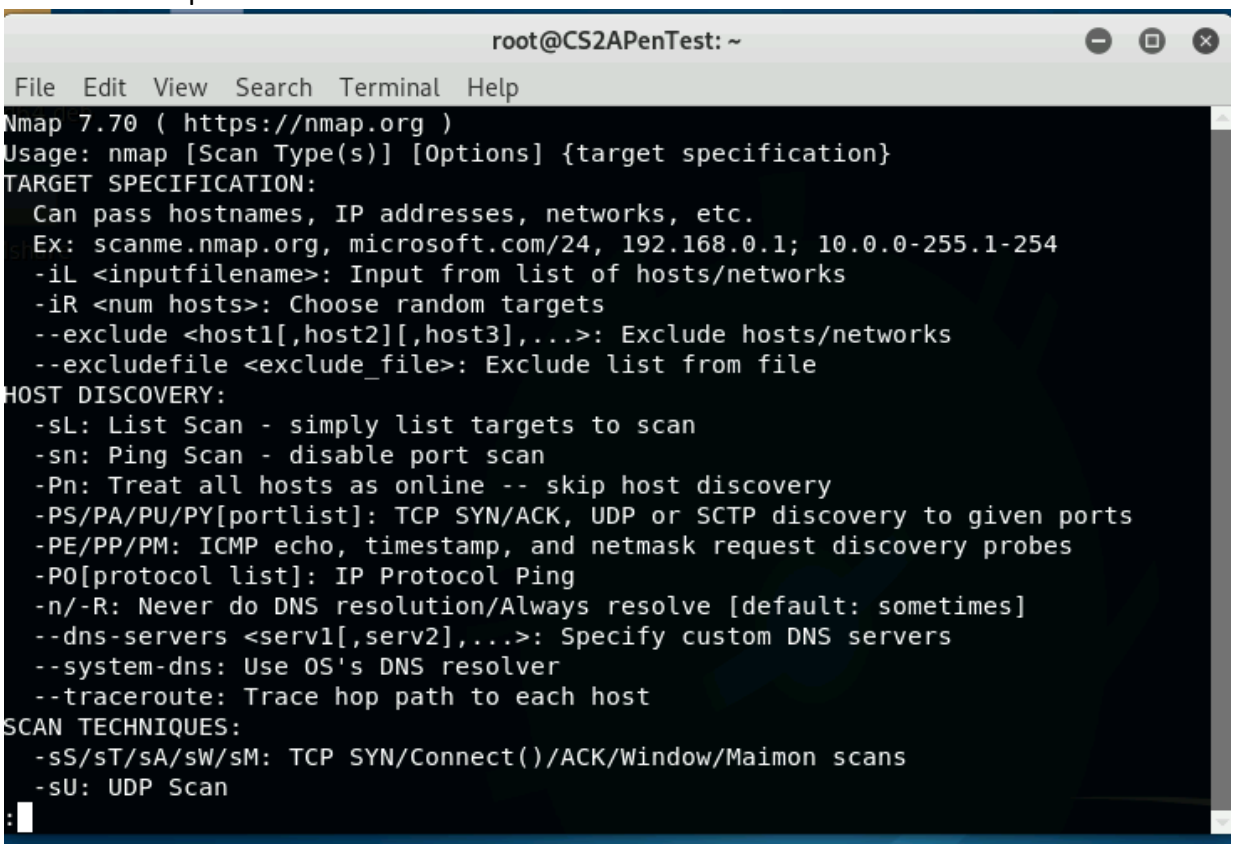
Assignment-4 -Vulnerability Scan

CYSE 450 -Ethical Hacking and Penetration Testing

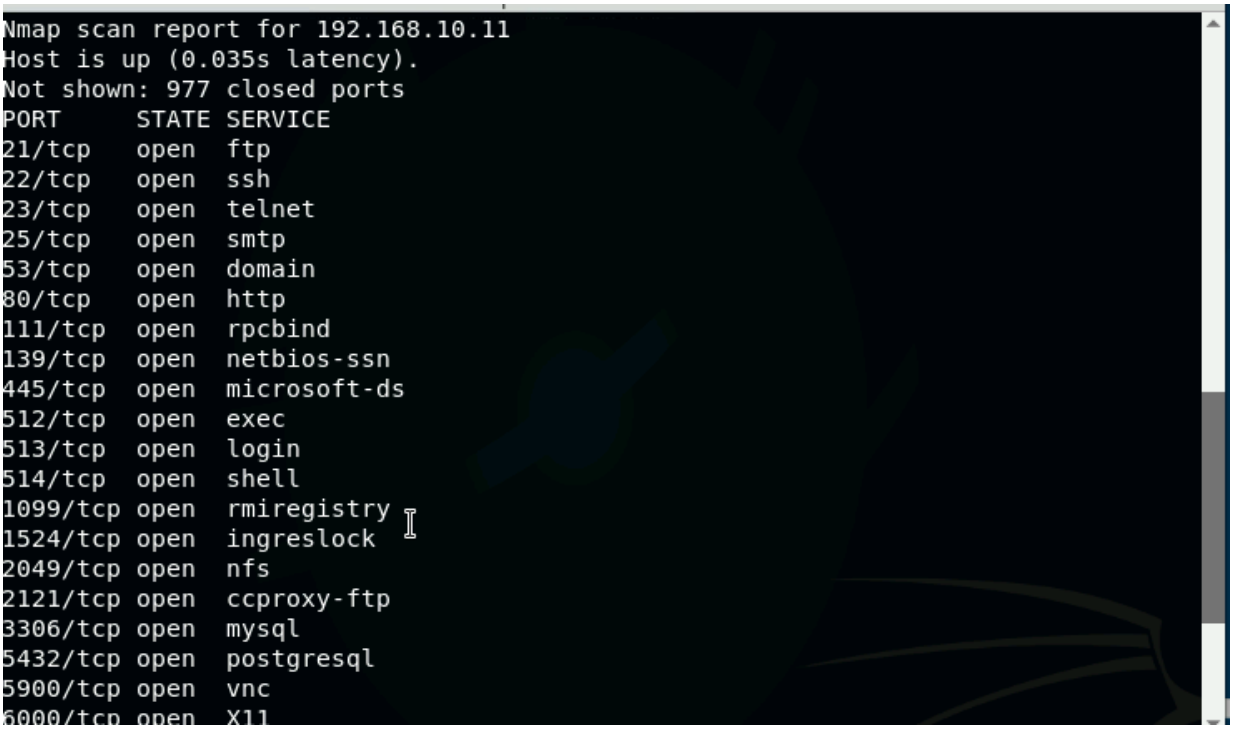
Task-A: Stealth Scan using nmap [40 Points]

1. Open the **Root Terminal** in Kali Linux. Type **nmap -h** | **less** and press **Enter** to see all available Nmap commands. Submit the screenshot for the results.



