Analysis of Man-In-The-Middle Dropbox Attacks evasion and effectiveness against SOC tools

Aziel Orozco
Department of Computer Science and Information Systems
University of North Georgia
Dahlonega, Georgia
aaoroz9881@ung.edu

***Abstract*—This document analyzes man-in-the-middle(MitM) dropbox attacks and their ability to evade detection by scrutinizing their efficacy against diverse Security Operation(SOC) tools. The core inquiry revolves around, what factors affect the success of different MitM attacks and evasion techniques on red team engagements against various Security Operation Center(SOC) tools? To address this, a Windows Active Directory was deployed into a real network environment along side Elastic Cloud's Security Information and Event Management capabilities of integrating SOC tools to oversee the Active Directory network. The Active Directory environment contained a Windows 2022 Server configured as a domain controller and a Windows 10 Enterprise virtual machine. Two types of dropbox devices were used to execute the MitM attacks: Hak5's LAN Turtle, designed for MitM attacks and persistence in a network, and a custom Raspberry Pi 4. This research offers practical insights into MiTM attacks's and their effectiveness against SOC tools, bridging the gap between red team engagement dropbox usage and SOC tool effectiveness against them to aid Cybersecurity professionals in defending against attacks of this nature.**

Keywords—Man-in-the-Middle, Red Team Engagements, dropbox, Penetration Testing, Security Operation Center, SOC, Network Security, Kali Linux, Security Information and Event Management, SIEM, LAN Turtle, Raspberry Pi, Active Directory

I. INTRODUCTION

In the evolving landscape of Cybersecurity, the relentless efforts of adversaries to breach network defenses demands vigilant scrutiny from Cybersecurity professionals. Beyond the scope of network intrusion lies a potent and often underestimated attack vector, physical access. Adversaries who gain physical access to corporate buildings' are able to plant a device known as a "dropbox" into the network via a network ethernet port or networking closet and are able to maintain persistent access to the network and further enumerate and execute attacks on the enterprise's internal network. Understanding and detecting this threat from a network security perspective is an important task for Cybersecurity professionals' in today's digital age. Penetration testers and red team operators, who focus on defense through offensive techniques, undertake the task of emulating the tactics, techniques, and procedures of adversaries in efforts' to better a corporation's security posture and understanding by identifying any potential vulnerabilities in the internal network. These skilled practitioners simulate scenarios in an Active Directory environment specified in the rules of engagement outlined by the client and simulate adversaries who try to breach physical perimeters through social engineering tactics, exploit physical vulnerabilities, and plant dropbox devices to further enumerate the internal network and identify vulnerabilities.

Complementing these efforts are blue team operators, such as this operating within Security Operation Centers'(SOC) stand as the front lines of defense. They must detect and respond to any potential network breaches or anomalies in the network. Blue team operators also work in conjunction with red teasers, forming a purple team engagement, where valuable lessons are drawn to significantly enhance the SOC's ability to protect, defend, respond, and recover from any network intrusions[1].

This research aims to analyze the inner workings of MiTM dropbox attacks executed within an internal Active Directory environment where physical and internal access is assumed. By understanding the effectiveness of various attacks and dropbox device usage against SOC tools, this research provides Cybersecurity professionals and corporations' with practical insights on why these attacks' pose a threat in an internal Active Directory environment. Exploring MitM attacks, dropbox devices, and the tactics employed by penetration and red team operators in a SOC environment allows for a better understanding of real world scenarios and the effectiveness of safeguarding digital assets in an increasingly interconnected world.

II. LITERATURE REVIEW

A. Man-In-The-Middle Attacks'

Man-in-the-Middle attacks, are attacks in which the attacker secretly intercepts and alters the communication between two device without the parties knowledge or consent[2]. In a MitM attack, the attacker positions a device between the flow of communication between device 1 and device 2. In doing so, the attacker can then eavesdrop, capture sensitive information, inject malicious packets, and manipulate any and all traffic between the two devices[6].

Common goals and objectives of adversaries in executing MitM attacks are to exfiltrate sensitive data and manipulate traffic[6]. This poses a serious risk to enterprise networks in a wide range of industries that carry sensitive information for their customers including:

- Usernames
- Passwords
- Email Addresses
- Credit Card Information
- Personal Identifiable Information(PII)

Techniques used by attackers to conduct MitM attacks vary on the objective, some objectives include:

- Intercepting Sensitive Data
- Gaining Unauthorized Access to systems

• Manipulating communication protocols for malicious purposes

MitM attack techniques can vary in complexity and sophistication, the most common techniques used on penetration tests and red team engagements in an Active Directory environment are analyzed, such as ARP Poisoning, DNS Spoofing, LLMNR Poisoning, NTLM Relay Attack, and IPv6 DNS Takeover[7].

ARP Poisoning is when attackers manipulate the Address Resolution Protocol(ARP) to associate their MAC address with the IP address of a legitimate device in the local network. This causes traffic intended for the legitimate device to be redirected to the attacker's system[1]. In 2014, a MitM attack known as "Dark Hotel" campaign targeted high profile business travelers staying at luxury hotels. Attackers used ARP poisoning to intercept and manipulate network traffic, infecting victims with malware.

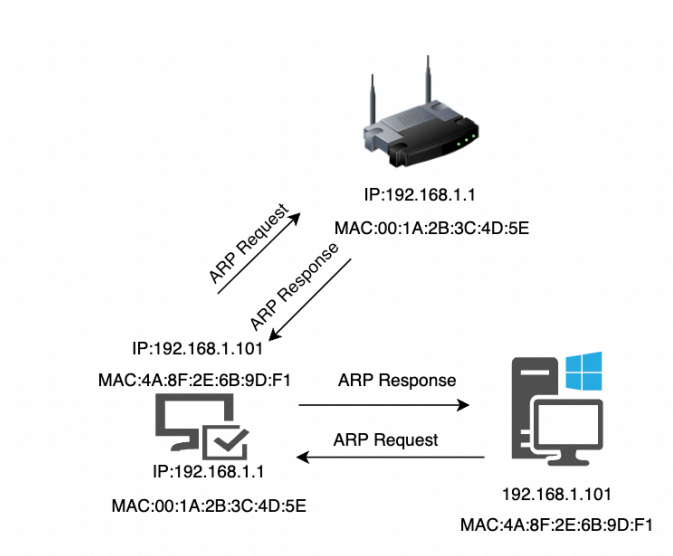

Figure 1: ARP Poisoning

DNS Cache Poisoning, is when an attacker alters DNS(Domain Name System) records to redirect users to malicious websites when trying to access a legitimate website[1]. This techniques often used for phishing attacks, in the attempt to obtain a victim's login credentials.

