Project-1: Sandbox, Firewall & Access Control

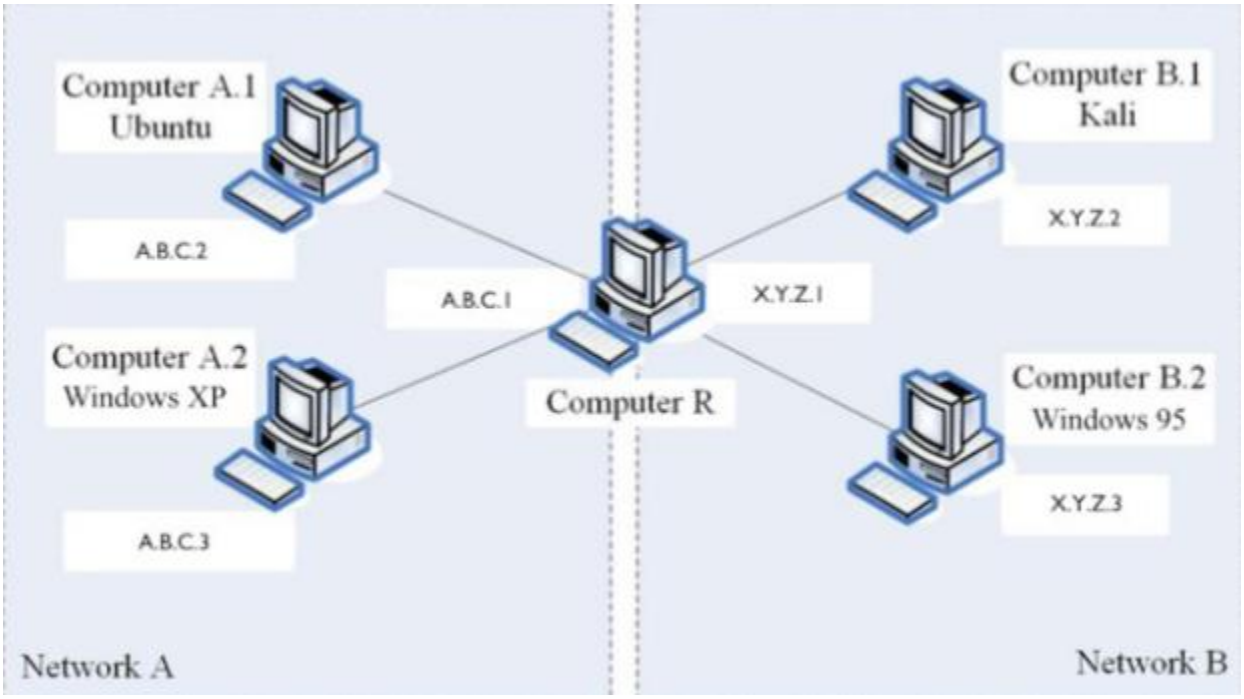
Jesse Ebosele

1 Introduction

This project focuses on understanding and applying security policies within computer networks by building and testing a sandbox environment. The idea is that running security experiments directly on production systems is risky, so creating a controlled virtual environment would allow me to explore networking, system configuration, and security enforcement safely. Using tools such as VirtualBox/VMware, pfSense, NMap, and Wireshark, I'd set up a virtual network consisting of a router and four machines running different operating systems (Ubuntu, Windows XP, Kali Linux, and Windows 95). My goals include constructing and configuring a sandbox virtual network, testing network connectivity and diagnosing traffic with security tools, implementing and enforcing a formal security policy through router rules and server configurations, and verifying security enforcement by analyzing network traffic and scanning exposed services.

2 Section II

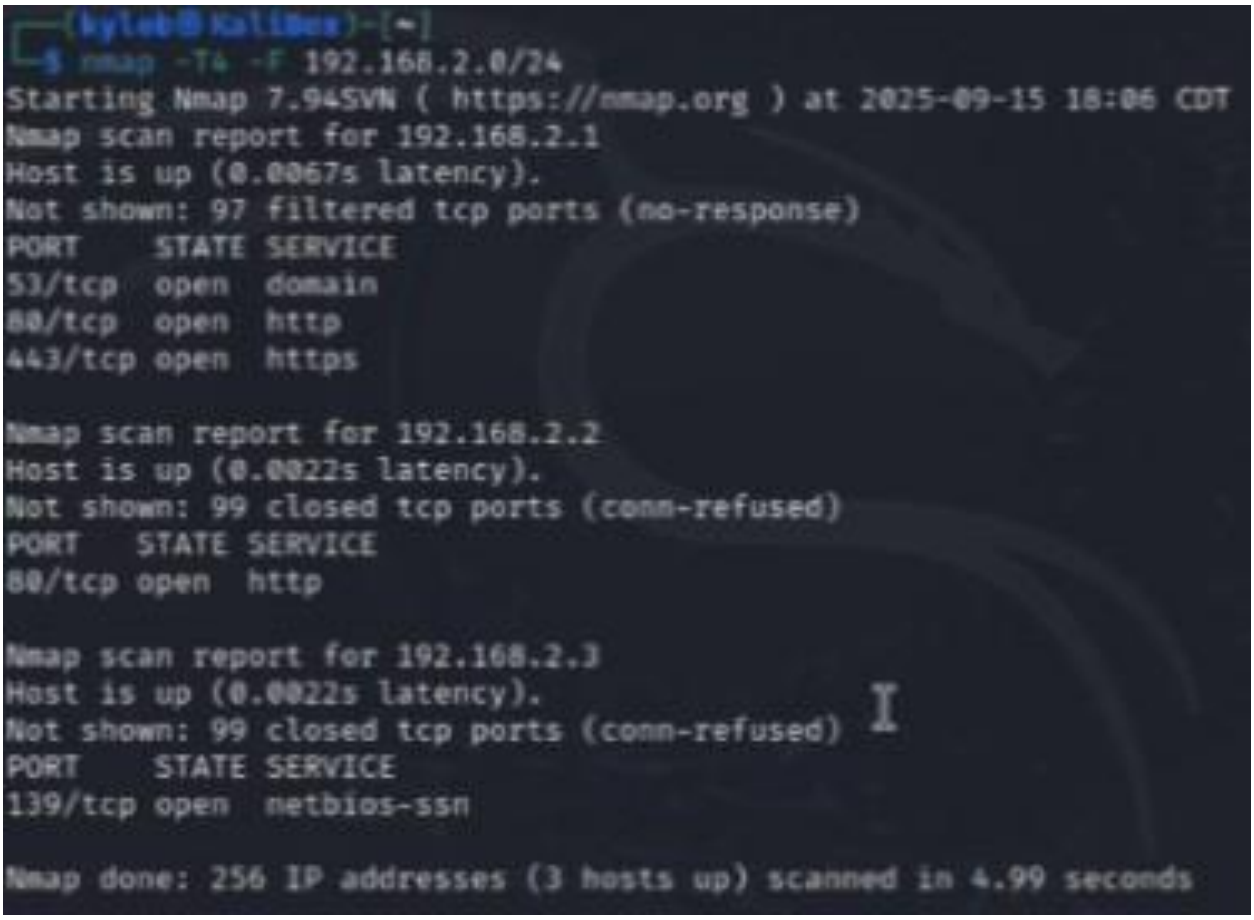
Screenshot of machines on V.M



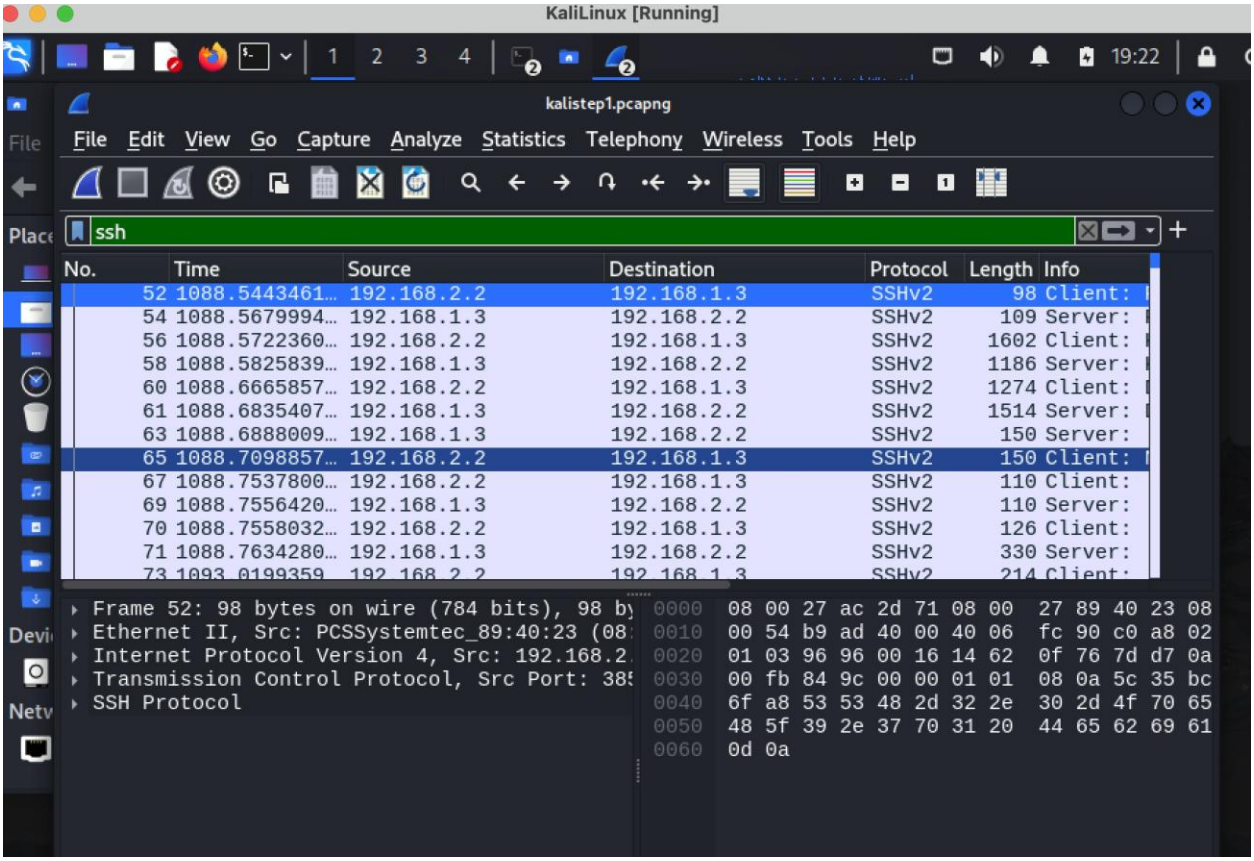
An abstract
view of the machines, where A.B.C.? and X.Y.Z.? represent /24 group IP addresses

