies and procedures, and deliberate cyber-attacks.

2.1 Literature Review References

The sources referenced in this literature review are condensed and outlined in Table 1. The methodology employed encompasses a mixed-method approach, combining both quantitative and qualitative techniques.

Table 1 Table of Reference

Reference	Relevance	Methodology	Strengths	Contribution	Limitations
Kadiric, F., 2022	5	Experimental	Provides an innovative approach to generating labelled APT datasets, offering fine-grain attack labels.	Proposes the use of Caldera, Sysmon, and the labelling tool to create labelled APT datasets	Raw logs are manually extracted and processed, which might introduce human error.
Salim, D.T., Singh, M.M. and Keikhosrokiani, P., 2023	4	Literature review	Analyses APT attack detection methods and assessment metrics for network systems.	Provides an efficient model that identifies and forecasts mobile network APTs for cyber situational awareness	Focuses only on network-based APT detection, neglecting broader attack vectors.
Ghafir, I., 2017	4	Experimental	The research adopts a multi-phase approach, encompassing threat detection, alert correlation, and attack prediction	Introducing a significant machine-learning attack prediction module to assesses early alerts for APT escalation	Machine learning models may struggle to predict APT attacks across diverse scenarios.

Chen, J., Su, C., Yeh, K.H. and Yung, M., 2018	3	Literature review	Discusses the concept of APT and how to detect the threats.	Explored new tools, concepts and techniques concerning APT detection	The context and environment for applying the discussed APT detection techniques are unspecified, impacting their effectiveness across diverse scenarios.
Adelaiye, O.I., Showole, A. and Faki, S.A., 2018	3	Literature review	Research employs method-based analysis, studying 25 papers to assess 12 mitigation techniques.	The research is centred on evaluating and comparing mitigation techniques for APT	Relies only on existing literature
Karabacak, B. and Whittaker, T., 2022	4	Qualitative	Introduces zero trust architecture in mitigation of APT attacks	Utilises the MITRE's ATT&CK framework to extract how the APT29 threat group techniques could be mitigated to prevent initial access to federal networks	Focuses only on prevention of initial access and neglects detection of APT if prevention fails.
Kinnunen, J., 2022.	3	Qualitative Design science research	Detecting adversary behaviour using different solutions	Introduces gap analysis in detecting APT to measure current defensive solutions coverage against adversary capabilities.	The evaluation of research results using a questionnaire within the organization introduces potential bias

Li, Y., Zhang, T., Li, X. and Li, T., 2019	4	Experimental	The use of a red-blue confrontation game model for APT defence	Defence game model rooted in the theory of red-blue confrontation	Lacks empirical evidence and case studies
Messaoud, B.I., Guennoun, K., Wahbi, M. and Sadik, M., 2016	3	Quantitative	Comprehensive adaptation to evolving cyber-threats through an attacker-centric APT life cycle model, evaluating camouflage tactics and emerging protection technologies.	Introduces a lifecycle model based on attacker's objectives rather than tactics	It does not provide insights on the limitations of the techniques
Xiao, L., Xu, D., Xie, C., Mandayam, N.B., and Poor, H.V., 2017	3	Experimental	Uses prospect theory to model interactions between cloud defender and APT attacker,	The study enhances APT defence understanding by integrating prospect theory, highlighting its impact on defender-attacker interactions	The research assumes a subjective attacker perspective, potentially oversimplifying actual APT behaviours.
Vance, A., 2014	3	Quantitative	Focuses on the vulnerability of cloud computing to APTs using flow-based monitoring.	The research introduces an innovative approach that applies flow-based monitoring with statistical anomaly detection	The study acknowledges that some APT activities may leverage zero-day exploits, and C2 IP addresses can change

Bere, M., Bhunu-Shava, F., Gamundani, A. and Nhamu, I., 2015	3	Literature review	Highlights a critical aspect of APT attacks – the human factor	The paper recognizes the complexity of human behaviour in the context of APTs and advocates for addressing it from a behavioural perspective.	The research appears to heavily rely on existing literature
Gjerstad, J. L., 2022	4	Experimental	leverages industry-standard frameworks (MITRE ATT&CK and CALDERA) for simulating APT attacks and generating datasets	It demonstrates the successful use of MITRE ATT&CK and CALDERA for simulating APT attacks	Focuses on a specific APT group's behaviour in CALDERA simulations
Moon, D., Im, H., Lee, J.D., and Park, J.H., 2014	3	Case study	The proposed Multi-Layer Defence System (MLDS) offers a practical approach to defending against APT	The research primarily focuses on proposing and explaining the Multi-Layer Defence System (MLDS) as a defence mechanism against APT attacks.	The case studies provide a basic overview of how MLDS might work in certain scenarios, but they do not account for the complexity of real-world APT attacks

Cole, 2013	4	Literature review	The research provides a critical analysis of the prevalent approach of prioritizing prevention over detection in cybersecurity	It highlights the limitations of relying solely on traditional prevention technologies and to propose enhancements for these technologies to bolster detection capabilities	The research relies on existing breach statistics and expert opinions, which might not fully capture the diversity of organizational contexts and security challenges.
Quadri and Khan, 2019	3	Qualitative	Proposes a collective cyber-defence front with regional allies for a stronger front.	Provides contextual awareness of a visionary framework for regional collaboration	Does not discuss partnership with global partners

2.2 Security Issues in the Context of Cloud Computing

The security of cloud computing is a crucial concern that significantly impacts the adoption of this technology (Ennajjar et al., 2014). In 2010, there was a notable incident where Amazon's network host service, S3 (Simple Storage Service), experienced a four-hour breakdown. There was a technical failure that affected its availability and caused disruptions for its users. This event served as a wake-up call for users and organizations about the potential risks associated with storing user data in the cloud (Zhang et al., 2012). Similar research conducted by Hussain et al. (2020) discusses the security vulnerabilities, threats, and attacks associated with centralized storage systems in a cloud environment. The authors propose a framework to address these vulnerabilities and threats, which is a layered model that includes security and management at various tiers.

In recent years, cloud security breaches have garnered significant attention due to their far-reaching implications and potential for widespread data exposure. Several notable cases underscore the evolving landscape of cloud security challenges:

Cloud Misconfiguration

Cloud misconfiguration is a prevalent security concern that can occur due to the rapid pace of cloud migration and improper selection of cloud configurations. Even major Infrastructure-as-a-Service (IaaS) providers like Microsoft are not immune to this risk. In 2021, Microsoft experienced a significant misconfiguration issue in its cloud storage service, Microsoft Azure, resulting in the exposure of sensitive internal data and records of numerous companies, including intellectual properties (IP) and personally identifiable information (PII). This misconfiguration incident impacted not only Microsoft but also various industries, including healthcare, aviation, and logistics. It serves as a reminder that proper attention and precautions are necessary to prevent misconfigurations and their potential consequences. Tech giant Amazon was also not spared when it inadvertently left a Prime Video database called "Sauron" exposed and unprotected. This incident resulted in the exposure of approximately 215 million records containing Prime Video viewing habits. The database, which was stored on an internal server within Amazon's infrastructure, consisted of numerous pseudonymized records. These records contained information about the shows or movies streamed, the devices used for streaming, network quality, subscription details, and the customer's Prime status (ImmuniWeb, 2023).

Vulnerable API

Application Programming Interfaces or API serve as the bridge between applications, facilitating their interaction, communication, and data transmission. While APIs are designed to provide third-party partners access to software platforms, their vulnerabilities, especially weak authentication measures, can become entry points for cyber attackers seeking unauthorized access to sensitive corporate data (Suryateja, 2018). One common exploit involves hackers leveraging vulnerable APIs to scrape user data. A notable incident occurred in 2021 when malicious actors exploited LinkedIn's API, gaining illicit entry to publicly available user account information. Subsequently, they compiled and offered hundreds of millions of authentic user details for sale on an underground platform. As a result, LinkedIn users became susceptible to phishing scams and identity theft due to the exposure of their personal information.

2.3 Understanding the Impact of Advanced Persistent Threats

Advanced Persistent Threats represent a category of sophisticated cyberattacks intended to execute intelligent and highly impactful assaults with the goal of evading detection by leveraging extensive reconnaissance activities (Halabi et al., 2022). The National Institute of Standards and Technology provides a definition for Advanced Persistent Threats (APTs), stating that they refer to adversaries who possess advanced levels of expertise and substantial resources. These capabilities enable them to exploit various attack vectors, such as cyber, physical, and deception techniques, to create favourable circumstances for achieving their objectives.

Unlike script kiddies or insider threats, APTs demonstrate resourcefulness and strategic planning rather than relying on opportunistic actions (Singh et al., 2019). APTs are driven by objectives such as cyber espionage, sabotage, and subversion, achieved through a careful and continuous presence within the target system. This deliberate approach allows APT attacks to remain undetected by design, enabling attackers to covertly steal information over an extended duration. APT attacks exhibit a persistent nature by continuously pursuing their objectives over an extended duration. They possess the ability to adapt to defensive measures employed by those trying to thwart them while displaying unwavering determination to sustain the required level of engagement to accomplish their goals. In the realm of cybersecurity, vulnerabilities are unavoidable. Sophisticated state-sponsored cyber actors, known as APT groups, employ intricate techniques to target and compromise various networks and systems (Karabacak and Tatar, 2014). Indeed, the success of APT attacks is seemingly inevitable, leading to a substantial focus on research and literature related to APT detection.

Quadri and Khan (2019) describe APTs as sophisticated, professional, and state-supported cyber-attack programs that are systematically executed over an extended period. These attacks involve a group of skilled hackers who coordinate their efforts with a specific motive, targeting high-profile companies and governments. The attackers aim to achieve privilege escalation and expand their foothold within the targeted networks. They employ tactics such as sending malware-laden emails or using USB drives infected with malware. Once inside the critical systems, they remain hidden while gathering intellectual property and other valuable assets for purposes of sabotage or corporate espionage.

2.3.1 Symptoms of APTs

APTs represent a distinct type of hackers who pose an ongoing and danger to companies and networks worldwide. These hackers often operate as a highly organized team, aiming to illicitly obtain valuable intellectual property like confidential project details, contracts, and patent information. While APT hackers may employ common tactics such as phishing emails or deceptive methods to trick users into downloading malware, their objectives are typically much more ambitious. If a security breach primarily targets financial theft, it is unlikely to be an APT hack (Kandukuri et al., 2018). APT hackers seek to infiltrate organisations. Detecting APT hacks involves recognizing distinct indicators since these hackers employ different techniques compared to typical hackers. Despite their inherent difficulty to detect, advanced persistent threats (APTs) often exhibit specific warning signs. When an organization becomes a target of an APT, there are certain symptoms that it may observe, as outlined by Rouse (2020):

- Unusual activity on user accounts: Organizations may observe abnormal behaviour associated with user accounts. This can include unauthorized access attempts, changes in user privileges, or unusual file downloads. These signs suggest that APT actors may have compromised user credentials to gain access to the organization's systems.

- Use of backdoor Trojan horse malware: APTs often utilize backdoor Trojan horse malware to maintain persistent access to the targeted systems. Detecting extensive usage of such malware can be an indication of an APT attack. Additionally, organizations should be vigilant for uncharacteristic database activity, such as a sudden surge in database operations involving large volumes of data. These anomalies may signify APT actors attempting to manipulate or exfiltrate data.
- Presence of unusual data files: The existence of unfamiliar data files within the organization's systems can be a red flag for APT activity. These files may have been created and bundled specifically to aid in the exfiltration of sensitive data.
- Detecting unusual patterns or anomalies in outbound data is considered one of the most effective methods for cybersecurity professionals to ascertain whether a network has been subjected to an APT attack.

2.3.2 Notable Examples of APT Attacks and their Impact

The cloud security landscape has been significantly influenced by several noteworthy instances of APT attacks. Some notable examples of APT attacks are listed below:

Deep Panda

In 2015, a notable cyber-attack targeted the Office of Personnel Management (OPM) of the United States Government. This attack, which is believed to be part of an ongoing cyber conflict between China and the U.S., garnered attention under various codenames. One of the frequently used codenames associated with these attacks is Deep Panda. The incident that took place in May 2015 resulted in the compromise of more than 4 million personnel records of U.S. individuals. Concerns were also raised regarding the potential theft of information related to secret service personnel (Adelaiye et al., 2018).

More recently in 2022, Deep Pander launched new attacks that exploited the Log4Shell to deploy the new Fire Chili rootkit. This rootkit is designed to keep activities under the radar and is deployed alongside the Milestone backdoor (Osborne, 2022). Deep Panda's primary objective is to infiltrate networks and acquire sensitive information from both state and private organizations. This well-organized group possesses the ability to remain undetected on networks for extended periods, even when their presence is known to security teams. It can take several months to completely remove Deep Panda from a network. Deep Panda employs multiple malware components in their attacks. These tools facilitate device and network connectivity, code writing for infecting connected systems, and the removal of log data to conceal their online presence from system monitors. One of its strengths lies in its proficiency at establishing numerous "backdoors" within a compromised system (Adelaiye et al., 2018). These backdoors ensure continuous access, even when security teams change passwords. Due to Deep Panda's strategic creation of backdoors, eliminating their presence from a network typically requires several months of effort as they continuously outsmart removal attempts.

Stuxnet

The Stuxnet malware was specifically created to target essential industrial infrastructure. By leveraging various undisclosed vulnerabilities and employing advanced attack techniques, it successfully executed malicious code through multiple infection routes, all while evading detection for an extended period. This highly autonomous malware serves as a notable illustration of a "fire and forget" type of malicious software (Kumar et al., 2022). Stuxnet was responsible for damaging numerous centrifuges at Iran's Natanz uranium enrichment facility, leading them to burn out. Subsequently, various groups adapted the virus to target other facilities like water treatment plants, power plants, and gas lines.

Stuxnet consists of three essential components: a worm, a link file, and a rootkit, each with its specific purpose. The worm's role is to enter a computer system and execute the necessary procedures to deliver the primary payload. The link file, once in place, triggers the payload, initiating the attack and automatically infecting the system. The rootkit conceals the activities of both the worm and the link file, making them undetectable. What distinguished Stuxnet at the time was its utilization of a zero-day exploit, which enabled it to operate without any user actions or safeguards in place. This exploit allowed Stuxnet to successfully infiltrate systems while making its origin untraceable. By combining these three components, Stuxnet managed to bypass established security measures, infect computers, and inflict damage on facilities (Bakic et al., 2021). Stuxnet gained notoriety as the first cyberweapon and the initial computer worm capable of disrupting computers responsible for critical infrastructure, leading to physical harm. The attack had significant consequences, causing widespread repercussions in the cybersecurity field.

SolarWinds Hack

In 2020, a significant cybersecurity incident known as the SolarWinds attack unfolded, involving the infiltration of multiple US organizations and government agencies, resulting in a string of data breaches. It is suspected that the hacking incident was coordinated by the hacker collective Nobelium, which is also recognized as APT29 or cozy bear. There are allegations that the Russian government may have been involved in aiding for this attack (Durojaye and Raji, 2022). The primary target of the attack was the SolarWinds Orion System, a product developed by SolarWinds specifically designed to provide IT performance monitoring services to its clients. Taking advantage of the privileged access linked to the Orion platform, the cyber assault facilitated unauthorized intrusion into SolarWinds' diverse array of customer IT systems, networks, and data. It is estimated that more than 30,000 private and public organizations, relying on the Orion platform for their IT resource management, were impacted by this incident (Oladimeji and Kerner, 2022). Through this unauthorized access, the hacker group leveraged the Orion platform as a backdoor to access and impersonate users and accounts, disguising their activity as legitimate SolarWinds operations to evade detection by intrusion detection and prevention systems and antivirus software deployed within various organizations (Alert, 2020).

The consequences of the SolarWinds attack were twofold, encompassing both espionage and intellectual property theft. Government departments, including the Department of Homeland Security, were among the primary victims, with evidence indicating that some of their emails were exfiltrated from compromised systems. Additionally, the attack involved intellectual property theft, as evidenced by the discovery that FireEye, a cybersecurity company credited with identifying the vulnerability, had one of its tools missing, leading to an audit that revealed the existence of the backdoor in the platform used to access their systems. The attackers operated covertly for an extensive duration, gaining access to the system in September 2019 and remaining undetected until December 2020, highlighting the high level of sophistication and persistence employed by state and state-sponsored actors throughout the attack lifecycle (Baker, 2021). Table 2 provides a summary of ten APT attacks, including details about their purpose, year, and impact (Kumar et al., 2022).

Table 2 Major APT Attacks and their Impact

APT	Purpose	Initial Attack Method	Impact	Year
Wannacry	Financial	Exploiting Windows EternalBlue vulnerability	Losses of up to $4 billion	2017
Equifax Hack	Espionage	Vulnerability in Apache Struts web application framework	143 million users exposed in a data leak	2017
Cloud Atlas	Espionage	Spear phishing emails with malware.	Sensitive information Data leak targeting workers in the financial, telecoms and energy sectors.	2014
Carbanak	Financial	Spear phishing emails with malicious attachments and links	$1 billion stolen	2013
Adwind	Espionage	Socially engineered emails with malicious attachments (Adwind RAT)	Data leak	2012
Shamoon	Denial of service	Spear phishing emails with malicious attachments	Over 30,000 oil company systems experienced data loss.	2012
Operation Aurora	Espionage	Spear phishing with malicious attachments.	Data leak targeted Google and other companies	2009
GhostNet	Espionage	Spear phishing emails with a malicious attachment	Thousands of computers breached globally, including embassies and foreign ministries	2009
Gozi	Espionage and financial	Vulnerabilities in web browsers or plugins (malicious websites)	Infected about 1 million computers	2007
Flame	Espionage	Spear phishing emails with malicious attachments	Middle East data leak impacts 282 institutions.	2007

The data clearly demonstrates that most initial penetration occur through deceiving individuals into opening files with malicious extensions or enticing them to visit compromised websites. In accordance with this, Hejase et al., (2020) contend that the success of the reconnaissance and delivery stages in APTs can largely be attributed to their ability to manipulate human behaviour.

2.4 Existing Detection Strategies of APT Attacks

Considering the detrimental impact of APT on cloud platforms, experts like Karantzas and Patsakis (2021) argue that while prevention is desirable, detection is indispensable in combatting APT. He stresses the significance of striking a balance between prevention and detection, as companies often overlook detection measures in favour of emphasizing prevention strategies. Acknowledging this reality is essential to strengthen overall cybersecurity defences against APT threats. Disturbing breach statistics reveal that organizations have unknowingly suffered the theft of millions of records, sometimes remaining undetected for months or even years (Cole, 2013). Cole stresses the importance of supplementing traditional prevention technologies with additional measures. For IPS augmentation, the focus is on minimizing false positives and fine-tuning detection to identify APT indicators. Augmenting DLP involves integrating it with a Digital Rights Management solution. However, Cole concludes that relying solely on these foundational technologies will not be sufficient to effectively combat APT.

The presence of encryption and the utilization of cloud-based communication networks pose significant challenges to detection. Advanced Persistent Threats (APTs) employ encrypted malicious code, and once the targeted system executes the malware, the infected machines establish encrypted channels to communicate with Command and Control (C2) systems. The multiple layers of encryption involved in these processes make it difficult to detect such activities at the network level (Rouse, 2020). Traditional security mechanisms like signature string matching prove ineffective in these scenarios, allowing attackers to successfully hide their actions from network-based detection. Furthermore, the intentionally distributed nature of cloud-based communication architectures prevents effective coordination of intrusion detection sensors, further complicating the detection process (Vance, 2014).

In a study by Liu (2014), a network security architecture is proposed for APT detection and prevention. The author primarily focuses on the detection aspect and suggests a centralized analysis and control module. Research conducted by Adelaiye et al. (2019)

highlights 12 mitigation techniques conducted by 25 researchers. The authors highlight that promising methods for mitigating Advanced Persistent Threats (APTs) include traffic/data analysis, pattern recognition, and anomaly detection. These methods primarily focus on detective controls. Among the 12 techniques emphasized, there are also preventive methods such as whitelists, blacklists, intrusion detection systems (IDS), awareness programs, deception techniques, risk assessment, and multi-layer security.

2.5 Prevention and Mitigation Techniques in APT Attacks

There have been several techniques proposed by different researchers to prevent APT attacks in the past. Moon et al. (2014) proposed a multi-layer defence system for preventing and detecting Advanced Persistent Threats (APTs). Their system involves collecting and analysing log information from endpoints, utilizing eight components. They provide two cases, namely infection through USB and spear phishing, to exemplify the system's preventive measures. While the proposed defence system may effectively prevent specific cyberattacks, its applicability to all scenarios is limited. Mohamed et al. (2018) published a similar study emphasizing two important social aspects of APT prevention: security awareness and information security policies. They suggest enhancing the MITRE ATT&CK Mitigations by implementing automatic termination of connections between victims and attackers in response to specific incidents caused by malware infections. However, their proposed solution is not comprehensive or mature enough to mitigate a wide range of evolving APT tactics and techniques.

Messaoud et al. (2016) present a list of technologies, including sandboxing, honeypots, SIEM (Security Information and Event Management), and user behaviour analytics, for protecting against APT actors. They map these technologies to different attack phases in the APT lifecycle using a matrix. According to their matrix, all these technologies are effective in preventing APT attacks. However, they do not provide insights into the potential limitations of these four technologies in preventing APT attacks.

Xiao et al. (2017) conducted a research study that presents a theoretical analysis of APT defence. The study investigates the influence of an APT attacker's subjective perspective on the security levels of data stored in a cloud environment. The research paper introduces an asymmetric evolutionary game model, which explores the dynamics between the APT attacker and the defender of cloud storage. The objective is to identify the evolutionary stable strategies within the APT defence games. Similarly, Yue Li et al. (2019) presented a technical framework to address the challenge of identifying unknown threats concealed within Advanced Persistent Threat (APT) attacks. Their approach is based on the collaboration theory of "cloud, transport layer, endpoint, and human response," drawing from practical experience. Meanwhile, M. Min et al. (2018) have focused on cloud storage systems and put forth a CPU allocation scheme that utilizes a "hot start" strategy to optimize performance and overcome obstacles effectively.

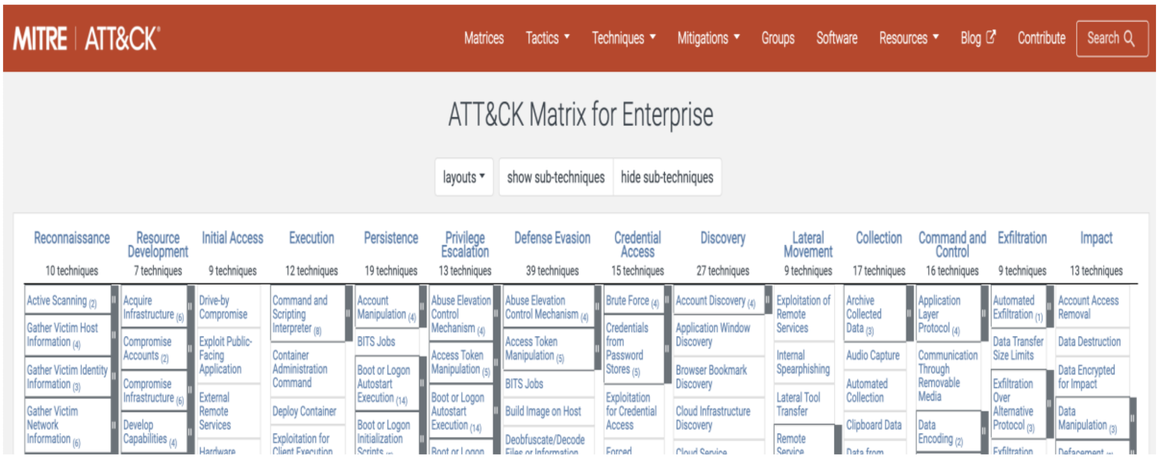
Besides the solutions and suggestions put forth by the academic community, security vendors consistently enhance their product offerings to mitigate APT attacks directly or indirectly. These include widely used products such as firewalls, antivirus software, intrusion prevention systems (IPS), web application firewalls, web, and email protection tools, as well as sandboxing technologies (Hudson, 2014).

