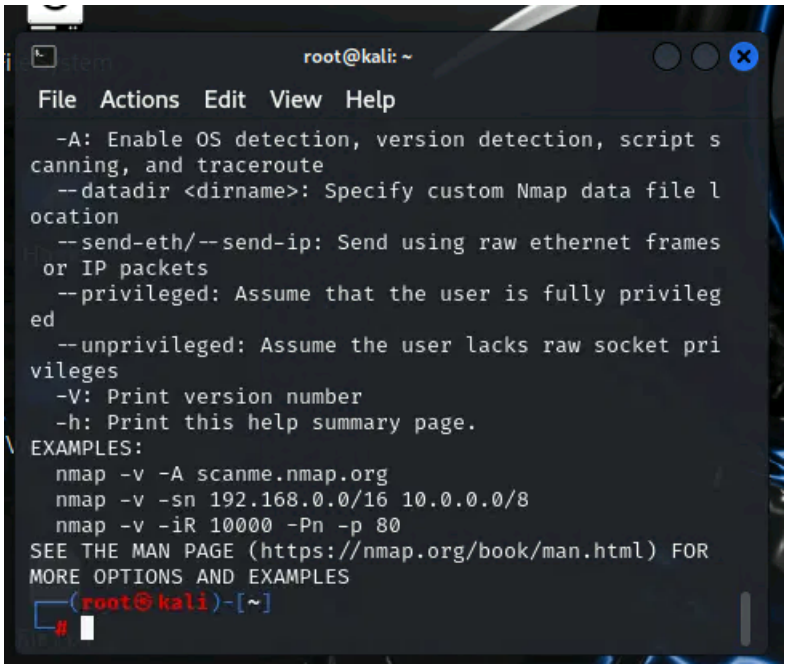
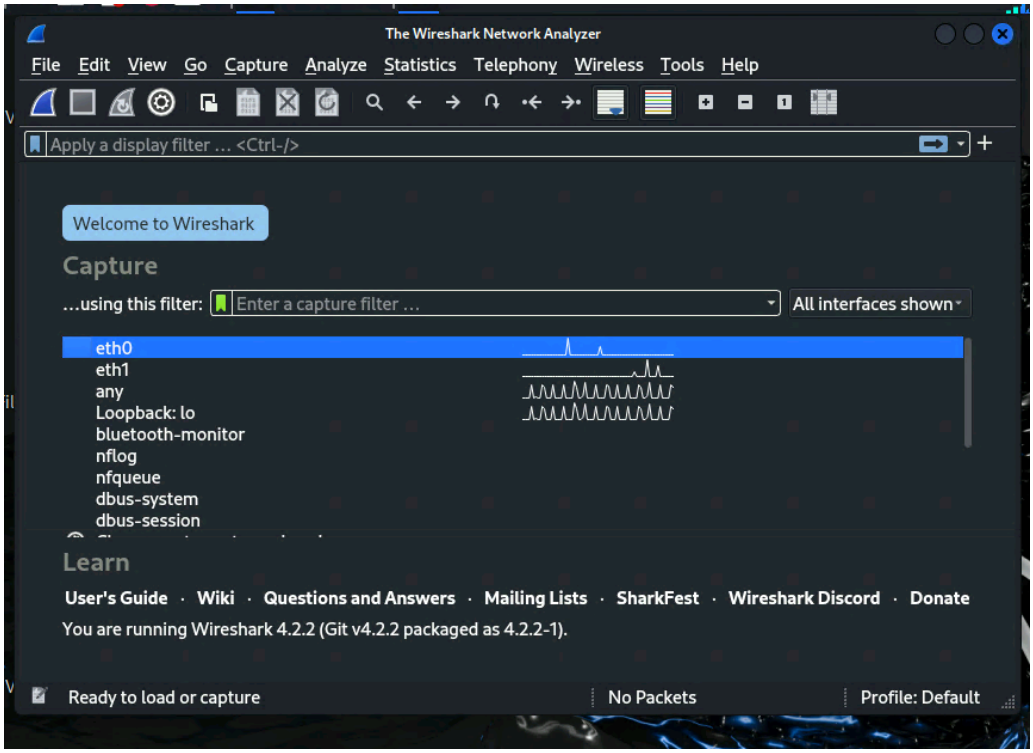
Task A

1. Use Nmap in External Kali to profile the basic information about the subnet topology (including open ports information, operating systems, etc.)





