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**.

   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.
2. What is the purpose of using Macchanger tool in hacking?

Extra Credit Question:

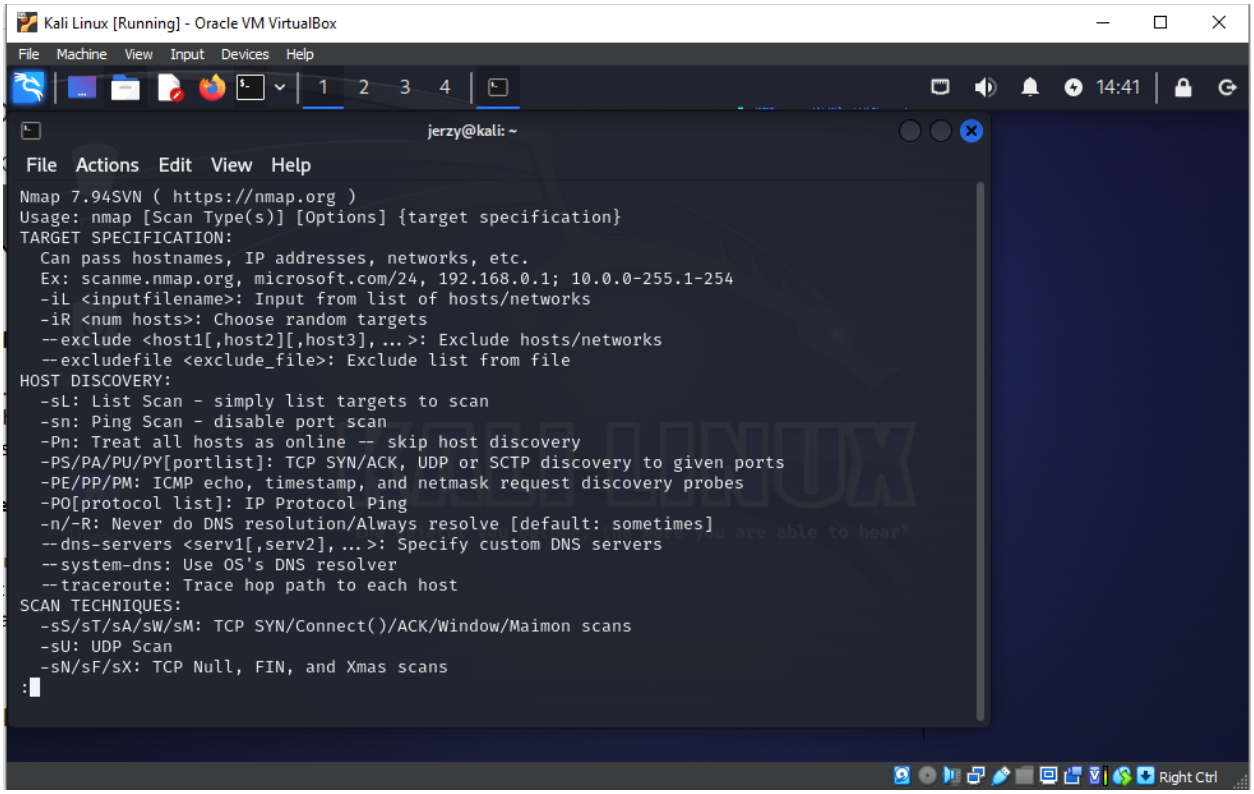
Research question [10 points]

1. Open your web browser and go to https://osintframework.com/.
2. Explore the framework by expanding nodes to discover different tools. Choose two tools. In 2-3 paragraphs describe what these two tools can do, how to use them, and how they would be useful in footprinting.

Note: Your Answer should contain 2-3 paragraphs, at least one paragraphs per tool chosen. The **name** of the tool, **website location**, **brief instructions**, and how the tool is useful in footprinting should be discussed.