2.6 MITRE ATT&CK Framework and Caldera

The MITRE ATT&CK framework is a publicly available threat intelligence database that categorizes cyber actors' techniques into 14 tactics based on real-world observations (MITRE, 2021). It includes customized matrices for enterprise, mobile, and industrial control systems. The framework consists of 188 techniques and 379 sub-techniques grouped under the tactics. The ATT&CK Navigator provides specific techniques used by threat groups. Additionally, the ATT&CK website shares information on threat groups and associated tools. The latest version (v10) covers 129 threat groups and 637 software used in cyber-attacks. MITRE also developed the PRE-ATT&CK matrix, which focuses on reconnaissance, weaponization, and delivery stages of the kill chain. It complements the ATT&CK Enterprise Framework by facilitating analysis throughout the attack lifecycle. ATT&CK methodology helps analysts detect attacks by studying cyber artefacts and provides behavioural observables (Karabacak and Whittaker, 2022).

The ATT&CK framework provides a comprehensive understanding of how adversaries infiltrate organizations, traverse networks, escalate privileges, and circumvent defensive measures. It serves as a valuable resource for identifying the specific methods employed by adversaries in carrying out malicious activities against targeted organizations. By categorizing adversary behaviours into Tactics, Techniques, and Sub techniques, the ATT&CK framework offers insights into the strategies employed by attackers. Importantly, this framework can be utilized from both offensive and defensive perspectives, aiding organizations in enhancing their security posture. In his research, Hallberg showcased a proof-of-concept implementation of how the MITRE ATT&CK framework can be effectively utilized for intrusion detection and visualization (Hallberg, 2020). This demonstrates the practical application of the framework in real-world scenarios. Given its relevance and alignment with previous research, the MITRE ATT&CK framework is well-suited for supporting the artefacts created in this thesis.

In relation to this thesis, Caldera incorporates a crucial element by utilizing ATT&CK TTPs to direct atomic activities. Caldera is a platform developed by MITRE that leverages the ATT&CK framework for simulating and analysing cyber threat scenarios. This implies that Caldera encompasses tactics and techniques aligned with ATT&CK framework (Applebaum et al., 2016). The framework also offers flexibility for customization, allowing the addition of new features and enabling various plugins to extend its functionality. For instance, it can simulate human behaviour, incorporate encrypted traffic using HTTPS, and execute adversary emulation (EMU) plans. Notably, the EMU plans concentrate on specific APT groups as addressed in ATT&CK. This experiment will emulate the APT 29 tactics, techniques, and procedures. Figure 2 displays an abridged version of the ATT&CK Matrix, including all 14 tactics and several techniques (Mitre, 2021).



ATT&CK Matrix for Enterprise

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	7 techniques	9 techniques	12 techniques	19 techniques	13 techniques	39 techniques	15 techniques	27 techniques	9 techniques	17 techniques	16 techniques	9 techniques	13 techniques
Active Scanning (2)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Brute Force (4)	Account Discovery (4)	Exploitation of Remote Services	Archive Collected Data (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Credentials from Password Stores (5)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (14)	Boot or Logon Autostart Execution (14)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware	Exploitation for Client Execution	Boot or Logon Initialization Scripts	Boot or Logon	Build Image on Host	Forced	Cloud Infrastructure Discovery	Remote Service	Clipboard Data		Exfiltration	Data Manipulation (3)
						Deobfuscate/Decode Files or Information		Cloud Service		Data from			Defacement

Figure 2 Abridged version of MITRE's ATT&CK Matrix

2.7 Summary

APTs have the potential to inflict significant harm on cloud infrastructure long before they are detected, posing risks to both government and commercial organizations (Chen et al., 2018). The literature review in this section has revealed that while there is existing research on different emerging cloud security threats, only a limited number of studies focus on APT attacks on cloud environments. However, they do not specifically address the implications and effective detection of APT attacks on a cloud environment. As at the time of this report, and to the best of my knowledge, there is currently no documented literature that integrates Caldera, Snort and Nessus for the purpose of investigating the impact, identifying detections, and uncovering vulnerabilities exploited by APTs on cloud environments.

This study will address this gap by conducting a comprehensive analysis of the real-time impact of APT attacks on cloud security, an exploratory approach will be taken to detect APTs using open-source tools like Caldera, Snort and Nessus scanner on a cloud environment. The findings of this study will contribute empirical evidence and insights to expand the current understanding of APTs and guide future research in this area.

3.0 METHODOLOGY

The collective opinion among security experts, professionals, and researchers is that the primary objective of information security is to safeguard an enterprise's information, ensuring its availability, integrity, and confidentiality (Taherdoost, 2022). Nevertheless, businesses must be persuaded of their security measures as they consider migrating to the cloud. Hence, this study aims to ensure the security of cloud infrastructure and data by proposing an objective approach that utilizes open-source tools to identify the impact and detect these threats proactively, thereby mitigating potential damage. This chapter

3.1 Research Philosophy

The research questions in this study are approached from an epistemological standpoint that acknowledges knowledge as being constructed through interactions between the researcher and the research participants or components. It recognizes the importance of considering multiple perspectives to gain a comprehensive understanding of complex phenomena. The study adopts a pragmatic research approach that emphasizes the practical application of knowledge to real-world problems. The primary objective is to assess the impact of APT on cloud security. To achieve this, data is collected from reviewed literature and through experimental simulations. Statistical methods are then employed to analyse the collected data, allowing for a deeper understanding of the implications of APT attacks on cloud security. By combining theoretical insights from the literature review, data from simulated environments, and statistical analysis, the study aims to provide practical insights and recommendations for addressing APT in cloud environments.

3.2 Research Design

To gain a comprehensive understanding of this study, the research will adopt an exploratory approach, employing a combination of quantitative and qualitative research methods. This multifaceted approach aims to delve deeply into the subject matter and explore it from various angles, allowing for a thorough investigation. By employing both quantitative and qualitative methods, this research seeks to gather diverse perspectives and obtain a rich and nuanced understanding of the topic at hand.

The study employs a dual-research approach to gather data. The qualitative component of this research will involve reviewing literature on existing approaches for addressing APT in cloud environments, researching, and gathering information on specific tactics and techniques on the MITRE attack framework. The quantitative component will follow an experimental approach, implementing a cloud environment APT attack simulation, and vulnerability scanning to assess the detection and mitigation techniques. Thematic analysis will be used to analyse the data obtained to recognise common themes and patterns. The research methodology shown in figure 3 reveals the entire flowchart used in this research.

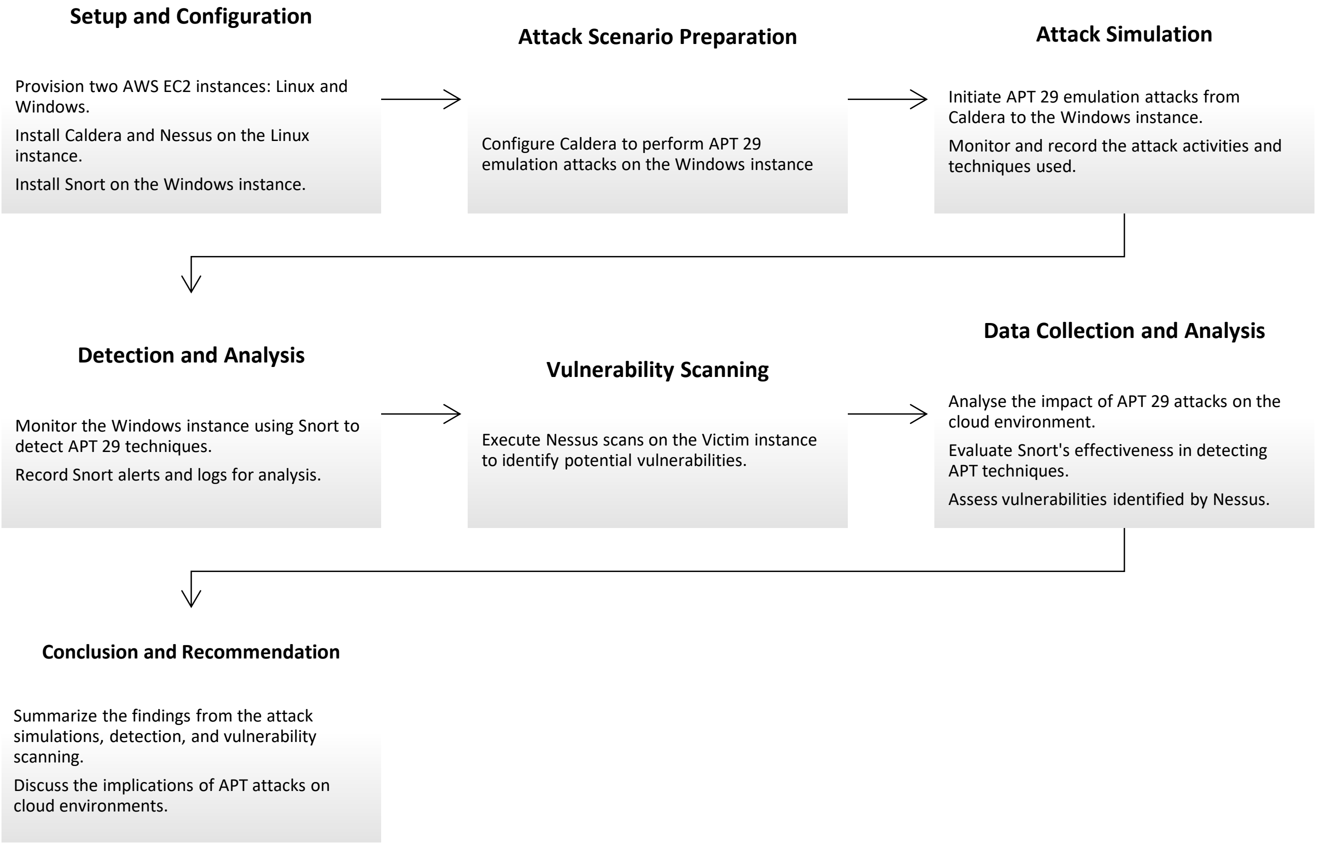

Setup and Configuration
Provision two AWS EC2 instances: Linux and Windows.
Install Caldera and Nessus on the Linux instance.
Install Snort on the Windows instance.
Attack Scenario Preparation
Configure Caldera to perform APT 29 emulation attacks on the Windows instance
Attack Simulation
Initiate APT 29 emulation attacks from Caldera to the Windows instance.
Monitor and record the attack activities and techniques used.
Detection and Analysis
Monitor the Windows instance using Snort to detect APT 29 techniques.
Record Snort alerts and logs for analysis.
Vulnerability Scanning
Execute Nessus scans on the Victim instance to identify potential vulnerabilities.
Data Collection and Analysis
Analyse the impact of APT 29 attacks on the cloud environment.
Evaluate Snort's effectiveness in detecting APT techniques.
Assess vulnerabilities identified by Nessus.
Conclusion and Recommendation
Summarize the findings from the attack simulations, detection, and vulnerability scanning.
Discuss the implications of APT attacks on cloud environments.

Figure 3 Research Flowchart

3.3 Experiment Workflow

The workflow employed to achieve the experiment is laid out as shown in Figure 4. The flowchart depicts the comprehensive progression of the experiment, encompassing the cloud setup, configuration and simulation of attacks using Cadera, detection using Snort, and vulnerability scanning using Nessus.

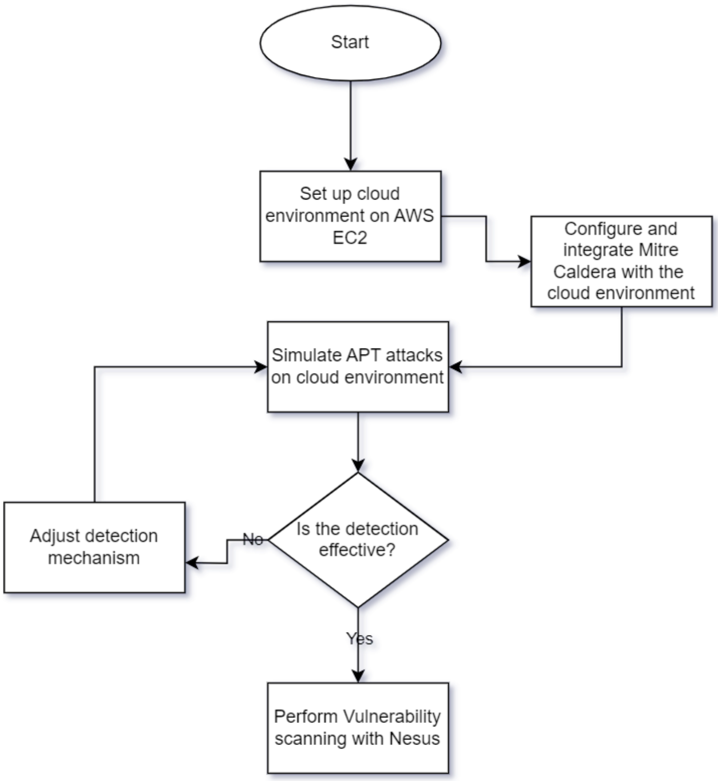

Start
Set up cloud environment on AWS EC2
Configure and integrate Mitre Caldera with the cloud environment
Simulate APT attacks on cloud environment
Is the detection effective?
No
Adjust detection mechanism
Yes
Perform Vulnerability scanning with Nesus

Figure 4 Flow chart of Simulation

3.4 Simulation of the Experiment

In this phase, the designed cloud environment serves as the canvas for the APT29 adversary emulation experiment. The simulated environment shown in figure 5 closely mirrors real-world cloud infrastructures, allowing for a controlled and secure emulation of advanced cyber threats. Two instances will be setup (Linux and Windows), Caldera will be used to initiate the APT attacks from the Linux instance to the windows, Snort will be used for detection of the APT attacks, and the Nessus scanner will be employed for scanning vulnerabilities that can be exploited on the target system. A more detailed explanation of this process will be discussed in the subsequent section.

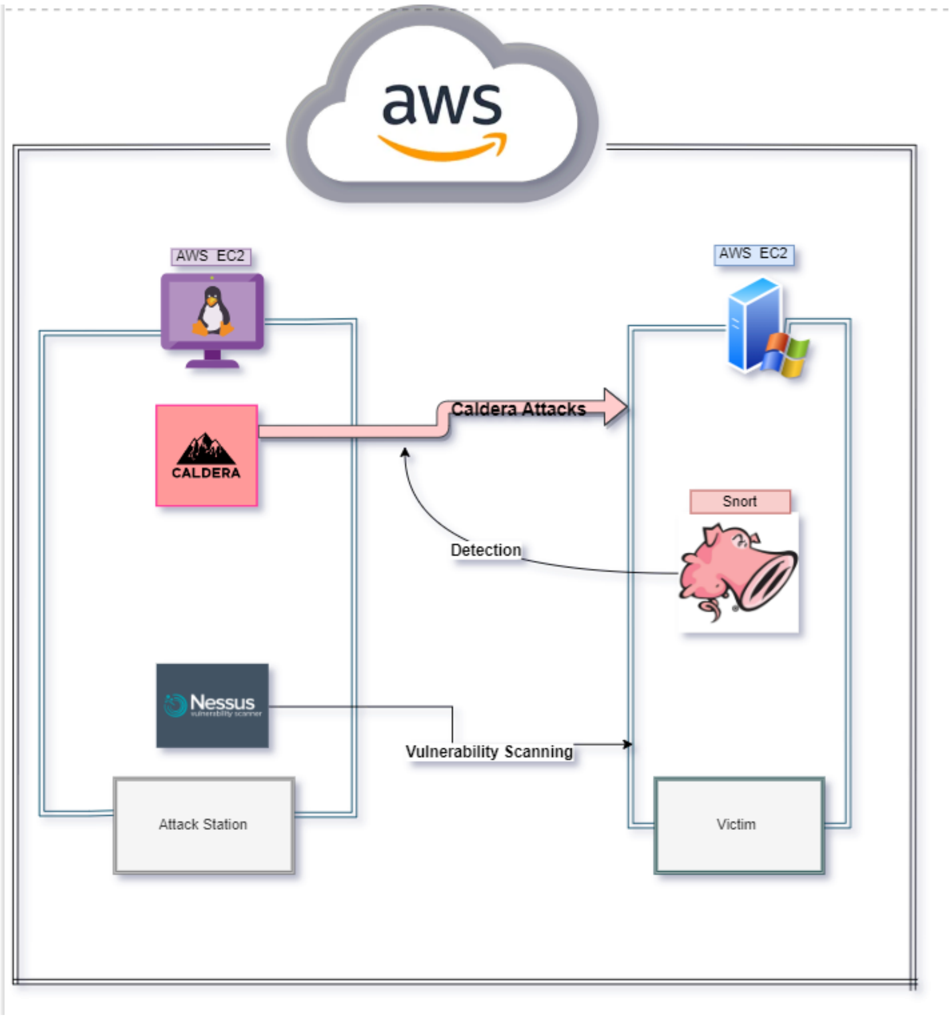


Figure 5 Components of the Simulation

3.4.1 Simulation of the Cloud Environment

a. Infrastructure Selection: A representative cloud environment will be set up using amazon web service, AWS EC2 instance. Two instances will be created, Linux OS for the attack station, and windows for the victim system.

b. Virtualization and Networking: A windows virtual machine will be set up on the EC2 instance, with networking components, and cloud services to replicate a realistic cloud environment. This will ensure proper isolation, segmentation, and network configuration to conduct the experiments securely.

c. Security Controls: The instance will be configured with proper security controls. Implement appropriate security controls, including firewalls, intrusion detection/prevention systems, encryption mechanisms, access controls, and logging mechanisms, to protect the simulated cloud environment from unauthorized access and mitigate potential risks.

d. Cloud Service Configuration: Provisioning and configuring relevant cloud services, such as storage, databases, and virtual networks, to emulate a functional cloud infrastructure for conducting the experiments.

3.4.2 Simulating APT Attacks on the Controlled Cloud Environment

The following steps will be carried out to simulate this experiment in the cloud environment.

1. Define APT Attack Scenarios

   Research APT techniques: This involves studying the MITRE ATT&CK framework and researching real-world APT techniques commonly observed in cloud environments.

   Choose relevant attack scenarios: Defining attack scenarios, following tactics and techniques as outlined by MITRE to ensure it aligns with the set objectives.
2. Configure and Customize Caldera

   Installing MITRE Caldera: MITRE Caldera will be set up in the controlled environment following the installation instructions provided by the project's documentation.

   Configure agents: Setting up Caldera agents on target systems within the cloud environment. These agents will simulate the presence of adversaries.

   Create adversary profiles: Customizing adversary profiles in Caldera to represent the APT29 attack scenarios to simulate.
3. Simulate APT Attacks

   Running simulations: Caldera will be utilised to initiate the APT attack simulations on the cloud environment. The agents will carry out actions based on the configured adversary profiles.

   Observe and record: Monitoring the simulated APT attacks and recording their behaviours, tactics, techniques, and procedures (TTPs) as they unfold in the cloud environment.
4. Assess Detection Capabilities

   Assess detection using Snort with configured rules.

   Evaluate detection rates: Determine how effective snort is in detecting APT-like activities and triggering alerts.

5. Record Findings

   Documenting results: Recording all findings from the APT simulations and detection assessments in detail, including any strengths or weaknesses identified in the cloud security.

   Analysing discrepancies: Comparing the results with the set objectives to see if there are any gaps between the expected and observed outcomes.

6. Utilize Nessus Vulnerability Scanning

   Set up Nessus: Install Nessus Vulnerability Scanner in the controlled cloud environment and configure it to scan the cloud infrastructure for vulnerabilities.

   Initiate scans: Run Nessus scans to identify potential vulnerabilities in the cloud systems, applications, and services.

   Analyse scan results: Review the scan results to identify vulnerabilities and prioritize them based on severity.

3.5 APT29 Emulation Plan

The EMU plan for APT29 integrates various techniques that the group has been observed employing in their operations, resulting in an Operation Flow. This EMU plan, and consequently the operation flow, can be categorized into two distinct approaches. By combining these scenarios and their respective techniques outlined in figure 6, APT29 emulation plan (ATT&CK Evaluations, 2019) creates a comprehensive and adaptable plan to carry out their cyber-espionage activities. This EMU plan will be utilised for our operation in this research.

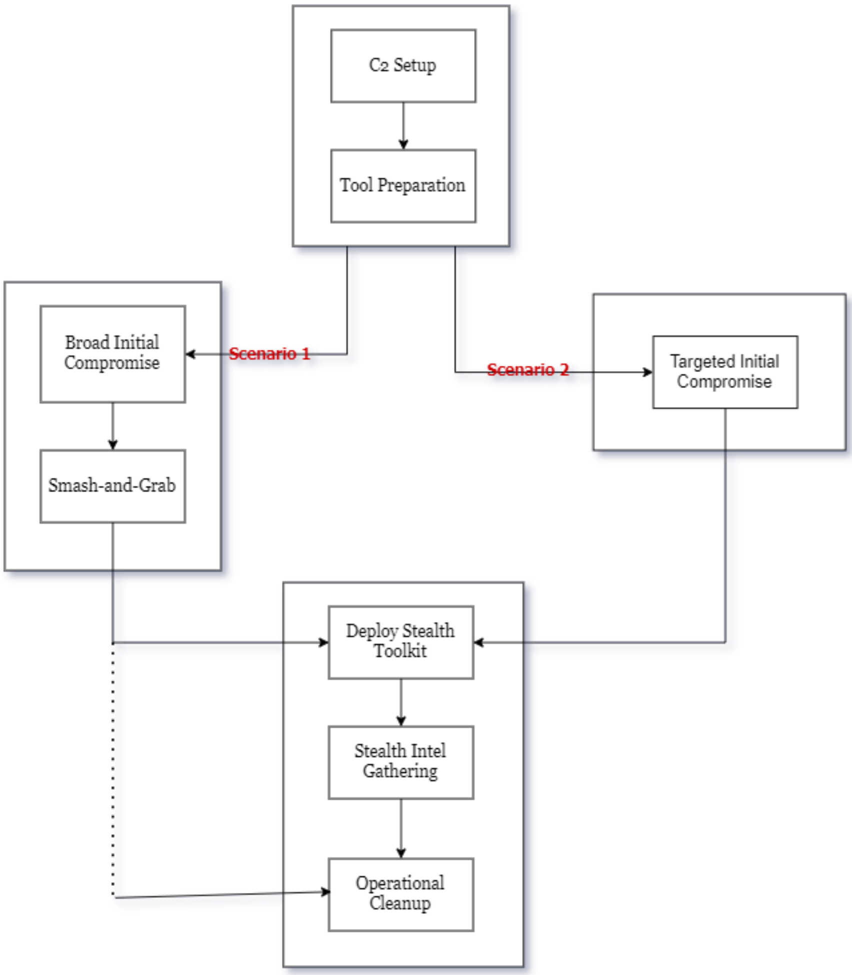


Figure 6 Operation flow of APT 29 EMU plan

Scenario 1: In this approach, APT29 adopts a "smash-and-grab" tactic for collection and exfiltration of data. They initiate widespread phishing attempts, casting a broad net to identify potentially valuable targets. Once they ascertain the value of a target, the group proceeds to deploy stealthier and more sophisticated malware to facilitate long-term exploitation of the compromised system.

Scenario 2: Here, APT29 employs a "low and slow" strategy to compromise a specific target through spear phishing. This method involves a more systematic and patient approach, aiming to gain initial control over the targeted entity. Over time, their objective is to expand their influence and ultimately take control of the entire domain.

