

Project-1: Sandbox, Firewall & Access Control

CS4371/CS5378 Spring 2025

FLR

Reed Kotrla, Robert Jones, Posan Gc

February 10, 2025

1 Introduction

This project focuses on building a sandbox environment for security experiments, building virtual machines, setting up firewalls, and implementing network security policies. The objectives include learning networking tools, analyzing security policies, and verifying secure configurations. The goals of this project was to design and implement a secure network infrastructure that has solid control rules, analyze network traffic before and after an implementation to get a full understanding of the security, by allowing only certain devices access and blocking external pings.

2 Task-II & III: Network Setup and Diagnosis

2.1 Virtual Machine Setup

Below is a screenshot showing the VM setup in the virtual machine manager:

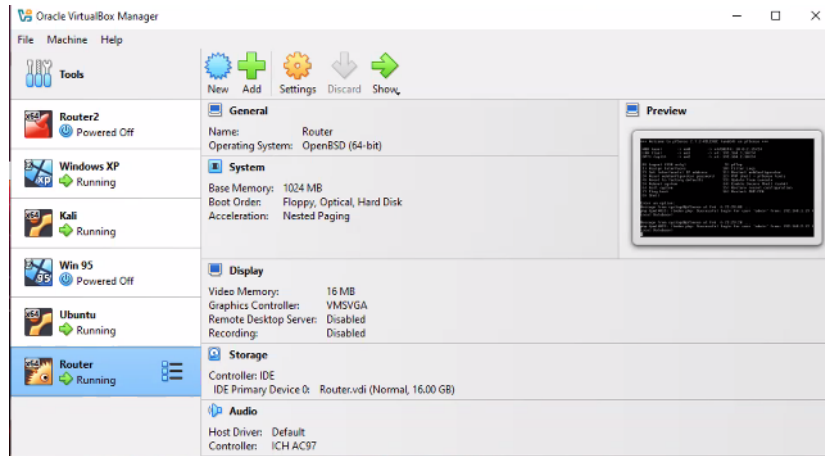


Figure 1: Virtual Machines in Virtual Machine Manager

2.2 NMap Scans

We used NMap to scan network A and B. The commands used are:

```
% Quick Scan of Network A:
nmap -T4 -F 192.168.A.0/24
% Regular Scan of Network A:
nmap 192.168.A.0/24
% Quick Scan of Network B:
nmap -T4 -F 192.168.B.0/24
% Regular Scan of Network B:
nmap 192.168.B.0/24
```

2.3 Wireshark Traffic Analysis

Screenshots of Wireshark captures before implementing security policies:

4	6.858143896	192.168.2.12	192.168.1.19	ICMP	98 Echo
5	6.858547207	192.168.1.19	192.168.2.12	ICMP	98 Echo
6	7.866368137	192.168.2.12	192.168.1.19	ICMP	98 Echo
7	7.867043995	192.168.1.19	192.168.2.12	ICMP	98 Echo

Figure 2: Ping from B.1 to A.1

207	232.757920696	192.168.2.12	192.168.1.19	TCP
208	232.758298661	192.168.1.19	192.168.2.12	TCP
209	232.758321802	192.168.2.12	192.168.1.19	TCP
210	232.758381668	192.168.2.12	192.168.1.19	HTTP
211	232.758585306	192.168.1.19	192.168.2.12	TCP
212	232.759553964	192.168.1.19	192.168.2.12	TCP

Figure 3: Curl from B.1 to A.1

39	185.383737790	192.168.2.12	192.168.1.19	TCP
40	185.383894378	192.168.2.12	192.168.1.19	SSHv2
41	185.384343480	192.168.1.19	192.168.2.12	TCP
42	185.491181211	192.168.1.19	192.168.2.12	SSHv2
43	185.491225328	192.168.2.12	192.168.1.19	TCP
44	185.491419504	192.168.2.12	192.168.1.19	SSHv2

Figure 4: SSH from B.1 to A.1

23	64.909494543	192.168.2.12	192.168.1.12	ICMP	98 Echo (ping) request
24	64.910141648	192.168.1.12	192.168.2.12	ICMP	98 Echo (ping) reply

