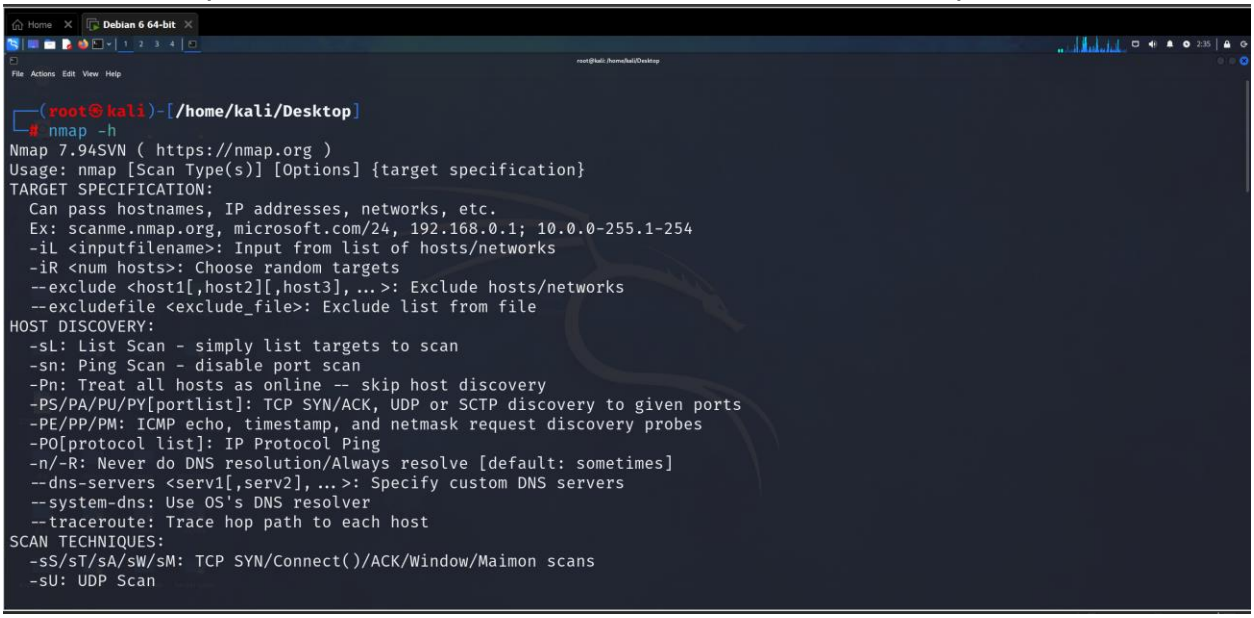
Activity 5-1: Getting to Know Nmap

Time Required: 30 minutes

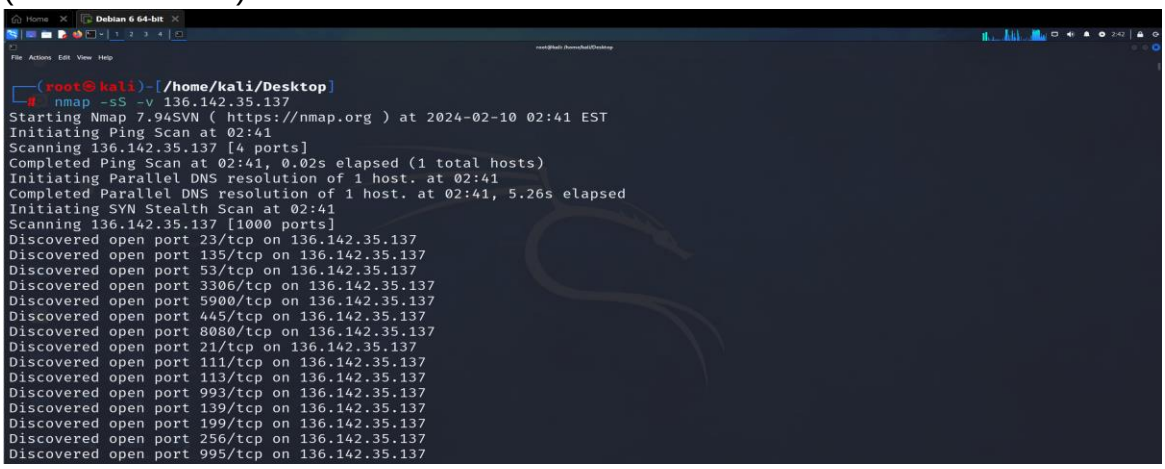
Objective: Learn the basic commands and syntax of Nmap.

Description: In this activity, you use Nmap to perform quick scans of a network. You send a SYN packet to a host on the attack network your instructor has supplied. In this example, the attack network IP addresses are 136.142.35.137 to 136.142.35.140. Make sure to follow the rules of engagement, and don't perform port scanning on any systems not included in the IP range your instructor gives you.

