Name: Anil Budthapa

Student ID: 12230757

Task 2: Attack

Scope: Win2022VM (192.168.56.50)

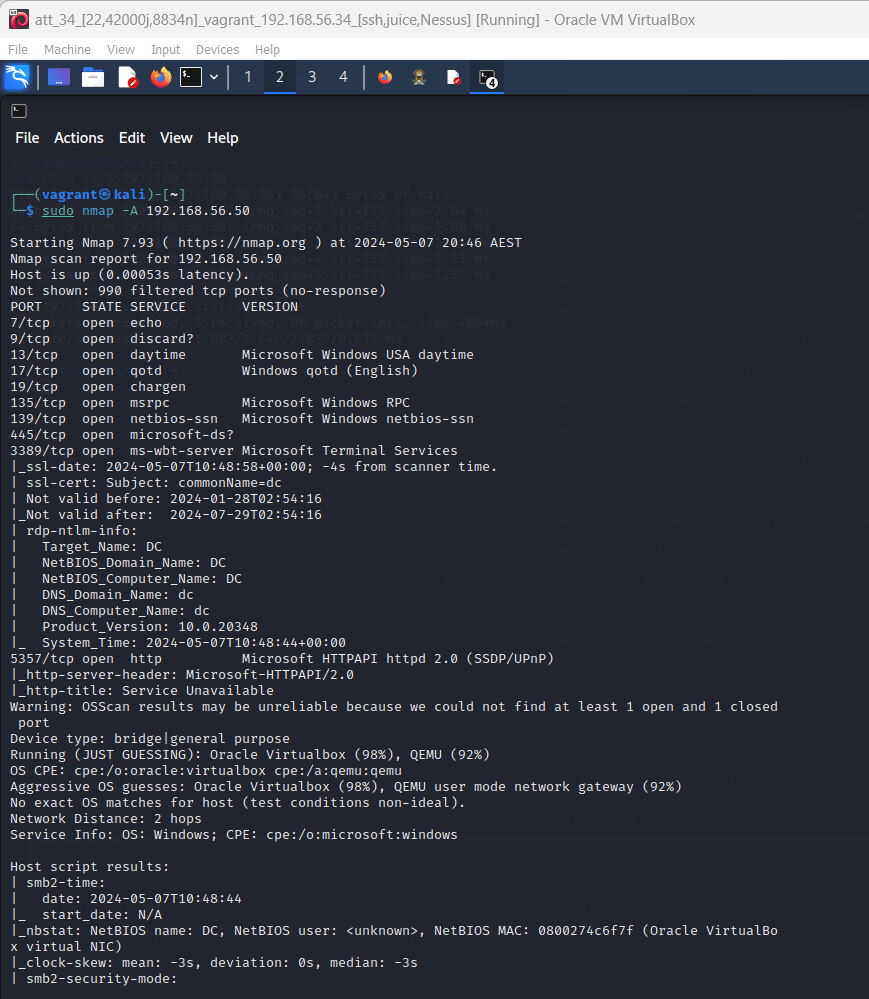
Github Link: <https://github.com/anilH3inso/anil.win2022>

**Task A: Scanning All nodes.**

First I setup two machines in my Oracle VM’s which are kali(Custom) and Win2022(venerable ) then we install another file ` [coit11241/office\_2019.exe at main · jamieshield/coit11241 · GitHub](https://github.com/jamieshield/coit11241/blob/main/office_2019.exe)` which is a kind of malicious file on Win2022 that makes more vulnerable to that system. Now, I will use three different tools for Scanning all nodes of host. i.e 192.168.50.56