2. You need to submit a table summarizing the following (please add more rows if required):

IP address of VMs	Open ports	Service versions	Operating system detection	Backend software information
192.168.10.19	135 139 445	msrpc netbios-ssn microsoft-ds?	Windows; CPE	N/A
192.168.10.18	21 22	Ftp ssh	Unix, Linux;	N/A

3. Please write a 200-word critical evaluation.

The results from my Nmap and Wireshark scans helped me understand what the network exposes and how an attacker might use that information. The scans showed which devices were active, which ports were open, and what services were running. Any open or unnecessary ports increase the attack surface, and services running older or unpatched versions can create additional risks. Seeing this information laid out makes it clear how much a network reveals even before an attack begins.

From an attacker's point of view, this information is extremely useful. Open ports, service versions, and operating system details help an attacker choose the right tools or exploits. If a device is running something outdated or misconfigured, it becomes a much easier target. Even basic network discovery can guide an attacker toward the weakest system.

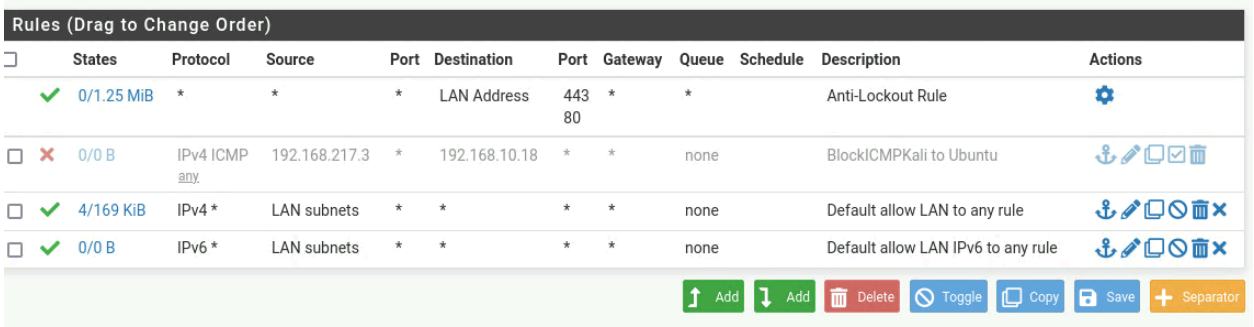
For defenders, the scan results highlight what needs improvement. Closing unused ports, updating software, and tightening firewall rules would reduce exposure. The results also show whether the network is segmented properly or if too many devices are visible at once.

There are some limitations, such as firewalls blocking certain probes or OS detection not being perfect. Still, the scans provide a clear picture of the network's strengths and weaknesses.

Task B

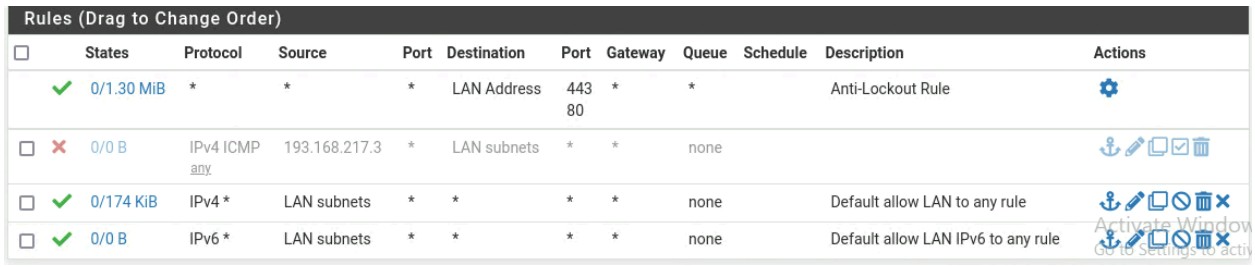
1. Configure the pfSense firewall rule to block the ICMP traffic from External Kali to the Ubuntu VM.

Rule #	interface	action	Source ip	Destination ip	protocol
1	Lan	block	External IP	Ubuntu ip	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
1	Lan	block	External IP	Lan subnet	icmp