2. To send a SYN packet to an IP address of metasploitable 2 /Windows VM, type the following in Kali terminal.

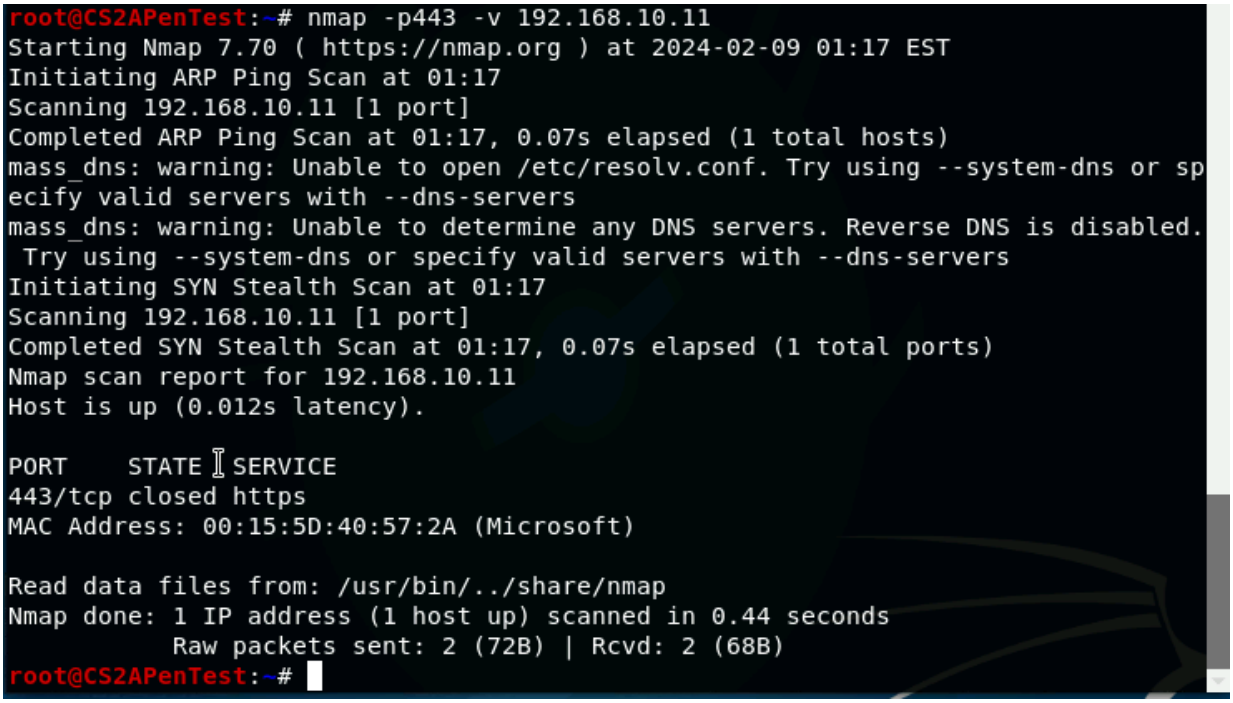
   nmap -sS -v <ip-of-metasploitableo or Windows VM> and press **Enter**.



nam

What are the results of your SYN scan? Submit the screenshot.

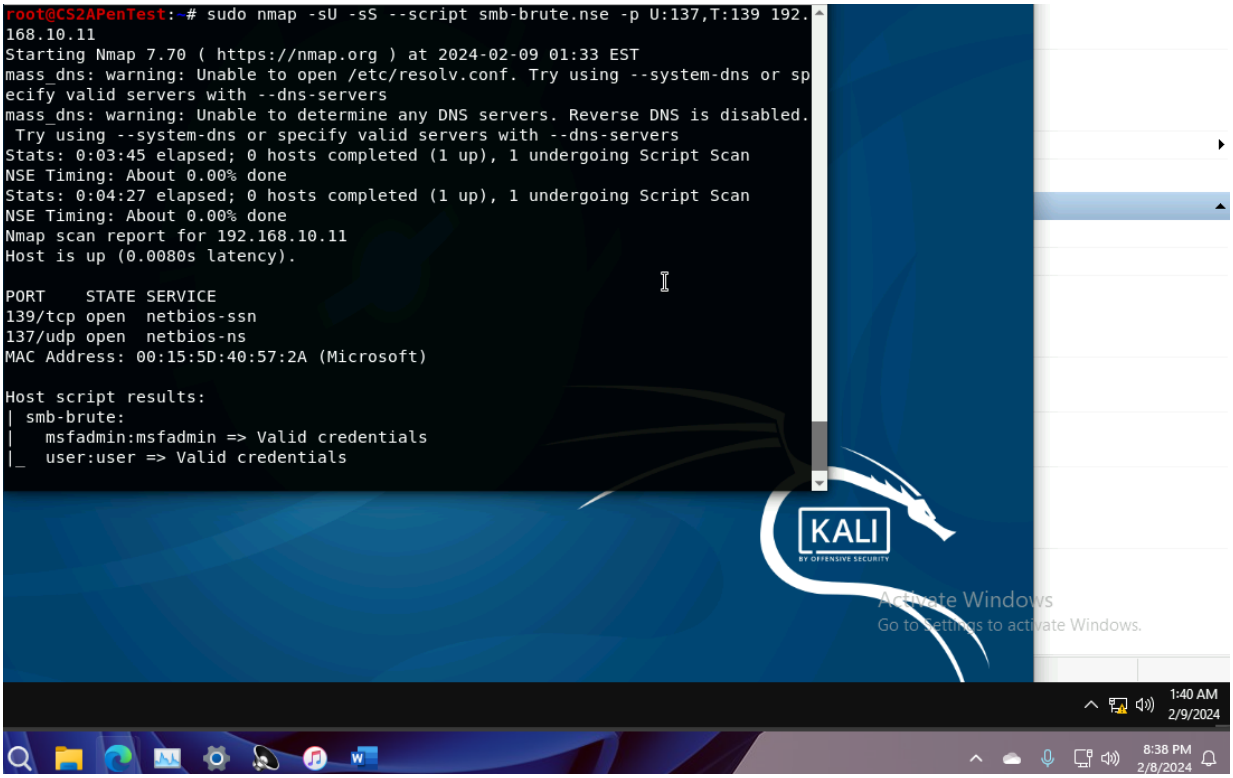
3. Limit the scope so you scan only port 443 by using the –p flag (**nmap –p44 3 –v ip-ofmetasploitable**). This makes the Nmap scan more targeted and less noticeable. Please submit the screenshot.