3.5.1 Breakdown of APT29 Emulation Plan

APT29 is considered a well-structured and sufficiently funded cyber threat actor also known as "Cozy Bear", is a threat actor group believed to be associated with the Russian government. This group is believed to have been active since at least 2008 and may have achieved operational successes as recently as 2020. The emulation plan according to Centre for Threat-Informed Defence (2021) for APT29 is broken down below:

"Scenario 1 - Smash-and-grab

1. Initial Breach

   1.A - Method of Entry: Malicious File Execution (T1204 / T1204.002)

   1.B - Command and Scripting Interpreter: PowerShell (T1086 / T1059.001)

2. Rapid Collection and Exfiltration

   2.A - Data Collection (T1119, T1005, T1002 / T1560.001)

   2.B - Data Exfiltration via Command-and-Control Channel (T1041)

3. Deploy Stealth Toolkit

   3.A - Tool Transfer into the Environment (T1105)

   3.B - Bypass User Access Control to Elevate Privileges (T1088 / T1548.002)
   3.C - Registry Modification (T1112)

4. Defence Evasion and Discovery

   4.A - Tool Transfer into the Environment (T1105)

   4.B - Host Indicator Removal: File Deletion (T1107 / T1070.004)

   4.C - Discovery of System Information (T1016, T1033, T1063 / T1518.001, T1069, T1082, T1083)

5. Persistence

   5.A - Creation or Modification of a System Process: Windows Service (T1031 / T1543.003)

5.B - AutoStart Execution during Boot or Logon: Registry Run Keys / Startup Folder (T1060 / T1547.001)

6. Credential Access

6.A - Acquisition of Credentials from Password Stores: Credentials from Web Browsers (T1003 / T1555.003)

6.B - Acquisition of Unsecured Credentials: Private Keys (T1145 / T1552.004)
6.C - OS Credential Dumping: Security Account Manager (T1003 / T1003.002)

7. Collection and Exfiltration

7.A - Monitoring User Activities (T1113, T1115, T1056 / T1056.001)

7.B - Compression and Exfiltration of Data (T1048, T1002, T1022 / T1560.001)

8. Lateral Movement

8.A - Use of Remote Services: Windows Remote Management (T1021 / T1021.006)

8.B - Tool Transfer within the Environment (T1105)

8.C - Execution of System Services: Service Execution (T1035 / T1569.002)

9. Collection

9.A - Tool Transfer within the Environment (T1105)

9.B - Data Collection and Exfiltration (T1005, T1041, T1002, T1022 / T1560.001)

9.C - Host Indicator Removal: File Deletion (T1107 / T1070.004)

10. Persistence Execution

10.A - Execution of System Services: Service Execution (T1035 / T1569.002)

10.B - AutoStart Execution during Boot or Logon: Registry Run Keys / Startup Folder (T1060 / T1547.001)

Scenario 2 - "Low and Slow"

11. Initial Breach

    11.A - Method of Entry: Malicious File Execution (T1204 / T1204.002)

12. Fortify Access

    12.A - Host Indicator Removal: Time stomp (T1099 / T1070.006)

    12.B - Discovery of Security Software (T1063 / T1518.001)

    12.C - Software Discovery (T1518 / T1518.001)

13. Local Enumeration

    13.A - Discovery of System Information (T1082)

    13.B - Discovery of System Network Configuration (T1016)

    13.C - Discovery of System Owner/User Information (T1033)

    13.D - Discovery of Running Processes (T1057)

14. Elevation

    14.A - Bypass User Access Control to Elevate Privileges (T1088 / T1548.002)

    14.B - OS Credential Dumping: LSASS Memory (T1003 / T1003.001)

15. Establish Persistence

    15.A - Event-Triggered Execution: Windows Management Instrumentation Event Subscription (T1084 / T1546.003)

16. Lateral Movement

    16.A - Remote System Discovery (T1018)

    16.B - Discovery of System Owner/User Information (T1033)

    16.C - Use of Remote Services: Windows Remote Management (T1028 / T1021.006)

    16.D - OS Credential Dumping (T1003 / T1003.001)

17. Collection

    17.A - Collection of Emails: Local Email Collection (T1114 / T1114.001)

17.B - Data Collection from Local System (T1005)

17.C - Use of Obfuscated Files or Information (T1027)

18. Exfiltration

18.A - Data Exfiltration over Alternative Protocol (T1048 / T1567.002)

19. Clean Up

19.A - Host Indicator Removal: File Deletion (T1107 / T1070.004)

19.B - Host Indicator Removal: File Deletion (T1107 / T1070.004)

19.C - Host Indicator Removal: File Deletion (T1107 / T1070.004)

20. Leverage Persistence

20.A - Persistence Execution (T1085 / T1218.011, T1084 / T1546.003)

20.B - Use of Alternate Authentication Material: Pass the Ticket (T1097 / T1550.001, T1550.003)."

3.6 Data Analysis

Thematic analysis will be applied to analyse the qualitative data obtained from the literature review, focusing on identifying significant findings related to APT in cloud environments, as well as the existing approaches for detection and mitigation. The quantitative data gathered from the cloud experiments and vulnerability scanning will be subjected to thorough analysis and appropriate statistical techniques.

3.7 Ethical Considerations

In the realm of cybersecurity, a disheartening reality exists where offensive security tools originally intended for defenders to identify vulnerabilities are often misused by malicious individuals. The MITRE ATT&CK Matrix has raised awareness about various advanced persistent threats that capitalize on open-source offensive security tools. For example, APT 41, a state-sponsored espionage group from China, has utilized tools like Cobalt Strike, a tool like Caldera, for adversarial emulation purposes (MITRE Corporation, 2021). Caldera distinguishes itself as a responsible tool for emulating adversaries, and MITRE has implemented numerous safeguards to mitigate the risk of its misuse by malicious entities. For instance, the SandCat agent, which manages infected machines, deliberately avoids employing obfuscation techniques or attempting to camouflage itself within regular traffic patterns (Applebaum et al., 2016). Additionally, the open-source version of CALDERA is shipped with default, low-risk adversary profiles, while potentially malicious adversary profiles are concealed in the enterprise version. Notably, specific profiles like a basic ransomware adversary profile are not accessible to the public in the open-source CALDERA. To comprehend our adversaries in cyberspace better, it is imperative to understand their tactics and capabilities by simulating their attacks. Nevertheless, in developing such a system, a fundamental goal is to emulate adversaries responsibly and avoid empowering them.

4.0 IMPLEMENTATION

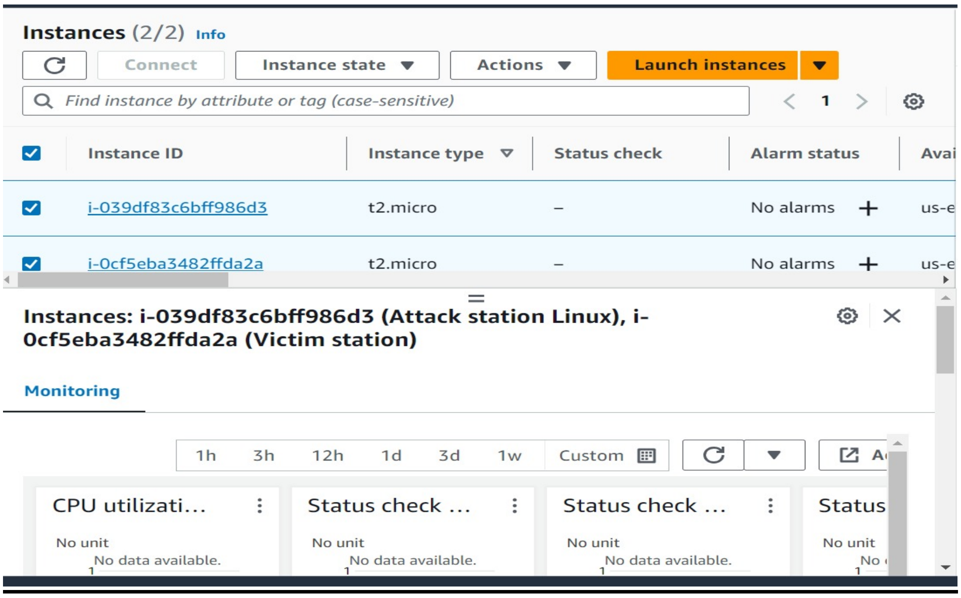
In this section, a comprehensive description of the procedures and configurations employed to establish the cloud environment on Amazon EC2, configure MITRE Caldera, and set up the attack tools for simulating APT attacks on the configured cloud environment is presented.

4.1 Setting Up the Infrastructure

The infrastructure required for the successful execution of this experiment has been carefully established and configured, including networking and security controls. This setup guarantees our ability to establish connectivity from the attack station to the victim station, ensuring the effectiveness of all simulations conducted using red team tactics for our APT simulations.

4.1.1 Setting Up the Cloud Environment

The process of establishing the cloud environment entails several key steps, including setting up the instance on AWS EC2, configuring virtualization and networking, implementing security controls, and configuring various cloud services to create a realistic and representative cloud environment. In this initial step, a virtual instance is provisioned within the AWS EC2 platform shown in figure 7. The specifications of this instance, including computing resources and operating system, are carefully tailored to replicate a genuine cloud environment.

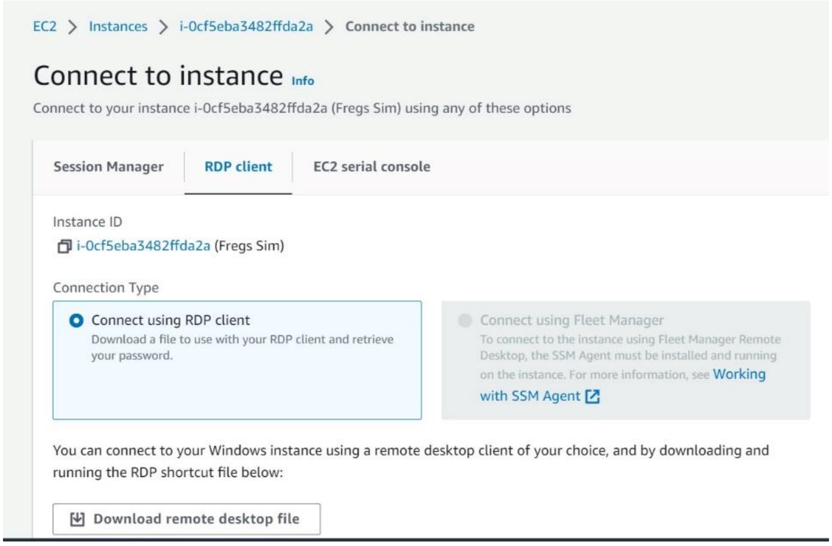


☑	Instance ID	Instance type	Status check	Alarm status	Avai
☑	i-039df83c6bff986d3	t2.micro	–	No alarms	us-e
☑	i-0cf5eba3482ffda2a	t2.micro	–	No alarms	us-e

Instances: i-039df83c6bff986d3 (Attack station Linux), i-0cf5eba3482ffda2a (Victim station)

Figure 7 EC2 Instances

With the cloud environment meticulously established, the next phase involves facilitating remote access to the virtual instance. This access is instrumental in enabling researchers to assume the role of the APT adversary and execute the planned emulation operation. Figure 8 shows connecting to the victim instance (windows) via the Remote Desktop Protocol (RDP), which is a fundamental mechanism for interacting with the virtual environment.



EC2 > Instances > i-0cf5eba3482ffda2a > Connect to instance

Connect to instance Info

Connect to your instance i-0cf5eba3482ffda2a (Fregs Sim) using any of these options

Session Manager | RDP client | EC2 serial console

Instance ID
i-0cf5eba3482ffda2a (Fregs Sim)

Connection Type

● Connect using RDP client
Download a file to use with your RDP client and retrieve your password.

○ Connect using Fleet Manager
To connect to the instance using Fleet Manager Remote Desktop, the SSM Agent must be installed and running on the instance. For more information, see Working with SSM Agent

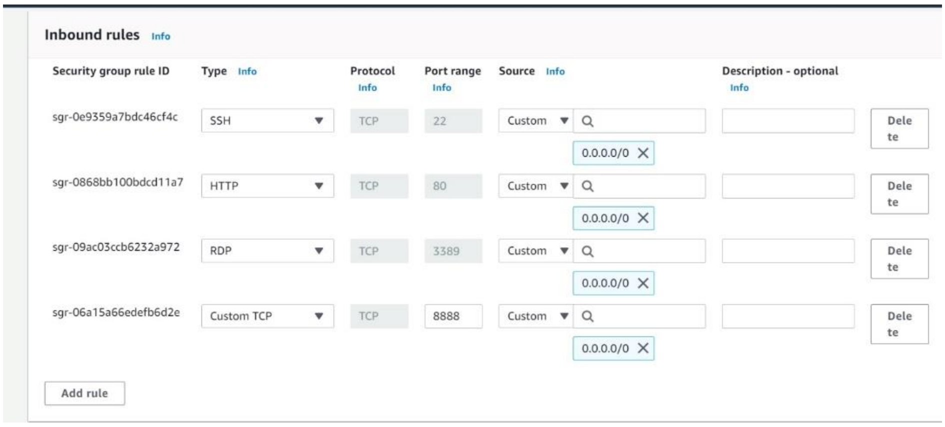
You can connect to your Windows instance using a remote desktop client of your choice, and by downloading and running the RDP shortcut file below:

Download remote desktop file

Figure 8 Connecting to EC2 instance through RDP.

The RDP configuration commences with the assignment of a designated public IP address to the virtual instance. Subsequently, appropriate security credentials, including usernames and passwords, are established to ensure secure access. These credentials are carefully managed to prevent unauthorized entry.

Inbound rules shown in figure 9 govern the incoming traffic allowed to access the virtual instance. These rules are meticulously configured to align with the APT adversary's tactics and methods, ensuring the accurate emulation of their activities. For example, specific ports associated with common attack vectors, such as Command and Control (C2) communication, might be opened to mimic an APT adversary's strategy. To facilitate RDP access, inbound firewall rules are configured to permit incoming traffic on the RDP port (typically port 3389). However, this access is judiciously restricted to authorized IP addresses, bolstering security, and mitigating potential risks associated with unauthorized access attempts.

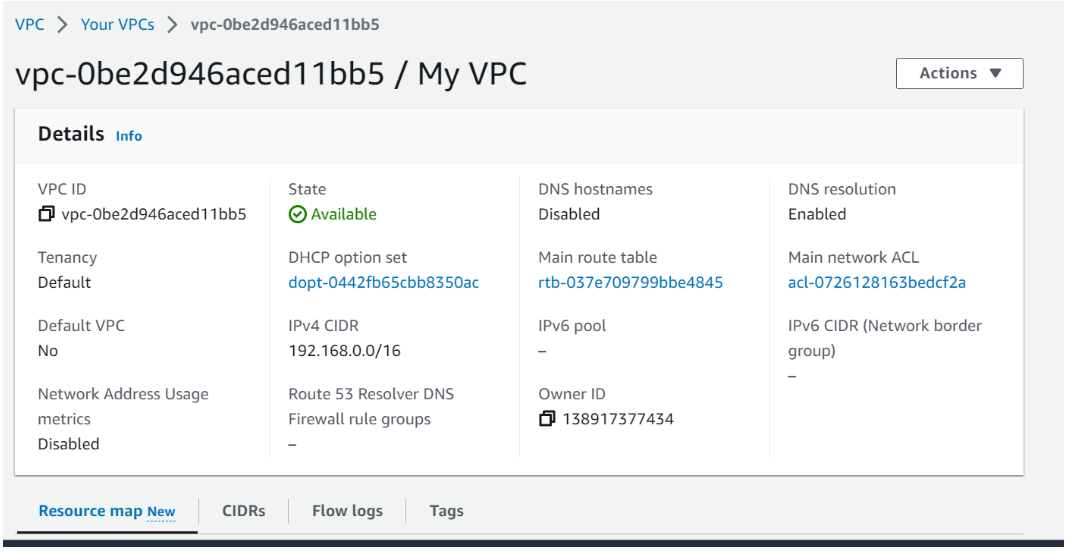


Inbound rules Info

Security group rule ID	Type Info	Protocol Info	Port range Info	Source Info	Description - optional Info	
sgr-0e9359a7bdc46cf4c	SSH	TCP	22	Custom 0.0.0.0/0		Delete
sgr-0868bb100bdcd11a7	HTTP	TCP	80	Custom 0.0.0.0/0		Delete
sgr-09ac03ccb6232a972	RDP	TCP	3389	Custom 0.0.0.0/0		Delete
sgr-06a15a66edefb6d2e	Custom TCP	TCP	8888	Custom 0.0.0.0/0		Delete

Figure 9 Inbound rules

Using the Amazon Virtual Private Cloud (VPC) we can make logically defined private networks within the AWS cloud. It empowers us with complete control over their network environment, enabling them to define their own IP address range, configure subnets, and set up routing tables and network gateways. With VPC, we can deploy AWS resources, such as EC2 instances and functions, in a secure, scalable, and highly available manner while maintaining data privacy and isolation. Overall, the VPC depicted in Figure 10 provides a flexible and customizable network infrastructure that allows us to manage our cloud-based applications with ease and confidence. The IPV4 CIDR notation 192.168.0.0/16 represents the range of IP addresses that will be used within the VPC indicating that the first 16 bits of the 32-bit IPv4 address are the network address, leaving 16 bits for host addresses within the subnet.



vpc-0be2d946aced11bb5 / My VPC

Details Info

VPC ID
vpc-0be2d946aced11bb5

State
Available

DNS hostnames
Disabled

DNS resolution
Enabled

Tenancy
Default

DHCP option set
dopt-0442fb65cbb8350ac

Main route table
rtb-037e709799bbe4845

Main network ACL
acl-0726128163bedcf2a

Default VPC
No

IPv4 CIDR
192.168.0.0/16

IPv6 pool
–

IPv6 CIDR (Network border group)
–

Network Address Usage metrics
Disabled

Route 53 Resolver DNS Firewall rule groups
–

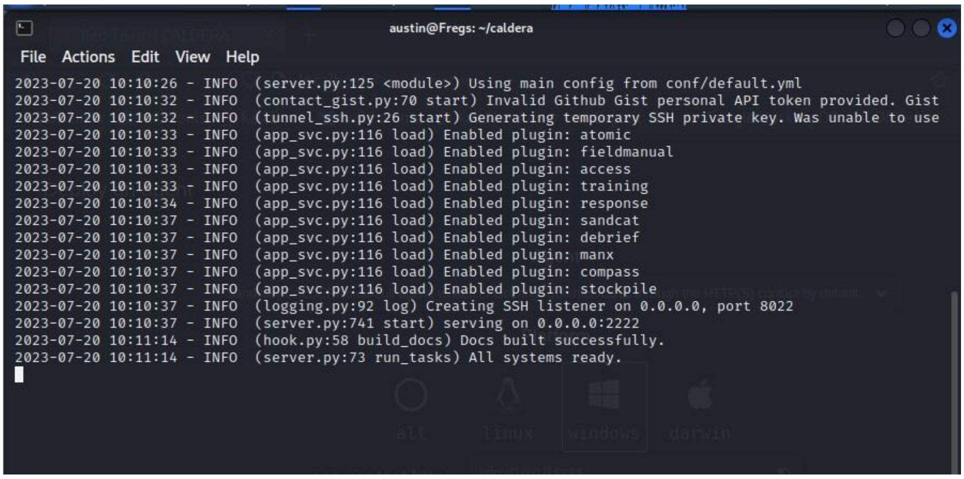
Owner ID
138917377434

Figure 10 VPC setup

4.1.2 Setting Up the Attack Station

In this section, we delve into the intricate process of configuring the attack station, installing essential dependencies for the Caldera framework, initiating simulated attacks, and orchestrating covert APT-like actions within the cloud environment. A Linux workstation is prepared to emulate the APT actors' activities. The APT actors use phishing techniques and the Caldera framework to deliver and execute malicious files on a Windows victim machine from the Linux workstation for initial access. The attack station serves as the command centre for orchestrating the APT adversary emulation operation. Its configuration involves setting up a designated system with the necessary tools and software for controlling the emulation environment.

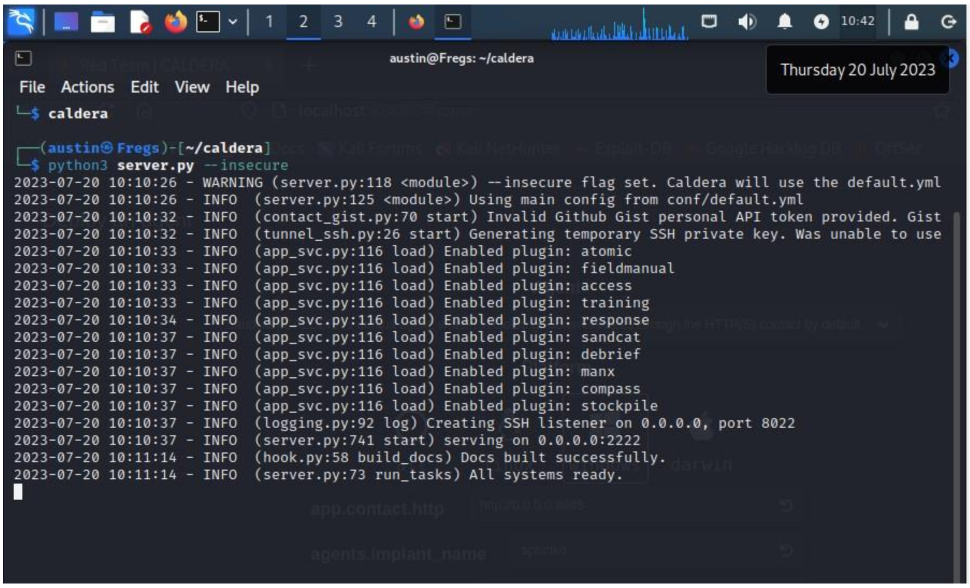
Prior to launching any attack, the Caldera framework's dependencies must be installed on the attack station as shown in Figure 11. These dependencies encompass essential components that empower Caldera's functionality, including Python libraries, database systems, and third-party modules.



```
2023-07-20 10:10:26 - INFO  (server.py:125 <module>) Using main config from conf/default.yml
2023-07-20 10:10:32 - INFO  (contact_gist.py:70 start) Invalid Github Gist personal API token provided. Gist
2023-07-20 10:10:32 - INFO  (tunnel_ssh.py:26 start) Generating temporary SSH private key. Was unable to use
2023-07-20 10:10:33 - INFO  (app_svc.py:116 load) Enabled plugin: atomic
2023-07-20 10:10:33 - INFO  (app_svc.py:116 load) Enabled plugin: fieldmanual
2023-07-20 10:10:33 - INFO  (app_svc.py:116 load) Enabled plugin: access
2023-07-20 10:10:33 - INFO  (app_svc.py:116 load) Enabled plugin: training
2023-07-20 10:10:34 - INFO  (app_svc.py:116 load) Enabled plugin: response
2023-07-20 10:10:37 - INFO  (app_svc.py:116 load) Enabled plugin: sandcat
2023-07-20 10:10:37 - INFO  (app_svc.py:116 load) Enabled plugin: debrief
2023-07-20 10:10:37 - INFO  (app_svc.py:116 load) Enabled plugin: manx
2023-07-20 10:10:37 - INFO  (app_svc.py:116 load) Enabled plugin: compass
2023-07-20 10:10:37 - INFO  (app_svc.py:116 load) Enabled plugin: stockpile
2023-07-20 10:10:37 - INFO  (logging.py:92 log) Creating SSH listener on 0.0.0.0, port 8022
2023-07-20 10:10:37 - INFO  (server.py:741 start) serving on 0.0.0.0:2222
2023-07-20 10:11:14 - INFO  (hook.py:58 build_docs) Docs built successfully.
2023-07-20 10:11:14 - INFO  (server.py:73 run_tasks) All systems ready.
```

Figure 11 Installing caldera dependencies.

