OLD DOMINION UNIVERSITY

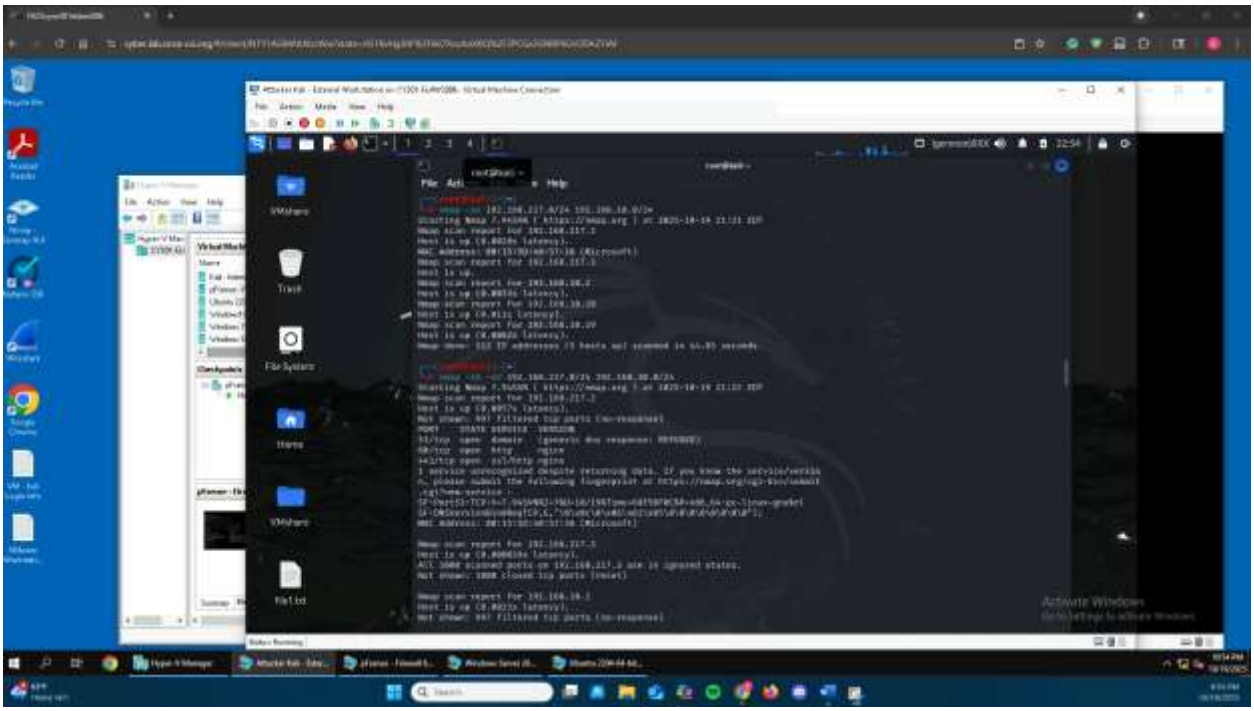
CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