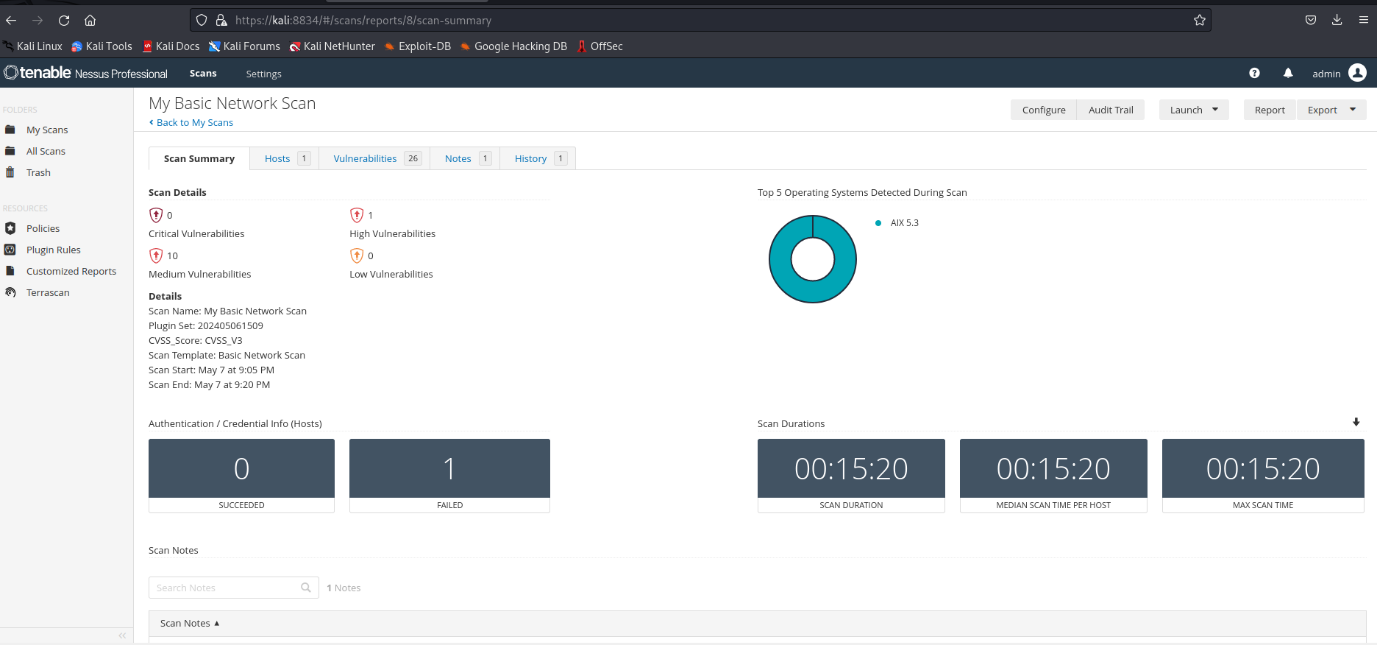
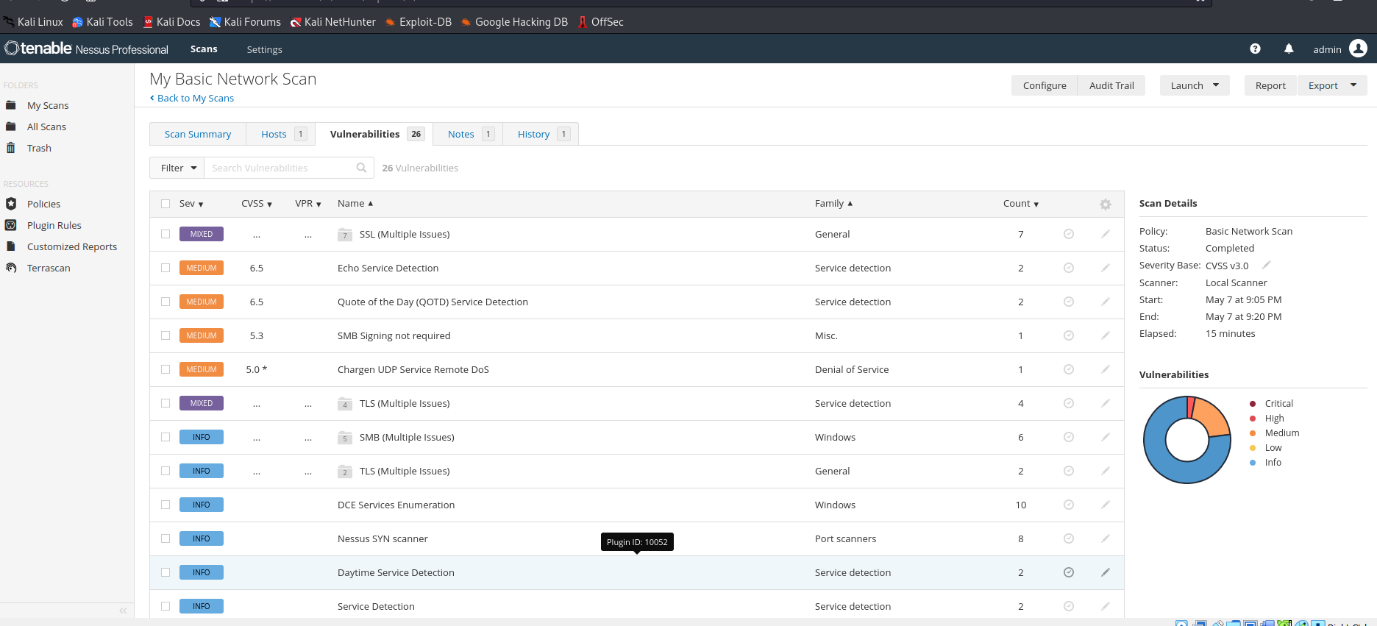
1. Nmap