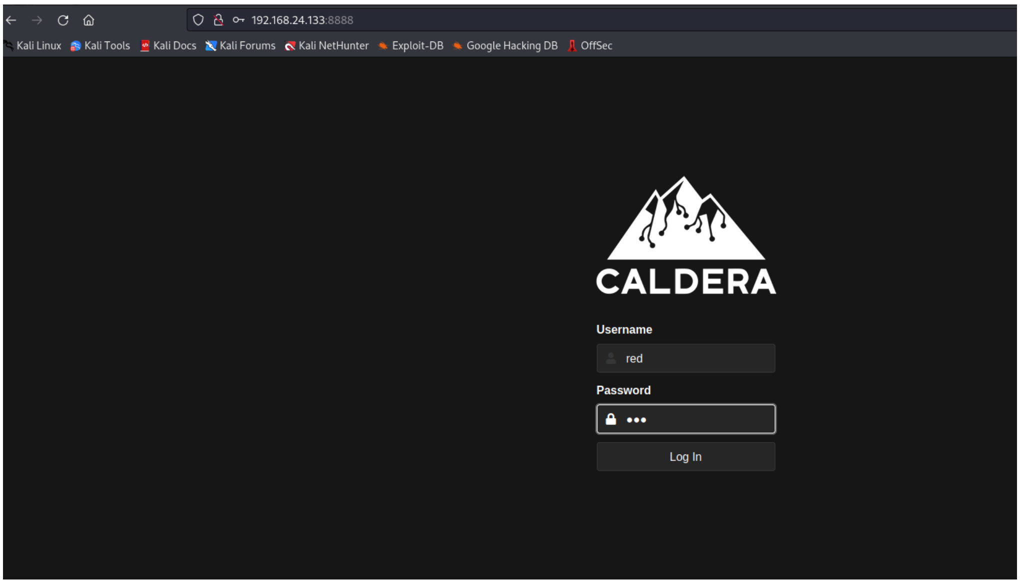
With the dependencies in place, Caldera is initiated on the attack station. Figure 12 shows caldera initialised successfully. The Caldera interface serves as the control hub, enabling experts to deploy and manage the various elements of the APT adversary emulation operation.



```
└─$ caldera

┌──(austin㉿Fregs)-[~/caldera]
└─$ python3 server.py --insecure
2023-07-20 10:10:26 - WARNING (server.py:118 <module>) --insecure flag set. Caldera will use the default.yml
2023-07-20 10:10:26 - INFO  (server.py:125 <module>) Using main config from conf/default.yml
2023-07-20 10:10:32 - INFO  (contact_gist.py:70 start) Invalid Github Gist personal API token provided. Gist
2023-07-20 10:10:32 - INFO  (tunnel_ssh.py:26 start) Generating temporary SSH private key. Was unable to use
2023-07-20 10:10:33 - INFO  (app_svc.py:116 load) Enabled plugin: atomic
2023-07-20 10:10:33 - INFO  (app_svc.py:116 load) Enabled plugin: fieldmanual
2023-07-20 10:10:33 - INFO  (app_svc.py:116 load) Enabled plugin: access
2023-07-20 10:10:33 - INFO  (app_svc.py:116 load) Enabled plugin: training
2023-07-20 10:10:34 - INFO  (app_svc.py:116 load) Enabled plugin: response
2023-07-20 10:10:37 - INFO  (app_svc.py:116 load) Enabled plugin: sandcat
2023-07-20 10:10:37 - INFO  (app_svc.py:116 load) Enabled plugin: debrief
2023-07-20 10:10:37 - INFO  (app_svc.py:116 load) Enabled plugin: manx
2023-07-20 10:10:37 - INFO  (app_svc.py:116 load) Enabled plugin: compass
2023-07-20 10:10:37 - INFO  (app_svc.py:116 load) Enabled plugin: stockpile
2023-07-20 10:10:37 - INFO  (logging.py:92 log) Creating SSH listener on 0.0.0.0, port 8022
2023-07-20 10:10:37 - INFO  (server.py:741 start) serving on 0.0.0.0:2222
2023-07-20 10:11:14 - INFO  (hook.py:58 build_docs) Docs built successfully.
2023-07-20 10:11:14 - INFO  (server.py:73 run_tasks) All systems ready.
```

Figure 12 Starting Caldera

Upon successful initialization, we can access the Caldera Red Team interface via a web browser on the local host. This interface shown in figure 13 offers a visual dashboard that provides an overview of ongoing operations, adversaries, abilities, and executed attacks.



Username: red

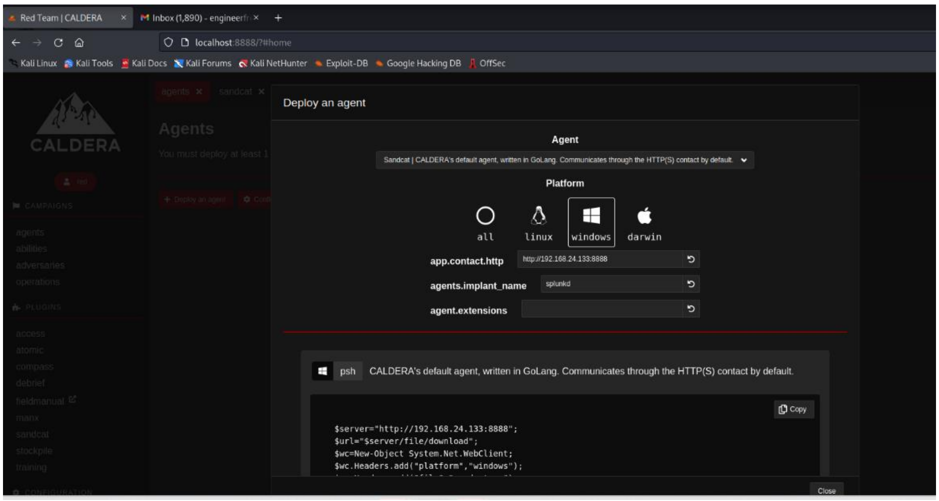
Password: •••

Figure 13 Accessing caldera red team on Local host.

4.2 Simulating Attacks on Mitre Caldera

The objective of this stage is to design and implement an operation that mimics the tactics, techniques, and procedures (TTPs) of an APT adversary. This involves planning the attack methods that the APT actors would use to breach the cloud environment through social engineering and advanced attack tools. Caldera will be used to emulate an APT29 operation with abilities as outlined from MITRE ATT&CK. The steps employed to achieve this are outlined in the subsequent sections.

The first step involves deploying an agent on Caldera depicted in Figure 14, which serves as the foothold within the cloud environment for executing the APT-like activities. This agent can be strategically positioned to initiate attacks from within the simulated environment.



Deploy an agent

Agent

Sandcat | CALDERA's default agent, written in GoLang. Communicates through the HTTP(S) contact by default.

Platform

all linux [✓ windows] darwin

app.contact.http: http://192.168.24.133:8888

agents.implant_name: splunkd

agent.extensions:

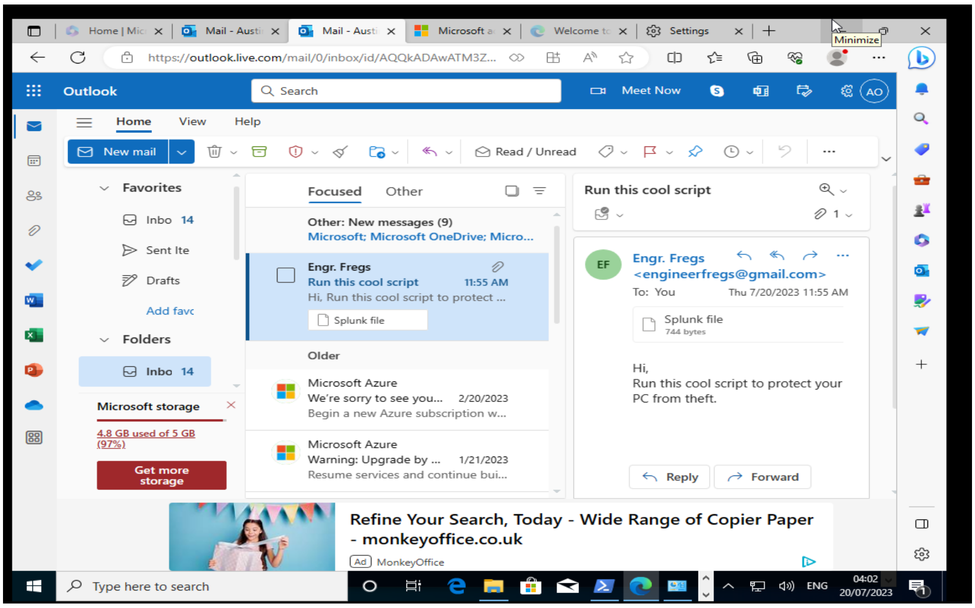
psh CALDERA's default agent, written in GoLang. Communicates through the HTTP(S) contact by default.

```
$server="http://192.168.24.133:8888";
$url="$server/file/download";
$wc=New-Object System.Net.WebClient;
$wc.Headers.add("platform","windows");
```

Figure 14 Deploying an agent on Caldera.

The APT group initiates the attack by conducting thorough reconnaissance to identify potential targets within the cloud environment. They may analyze publicly available information like staff email address, network scanning results, or gather intelligence from open-source channels to identify vulnerable systems.

Once the targets are identified, the attackers craft convincing and personalized phishing emails as depicted in Figure 15. These emails are carefully designed to appear legitimate and often mimic reputable sources, such as business partners, service providers, or internal colleagues. The email includes social engineering tactics to lure the target into downloading and executing the malicious file attachment.



Other: New messages (9)
Microsoft; Microsoft OneDrive; Micro...

Engr. Fregs
Run this cool script 11:55 AM
Hi, Run this cool script to protect ...
Splunk file

Older

Microsoft Azure
We're sorry to see you... 2/20/2023
Begin a new Azure subscription w...

Microsoft Azure
Warning: Upgrade by ... 1/21/2023
Resume services and continue bui...

Run this cool script

Engr. Fregs
<engineerfregs@gmail.com>
To: You Thu 7/20/2023 11:55 AM

Splunk file
744 bytes

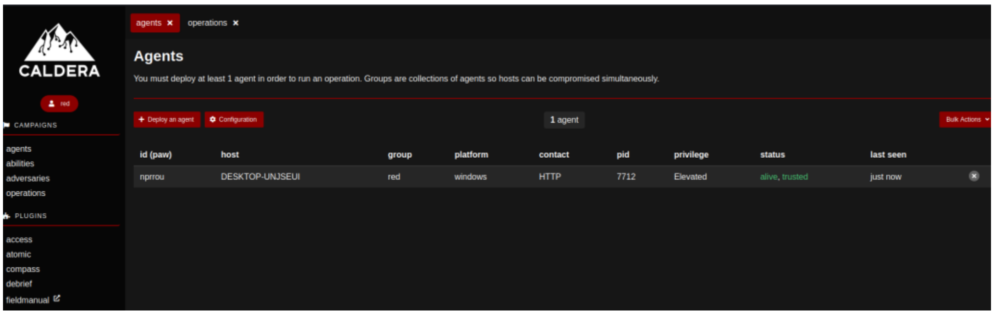
Hi,
Run this cool script to protect your PC from theft.

Refine Your Search, Today - Wide Range of Copier Paper - monkeyoffice.co.uk
Ad MonkeyOffice

Figure 15 Malicious file sent via Phishing email to user.

The malicious file attached to the phishing email is the primary payload of the attack. Using their Linux workstation, the attackers create a tailored and evasive malware executable that can bypass traditional security measures. The malware may be obfuscated or packed to avoid detection by antivirus software.

The malicious file attachment serves as a conduit for establishing a Command and Control (C2) connection between the attacker and the compromised instance (victim). This connection replicated in Figure 16 depicts the covert communication channels that APT adversaries commonly utilize. Upon successful execution of the initial access, the C2 connection is established between the compromised agent within the cloud environment and the Caldera control station. This enables us to monitor and analyse the communication flow, further refining the emulation process.



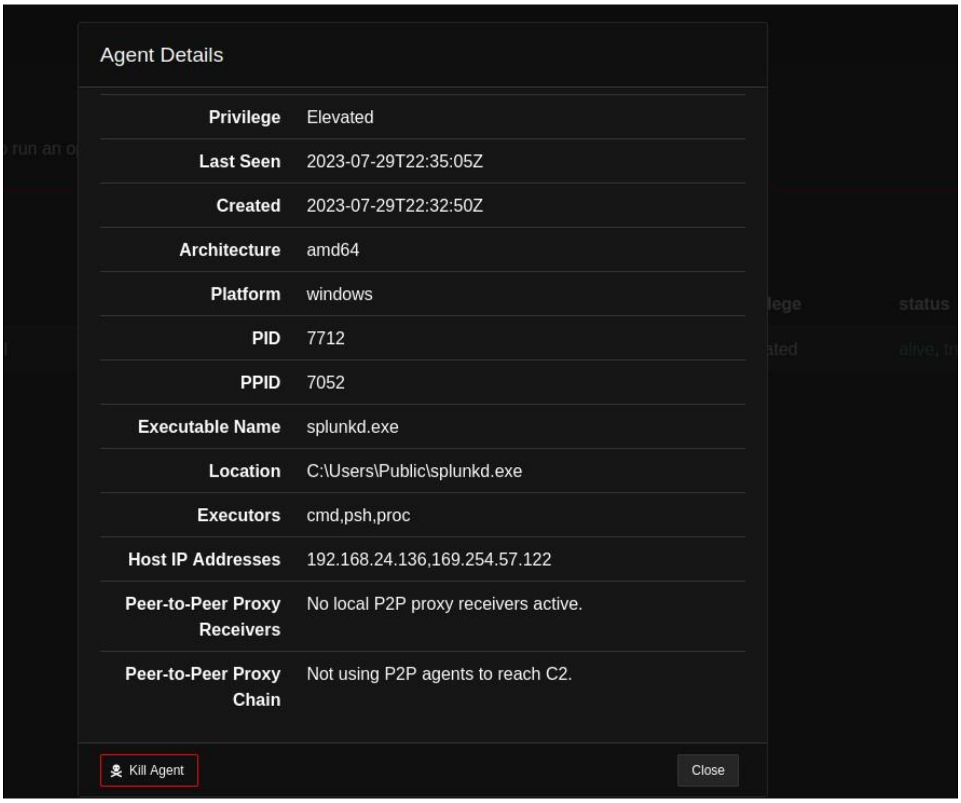
Agents

You must deploy at least 1 agent in order to run an operation. Groups are collections of agents so hosts can be compromised simultaneously.

id (paw)	host	group	platform	contact	pid	privilege	status	last seen
nprrou	DESKTOP-UNJSEUI	red	windows	HTTP	7712	Elevated	alive, trusted	just now

Figure 16 Command and Control Access established.

Comprehensive details about the agent, including its characteristics, elevation status, process identifier and IP address, are meticulously logged and tracked as shown in Figure 17. These details contribute to a holistic understanding of the attack's impact and effectiveness.



Agent Details

Privilege	Elevated
Last Seen	2023-07-29T22:35:05Z
Created	2023-07-29T22:32:50Z
Architecture	amd64
Platform	windows
PID	7712
PPID	7052
Executable Name	splunkd.exe
Location	C:\Users\Public\splunkd.exe
Executors	cmd,psh,proc
Host IP Addresses	192.168.24.136,169.254.57.122
Peer-to-Peer Proxy Receivers	No local P2P proxy receivers active.
Peer-to-Peer Proxy Chain	Not using P2P agents to reach C2.

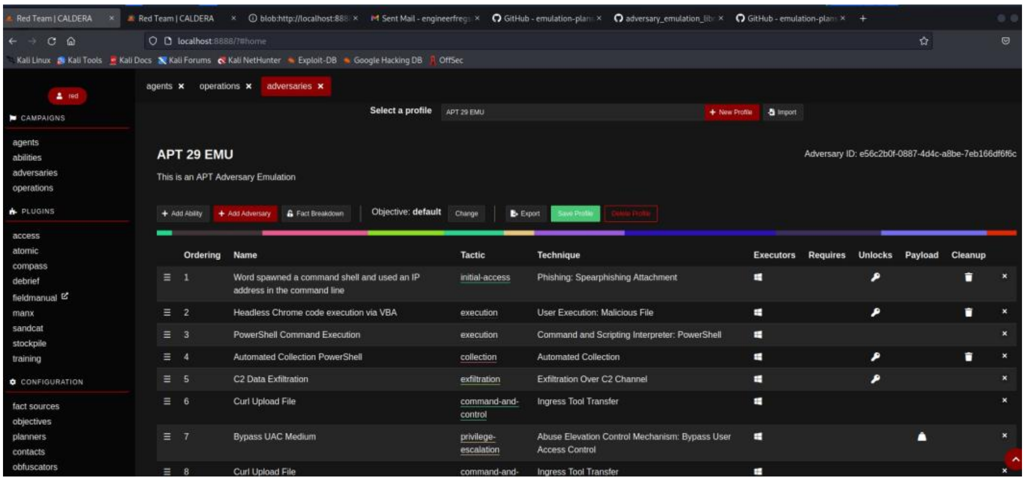
Figure 17 Agent details

In this emulated scenario, the attacker employs a range of tactics to achieve their objectives within the cloud environment. Privilege escalation and lateral movement are central to their strategy, as they skilfully exploit vulnerabilities across systems and accounts, gaining higher levels of access and manoeuvring stealthily across the infrastructure. Notably, the attacker directs their attention towards cloud resources, strategically targeting databases, storage repositories, and virtual machines. This precision allows them to exfiltrate critical data or disrupt vital services, potentially causing significant harm. The peak of their effort rests on data exfiltration, wherein valuable information is carefully extracted from the cloud, setting the stage for potential exploitation or illicit sale. As the APT operation unfolds, an inherent emphasis on secrecy is evident. The attackers meticulously erase traces of their activities, scrubbing logs and eradicating any footprint that could trigger detection. This calculated approach ensures their covert presence and heightens the challenge for security teams aiming to thwart their malicious endeavours.

4.3 Implementing the APT29 Emulation Plan

The Emulation plan selected for this experiment is the APT29 Emu plan and it is broken into 2 scenarios. Scenario 1 involves a quick and noisy intrusion, followed by a focused mission to collect data and exfiltrate it. Next, the scenario shifts to more stealthy techniques for persistence, data collection, credential access, and lateral movement. The scenario concludes with the implementation of previously established persistence methods. On the other hand, Scenario 2 follows a slower asnd more discreet approach, compromising the initial target, establishing persistence, acquiring credentials, and systematically compromising the entire domain. The scenario ends by executing the previously established persistence mechanism (Centre for Threat-Informed Defence, 2021).

Creating the adversary emulation involves the strategic selection and configuration of abilities, Figure 18 represents a spectrum of distinct attack actions that the APT29 emulation can execute. These abilities encompass a wide array of manoeuvres, spanning from lateral movement and data exfiltration to privilege escalation to data exfiltration. The process requires a careful tailoring of the APT29 toolkit to precisely match specific attack scenarios.



Select a profile: APT 29 EMU

APT 29 EMU

This is an APT Adversary Emulation

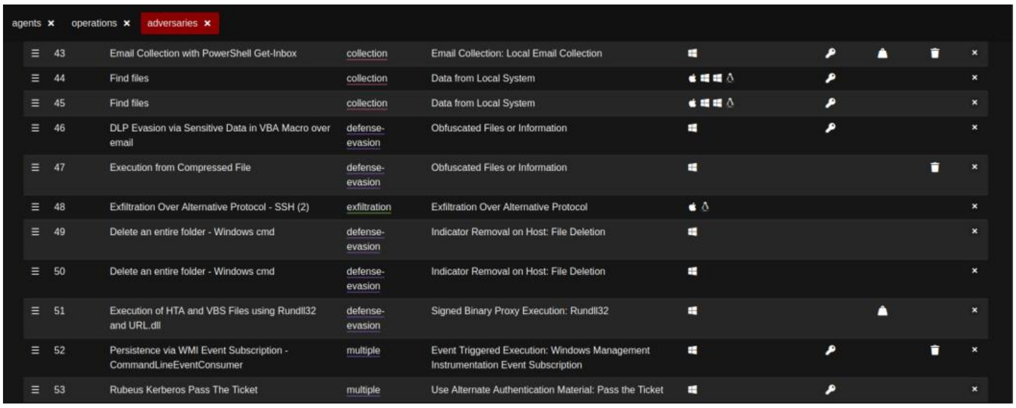
Adversary ID: e56c2b0f-0887-4d4c-a8be-7eb166df6f6c

Objective: **default**

Ordering	Name	Tactic	Technique	Executors	Requires	Unlocks	Payload	Cleanup
1	Word spawned a command shell and used an IP address in the command line	initial-access	Phishing: Spearphishing Attachment	⊞		🔑		🗑
2	Headless Chrome code execution via VBA	execution	User Execution: Malicious File	⊞		🔑		🗑
3	PowerShell Command Execution	execution	Command and Scripting Interpreter: PowerShell	⊞				
4	Automated Collection PowerShell	collection	Automated Collection	⊞		🔑		🗑
5	C2 Data Exfiltration	exfiltration	Exfiltration Over C2 Channel	⊞		🔑		
6	Curl Upload File	command-and-control	Ingress Tool Transfer	⊞				
7	Bypass UAC Medium	privilege-escalation	Abuse Elevation Control Mechanism: Bypass User Access Control	⊞			▲	
8	Curl Upload File	command-and-	Ingress Tool Transfer	⊞				

Figure 18 Adding Abilities to the Adversary

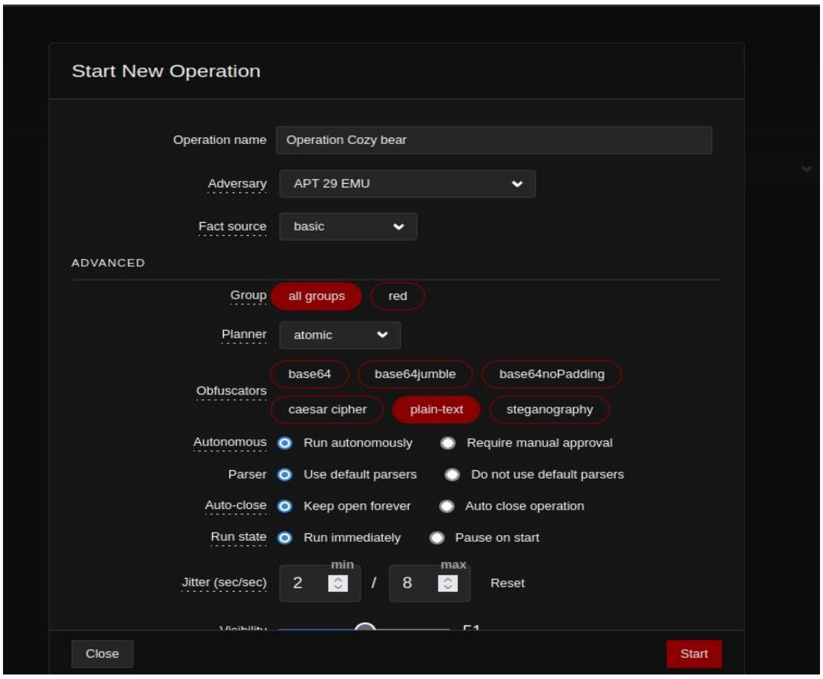
This step involves the strategic selection and configuration of abilities, representing a spectrum of distinct attack actions that the APT29 emulation can execute. These abilities carefully selected and added to the adversary profile shown in Figure 19 encompass a wide array of manoeuvres, spanning from lateral movement and data collection, exfiltration to privilege escalation and clean up. The process requires a careful tailoring of the APT29 toolkit to precisely match specific attack scenarios.



43	Email Collection with PowerShell Get-Inbox	collection	Email Collection: Local Email Collection
44	Find files	collection	Data from Local System
45	Find files	collection	Data from Local System
46	DLP Evasion via Sensitive Data in VBA Macro over email	defense-evasion	Obfuscated Files or Information
47	Execution from Compressed File	defense-evasion	Obfuscated Files or Information
48	Exfiltration Over Alternative Protocol - SSH (2)	exfiltration	Exfiltration Over Alternative Protocol
49	Delete an entire folder - Windows cmd	defense-evasion	Indicator Removal on Host: File Deletion
50	Delete an entire folder - Windows cmd	defense-evasion	Indicator Removal on Host: File Deletion
51	Execution of HTA and VBS Files using Rundll32 and URL.dll	defense-evasion	Signed Binary Proxy Execution: Rundll32
52	Persistence via WMI Event Subscription - CommandLineEventConsumer	multiple	Event Triggered Execution: Windows Management Instrumentation Event Subscription
53	Rubeus Kerberos Pass The Ticket	multiple	Use Alternate Authentication Material: Pass the Ticket

Figure 19 Configuring abilities Line 43 to 53

Once the arsenal of abilities is setup, the emulation journey advances with the initiation of "Operation Cozy Bear" within the Caldera framework. This operation with details shown in figure 20 encapsulates a meticulously planned sequence of actions, intricately mirroring the precise techniques and strategic manoeuvres synonymous with APT29.