Figure 5: Ping from B.1 to A.2

27	95.701019439	192.168.2.12	192.168.1.12	TCP	74 43190 - 80
28	95.701614491	192.168.1.12	192.168.2.12	TCP	60 80 - 43190
29	100.908993045	PCSSystemtec_74:55:f8	PCSSystemtec_a1:db:16	ARP	42 Who has 192.1
30	100.909244109	PCSSystemtec_a1:db:16	PCSSystemtec_74:55:f8	ARP	60 192.168.2.1
31	109.975769304	192.168.2.12	192.168.1.12	TCP	74 45780 - 22
32	109.976321796	192.168.1.12	192.168.2.12	TCP	60 22 - 45780

Figure 6: SSH and Curl from B.1 to A.2

5	3.691346592	192.168.2.13	192.168.2.12	ICMP	98 Echo (ping)
6	4.693702212	192.168.2.12	192.168.2.13	ICMP	98 Echo (ping)
7	4.693907762	192.168.2.13	192.168.2.12	ICMP	98 Echo (ping)
8	5.721926435	192.168.2.12	192.168.2.13	ICMP	98 Echo (ping)

Figure 7: Ping from B.1 to B.2

1	0.000000000	192.168.2.12	192.168.2.13	TCP	74 57754 - 22
2	0.000176046	PCSSystemtec_01:b6:f2	Broadcast	ARP	60 Who has 192.1
3	0.000182369	PCSSystemtec_74:55:f8	PCSSystemtec_01:b6:f2	ARP	42 192.168.2.12
4	0.000203451	192.168.2.13	192.168.2.12	TCP	60 22 - 57754

Figure 8: SSH from B.1 to B.2

28	75.971049291	192.168.1.19	192.168.1.12	TCP	74 48370 - 22
29	75.971304528	192.168.1.12	192.168.1.19	TCP	60 22 - 48370

Figure 9: SSH from A.2 to A.1

1	0.000000000	192.168.1.19	192.168.2.12	ICMP	98 Echo (ping) request
2	0.000559419	192.168.2.12	192.168.1.19	ICMP	98 Echo (ping) reply
3	1.033309095	192.168.1.19	192.168.2.12	ICMP	98 Echo (ping) request
4	1.033843698	192.168.2.12	192.168.1.19	ICMP	98 Echo (ping) reply
5	2.062948566	192.168.1.19	192.168.2.12	ICMP	98 Echo (ping) request
6	2.063452822	192.168.2.12	192.168.1.19	ICMP	98 Echo (ping) reply

Figure 10: Ping from A.2 to A.1

7	7.873711254	192.168.1.19	192.168.1.12	TCP	74 38992 - 80
8	7.873961543	PCSSystemtec_da:e4:bb	Broadcast	ARP	60 Who has 192.1
9	7.873968833	PCSSystemtec_28:61:bf	PCSSystemtec_da:e4:bb	ARP	42 192.168.1.12
10	7.874158139	192.168.1.12	192.168.1.19	TCP	60 80 - 38992

Figure 11: Curl from A.2 to A.1

2.4 Router Configuration

Here are the web services allowed between computers.

- A) The Ubuntu Server (A.1) provides only web service to external computers (in Network B).
- (B) The Ubuntu Server (A.1) provides only SSH and web service to the companys workstations (A.2).
- (C) The Ubuntu Server (A.1) shall not access any services on external computers (no outbound to B), except it is allowed to ping external hosts (see item G).
- (D) The Windows XP Workstations (A.2) shall not provide any services.
- (E) Workstations (A.2) can access the Ubuntu servers (A.1) SSH and web services.
- (F) Workstations (A.2) can access only the web service provided by external computers through Ubuntu server.
- (G) Both the Ubuntu server (A.1) and the XP workstations (A.2) can ping any other computers.
- (H) External computers cannot ping either the Ubuntu server (A.1) or the XP workstations (A.2). show the web services allowed between computers

3 Task-IV and V: Access Control and Policy Enforcement

3.1 Access Control Matrix

The access control matrix is shown below, outlining the permitted and restricted interactions between different network entities.