Command – nmap -A 192.168.50.56



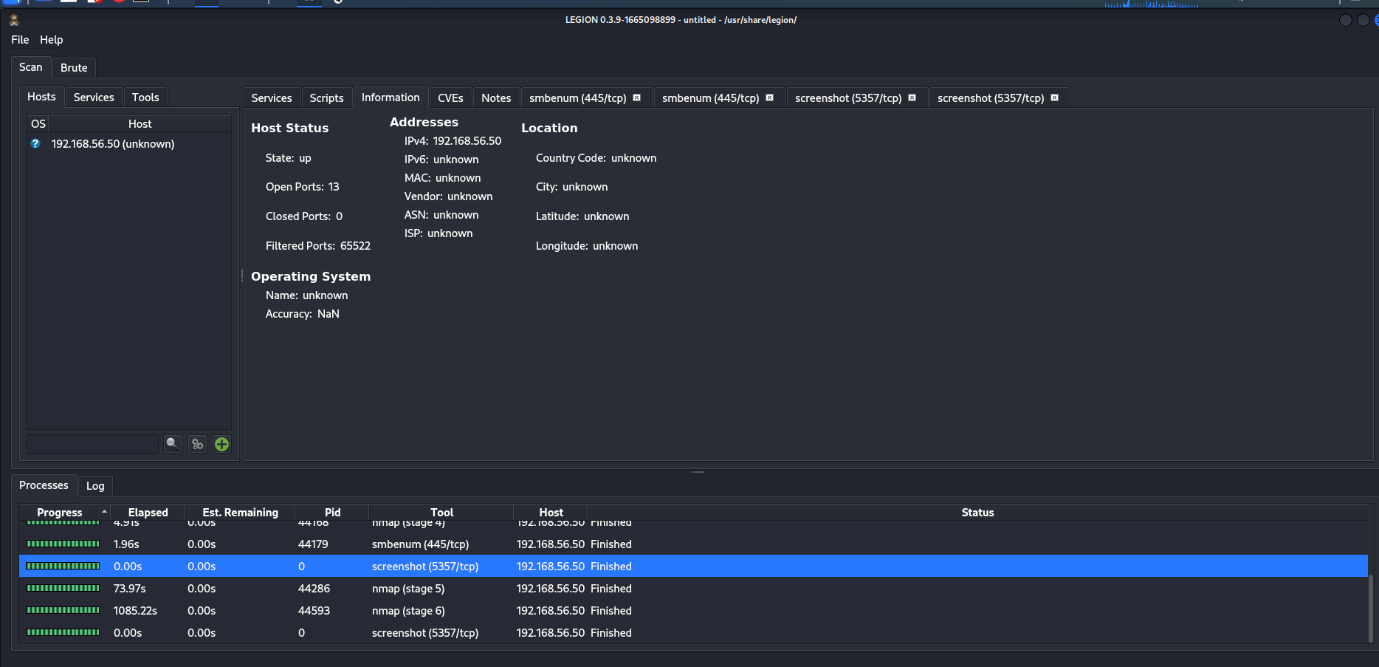
GitHub link: <https://github.com/anilH3inso/anil.win2022/tree/main/nmap>