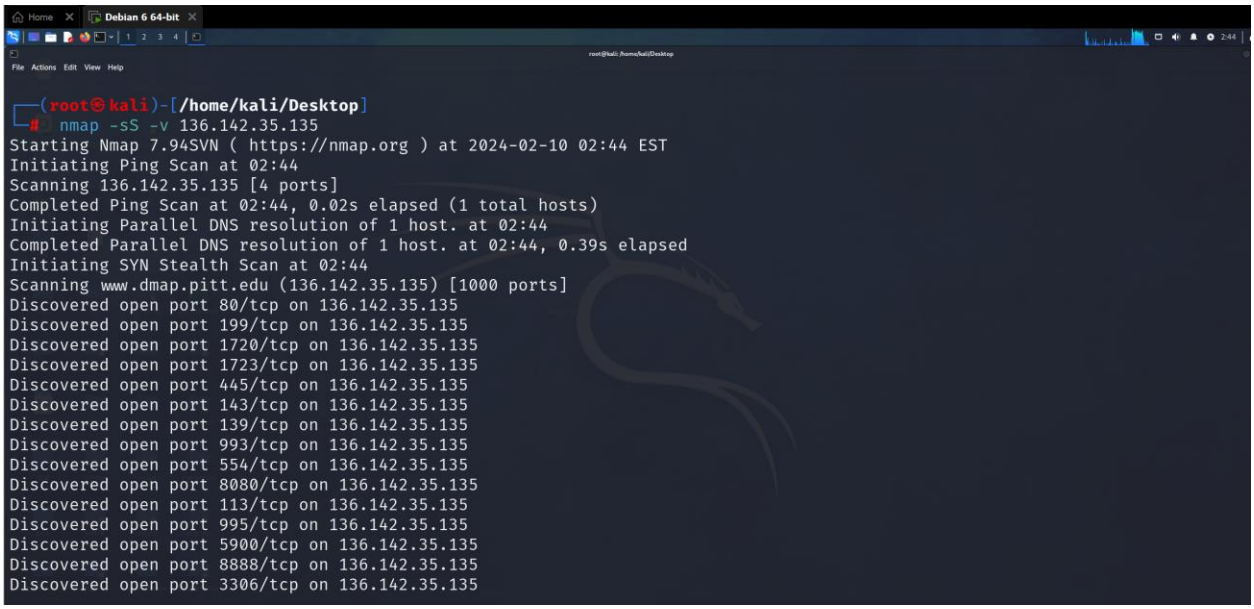
1. Boot your computer into Linux. Open a command shell by clicking the Terminal icon on the panel taskbar. Type nmap -h | less and press Enter to see all available Nmap commands. You can scroll to review the command parameters.



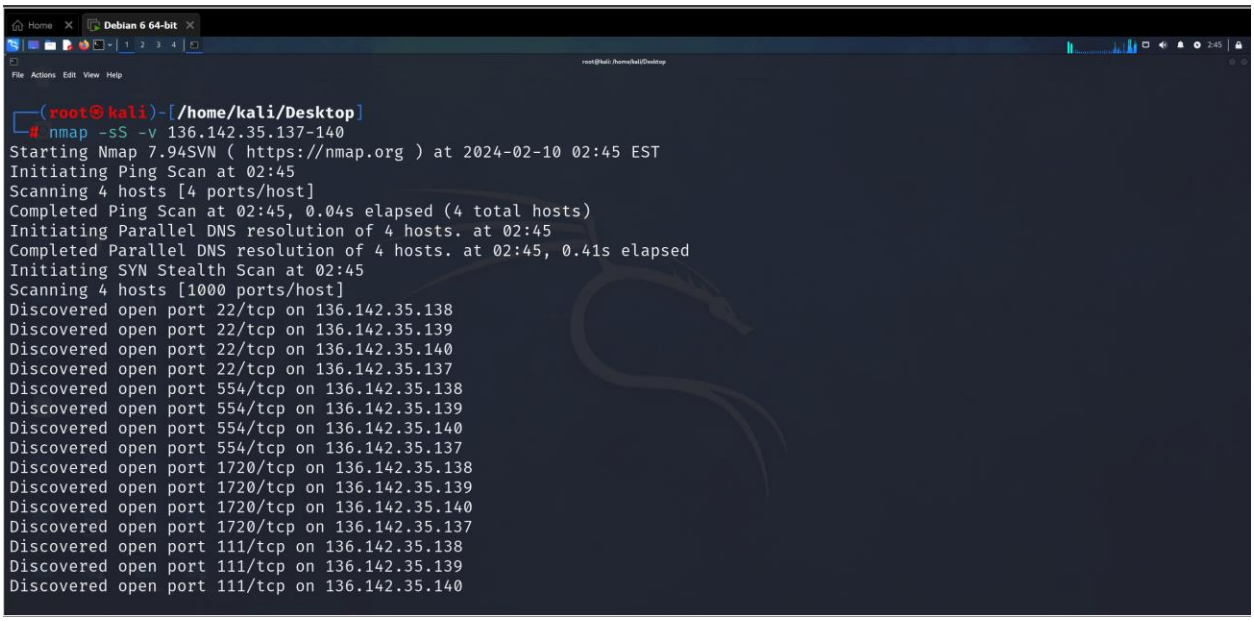
2. To send a SYN packet to an IP address in your attack range, type nmap -sS -v 136.142.35.137 and press Enter. What are the results of your SYN scan? (SCREENSHOT)