NMAP for network 1

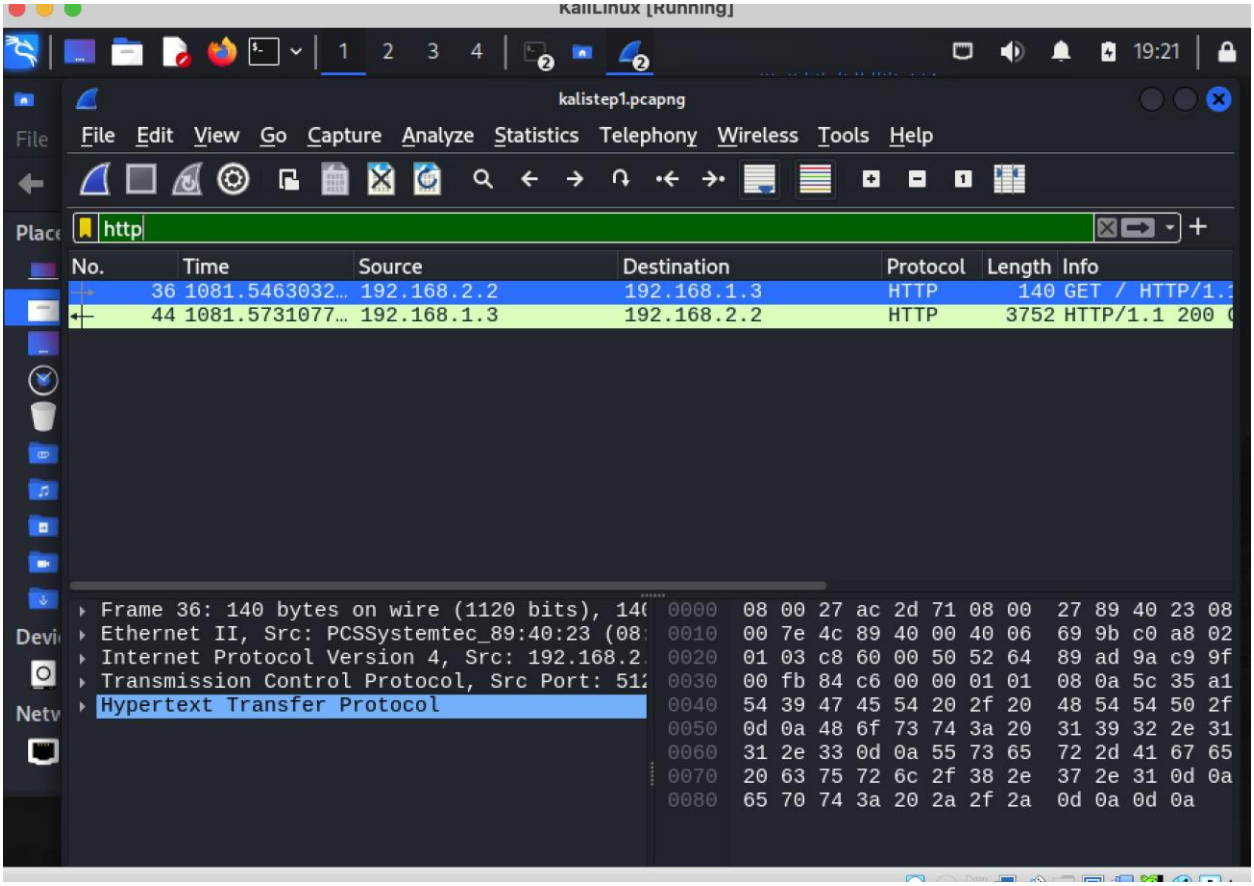
NMAP network 2



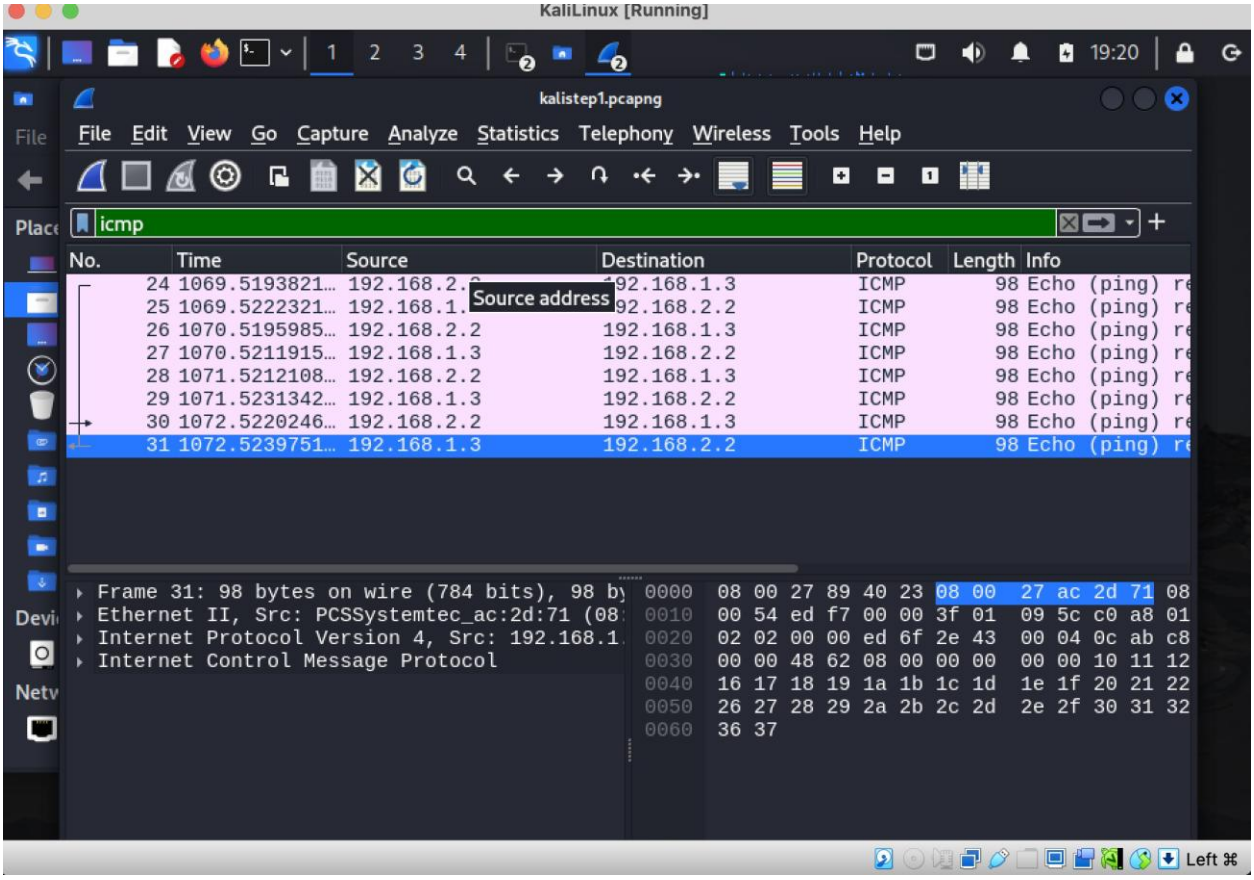
Network discovery packets, Kali to Ubuntu – Kali's perspective


KaliLinux [Running]
kalistep1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ssh
No. Time Source Destination Protocol Length Info
52 1088.5443461… 192.168.2.2 192.168.1.3 SSHv2 98 Client:
54 1088.5679994… 192.168.1.3 192.168.2.2 SSHv2 109 Server:
56 1088.5722360… 192.168.2.2 192.168.1.3 SSHv2 1602 Client:
58 1088.5825839… 192.168.1.3 192.168.2.2 SSHv2 1186 Server:
60 1088.6665857… 192.168.2.2 192.168.1.3 SSHv2 1274 Client:
61 1088.6835407… 192.168.1.3 192.168.2.2 SSHv2 1514 Server:
63 1088.6888009… 192.168.1.3 192.168.2.2 SSHv2 150 Server:
65 1088.7098857… 192.168.2.2 192.168.1.3 SSHv2 150 Client:
67 1088.7537800… 192.168.2.2 192.168.1.3 SSHv2 110 Client:
69 1088.7556420… 192.168.1.3 192.168.2.2 SSHv2 110 Server:
70 1088.7558032… 192.168.2.2 192.168.1.3 SSHv2 126 Client:
71 1088.7634280… 192.168.1.3 192.168.2.2 SSHv2 330 Server:
Frame 52: 98 bytes on wire (784 bits), 98 by
Ethernet II, Src: PCSSystemtec_89:40:23 (08
Internet Protocol Version 4, Src: 192.168.2
Transmission Control Protocol, Src Port: 385
SSH Protocol
0000 08 00 27 ac 2d 71 08 00 27 89 40 23 08
0010 00 54 b9 ad 40 00 40 06 fc 90 c0 a8 02
0020 01 03 96 96 00 16 14 62 0f 76 7d d7 0a
0030 00 fb 84 9c 00 00 01 01 08 0a 5c 35 bc
0040 6f a8 53 53 48 2d 32 2e 30 2d 4f 70 65
0050 48 5f 39 2e 37 70 31 20 44 65 62 69 61
0060 0d 0a

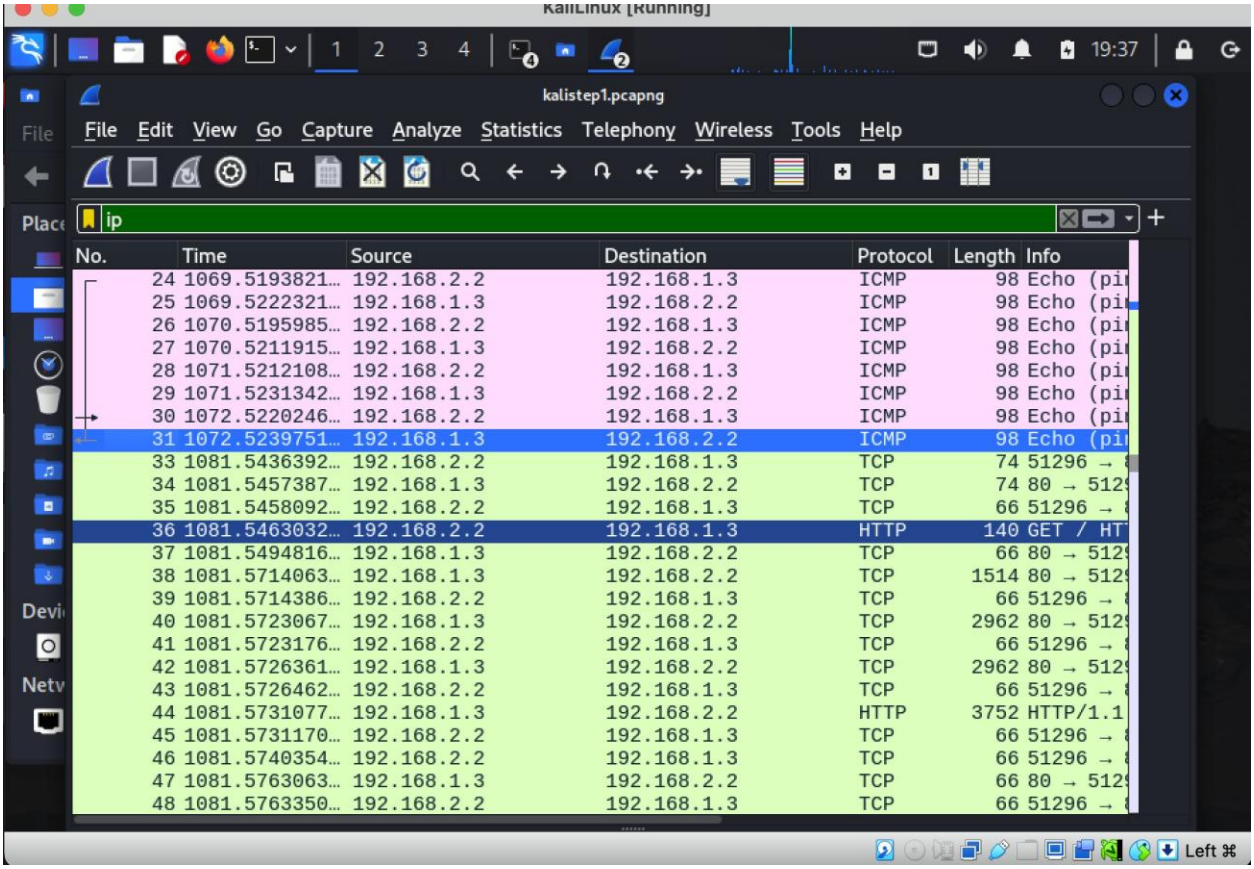
SSH


KaliLinux [Running]
19:21
kalistep1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
36 1081.5463032… 192.168.2.2 192.168.1.3 HTTP 140 GET / HTTP/1.1
44 1081.5731077… 192.168.1.3 192.168.2.2 HTTP 3752 HTTP/1.1 200
Frame 36: 140 bytes on wire (1120 bits), 140
Ethernet II, Src: PCSSystemtec_89:40:23 (08
Internet Protocol Version 4, Src: 192.168.2.
Transmission Control Protocol, Src Port: 512
Hypertext Transfer Protocol
0000 08 00 27 ac 2d 71 08 00 27 89 40 23 08
0010 00 7e 4c 89 40 00 40 06 69 9b c0 a8 02
0020 01 03 c8 60 00 50 52 64 89 ad 9a c9 9f
0030 00 fb 84 c6 00 00 01 01 08 0a 5c 35 a1
0040 54 39 47 45 54 20 2f 20 48 54 54 50 2f
0050 0d 0a 48 6f 73 74 3a 20 31 39 32 2e 31
0060 31 2e 33 0d 0a 55 73 65 72 2d 41 67 65
0070 20 63 75 72 6c 2f 38 2e 37 2e 31 0d 0a
0080 65 70 74 3a 20 2a 2f 2a 0d 0a 0d 0a