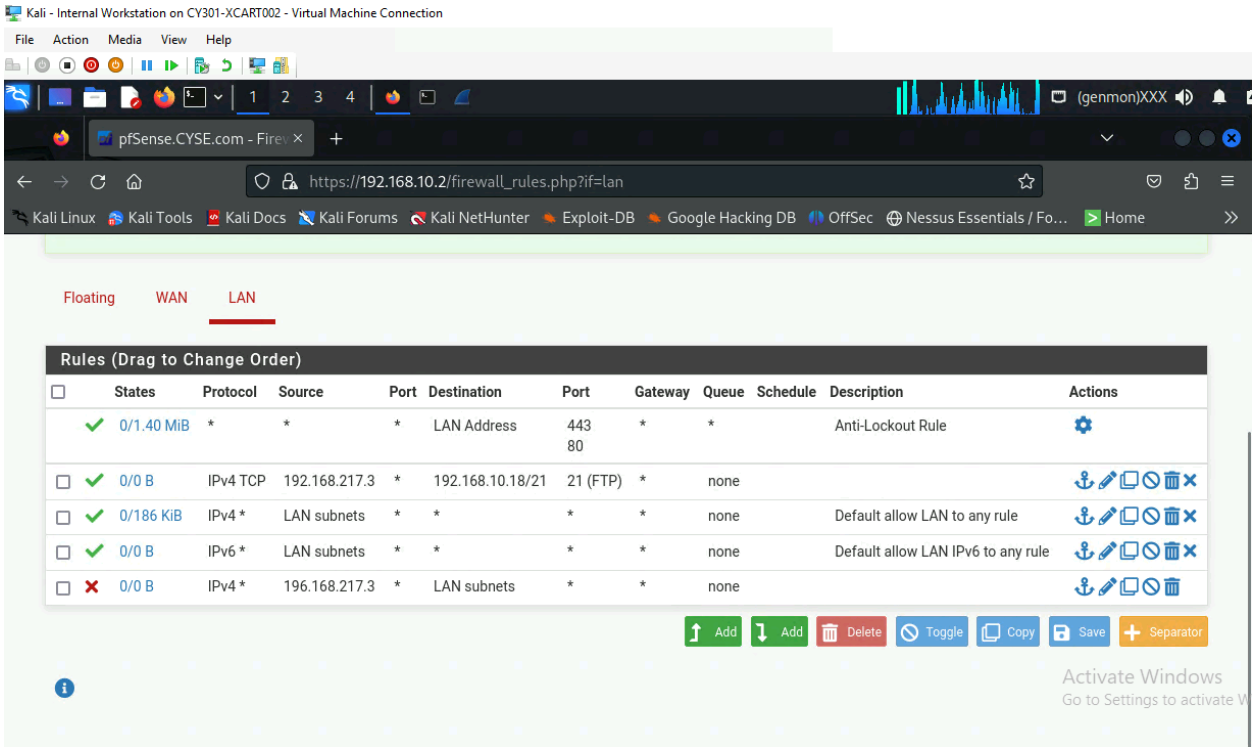
Blocking ICMP traffic from the External Kali machine to the LAN provides important defensive benefits. ICMP is commonly used during the reconnaissance phase of an attack, especially for host discovery and network mapping. By blocking ICMP, the defender prevents an attacker from easily identifying which systems are active, which IP addresses respond, and how the network is structured. This reduces the attacker's ability to plan targeted attacks and forces them to rely on slower or less reliable scanning methods. It also helps hide internal systems by making them appear offline or unreachable.

However, blocking ICMP also creates disadvantages for normal network operations. ICMP is used for legitimate troubleshooting tasks such as checking connectivity, measuring latency, and diagnosing routing issues. Without ICMP responses, administrators may have

difficulty determining whether a device is down or simply filtered. Some network functions, like Path MTU Discovery, also rely on ICMP. Because of this, ICMP blocking improves security but can reduce visibility and complicate network management.

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 directed towards Ubuntu. You can add more rows in the table here, if necessary.

Rule #	interface	action	Source ip	Destination ip	protocol
1	Lan	block	External IP	Lan subnet	any
2	lan	pass	External ip	Ubuntu up	Tcp 21



4.

Category	Before Firewall Rules	After Firewall Rules
Open Ports	Multiple ports visible	Only FTP (21) visible; others filtered
OS Detection	Accurate OS fingerprinting	OS detection fails or shows “unknown”

Service Enumeration	Detailed service versions	Most services hidden or filtered
Host Discovery	All hosts respond to pings	Hosts appear offline due to ICMP blocking

Before applying the firewall rules, Nmap was able to gather detailed information about the network. It detected multiple open ports, identified operating systems, and enumerated services running on different hosts. This level of visibility makes it easy for an attacker to understand the network layout and choose potential targets. The initial scan provided clear OS fingerprints, service versions, and port states, giving an attacker everything needed to plan an effective attack.

After applying the firewall rules, the results changed significantly. Many ports appeared as “filtered,” meaning the firewall blocked the probes instead of allowing a response. This prevents Nmap from determining whether a port is open or closed. Blocking ICMP also caused hosts to appear offline, which disrupts host discovery and OS detection. With most traffic blocked, Nmap could no longer identify services or versions, and OS fingerprinting became unreliable or impossible.

These changes demonstrate how effective firewall rules can be at reducing an attacker’s visibility. By limiting what information is exposed, the defender makes reconnaissance much harder. This strengthens the overall security posture by hiding internal systems and preventing attackers from gathering the details needed to exploit vulnerabilities.