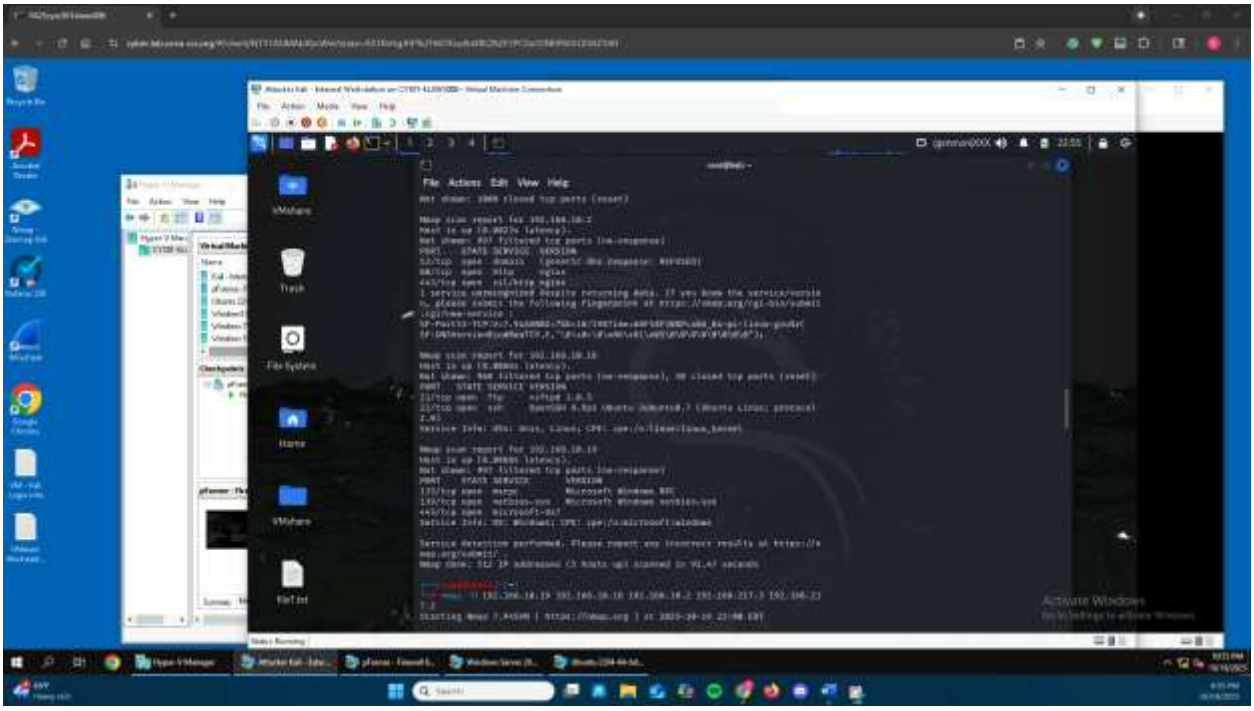
Assignment #1 Basic Linux Commands

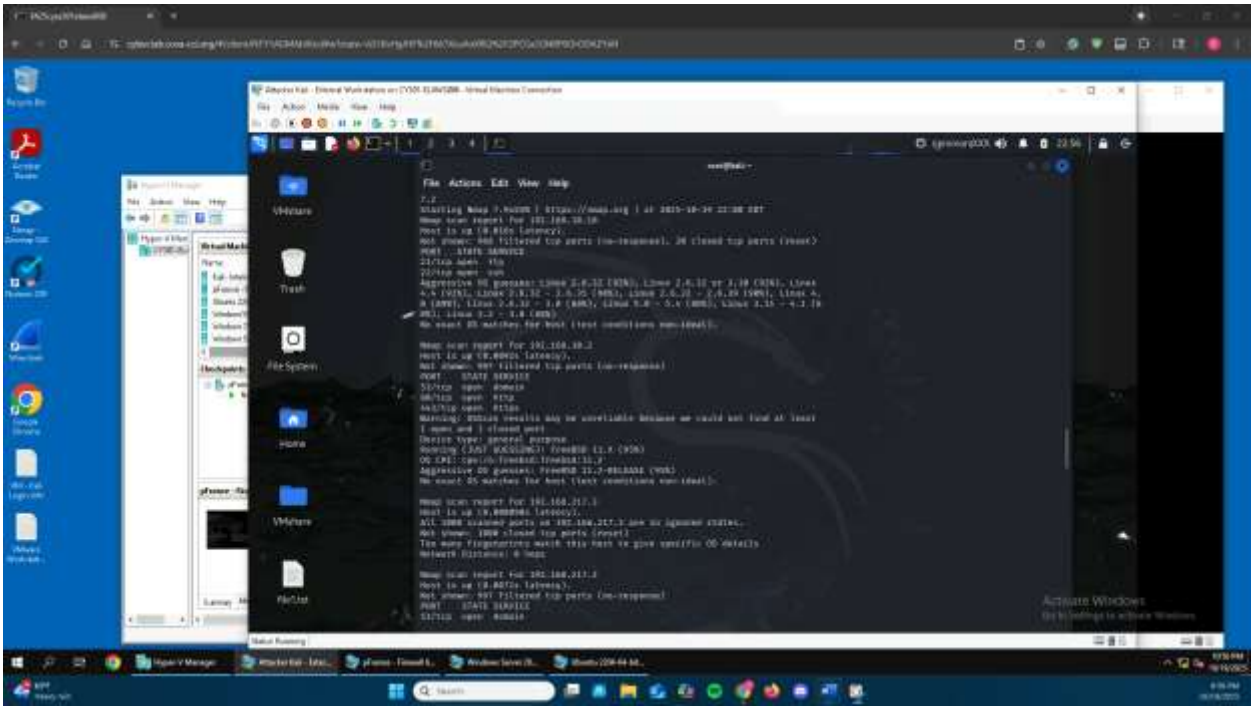
Ethan Lawson

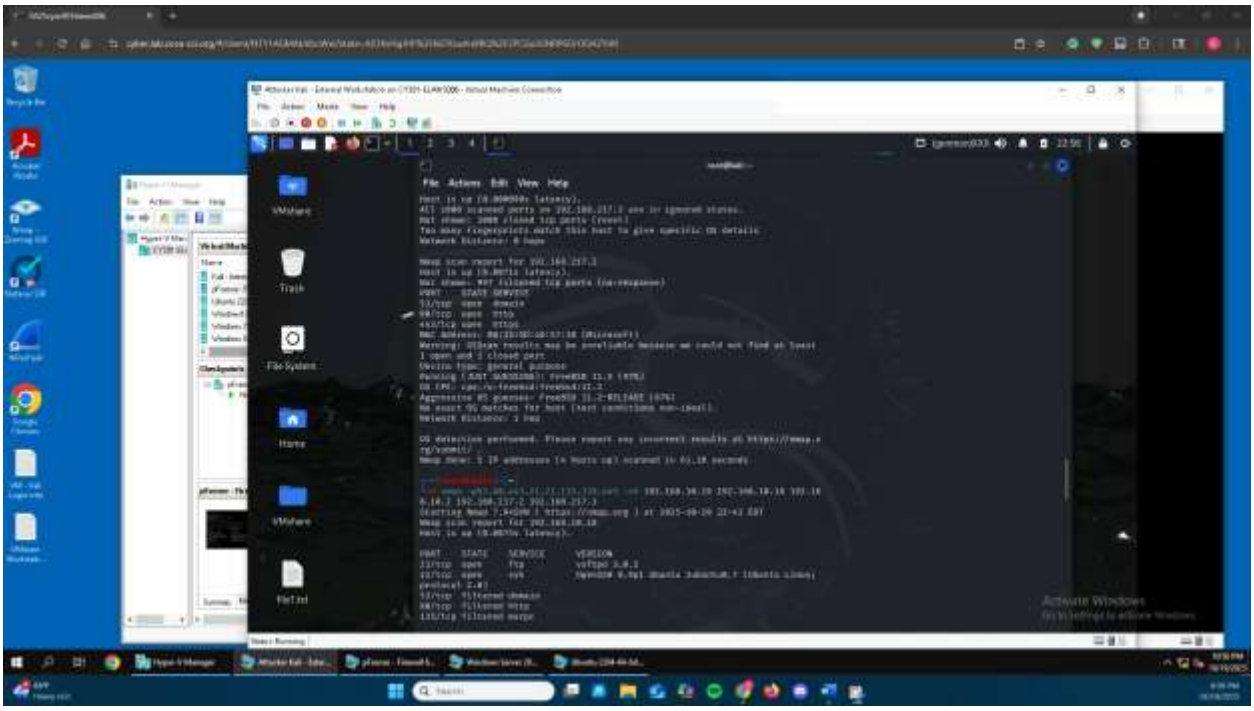
TASK A

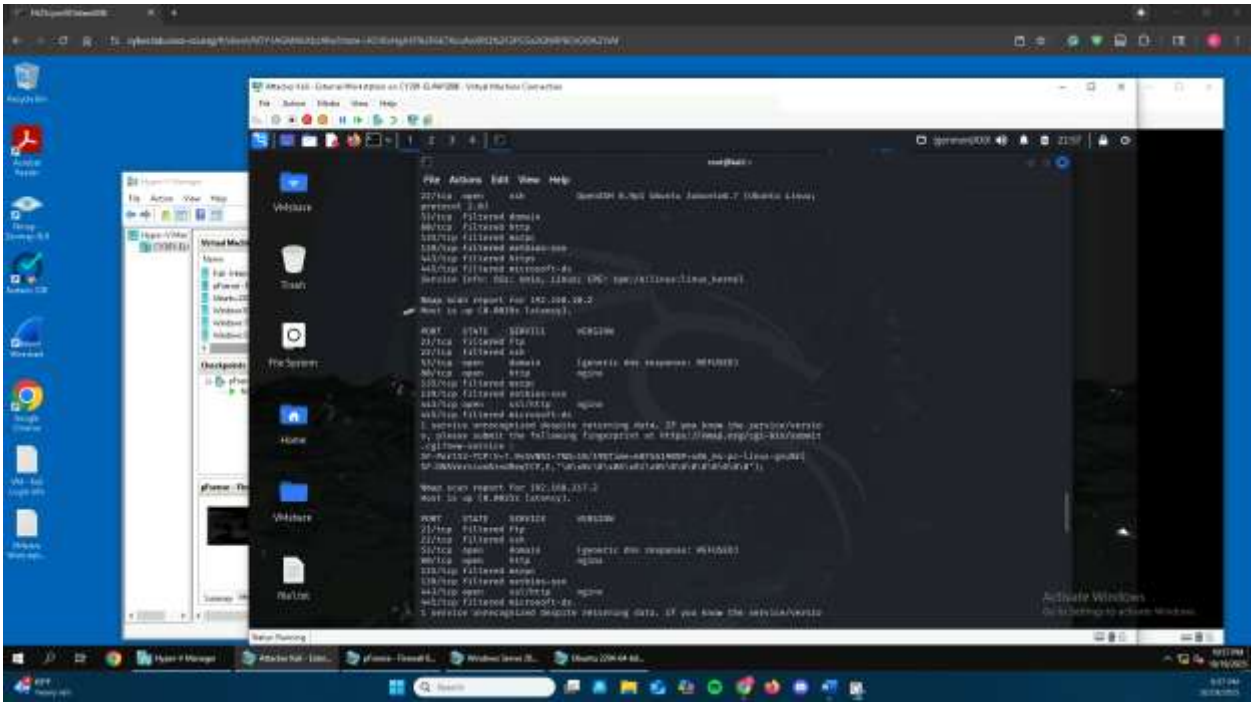
1. Use Nmap to profile the basic information about the subnet topology (including open ports information, operation systems, etc.) You need to get the service and backend software information associated with each opening port in each VM.

