Volume 9, Issue 12, December – 2024 International Journal of Innovative Science and Research Technology
ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14598602

The Impact of Emerging Cloud Security Threats: A Focus on Advanced Persistent Threats

Austin Orumwense[1*]; Mansoor Ihsan[2]
[1]Graduate Student, University of Bolton, UK.
[2]Lecturer, Department of Computing, University of Bolton, UK.

Corresponding Author:- Austin Orumwense[1*]

Abstract:- The rapid advancement in cloud computing technology is continually evolving, with threat actors refining their tactics, exploiting new vulnerabilities, and expanding their influence. This dynamic environment exposes cloud infrastructure to emerging cyber-attacks, including Advanced Persistent Threats (APT), impacting both customers and service providers. Understanding the gap in APT detection literature is crucial for researchers. The research aims to comprehensively understand APTs' influence on cloud security, analyse existing approaches, emulate adversary plans, simulate attacks using Mitre Caldera, employ Snort for detection, and utilise the Nessus vulnerability scanning tool.

The study addresses 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. The findings underscore the intricate interplay between APT activities and cloud environments, emphasising the need for robust detection and mitigation strategies. The combination of APT simulation, vulnerability assessment, and detection mechanism analysis yields invaluable insights into the evolving threat landscape within cloud ecosystems. As organisations increasingly embrace cloud technologies, the lessons from this study contribute substantially 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.*

I. INTRODUCTION

Cloud computing has rapidly gained traction, driven by market dynamics and technological advancements. The evolving business landscape necessitates transformations in computing infrastructures, with enterprise services and applications continually being added or retired. The concept of cloud computing has various interpretations; for instance, Buyya et al. (2010) describe it as the "fifth utility," likening it to essential services like water and electricity. 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 (Singh et al., 2023). To prevent service disruptions, it is imperative to proactively identify potential vulnerabilities and establish robust defence mechanisms in advance.

➢ *Importance of Security in the cloud*

With cloud computing becoming the primary method of delivering IT services, the availability and dependability of these services are critical. Large-scale data centres, hosting extensive server clusters, are increasingly used to support internet and business applications. However, these data centres face significant security challenges. Emerging attacks, including zero-day exploits and advanced persistent threats (APTs), pose serious risks to the confidentiality, integrity, and availability of cloud-based data and services (Zulkefli et al., 2022). 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 (Wang et al., 2016).

In recent times, cyber-attacks have grown increasingly sophisticated, characterized by their high level of targeting and long-term nature. 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).

To prevent service disruptions, it is imperative to proactively identify potential vulnerabilities and establish robust defence mechanisms in advance. 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).

➢ *Advanced Persistent Threats (APTs)*

APTs are sophisticated, long-term cyber-attacks often attributed to state-sponsored entities. These attacks aim to infiltrate and extract sensitive information from targeted

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14598602

organizations, posing severe threats to cloud security (Khaleefa & Abdulah, 2022). 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). Traditional security measures, such as identity, authentication, and authorization, are insufficient in combating these advanced threats. Effective defence against APTs requires a combination of technical and physical security measures.

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.

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).

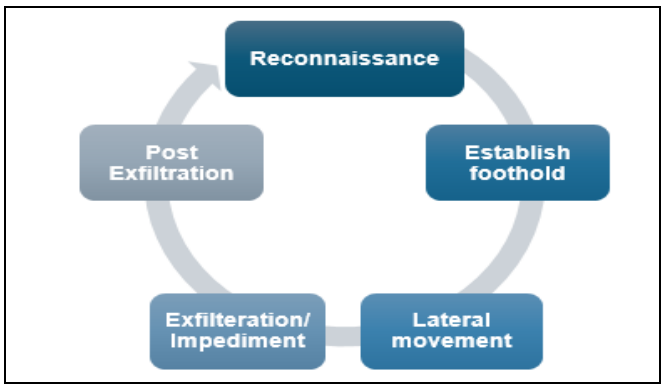

Fig 1 APT Lifecycle

➢ *Problem Statement*

The increasing reliance on cloud computing heightens the risk of cyber-attacks, particularly APTs. These threats can lead to significant data breaches, service interruptions, and other serious consequences, highlighting the inadequacy of traditional mitigation techniques. This study aims to identify the impact of APTs on cloud security and propose effective detection and mitigation strategies.

➢ *Research Aims and Objectives*

The primary aim of this research is to evaluate the impact of APTs in cloud environments and develop efficient mitigation strategies. Specific objectives include:

- Investigating the impact of APTs on cloud security.
- Analysing current approaches to addressing APTs.
- Designing an operation to emulate an APT adversary plan.
- Simulating APT attacks using tools like Mitre Caldera and Snort.
- Identifying potential vulnerabilities with Nessus Vulnerability scanning tool.

II. LITERATURE REVIEW

Researchers have recently investigated the different ways in which emerging threats can affect the security of cloud computing. 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 organisations about the potential risks associated with storing user data in the cloud (Sun et al., 2014). Similar research conducted by Kalid et al. (2023) discusses the security vulnerabilities, threats, and attacks associated with centralised 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 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, 2022). Table 1 shows 10 major APT attacks and their impact. Indeed, the success of APT attacks is seemingly inevitable, leading to a substantial focus on research and literature related to APT detection.