Task-B: Vulnerability Scan Using Nmap Script [20 Points]

1. Open the terminal in Kali Linux.
2. Using **nmap script** for brute force attack, scan the target machine (IP of Metasploitable or Windows) to guess its username/password.

   HINT: Please refer to the recording for the lecture (in Media Gallery on Canvas) and/or https://nmap.org/nsedoc/scripts/smb-brute.html



Task-C: Secure Hacking Environment [20 Points]

1. How can you create a secure hacking environment, using web-based proxy, as an attacker? Please explain with examples. Creating a secure hacking environment using a web-based proxy involves several steps to anonymize network traffic and hide the attacker's true IP address. To start, the attacker selects a reliable web-based proxy service that offers features such as HTTPS encryption, anonymity, and reliable uptime, such as TOR, ProxySite, HideMyAss, or CyberGhost. Once chosen, the attacker configures their web browser or network tools to use the selected web-based proxy, typically by entering the proxy server's address and port number in the network settings of the application. After configuring the proxy settings, the attacker verifies their anonymity by testing the connection to ensure that their traffic is being routed through the web-based proxy and that their real IP address is hidden. This can be done using online services like WhatIsMyIPAddress or IPLeak. With the secure hacking environment set up, the attacker can then proceed to conduct penetration testing, vulnerability assessments, or other security assessments against target systems, ensuring to follow ethical guidelines, obtain proper authorization, and respect the privacy and security of others at all times.
2. What is the purpose of using Macchanger tool in hacking?

The Macchanger tool, available on Unix-like operating systems such as Linux, serves the purpose of manipulating the MAC address of network interfaces. This unique identifier is assigned to network interfaces and changing it can provide anonymity and privacy, particularly in scenarios where network traffic monitoring or tracking based on MAC addresses is a concern. Macchanger is used primarily for anonymizing network traffic by changing the MAC address of the network interface, making it difficult for network administrators or attackers to track activities based on MAC addresses. It can also aid in evading MAC address filtering, a security measure implemented by some networks to only allow specific devices to connect. Macchanger allows users to spoof a MAC address that is allowed on the network, enabling unauthorized devices to connect. In penetration testing or ethical hacking scenarios, Macchanger can simulate different devices on a network, test network security controls, or bypass MAC address-based security mechanisms. However, it's essential to note that while Macchanger can provide anonymity and aid in certain hacking scenarios, its use must comply with legal and ethical standards. Unauthorized manipulation of MAC addresses or network interfaces may be illegal and unethical, necessitating proper authorization before using such tools in security assessments or penetration tests.