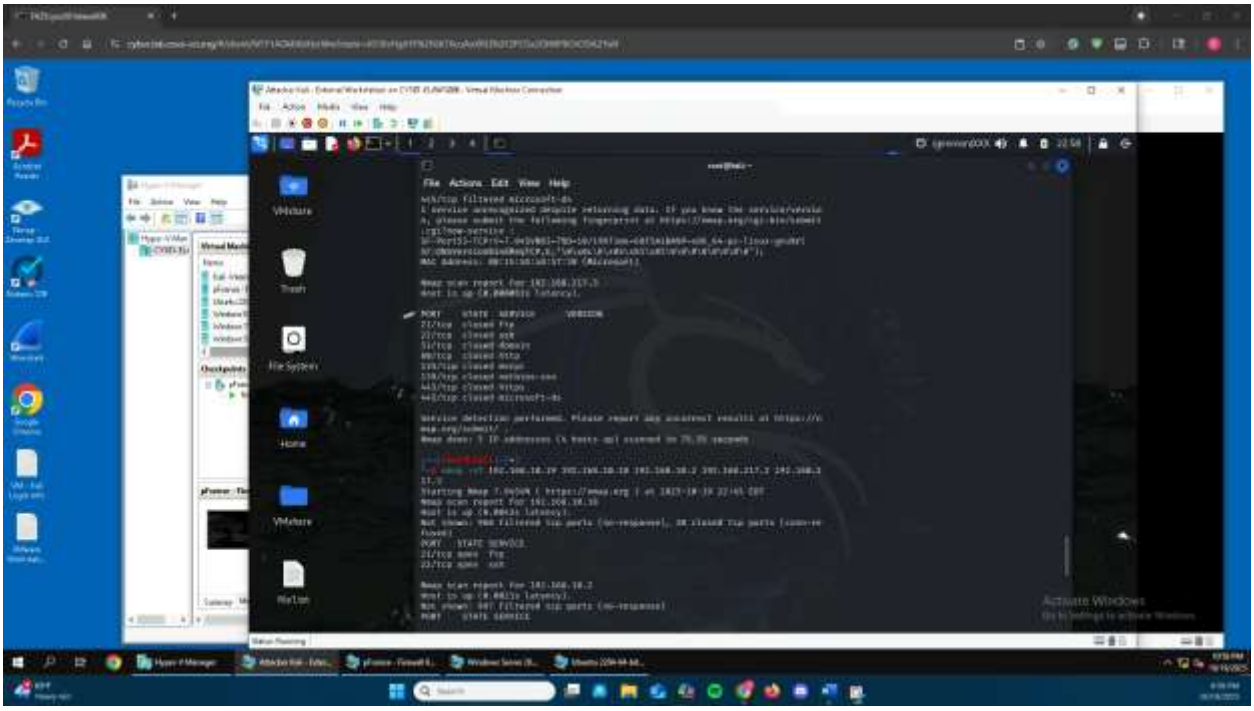


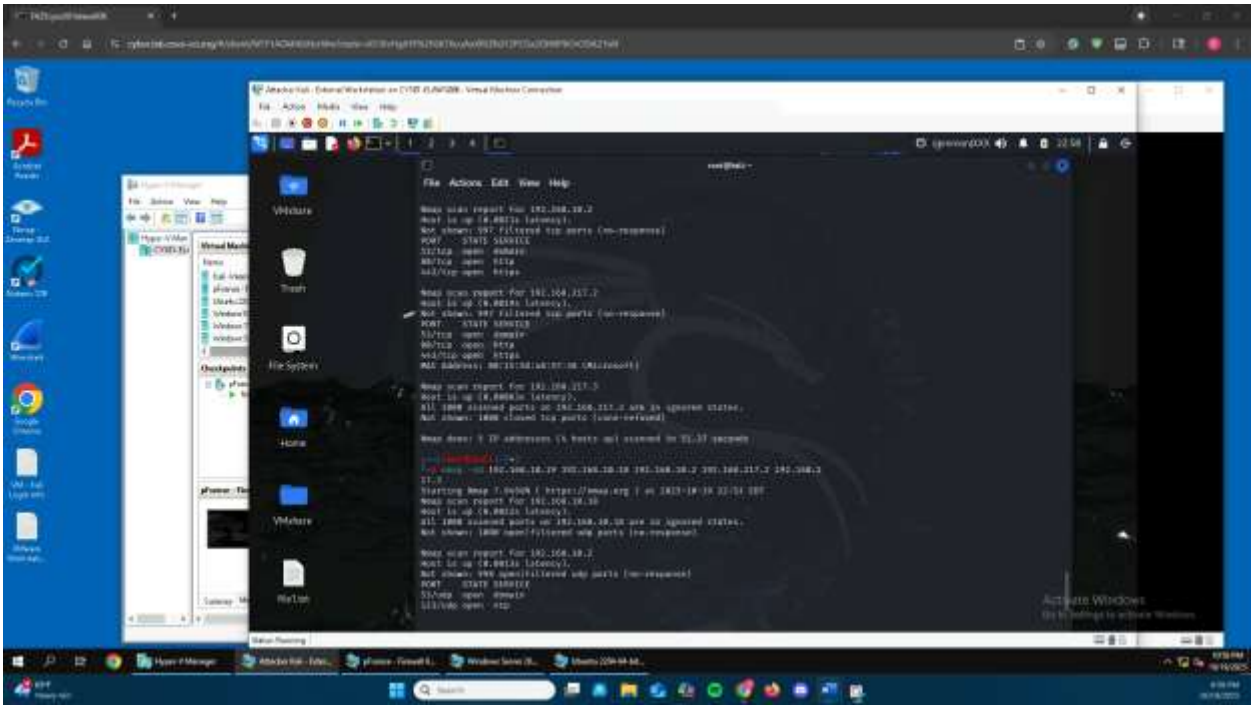


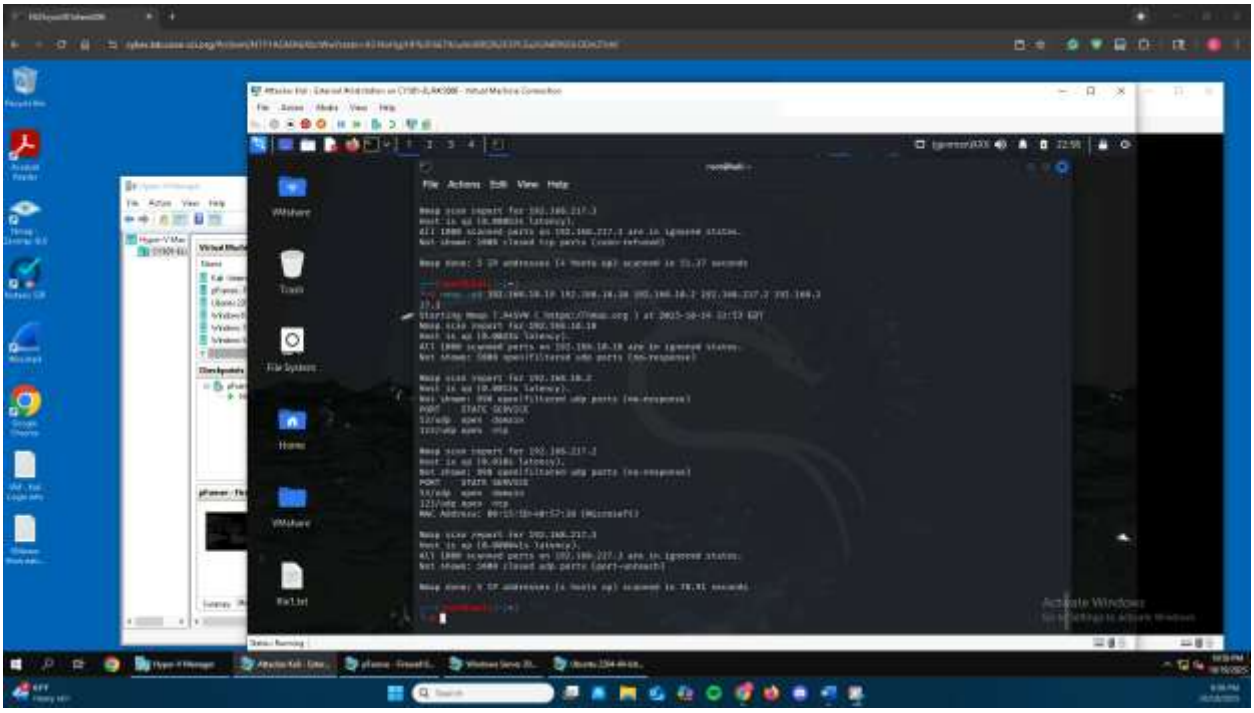


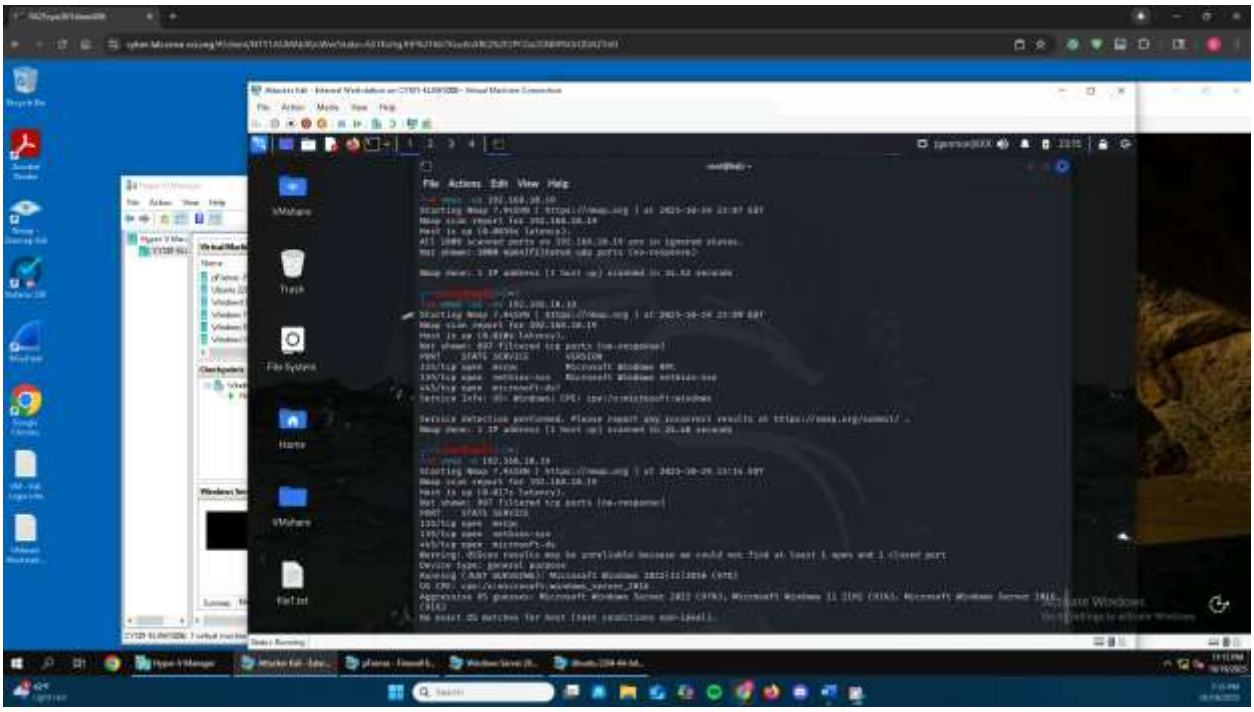






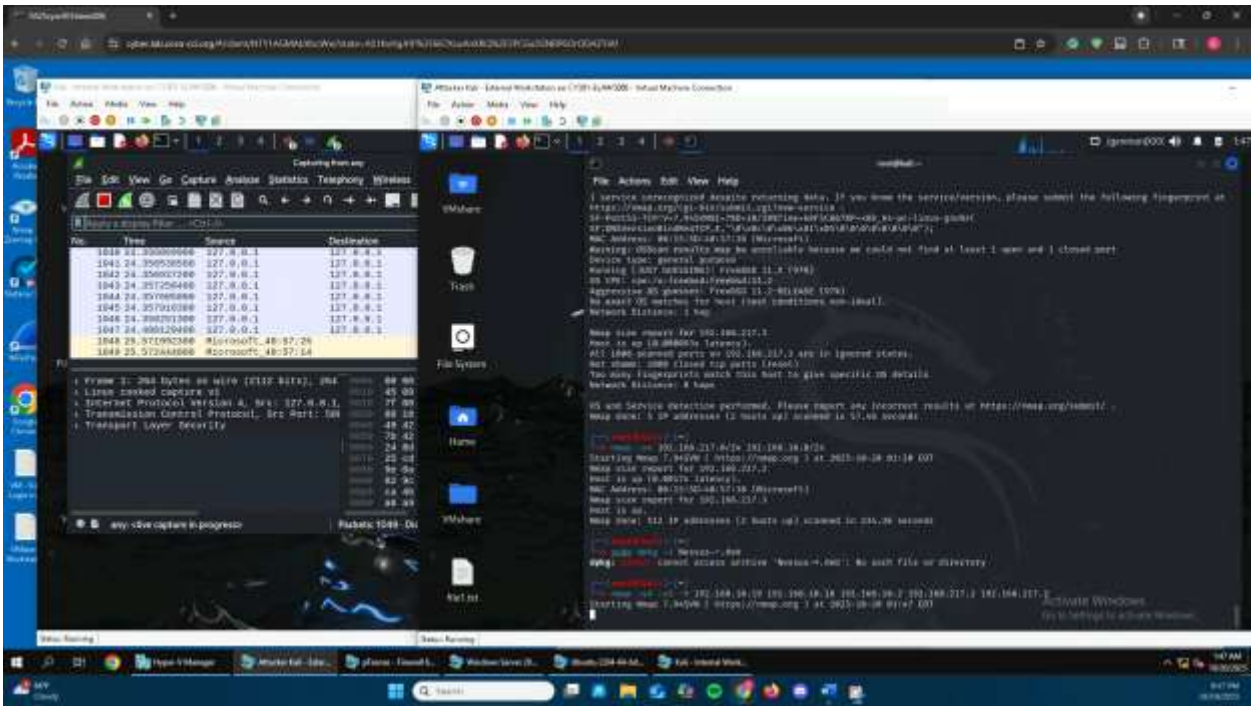






I used to discover which hosts were live on each subnet, -sS & -sV for open TCP ports + service/version, -O to determine the operating system, -p & -sV for port and version info, -sU for UDP ports, and -sT for full TCP connect.

2. Run Wireshark in Internal Kali VM while External Kali is scanning the network. Discuss the traffic pattern you observed. What do you find? Please write a 200-word essay to discuss your findings.