Table 1 Major APT Attacks and their Impact (Kumar et al., 2022)

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

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14598602

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

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). This study addresses 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.

III. METHODOLOGY

The primary objective of information security is to safeguard an enterprise's information, ensuring its availability, integrity, and confidentiality (Taherdoost, 2022). To ensure businesses feel secure migrating to the cloud, this study aims to propose an approach using open-source tools to identify and proactively detect threats, thereby mitigating potential damage.

➢ *Research Philosophy*

This study adopts a pragmatic research approach, emphasizing the practical application of knowledge to real-world problems. The primary objective is to assess the impact of APTs on cloud security. Data is collected from reviewed literature and through experimental simulations, and statistical methods are employed to analyse the data. By combining theoretical insights from literature, data from simulations, and statistical analysis, the study aims to provide practical insights and recommendations for addressing APTs in cloud environments.

➢ *Research Design*

This research employs an exploratory approach, combining quantitative and qualitative methods. The qualitative component involves reviewing the literature on existing approaches for addressing APTs in cloud environments and researching tactics and techniques from the MITRE ATT&CK framework. The quantitative component includes experimental simulations of APT attacks in a cloud environment and vulnerability scanning to assess detection and mitigation techniques. Thematic analysis is used to identify common themes and patterns in the data.

➢ *Experiment Workflow*

The experiment workflow includes the following steps:

- Setting up the cloud environment.
- Configuring and simulating attacks using Caldera.
- Detecting attacks using Snort.
- Scanning for vulnerabilities using Nessus.

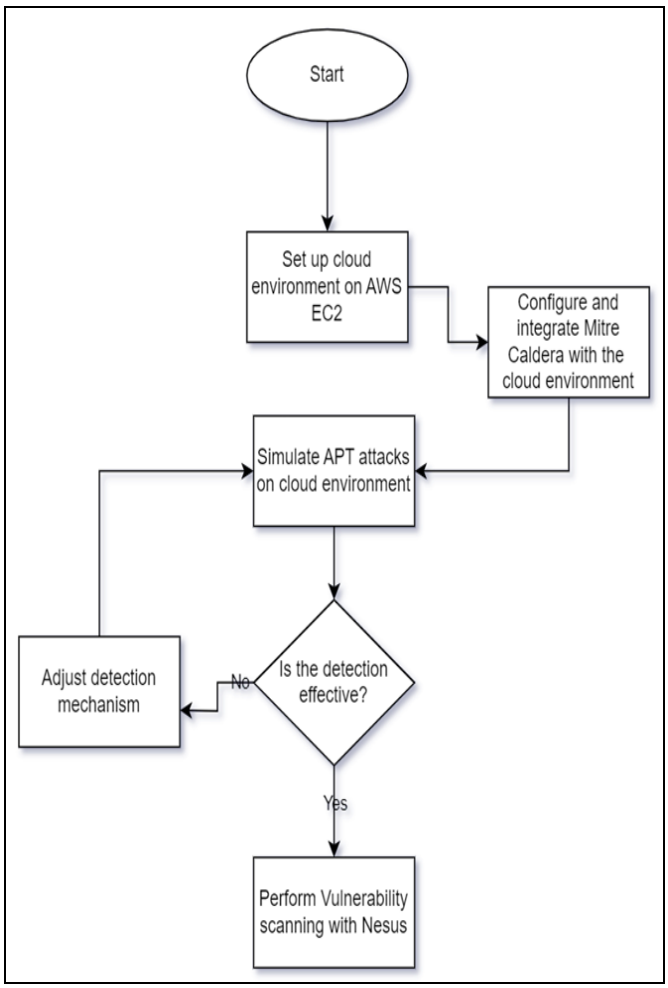

Fig 2 Experiment Workflow

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14598602

➢ *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 3 closely mirrors real-world cloud infrastructures, allowing for a controlled and secure emulation of advanced cyber threats. Two instances were setup (Linux and Windows), Caldera was used to initiate the APT attacks from the Linux instance to the Windows, Snort was used for the detection of the APT attacks, and the Nessus scanner was 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.