Access Control Matrix						
Object Subject	ubuntu http	ubuntu SSH	ubuntu ICMP (Ping)	external any services	XP ICMP Ping	web services port
Web server	✓ Server gets to connect to web	X No outside computer coming in.	X NO other	X systems or services	X in subnet 1 access the web.	N/A
Windows XP	✓ workstations connect to server	✓ can connect to server ssh	✓ Can Ping other computers	X no other outside services	N/A	✓ Through the server
ubuntu (the server)	N/A	N/A	N/A	X will not access outside services	Not Hosting any services	✓ server can ping external hosts

Figure 12: Access Control Matrix

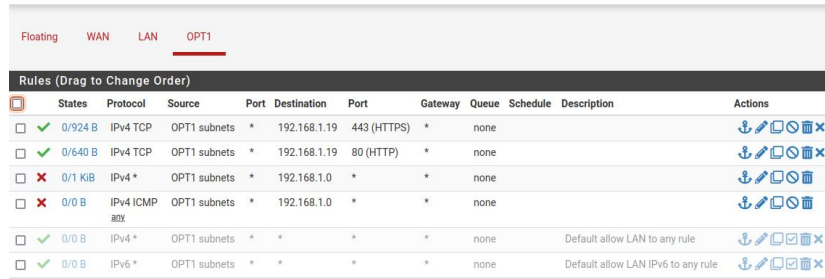
3.2 Policy Limitations

The following policies **CANNOT** be completely enforced by the router rules on R:

- Restricting access based on user authentication levels.
- Preventing unauthorized data exfiltration through encrypted channels.
- Enforcing time-based access restrictions.

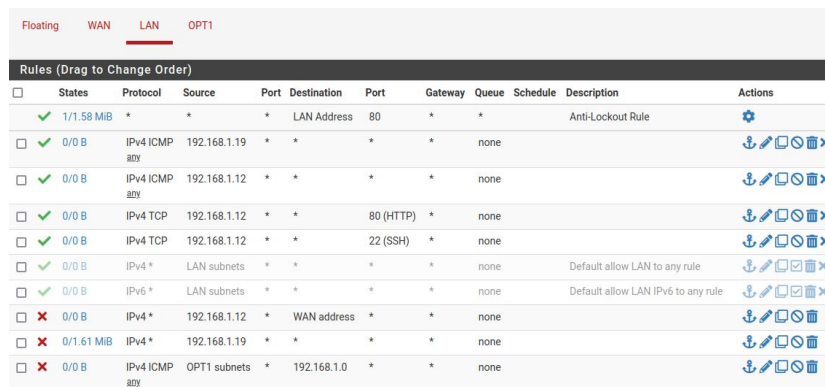
3.3 Router Rules on R

Below is a screenshot of the implemented router rules, along with an explanation of each rule's purpose.



Rules (Drag to Change Order)	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0/924 B	IPv4 TCP	OPT1 subnets	*	192.168.1.19	443 (HTTPS)	*	none		↓ ✎ 🔍 🗑️ ✖
<input type="checkbox"/>	✓	0/640 B	IPv4 TCP	OPT1 subnets	*	192.168.1.19	80 (HTTP)	*	none		↓ ✎ 🔍 🗑️ ✖
<input type="checkbox"/>	✗	0/1 KiB	IPv4 *	OPT1 subnets	*	192.168.1.0	*	*	none		↓ ✎ 🔍 🗑️
<input type="checkbox"/>	✗	0/0 B	IPv4 ICMP	OPT1 subnets	*	192.168.1.0	*	*	none		↓ ✎ 🔍 🗑️
<input type="checkbox"/>	✓	0/0 B	IPv4 *	OPT1 subnets	*	*	*	*	none	Default allow LAN to any rule	↓ ✎ 🔍 🗑️ ✖
<input type="checkbox"/>	✓	0/0 B	IPv6 *	OPT1 subnets	*	*	*	*	none	Default allow LAN IPv6 to any rule	↓ ✎ 🔍 🗑️ ✖

