Branden Barnes

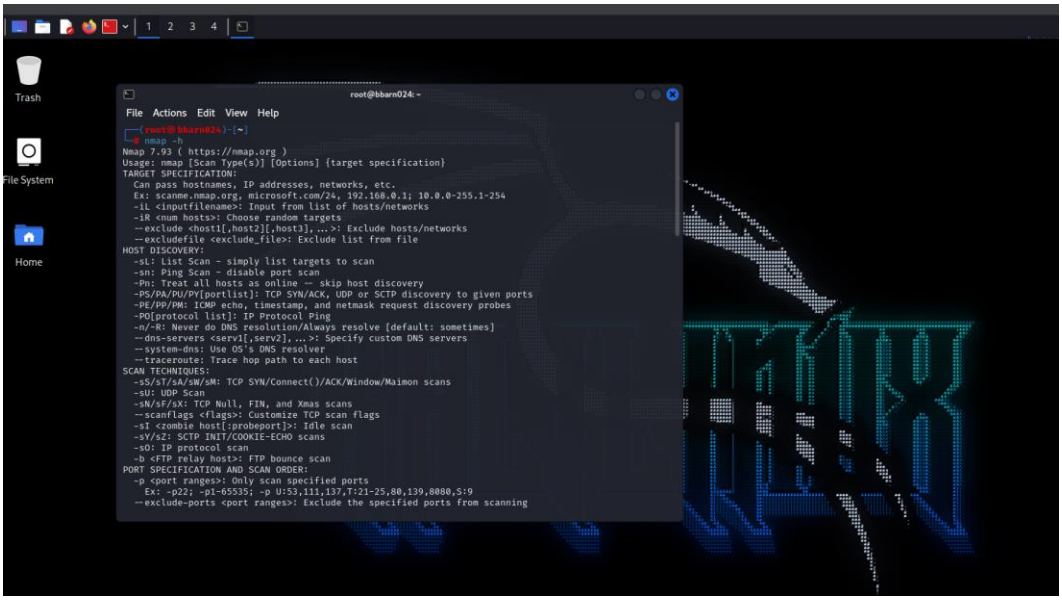
Professor Vatsa

CYSE 450

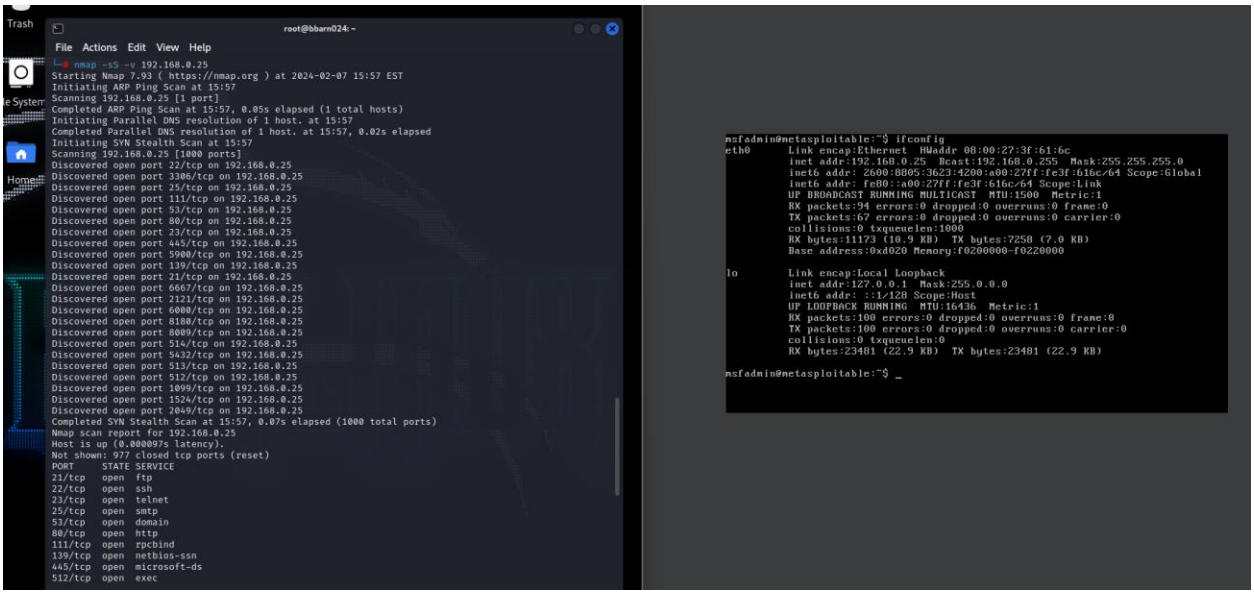
Vulnerability Scan

Task A: **Stealth Scan Using NMAP**

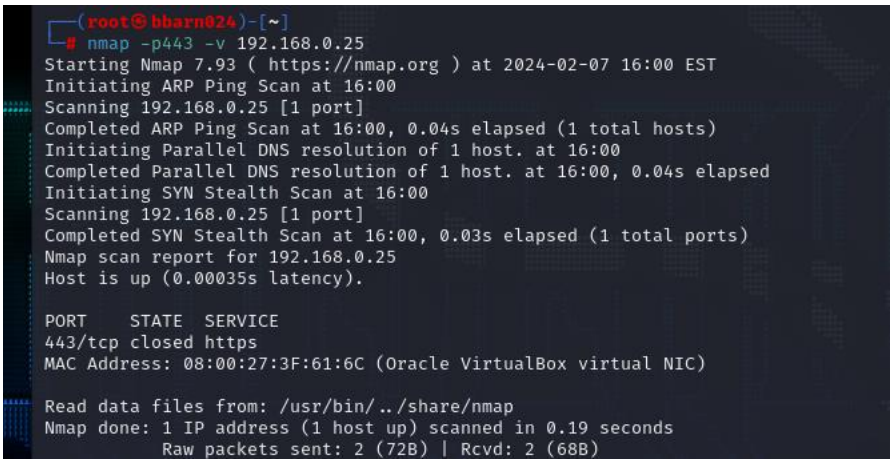
1. Open the Root Terminal in Kali Linux. Type nmap -h | less and press Enter to see all available Nmap commands



2. Send a SYN packet to an IP address of metasploitable 2/ Windows VM.



3. Limit the scope so only port 443 is scanned.



Task B: **Vulnerability Scan Using Nmap Script**

1. Open the Terminal in Kali Linux
2. Using nmap script for brute force attack, scan the target machine to guess its username/password

Task C: **Secure Hacking Environment**

1. To secure your web-based proxy, start with SSL connections. These connections are what secures transmissions involving encryption and decryption between servers. Enable SSL connections and establish a key ring database with a key ring password file. When configuring your proxy server into a forward proxy server, enable SSL Tunneling as to pass encrypted requests, but encrypted information is not cached. Choosing the proper proxy to use enhances your security and privacy in routing traffic. For example, the proxy server Squid, when you route your traffic through it, that proxy forwards your request on your behalf. You need to configure your proxy in a way that won't ping back to you from the internet. A tool for hackers to use is ProxyChains which force TCP connections to go through various proxies. This allows hackers to hide their IP address, run applications, and active/passive reconnaissance the local intranet from external proxy.
2. The Macchanger tool in hacking manipulates MAC addresses of network interfaces. Changing your MAC address frequently makes it very difficult to track your computer. GNU MAC Changer is a utility that can be programmed to feature many different specifics of your MAC address.