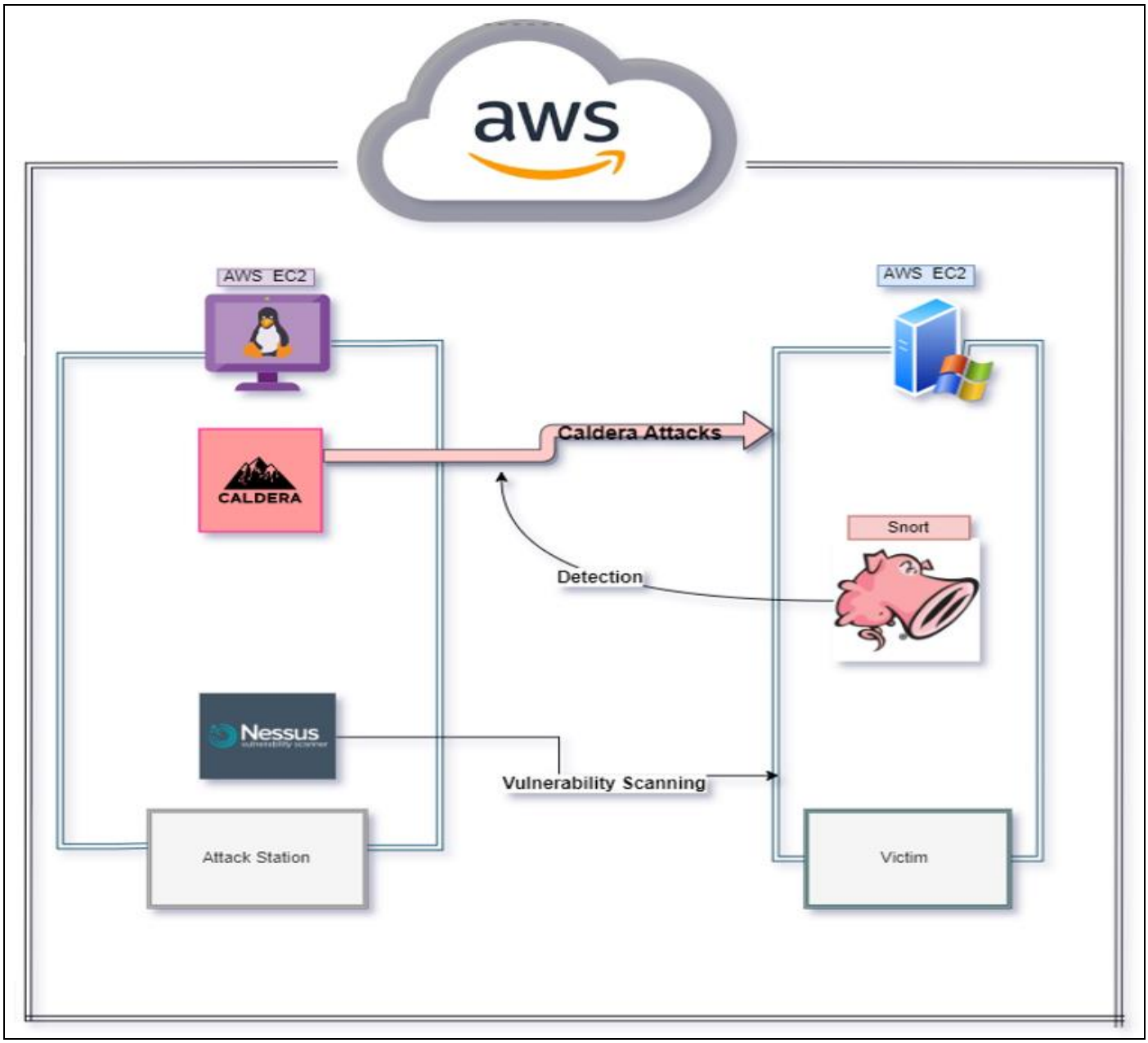

Fig 3 Components of the Simulation

➢ *Simulation of the Cloud Environment*

- Infrastructure Selection: A representative cloud environment was set up using AWS EC2 instances, with Linux for the attack station and Windows for the victim system.
- Virtualization and Networking: A Windows virtual machine is set up on the EC2 instance, with networking components and cloud services to replicate a realistic cloud environment.
- Security Controls: Appropriate security controls, including firewalls, IDS/IPS, encryption, access controls, and logging mechanisms, are implemented to protect the simulated cloud environment.
- Cloud Service Configuration: Relevant cloud services such as storage, databases, and virtual networks are configured to emulate a functional cloud infrastructure for the experiments.

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14598602

➢ *Simulating APT Attacks on the Cloud Environment*

- Define APT Attack Scenarios: Research APT techniques using the MITRE ATT&CK framework and define attack scenarios.
- Configure and Customize Caldera: Set up Caldera in the controlled environment, configure agents on target systems, and create adversary profiles to simulate APT29 attack scenarios.
- Simulate APT Attacks: Use Caldera to initiate APT attack simulations, monitor the attacks, and record their behaviours, TTPs, and outcomes.
- Assess Detection Capabilities: Use Snort to detect APT-like activities and evaluate detection rates.
- Record Findings: Document findings from the APT simulations and detection assessments.
- Utilize Nessus Vulnerability Scanning: Install and configure Nessus to scan for vulnerabilities, initiate scans, and analyse the results.

➢ *APT29 Emulation Plan*

The APT29 emulation plan integrates various techniques observed in their operations, categorized into two approaches: "smash-and-grab" and "low and slow." Each approach as shown in fig. 4, follows specific tactics and techniques to simulate cyber-espionage activities, which are used in this research to carry out the operation.