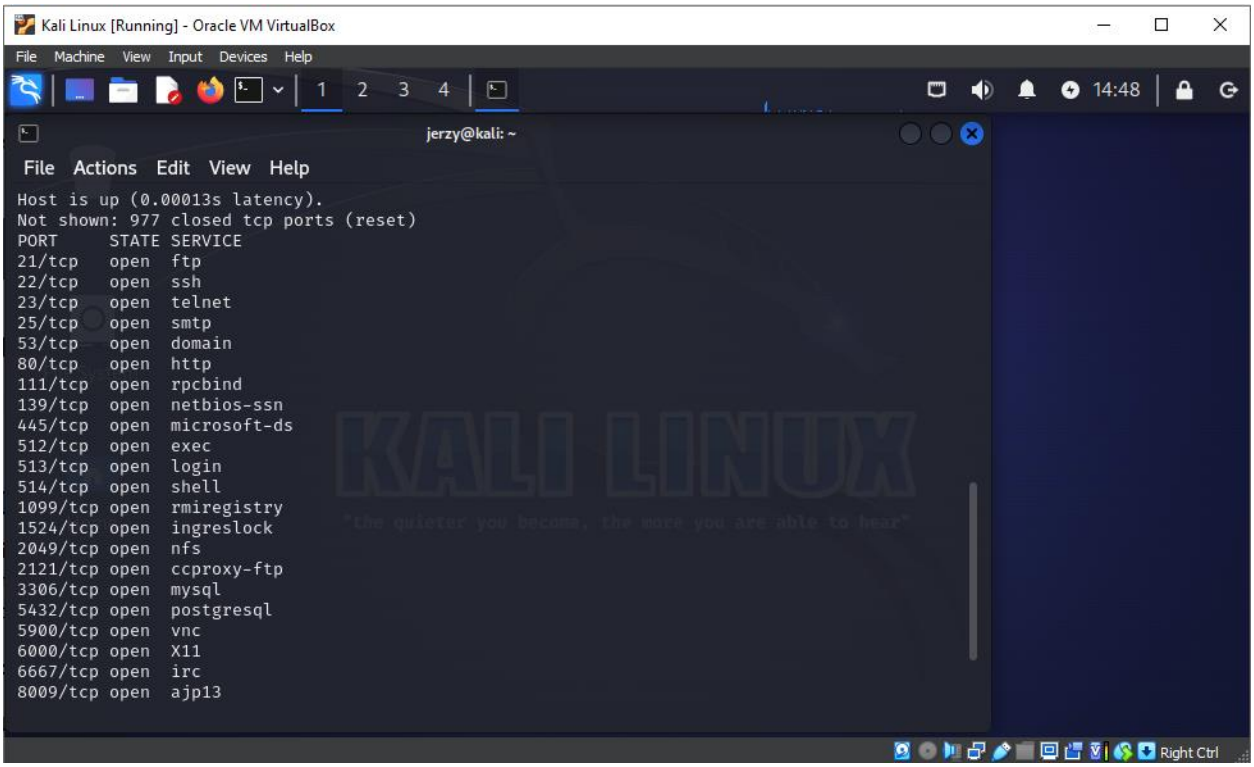
Task A

1.



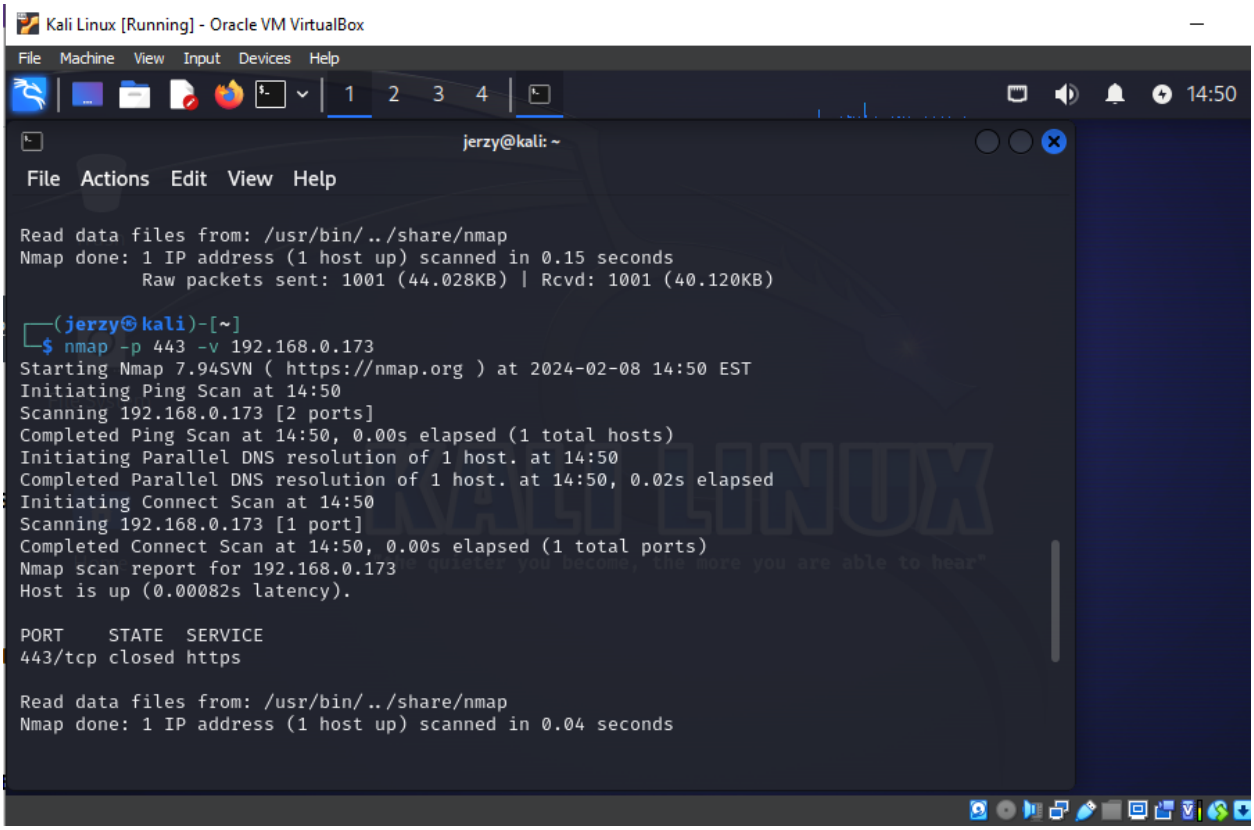
“nmap -h | less” was the exact command used