HTTP

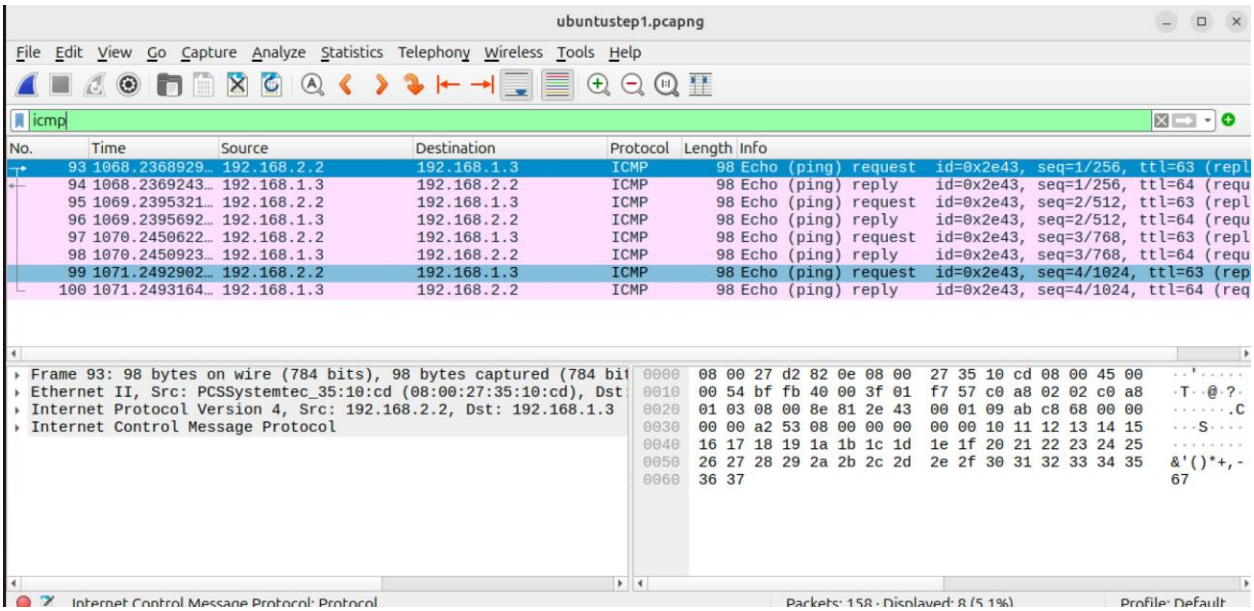

KaliLinux [Running]
19:20
kalistep1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
No. Time Source Destination Protocol Length Info
24 1069.5193821… 192.168.2.2 192.168.1.3 ICMP 98 Echo (ping) re
25 1069.5222321… 192.168.1.3 192.168.2.2 ICMP 98 Echo (ping) re
26 1070.5195985… 192.168.2.2 192.168.1.3 ICMP 98 Echo (ping) re
27 1070.5211915… 192.168.1.3 192.168.2.2 ICMP 98 Echo (ping) re
28 1071.5212108… 192.168.2.2 192.168.1.3 ICMP 98 Echo (ping) re
29 1071.5231342… 192.168.1.3 192.168.2.2 ICMP 98 Echo (ping) re
30 1072.5220246… 192.168.2.2 192.168.1.3 ICMP 98 Echo (ping) re
31 1072.5239751… 192.168.1.3 192.168.2.2 ICMP 98 Echo (ping) re
Source address
Frame 31: 98 bytes on wire (784 bits), 98 by
Ethernet II, Src: PCSSystemtec_ac:2d:71 (08:
Internet Protocol Version 4, Src: 192.168.1.
Internet Control Message Protocol
0000 08 00 27 89 40 23 08 00 27 ac 2d 71 08
0010 00 54 ed f7 00 00 3f 01 09 5c c0 a8 01
0020 02 02 00 00 ed 6f 2e 43 00 04 0c ab c8
0030 00 00 48 62 08 00 00 00 00 00 10 11 12
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32
0060 36 37
Left ⌘

ICMP

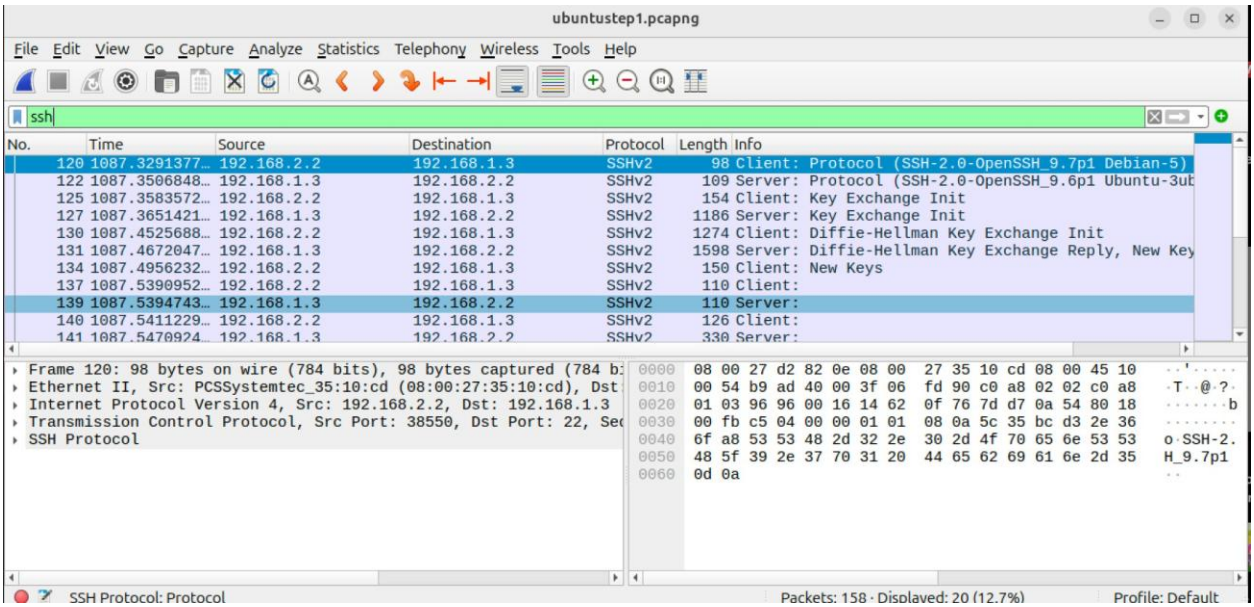


IP traffic

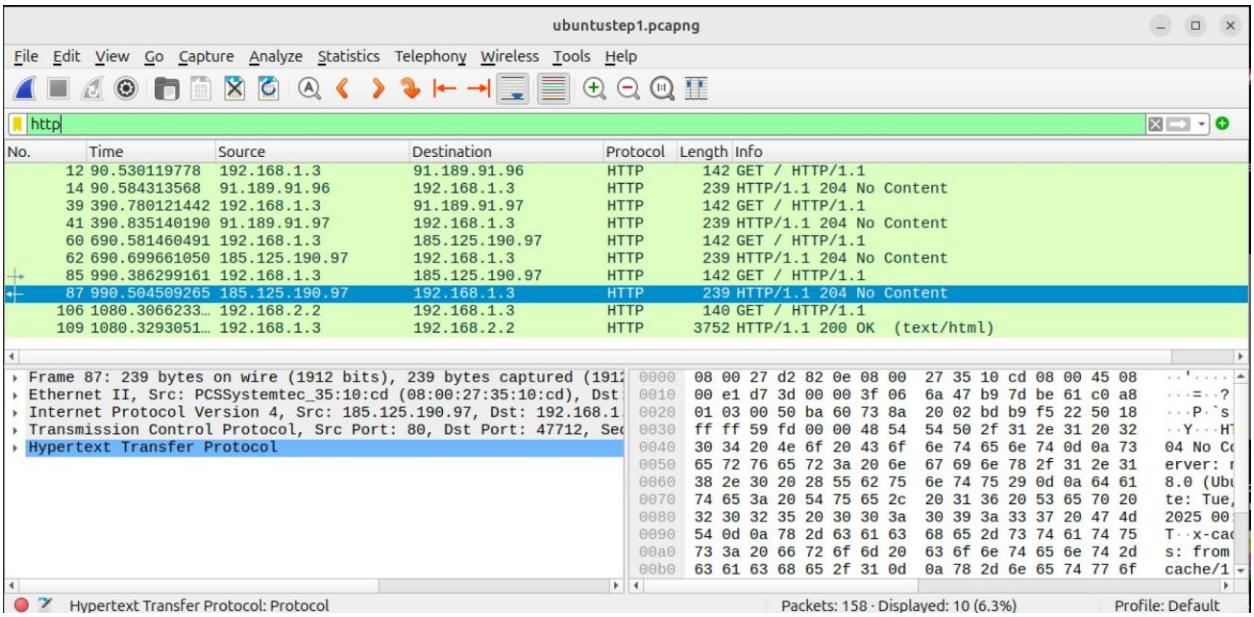
Ubuntu's perspective



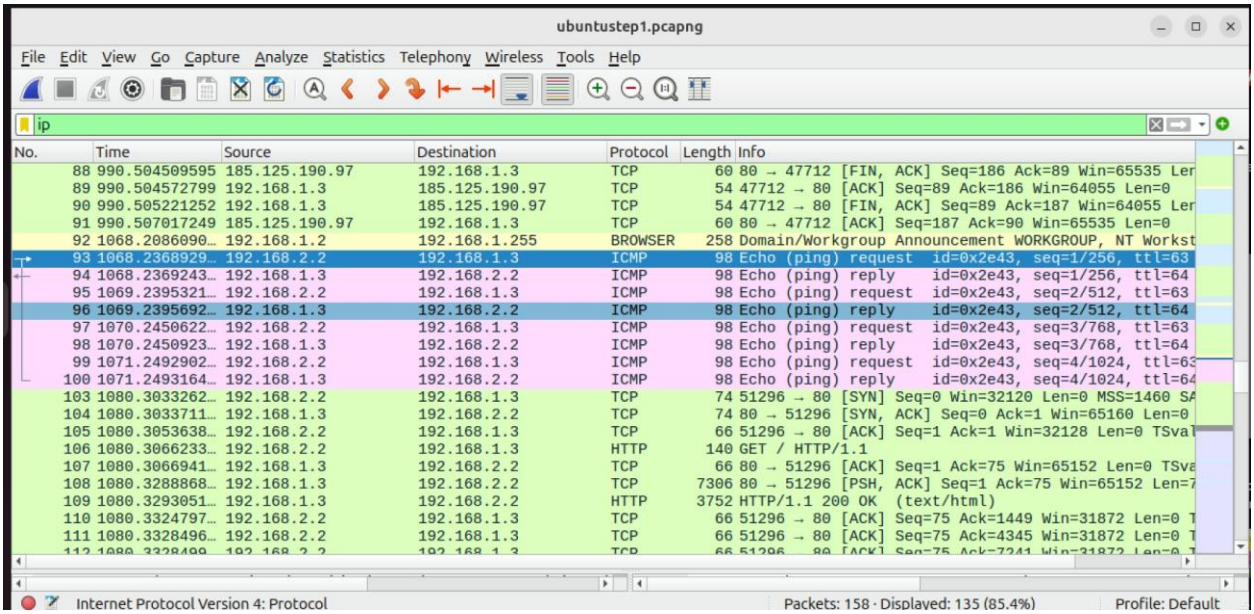
ICMP


ubuntustep1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ssh
No. Time Source Destination Protocol Length Info
120 1087.3291377… 192.168.2.2 192.168.1.3 SSHv2 98 Client: Protocol (SSH-2.0-OpenSSH_9.7p1 Debian-5)
122 1087.3506848… 192.168.1.3 192.168.2.2 SSHv2 109 Server: Protocol (SSH-2.0-OpenSSH_9.6p1 Ubuntu-3ub
125 1087.3583572… 192.168.2.2 192.168.1.3 SSHv2 154 Client: Key Exchange Init
127 1087.3651421… 192.168.1.3 192.168.2.2 SSHv2 1186 Server: Key Exchange Init
130 1087.4525688… 192.168.2.2 192.168.1.3 SSHv2 1274 Client: Diffie-Hellman Key Exchange Init
131 1087.4672047… 192.168.1.3 192.168.2.2 SSHv2 1598 Server: Diffie-Hellman Key Exchange Reply, New Key
134 1087.4956232… 192.168.2.2 192.168.1.3 SSHv2 150 Client: New Keys
137 1087.5390952… 192.168.2.2 192.168.1.3 SSHv2 110 Client:
139 1087.5394743… 192.168.1.3 192.168.2.2 SSHv2 110 Server:
140 1087.5411229… 192.168.2.2 192.168.1.3 SSHv2 126 Client:
141 1087.5470924… 192.168.1.3 192.168.2.2 SSHv2 330 Server:
Frame 120: 98 bytes on wire (784 bits), 98 bytes captured (784 b
Ethernet II, Src: PCSSystemtec_35:10:cd (08:00:27:35:10:cd), Dst
Internet Protocol Version 4, Src: 192.168.2.2, Dst: 192.168.1.3
Transmission Control Protocol, Src Port: 38550, Dst Port: 22, Se
SSH Protocol
0000 08 00 27 d2 82 0e 08 00 27 35 10 cd 08 00 45 10
0010 00 54 b9 ad 40 00 3f 06 fd 90 c0 a8 02 02 c0 a8
0020 01 03 96 96 00 16 14 62 0f 76 7d d7 0a 54 80 18
0030 00 fb c5 04 00 00 01 01 08 0a 5c 35 bc d3 2e 36
0040 6f a8 53 53 48 2d 32 2e 30 2d 4f 70 65 6e 53 53
0050 48 5f 39 2e 37 70 31 20 44 65 62 69 61 6e 2d 35
0060 0d 0a
SSH Protocol: Protocol
Packets: 158 · Displayed: 20 (12.7%)
Profile: Default