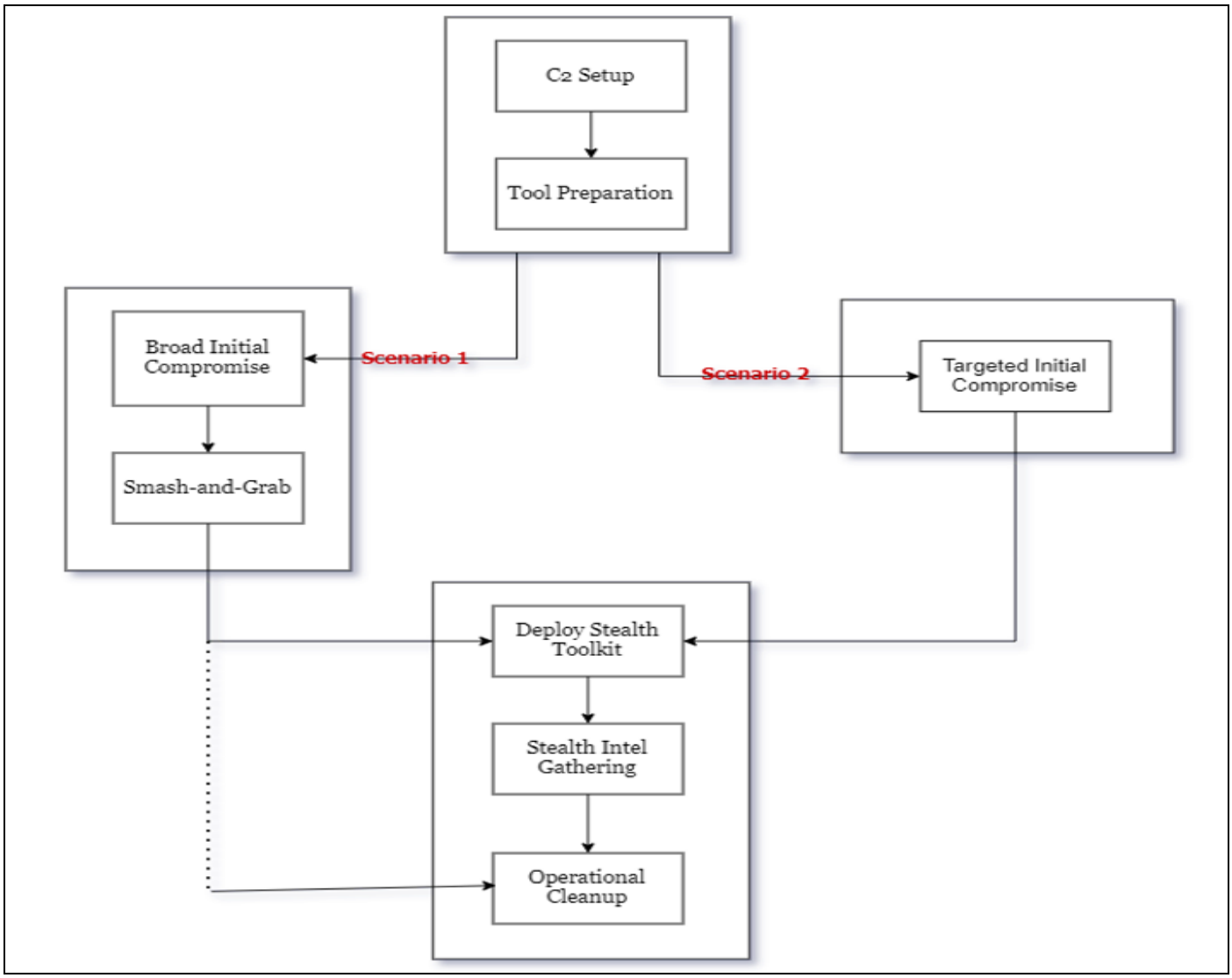

Fig 4 Operation Flow of APT 29 EMU Plan

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.

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14598602

➢ *Ethical Considerations*

Offensive security tools, originally intended for defenders, are often misused by malicious actors. MITRE Caldera, used responsibly in this study, includes safeguards to prevent misuse. The open-source version of Caldera ships with default, low-risk adversary profiles, while more dangerous profiles are hidden in the enterprise version. This study ensures responsible emulation of adversaries to better understand their tactics and capabilities without empowering them.

IV. RESULTS AND DISCUSSION

During the emulation of an APT29 attack using the MITRE Caldera framework, the process showed a significant level of proficiency in replicating many of the attack stages detailed in the emulation plan. The foundational architecture strictly adhered to the prescribed configuration parameters from the emulation library, though prudent adjustments were necessary for the seamless execution of specific aspects of the emulation blueprint. These adjustments were crucial to overcoming challenges encountered during the simulated attack.

➢ *APT29 Emulation Results*

The successful emulation involved a meticulously choreographed series of steps, each essential to the attack sequence. Certain steps required insights from previous actions, including thorough host and network reconnaissance and identification of administrative users. Some phases depended on the precise and sequential completion of preceding actions, such as establishing persistent access before initiating a system-wide reboot.

Despite the overall success, some challenges highlighted the intricate dependencies between different attack phases. These were especially noticeable, emphasising the complex interconnections stemming from earlier stages. An example of CALDERA's adaptability was evident when a designated file already existed in the specified location. CALDERA smoothly incorporated the malicious payload into the existing file, demonstrating its flexibility in scenarios where threat actors manipulate existing files.

However, CALDERA struggled with effectively triggering established persistence mechanisms designed to activate upon rebooting the victim machine. After reboot, the CALDERA agent failed to communicate with the server, leading to premature emulation termination. Manual activation attempts of persistence mechanisms also failed, leading to the removal of the reboot directive from the emulation plan. Post-adjustment, the emulation showed comprehensive execution with an acceptable ratio of successful operations as reported by CALDERA.