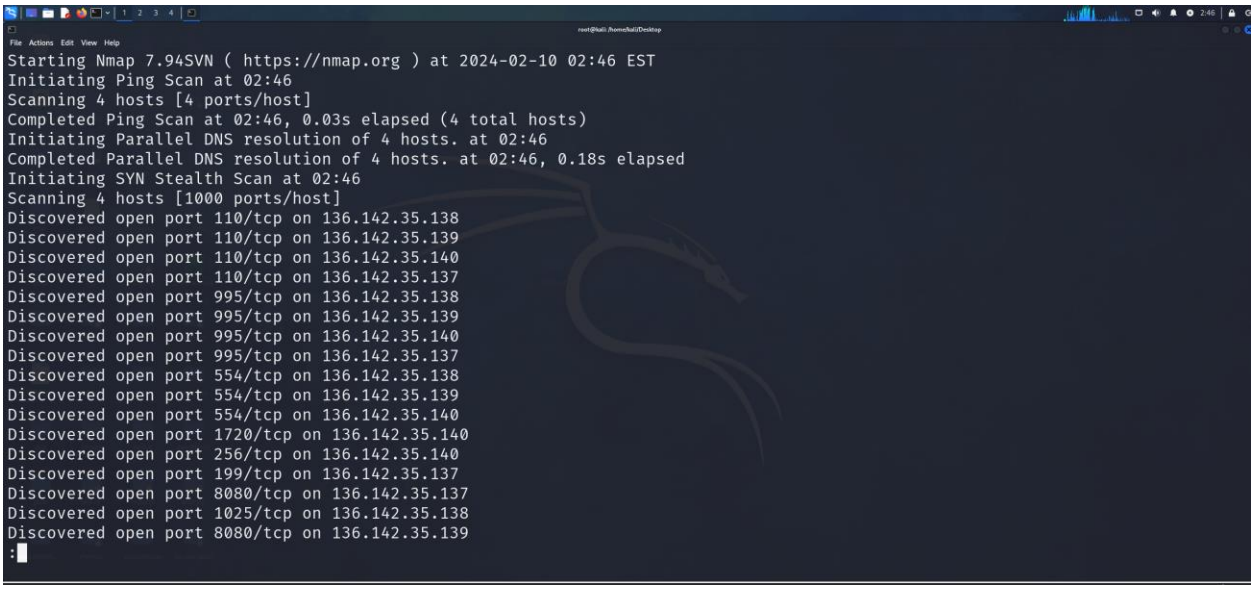
3 . Next, try sending a new SYN packet to a different IP address in your attack range. What are the results of this new scan? Do you see any differences? If so, list them. (SCREENSHOT)



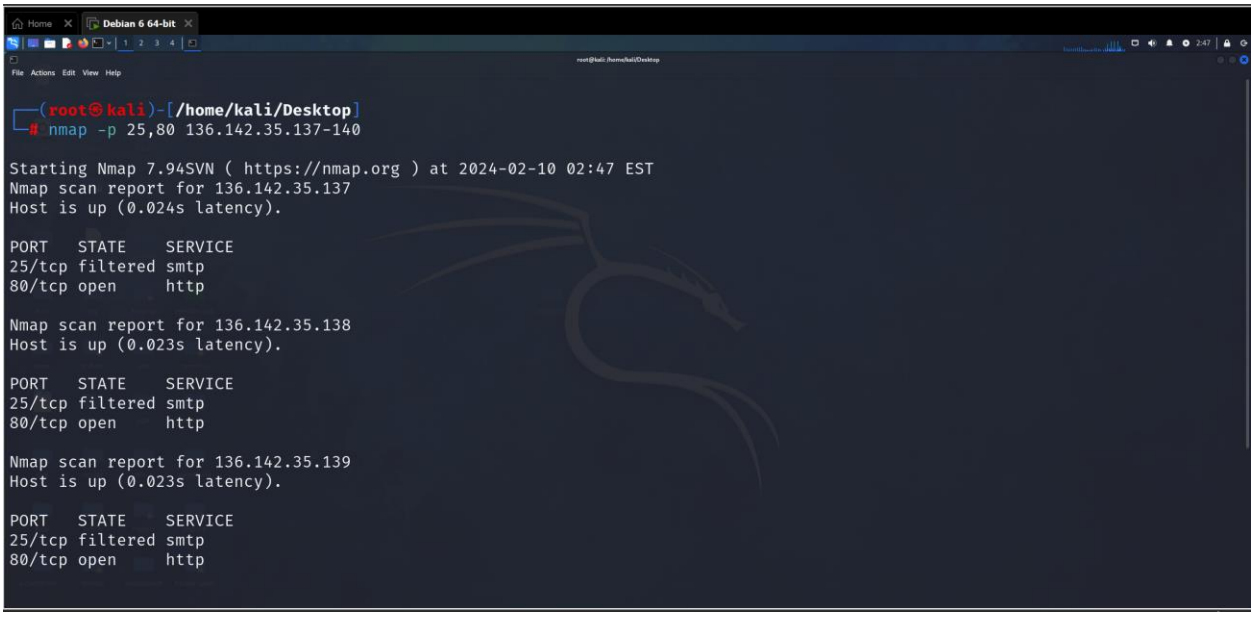
4 . Nmap can scan through a range of IP addresses, so entering one IP address at a time isn't necessary. To send a SYN packet to every IP address in your attack range, type nmap -sS -v 136.142.35.137-140 and press Enter. (SCREENSHOT)