SSH

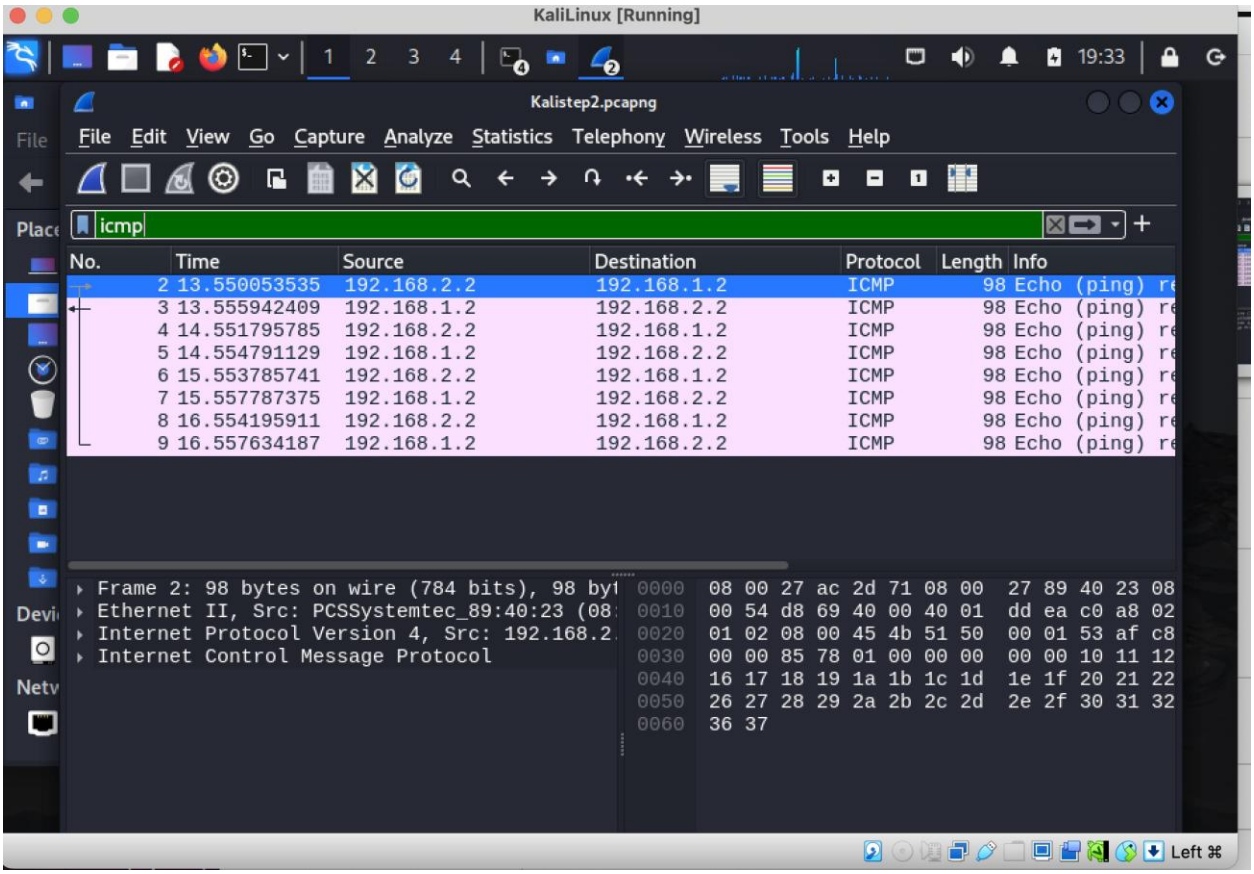

ubuntustep1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
12 90.530119778 192.168.1.3 91.189.91.96 HTTP 142 GET / HTTP/1.1
14 90.584313568 91.189.91.96 192.168.1.3 HTTP 239 HTTP/1.1 204 No Content
39 390.780121442 192.168.1.3 91.189.91.97 HTTP 142 GET / HTTP/1.1
41 390.835140190 91.189.91.97 192.168.1.3 HTTP 239 HTTP/1.1 204 No Content
60 690.581460491 192.168.1.3 185.125.190.97 HTTP 142 GET / HTTP/1.1
62 690.699661050 185.125.190.97 192.168.1.3 HTTP 239 HTTP/1.1 204 No Content
85 990.386299161 192.168.1.3 185.125.190.97 HTTP 142 GET / HTTP/1.1
87 990.504509265 185.125.190.97 192.168.1.3 HTTP 239 HTTP/1.1 204 No Content
106 1080.3066233… 192.168.2.2 192.168.1.3 HTTP 140 GET / HTTP/1.1
109 1080.3293051… 192.168.1.3 192.168.2.2 HTTP 3752 HTTP/1.1 200 OK (text/html)
Frame 87: 239 bytes on wire (1912 bits), 239 bytes captured (191
Ethernet II, Src: PCSSystemtec_35:10:cd (08:00:27:35:10:cd), Dst
Internet Protocol Version 4, Src: 185.125.190.97, Dst: 192.168.1
Transmission Control Protocol, Src Port: 80, Dst Port: 47712, Se
Hypertext Transfer Protocol
0000 08 00 27 d2 82 0e 08 00 27 35 10 cd 08 00 45 08
0010 00 e1 d7 3d 00 00 3f 06 6a 47 b9 7d be 61 c0 a8
0020 01 03 00 50 ba 60 73 8a 20 02 bd b9 f5 22 50 18
0030 ff ff 59 fd 00 00 48 54 54 50 2f 31 2e 31 20 32
0040 30 34 20 4e 6f 20 43 6f 6e 74 65 6e 74 0d 0a 73
0050 65 72 76 65 72 3a 20 6e 67 69 6e 78 2f 31 2e 31
0060 38 2e 30 20 28 55 62 75 6e 74 75 29 0d 0a 64 61
0070 74 65 3a 20 54 75 65 2c 20 31 36 20 53 65 70 20
0080 32 30 32 35 20 30 30 3a 30 39 3a 33 37 20 47 4d
0090 54 0d 0a 78 2d 63 61 63 68 65 2d 73 74 61 74 75
00a0 73 3a 20 66 72 6f 6d 20 63 6f 6e 74 65 6e 74 2d
00b0 63 61 63 68 65 2f 31 0d 0a 78 2d 6e 65 74 77 6f
Hypertext Transfer Protocol: Protocol
Packets: 158 · Displayed: 10 (6.3%)
Profile: Default