2.



Used “sudo nmap -sS -v 192.168.0.173”

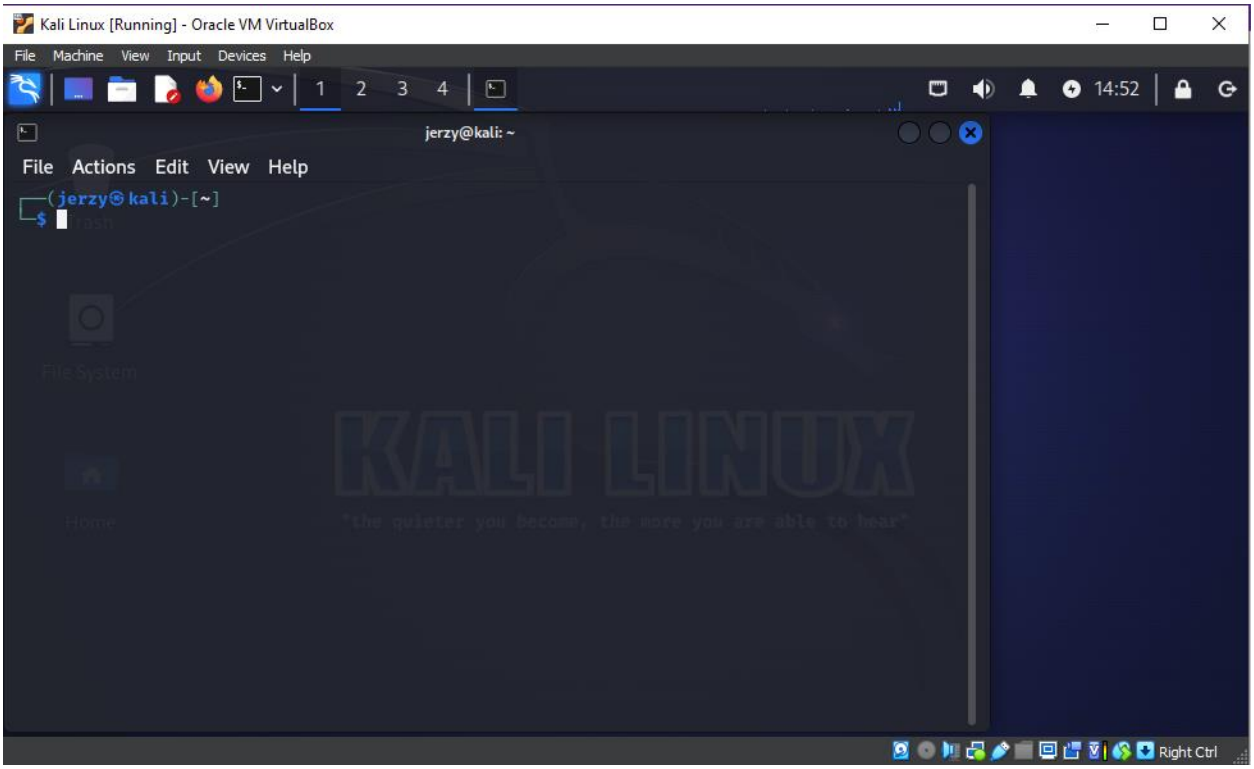
3.