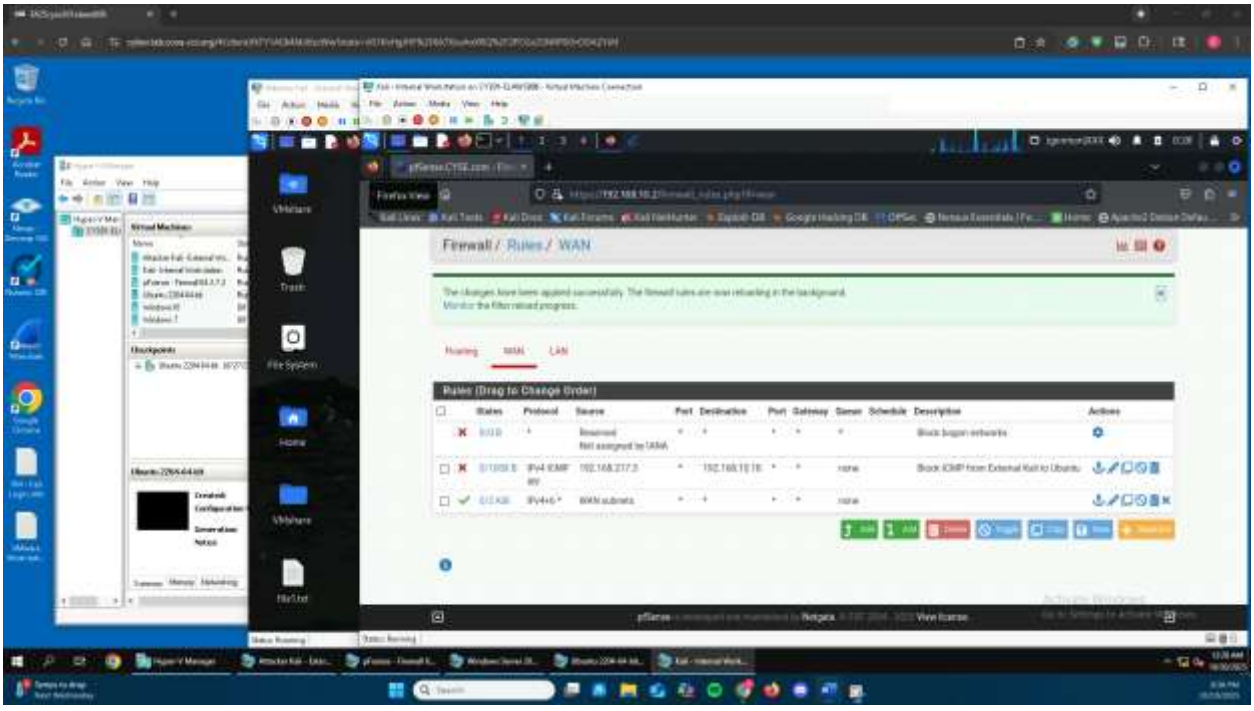


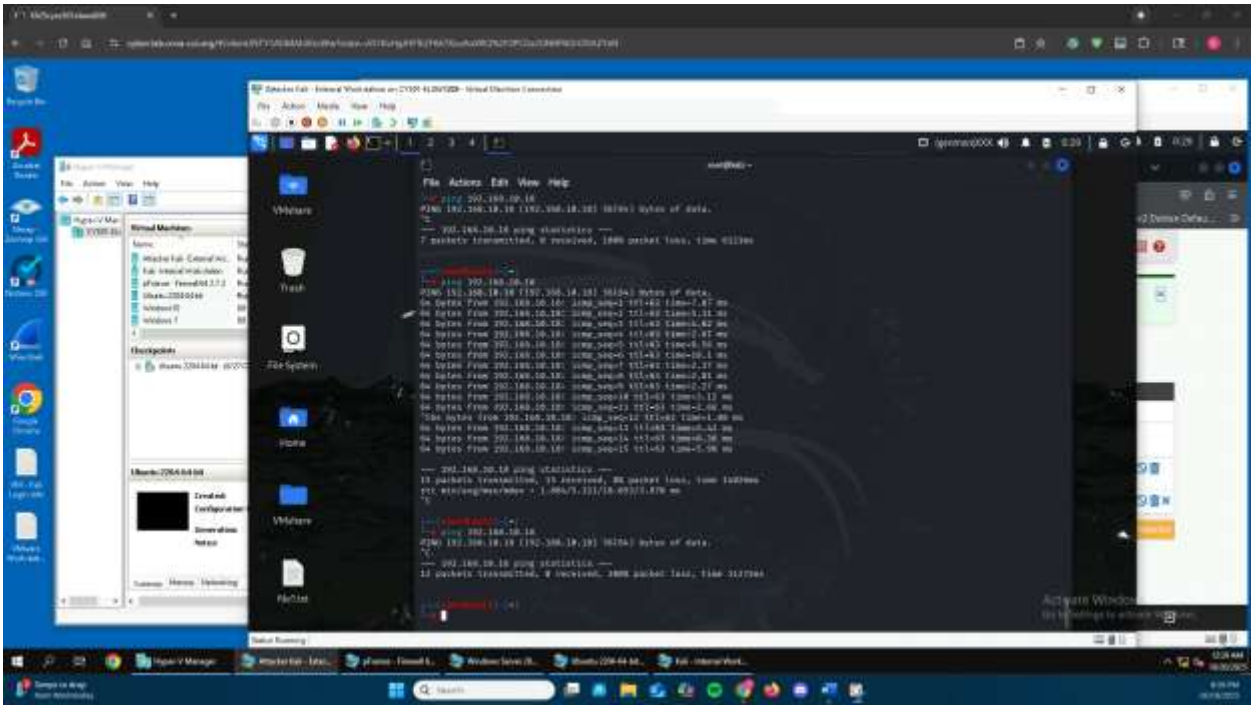
While running Wireshark on the Internal Kali VM I scanned its network from the External Kali using the “nmap -sV, -sS, -O 192.168.10.13” command. The first communication I see between the two machines is ICMP followed by TCP SYN. The internal Kali responded to the echo and timestamp request. The first TCP packet received a [RST, ACK] meaning that port was closed. A little later it started trying many other TCP ports all of which seemed to fail. These failures seem to be the work of the -sS or SYN sweep part of the command. I found a few that received [SYN, ACKs] at the bottom on ports 8000 to 39000 and 8089 to 51012. It works to find open TCP ports which respond with SYN-ACKs while closed ports send RSTs. After the barrage of TCP SYNs, the external attacker Kali started trying other protocols like http, Portmap, and TLSv1.2. The -sV part of my command probes application protocols for service banners, names, and versions. The -O option attempts to find the type of operating system by observing TCP/IP stack behavior. The firewall probably played a role in the results received. Overall, this network scan revealed part of the attack surface on this Internal Kali machine by finding open ports, backend software, and operating system.