HTTP



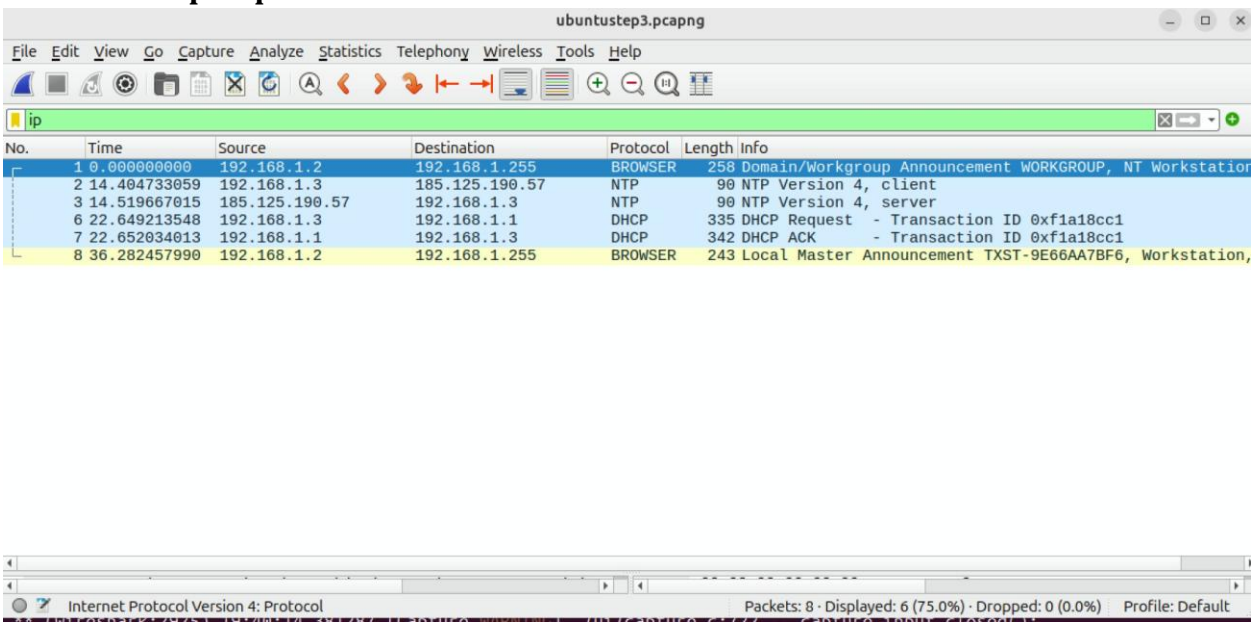
IP traffic

Kali to XP – Kali's perspective

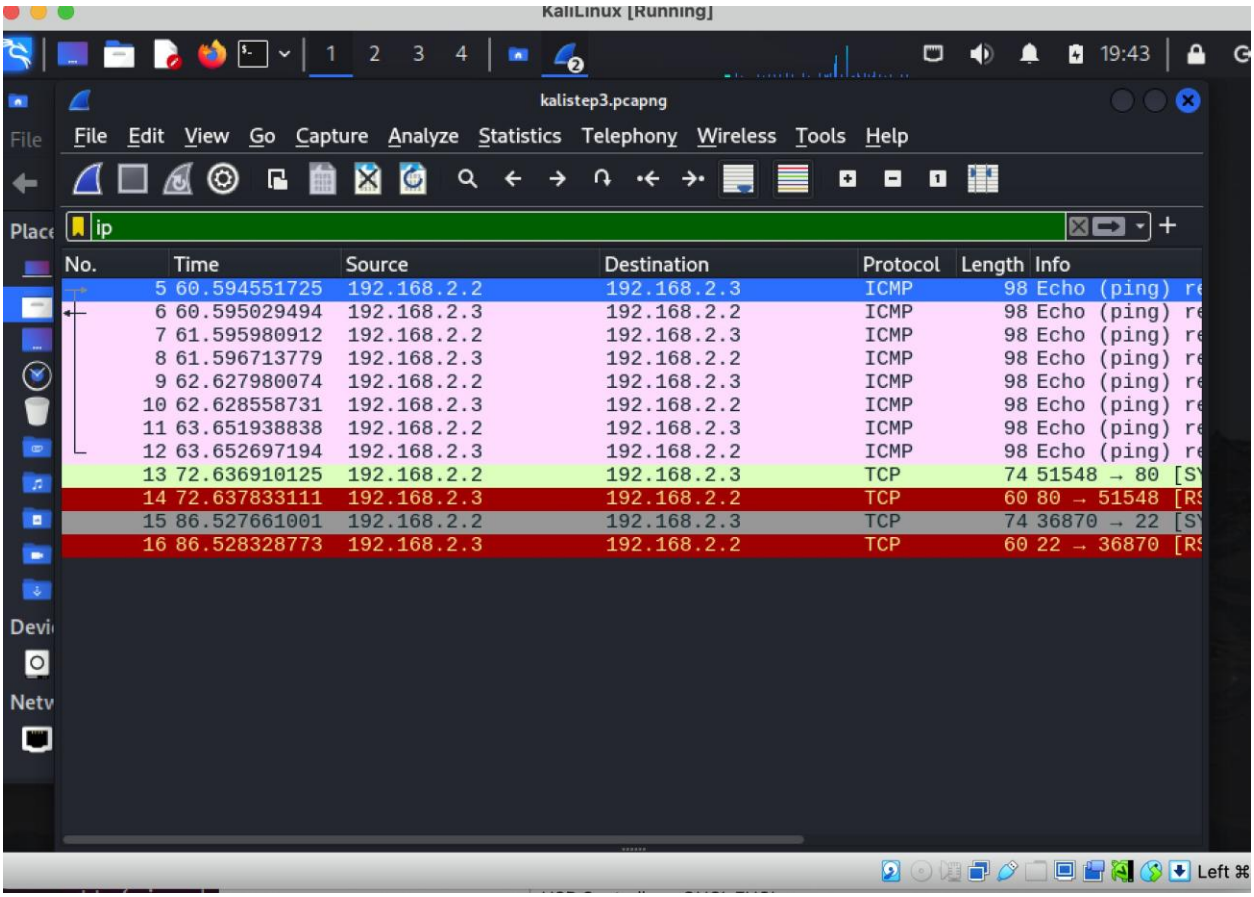


ICMP

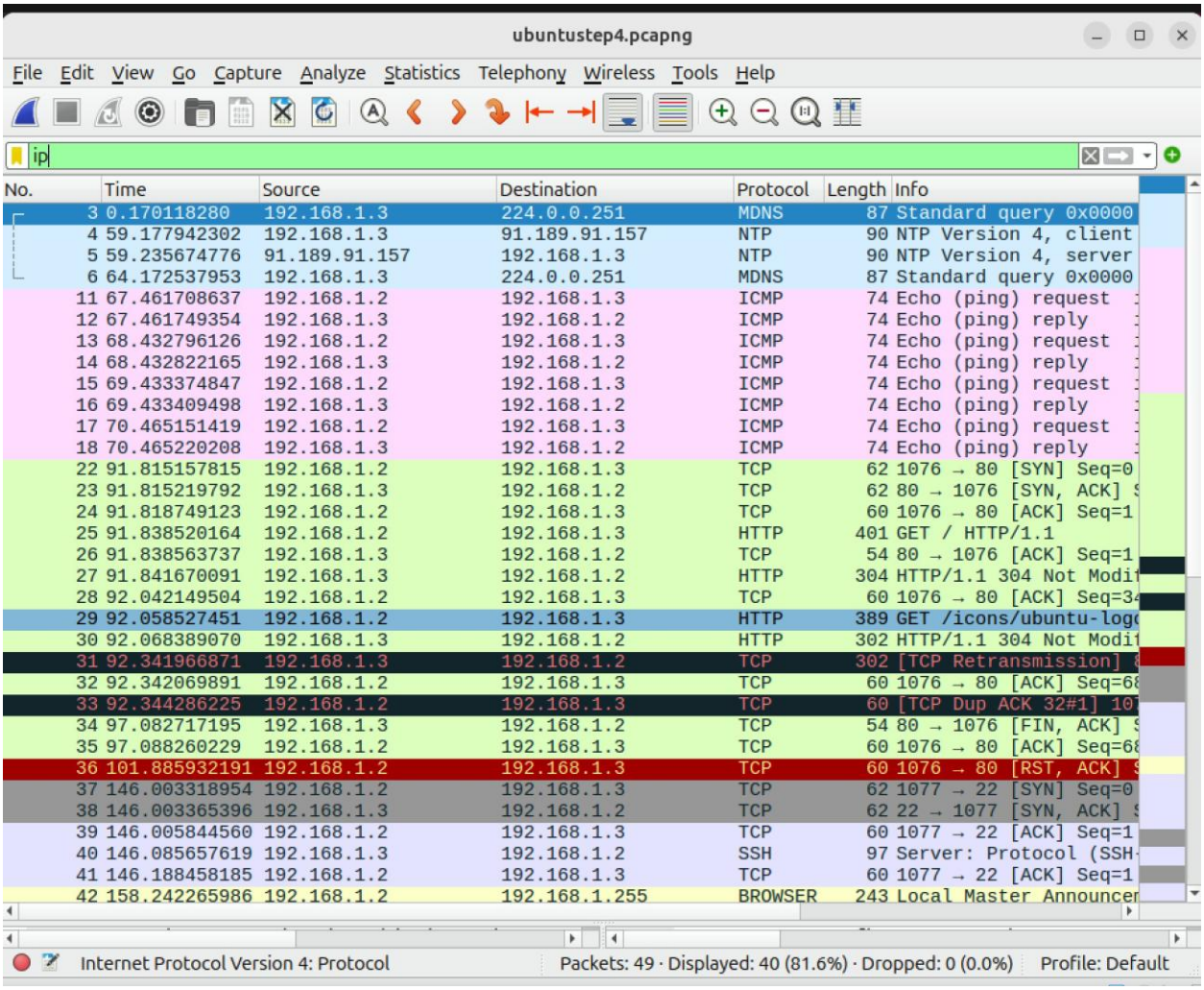
Ubuntu's perspective



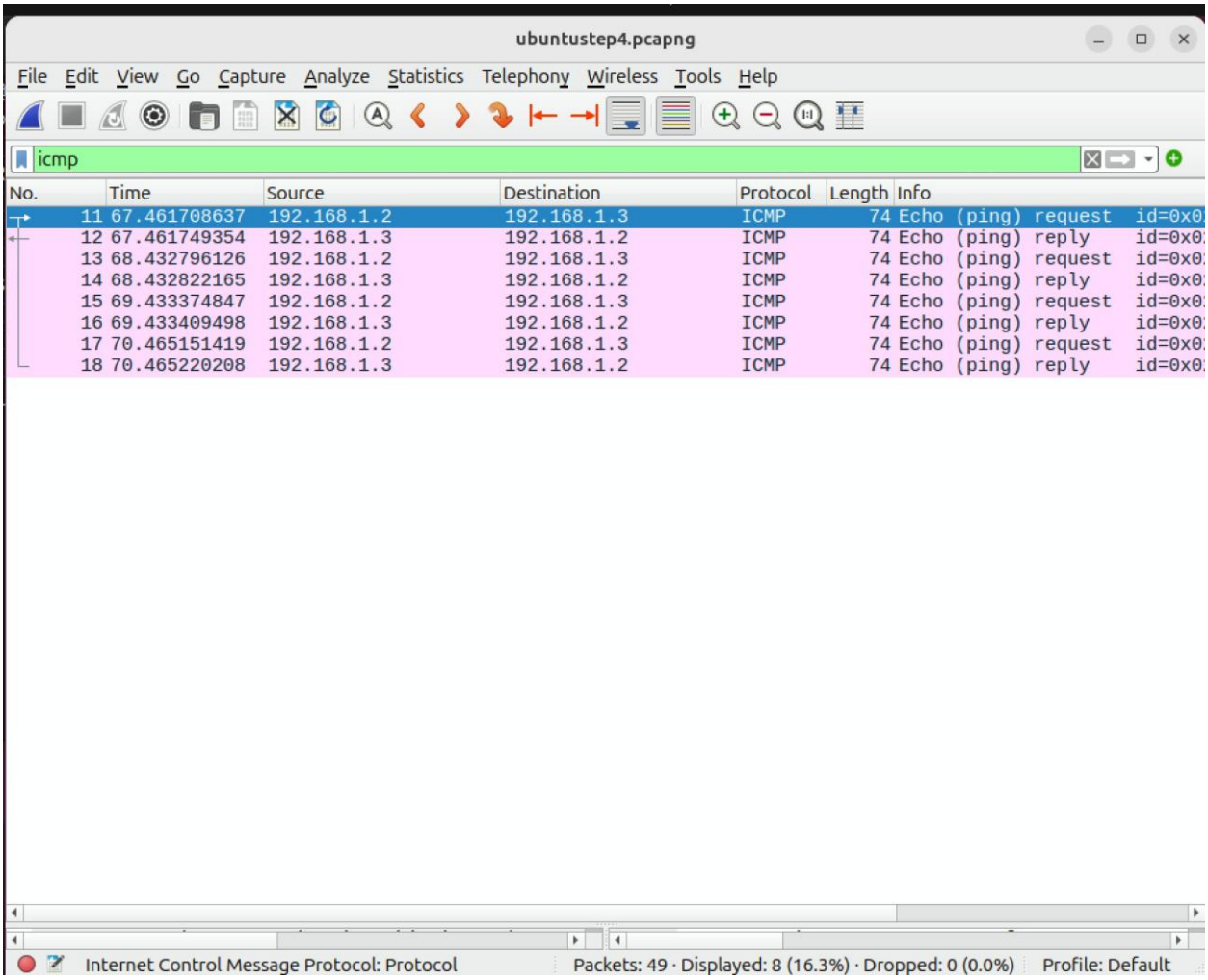
IP: Kali to 95, with Kali's perspective, pings succeeded, HTTP and SSH failed