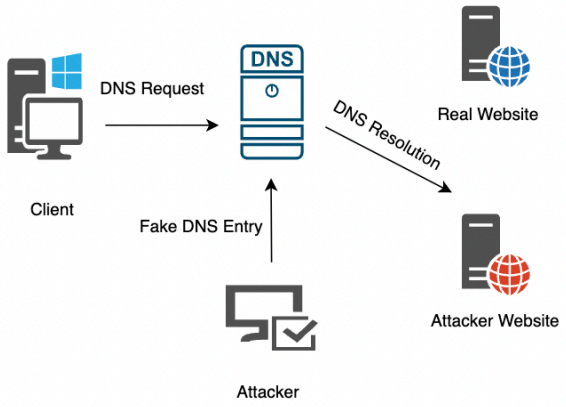

Figure 2: DNS Cache Poisoning

LLMNR(Link-Local Multicast Name Resolution) Poisoning, is when an attacker exploits the LLMNR protocol to intercept DNS queries on the local network. LLMNR is used to resolve hostnames to IP addresses when DNS fails to do so or does not exist in the local network. For example, a user requests connection to a network share named "FinanceDocuments", if the DNS fails to resolve the share or if DNS does not exist in the network, the attacker sends a malicious LLMNR response to the user redirecting them to the attacker's machine instead of the server hosting the network share. By responding to LLMNR queries with false information, attackers can trick computers on the internal network into sending sensitive information across the network such as NTLMv2 password hashes to the attacker's dropbox device[7].

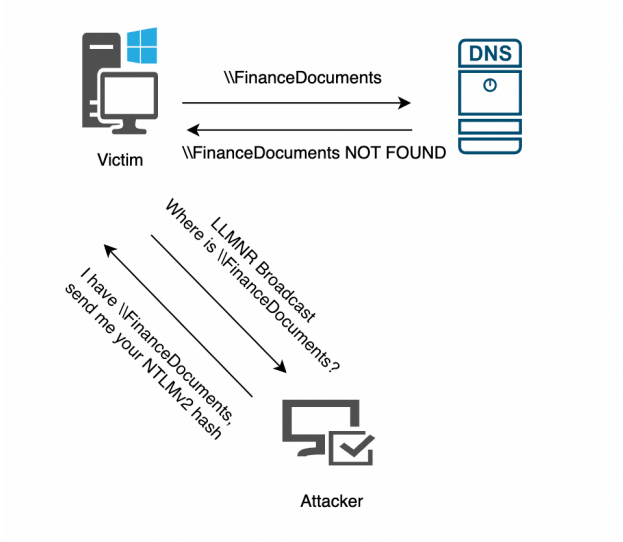

Figure 3: LLMNR Poisoning

NTLM(NT LAN Manager) Relay Attack, this attack involves intercepting authentication attempts that use NTLM. By capturing authentication attempts between a client and a server(such as a username and hashed password), the attacker can relay this information to another system to a target server to gain unauthorized access. Attackers' often exploit the trust relationship between systems to perform this attack and potentially gain access to other systems in an Active Directory environment. For example, an attacker, as the man in the middle, intercepts and monitors network traffic and impersonates devices by relaying authentication attempts, impersonating both ends of the communication. In figure 4, "UserA" sends an NTLM authentication request to the server to access a resource. The attacker intercepts the NTLM authentication request sent by UserA's system to the target server. The attacker then can relay the intercepted NTLM authentication request to the target server. The server receives the authentication request from the attacker instead of UserA. The server then sends a challenge to UserA, but instead of UserA responding, the attacker relays this challenge to UserA, pretending to be the server. UserA believes the attacker is the server and sends the response to the challenge, the attacker then relays the challenge to the server, authenticating to the server and granting access to the attacker impersonating UserA.

Figure 4: NTLM Relay Attack

IPv6 DNS Takeover, this attack involves an attacker manipulating IPv6 DNS records to redirect IPv6 traffic from its intended destination to the attacker's dropbox in the internal network. By acting as a rogue DNS and DHCPv6 server, the attacker provides an IPv6 address to the victim, redirecting their IPv6 traffic to the attacker's dropbox.

As shown in Figure 5, the attacker can manipulate settings related to the Web Proxy Auto-Discover Protocol(WPAD) protocol to deceive the victim into using a proxy controlled by the attacker and intercepting any web traffic.

As a result, the attacker intercepts NTLM authentication attempts and utilizes an NTLM relay attack. The attacker can then relay these credentials to other systems, such as an LDAP(Lightweight Directory Access Protocol) server, and gain unauthorized access to domain resources.

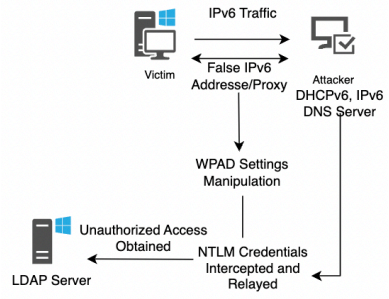

Figure 5: IPv6 DNS Takeover

B. *Security Operation Center Tools*

Effective cybersecurity defense lies in Security Operation Center(SOC) tools'. SOC tool's fundamental functions are to continuously monitor network traffic, detect, and analyze security incidents, and respond promptly to mitigate threats. SOCs' serve as an active defense in an organization's digital assets, combining advanced technologies such as Security Information Event Management(SIEM) solutions , intrusion detection systems(IDS), intrusion prevention systems(IPS). SOC tools also provide an indispensable contribution to safeguarding organizations by aggregating vast amount of data and events from security tools across the entire organization to identify suspicious patterns, providing security analysts with insights needed to identify, detect, and respond to potential security threats[4].