Figure 13: WAN Rules



Rules (Drag to Change Order)	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	1/1.58 MiB	*	*	*	LAN Address	80	*	*	Anti-Lockout Rule	⚙️
<input type="checkbox"/>	✓	0/0 B	IPv4 ICMP	192.168.1.19	*	*	*	*	none		↓ ✎ 🔍 🗑️ ✖
<input type="checkbox"/>	✓	0/0 B	IPv4 ICMP	192.168.1.12	*	*	*	*	none		↓ ✎ 🔍 🗑️ ✖
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	192.168.1.12	*	*	80 (HTTP)	*	none		↓ ✎ 🔍 🗑️ ✖
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	192.168.1.12	*	*	22 (SSH)	*	none		↓ ✎ 🔍 🗑️ ✖
<input type="checkbox"/>	✓	0/0 B	IPv4 *	LAN subnets	*	*	*	*	none	Default allow LAN to any rule	↓ ✎ 🔍 🗑️ ✖
<input type="checkbox"/>	✓	0/0 B	IPv6 *	LAN subnets	*	*	*	*	none	Default allow LAN IPv6 to any rule	↓ ✎ 🔍 🗑️ ✖
<input type="checkbox"/>	✗	0/0 B	IPv4 *	192.168.1.12	*	WAN address	*	*	none		↓ ✎ 🔍 🗑️
<input type="checkbox"/>	✗	0/1.61 MiB	IPv4 *	192.168.1.19	*	*	*	*	none		↓ ✎ 🔍 🗑️
<input type="checkbox"/>	✗	0/0 B	IPv4 ICMP	OPT1 subnets	*	192.168.1.0	*	*	none		↓ ✎ 🔍 🗑️

Figure 14: LAN Rules

Rule Purposes

LAN Firewall Rules

```
Allow HTTP traffic to LAN Address (Anti-Lockout Rule).
Allow ICMP (Ping) from 192.168.1.19 to any destination.
Allow ICMP (Ping) from 192.168.1.12 to any destination.
Allow HTTP traffic from 192.168.1.12.
Allow SSH traffic from 192.168.1.12.
Allow all traffic from LAN subnets (default rule).
Block traffic from 192.168.1.12 to WAN Address.
Block all other traffic from 192.168.1.19.
Block ICMP from OPT1 subnets to 192.168.1.0.
```

WAN Rules

```
Allow HTTPS traffic from OPT1 subnets to 192.168.1.19.
Allow HTTP traffic from OPT1 subnets to 192.168.1.19.
Block all other IPv4 traffic from OPT1 subnets to
    192.168.1.0.
Block ICMP from OPT1 subnets to 192.168.1.0.
Allow all other traffic from OPT1 subnets (default rule).
```

3.4 NMap Results of Exposed Computers and Ports in Network A

The following screenshots display the results of NMap scans performed on Network A to identify exposed computers and open ports.

3.5 Wireshark Results: Web Service Checks

Screenshots of Wireshark captures for web service interactions between different nodes:


```

(victim@vbox)-[~]
$ ping 192.168.1.19
PING 192.168.1.19 (192.168.1.19) 56(84) bytes of data.
^C
— 192.168.1.19 ping statistics —
3 packets transmitted, 0 received, 100% packet loss, time 2057ms

(victim@vbox)-[~]
$ nmap -T4 -F 192.168.1.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-09 23:17 CST
Nmap scan report for 192.168.1.19
Host is up (0.00045s latency).
Not shown: 98 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   closed https

Nmap done: 256 IP addresses (1 host up) scanned in 37.30 seconds

(victim@vbox)-[~]
$ nmap 192.168.1.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-09 23:18 CST
Nmap scan report for 192.168.1.19
Host is up (0.00044s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   closed https

Nmap done: 256 IP addresses (1 host up) scanned in 132.16 seconds