CALDERA accurately replicated a wide array of tactics and techniques used by APT29. Table 2 outlines the tactics and techniques implemented in this simulation, covering data collection, command-and-control, credential access, defence evasion, discovery, execution, exfiltration, lateral movement, multiple tactics, and privilege escalation.

The framework's success in simulating these actions indicates its efficacy in modelling complex attack scenarios. However, the emulation had limitations, such as unsuccessful execution or skipping of certain tactics. For instance, the framework struggled with persistence, lateral movement, and exfiltration, possibly due to the intricacies of advanced tactics, emulation environment constraints, or the need for further calibration.

The graph in Figure 5 illustrates the intricate nature of the CALDERA simulation, revealing a mix of successful executions, failures, and skipped operations. These outcomes highlight both the capabilities and limitations of the simulation framework, prompting a critical analysis of its fidelity and implications for understanding APT attack behaviours.

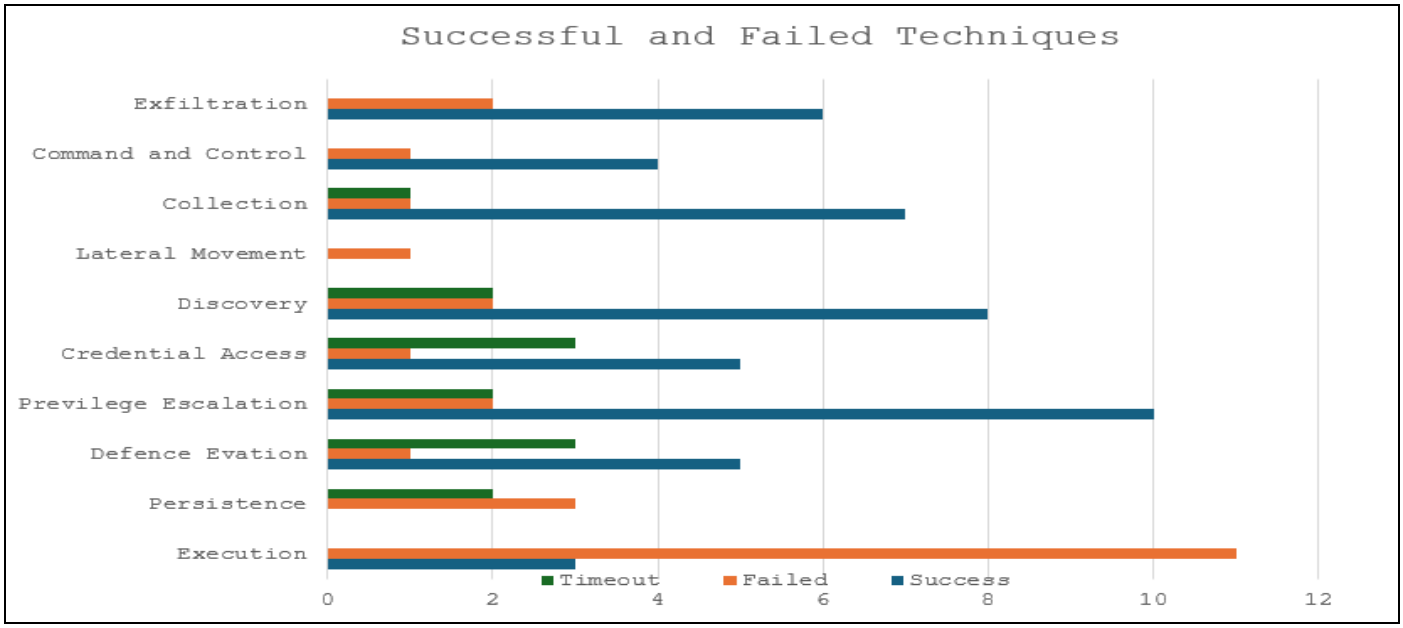

Fig 5 Successful and Failed Techniques from Caldera

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14598602

Success rates across different technique categories show notable disparities. Privilege Escalation and Execution had relatively higher success rates, with 10 and 3 successful executions, respectively. In contrast, Persistence techniques were either entirely skipped or failed, indicating potential challenges in simulating these intricate phases of an APT attack.

A closer examination of individual technique categories reveals intriguing dynamics. Defence Evasion had a respectable success rate of 5 but also experienced 1 failure and 3 timeouts. This suggests CALDERA successfully evaded some defences but encountered hurdles in others, hinting at the complexity of evading diverse security measures. Credential Access techniques showed a balanced success and failure rate, each accounting for 5 and 1, respectively, with 3 timeouts. This distribution reflects the intricacies of accessing credentials in a simulated attack.

Lateral Movement and Exfiltration outcomes raise questions. Lateral Movement operations were entirely skipped, suggesting a limitation in CALDERA's emulation capabilities in this area. Exfiltration techniques had a higher success rate of 6 but also had 2 failures. The reasons for skipping Lateral Movement techniques and mixed Exfiltration outcomes highlight the complexity of these aspects in APT attack simulations.