6. To see the output in a format you can scroll, press the Up Arrow key, add the | less option to the end of the Nmap command, and press Enter. The command should look like this: nmap -sS -v 136.142.35.137-140 | less.



7. Next, add one more parameter to the Nmap command to determine which computers in your attack range have the SMTP service or HTTP service running. Using what you've learned so far in this activity, enter the command and note the output. (Hint: What ports do SMTP and HTTP use?) The command's output might vary, but what's important is learning how to build on the Nmap command. You can select specific ports in the Nmap command, so not all 65,000 ports must be scanned.



8. Leave the Terminal shell open for the next activity.

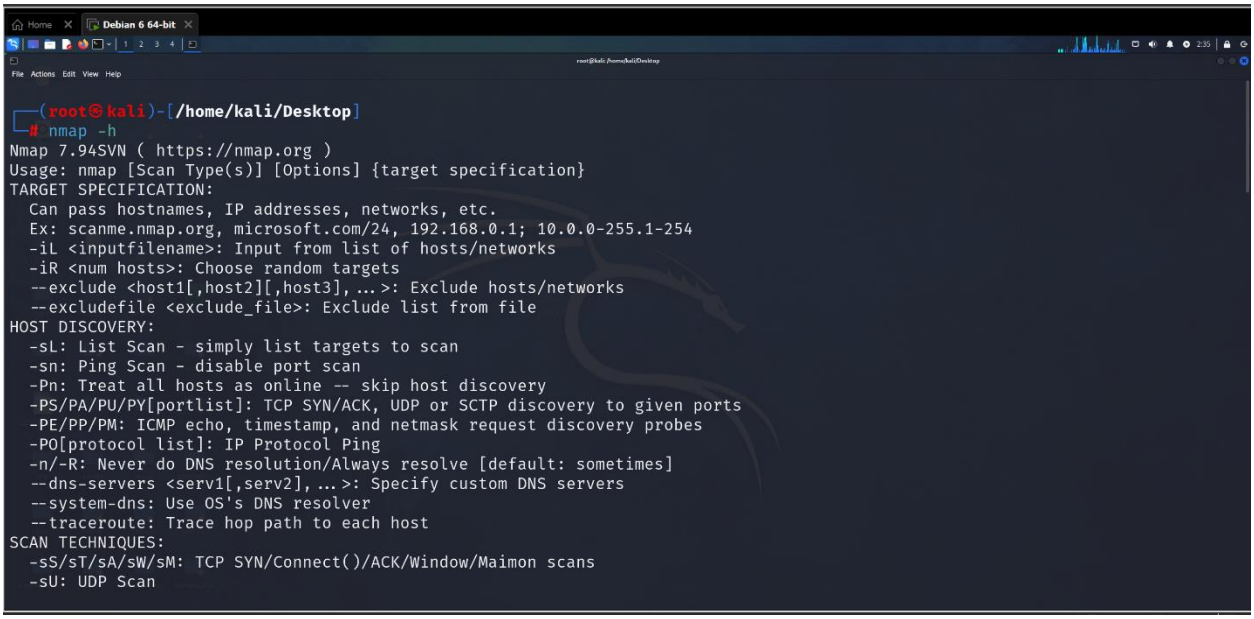
Activity 5-2: Using Additional Nmap Commands

