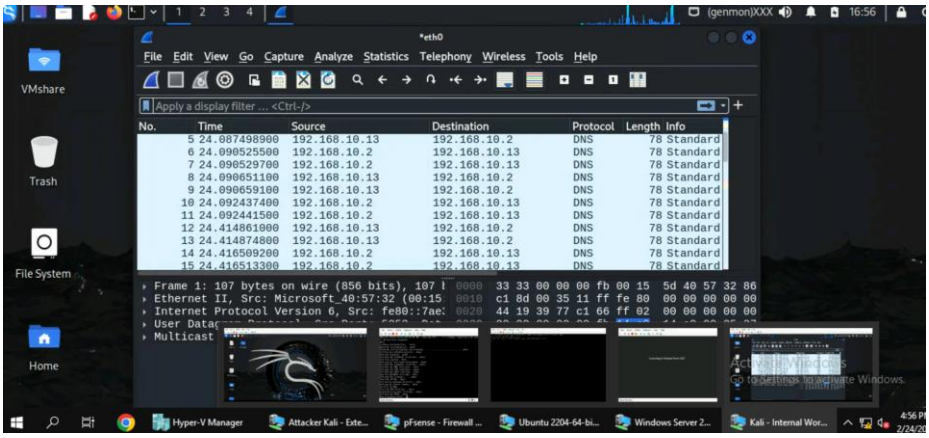
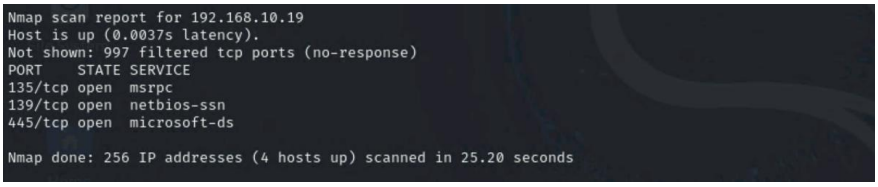
1)



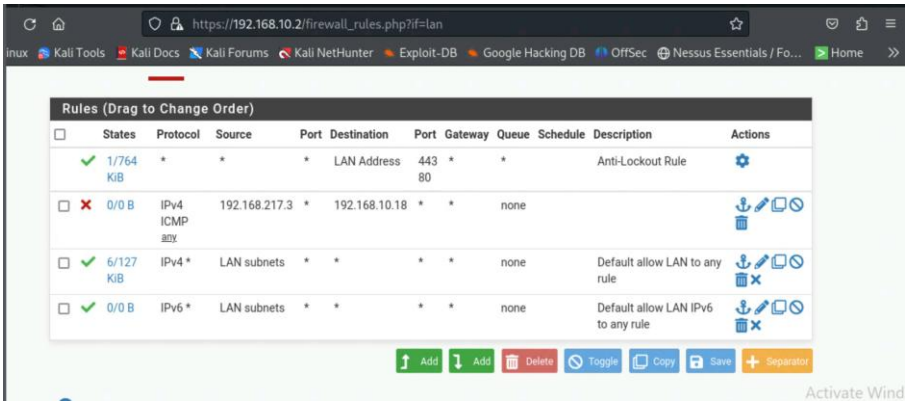
2/3) An Nmap scan was done on the 192.168.10.0/24 network. Four active hosts were found: 192.168.10.2, 192.168.10.13, 192.168.10.18, and 192.168.10.19.192.168.10.2 has ports 53 (DNS), 80 (HTTP), and 443 (HTTPS) open, which means it is likely running web and DNS services. 192.168.10.13 has ports 8000 and 8089 open, which are commonly used for web services. 192.168.10.18 has ports 21 (FTP) and 22 (SSH) open, which are used for file transfer and remote login. 192.168.10.19 has ports 135, 139, and 445 open, which are usually found on Windows systems and are used for file sharing.Service versions and operating system details were not shown because only a basic scan was performed.