Start New Operation

Operation name: Operation Cozy bear

Adversary: APT 29 EMU

Fact source: basic

ADVANCED

Group: [✓ all groups] red

Planner: atomic

Obfuscators: base64 base64jumble base64noPadding caesar cipher [✓ plain-text] steganography

Autonomous: ● Run autonomously ○ Require manual approval

Parser: ● Use default parsers ○ Do not use default parsers

Auto-close: ● Keep open forever ○ Auto close operation

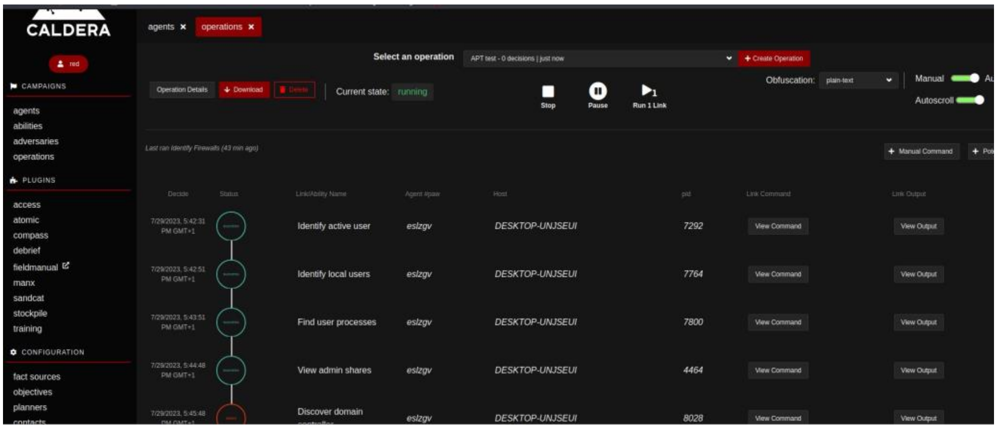
Run state: ● Run immediately ○ Pause on start

Jitter (sec/sec): min 2 / max 8 Reset

Visibility: 51

Figure 20 Starting Operation Cozy Bear

The execution of Operation Cozy Bear revealed in figure 21 triggers a series of calculated actions, including but not limited to phishing campaigns, lateral movement, exploitation, and data manipulation. This dynamic and multifaceted operation serves as a comprehensive emulation of APT29's modus operandi.



Select an operation: APT test - 0 decisions | just now

Current state: running

Obfuscation: plain-text

Manual

Autoscroll

Last ran Identify Firewalls (43 min ago)

Decide	Status	Link/Ability Name	Agent #paw	Host	pid	Link Command	Link Output
7/29/2023, 5:42:31 PM GMT+1		Identify active user	eslzgv	DESKTOP-UNJSEUI	7292	View Command	View Output
7/29/2023, 5:42:51 PM GMT+1		Identify local users	eslzgv	DESKTOP-UNJSEUI	7764	View Command	View Output
7/29/2023, 5:43:51 PM GMT+1		Find user processes	eslzgv	DESKTOP-UNJSEUI	7800	View Command	View Output
7/29/2023, 5:44:48 PM GMT+1		View admin shares	eslzgv	DESKTOP-UNJSEUI	4464	View Command	View Output
7/29/2023, 5:45:48 PM GMT+1		Discover domain controller	eslzgv	DESKTOP-UNJSEUI	8028	View Command	View Output

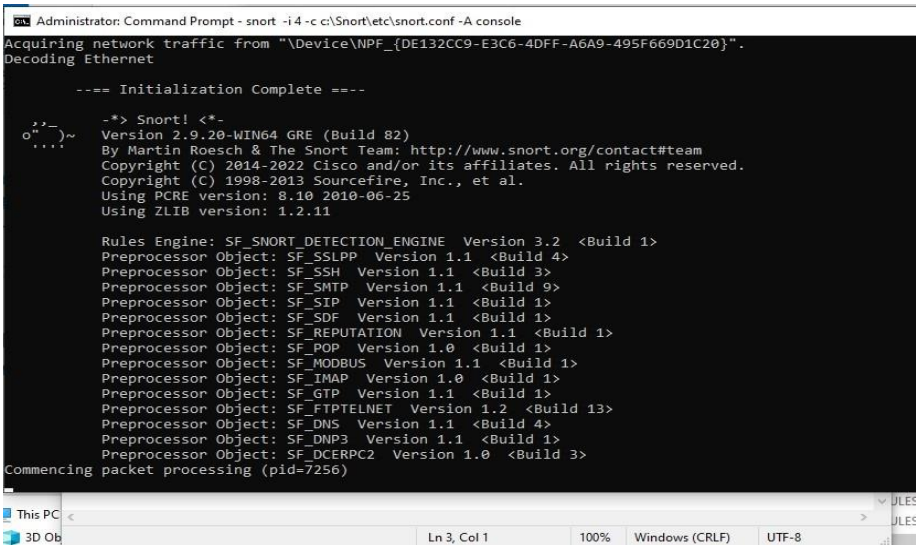
Figure 21 Running operation Cozy Bear

Through the meticulous setup of the attack station, the deployment of agents, the orchestration of malicious activities, and the execution of abilities, the APT adversary emulation operation unfolds, shedding light on the intricacies of advanced cyber threats within a controlled and secured environment.

4.4 Snort Configuration for Detection

To enhance the environment's capability to identify APT-like behaviors, a widely recognized intrusion detection system, is implemented. The process of installing Snort and configuring rules for APT29 detection on the Windows victim station encompasses the establishment of an intrusion detection system (IDS). This includes defining rules designed to pinpoint network patterns aligned with APT29's methods. Initiating Snort on the victim station, as depicted in figure 22, serves to identify any APT-like behaviours present on the target station's network.

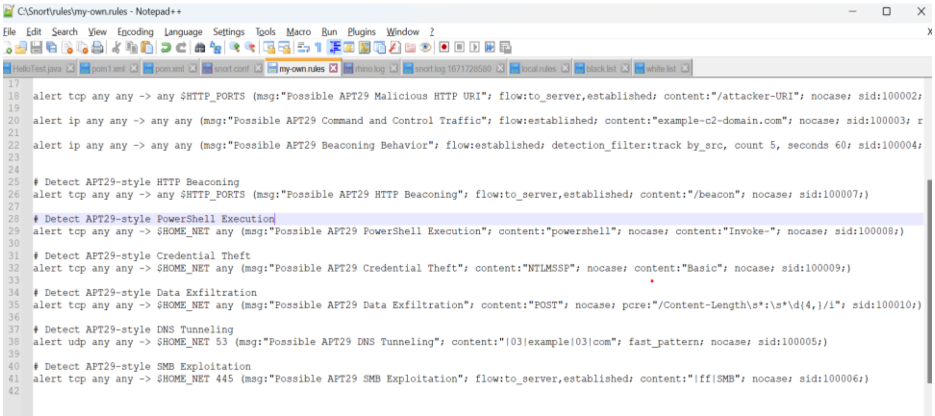
.


Administrator: Command Prompt - snort -i 4 -c c:\Snort\etc\snort.conf -A console
This PC
3D Ob
Ln 3, Col 1
100%
Windows (CRLF)
UTF-8

```
Acquiring network traffic from "\Device\NPF_{DE132CC9-E3C6-4DFF-A6A9-495F669D1C20}".
Decoding Ethernet

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.20-WIN64 GRE (Build 82)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using PCRE version: 8.10 2010-06-25
           Using ZLIB version: 1.2.11

           Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 3.2  <Build 1>
           Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
           Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
           Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
           Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
           Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
           Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
           Preprocessor Object: SF_POP  Version 1.0  <Build 1>
           Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
           Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
           Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
           Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
           Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
           Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
           Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
Commencing packet processing (pid=7256)
```

Figure 22 Initialising Snort

A strategic selection of Snort rules is paramount. These rules are meticulously tailored to identify and flag activities characteristic of APT attacks. They encompass a spectrum of behaviours, including unusual network traffic patterns, anomalous data exfiltration attempts, and signs of lateral movement. Each Snort rule is precisely defined as shown in Figure 23, specify the network behaviours or traffic patterns it aims to detect. These rules are expertly honed to mirror the tactics, techniques, and procedures associated with APT29, aligning the detection mechanism with the adversary's modus operand.

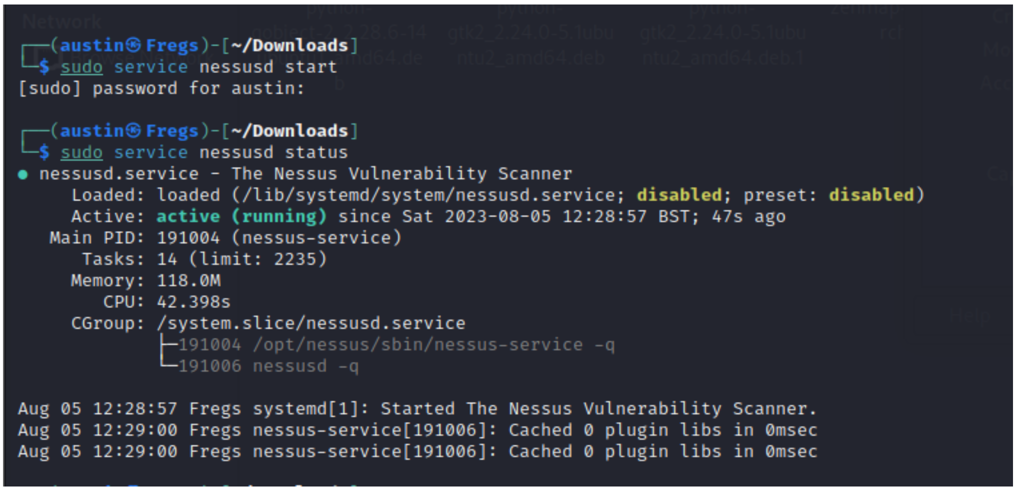


```

alert tcp any any -> any $HTTP_PORTS (msg:"Possible APT29 Malicious HTTP URI"; flow:to_server,established; content:"/attacker-URI"; nocase; sid:100002;

alert ip any any -> any any (msg:"Possible APT29 Command and Control Traffic"; flow:established; content:"example-c2-domain.com"; nocase; sid:100003; r

alert ip any any -> any any (msg:"Possible APT29 Beaconing Behavior"; flow:established; detection_filter:track by_src, count 5, seconds 60; sid:100004;


# Detect APT29-style HTTP Beaconing
alert tcp any any -> any $HTTP_PORTS (msg:"Possible APT29 HTTP Beaconing"; flow:to_server,established; content:"/beacon"; nocase; sid:100007;)

# Detect APT29-style PowerShell Execution
alert tcp any any -> $HOME_NET any (msg:"Possible APT29 PowerShell Execution"; content:"powershell"; nocase; content:"Invoke-"; nocase; sid:100008;)

# Detect APT29-style Credential Theft
alert tcp any any -> $HOME_NET any (msg:"Possible APT29 Credential Theft"; content:"NTLMSSP"; nocase; content:"Basic"; nocase; sid:100009;)

# Detect APT29-style Data Exfiltration
alert tcp any any -> $HOME_NET any (msg:"Possible APT29 Data Exfiltration"; content:"POST"; nocase; pcre:"/Content-Length\s*:\s*\d{4,}/i"; sid:100010;)

# Detect APT29-style DNS Tunneling
alert udp any any -> $HOME_NET 53 (msg:"Possible APT29 DNS Tunneling"; content:"|03|example|03|com"; fast_pattern; nocase; sid:100005;)

# Detect APT29-style SMB Exploitation
alert tcp any any -> $HOME_NET 445 (msg:"Possible APT29 SMB Exploitation"; flow:to_server,established; content:"|ff|SMB"; nocase; sid:100006;)

```

Figure 23 Snort Rules for APT Detection

4.5 Nessus Configuration Vulnerability Scanning

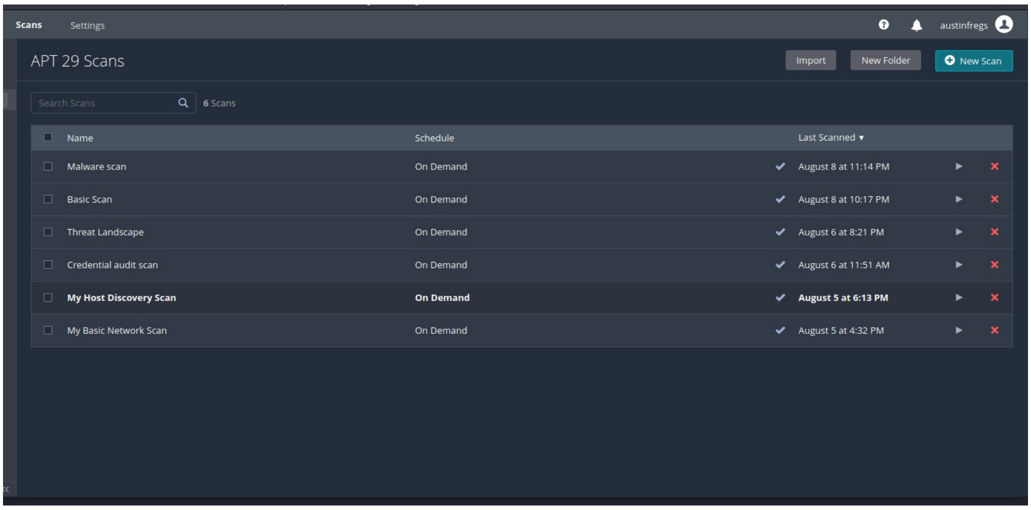
The next pivotal step involves leveraging Nessus for methodical vulnerability assessment within the cloud environment. Nessus is meticulously installed and configured, providing a powerful vulnerability assessment tool capable of identifying potential weak points across the cloud infrastructure. Nessus is initiated on the Linux instance as depicted in figure 24 to start the service



```
┌──(austin㉿Fregs)-[~/Downloads]
└─$ sudo service nessusd start
[sudo] password for austin:

┌──(austin㉿Fregs)-[~/Downloads]
└─$ sudo service nessusd status
● nessusd.service - The Nessus Vulnerability Scanner
     Loaded: loaded (/lib/systemd/system/nessusd.service; disabled; preset: disabled)
     Active: active (running) since Sat 2023-08-05 12:28:57 BST; 47s ago
   Main PID: 191004 (nessus-service)
      Tasks: 14 (limit: 2235)
     Memory: 118.0M
        CPU: 42.398s
     CGroup: /system.slice/nessusd.service
             ├─191004 /opt/nessus/sbin/nessus-service -q
             └─191006 nessusd -q

Aug 05 12:28:57 Fregs systemd[1]: Started The Nessus Vulnerability Scanner.
Aug 05 12:29:00 Fregs nessus-service[191006]: Cached 0 plugin libs in 0msec
Aug 05 12:29:00 Fregs nessus-service[191006]: Cached 0 plugin libs in 0msec
```

Figure 24 Starting Nessus Service

With Nessus in operation, a series of systematic vulnerability scans are conducted as illustrated in figure 25. These scans traverse the cloud environment, meticulously probing for potential vulnerabilities in network configurations, applications, and system components.



APT 29 Scans

6 Scans

□	Name	Schedule		Last Scanned ▾		
□	Malware scan	On Demand	✓	August 8 at 11:14 PM	▶	✕
□	Basic Scan	On Demand	✓	August 8 at 10:17 PM	▶	✕
□	Threat Landscape	On Demand	✓	August 6 at 8:21 PM	▶	✕
□	Credential audit scan	On Demand	✓	August 6 at 11:51 AM	▶	✕
□	**My Host Discovery Scan**	**On Demand**	✓	**August 5 at 6:13 PM**	▶	✕
□	My Basic Network Scan	On Demand	✓	August 5 at 4:32 PM	▶	✕

Figure 25 Scans on Nessus

The expert version of Nessus is employed for this experiment to enable a wide range of scans to detect extensive varieties of vulnerabilities and provide invaluable insight into the cloud environment's susceptibility to potential attacks. Vulnerabilities are highlighted, categorized, and prioritized, enabling security teams to focus their efforts on addressing the most critical issues first. Incorporating Snort's vigilant intrusion detection capabilities and leveraging Nessus's systematic vulnerability assessments, the APT29 emulation venture attains an augmented ability to anticipate, detect, and respond to potential threats. The synergy of these components contributes to a holistic understanding of the cloud environment's security posture and further enriches the emulation's depth and effectiveness.

4.6 Summary

This section provided a detailed walkthrough of how an APT adversary emulation plan is implemented within a cloud environment. It provides a comprehensive overview of the steps taken to design, implement, and execute an APT adversary emulation operation within a cloud environment, utilizing tools like MITRE Caldera, Snort, and Nessus to enhance detection and response capabilities. The goal is to analyse the consequences of a successful attack, assess the environment's security posture and improve its ability to detect APT-like threats.

5.0 RESULTS AND DISCUSSION

While emulating an APT29 attack via the Mitre Caldera framework, the emulation process demonstrated a commendable degree of proficiency in replicating a substantive portion of the outlined attack stages detailed in the emulation plan. While the foundational architecture adhered rigorously to the prescribed configuration parameters articulated within the emulation library, prudent adjustments were requisite to facilitate the seamless execution of discrete facets of the emulation blueprint. These deliberate adaptations served as pivotal measures to surmount challenges encountered during the enactment of the simulated attack scenario.

5.1 APT29 Emulation Results

The successful emulation of the APT29 attack encompassed a meticulously choreographed series of orchestrated steps, each constituting an essential building block in the unfolding of the attack sequence. Certain steps were contingent upon the assimilation of insights garnered from antecedent actions, encompassing aspects such as thorough host and network reconnaissance, coupled with the discernment of administrative user designations. Additionally, the efficacious implementation of specific phases hinged upon the precise and sequential completion of preceding actions, a salient instance being the establishment of enduring access prior to initiating a system-wide reboot.

Despite achieving an overall successful emulation, certain challenges emerged during the exercise that highlighted the intricate dependencies between different attack phases. These challenges were particularly noticeable, emphasizing the complex interconnections that stem from earlier stages of the attack. This interplay became evident through a ripple effect, where executing specific actions relied on successfully completing preceding steps, creating a sophisticated web of interactions in the simulated attack scenario. An interesting observation relates to how files were managed within the simulated environment. Specifically, when a designated file was already present in the specified location, CALDERA demonstrated its ability to smoothly incorporate the malicious payload into the existing file. This flexibility underscores CALDERA's adaptability to scenarios where threat actors manipulate existing files to advance their hidden agendas.

It is also important to note that CALDERA encountered difficulties in effectively triggering the established persistence mechanisms. These mechanisms were designed to activate upon rebooting the victim machine. However, after a reboot, the CALDERA agent failed to communicate with the server, leading the server to prematurely terminate the emulation, assuming agent failure. These challenges persisted even when attempting manual activation of the persistence mechanisms. Consequently, the directive to reboot the victim machine was entirely removed from the emulation plan. After making these adjustments, the emulation demonstrated comprehensive execution, showing an acceptable ratio of successful operations, as reported by CALDERA.

The CALDERA emulation displayed commendable accuracy in replicating a wide array of tactics and techniques employed by APT 29. Table 3 outlines the tactics and techniques implemented in this simulation, this includes data collection, command-and-control, credential access, defence evasion, discovery, execution, exfiltration, lateral movement, multiple tactics, and privilege escalation.

Table 3 Tactics and techniques

Tactics	Techniques	Abilities
Collection	T1005: Data from Local System T1560.001: Archive Collected Data: Archive via Utility T1115: Clipboard Data	Find files Compress Data for Exfiltration With Rar Copy Clipboard
Command-and-control	T1105: Ingress Tool Transfer	Curl Upload File
Credential-access	T1003: OS Credential Dumping T1552.004: Unsecured Credentials: Private Keys T1003.002: OS Credential Dumping: Security Account Manager T1003.001: OS Credential Dumping: LSASS Memory	Dump Credential Manager using keymgr.dll and rundll32.exe Find private keys Registry dump of SAM, creds, and secrets Credential Dumping with NPPSpy Create Mini Dump of LSASS.exe using ProcDump

Defense-evasion	T1036: Masquerading T1059.001: PowerShell T1112: Modify Registry T1070.004: Indicator Removal on Host: File Deletion T1070.006: Indicator Removal on Host: Timestomp	Malware Masquerading and Execution from Zip File Move Powershell & triage Modify Registry of Current User Profile - cmd Delete a single file - Windows cmd Delete a single file - Windows PowerShell Windows - Timestomp a File
Discovery	T1083: File and Directory Discovery T1016: System Network Configuration Discovery T1518.001: Software Discovery: Security Software Discovery T1518: Software Discovery T1082: System Information Discovery T1033: System Owner/User Discovery T1057: Process Discovery T1018: Remote System Discovery	File and Directory Discovery (PowerShell) System Network Configuration Discovery on Windows Discover antivirus programs Applications Installed System Information Discovery with WMIC Find Domain Current User System processes Discover domain controller
Execution	T1204.002: User Execution: Malicious File T1569.002: System Services: Service Execution	OSTap Payload Download Use PsExec to execute a command on a remote host Execute a Command as a Service LNK Payload Download
Exfiltration	T1041: Exfiltration Over C2 Channel T1048: Exfiltration Over Alternative Protocol	C2 Data Exfiltration DNSExfiltration (doh)
Lateral movement	T1021.006: Remote Services: Windows Remote Management	Enable Windows Remote Management

Multiple	T1543.003: Create or Modify System Process: Windows Service T1547.001: Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder T1546.003: Event Triggered Execution: Windows Management Instrumentation Event Subscription	Service Installation CMD Modify BootExecute Value Windows MOFComp.exe Load MOF File
Privilege-escalation	T1548.002: Abuse Elevation Control Mechanism: Bypass User Access Control	Bypass UAC Medium

The framework's success in simulating these actions is indicative of its efficacy in modelling complex attack scenarios. However, the emulation's limitations are notable in certain areas, such as unsuccessful execution or complete skipping of tactics. For instance, the framework struggled with certain aspects of persistence, lateral movement, and exfiltration. These limitations could arise from the intricacies of emulating advanced tactics, the constraints of the emulation environment, or the need for further calibration of the framework.

The graph in figure 26 underscores the intricate nature of the CALDERA simulation in emulating an APT attack, revealing a mixed array of successful executions, failures, and instances where operations were entirely skipped. These outcomes shed light on both the capabilities and limitations of the simulation framework, prompting a critical analysis of the simulation's fidelity and its implications for understanding APT attack behaviours.