Used “nmap -p 443 -v 192.168.0.173”

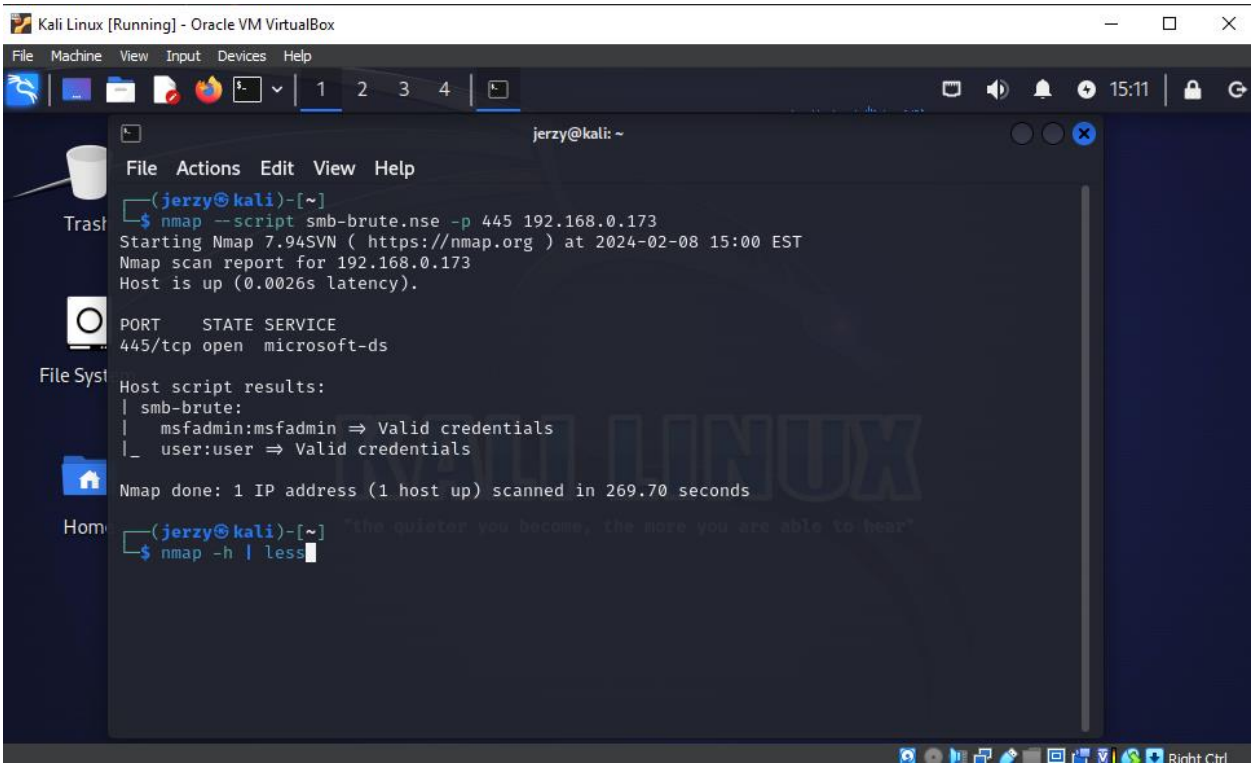
Task B

1.



I opened the terminal

2.



I used “nmap –script smb-brute.nse -p 445 192.168.0.173”
The credentials are displayed in the screenshot.

Task C

1.

Using proxy's essentially hides your IP address as your data uses the IP address of the proxy rather than your computers actual IP address. While this doesn't 100% guarantee that your activity cannot be traced back to you it significantly increases your anonymity. Additionally, you can use multiple proxy's to even further hide this. There are proxy plugins and applications that are available online. Using a VPN is also an option.

2.

Macchanger allows users to change their machines mac address. This is useful for impersonating other machines or to otherwise hide your real mac address. Useful for essentially the same reasons IP spoofing is useful.

Extra Credit

Photon is a data extraction tool used to grab URLs, files, strings, DNS related data, and other intel. You simply run the tool and direct it towards a URL and it will scrape together useful data. This tool is useful for foot printing because it catalogues all the data regarding a website including URLs, emails, keys, hashes, subdomains, files, and more.

https://github.com/s0md3v/Photon

Inquisitor is a tool for gathering information specifically regarding companies. It uses and compiles data publicly available about a company to extract even more information. It displays the relationships between a company's assets, employees, etc. For foot printing, this tool displays information such as employee LinkedIn and email, as well as other helpful information.

https://github.com/penafieljlm/inquisitor