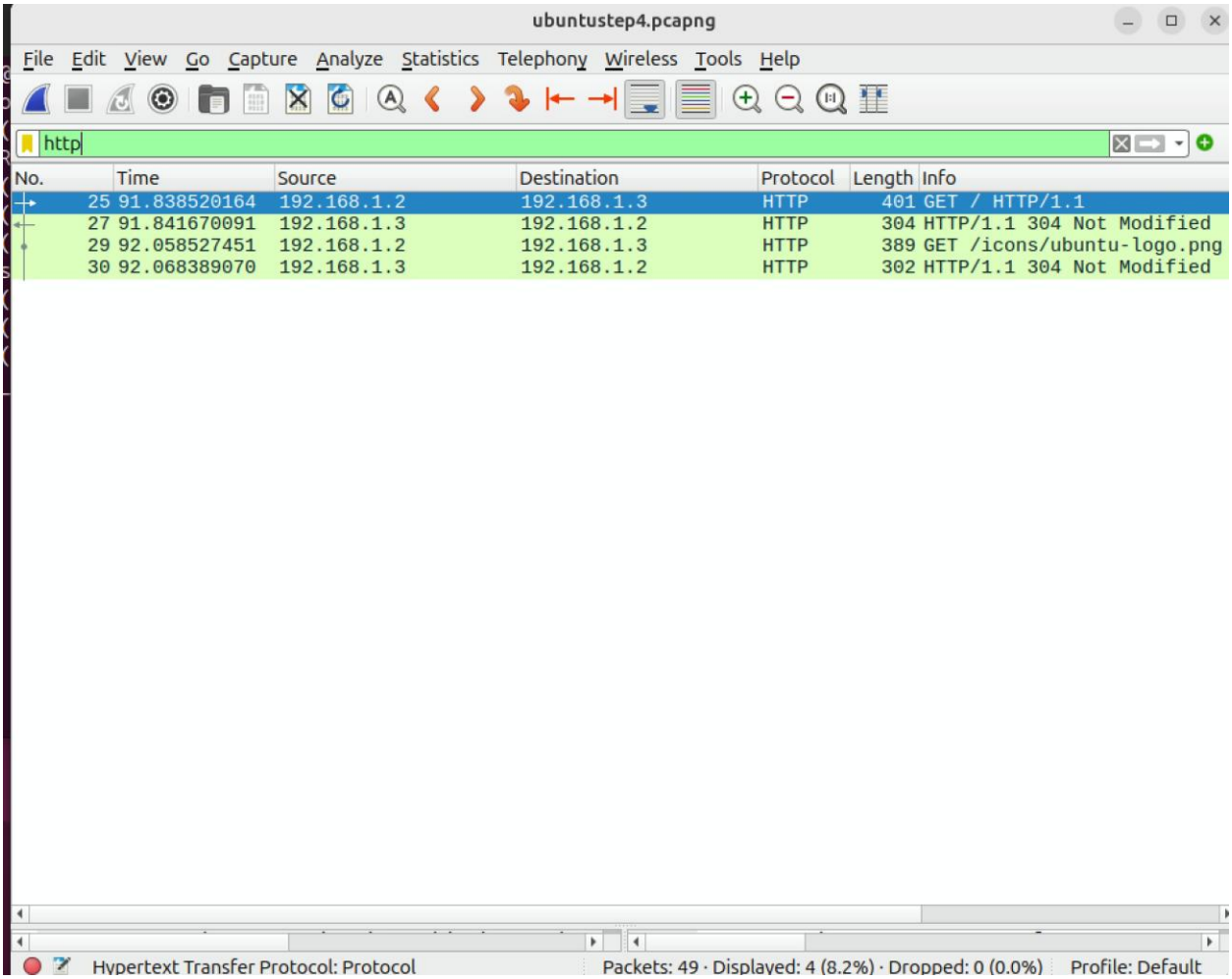
XP to Ubuntu



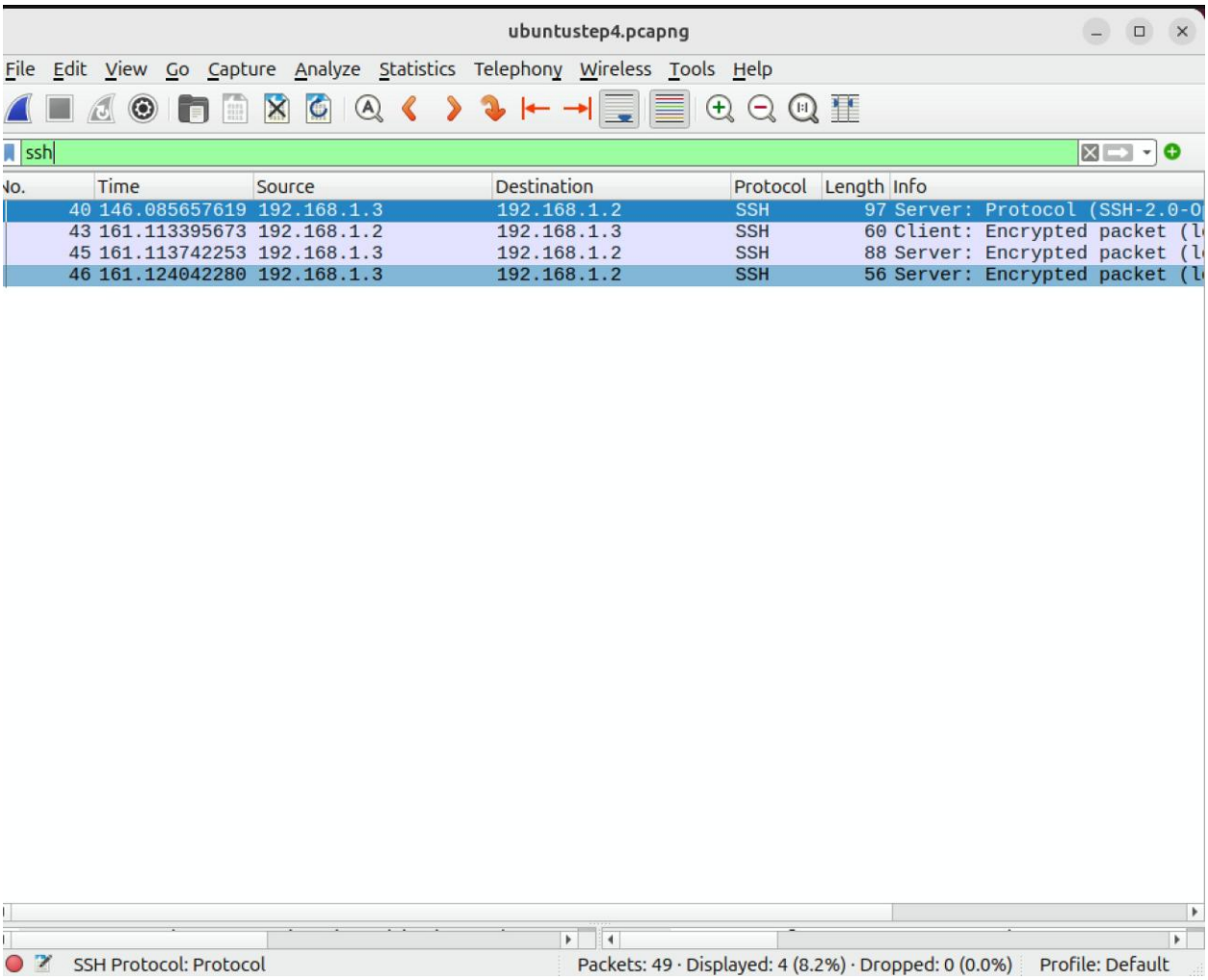
IP traffic


ubuntustep4.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
No. Time Source Destination Protocol Length Info
11 67.461708637 192.168.1.2 192.168.1.3 ICMP 74 Echo (ping) request id=0x0
12 67.461749354 192.168.1.3 192.168.1.2 ICMP 74 Echo (ping) reply id=0x0
13 68.432796126 192.168.1.2 192.168.1.3 ICMP 74 Echo (ping) request id=0x0
14 68.432822165 192.168.1.3 192.168.1.2 ICMP 74 Echo (ping) reply id=0x0
15 69.433374847 192.168.1.2 192.168.1.3 ICMP 74 Echo (ping) request id=0x0
16 69.433409498 192.168.1.3 192.168.1.2 ICMP 74 Echo (ping) reply id=0x0
17 70.465151419 192.168.1.2 192.168.1.3 ICMP 74 Echo (ping) request id=0x0
18 70.465220208 192.168.1.3 192.168.1.2 ICMP 74 Echo (ping) reply id=0x0
Internet Control Message Protocol: Protocol
Packets: 49 · Displayed: 8 (16.3%) · Dropped: 0 (0.0%)
Profile: Default

ICMP


ubuntustep4.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
25 91.838520164 192.168.1.2 192.168.1.3 HTTP 401 GET / HTTP/1.1
27 91.841670091 192.168.1.3 192.168.1.2 HTTP 304 HTTP/1.1 304 Not Modified
29 92.058527451 192.168.1.2 192.168.1.3 HTTP 389 GET /icons/ubuntu-logo.png
30 92.068389070 192.168.1.3 192.168.1.2 HTTP 302 HTTP/1.1 304 Not Modified
Hypertext Transfer Protocol: Protocol
Packets: 49 · Displayed: 4 (8.2%) · Dropped: 0 (0.0%)
Profile: Default

HTTP



TCP

Note: Processes allowed before security implementation: Everything. The firewall is set to allow all processes to and from all computers.

3 Section III

From \ To	A.1 (80,443,22)	A.2 (no services)	B.1/B.2 (External)
A.1	–	(N/A)	❌ services (may ping)
A.2	✅ 22,80,443	–	✅ web only (80,443)
External (B.*)	✅ web only (80,443)	❌	–

Plus ICMP: **A.*** may ping out; **External cannot ping A.***. You're required to include an ACM in Task-IV.1.

Access Control Matrix

1) Access Control Matrix (subjects → objects/services)

Notation

- Hosts: **A.1** (server), **A.2** (workstation), **B.1/B.2** (external)
- Services (objects) shown as "Host:port/proto" or "ICMP"
- "✓ allow", "× deny"

Subject \ Object	A.1:80/443 (web)	A.1:22 (ssh)	A.2:any (any service)	B.*:80/443 (external web)	B.*:any (all other)	ICMP (ping)
B. →*	✓ (A)	× (A)	× (D,H)	n/a	n/a	× (H)
A.2 →	✓ (B,E)	✓ (B,E)	n/a	✓ (F)	× (F)	✓ (G)
A.1 →	n/a	n/a	× (B/E imply server doesn't consume ws services)	× (C)	× (C)	✓ (G)
A. (internal) → *internal**	As above; A.2→A.1 web/ssh allowed; A.1→A.2 services **not required**					✓ (G)

Policies that cannot be completely enforced by router rules:

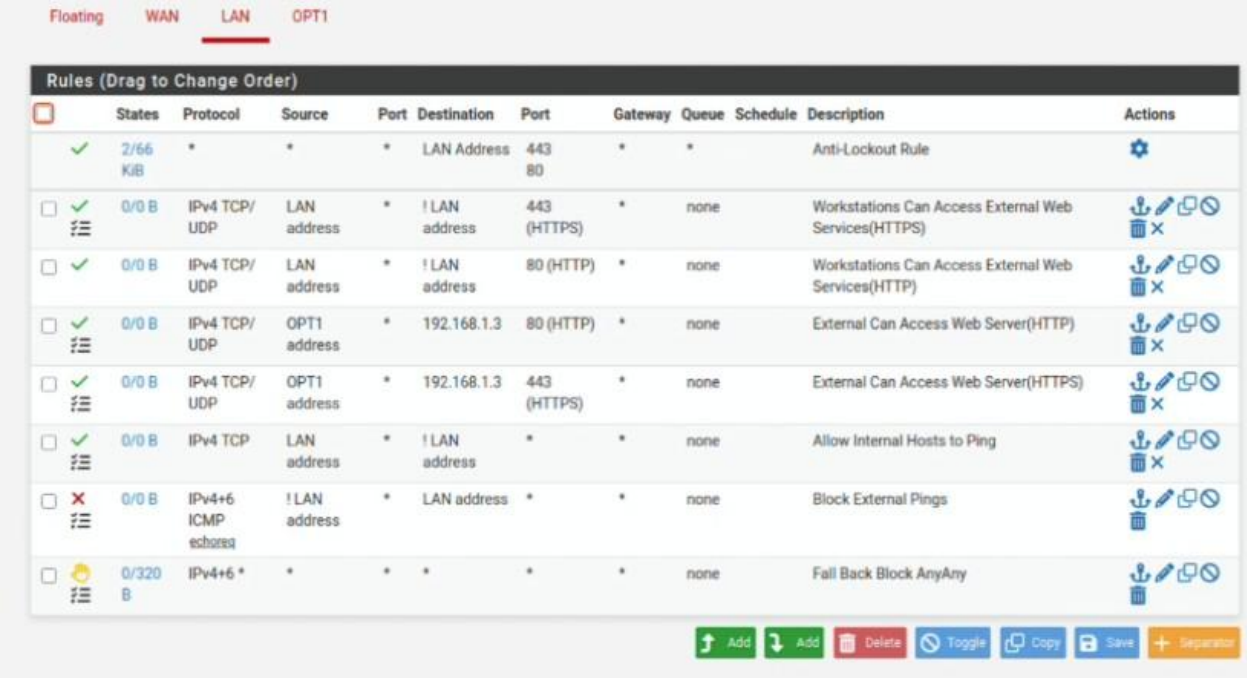
B. The server provides only SSH and web service to the workstations.

D. The workstations shall not provide any services.

E. The workstations can access the services hosted by the server.

As these functions are local to the 192.168.1.0/24 subnet, they do not need to travel through the routing interfaces and are not subject to the router's firewall rules.

Rules for LAN1 interface:



Rules 1–3: Matches policies B, E, F. These rules let internal users reach the server for management (SSH and web) and also allow them to browse external web pages. They enforce the policy that workstations only get web access when reaching the outside world.

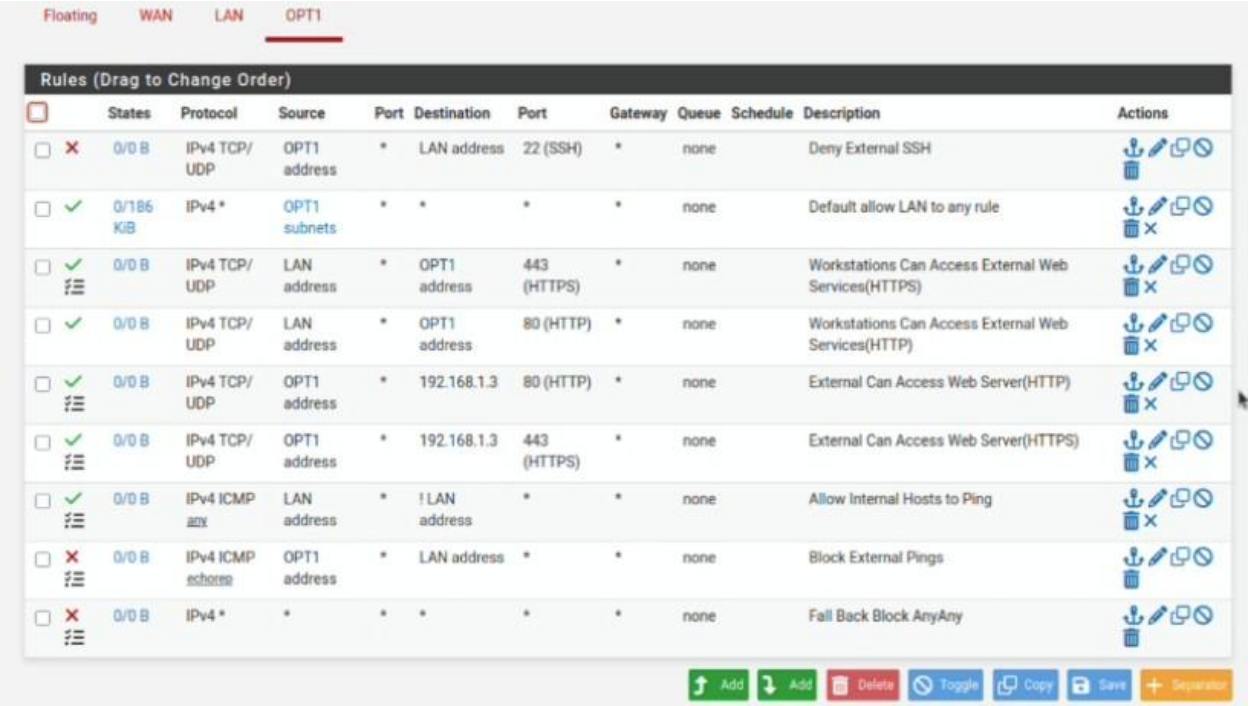
Rules 4–5: Policy A. These rules open port 80/443 from the internet to the server so outsiders can access the website, but they block everything else.

Rule 6: Allows LAN clients to use ping.

Rule 7: Blocks pings coming from the internet to the firewall.

Rule 8: Blocks everything else (default deny).