Time Required: 30 minutes

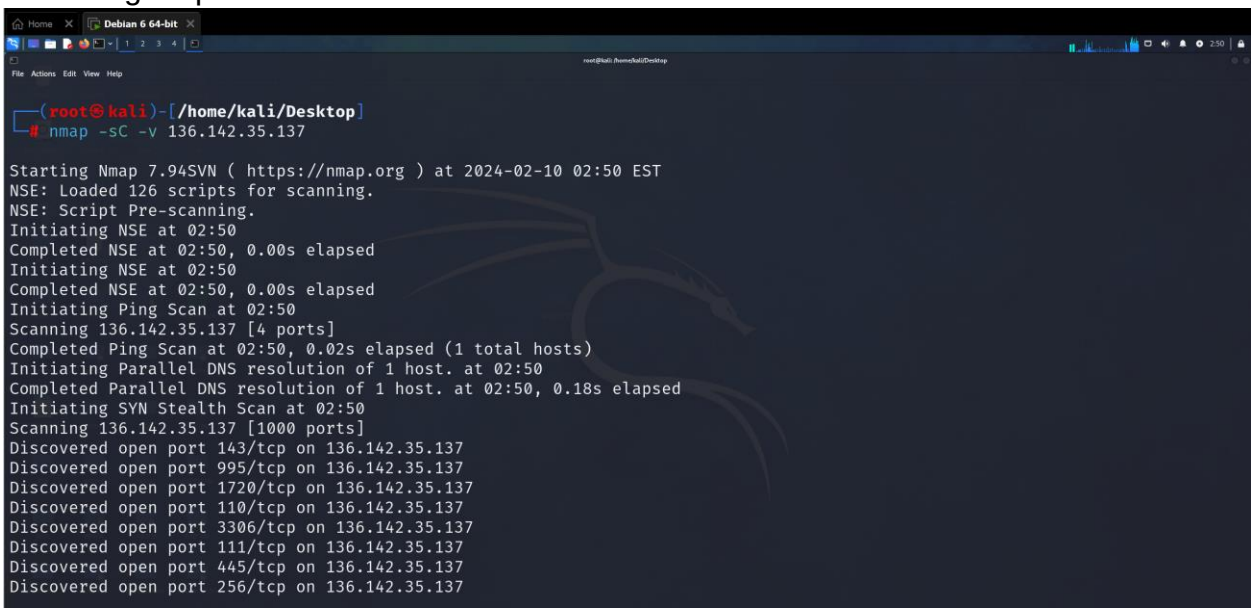
Objective: Perform more complex port-scanning attacks with Nmap.

Description: In this activity, you continue to use Nmap for port scanning on your attack network. You add to the parameters used in Activity 5-1 using Nmap scripts to discover more information about the remote host. You should practice these commands until they are second nature, but Fyodor developed a well-written help page (called a “man page” in UNIX/Linux circles) that you can use as a resource. You begin this activity by looking at this help page.

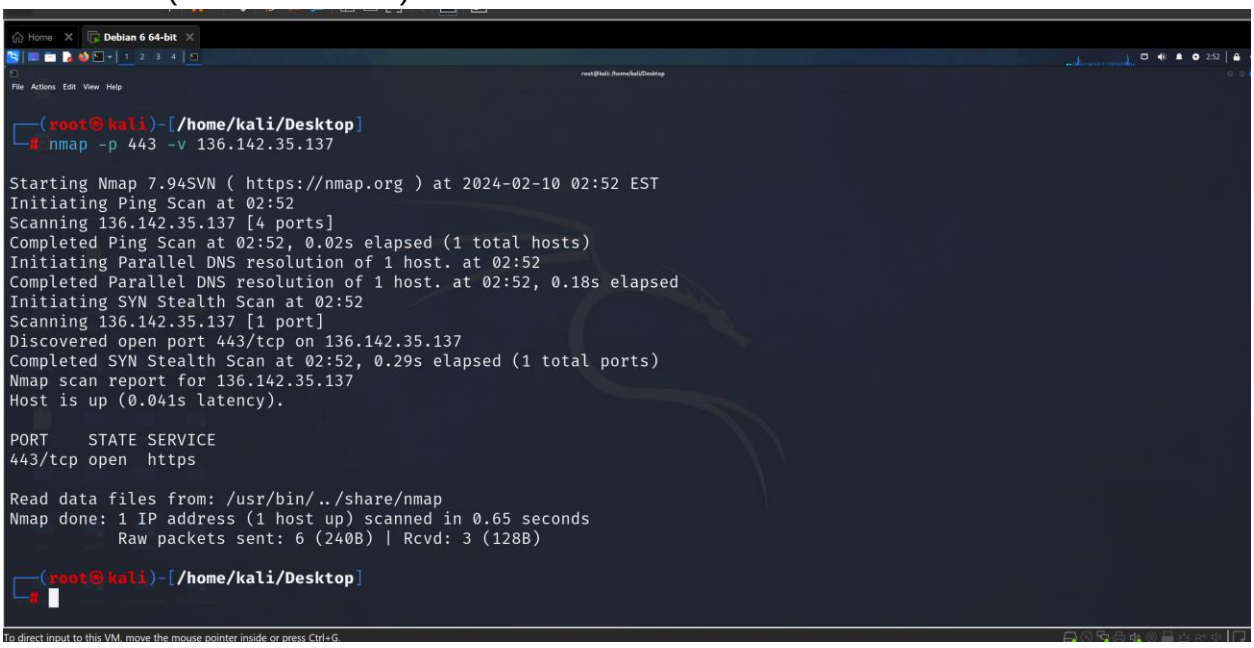
1. If a Terminal window isn’t open, boot your computer into Kali Linux, open a Terminal shell, and at the command prompt, type man nmap and press Enter. You can see that this command produces more information than the nmap -h command. Don’t be concerned about memorizing the manual; just know it’s there when you need it.



2. Next, enter the command to send a default script scan to 136.142.35.137 (nmap –sC –v 136.142.35.137). You can read more about the default scripts included with the default scan setting at https://nmap.org/nsedoc/categories/default.html. What are the results of the script scan? What brand and version of HTTP server is running on ports 80 and 443?