1. Nessus



GitHub Link: <https://github.com/anilH3inso/anil.win2022/tree/main/Nessus>

1. Legion(root)

A screenshot of a computer

Description automatically generated

GitHub link: <https://github.com/anilH3inso/anil.win2022/tree/main/Legion>

**Task B: Write an Intel Report.**

**Intel Report: Identifying Top 5 ATT&CK Codes Post MedusaLocker Ransomware Attack**

*Prepared by: Anil Budthapa, Cybersecurity Analyst, Kadac Australia*

*Date: April 8,2024*

**Executive Summary:**

Following the recent ransomware attack by the threat actor (TA) Medusa on Kadac Australia, it is imperative to assess the attack surface and identify the most crucial ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) codes employed by the adversary. Understanding these techniques will facilitate proactive mitigation strategies and strengthen our cybersecurity posture.

**1. Reconnaissance (ATT&CK ID: T1590):**

Medusa likely conducted extensive reconnaissance activities to identify vulnerabilities within Kadac Australia's network infrastructure. This includes scanning for open ports, identifying services running on these ports, and gathering information about the organization's systems and applications. Detection and response mechanisms should be enhanced to identify and thwart reconnaissance attempts effectively.

**2. Credential Access (ATT&CK ID: T1110):**

Once initial access was established, Medusa sought to escalate privileges and obtain valid credentials to move laterally within the network. Credential access techniques such as password spraying, brute force attacks, or exploiting weak credentials might have been employed. Strengthening password policies, implementing multi-factor authentication (MFA), and conducting regular credential audits are essential to mitigate this threat.

**3. Execution (ATT&CK ID: T1059):**

Medusa utilized various methods to execute malicious payloads across Kadac Australia's network. This could involve leveraging legitimate applications and processes or executing files through remote services. Endpoint detection and response (EDR) solutions should be deployed to monitor and block suspicious execution attempts effectively.

**4. Defense Evasion (ATT&CK ID: T1562):**

To evade detection by security controls, Medusa likely employed tactics to obfuscate malicious payloads and disguise their activities. This could include using encryption, packing, or other techniques to conceal malware from antivirus solutions and security monitoring tools. Implementing behavior-based detection mechanisms and regularly updating antivirus signatures can enhance defense evasion resilience.

**5. Impact (ATT&CK ID: T1486):**

The ultimate objective of the MedusaLocker ransomware attack was to disrupt Kadac Australia's operations and extort ransom payments. The impact extended beyond data encryption, potentially causing downtime, financial losses, and reputational damage. Robust data backup strategies, incident response plans, and employee training on ransomware awareness are critical to mitigating the impact of future attacks.

**Conclusion:**

Identifying and prioritizing the top 5 ATT&CK codes utilized by Medusa in the ransomware attack on Kadac Australia provides valuable insights for enhancing our cybersecurity defenses. By focusing on reconnaissance, credential access, execution, defense evasion, and impact mitigation strategies, we can fortify our resilience against similar threats in the future.