Common SOC Tools

Navigating the landscape of SOC operations requires a comprehensive understanding of the tools that enable security professionals to identify, detect, and respond to potential security network threats. These tools include SIEM and Endpoint Detection and Response platforms such as Elastic Security deployed on Elastic Cloud which utilizes Elasticsearch, Kibana, and Logstash (ELK Stack) to aggregate and collect data from multiple devices. It also offers the ability to integrate and aggregate data from other security solutions within a network such as Elastic Defend, Sysmon, OPNsense firewall, and Snort IDS. Each of these security solutions provide powerful network security capabilities for intrusion detection and endpoint response, providing a vital role in contributing to a SOC's ability to quickly identify assets, detect, and respond to threats including MitM attacks.

Challenges and Limitations of SOC tools

As powerful as they may be, SOC tools also face challenges and limitations leading to concerns related to accuracy, scalability, and adaptability. In terms of accuracy, SOC tools heavily rely on automated detection mechanisms, including signature-based detection and anomaly detection algorithms[5]. However, they can produce false positives, mistakenly identifying benign activities as security threats and false negatives. This overwhelms security analysts with a great number of alerts potentially leading to reduced efficiency in responding to real threats.

Moreover, scalability poses also a significant challenge, particularly for organizations experiencing a rapid growth in managing extensive network infrastructures. Ensuring SOC tools can efficiently handle the escalating volume of data, traffic, and event logs is important to maintain their effectiveness as a SOC.

C. *Red Team Engagements*

As mentioned before, red team engagements are common for assessing an organization's security posture. Red team engagements simulate a real world cyber attack, serving as a proactive approach to identifying vulnerabilities and weaknesses within an organization's network. By adopting the perspective of an adversary, red teams challenge an organization's defenses in order to reveal potential areas of improvement[3]. This is accomplished using a range of tactics, techniques, and procedures(TTPs) that replicate real world adversaries. Engagements of this nature often include MitM attack scenarios in an Active Directory environment. In doing so this also serves as a measure of an organizations defense capabilities of their SOC and provide organizations and SOC teams with actionable insights into their network's security weaknesses. Understanding how these engagements are executed allows security professionals to better prepare for and defend against MitM attacks an other sophisticated cyber threats[8].

III. DESIGN AND METHODOLOGY

In the methodology section of this document, an outline of the configuration and procedures used to analyze the factors influencing the success of MitM dropbox attacks against various SOC tools in an Active Directory environment is provided. This section also details the network environment, configuration and deployment of the MitM dropbox devices, and the SOC solutions used. By bridging the insights from the literature with a hands-on implementation, a valuable contribution is provided to the understanding of MitM attacks' effectiveness against SOC tools in the context of a red team engagement where physical access is obtained and the red team operator has implanted a dropbox into the internal Active Directory environment.

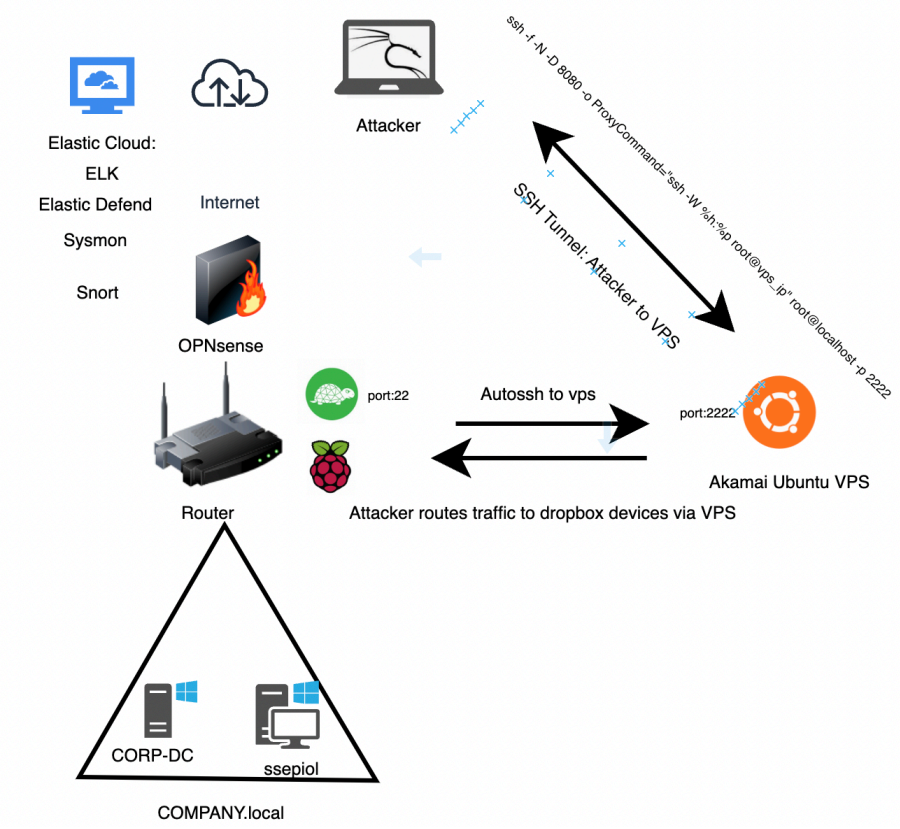

Figure 6: Network Design

A. Network Design

The internal network design for this research consists of two virtual machines using VMware Player that are apart of the COMPANY.local:

- Windows Server 2022 Domain Controller(CORP-DC)
- Windows 10 Enterprise Workstation(ssepiol)

The dropbox devices planted as MitM devices consist of two devices:

- Hak5's LAN Turtle
- Raspberry Pi 4 Model B

Elastic cloud utilizes ELK stack to collect and aggregate data from the logs of the following SOC tools monitoring the Active Directory agents enrolled into Elastic Cloud

- Elastic Defend
- Sysmon
- OPNsense
- Snort

In this network design as shown above in Figure 6, two dropbox devices are configured to autossh to a Virtual Private Server(VPS) once connected to an ethernet port or switch on the internal network, mapping port 22 on the dropbox to port 2222 on the VPS, this allows an attacker or red team operator to SSH into their VPS from a attack device on a different network as shown in Figure 7, and from there access the dropbox device from the VPS using "root@localhost -p 2222" as shown in Figure 8. As a proof of concept, Figure 9 shows the internal network CIDR notation that the dropbox is deployed in. The Raspberry Pi 4 is also configured in this way , allowing itself to be accessible to the attacker and red team operator by using autossh and a VPS.