```

Figure 15: NMap Results of Network A

Time	Source	Destination	Protocol	Length	Info
1 0.000000000	00000000.00002701b6f2	00000000.ffffffffffff	IPX SAP	80	General Query
2 7.899340780	192.168.2.12	192.168.1.19	ICMP	98	Echo (ping) request
3 8.934223523	192.168.2.12	192.168.1.19	ICMP	98	Echo (ping) request
4 9.964265515	192.168.2.12	192.168.1.19	ICMP	98	Echo (ping) request
5 10.994055987	192.168.2.12	192.168.1.19	ICMP	98	Echo (ping) request
6 13.131442950	PCSSystemtec_74:55:f8	PCSSystemtec_a1:db:16	ARP	42	Who has 192.168.2.1
7 13.131616570	PCSSystemtec_a1:db:16	PCSSystemtec_74:55:f8	ARP	60	192.168.2.10 is at
8 26.819692364	192.168.2.12	192.168.1.19	TCP	74	37442 → 22 [SYN] Seq
9 27.942447451	192.168.2.12	192.168.1.19	TCP	74	[TCP Retransmission
10 28.068343476	192.168.2.12	192.168.1.19	TCP	74	[TCP Retransmission
11 29.092479660	192.168.2.12	192.168.1.19	TCP	74	[TCP Retransmission
12 30.118112991	192.168.2.12	192.168.1.19	TCP	74	[TCP Retransmission
13 31.143108369	192.168.2.12	192.168.1.19	TCP	74	[TCP Retransmission
14 33.156125171	192.168.2.12	192.168.1.19	TCP	74	[TCP Retransmission
15 58.113581671	192.168.2.12	192.168.1.19	TCP	74	43024 → 80 [SYN] Seq
16 58.114047648	192.168.1.19	192.168.2.12	TCP	74	80 → 43024 [SYN, AC
17 58.114068282	192.168.2.12	192.168.1.19	TCP	66	43024 → 80 [ACK] Seq
18 58.114098294	192.168.2.12	192.168.1.19	HTTP	142	GET / HTTP/1.1
19 58.114352873	192.168.1.19	192.168.2.12	TCP	66	80 → 43024 [ACK] Seq
20 58.114811186	192.168.1.19	192.168.2.12	TCP	4410	80 → 43024 [ACK] Seq
21 58.1148119952	192.168.2.12	192.168.1.19	TCP	66	43024 → 80 [ACK] Seq
22 58.114855469	192.168.1.19	192.168.2.12	TCP	2962	80 → 43024 [PSH, AC
23 58.114855528	192.168.1.19	192.168.2.12	TCP	2962	80 → 43024 [ACK] Seq
24 58.114869101	192.168.2.12	192.168.1.19	TCP	66	43024 → 80 [ACK] Seq
25 58.114874912	192.168.2.12	192.168.1.19	TCP	66	43024 → 80 [ACK] Seq
26 58.114897193	192.168.1.19	192.168.2.12	HTTP	856	HTTP/1.1 200 OK (t
27 58.114900479	192.168.2.12	192.168.1.19	TCP	66	43024 → 80 [ACK] Seq
28 58.115007784	192.168.2.12	192.168.1.19	TCP	66	43024 → 80 [FIN, AC
29 58.115331370	192.168.1.19	192.168.2.12	TCP	66	80 → 43024 [FIN, AC
30 58.115337181	192.168.2.12	192.168.1.19	TCP	66	43024 → 80 [ACK] Seq

Figure 16: Web service check: B.1 to A.1

41	47.556981886	192.168.1.19	192.168.1.12	TCP	74 54726 → 88 [SYN] Seq=0
42	47.557232258	192.168.1.12	192.168.1.19	TCP	68 88 → 54726 [RST, ACK]
43	50.286511350	192.168.1.19	192.168.1.10	DNS	100 Standard query end=0
44	52.400080893	192.168.1.19	192.168.1.10	DNS	100 Standard query 0xd744
45	52.400133710	192.168.1.19	192.168.1.10	DNS	95 Standard query 0x499d
46	55.410410090	192.168.1.19	192.168.1.10	DNS	100 Standard query 0x6067
47	57.632935216	192.168.1.19	192.168.1.10	DNS	100 Standard query 0xd744
48	57.632978448	192.168.1.19	192.168.1.10	DNS	95 Standard query 0x499d
49	59.787442046	192.168.1.19	192.168.1.12	TCP	74 52422 → 88 [SYN] Seq=0
50	59.787470151	192.168.1.12	192.168.1.19	TCP	68 88 → 52422 [RST, ACK]
51	62.835505558	192.168.1.19	192.168.1.10	DNS	100 Standard query 0xd744