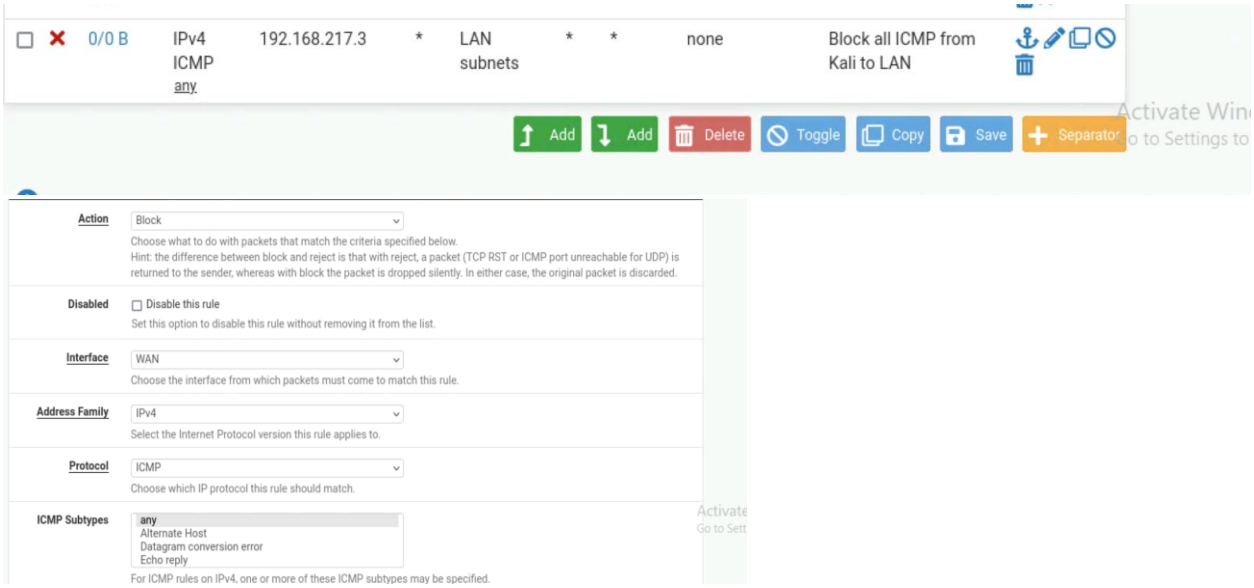


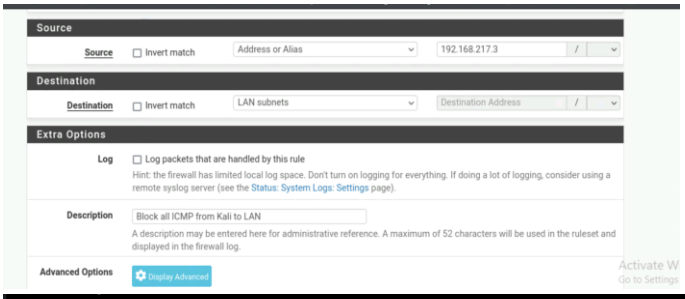
Task B

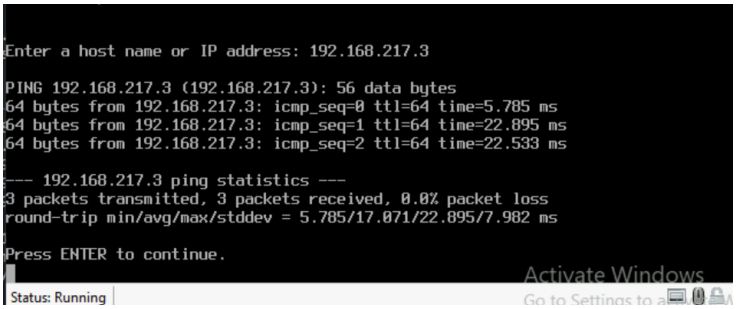
1)


https://192.168.10.2/firewall_rules.php?if=lan
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Nessus Essentials / Fo...
Home
Rules (Drag to Change Order)
States
Protocol
Source
Port
Destination
Port
Gateway
Queue
Schedule
Description
Actions
1/764 KiB
Anti-Lockout Rule
0/0 B
IPv4 ICMP any
192.168.217.3
192.168.10.18
none
6/127 KiB
IPv4 *
LAN subnets
Default allow LAN to any rule
0/0 B
IPv6 *
LAN subnets
Default allow LAN IPv6 to any rule
Add
Add
Delete
Toggle
Copy
Save
Separator