Figure 7: SSH from the attack machine to the VPS

Figure 8: SSH from the VPS to the LAN Turtle

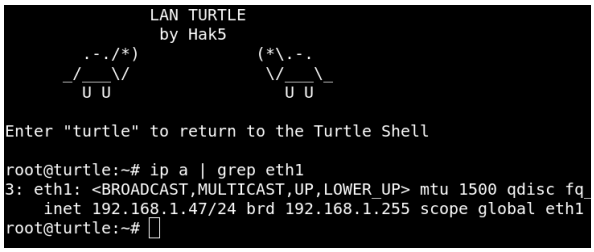

Figure 9: Internal Network CIDR

An alternative to using SSH twice on the attack machine, the attacker or red team operator can route their attack machine traffic using a dynamic application-level port

forwarding proxy such as SOCKS(Socket Secure) proxy on the local machine and tunnel traffic through the first SSH connection, which is from the attacker machine to the VPS, and then the second SSH connection, which is from the VPS to the dropbox device. As shown in Figure 11 the command to do so is: ssh -f -N -D 8080 -o ProxyCommands="ssh -W %h:%p root @vps_ip" root@ localhost -p 2222. Routing traffic through a SOCKS proxy by specifying the port to use in the "/etc/proxychains.conf" file as shown in Figure 10 allows for the use of proxychains to route traffic and attacks through the SSH tunnels and potentially evade detection. Accessing either dropbox via ssh or tunneling traffic are viable options for this methodology.

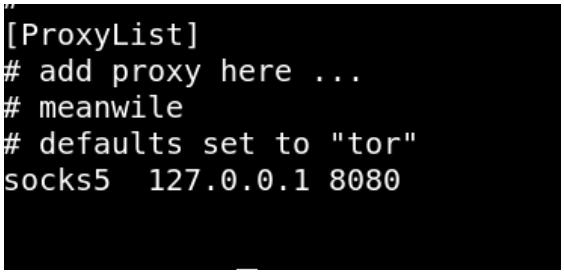

Figure 10: /etc/proxychains.conf

In order for Elastic Cloud to collect and aggregate data from the logs of SOC tools running as services on the Active Directory machines in the internal network, the devices are first enrolled as agents as shown in Figure 14. Once they are enrolled as agents, an agent policy is created for each individual machine, as shown in Figure 15, integrating Elastic Defend, Windows Sysmon, OPNsense, and Snort logs are sent to the ELK stack for further analysis and aggregation.

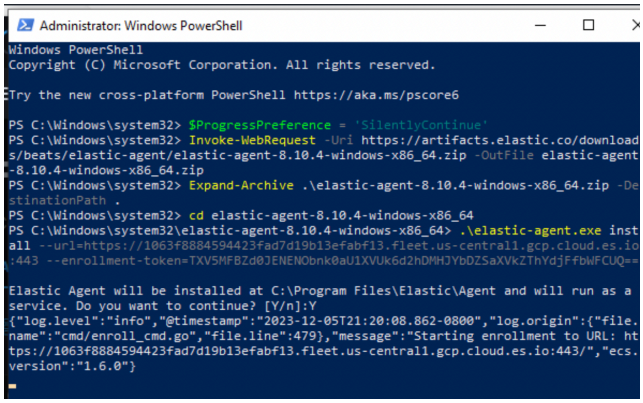

Figure 14: Elastic Agent installation on AD Windows Machine

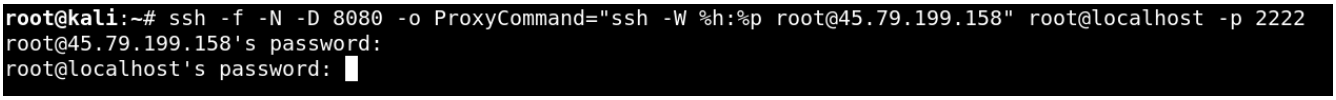

Figure 11: SSH one liner routing attack machine traffic through VPS to the LAN Turtle

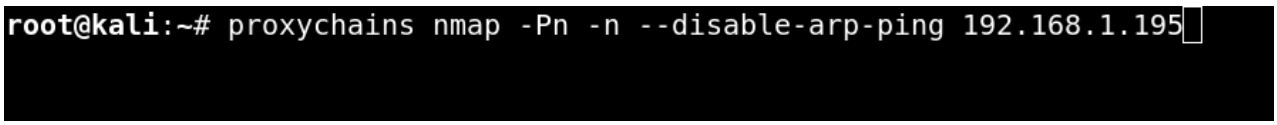

Figure 12: proxychains test command with nmap

Figure 13: Test Nmap results of a device in the internal network

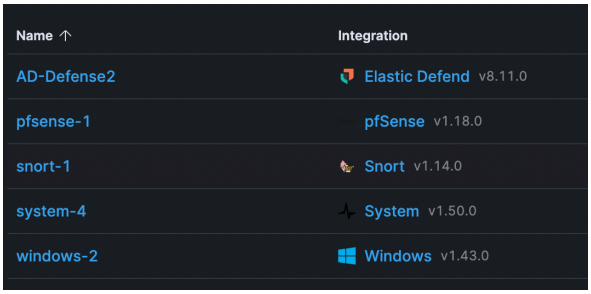

Figure 15: Policy Integrations for AD agents(pfSense includes OPNsense)

$$Mean(\bar{X}) = \frac{\sum_{i=1}^{n} x_i}{n} \quad (1)$$

- x_i represents individual data points
- n represents the total number of data points

$$Standard\ Deviation(\sigma) = \sqrt{\frac{\sum_{i=1}^{n} (x_i - \bar{X})^2}{(n-1)}} \quad (2)$$

- $\bar{X}$ is the mean
- x_i are the individual data points

Figure 16: Mean and Standard Deviation Formulas

$$t = \frac{(\bar{X}_1 - \bar{X}_2)}{\sqrt{\frac{s_1^2}{n_1} + \frac{s_2^2}{n_2}}} \quad (3)$$

- Group 1: MitM attacks conducted using the LAN Turtle device
- Group 2: MitM Attacks conducted using the Raspberry Pi 4 device
- $\bar{X}_1$ and $\bar{X}_2$ are the sample means of Group 1 and Group 2
- s_1^2 and s_2^2 are the sample variances of Group 1 and Group 2
- n_1 and n_2 represent the sample sizes of Group 1 and Group 2

Figure 17: T-test formula

B. *Variables and Metrics*

In order to investigate the efficacy of MitM attacks devices along side the effectiveness of SOC tools in detecting these attacks. The independent variable involves the attack types of MitM devices performed using the LAN Turtle and Raspberry Pi 4 dropbox devices. The dependent variables include the evasion effectiveness and success rates of MitM attacks. Success rate of each MitM attack used by the different dropbox devices quantifies the effectiveness of the MitM attack in achieving the objective of intercepting and or manipulating network traffic as an attacker would. The evasion effectiveness against SOC tools is measured by the proportion of the total amount of times the SOC tool was able to successfully detect an attack executed by one of the dropbox devices. Several hypotheses are formulated for this research.