The facts graph in Figure 6 outlines information extracted during the operation, including executed commands and the associated agent responsible for discovering the information. Each fact is assigned a score of 1 by default. Significant facts, such as host.user.password, can be allocated a score of 5. Facts required to populate variables prioritize those with the highest scores. Facts with a score of 0 are blacklisted and ineligible for use within an operation.

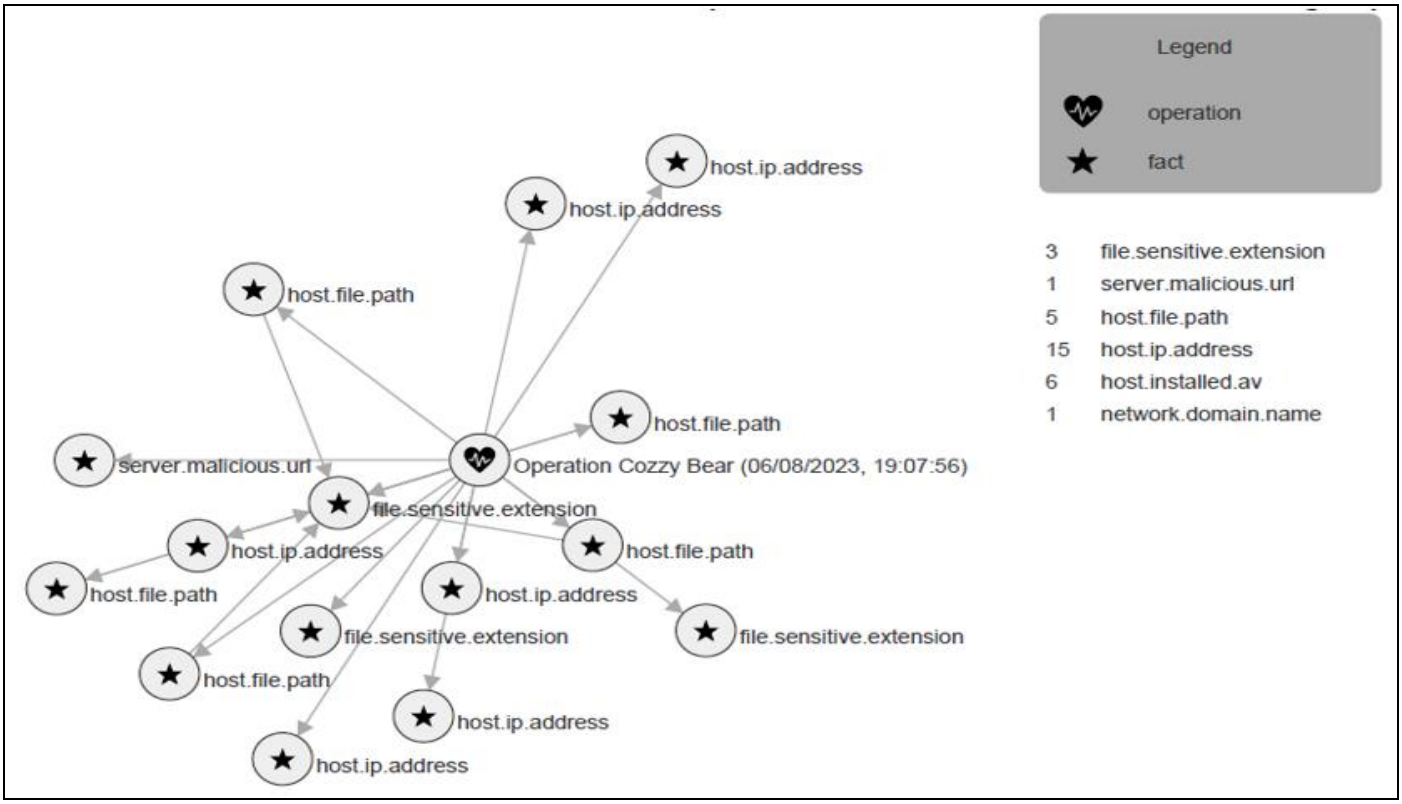

Fig 6 Facts Graph

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

This diverse array of traits, culminating in 31 facts, provides valuable insights into the simulation's complexity and fidelity. By capturing multifaceted aspects such as IP addresses, antivirus presence, and file paths, this data enriches the understanding of the simulated APT29 attack's scope and authenticity. It enables informed assessments of the simulation's alignment with real-world APT29 behaviours, facilitating deeper analysis of its effectiveness and potential for accurately replicating sophisticated attack scenarios.