3. Now, limit the scope so you scan only port 443 by using the –p flag (nmap –p443 –v 136.142.35.137). This makes the Nmap scan more targeted and less noticeable. (SCREENSHOT)



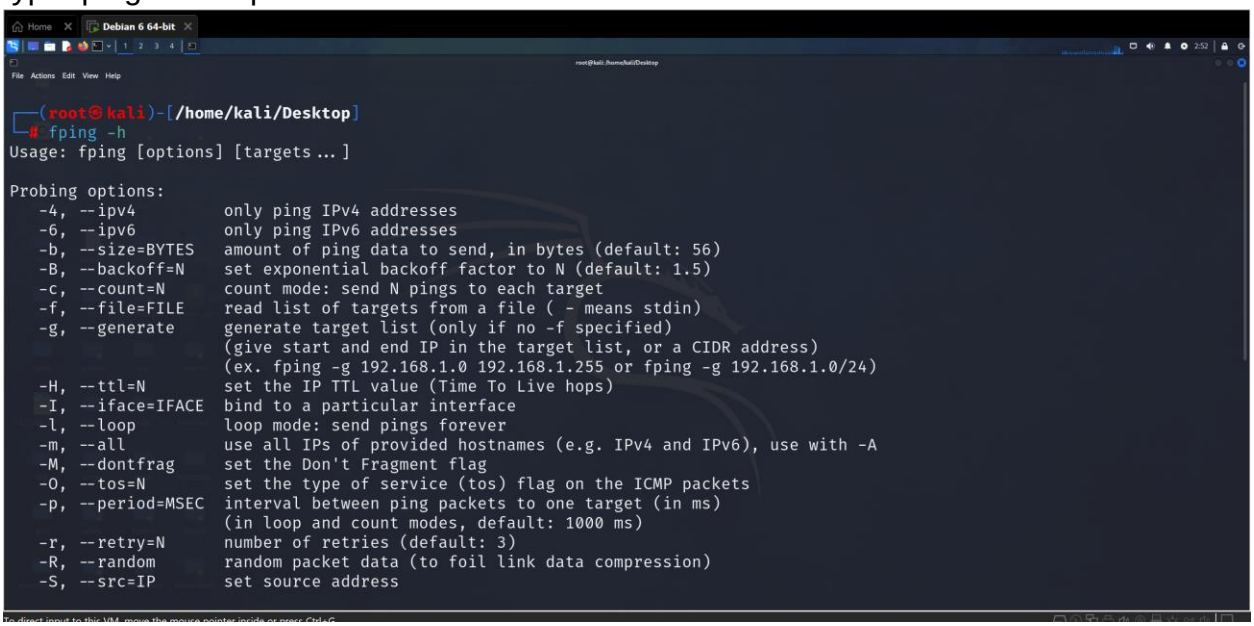
Activity 5-3: Crafting IP Packets with Fping and Hping3

Time Required: 30 minutes

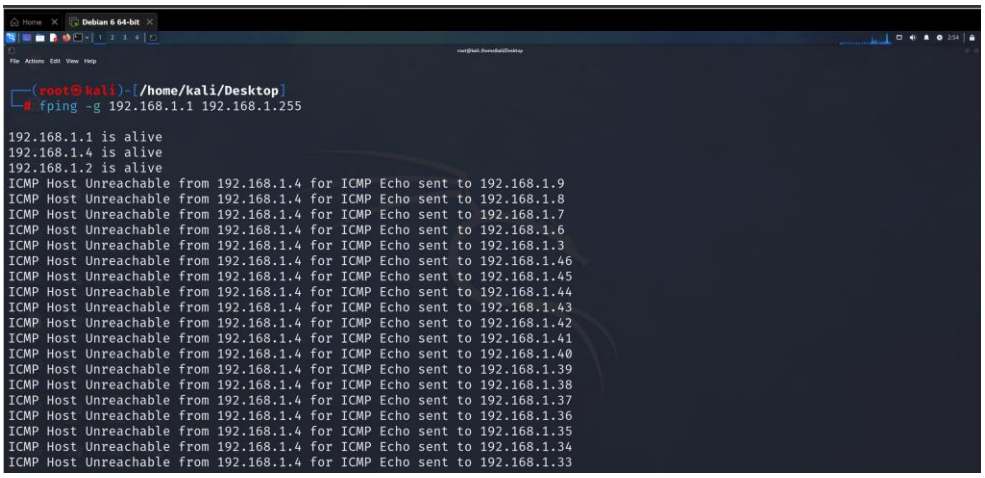
Objective: Learn to craft IP packets with Fping and Hping3.

Description: In this activity, you see how security testers can craft IP packets to find out what services are running on a network. The more ways you know how to send a packet to an unsuspecting port on a computer and get a response, the better. If a computer doesn't respond to an ICMP packet sent to a particular port, it doesn't mean any packet sent to the same port will get the same response. You might need to send different packets to get the results you need for a thorough security test.