Firstly, the null hypothesis is that there is no variability among the success rates of different attacks. The alternate hypothesis is that there is some inconsistency among the success rates of different attacks. Note, the MitM attacks' command execution is consistent across both dropbox devices, only the attack type varies.

Secondly, the null hypothesis is that there is are no varying levels of effectiveness in SOC tools in detecting MitM attacks across different dropbox devices. The alternate hypothesis is that SOC tools exhibit varying levels of effectiveness in detecting MitM attacks across different dropbox devices.

Finally, the null hypothesis is that there is no significant difference between the effectiveness between the two dropbox devices. The alternate hypothesis is that there is a difference in the success rates of MitM attacks between LAN Turtle and Raspberry Pi devices across different attack types. Analysis for this research includes descriptive statistics and t-tests to interpret, understand, and reach conclusions based on the data collected after executing the MitM attacks on each dropbox device.

Descriptive statistics summarize and present the dataset employing measures such as mean and standard deviation. For instance, computations will include determining the mean success rate for attacks executed on each dropbox device and evasion rates for each device. The formulas for these measures are shown in Figure 16. T-tests are also performed to compare the mean success rates between the LAN Turtle and Raspberry Pi 4 for all attack types and are shown in Figure 17.

To measure these variables a series of MitM attack scenarios are conducted using both the LAN Turtle and Raspberry Pi 4 devices. The LAN Turtle will execute all attacks first while the SOC tools monitor the Active Directory environment, collect data, and send it to the ELK stack where it is then aggregated. Then the Raspberry Pi 4 device will execute the exact same attacks while the SOC tools monitor the Active Directory environment, collect data, and send it to the ELK stack where it is then aggregated.

C. *Man-in-the-Middle Attacks*

Several MitM attacks were outlined earlier in this research, all of which are utilized in the internal network environment, targeting the Windows Active Directory environment consisting of a Domain Controller "CORP-DC" and the workstation user "ssepiol". The following attacks are executed on the internal network using the dropbox device: ARP Poisoning, DNS Cache Poisoning, LLMNR Poisoning, NTLM Relay Attack, and IPv6 DNS

Takeover. All of which achieve the objective of intercepting sensitive information and or manipulating network traffic as an attacker would. First an attacker would enumerate the target network, identifying any vulnerable hosts.

```
root@turtle:~# nmap -sn 192.168.1.47/24
Starting Nmap 7.70 ( https://nmap.org ) at 2023-1
Stats: 0:00:01 elapsed; 0 hosts completed (0 up),
ARP Ping Scan Timing: About 7.45% done; ETC: 02:3
Nmap scan report for 192.168.1.1
Host is up (-0.17s latency).
MAC Address: 34:53:D2:C4:DE:FA (Unknown)
Nmap scan report for 192.168.1.13
Host is up (-0.077s latency).
MAC Address: 5C:E0:C5:80:08:72 (Intel Corporate)
Nmap scan report for 192.168.1.95
Host is up (0.21s latency).
MAC Address: 4C:C9:5E:43:1B:06 (Unknown)
Nmap scan report for 192.168.1.101
Host is up (-0.069s latency).
MAC Address: 5C:E0:C5:80:08:72 (Intel Corporate)
Nmap scan report for 192.168.1.126
Host is up (0.010s latency).
MAC Address: E6:91:AE:C6:6D:AF (Unknown)
Nmap scan report for 192.168.1.180
Host is up (0.010s latency).
MAC Address: 5C:E0:C5:80:08:72 (Intel Corporate)
Nmap scan report for 192.168.1.230
Host is up (0.011s latency).
MAC Address: BC:D0:74:0F:86:4D (Unknown)
Nmap scan report for 192.168.1.47
Host is up.
```

Figure 18: Host Discovery using Nmap

After identifying the domain controller and the workstation internal IP addresses, they can be further enumerated to see what ports are open.

```
Nmap scan report for 192.168.1.13
Host is up (0.0055s latency).
Not shown: 988 filtered ports
PORT     STATE SERVICE
53/tcp   open  domain
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
5357/tcp open  wsdapi
MAC Address: 5C:E0:C5:80:08:72 (Intel Corporate)
```

Figure 19: CORP-DC Port Scan

The LAN Turtle Responder module can then be started to begin intercepting any NTLM authentication in the internal network and execute an LLMNR Poisoning attack.

This results in captured NTLM hashes as shown below:

An NTLM Relay Attack is also used, in this case SMB signing must be disabled for this attack to be successful.Using ntlmrelayx.py in conjunction with

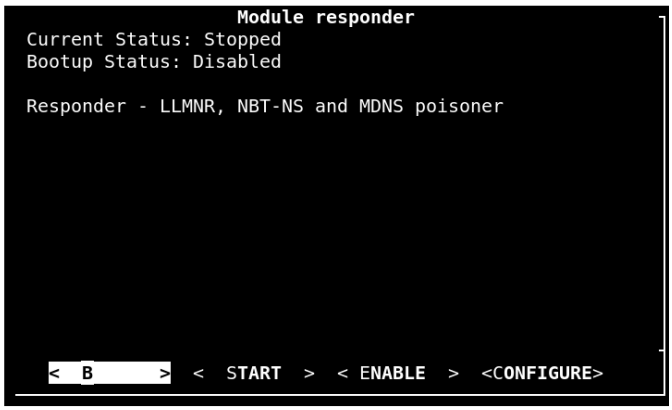

Figure 20: LAN Turtle Responder Module

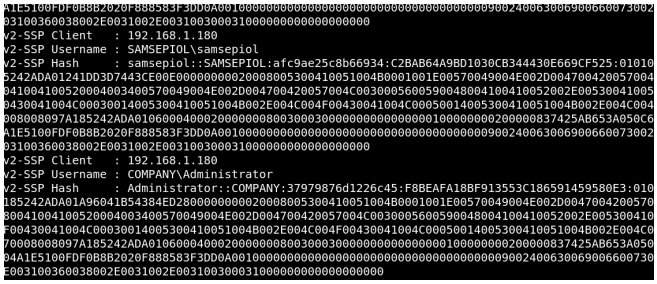

Figure 21: Captured NTLMv2 Hashes

responder allows for this attack to be executed, but once again, SMB signing enabled and required will not enable us to successful execute this attack unless it is disabled intentionally.