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14598602

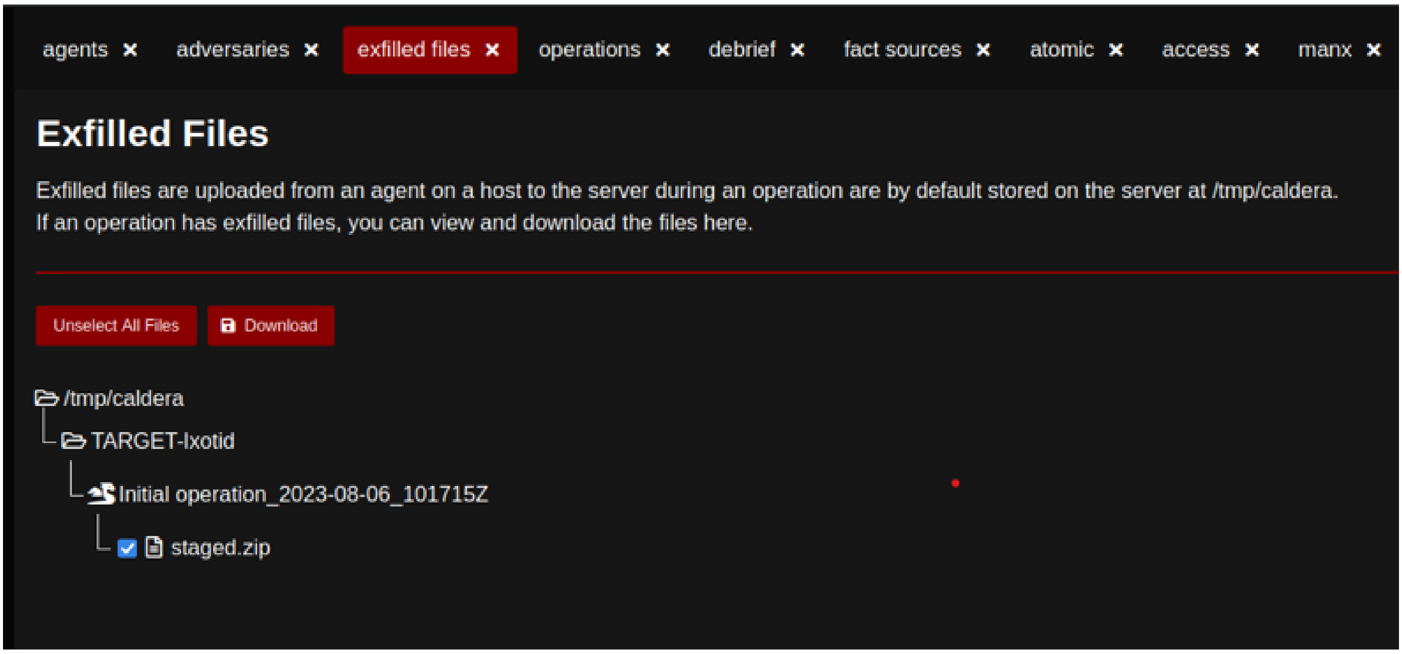

Fig 7 Exfiltrated Files

Figure 7 shows that some files were successfully exfiltrated, indicating that the APT29 emulation completed its lifecycle and data espionage was indeed successful.

➢ *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 8, can indicate deviations from established network communication norms.

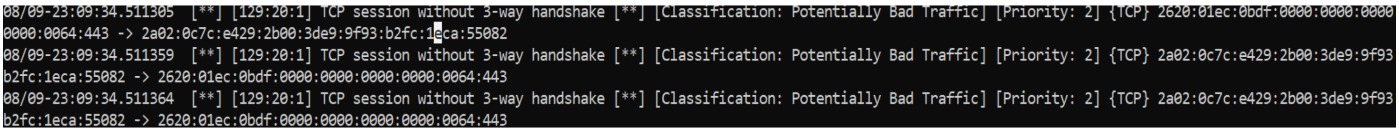

Fig 8 Session without 3-way Handshake Detected

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.

Fig 9 APT29 Traffic Detected

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14598602

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.

➢ *Nessus 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 is noteworthy that default paranoid checks are enabled, as certain checks may necessitate them to function properly.