Task B

1. Configure the pfSense firewall rule to block the ICMP traffic from External Kali to Ubuntu VM.

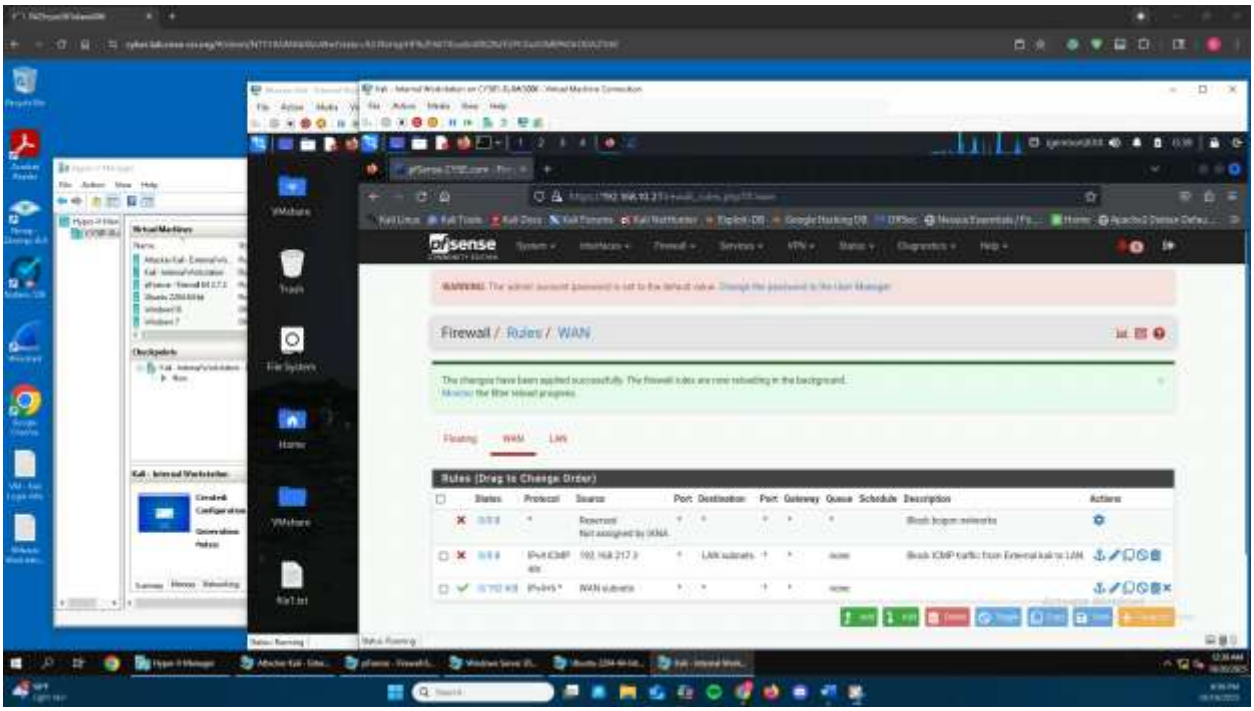
Rule #	Interface	Action	Source IP	Destination IP	Protocol Port #
1	WAN	Block	192.168.217.3	192.168.10.18	ICMP

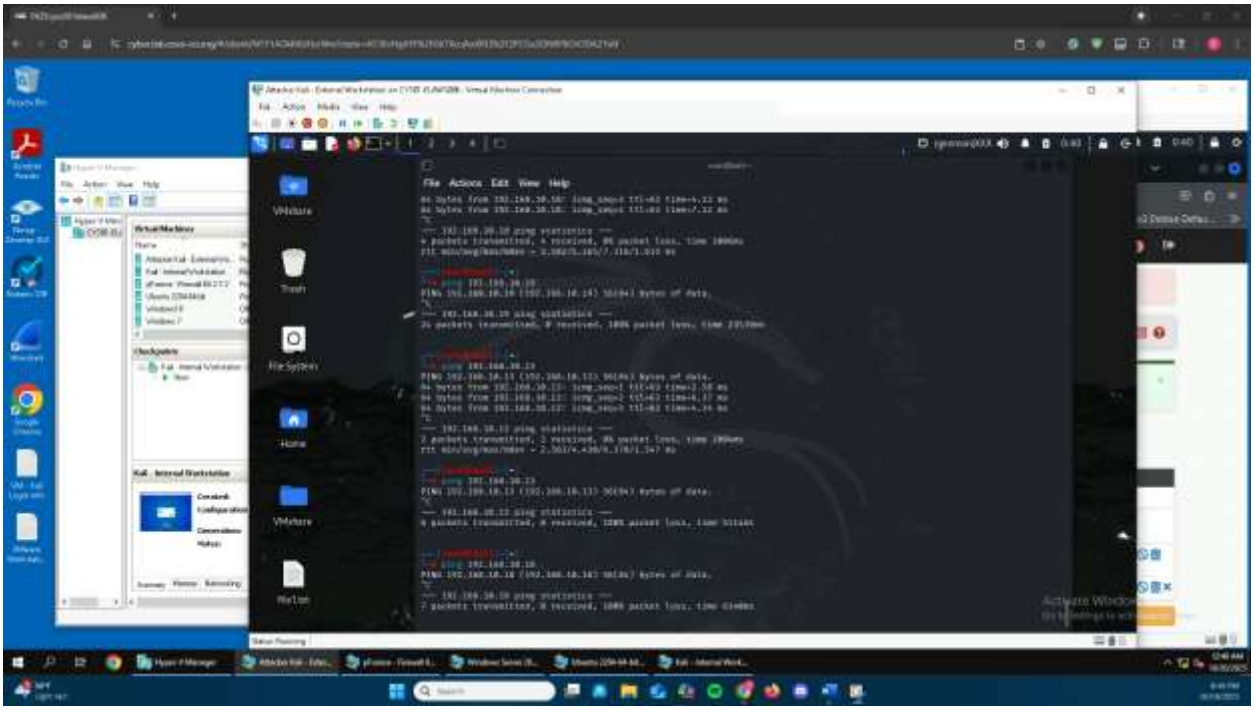




2. Clear the previous firewall policies and configure the pfSense firewall to block all ICMP traffic from External Kali to the LAN side.