This results in a connection received by the local admin ssepiol as shown below:

```
$ ntlmrelayx.py -tf targets.txt -smb2support
```

Figure 22: ntlmrelayx.py usage

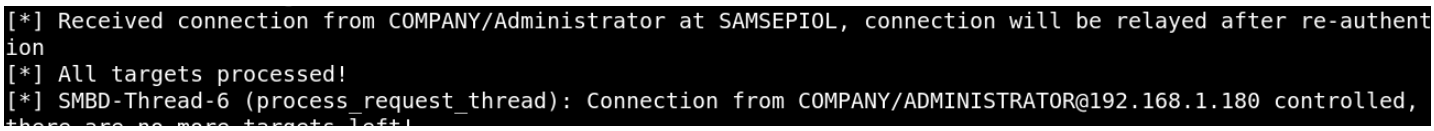

Figure 23: connection received from ssepiol in a NTLM Relay Attack

Finally, another attack executed is an IPv6 take over attack used with mitm6 and ntlmrelayx to once again obtain NTLM credentials and obtain unauthorized access to a machine as shown below:

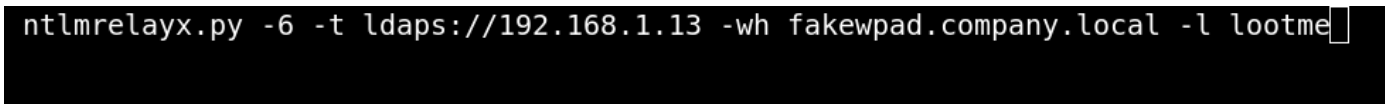

Figure 24: ntlmrelayx usage in IPv6 DNS Takeover Attack

Figure 25: mitm6 usage in IPv6 DNS Takeover Attack

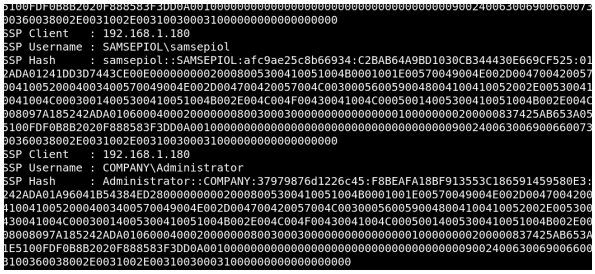

Figure 26: NTLMv2 Hashes Captured

IV. RESULTS

A. Data Collection and Analysis

For the standard deviation of success rates, the standard deviation measures the amount of variability among the success rates of different attack types/devices. Recall the null hypothesis is that there is no variability among the success rates of different attacks. The alternate hypothesis is that there is some inconsistency among the success rates of different attacks.A larger standard deviation suggests more variability or inconsistency among the success rates for different attacks. A smaller standard deviation indicates that the success rates are closer to the average success rate and that there is less variability among the attack types/devices. Utilizing aggregate data collection and python libraries the following can be visualized.

The standard deviation for Detection percentages measures the variability among the percentages of successful detections by SOC tools for different devices because the attacks are executed exactly the same on both devices. Recall hypothesis the null hypothesis is that there is are no varying levels of effectiveness in SOC tools in detecting MitM attacks across different dropbox devices. The alternate hypothesis is that SOC tools exhibit varying levels of effectiveness in detecting MitM attacks across different dropbox devices. A larger standard deviation in the detection percentages suggests more inconsistency in the effectiveness of SOC tools in detecting attacks common from different devices. A smaller standard deviation implies that the SOC tools' detection rates are more consistent across both devices using the same attacks. Utilizing data from Table 2, a python script visualizes the standard deviation as shown below:

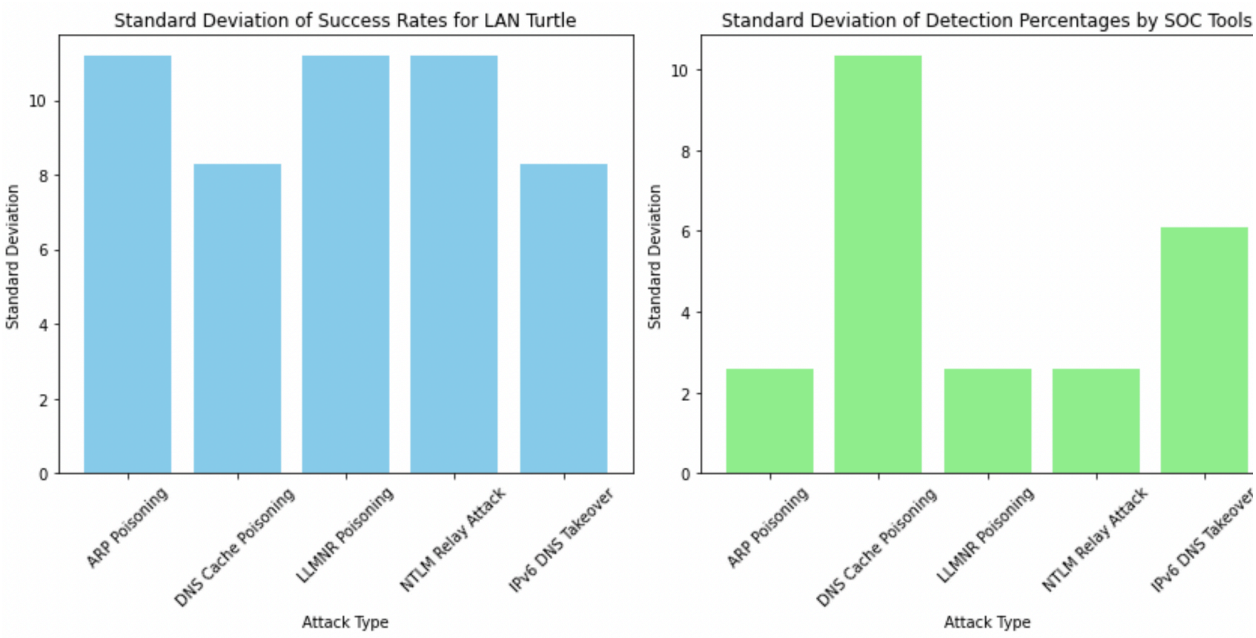

Figure 26: Standard Deviation of Success Rates and Detection Percentage by SOC Tools for the LAN Turtle