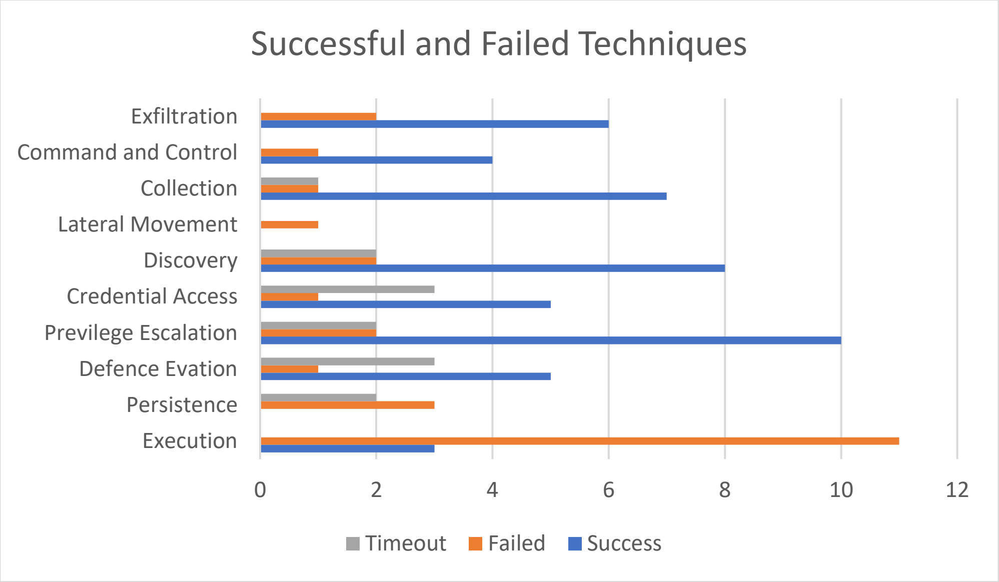


Figure 26 Successful and failed techniques from Caldera

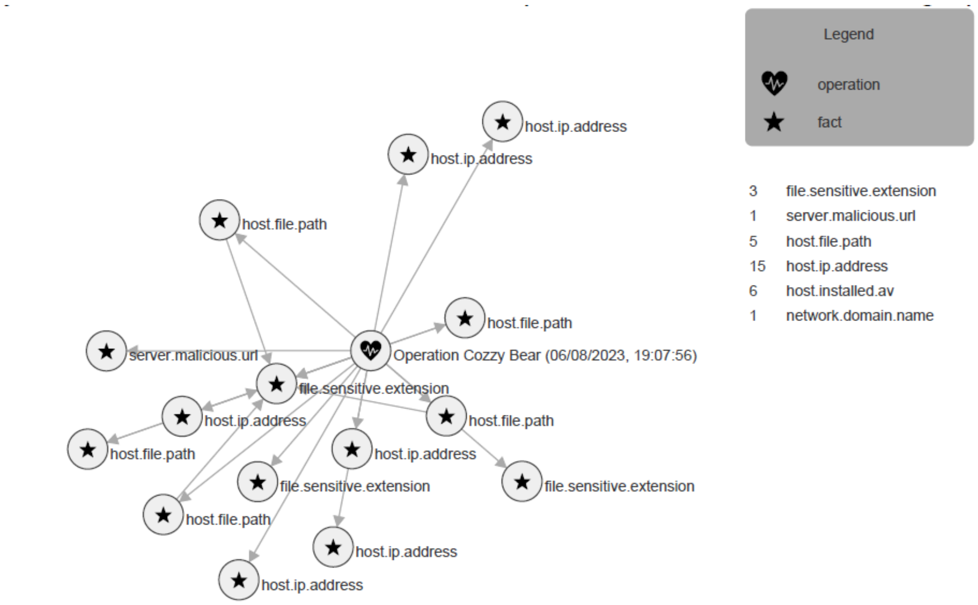
The success rates across different technique categories reveal notable disparities. For instance, techniques related to Privilege Escalation and Execution demonstrate a relatively higher success rate, with 10 and 3 successful executions, respectively. In contrast, Persistence techniques were either entirely skipped or faced failure, indicating potential challenges in accurately simulating these intricate phases of an APT attack.

A closer examination of individual technique categories reveals intriguing dynamics. Defence Evasion, while demonstrating a respectable success rate of 5, is accompanied by a concerning failure rate of 1 and 3 instances of timeouts. This blend of outcomes suggests that while CALDERA successfully evaded certain defences, it encountered hurdles in other instances, hinting at the complexity of evading diverse security measures. Similarly, Credential Access techniques exhibited a relatively balanced success and failure rate, each accounting for 5 and 1, respectively, accompanied by 3 timeouts. This nuanced distribution of outcomes reflects the intricacies associated with accessing credentials within a simulated attack context.

The outcomes pertaining to Lateral Movement and Exfiltration techniques raise intriguing questions. The fact that Lateral Movement operations were entirely skipped suggests a potential limitation in CALDERA's emulation capabilities in this specific area. On the other hand, Exfiltration techniques displayed a comparatively higher success rate of 6 but were also plagued by 2 instances of failure. The absence of a clear indication for the reasons behind the skipping of Lateral Movement techniques and the mixed outcomes in Exfiltration further underscore the complexity of these aspects within APT attack simulations**.**

5.1.1 Facts Discovered

The facts graph in figure 27 outlines the information extracted during the operation, including the executed command and the associated agent responsible for discovering the information. Each fact, by default, is assigned a score of 1. Should a specific fact, such as host.user.password, hold significant relevance or a heightened probability of success when utilized, there is an option to allocate a score of 5 to it. When abilities require facts to populate variables, those with the highest scores will be prioritized for use. Notably, a fact bearing a score of 0 is deemed blacklisted, rendering it ineligible for utilization within an operation.



3	file.sensitive.extension
1	server.malicious.url
5	host.file.path
15	host.ip.address
6	host.installed.av
1	network.domain.name

Figure 27 Facts Graph

The chart in figure 28 further presents a snapshot of the counts for various traits extracted during the operation. These traits encompass details related to host IP addresses, installed antivirus software, file paths, sensitive file extensions, malicious URLs, and network domain names. The analysis indicates the frequency of each trait, providing insights into the prevalence and distribution of these attributes within the operation's scope.

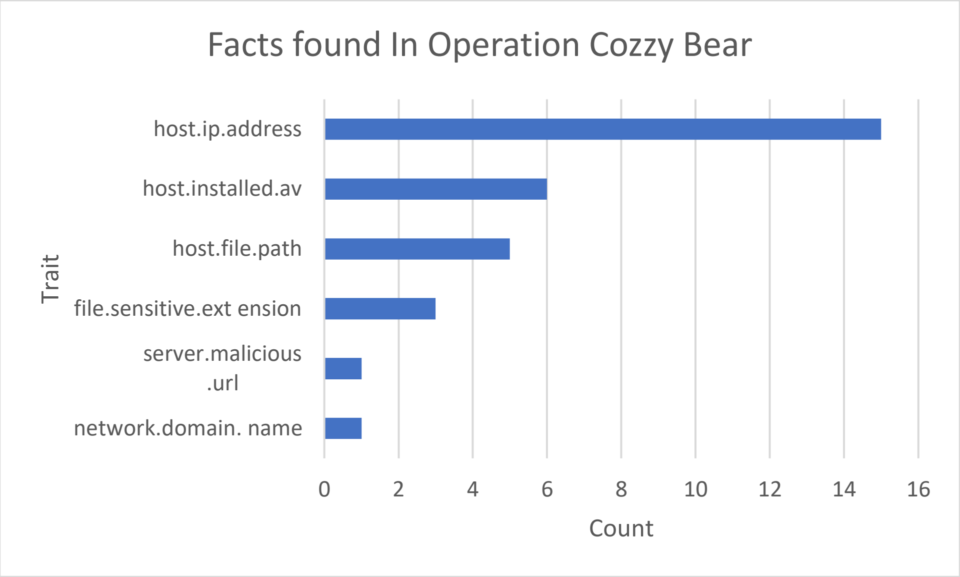
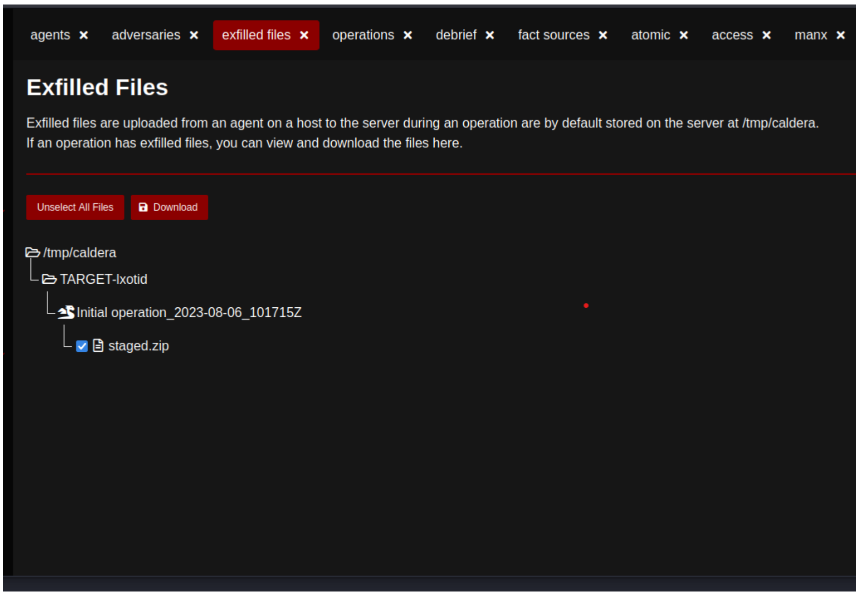


Figure 28 Traits of facts found.

The dataset produced by the facts found offers a comprehensive view of the simulated APT29 attack conducted within the CALDERA framework. It presents a breakdown of acquired traits, wherein each fact serves as a distinct identifier of specific aspects related to the attack scenario. Notably, the observation of host IP addresses (15 instances) suggests a strategic engagement with multiple host systems, possibly indicating reconnaissance or lateral movement strategies. Additionally, the presence of installed antivirus software (6 instances) signifies a consideration of defensive measures, potentially indicating an attempt to circumvent security protocols. Moreover, the identification of file paths (5 instances) highlights a focus on file manipulation, while the recognition of sensitive file extensions (3 instances) hints at the targeting of valuable data. The solitary instance of a malicious server URL denotes potential external communication, potentially indicative of command-and-control activities. The inclusion of a network domain name (1 instance) implies engagement with specific network domains.

This diverse array of traits, culminating in a total of 31 facts, offers valuable insights into the simulation's complexity and fidelity. By capturing multifaceted aspects such as IP addresses, antivirus presence, file paths, and more, this data enriches the understanding of the simulated APT29 attack's scope and authenticity. It provides a foundation for informed assessments of the simulation's alignment with real-world APT29 behaviours, enabling a deeper analysis of its effectiveness and potential for accurately replicating sophisticated attack scenarios. Figure 29 shows Exfiltration of some files were successful indicating the APT29 emulation completed its lifecycle and data espionage was indeed successful.



Exfilled Files

Exfilled files are uploaded from an agent on a host to the server during an operation are by default stored on the server at /tmp/caldera.
If an operation has exfilled files, you can view and download the files here.

```
/tmp/caldera
└ TARGET-lxotid
  └ Initial operation_2023-08-06_101715Z
    └ ☑ staged.zip
```

Figure 29 Exfiltrated Files

5.2 Caldera as a Framework

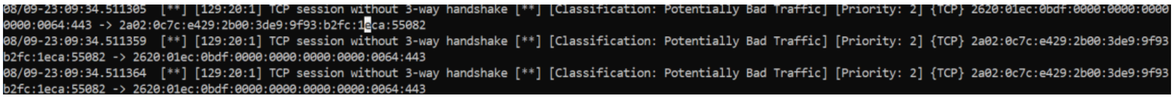
The central focus of CALDERA's design revolves around autonomous simulations, manual engagements by red teams, and automated incident response. However, its original scope did not encompass capturing network traffic from simulated attacks or evaluating the target system's detection capabilities. Despite this initial focus, CALDERA has demonstrated competence in these aspects and shows promise for future expansion. CALDERA's intuitive autonomous features are supported by comprehensive documentation from MITRE, offering valuable insights into its framework. The tool facilitates tailored attack operations, enabling users to execute predefined adversary profiles reminiscent of APT29 or craft entirely new profiles. Moreover, CALDERA's compatibility with custom commands hints at its potential synergy with other frameworks for supplementary attacks. This adaptability positions CALDERA as a versatile foundational framework for a wide range of attack scenarios.

An analysis reveals a noticeable gap between the anticipated capabilities outlined in MITRE's EMU plans and the practical outcomes achieved. Although a majority of APT29 EMU plan attacks were initiated, a notable subset failed due to missing payloads or their omission from the EMU plan. The precise reasons behind these omissions remain unclear, with speculation suggesting that CALDERA's LAVA engine, responsible for prioritizing executions, may play a role. Numerous attack steps within the EMU plans hinged on the successful completion of preceding stages, relying on outputs or files generated by earlier actions. As a result, when the initial attack didn't succeed or was missed, it set off a chain reaction that affected what came after. The successful execution of APT29's plan for attacks mostly involved basic steps, often using short PowerShell commands. On the other hand, more complex attacks in the plan often failed because the harmful parts were missing.

5.3 Snort for Detecting APT29 Traffic

Snort was configured with predefined rules specifically tailored to identify APT29 attack patterns, deployed within the cloud environment to meticulously monitor network traffic and promptly recognize potential malicious activities. In the process of simulating APT29 attacks, Snort effectively identified a subset of the simulated attack techniques. The alerts triggered by Snort's detection mechanism were systematically categorized and meticulously analysed, considering their severity and alignment with APT29 tactics.

The absence of a proper 3-way handshake in TCP connections as revealed in figure 30, can indicate deviations from established network communication norms.



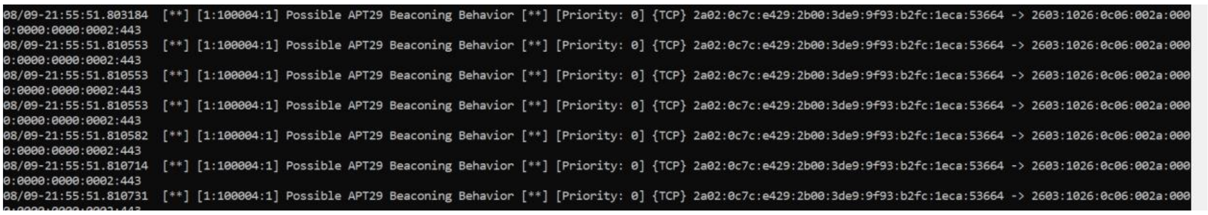
```
08/09-23:09:34.511305  [**] [129:20:1] TCP session without 3-way handshake [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 2620:01ec:0bdf:0000:0000:0000
0000:0064:443 -> 2a02:0c7c:e429:2b00:3de9:9f93:b2fc:1eca:55082
08/09-23:09:34.511359  [**] [129:20:1] TCP session without 3-way handshake [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 2a02:0c7c:e429:2b00:3de9:9f93
b2fc:1eca:55082 -> 2620:01ec:0bdf:0000:0000:0000:0000:0064:443
08/09-23:09:34.511364  [**] [129:20:1] TCP session without 3-way handshake [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 2a02:0c7c:e429:2b00:3de9:9f93
b2fc:1eca:55082 -> 2620:01ec:0bdf:0000:0000:0000:0000:0064:443
```

Figure 30 Session without 3-way handshake detected.

The 3-way handshake is a fundamental mechanism for ensuring reliable and synchronized connections. Its absence raises concerns about the integrity and legitimacy of the observed sessions. This could signify anomalies, misconfigurations, or potentially malicious attempts to evade detection, all of which are synonymous with the cozy bear tactics for defence evasion.

The outcomes of Snort's performance in detecting simulated APT29 attacks within the cloud environment were notably encouraging. The system adeptly identified some

APT29 beaconing behaviour as configured, in figure 31 an alert is generated in snort IDS. Throughout the evaluation, Snort showcased a remarkable ability to discern and flag distinct APT29 beaconing behaviours as they were configured for the test scenario. Beaconing behaviour, a characteristic of APT operations, involves periodic communications between compromised systems and command-and-control servers. By adeptly recognizing and alerting about these activities, Snort effectively contributes to the timely detection of potential threats. This event serves as a tangible demonstration of Snort's real-time monitoring capabilities, effectively translating detected threat indicators into actionable alerts for the security team.



```
08/09-21:55:51.803184  [**] [1:100004:1] Possible APT29 Beaconing Behavior [**] [Priority: 0] {TCP} 2a02:0c7c:e429:2b00:3de9:9f93:b2fc:1eca:53664 -> 2603:1026:0c06:002a:000
0:0000:0000:0002:443
08/09-21:55:51.810553  [**] [1:100004:1] Possible APT29 Beaconing Behavior [**] [Priority: 0] {TCP} 2a02:0c7c:e429:2b00:3de9:9f93:b2fc:1eca:53664 -> 2603:1026:0c06:002a:000
0:0000:0000:0002:443
08/09-21:55:51.810553  [**] [1:100004:1] Possible APT29 Beaconing Behavior [**] [Priority: 0] {TCP} 2a02:0c7c:e429:2b00:3de9:9f93:b2fc:1eca:53664 -> 2603:1026:0c06:002a:000
0:0000:0000:0002:443
08/09-21:55:51.810553  [**] [1:100004:1] Possible APT29 Beaconing Behavior [**] [Priority: 0] {TCP} 2a02:0c7c:e429:2b00:3de9:9f93:b2fc:1eca:53664 -> 2603:1026:0c06:002a:000
0:0000:0000:0002:443
08/09-21:55:51.810582  [**] [1:100004:1] Possible APT29 Beaconing Behavior [**] [Priority: 0] {TCP} 2a02:0c7c:e429:2b00:3de9:9f93:b2fc:1eca:53664 -> 2603:1026:0c06:002a:000
0:0000:0000:0002:443
08/09-21:55:51.810714  [**] [1:100004:1] Possible APT29 Beaconing Behavior [**] [Priority: 0] {TCP} 2a02:0c7c:e429:2b00:3de9:9f93:b2fc:1eca:53664 -> 2603:1026:0c06:002a:000
0:0000:0000:0002:443
08/09-21:55:51.810731  [**] [1:100004:1] Possible APT29 Beaconing Behavior [**] [Priority: 0] {TCP} 2a02:0c7c:e429:2b00:3de9:9f93:b2fc:1eca:53664 -> 2603:1026:0c06:002a:000
0:0000:0000:0002:443
```

Figure 31 APT29 traffic detected.

These findings underscore the significance of integrating intrusion detection systems like Snort into cloud environments, as they play a pivotal role in bolstering the overall security stance and mitigating the inherent risks associated with Advanced Persistent Threats. The potential for further research and the fine-tuning of detection rules holds promise in augmenting Snort's capability to discern even more intricate APT attack methods, thereby providing an elevated level of safeguarding for cloud-based systems.

5.4 Nessus Vulnerability Scan

The Nessus vulnerability scan successfully identified critical, high, medium, and informative vulnerabilities within the network. It highlighted potential avenues for exploitation that could be leveraged by advanced threat actors like APT29. The insights gained from this assessment are crucial for implementing effective mitigation measures, enhancing network defences, and safeguarding against potential APT attacks.

5.4.1 Basic Vulnerability Scan

The first scan was executed as a "Basic Network Scan" using Nessus scanner. The assessment was comprehensive and concluded within a timeframe of approximately 30 minutes. The primary focus of the scan was to identify vulnerabilities utilizing the

Common Vulnerability Scoring System (CVSS) version 3.0 for precise severity assessment. The scan was initiated and successfully concluded on the same day, commencing at 9:47 PM and concluding at 10:17 PM.

A comprehensive scan using Nessus expert was conducted as depicted in figure 32, yielding a total of 244 vulnerabilities detected across the target environment. The vulnerabilities were categorized by their severity levels: 25 critical, 20 high, 4 medium, and 195 informative. This report details the findings and their potential implications for the security of the network.

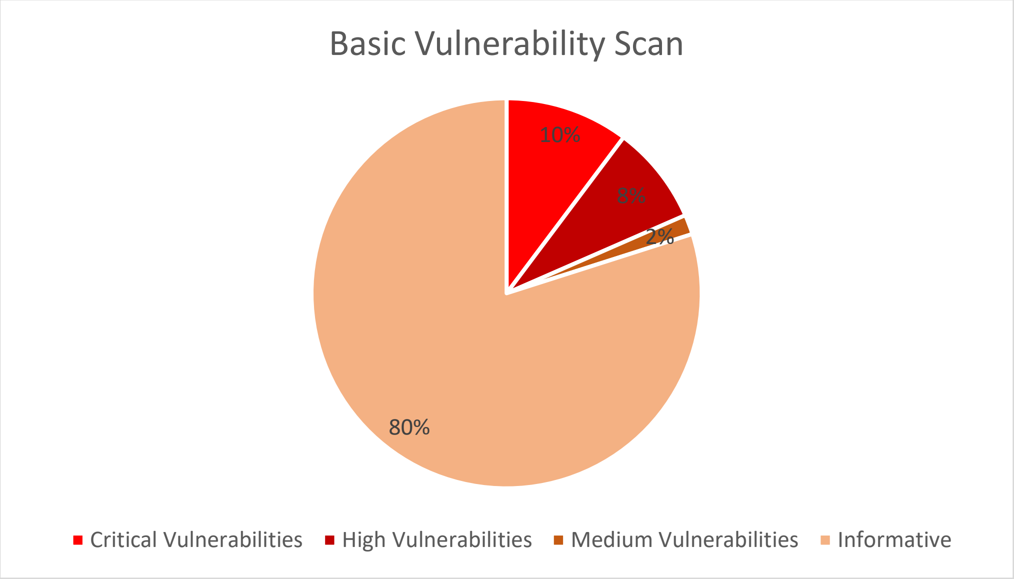
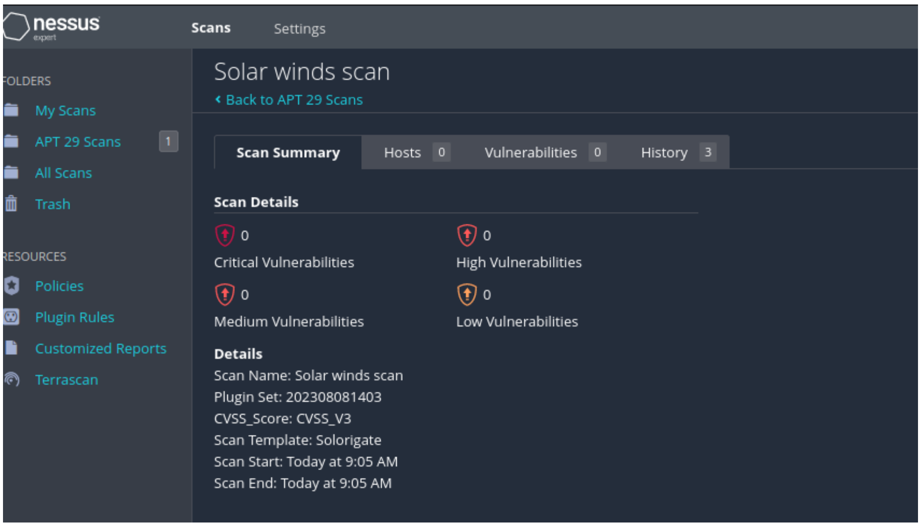


Figure 32 Basic Nessus Vulnerability Scan

The scan outcomes present a comprehensive overview of the vulnerabilities that exist within the network infrastructure. The provided data offers valuable insights into the security posture of the systems, enabling informed decision-making regarding necessary remediation measures.

5.4.2 Solar Winds Vulnerability Scan

The SolarWinds breach is credited to APT29, showcasing their adept use of cutting-edge and intricate strategies (Kunkle, 2021). This resourcefulness has complicated the identification process due to their deployment of less obvious techniques. The compromise of SolarWinds' Orion software served as an entry point, offering attackers a portal into victim networks. This enabled lateral movement and, potentially, the extraction of sensitive data. In response to the SolarWinds incident, Nessus has devised specialized scan checks tailored to spot signs of compromise stemming from the malicious Orion updates. These measures are aimed at detecting SolarWinds vulnerabilities connected to the Solorigate event. It's noteworthy that default paranoid checks are enabled, as certain checks may necessitate them to function properly.



Solar winds scan

Scan Details

0 Critical Vulnerabilities
0 High Vulnerabilities
0 Medium Vulnerabilities
0 Low Vulnerabilities

Details
Scan Name: Solar winds scan
Plugin Set: 202308081403
CVSS_Score: CVSS_V3
Scan Template: Solorigate
Scan Start: Today at 9:05 AM
Scan End: Today at 9:05 AM

Figure 33 Solar winds scan

Adopting a dedicated Nessus scan template aligned with the SolarWinds attack involves scrutinizing for indicators of compromise, such as malicious files, registry entries, network connections, or system artifacts linked to the SolarWinds backdoor. An important observation is that the default SolarWinds vulnerability scan with Nessus depicted in figure 33 yielded no vulnerabilities.

5.4.3 Identified Critical Vulnerabilities Exploitable by APT

The basic Nessus vulnerability scan unveiled a total of 25 critical vulnerabilities. Among these, four have been specifically pinpointed as exploitable using APT tactics and techniques. The specifics of the impact and tactics employed in exploiting these vulnerabilities are detailed in Table 4.