1. If necessary, boot your computer into Linux. Open a Terminal shell, and then type fping -h and press Enter.

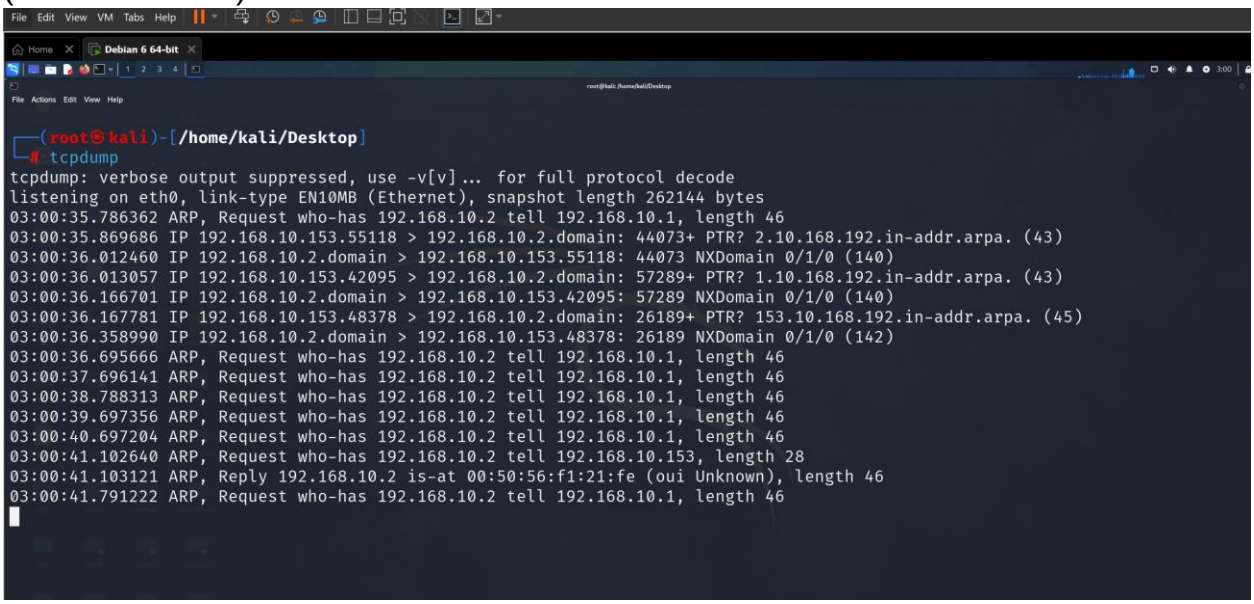


2. To see the live computers in the attack range, type fping -g BeginningIPaddress EndingIPaddress and press Enter. Note the results. (Be sure to use the beginning and ending IP addresses in your attack range.) (SCREENSHOT)



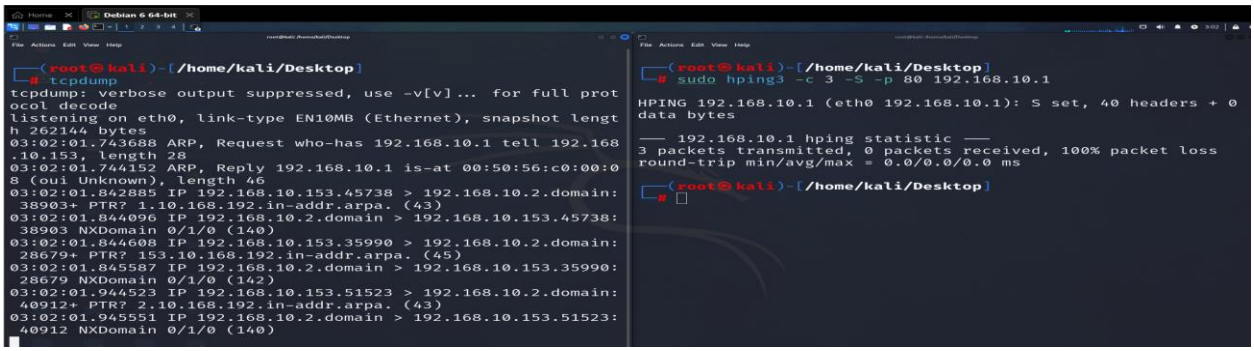
3. Next, type hping3 -S IPAddressAttackedComputer (substituting an IP address from your attack range) and press Enter. By using the -S parameter, you craft a TCP SYN packet.