Rules for OPT1 interface:

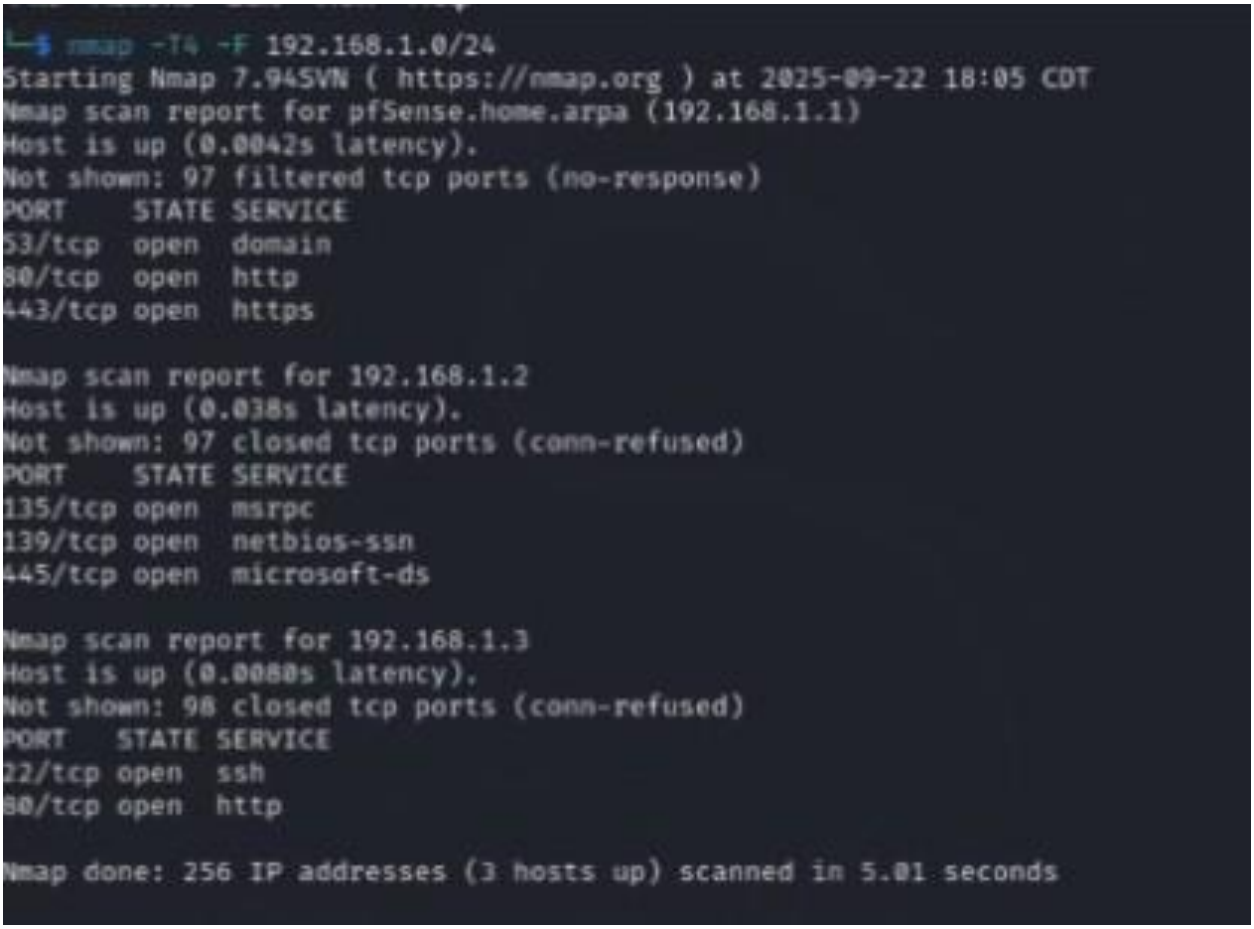


Rules 1–3 Policy F: Let LAN workstations access the web (HTTP/HTTPS) and manage baseline connectivity. These rules allow outbound traffic from LAN devices to external web servers (ports 80 and 443).

Rules 4–5 Policy A: Expose the internal web server (192.168.1.3) to the internet. These rules allow inbound HTTP (80) and HTTPS (443) from external hosts to the server.

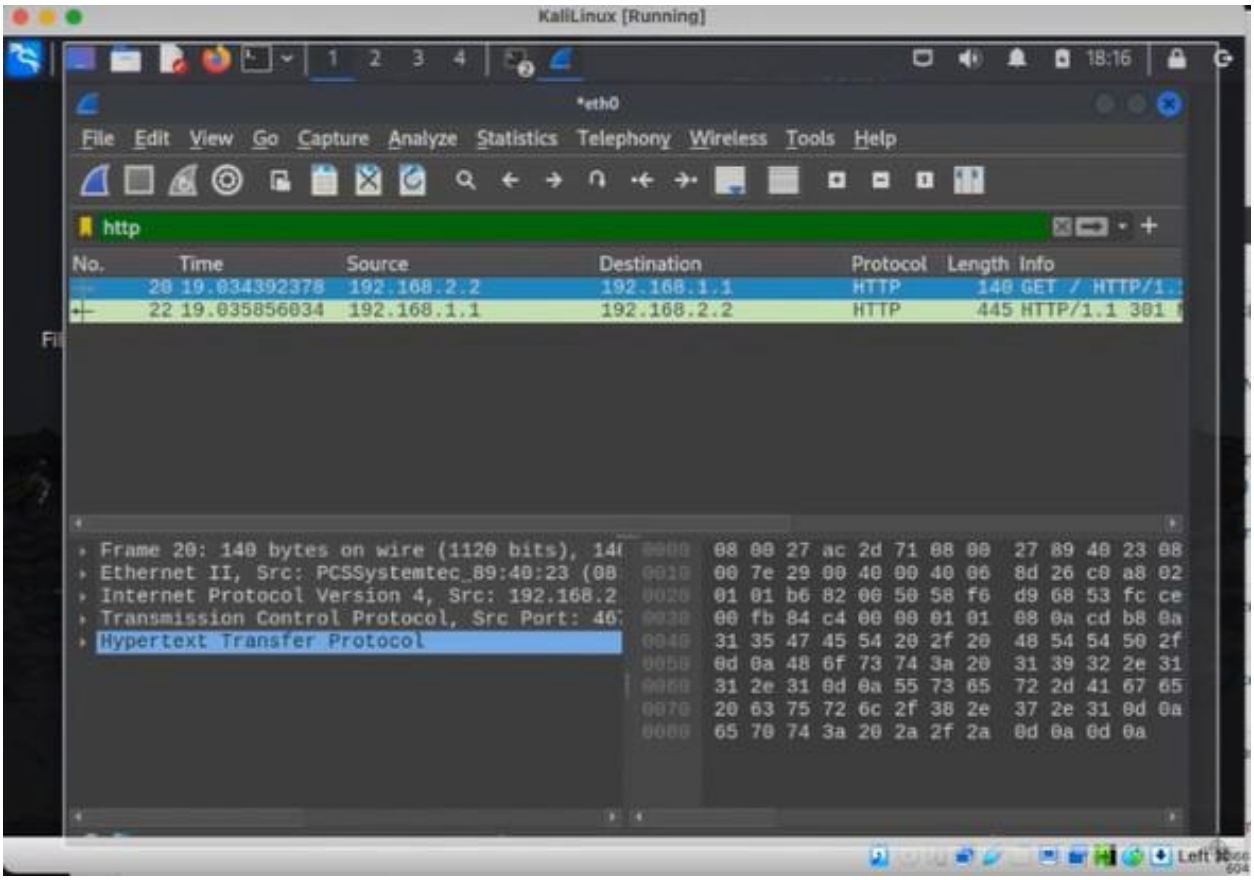
Rule 6 Policy G: Allow LAN devices (workstations and server) to ping other computers.
This rule permits ICMP echo requests from LAN clients to other systems.
Rule 7 Policy H: Block pings coming from the internet to internal devices. This prevents external machines from pinging LAN or the server.

Rule 8 Policy C&D: Block all other traffic by default. This is the fallback deny rule for anything not explicitly allowed.



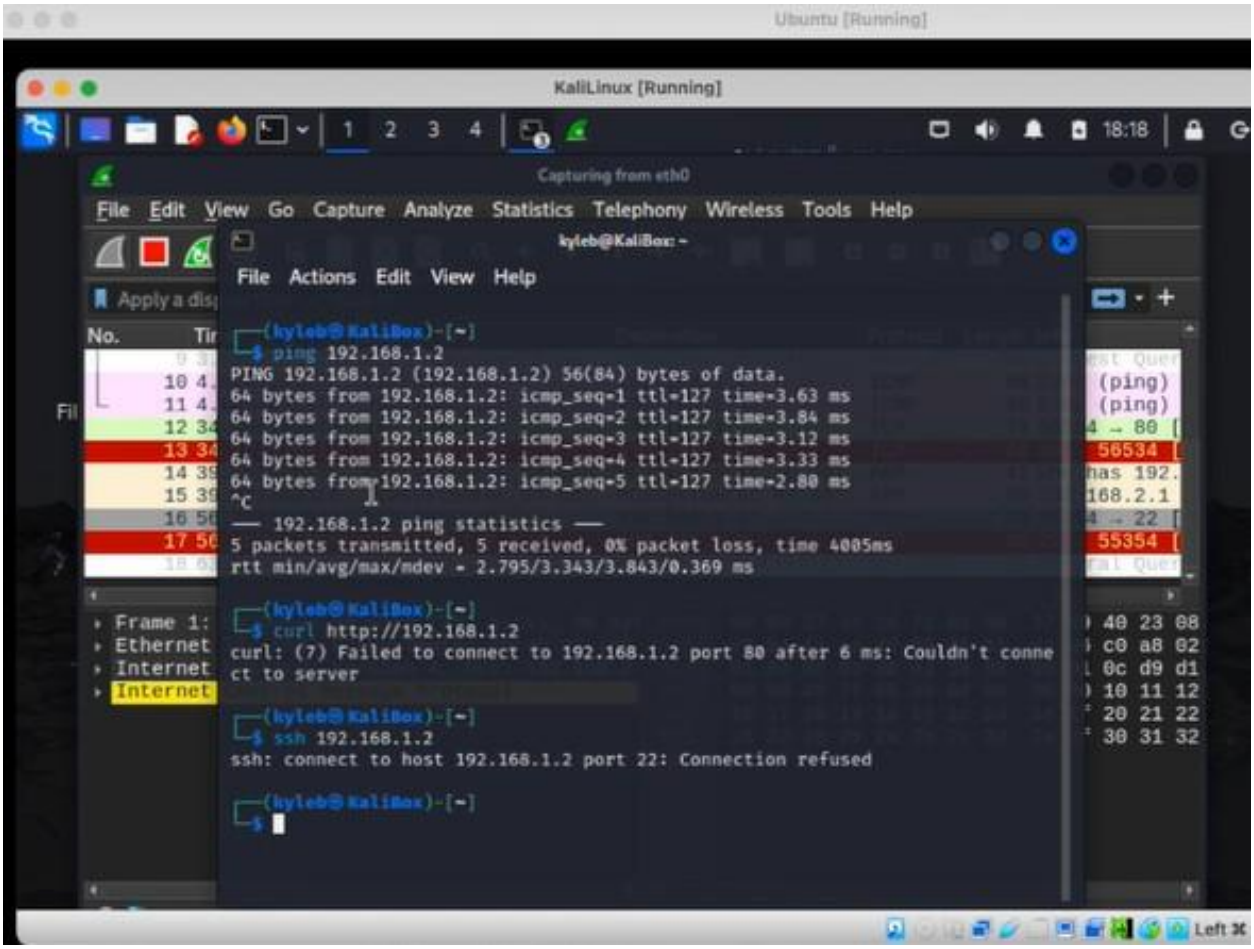
NMAP view after firewall implementation

The XP machine is showing multiple exposed ports that it shouldn't be, and the server is showing an open SSH port but a closed HTTPS port. Looking at the rules I set, I'm not sure why this is happening and have been unable to correct the problem.

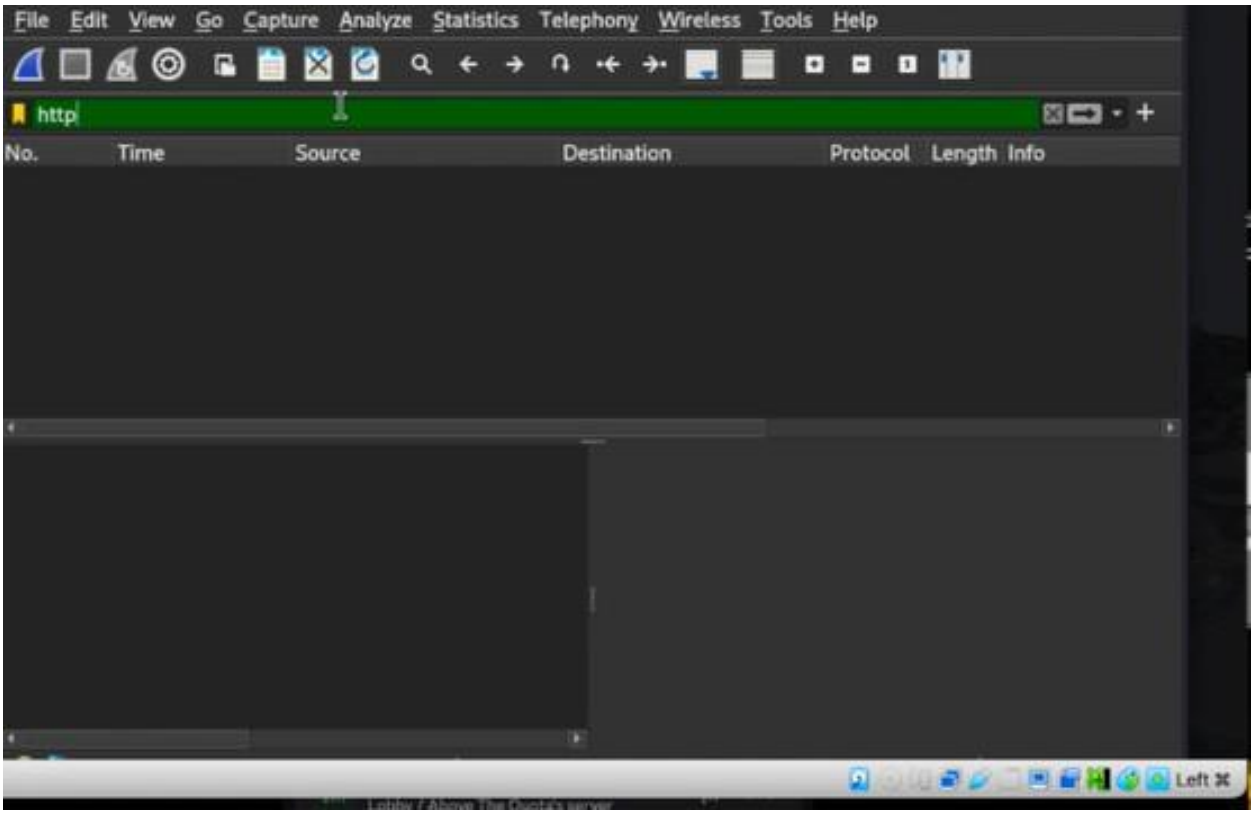


Kali B1 to A1 (HTTP)