**Recommendations:**

1. Conduct a comprehensive review of network security controls and implement measures to detect and prevent reconnaissance activities.
2. Enhance password management practices, enforce strong authentication mechanisms, and conduct regular credential audits.
3. Deploy endpoint detection and response (EDR) solutions to monitor and block malicious execution attempts.
4. Implement behavior-based detection mechanisms and update antivirus solutions to mitigate defense evasion tactics.
5. Develop and test incident response plans, including data backup and recovery procedures, to minimize the impact of ransomware attacks.

*This report is intended for internal use only and should not be distributed outside of authorized personnel.*

* 1. **Medusa’s Lifecycle** This is the summary of Medusa lifecycle.

Medusa’s main aim is to steal the credentials from the victim host. Medusa achieves this aim by (1) Gathering information by using various Sub techniques of reconnaissance ATT&CK ID: T1590 : [T1590.001](https://attack.mitre.org/techniques/T1590/001), [T1590.002](https://attack.mitre.org/techniques/T1590/002), [T1590.003](https://attack.mitre.org/techniques/T1590/003), [T1590.004](https://attack.mitre.org/techniques/T1590/004), [T1590.005](https://attack.mitre.org/techniques/T1590/005), [T1590.006](https://attack.mitre.org/techniques/T1590/006) where they do  [Active Scanning](https://attack.mitre.org/techniques/T1595) or [Phishing for Information](https://attack.mitre.org/techniques/T1598) by this way it gain initial access then it (2) brute force **. Credential Access (ATT&CK ID: T1110):** using this   
Sub-techniques:  [T1110.001](https://attack.mitre.org/techniques/T1110/001), [T1110.002](https://attack.mitre.org/techniques/T1110/002), [T1110.003](https://attack.mitre.org/techniques/T1110/003), [T1110.004](https://attack.mitre.org/techniques/T1110/004) to get credential data as we did in task 1. After this (3) **Execution (ATT&CK ID: T1059):** take place by using   
Sub-techniques:  [T1059.001](https://attack.mitre.org/techniques/T1059/001), [T1059.002](https://attack.mitre.org/techniques/T1059/002), [T1059.003](https://attack.mitre.org/techniques/T1059/003), [T1059.004](https://attack.mitre.org/techniques/T1059/004), [T1059.005](https://attack.mitre.org/techniques/T1059/005), [T1059.006](https://attack.mitre.org/techniques/T1059/006), [T1059.007](https://attack.mitre.org/techniques/T1059/007), [T1059.008](https://attack.mitre.org/techniques/T1059/008), [T1059.009](https://attack.mitre.org/techniques/T1059/009), [T1059.010](https://attack.mitre.org/techniques/T1059/010) which help in execution of file through remote access then (4) it will do **Defense Evasion (ATT&CK ID: T1562):** to bypass the security of host. It also use various   
Sub-techniques:  [T1562.001](https://attack.mitre.org/techniques/T1562/001), [T1562.002](https://attack.mitre.org/techniques/T1562/002), [T1562.003](https://attack.mitre.org/techniques/T1562/003), [T1562.004](https://attack.mitre.org/techniques/T1562/004), [T1562.006](https://attack.mitre.org/techniques/T1562/006), [T1562.007](https://attack.mitre.org/techniques/T1562/007), [T1562.008](https://attack.mitre.org/techniques/T1562/008), [T1562.009](https://attack.mitre.org/techniques/T1562/009), [T1562.010](https://attack.mitre.org/techniques/T1562/010), [T1562.011](https://attack.mitre.org/techniques/T1562/011), [T1562.012](https://attack.mitre.org/techniques/T1562/012) then (5) the impact **Impact (ATT&CK ID: T1486):** Of this attack is downtime, financial losses, and reputational damage.