4. Open another Terminal shell, and then type tcpdump and press Enter. (SCREENSHOT)

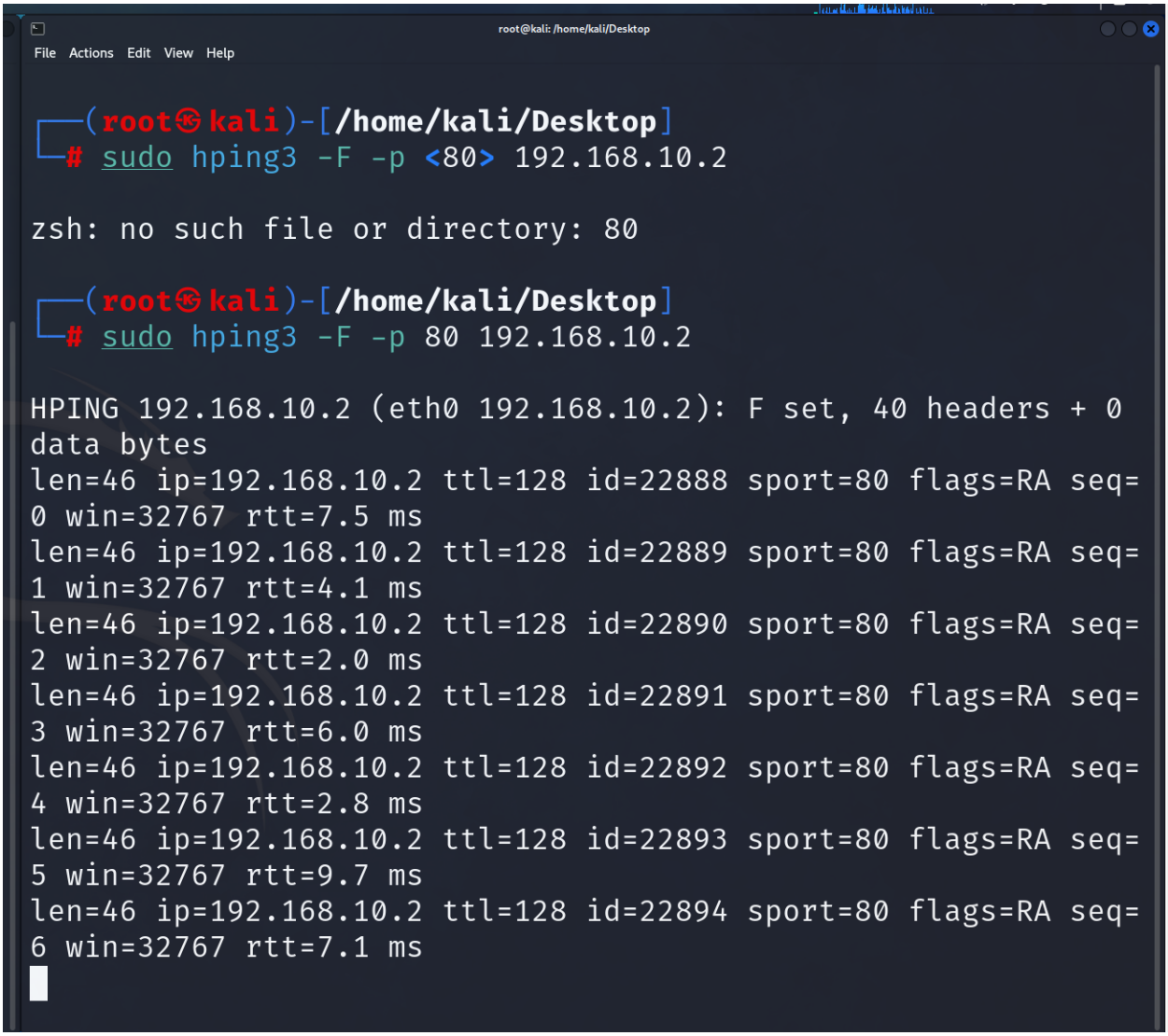


5. Arrange both shell windows next to each other so that you can observe what happens after entering the Hping3 command type hping3 -S

IPAddressAttackedComputer, and press Enter. Watch the Tcpdump window fill with the traffic that's generated. To stop Tcpdump from capturing packets, press Ctrl+C in that shell window. (SCREENSHOT)



6. Consult the Hping3 help pages and experiment with creating different types of packets. Note the differences in network traffic generated with the Tcpdump command. Security testers need to understand how slight variations in packets sent to an attacked computer can produce different results. For example, if a computer doesn't respond to a SYN packet, try sending an ACK packet. What happens when a FIN packet is sent? If you aren't having any success, try sending the same packets to different ports. Does this method change the response from the attacked computer?



By experimenting with different types of packets and observing the network traffic using tcpdump, you can gain insights into how slight variations in packets can produce different results and how target systems respond to different types of packets. This understanding is crucial for security testers to assess network security and identify potential vulnerabilities.

When you're done, close both shells.

Conclusions:

Through Activities 5-1 to 5-3, I gained practical insights into network scanning and packet crafting, enhancing my security testing proficiency. Experimenting with Nmap, Fping, and Hping3 underscored the importance of nuanced approaches for comprehensive vulnerability assessment.

References:

1- Bhuyan, M. H., Bhattacharyya, D. K., & Kalita, J. K. (2011). Surveying port scans and their detection methodologies. The Computer Journal, 54(10), 1565-1581.
2- Asrak, Z. (2020). Penetration Testing Tools.
3- Ganzy, E. G. (2014). Scalable Asset Discovery, Vulnerability Scanning, and Penetration Testing for Remote Sites and Wireless Spectrums Utilizing an Embedded Linux Plug-PwniPlug and the Raspberry Pi B+ as a Sample Pen Test (No. KSC-E-DAA-TN19263).