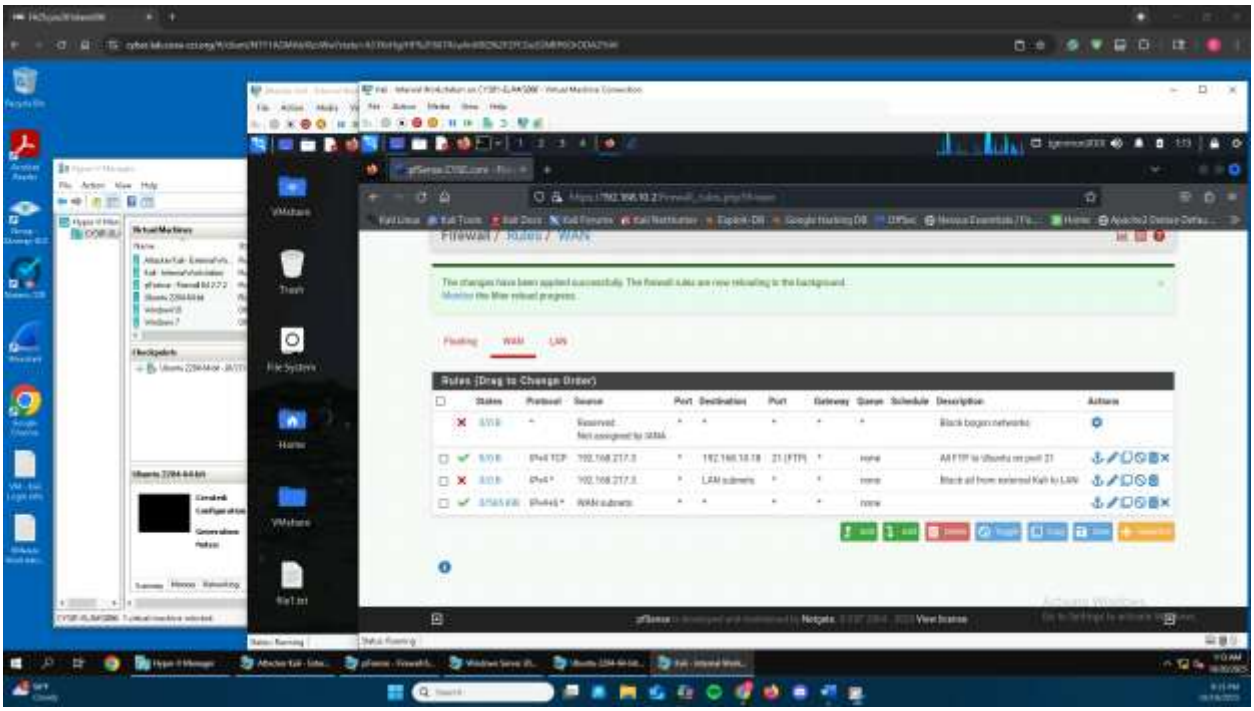
Rule #	Interface	Action	Source IP	Destination IP	Protocol Port #
1	WAN	Block	192.168.217.3	LAN subnets	ICMP