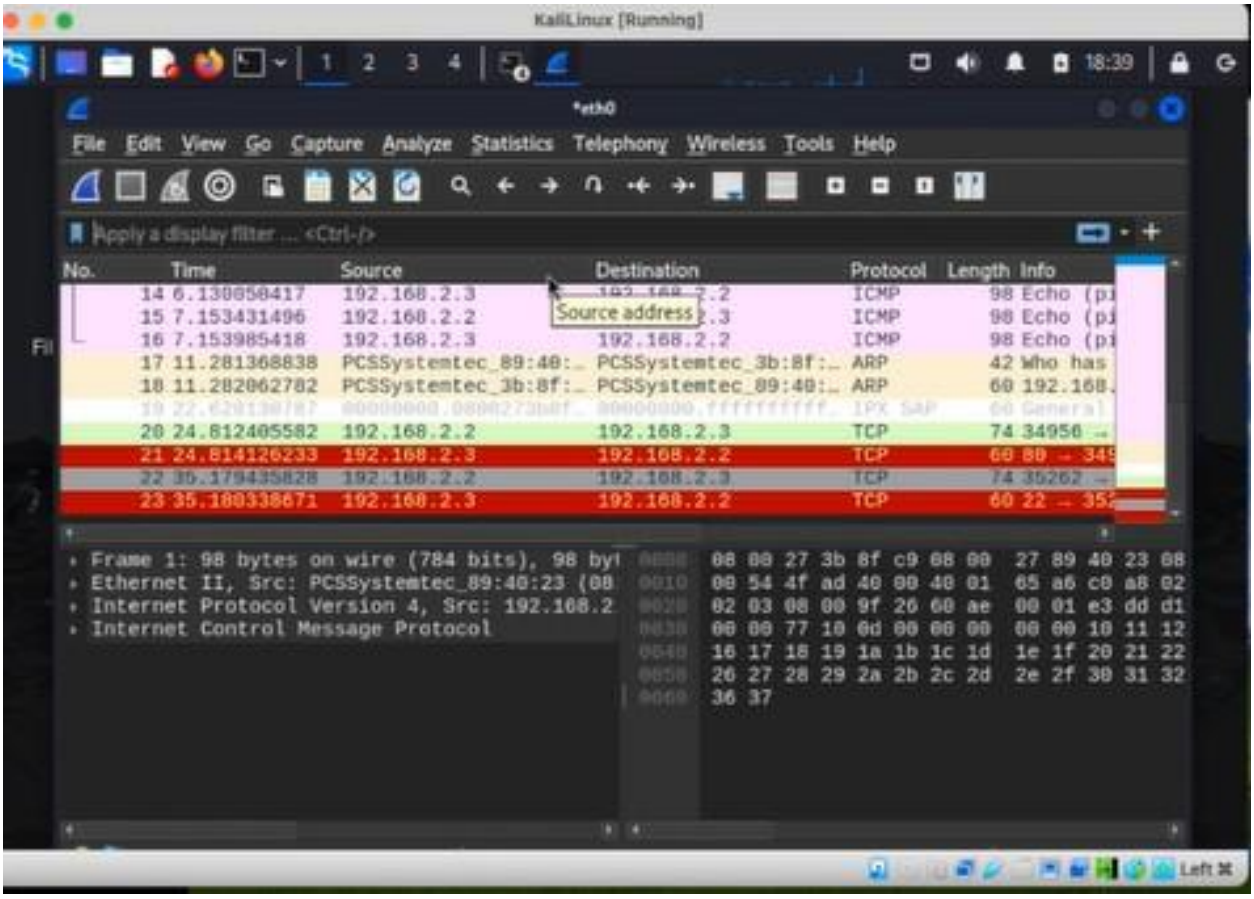
The traffic is the same as last time.


Ubuntu [Running]
KaliLinux [Running]
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
kyleb@KaliBox: ~
File Actions Edit View Help
(kyleb㉿KaliBox)-[~]
$ ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
64 bytes from 192.168.1.2: icmp_seq=1 ttl=127 time=3.63 ms
64 bytes from 192.168.1.2: icmp_seq=2 ttl=127 time=3.84 ms
64 bytes from 192.168.1.2: icmp_seq=3 ttl=127 time=3.12 ms
64 bytes from 192.168.1.2: icmp_seq=4 ttl=127 time=3.33 ms
64 bytes from 192.168.1.2: icmp_seq=5 ttl=127 time=2.80 ms
^C
— 192.168.1.2 ping statistics —
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 2.795/3.343/3.843/0.369 ms
(kyleb㉿KaliBox)-[~]
$ curl http://192.168.1.2
curl: (7) Failed to connect to 192.168.1.2 port 80 after 6 ms: Couldn't connect to server
(kyleb㉿KaliBox)-[~]
$ ssh 192.168.1.2
ssh: connect to host 192.168.1.2 port 22: Connection refused
(kyleb㉿KaliBox)-[~]
$

B.1 to A.2



B.1 to A.2 – There is no traffic in HTTP compared to last time



B.1 to B.2 – Ports 80/443 are allowed between computers

4 Web server firewall configurations

```
kyle@kyle-VirtualBox:~$ sudo iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere             state RELATED,ESTABLISHED
ACCEPT     all  --  anywhere             anywhere             state RELATED,ESTABLISHED
ACCEPT     tcp  --  192.168.1.2          192.168.1.3          multiport dports ssh,http,https
ACCEPT     tcp  --  192.168.2.0/24       192.168.1.3          multiport dports http,https
ACCEPT     icmp --  192.168.1.0/24       192.168.1.3          icmp echo-request

Chain FORWARD (policy DROP)
target     prot opt source               destination

Chain OUTPUT (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  anywhere             192.168.1.0/24
DROP       all  --  anywhere             192.168.2.0/24
ACCEPT     icmp --  anywhere             anywhere             icmp echo-request
kyle@kyle-VirtualBox:~$
```

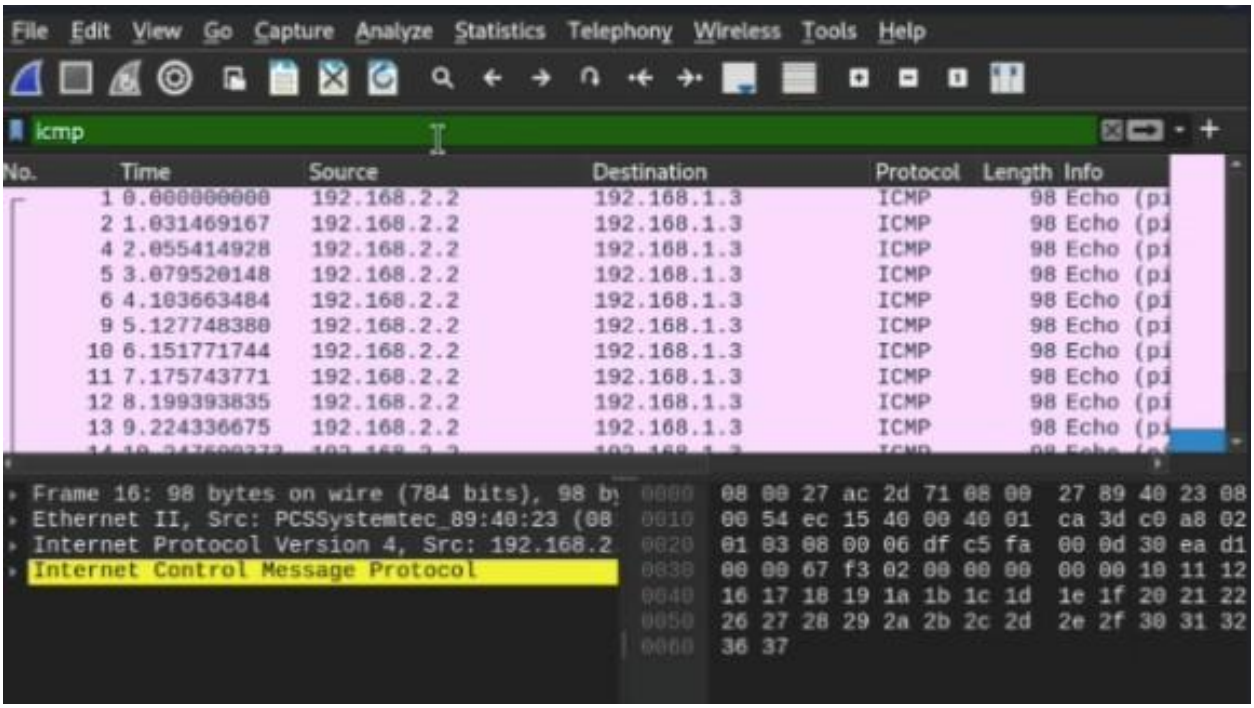
Policy DROP rules on the top for both INPUT and OUTPUT chains. Drop anything that isn't explicitly allowed.

INPUT chain–

1. Accept all anywhere RELATED/ESTABLISHED – Allow server to receive replies to connections it has initiated.
2. Accept TCP 192.168.1.2 – Workstations may access server's web services or SSH to it.
3. Accept TCP 192.168.2.0 – External computers may access server's web services.
4. Accept ICMP 192.168.1.0 – Workstations may ping the server.

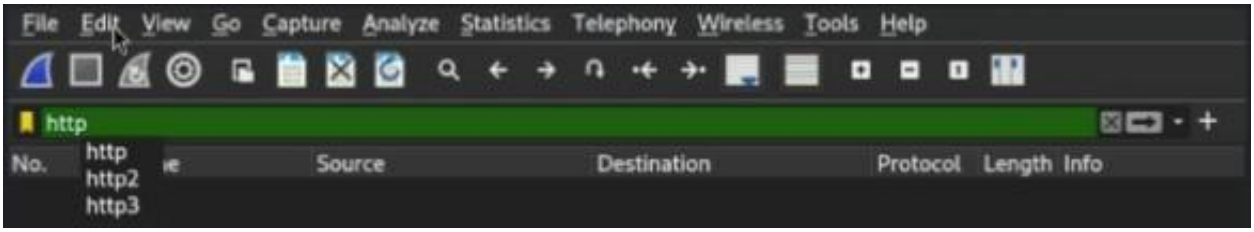
OUTPUT chain–

1. Accept all anywhere to 192.168.1.0 – The security specifications listed no restrictions onthe server being able to access the workstations.
2. Drop all anywhere 192.168.2.0 – Server should not access any services of external computers.
3. Accept ICMP anywhere anywhere – Server may ping anything.



Sniffing after implementing host firewall (IP 192.168.2.2 to 192.168.1.3)

Note: Pings are sent but the router drops them and there is no reply.



192.168.2.2 to 192.168.1.2

Results and Observations

Initial scans before implementing the firewall showed all systems fully reachable, indicating an open environment. After pfSense policies were enforced, Nmap scans from the external network revealed only the web ports (80/443) open on the internal server. Workstations and internal servers successfully communicated internally, but external pings and non-web traffic were dropped. Wireshark captures confirmed filtered ICMP and TCP handshakes consistent with the new firewall configurations.

Challenges and Problem-Solving

During the project, several configuration errors occurred, including misconfigured firewall syntax and rule ordering issues. These required iterative debugging using packet tracing and log analysis. One instance involved incorrect rule direction, blocking legitimate SSH traffic until adjusted. Another issue was the accidental flush of iptables on the Ubuntu host, which required full reconstruction of the policy set. These setbacks reinforced the importance of rule backup procedures and incremental configuration testing.

Lessons Learned and Outcomes

The project provided real-world insight into network hardening, firewall configuration, and the impact of policy design on network behavior. It demonstrated that even well-intentioned security policies can fail without precise implementation and validation. By constructing and testing multiple network scenarios, the experience strengthened practical skills in virtualization, packet inspection, and access control — key competencies for cybersecurity roles.

5 Conclusion

This project simulated an enterprise-grade cybersecurity workflow: environment design, threat surface analysis, policy implementation, and verification through active scanning and

monitoring. It highlights proficiency in pfSense, Nmap, Wireshark, and Linux network administration. The exercise also demonstrated adaptability, troubleshooting, and analytical reasoning — essential qualities for network security and system administration positions