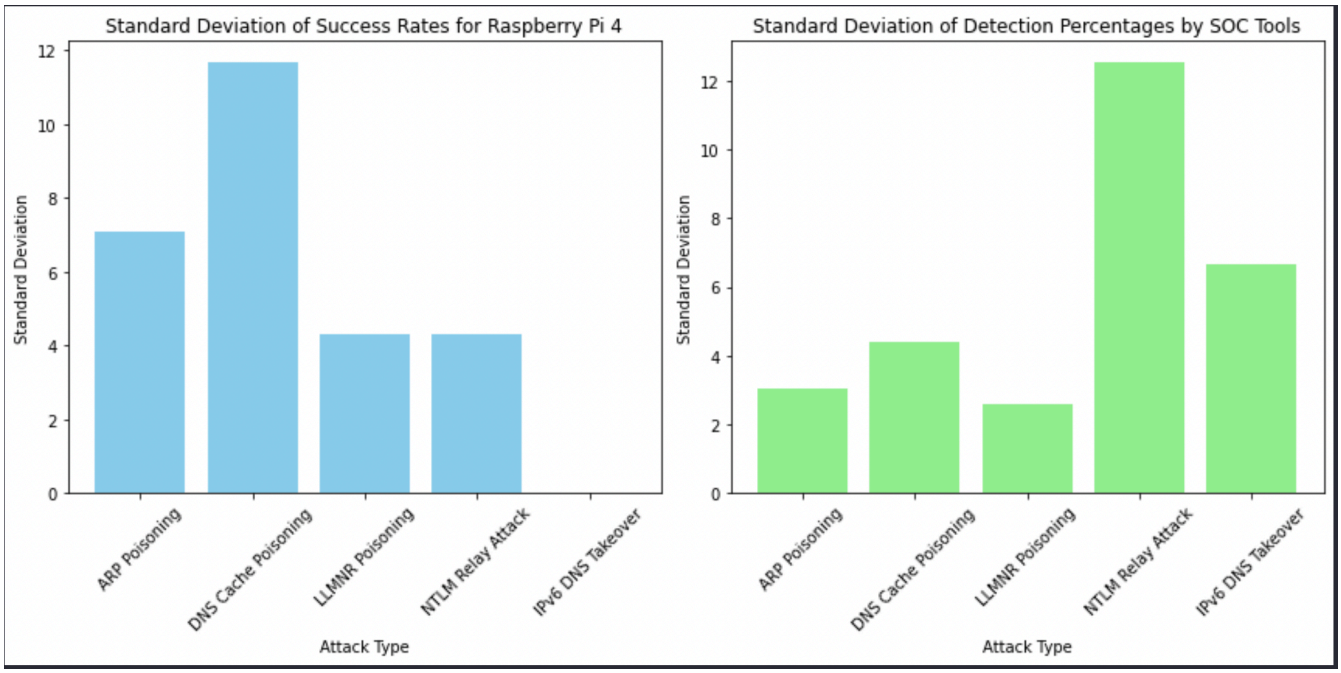

Figure 27:Standard Deviation of Success Rates and Detection Percentage by SOC tools for the Raspberry Pi 4

I. TABLE 1: DETECTION BY SOC TOOLS

Attack Type	*LAN Turtle Detection(%)*	*Raspberry Pi 4 Detection(%)*
ARP Poisoning	30.21	25.57
DNS Cache Poisoning	93.46	47.13
LLMNR Poisoning	25.32	27.14
NTLM Relay Attack	27.34	92.58
IPv6 DNS Takeover	63.29	61.51

II. TABLE 2: ATTACK SUCCESS RATES

Attack Type	*LAN Turtle(%)*	*Raspberry Pi 4 (%)*
ARP Poisoning	38	85
DNS Cache Poisoning	23	88
LLMNR Poisoning	63	92
NTLM Relay Attack	73	95
IPv6 DNS Takeover	48	98

T-tests were also used to compare the mean success rates between the LAN Turtle and Raspberry Pi 4 for all attack types. Also utilizing Python libraries to visualize the data and the mean success rates of the dropbox devices across multiple attack types. As shown below, the result of t-test indicate whether or not there is or there is not a significant difference when it comes to the success rates of MitM attacks between the LAN Turtle and Raspberry Pi. Across all attack types, there is a significant difference when it comes to the attack being executed on the Raspberry Pi 4.