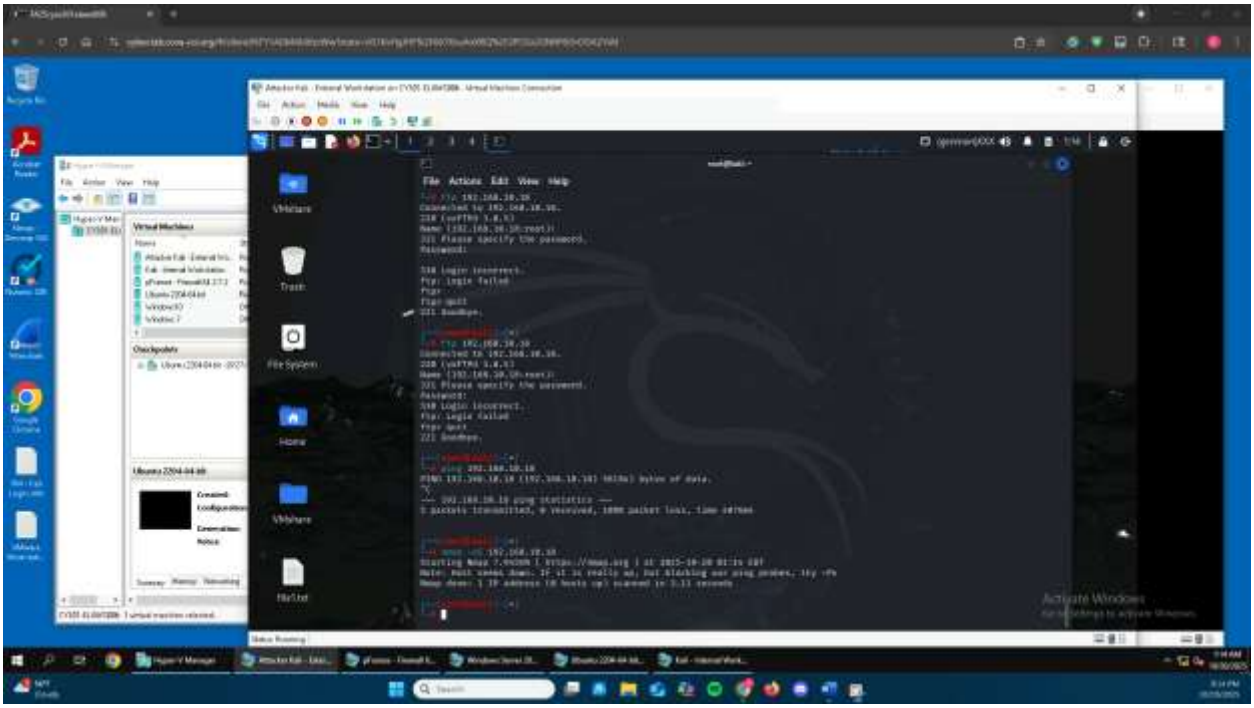




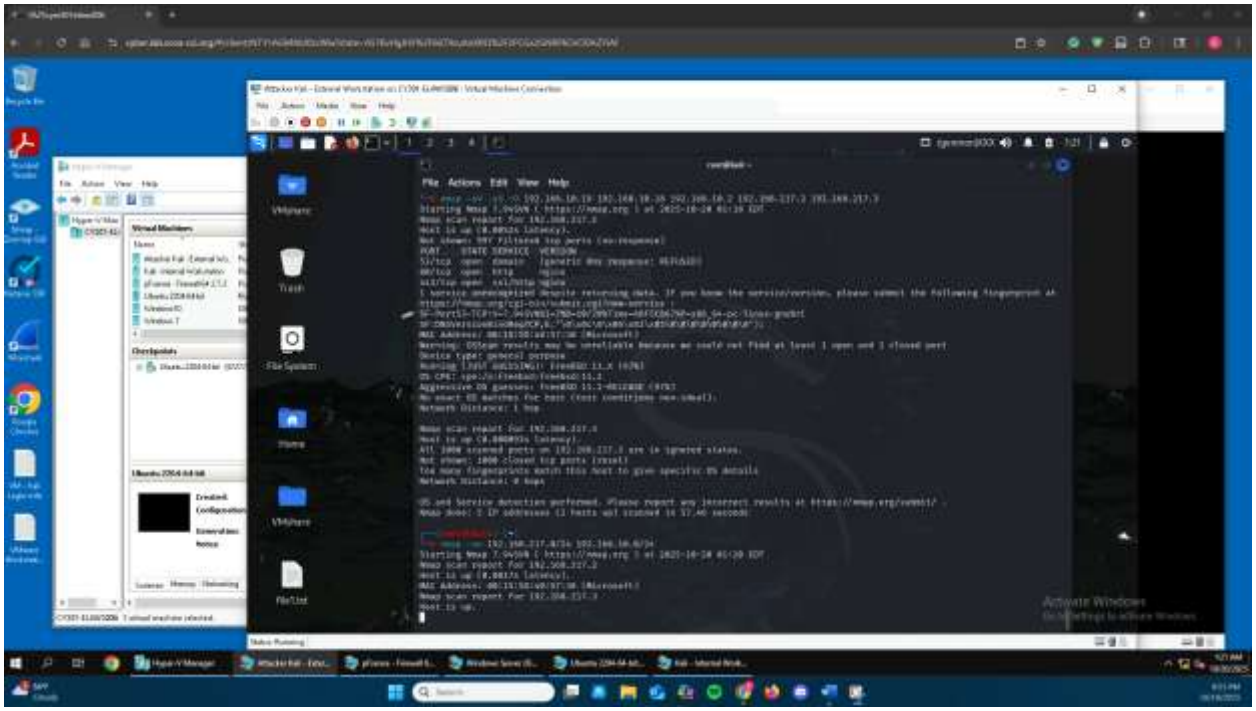
3. Clear the previous firewall policies and configure the pfSense firewall to block ALL traffic from External Kali to the LAN side, except for the FTP protocol towards Ubuntu.

Rule #	Interface	Action	Source IP	Destination IP	Protocol Port #
1	WAN	Pass	192.168.217.3	192.168.10.18	21 FTP
2	WAN	Block	192.168.217.3	LAN subnets	Any



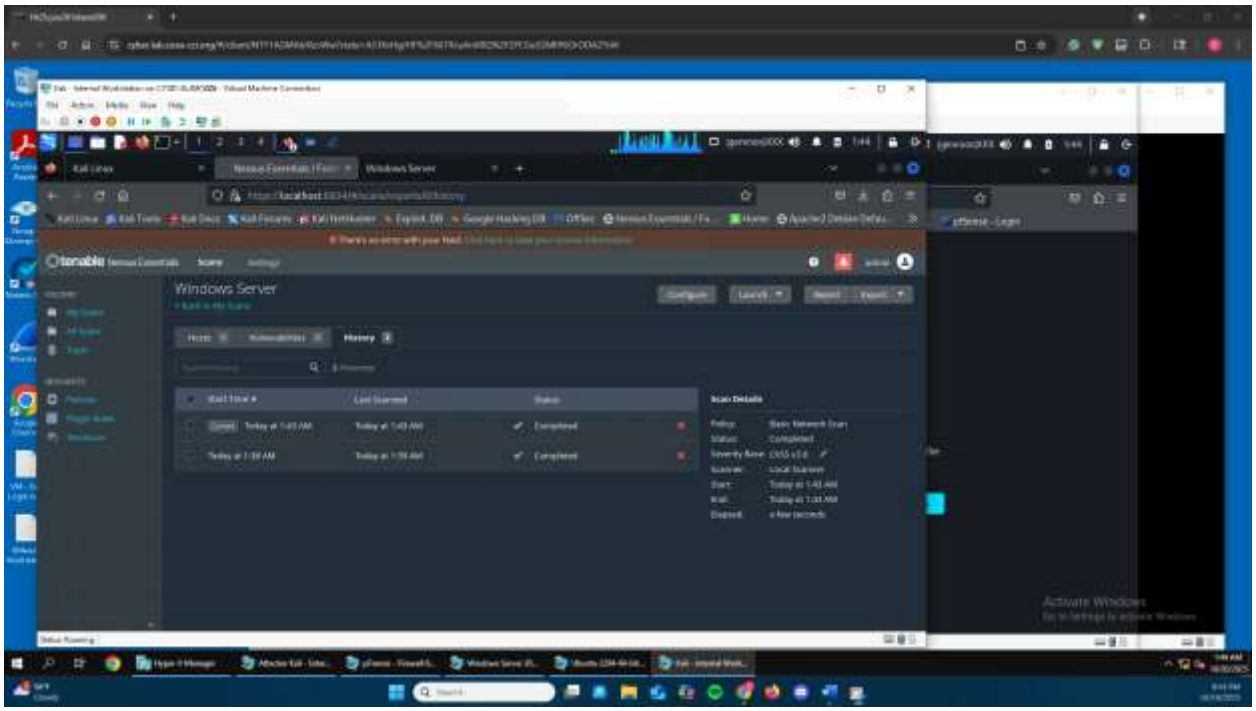


4. Keep the firewall policies you created in Task B.3 and repeat Task A.1. What's the difference?



After keeping the firewall policies from the last step which blocked all communications from external Kali to the LAN subnet (10.0) except FTP port 21 on Ubuntu, the results are significantly different. Without this firewall restriction Nmap was able to find several open ports on Ubuntu VM like 21, 22, 53, 80, and 443. There were many like this either open or filtered. It was also able to determine the versions of services. After, only port 21 is open which significantly reduces the attack surface and hiding of internal systems.

Extra credit (15 points): Use NESSUS to enumerate the security vulnerabilities of Microsoft Windows Server 2022 VM in the CCIA network.



Your lab report MUST satisfy the following Requirements. Otherwise, you will lose points.

- R1 - Include a cover page with your UIN and name.
- R2 - Align your screenshot(s) with the task ID and description.
- R3 – Use “Snipping tool” or other tools, such as “Snipaste”, to take screenshot. MacOS user can follow this post to take screenshots.
- R4 - Include the running VMs (1), system timestamp (2) and session information (3) in every single screenshot.
- R5 - Explain your step(s).