Table 4 Critical Vulnerabilities exploitable by APT

S/N	Vulnerability	Implication	APT Exploitation Tactics

I	Potential Exploitation of Software Vulnerabilities (KB5007189, KB4551762, KB5013945)	The identified software vulnerabilities, including KB5007189, KB4551762, and KB5013945, are susceptible to exploitation by sophisticated threat actors such as APT29. These actors often capitalize on well-known vulnerabilities to achieve unauthorized access to systems and networks	• Spear-phishing campaigns involving malicious attachments or links that trigger the vulnerabilities upon interaction. • Watering hole attacks by compromising legitimate websites to inject malicious code, thereby delivering exploits to unsuspecting users. • Utilizing exploit kits hosted on malicious websites to automatically disseminate exploit code to visitors' systems. • Exploiting the vulnerabilities as entry points for the delivery of malware after gaining initial access.
ii	Adobe Flash Player Vulnerability (APSB20-58)	The Adobe Flash Player vulnerability (APSB20-58) presents a potential avenue for APT29 to compromise systems with outdated versions of the software	• Drive-by downloads, wherein users are directed to malicious websites that automatically trigger downloads and exploit the vulnerability upon visiting. • Embedding exploit code within deceptive content, such as documents or multimedia files. • Leveraging email attachments that harbour malicious Flash content

			camouflaged as genuine attachments.
iii	Curl Use-After-Free Vulnerability (CVE-2022-43552)	The identified use-after-free vulnerability in Curl (CVE-2022-43552) could be exploited by APT29 to execute arbitrary code or achieve control over the targeted system	• Devising malicious input specifically designed to trigger the use-after-free condition, thereby executing malevolent code. • Engaging in supply chain attacks by injecting malicious code into the legitimate software development process reliant on Curl. • Exploiting dependencies on vulnerable Curl versions within software stacks of targeted systems.
iv	Microsoft Edge Vulnerabilities	The Microsoft Edge (Chromium) vulnerabilities serve as potential access points for APT29 to gain control over systems and access sensitive data.	• Directing users to malicious websites hosting exploit code through drive-by download tactics. • Developing malicious browser extensions that exploit vulnerabilities upon installation. • Distributing persuasive phishing emails to entice users into clicking on links leading to malicious websites.

5.5 Mitigation Strategies Against the Critical Vulnerabilities

I. Potential Exploitation of Software Vulnerabilities (KB5007189, KB4551762, KB5013945): The vulnerabilities (KB5007189, KB4551762, KB5013945) are real Windows Update patches.

a) Patch Management: Organizations should prioritize patch management to ensure systems are up to date with the latest security updates. Regularly monitor and apply patches from trusted sources.

b) Security Awareness: Conduct training for employees to recognize and report suspicious emails and links, reducing the effectiveness of spear-phishing campaigns.

c) Web Filtering: Employ web filtering solutions to block access to known malicious websites and prevent watering hole attacks.

d) Network Segmentation: Implement network segmentation to limit lateral movement in case an attacker gains access.

II. Adobe Flash Player Vulnerability (APSB20-58):

a) Flash Player Removal: Since Adobe Flash Player is no longer supported, organizations should completely remove it from their systems to eliminate this potential vulnerability.

b) Web Content Inspection: Implement content inspection mechanisms to detect and block malicious content, reducing the risk of drive-by downloads.

c) File Type Filtering: Configure email gateways and security solutions to block or scan files with Flash content.

d) Regular Updates: Maintain up-to-date software and applications to reduce the attack surface.

III. Curl Use-After-Free Vulnerability (CVE-2022-43552):

a) Vendor Patches: Apply vendor-supplied patches promptly to fix known vulnerabilities and protect against exploitation.

b) Code Review and Testing: Implement code reviews and security testing in the software development process to identify and address vulnerabilities early.

c) Dependency Management: Regularly update and audit dependencies in software stacks to prevent reliance on vulnerable components.

d) Zero-Trust Architecture: Implement a zero-trust approach to limit lateral movement and contain potential breaches.

IV. Microsoft Edge Vulnerabilities:

a) Browser Updates: Keep browsers up to date with the latest security patches and features.

b) Extension Review: Regularly review and audit browser extensions, removing any suspicious or unnecessary ones.

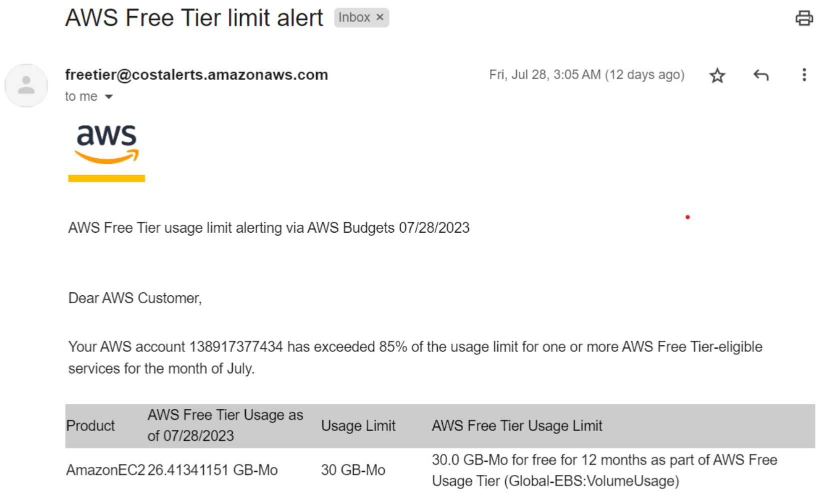
c) Security Configurations: Configure browser security settings to block potentially harmful content and prevent automatic downloads.

d) Multi-Factor Authentication: Implement multi-factor authentication to add an extra layer of security against phishing attacks.

5.6 Limitations

During the experimental phase, an effort was undertaken to create a Command and Control (C&C) connection. This was achieved by installing a CALDERA agent on the target system. However, Windows Defender promptly identified this activity on the victim VM, necessitating the deactivation of Windows Defender to establish both a foothold and C&C communication. Successful execution of CALDERA attacks mandated specific conditions, including the allowance of script execution through group policies and the deactivation of firewalls. While these settings may not be ideal in real-world scenarios, they could be applicable to certain organizations or users with elevated privileges. Notably, authentic environments may encounter variances and anomalies arising from the intricacies of contemporary networking. Elements such as delays in packet transmission caused by network congestion and unforeseen interruptions in connections, resets, or out-of-sequence packet arrivals can lead to fluctuations in actual network traffic. These variations, often absent in isolated or virtualized environments, underscore the challenge of replicating genuine network conditions. While acknowledging the absence of certain real-world intricacies, it's important to recognize that the primary focus of this experimentation was to analyse the impact of these threats on cloud environment, rather than striving for absolute realism in the experimental environment.

Another challenge worthy of note shown is the storage space limitations encountered while setting up dependencies and software configurations significant to this experiment, this is revealed in figure 34. While the kali Linux OS was more up to date with certain dependencies like Python, a single command "Sudo apt upgrade" installed most of the dependencies needed. However, this was not the case for the Windows OS. Dependencies like Python, Microsoft visual c++ redistributable, visual studio, and .Net all needed to be installed resulting in the depletion of storage space. This was resolved by removing apps and software not crucial to this project and subsequently purchasing extra storage.



AWS Free Tier limit alert

freetier@costalerts.amazonaws.com
to me

Fri, Jul 28, 3:05 AM (12 days ago)

AWS Free Tier usage limit alerting via AWS Budgets 07/28/2023

Dear AWS Customer,

Your AWS account 138917377434 has exceeded 85% of the usage limit for one or more AWS Free Tier-eligible services for the month of July.

Product	AWS Free Tier Usage as of 07/28/2023	Usage Limit	AWS Free Tier Usage Limit
AmazonEC2	26.41341151 GB-Mo	30 GB-Mo	30.0 GB-Mo for free for 12 months as part of AWS Free Usage Tier (Global-EBS:VolumeUsage)

Figure 34 Cloud storage limitation

5.7 Summary

Employing Snort for attack detection and Nessus for vulnerability scanning offers a superior approach compared to the methods mentioned in the reviewed literature. By capitalizing on real-time detection, proactive vulnerability assessment, and integrated analysis, this approach offers a robust methodology to mitigate risks and enhance overall security posture.

With regards to the research question “What is the impact of a successful Advanced persistent threat attack on cloud environment?” This thesis has demonstrated the severity of a successful APT attack and its impact on cloud environment using Caldera and its Emu plans. Sensitive files were successfully exfiltrated which ultimately leads to reputational damage and eroding client trust and relationships. The results from Nessus scans also addressed another research question “What are the vulnerabilities and potential attack vectors in cloud infrastructures that make them susceptible to APT attacks?”, revealing critical vulnerabilities and how the threat actors can exploit them on our cloud environment.

6.0 CONCLUSION AND RECOMMENDATION

This thesis embarked on a comprehensive investigation into Advanced Persistent Threats within cloud environments, delving into their inherent nature and the resultant implications for cloud security. Through detailed analysis, the strengths and weaknesses of existing approaches aimed at countering APT activities in cloud environments were critically examined, shedding light on the evolving challenges faced by organizations in safeguarding their cloud infrastructure. The use of Mitre Caldera for simulation was pivotal in this study, offering insights into APT attacks. 31 traits were identified, revealing the simulation's accuracy in mirroring real APT29 attacks. This data helped assess alignment with APT29 behaviours, enabling analysis of its effectiveness. The Nessus vulnerability tool highlighted network vulnerabilities exploitable by an APT, while Snort detected APT29 traffic. These insights improved understanding of system security, informing remediation decisions.

Comparatively, the utilization of Snort for attack detection and Nessus for vulnerability scanning presents a more advanced approach compared to the methodologies discussed in the reviewed literature. While the amalgamation of network and host datasets, as proposed by Gjerstad (2022), offers valuable insights, the incorporation of Snort's real-time intrusion detection capabilities enhances the proactive identification of APT29 attacks, allowing for swift responses. Furthermore, Nessus' comprehensive vulnerability scanning augments the dataset by pinpointing potential weaknesses in both network and host configurations, presenting a holistic view of security gaps. This dynamic synergy empowers a more robust and pre-emptive defence strategy, enriching the dataset's depth and bolstering the overall effectiveness of APT detection and mitigation endeavours.

The collective findings of this research underscore the intricate interplay between APT activities and cloud environments, highlighting the critical need for robust detection and mitigation strategies. The synthesis of APT simulation, vulnerability assessment, and analysis of detection measures has yielded valuable insights into the evolving threat landscape within cloud ecosystems. As organizations continue to leverage cloud technologies, the lessons derived from this study contribute to the ongoing discourse on fortifying cloud security against the backdrop of persistent and evolving cyber threats.

6.1 Recommendations

Based on the research findings presented in this thesis, several recommendations can be proposed to enhance cloud security and effectively counter Advanced Persistent Threats within cloud environments:

- Robust Detection Strategies: Given the evolving nature of APTs and their potential impact on cloud environments, organizations should prioritize the implementation of robust detection mechanisms. The integration of real-time intrusion detection systems like Snort enhances the capability to promptly identify and respond to APT activities, reducing the dwell time of attackers within the cloud ecosystem. Also, Integration of APT detection with the organization's incident response plan. Detection alerts should trigger a well-defined set of actions for investigating and mitigating potential APT activities.

- Comprehensive Security Architecture: Establish a comprehensive security architecture tailored to cloud environments. This architecture should encompass network segmentation, endpoint protection, intrusion detection systems, and security information and event management (SIEM) solutions. Implementing a defence-in-depth approach fortifies the cloud environment against various attack vectors. Such an architecture encompasses multiple layers of defence, combining various security solutions and strategies to create a resilient and adaptable defence framework.

- User Training and Awareness: Foster a security-aware culture by conducting regular training and awareness programs. Ensure that employees, from end-users to IT personnel, are educated about APTs, their tactics, and the significance of adhering to security best practices. Educate employees about APT risks, social engineering tactics, and safe browsing habits. Encourage prompt reporting of suspicious activities, enabling quick responses to potential threats.

- Collaborative Cloud Provider Engagement: Foster collaboration with industry peers and security communities to share threat intelligence and insights about APT activities. Collaborative efforts can help organizations stay informed about emerging threats and benefit from collective knowledge. Collaborate closely with cloud service providers to leverage their expertise and tools. Engage in joint threat intelligence sharing and incident response planning. Ensure that cloud providers align their security measures with your organization's requirements, enhancing the overall defence posture.

- Regular Red Teaming Exercises: Conduct regular red teaming exercises to simulate APT-like attacks within the cloud environment. These exercises help identify vulnerabilities and weaknesses in security controls, enabling proactive mitigation before actual adversaries exploit them. Continued use of APT emulation and simulation tools, like Mitre Caldera, proves invaluable for understanding APT attack behaviours and refining detection strategies. Regularly updating and expanding the emulation scenarios will enable organizations to stay ahead of emerging threats and adapt their defences accordingly.

6.2 Future Works

Drawing upon the findings of the conducted experiments within this thesis and their ensuing outcomes, numerous promising avenues for future research have come to light. While this investigation has provided valuable insights into the realm of APTs within cloud environments and the associated strategies for mitigation, there exist several untapped opportunities for further inquiry and scholarly exploration. These opportunities aim to bolster the comprehension of these dynamic threats and foster more robust countermeasures in response.

- Behavioural Analytics and Machine Learning Integration: One potential direction for future exploration involves delving into the integration of advanced behavioural analytics and cutting-edge machine learning algorithms. This endeavour seeks to amplify the efficacy of APT detection within cloud environments. The aspiration is to cultivate models capable of discerning irregular user behaviours, unravelling intricate network traffic patterns, and unveiling system activities that serve as telltale signs of APT incursions.
- Dynamic Sharing of Threat Intelligence: A promising realm ripe for future investigation entails the establishment of dynamic platforms for the sharing of threat intelligence. Collaboration among diverse stakeholders, including cloud service providers, organizations, and cybersecurity entities, becomes the focal point. By engineering mechanisms that facilitate real-time exchange of APT-

centric indicators, tactics, techniques, and procedures (TTPs), the overarching aim is to speed up detection and response.

- Advancement of Automated Incident Response Frameworks: The evolution of automated incident response frameworks stands as a significant area worthy of future exploration. This involves the development of frameworks with the capacity to instantaneously identify and counter APT activities in real time. The fusion of threat intelligence feeds, automated orchestration, and comprehensive response playbooks is envisioned to constitute a formidable mechanism for the rapid neutralization of APT threats, obviating the need for manual intervention.

6.3 Contribution to Knowledge

This study has contributed valuable insights to the realm of cloud security and APT mitigation. The findings underscore the evolving tactics employed by APT groups in cloud environments, necessitating a shift in security paradigms. The analysis of current approaches has highlighted the need for continuous innovation and adaptation to counter emerging APT threats. The integration of simulation techniques, vulnerability assessments, and detection strategies has yielded a holistic perspective on APT activities, enriching the body of knowledge surrounding cloud security.

In addition, the study underscores the significance of addressing APT risks in cloud environments, given the increasing adoption of cloud technologies. It underscores the importance of staying abreast of evolving attack methodologies and the imperative of collaborative efforts among stakeholders to effectively thwart APT activities.

6.4 Personal Reflection

Throughout this research journey, delving into the complex landscape of APT threats in cloud environments has been enlightening and intellectually stimulating. The process of simulating APT attacks using Mitre Caldera provided practical insights into the intricacies of adversary behaviours and tactics. The experience of vulnerability scanning using Nessus highlighted the dynamic nature of system vulnerabilities that could be exploited in this attack.

My journey with this thesis commenced with an exploration of emerging threats to data centres. Following an in-depth literature review and insightful discussions with my supervisor, I found myself grappling with the task of formulating a practical methodology for the project. Fortunately, my supervisor's weekly guidance steered me towards a promising path: selecting a single emerging threat and broadening my scope to the cloud. This redirection led me to delve deeper into the realm of advanced persistent threats, a concept I had heard of but had limited knowledge about. In the pursuit of a more objective approach to my methodology, my attention turned to the exploration of simulation tools. Among these, the discovery of Caldera stood out as a significant turning point. My engagement with Caldera was a truly captivating learning experience, one that expanded my horizons. In a bid to learn more about APTs and how they affect they affect organizations, I connected with two cloud security experts on LinkedIn who were very helpful, I also explored resources like Mitre ATT&CK platform, CTID (Centre for Threat Informed Defence).

As a researcher, I have gained a deeper appreciation for the intricate interplay between cloud technologies and cybersecurity. This study has reinforced the significance of continuous learning and adaptability in the face of ever-evolving cyber threats. It has also fostered a sense of responsibility to contribute to the collective efforts aimed at fortifying cloud security and safeguarding critical digital assets. Reflecting upon these experiences, I am profoundly grateful for embarking on this project. The past two months alone have been an extraordinary journey of discovery and growth. They have solidified my belief that with determination, I can master any subject I set my mind to learn.

REFERENCES

Adelaiye, O. I., Showole, A., and Faki, S. A. (2018) Evaluating advanced persistent threats mitigation effects: a review. *International Journal of Information Security Science*, *7*(4), 159-171.

Applebaum, A., Miller, D., Strom, B., Korban, C., and Wolf, R. (2016) Intelligent, automated red team emulation. In *Proceedings of the 32nd Annual Conference on Computer Security Applications* (pp. 363-373).

ATT&CK Evaluations (2019) Apt29 Enterprise Evaluation 2019, [Online]. Available: https://attackevals.mitre-engenuity.org/enterprise/apt29. [Accessed: June 19, 2023].

Baker, P. (2021) "The SolarWinds hack timeline: Who knew what, and when?" CSO [Online] Available at: https://www.csoonline.com/article/3613571/the-solarwinds-hacktimeline-who-knew-what-and-when.html [Accessed 18 July 2023].

Buyya, R., Broberg, J., and Goscinski, A. M. (Eds.). (2010) *Cloud computing: Principles and paradigms*. John Wiley & Sons.

Centre for Threat-Informed Defence (2021) Adversary Emulation Library: APT29. [Online]. Available from https://github.com/center-for-threat-informed-defense/adversary_emulation_library/tree/1545d37768122082c4b474bf74c96db4b3 8d5dab/apt29s [Accessed 8 July 2023]

Chen, J., Su, C., Yeh, K. H., and Yung, M. (2018) Special issue on advanced persistent threat. *Future Generation Computer Systems*, *79*, 243-246.

Cole, E. (2013) Advanced Persistent Threat: Understanding the Danger and How to Protect Your Organization. Syngress.

Durojaye, H., and Raji, O. (2022) Impact of State and State Sponsored Actors on the Cyber Environment and the Future of Critical Infrastructure. *arXiv preprint arXiv:2212.08036*.

Ghafir, I. (2017) *A machine-learning-based system for real-time advanced persistent threat detection and prediction*.

Gjerstad, J. L. (2022) *Generating labelled network datasets of APT with the MITRE CALDERA framework*. MSc. University of Oslo.

Halabi, T. Wahab, O. A., R. Al Mallah, and M. Zulkernine. (2021) Protecting the Internet of Vehicles Against Advanced Persistent Threats: A Bayesian Stackelberg Game. *IEEE Transactions on Reliability* 70(3), 970.

Hejase, H. J., Fayyad-Kazan, H. F., and Moukadem, I. (2020) Advanced persistent threats (apt): an awareness review. *Journal of Economics and Economic Education Research*, *21*(6), 1-8.

Hudson, B. (2014) Advanced persistent threats: Detection, protection, and prevention. *Sophos Ltd*.

ImmuniWeb. (2023) Top 10 Cloud Security Incidents in 2022. [Online]. Available from: https://www.immuniweb.com/blog/top-10-cloud-security-incidents-in-2022.html (Accessed: 1 July 2023).

Kadiric, F. (2022) *APT attack emulation and data labelling.* MSc. University of Oslo.

Kandukuri, S., Divya, B., Rajesh, C., and Shiva, J. (2018) A Survey Paper on APT (Advanced Persistent Threat) in Cloud Security. International Journal of Computer Science & Programming languages, 4(1), 8-11.

Karabacak, B., and Tatar, Ü. (2014) Strategies to Counter Cyberattacks: Cyberthreats and Critical Infrastructure Protection. *Critical Infrastructure Protection*, *116*, 63.

Karabacak, B., and Whittaker, T. (2022) Zero Trust and Advanced Persistent Threats: Who Will Win the War? In *International Conference on Cyber Warfare and Security* (Vol. 17, No. 1, pp. 92-101)

Karantzas, G., and Patsakis, C. (2021) An empirical assessment of endpoint detection and response systems against advanced persistent threats attack vectors. *Journal of Cybersecurity and Privacy*, *1*(3), 387-421.

Khaleefa, E. J., and Abdulah, D. A. (2022) Concept and difficulties of advanced persistent threats (APT): Survey. *International Journal of Nonlinear Analysis and Applications*, *13*(1), 4037-4052.

Khan, S., Nicho, M., and Takruri, H. (2016) IT controls in the public cloud: Success factors for allocation of roles and responsibilities. *Journal of information technology case and application research*, *18*(3), 155-180.

Kumar, R., Kela, R., Singh, S., and Trujillo-Rasua, R. (2022) APT attacks on industrial control systems: A tale of three incidents. *International Journal of Critical Infrastructure Protection*, *37*, 100521.

Kunkle, Z. (2021) *APTs attributed to Russia and their contributions to Russian policies.* MSc. Utica College.

Li, M., Huang, W., Wang, Y., Fan, W., and Li, J. (2016) The study of APT attack stage model. In *2016 IEEE/ACIS 15th International Conference on Computer and Information Science (ICIS)* (pp. 1-5). IEEE.

Li, Y., Zhang, T., Li, X., and Li, T. (2019) A model of APT attack defense based on cyber threat detection. In *Cyber Security: 15th International Annual Conference, CNCERT 2018, Beijing, China, August 14–16, 2018, Revised Selected Papers 15* (pp. 122-135). Springer Singapore.

Mendez Mena, D., Papapanagiotou, I., and Yang, B. (2018) Internet of things: Survey on security. *Information Security Journal: A Global Perspective*, *27*(3), 162-182.

Messaoud, B. I., Guennoun, K., Wahbi, M., and Sadik, M. (2016) Advanced persistent threat: New analysis driven by life cycle phases and their challenges. In *2016 International conference on advanced communication systems and information security (ACOSIS)* (pp. 1-6). IEEE.

Min, M., Xiao, L., Xie, C., Hajimirsadeghi, M., and Mandayam, N. B. (2018) Defense against advanced persistent threats in dynamic cloud storage: A colonel blotto game approach. *IEEE Internet of Things Journal*, *5*(6), 4250-4261.

MITRE (2021) 'APT29 Attack Navigator'. [Online] Available from: https://mitre-attack.github.io/attacknavigator//#layerURL=https://attack.mitre.org [Accessed 11 June 2023]

Mohamed, N. A., Jantan, A., and Abiodun, O. I. (2018) An improved behaviour specification to stop advanced persistent threat on governments and organizations network. In *proceedings of the International MultiConference of Engineers and Computer Scientists* (Vol. 1, pp. 14-16).

Moon, D., Im, H., Lee, J. D., and Park, J. H. (2014). MLDS: multi-layer defence system for preventing advanced persistent threats. *Symmetry*, *6*(4), 997-1010.

NIST. (2017). Managing Information Security Risk Organization, Mission, and Information System View [Online]. US Department of Commerce. Available: http://bit.ly/2iPT4qI [Accessed 5th May, 2023].

Oladimeji, S. and Kerner, S. M. (2022) "Solarwinds Hack explained: Everything you need to know: TechTarget," WhatIs.com. [Online] Available from: https://www.techtarget.com/whatis/feature/SolarWinds-hackexplained-Everything-you-need-to-know. [Accessed 1 June 2023].

Osborne, C. (2022). Chinese hackers Deep Panda return with Log4Shell exploits, new Fire Chili rootkit. ZDNet, [Online]. Available from: https://www.zdnet.com/article/chinese-hackers-deep-panda-return-with-log4shell-exploits-new-fire-chili-rootkit/ [Accessed: 21 June 2023].