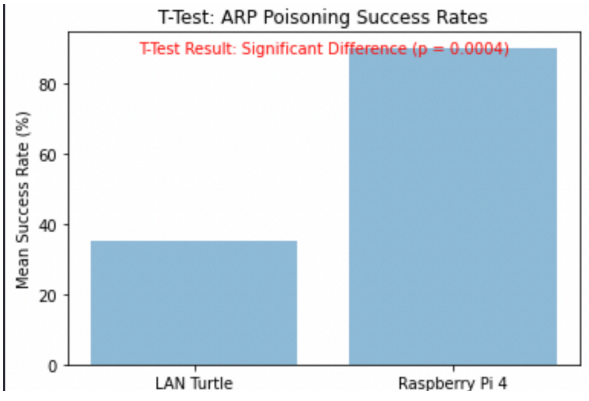

Figure 28: T-tests for ARP-Poisoning Success Rates

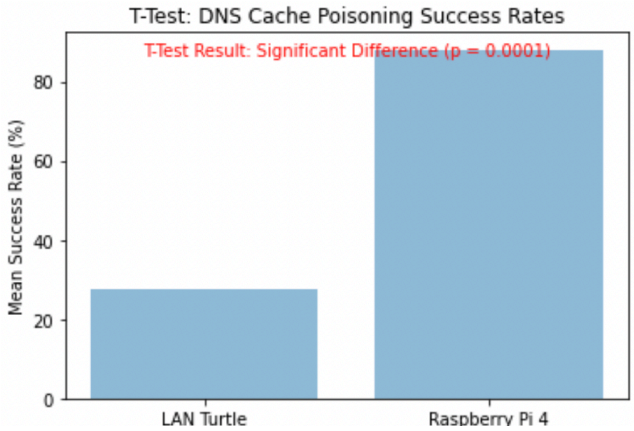

Figure 29: T-tests for DNS Cache Poisoning Success Rates

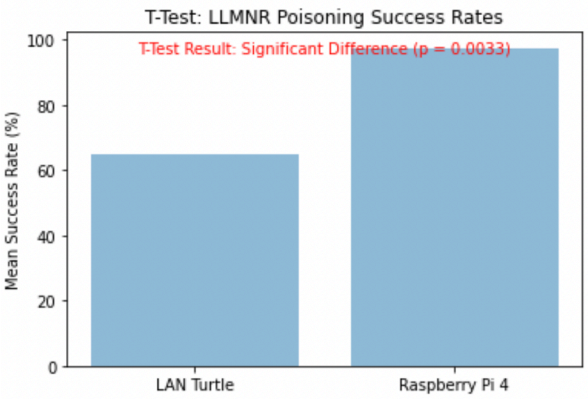

Figure 30: T-tests for LLMNR Poisoning Success Rates

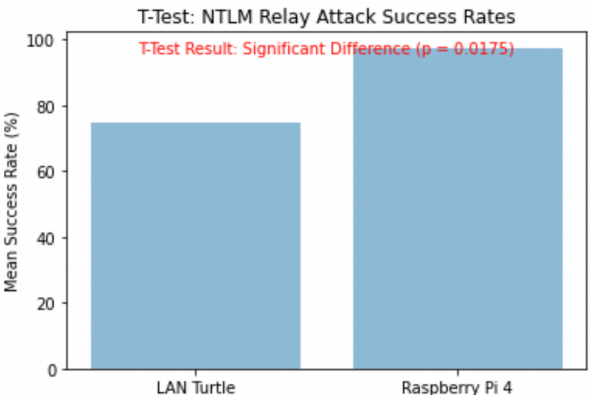

Figure 31: T-tests for NTLM Relay Attack Success Rates

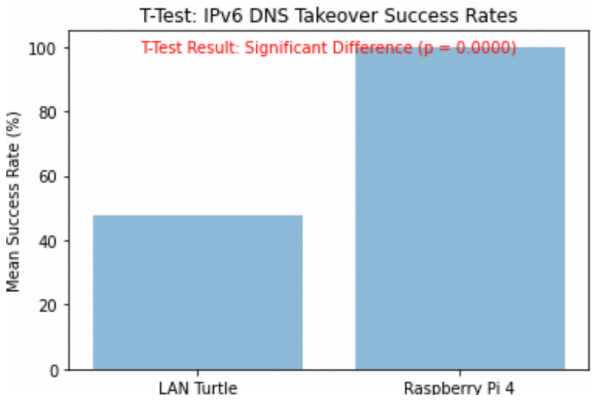

Figure 32: T-tests for IPv6 DNS Takeover Success Rates

V. CONCLUSION

In summary, this document analyzed the effectiveness of Man-in-the-Middle (MitM) Dropbox attacks and their evasion capabilities when scrutinized against a diverse array of Security Operation Center (SOC) tools. The primary inquiry revolved around examining the factors influencing the success of various MitM attacks and evasion techniques during red team engagements against different SOC tools. To address this, a real-world Windows Active Directory environment was deployed alongside Elastic Cloud's Security Information and Event Management, overseeing the network. Within this setup, a Windows 2022 Server served as the domain controller, accompanied by a Windows 10 Enterprise VM. MitM attacks were executed using two distinct devices: Hak5's LAN Turtle, known for MitM attacks and network persistence, and a custom Raspberry Pi 4. The research provided practical insights into the effectiveness of MitM attacks against SOC tools, bridging the gap between red team engagement strategies utilizing Dropbox devices and the efficiency of SOC tools. Ultimately, this study aimed to equip cybersecurity professionals with valuable insights to enhance defenses against such evolving attack methodologies.

REFERENCES

1. Georgios Gerontakis, Ioannis, Voyiatzis, Panayiotis Yannakopoulous. 2023. Security Operations Center in Education: Building an Educational Environment for Attack and Defense Scenarios. https://dl.acm.org/~3575879.3575962
2. Javeed, Danish & Mohammed Badamasi, Umar. (2020). Man in the Middle Attacks: Analysis, Motivation and Prevention. International Journal of Computer Networks and Communications Security. 8. 52-58. 10.47277/IJCNCS/8(7)1.
3. Khushboo Amin, Dr. Priyanka Sharma. 2020. Red Team Analysis of Information Security Measures and Response, Volume 07(4).https://www.irjet.net/archives/V7/i4/IRJET-V7I4823.pdf
4. M. Vielberth, F. Böhm, I. Fichtinger and G. Pernul, "Security Operations Center: A Systematic Study and Open Challenges," in IEEE Access, vol. 8, pp. 227756-227779, 2020, doi: 10.1109/ACCESS.2020.3045514.
5. Mughal, A. A. (2022). Building and Securing the Modern Security Operations Center (SOC). International Journal of Business Intelligence and Big Data Analytics, 5(1), 1–15. Retrieved from https://research.tensorgate.org/~ /21
6. Ronnie Swanink. 2016. Persistent effects of man-in-the-middle attacks, https://www.cs.ru.nl/bachelors-theses/2015/Ronnie_Swanink___4382838___Persistent-effects-of-man-in-the-middle-attacks.pdf
7. Team, H. (2020, April 3). *From Zero Credentials to Full Domain Compromise*. ExploitDB. https://www.exploit-db.com/docs/48282
8. Yanalitis, M. (2014, January). *Red teaming approach rationale and risks - researchgate*. RED TEAMING APPROACH, RATIONAL, AND RISKS.https://www.researchgate.net/profile/Mark-Yanalitis-2/publication259546738_Red_Teaming_Approach_Rationale_and_Risks/links0c96052c6e6a18dd8e000000/Red-Teaming-Approach-Rationale-and-Risks.pdf?origin=publication_detail