1. Medusa’s initial access technique: T1590.002 Gather Victim Network Information: Domain Properties via Active scanning like [WHOIS](https://attack.mitre.org/techniques/T1596/002) .
2. Now, try to get credential access with [T1110.001](https://attack.mitre.org/techniques/T1110/001) - Brute Force: Password Guessing which use wide range of password like [passwdlist](https://github.com/scipag/password-list).
3. Now Command and Scripting Interpreter: AppleScript take place which is execution process with processID: T1059.002 .
4. Then bypass the host security with sub technique: [T1562.002](https://attack.mitre.org/techniques/T1562/002) Impair Defenses: Disable or Modify Tools which may take many forms, such as killing security software processes or services, modifying / deleting Registry keys or configuration files so that tools do not operate properly, or other methods to interfere with security tools scanning or reporting information. Adversaries may also disable updates to prevent the latest security patches from reaching tools on victim systems.
5. At last company have to face various consequences such as it encrypts data on target systems or on large numbers of systems in a network to interrupt availability to system and network resources. They can attempt to render stored data inaccessible by encrypting files or data on local and remote drives and withholding access to a decryption key.
   1. **Analysis of likelihood of CVE exploitation by Medusa.**

CVE-2017-0144 wannacry ransome with pattern EternalBlue is a remote code execution vulnerability

|  |  |  |  |
| --- | --- | --- | --- |
| CWE | CAPEC | ATT&CK | Used by BumbleBee |
| 200 | 165 Connection Proxy | [Connection Proxy, Technique T0884 - ICS](https://attack.mitre.org/techniques/T0884) | yes |
|  | 100 Exploitation of Authentication Vulnerability | [Exploitation for Credential Access, Technique T1212 - Enterprise](https://attack.mitre.org/techniques/T1212) | yes |
|  | 121 Command Injection | [Exploitation of Remote Services, Technique T1210 - Enterprise](https://attack.mitre.org/techniques/T1210) | yes |
|  |  | [OS Credential Dumping, Technique T1003 - Enterprise](https://attack.mitre.org/techniques/T1003) | yes |
|  |  | [Defense Evasion, Tactic TA0005 - Enterprise](https://attack.mitre.org/tactics/TA0005) | yes |
|  |  | [Execution, Tactic TA0002 - Enterprise](https://attack.mitre.org/tactics/TA0002) | yes |
|  |  | [Impact, Tactic TA0040 - Enterprise](https://attack.mitre.org/tactics/TA0040) | yes |

Task 4. Emulate Attack.

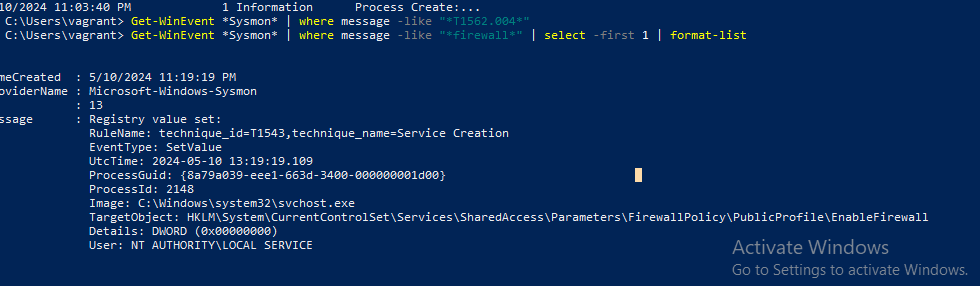
Attack 1. T1562.004 Disable Microsoft Firewall.