Quadri, A., & Khan, M. K. (2019). Cybersecurity Challenges of the Kingdom of Saudi Arabia.

Rouse, M (2020). Advanced Persistent Threat (APT). Tech Target. [Online] Available from https://searchsecurity.techtarget.com/definition/advanced-persistent-threat-APT Accessed [28 May, 2023]

Salim, D. T., Singh, M. M., & Keikhosrokiani, P. (2023). A systematic literature review for APT detection and effective cyber situational awareness (ECSA) conceptual model. *Heliyon*.

Singh, A. K., Koshy, A. S., & Gupta, M. (2023). Cloud Computing for Machine Learning and Cognitive Application. In *Cloud-based Intelligent Informative Engineering for Society 5.0* (pp. 107-121). Chapman and Hall/CRC.

Suryateja, P. S. (2018). Threats and vulnerabilities of cloud computing: a review. *International Journal of Computer Sciences and Engineering*, *6*(3), 297-302.

Taherdoost, H. (2022). Cybersecurity vs. Information Security. *Procedia Computer Science*, 215, 483-487.

Tatam, M., Shanmugam, B., Azam, S., & Kannoorpatti, K. (2021). A review of threat modelling approaches for APT-style attacks. *Heliyon*, *7*(1).

The MITRE Corporation. (2021). MITRE ATT&CK Matrix. [Online]. Available from: [https://attack.mitre.org/resources/updates/updates-october-2021]. Accessed [27 June, 2023].

Vance, A. (2014). Flow based analysis of Advanced Persistent Threats detecting targeted attacks in cloud computing. In *2014 First International Scientific-Practical Conference Problems of Infocommunications Science and Technology* (pp. 173-176). IEEE.

Wang X., Zheng, K., Xinxin N., Bin, W. and Wu, C. (2016) Detection of command and control in advanced persistent threat based on independent access. *IEEE International Conference on Communications* (ICC). IEEE.

Xiao, L., Xu, D., Xie, C., Mandayam, N. B., & Poor, H. V. (2017). Cloud storage defense against advanced persistent threats: A prospect theoretic study. *IEEE Journal on Selected Areas in Communications*, *35*(3), 534-544.

Xu, M., & Buyya, R. (2020). Managing renewable energy and carbon footprint in multi-cloud computing environments. *Journal of Parallel and Distributed Computing*, *135*, 191-202.

Zulkefli, Z., Singh, M. M., & Malim, N. H. A. H. (2015). Advanced persistent threat mitigation using multi-level security–access control framework. In *Computational Science and Its Applications--ICCSA 2015: 15th International Conference, Banff, AB, Canada, June 22-25, 2015, Proceedings, Part IV 15* (pp. 90-105). Springer International Publishing.

BIBLIOGRAPHY

Alert, C. I. S. A. (2020). Advanced persistent threat compromise of government agencies, critical infrastructure, and private sector organizations.

Bhadauria, R., & Sanyal, S. (2012). Survey on security issues in cloud computing and associated mitigation techniques. *arXiv preprint arXiv:1204.0764*.

Bronk, C., & Tikk-Ringas, E. (2013). Hack or attack? Shamoon and the Evolution of Cyber Conflict.

Ehrenfeld, J. M. (2017). Wannacry, cybersecurity and health information technology: A time to act. *Journal of medical systems*, *41*, 1-1.

Johnson, A. L. (2016). Cybersecurity for financial institutions: The integral role of information sharing in cyber-attack mitigation. NC Banking Inst., 20, 277.

Kandukuri, S., Divya, B., Rajesh, C., & Shiva, J. (2018). A Survey Paper on APT (Advanced Persistent Threat) in Cloud Security. *International Journal of Computer Science & Programming languages*, *4*(1), 8-11

Karabacak, B., & Whittaker, T. (2022, March). Zero Trust and Advanced Persistent Threats: Who Will Win the War?. In *International Conference on Cyber Warfare and Security* (Vol. 17, No. 1, pp. 92-101

Kinnunen, J. (2022). Threat Detection Gap Analysis Using MITRE ATT&CK Framework.

Messaoud, B. I., Guennoun, K., Wahbi, M., & Sadik, M. (2016, October). Advanced persistent threat: New analysis driven by life cycle phases and their challenges. In *2016 International conference on advanced communication systems and information security (ACOSIS)* (pp. 1-6). IEEE.

MITRE (2021) 'APT29 Attack Navigator'. [Online] Available from: https://mitre-attack.github.io/attacknavigator//#layerURL=https://attack.mitre.org [Accessed 11 June 2023]

Mitre (2019). Command and Control, Tactic TA0011 - Enterprise | MITRE ATT&CK®. [online] attack.mitre.org. Available from: https://attack.mitre.org/tactics/TA0011/. [Accessed 11 June 2023]

Patel, A., Shah, N., Ramoliya, D., & Nayak, A. (2020). A detailed review of cloud security: issues, threats & attacks. *4th International conference on electronics, communication, and aerospace technology (ICECA)* (pp. 758-764). IEEE.

Salim, D. T., Singh, M. M., & Keikhosrokiani, P. (2023). A systematic literature review for APT detection and effective cyber situational awareness (ECSA) conceptual model. *Heliyon*.

Smith, M., & Mulrain, G. (2017). Equi-failure: The national security implications of the equifax hack and a critical proposal for reform. *J. Nat'l Sec. L. & Pol'y*, *9*, 549.

Vance, A. (2014). Flow based analysis of Advanced Persistent Threats detecting targeted attacks in cloud computing. In *2014 First International Scientific-Practical Conference Problems of Infocommunications Science and Technology* (pp. 173-176). IEEE.

Xiao, L., Xu, D., Xie, C., Mandayam, N. B., & Poor, H. V. (2017). Cloud storage defense against advanced persistent threats: A prospect theoretic study. *IEEE Journal on Selected Areas in Communications*, *35*(3), 534-544.

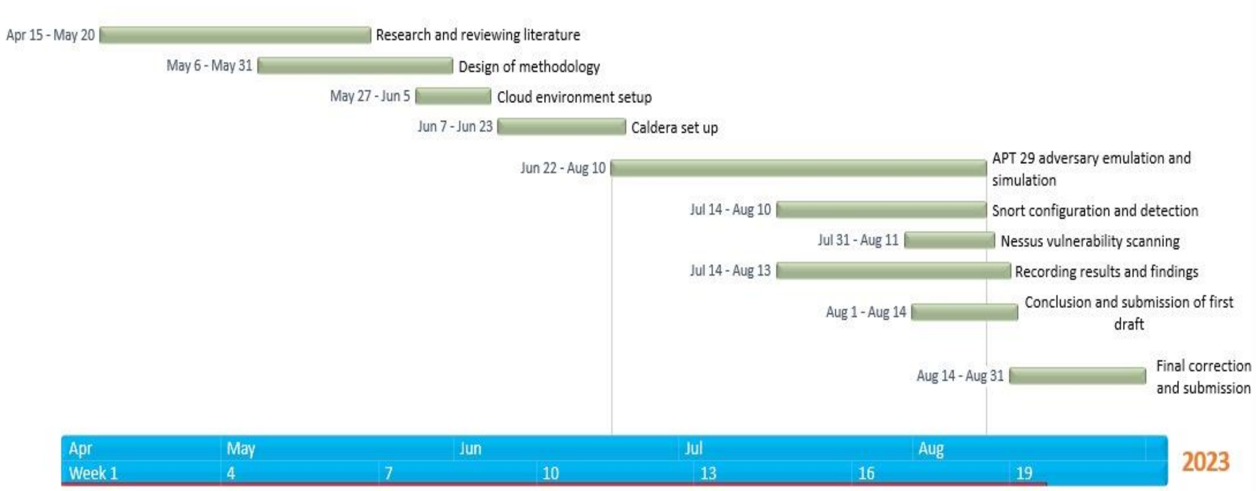
Xing, K., Li, A., Jiang, R., & Jia, Y. (2020, July). A review of apt attack detection methods and defense strategies. In *2020 IEEE Fifth International Conference on Data Science in Cyberspace (DSC)* (pp. 67-70). IEEE.

Xiong, W., Legrand, E., Åberg, O., & Lagerström, R. (2022). Cyber security threat modeling based on the MITRE Enterprise ATT&CK Matrix. *Software and Systems Modeling*, *21*(1), 157-177

Zulkefli, Z., Singh, M. M., & Malim, N. H. A. H. (2015). Advanced persistent threat mitigation using multi level security–access control framework. In *Computational Science and Its Applications--ICCSA 2015: 15th International Conference, Banff, AB, Canada, June 22-25, 2015, Proceedings, Part IV 15* (pp. 90-105). Springer International Publishing.

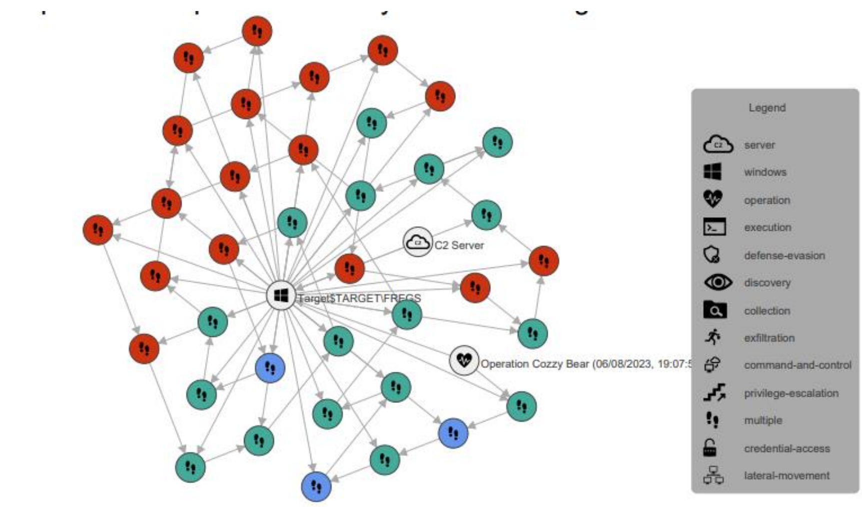
APPENDIX A Project Timeline

Gantt Chart of the Project timeline

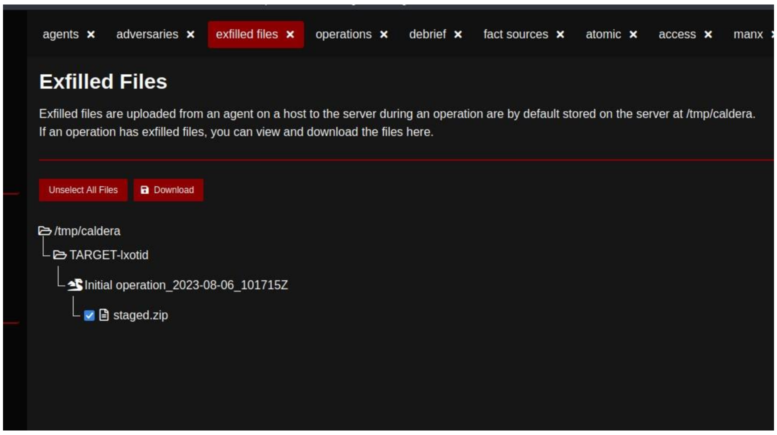


APPENDIX B Caldera Report

Steps Graph - Sequential stages of each operation as they pertain to the agents.



Exfiltrated Files – Files successfully Exfiltrated from the target

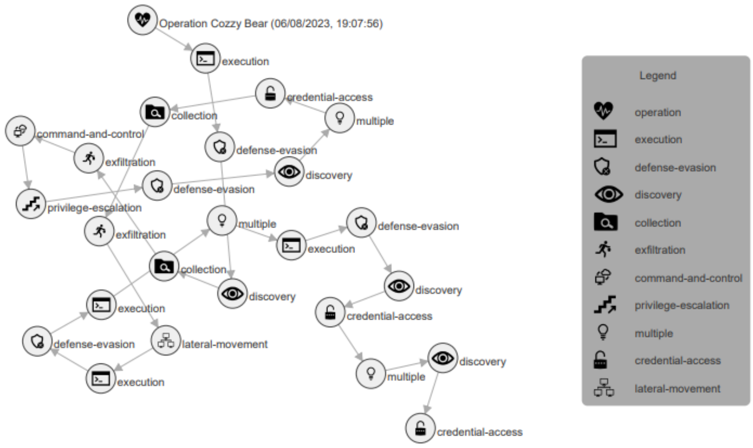


Exfilled Files

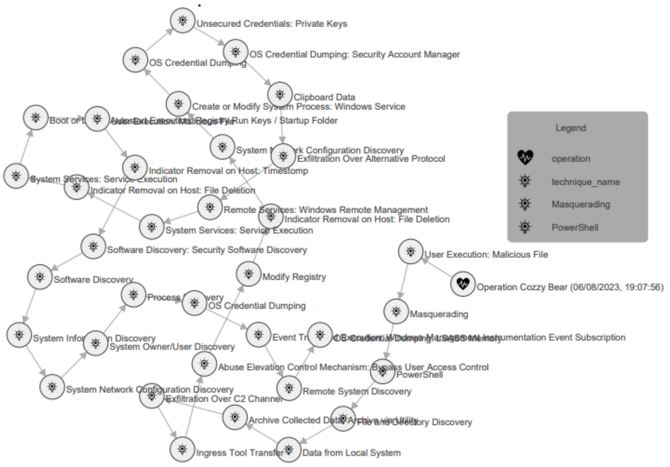
Exfilled files are uploaded from an agent on a host to the server during an operation are by default stored on the server at /tmp/caldera. If an operation has exfilled files, you can view and download the files here.

```
/tmp/caldera
└ TARGET-lxotid
  └ Initial operation_2023-08-06_101715Z
    └ ☑ staged.zip
```

Tactics Graph - A tactic explains the general purpose or the "why" of a step.



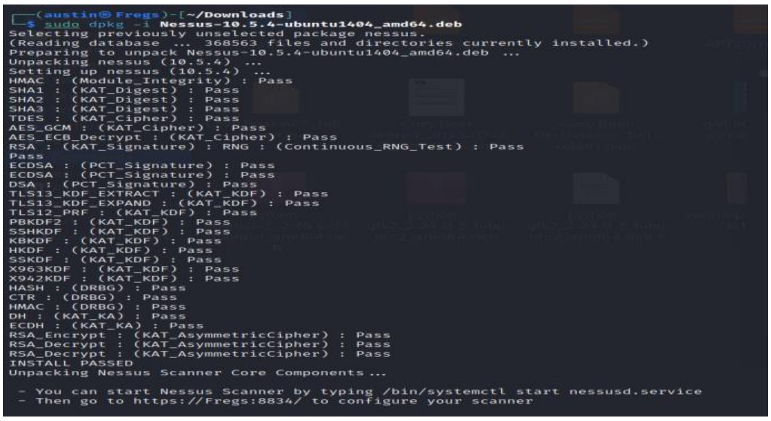
Technique Graph - A technique explains the technical method or the "how" of a step.


Unsecured Credentials: Private Keys
OS Credential Dumping: Security Account Manager
OS Credential Dumping
Clipboard Data
Create or Modify System Process: Windows Service
Boot or L
Run Keys / Startup Folder
System Network Configuration Discovery
Exfiltration Over Alternative Protocol
Indicator Removal on Host: Timestomp
System Services: Service Execution
Indicator Removal on Host: File Deletion
Remote Services: Windows Remote Management
Indicator Removal on Host: File Deletion
System Services: Service Execution
Software Discovery: Security Software Discovery
Software Discovery
Modify Registry
Process Discovery
OS Credential Dumping
System Information Discovery
System Owner/User Discovery
Event Tr
Instrumentation Event Subscription
Abuse Elevation Control Mechanism: Bypass User Access Control
PowerShell
System Network Configuration Discovery
Exfiltration Over C2 Channel
Remote System Discovery
Archive Collected Data
File and Directory Discovery
Ingress Tool Transfer
Data from Local System
User Execution: Malicious File
Operation Cozzy Bear (06/08/2023, 19:07:56)
Masquerading
Legend
operation
technique_name
Masquerading
PowerShell

APPENDIX D SNORT

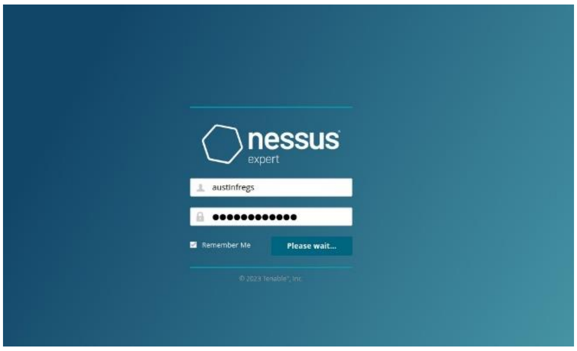
APPENDIX C Nessus

Nessus Installation



```
┌──(austin㉿Fregs)-[~/Downloads]
└─$ sudo dpkg -i Nessus-10.5.4-ubuntu1404_amd64.deb
Selecting previously unselected package nessus.
(Reading database ... 368563 files and directories currently installed.)
Preparing to unpack Nessus-10.5.4-ubuntu1404_amd64.deb ...
Unpacking nessus (10.5.4) ...
Setting up nessus (10.5.4) ...
HMAC : (Module_Integrity) : Pass
SHA1 : (KAT_Digest) : Pass
SHA2 : (KAT_Digest) : Pass
SHA3 : (KAT_Digest) : Pass
TDES : (KAT_Cipher) : Pass
AES_GCM : (KAT_Cipher) : Pass
AES_ECB_Decrypt : (KAT_Cipher) : Pass
RSA : (KAT_Signature) : RNG : (Continuous_RNG_Test) : Pass
Pass
ECDSA : (PCT_Signature) : Pass
ECDSA : (PCT_Signature) : Pass
DSA : (PCT_Signature) : Pass
TLS13_KDF_EXTRACT : (KAT_KDF) : Pass
TLS13_KDF_EXPAND : (KAT_KDF) : Pass
TLS12_PRF : (KAT_KDF) : Pass
PBKDF2 : (KAT_KDF) : Pass
SSHKDF : (KAT_KDF) : Pass
KBKDF : (KAT_KDF) : Pass
HKDF : (KAT_KDF) : Pass
SSKDF : (KAT_KDF) : Pass
X963KDF : (KAT_KDF) : Pass
X942KDF : (KAT_KDF) : Pass
HASH : (DRBG) : Pass
CTR : (DRBG) : Pass
HMAC : (DRBG) : Pass
DH : (KAT_KA) : Pass
ECDH : (KAT_KA) : Pass
RSA_Encrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
INSTALL PASSED
Unpacking Nessus Scanner Core Components...

 - You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
 - Then go to https://Fregs:8834/ to configure your scanner
```

Nessus Expert login Interface



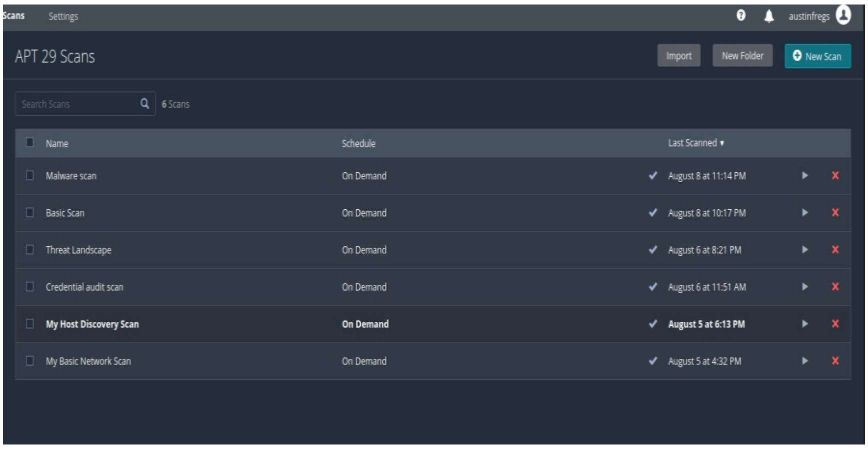
austinfregs

●●●●●●●●●●●●

☑ Remember Me

© 2023 Tenable®, Inc.

Vulnerability scans performed.



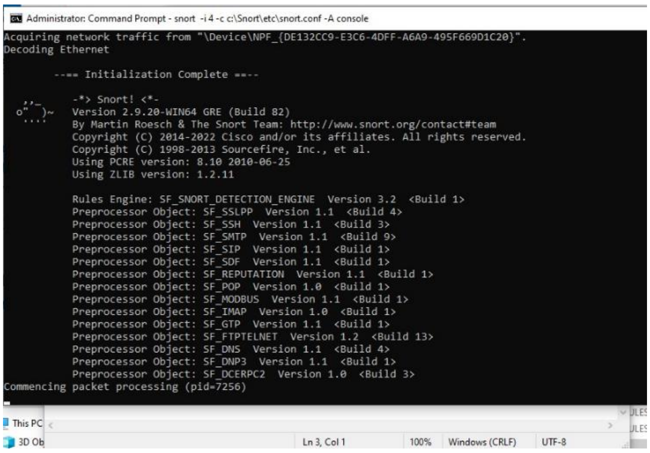
APT 29 Scans

6 Scans

□	Name	Schedule		Last Scanned ▾
□	Malware scan	On Demand	✓	August 8 at 11:14 PM
□	Basic Scan	On Demand	✓	August 8 at 10:17 PM
□	Threat Landscape	On Demand	✓	August 6 at 8:21 PM
□	Credential audit scan	On Demand	✓	August 6 at 11:51 AM
□	**My Host Discovery Scan**	**On Demand**	✓	**August 5 at 6:13 PM**
□	My Basic Network Scan	On Demand	✓	August 5 at 4:32 PM

Appendix D Snort

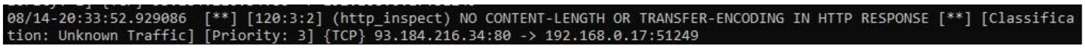
Initialising snort



Administrator: Command Prompt - snort -i 4 -c c:\Snort\etc\snort.conf -A console

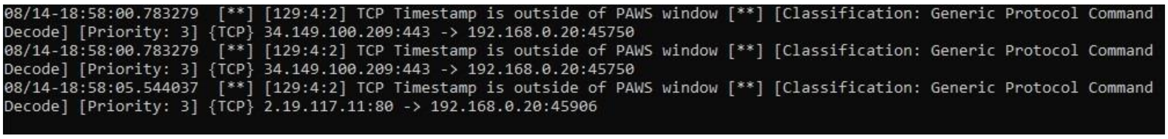
```
Acquiring network traffic from "\Device\NPF_{DE132CC9-E3C6-4DFF-A6A9-495F669D1C20}".
Decoding Ethernet

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.20-WIN64 GRE (Build 82)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using PCRE version: 8.10 2010-06-25
           Using ZLIB version: 1.2.11

           Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 3.2  <Build 1>
           Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
           Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
           Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
           Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
           Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
           Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
           Preprocessor Object: SF_POP  Version 1.0  <Build 1>
           Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
           Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
           Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
           Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
           Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
           Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
           Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
Commencing packet processing (pid=7256)
```

Bad traffic detected: No Content-Length.



```
08/14-20:33:52.929086  [**] [120:3:2] (http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE [**] [Classifica
tion: Unknown Traffic] [Priority: 3] {TCP} 93.184.216.34:80 -> 192.168.0.17:51249
```

Bad traffic detected: TCP Timestamp is outside of PAWS window.



```
08/14-18:58:00.783279  [**] [129:4:2] TCP Timestamp is outside of PAWS window [**] [Classification: Generic Protocol Command
Decode] [Priority: 3] {TCP} 34.149.100.209:443 -> 192.168.0.20:45750
08/14-18:58:00.783279  [**] [129:4:2] TCP Timestamp is outside of PAWS window [**] [Classification: Generic Protocol Command
Decode] [Priority: 3] {TCP} 34.149.100.209:443 -> 192.168.0.20:45750
08/14-18:58:05.544037  [**] [129:4:2] TCP Timestamp is outside of PAWS window [**] [Classification: Generic Protocol Command
Decode] [Priority: 3] {TCP} 2.19.117.11:80 -> 192.168.0.20:45906
```