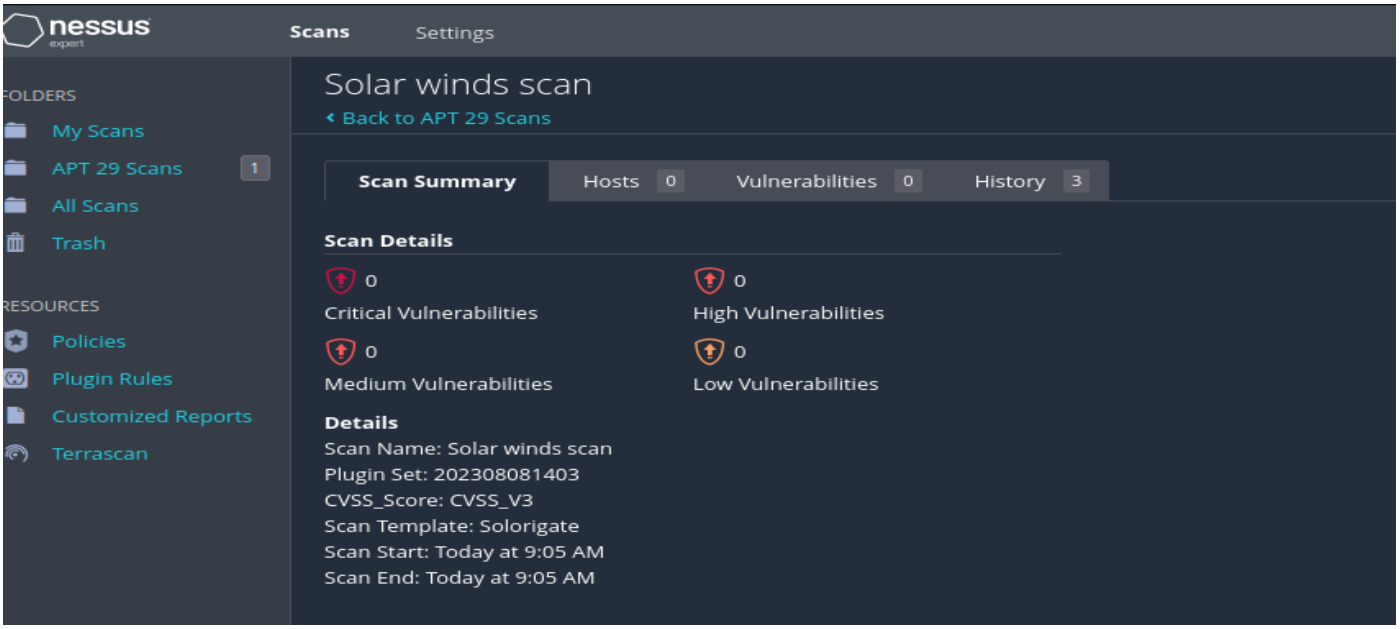

Fig 10 Solar Winds Scan

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 artefacts linked to the SolarWinds backdoor. An important observation is that the default SolarWinds vulnerability scan with Nessus depicted in figure 10 yielded no vulnerabilities.

➢ *Identified Critical Vulnerabilities Exploitable by APT*

Table 1 Identified 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.

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14598602

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.

➢ *Mitigation Strategies Against the Critical Vulnerabilities*

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

✓ 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.
✓ Security Awareness: Conduct training for employees to recognize and report suspicious emails and links, reducing the effectiveness of spear-phishing campaigns.
✓ Web Filtering: Employ web filtering solutions to block access to known malicious websites and prevent watering hole attacks.
✓ Network Segmentation: Implement network segmentation to limit lateral movement in case an attacker gains access.

- *Adobe Flash Player Vulnerability (APSB20-58):*

✓ Flash Player Removal: Since Adobe Flash Player is no longer supported, organizations should completely remove it from their systems to eliminate this potential vulnerability.
✓ Web Content Inspection: Implement content inspection mechanisms to detect and block malicious content, reducing the risk of drive-by downloads.
✓ File Type Filtering: Configure email gateways and security solutions to block or scan files with Flash content.
✓ Regular Updates: Maintain up-to-date software and applications to reduce the attack surface.

- *Curl use-after-Free Vulnerability (CVE-2022-43552):*

✓ Vendor Patches: Apply vendor-supplied patches promptly to fix known vulnerabilities and protect against exploitation.
✓ Code Review and Testing: Implement code reviews and security testing in the software development process to identify and address vulnerabilities early.
✓ Dependency Management: Regularly update and audit dependencies in software stacks to prevent reliance on vulnerable components.
✓ Zero-Trust Architecture: Implement a zero-trust approach to limit lateral movement and contain potential breaches.

- *Microsoft Edge Vulnerabilities:*

✓ Browser Updates: Keep browsers up to date with the latest security patches and features.
✓ Extension Review: Regularly review and audit browser extensions, removing any suspicious or unnecessary ones.
✓ Security Configurations: Configure browser security settings to block potentially harmful content and prevent automatic downloads.
✓ Multi-Factor Authentication: Implement multi-factor authentication to add an extra layer of security against phishing attacks.

V. RECOMMENDATIONS

Based on the research findings presented in this paper, 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.

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14598602

- 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.

VI. CONCLUSION

This paper embarked on investigating 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 comprehensive insights into APT attacks. The identification of 31 traits demonstrated the simulation's accuracy in mirroring real APT29 attacks, aiding in the assessment of alignment with APT29 behaviours and facilitating analysis of its effectiveness. Additionally, the Nessus vulnerability tool highlighted network vulnerabilities exploitable by an APT, while Snort detected APT29 traffic. These findings significantly enhanced the understanding of system security and informed remediation decisions.

The comparative analysis revealed that utilizing 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, incorporating Snort's real-time intrusion detection capabilities enhances the proactive identification of APT29 attacks, enabling 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 efforts.

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

REFERENCES

[1]. 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.

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

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

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

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

[6]. 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

[7]. 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.

[8]. Khalid, M. I., Ehsan, I., Al-Ani, A. K., Iqbal, J., Hussain, S., & Ullah, S. S. (2023). A comprehensive survey on blockchain-based decentralized storage networks. *IEEE Access*, *11*, 10995-11015.

[9]. 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.

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14598602

[10]. Knapp, K. J., Denney, G. D., & Barner, M. E. (2011). Key issues in data center security: An investigation of government audit reports. *Government Information Quarterly*, *28*(4), 533-541.
[11]. 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.
[12]. 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.
[13]. 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.
[14]. 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.
[15]. Sun, Y., Zhang, J., Xiong, Y., & Zhu, G. (2014). Data security and privacy in cloud computing. *International Journal of Distributed Sensor Networks*, *10*(7), 190903.
[16]. Taherdoost, H. (2022). Cybersecurity vs. Information Security. *Procedia Computer Science*, 215, 483-487.
[17]. 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.
[18]. 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.
[19]. 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.
[20]. 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.