Attack command: Run with PowerShell or make script and execute in PowerShell

C:/ netsh advfirewall set currentprofile state off

Monitoring the attack through Sysmon

C:/Get-WinEvent \*Sysmon\* |where message -like “\* firewall \*” | Select -first 1 | format-list



Attack 2:

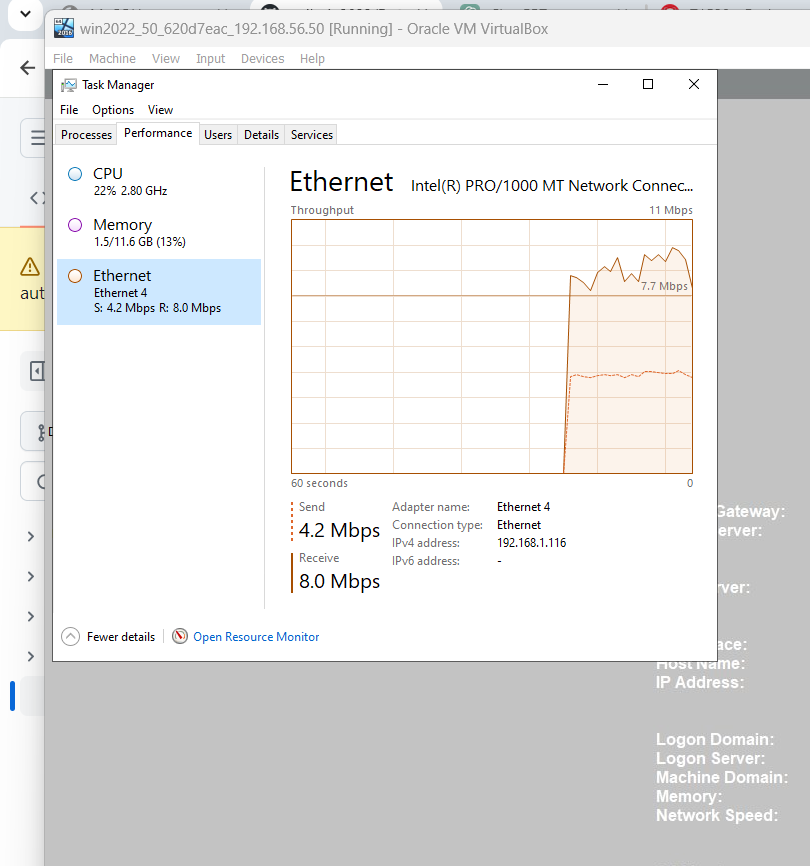
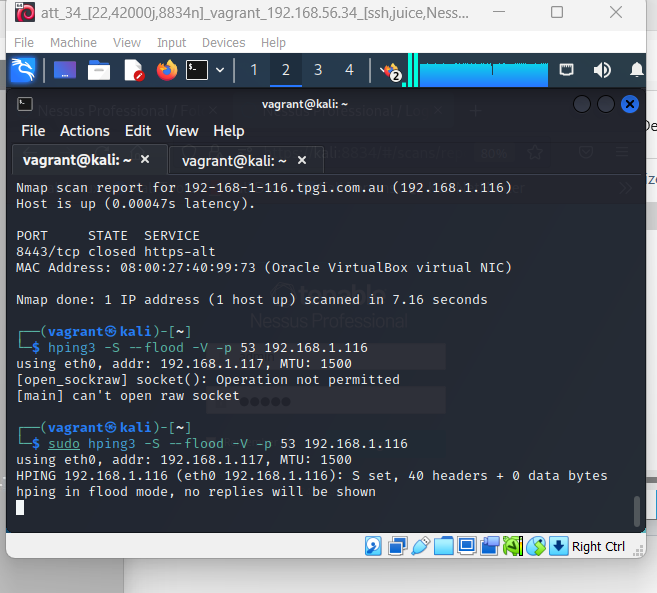
T1498.001 Direct Network Flood

from kali machine udp flooding that lead to ddos from udp smb signing not required.

root@kali: hping3 -S –flood -V -p 53 192.168.56.50

result : overflow of packet .

impact : slow your pc or stuck and use different



**REFERENCE:**

Atomic RED team, Accessed 7 April 2024, <https://atomicredteam.io/>

Mitre, Accessed 8 April 2024, <https://attack.mitre.org/>