2)


0/0 B
IPv4 ICMP any
192.168.217.3
LAN subnets
none
Block all ICMP from Kali to LAN
Add
Add
Delete
Toggle
Copy
Save
Separator
Action
Block
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.
Disabled
Disable this rule
Set this option to disable this rule without removing it from the list.
Interface
WAN
Choose the interface from which packets must come to match this rule.
Address Family
IPv4
Select the Internet Protocol version this rule applies to.
Protocol
ICMP
Choose which IP protocol this rule should match.
ICMP Subtypes
any
Alternate Host
Datagram conversion error
Echo reply
For ICMP rules on IPv4, one or more of these ICMP subtypes may be specified.

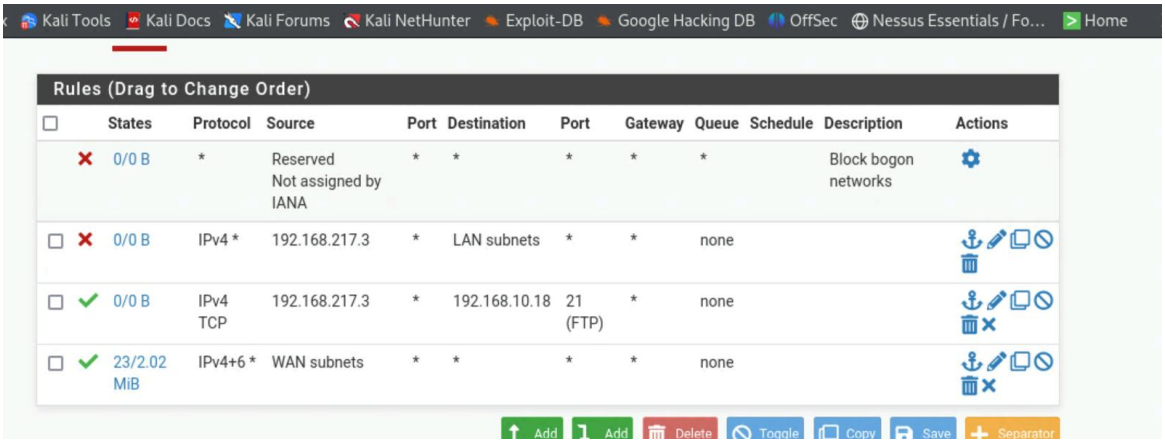




(I don’t know what I did wrong but it doesn’t wan to block)

Blocking ICMP improves security because it hides the network from attackers and stops ping-based attacks. However, it can cause problems for troubleshooting, prevent tools like ping or traceroute from working, and may affect some network functions that rely on ICMP. Often, networks block ICMP from outside but allow it inside to balance security and operation.

3)



4) Nmap shows a port as **filtered** instead of **closed** when it does not get a reply from the target. A closed port sends back a reset (RST) packet telling Nmap the port is not open. But when a firewall blocks or drops packets silently, Nmap cannot tell whether the port is open or closed, so it marks it as filtered.

Firewall behavior changes scan results because it controls which packets can reach the target system. In this lab, the firewall blocks most traffic from the External Kali machine and only allows FTP. This causes Nmap to see port 21 as open while other ports appear filtered. Blocking packets also reduces OS detection accuracy and limits service enumeration because Nmap cannot collect enough response data.

Firewalls hide important information from attackers. This includes which ports are open, what services are running, service versions, and operating system details. By filtering traffic, the firewall reduces the attack surface and makes network scanning harder. Attackers must spend more time guessing or bypassing filters, which improves overall security.