Figure 17: Web service check: B.1 to A.2

28	366065192	192.168.1.12	192.168.1.19	ICMP	98 Echo (ping) reply
29	426422195	192.168.1.19	192.168.1.12	ICMP	98 Echo (ping) request
29	42656024	192.168.1.12	192.168.1.19	ICMP	98 Echo (ping) reply
30	450738271	192.168.1.19	192.168.1.12	ICMP	98 Echo (ping) request
30	451071954	192.168.1.12	192.168.1.19	ICMP	98 Echo (ping) reply

Figure 18: Web service check: B.1 to B.2

84	105.189845473	192.168.1.19	192.168.1.12	TCP	74 43674 → 22
85	105.189839315	192.168.1.12	192.168.1.19	TCP	68 22 → 43674
86	106.671689768	192.168.1.19	192.168.1.10	DNS	100 Standard query
87	107.913547544	192.168.1.19	192.168.1.10	DNS	100 Standard query
88	111.688632929	192.168.1.19	192.168.1.12	TCP	74 52658 → 22
89	111.688652326	192.168.1.12	192.168.1.19	TCP	68 22 → 52658

Figure 19: Web service check: B.1 to A.2

1	0.000000000	192.168.2.12	192.168.2.13	ICMP	98 Echo (ping) request id=8x4d21, seq=1/256, tt
2	0.000189254	192.168.2.13	192.168.2.12	ICMP	98 Echo (ping) reply id=8x4d21, seq=1/256, tt
3	0.724759102	00000000.00002701b6f2	00000000.ffffffffffff	IPX SAP	60 General Query
4	1.020854547	192.168.2.12	192.168.2.13	ICMP	98 Echo (ping) request id=8x4d21, seq=2/512, tt
5	1.0208294162	192.168.2.13	192.168.2.12	ICMP	98 Echo (ping) reply id=8x4d21, seq=2/512, tt
6	2.047949911	192.168.2.12	192.168.2.13	ICMP	98 Echo (ping) request id=8x4d21, seq=3/768, tt
7	2.048115978	192.168.2.13	192.168.2.12	ICMP	98 Echo (ping) reply id=8x4d21, seq=3/768, tt
8	3.0659806075	192.168.2.12	192.168.2.13	ICMP	98 Echo (ping) request id=8x4d21, seq=4/1024, t
9	3.065275509	192.168.2.13	192.168.2.12	ICMP	98 Echo (ping) reply id=8x4d21, seq=4/1024, t
10	5.240697525	PCSSystemtec_74:55:f8	PCSSystemtec_01:b6:f2	ARP	42 Who has 192.168.2.13? Tell 192.168.2.12
11	5.240938759	PCSSystemtec_01:b6:f2	PCSSystemtec_74:55:f8	ARP	60 192.168.2.13 is at 00:00:27:01:b6:f2
12	16.40497527	192.168.2.12	192.168.2.13	TCP	74 56968 → 88 [SYN] Seq=0 Win=64240 Len=0 MSS=14
13	16.404734726	192.168.2.13	192.168.2.12	TCP	68 88 → 56968 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
14	16.404734726	192.168.2.13	192.168.2.12	TCP	74 43674 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=14
15	48.687327229	192.168.2.13	192.168.2.12	TCP	68 22 → 43674 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
16	53.881158419	PCSSystemtec_74:55:f8	PCSSystemtec_01:b6:f2	ARP	42 Who has 192.168.2.13? Tell 192.168.2.12
17	53.881359846	PCSSystemtec_01:b6:f2	PCSSystemtec_74:55:f8	ARP	60 192.168.2.13 is at 00:00:27:01:b6:f2
18	69.716818574	00000000.00002701b6f2	00000000.ffffffffffff	IPX SAP	60 General Query

Figure 20: Web service check: B.1 to A.2

1	0.000000000	192.168.2.12	192.168.1.12	ICMP	98 Echo (ping) request
2	1.027909573	192.168.2.12	192.168.1.12	ICMP	98 Echo (ping) request
3	2.059727820	192.168.2.12	192.168.1.12	ICMP	98 Echo (ping) request
4	3.074902594	192.168.2.12	192.168.1.12	ICMP	98 Echo (ping) request
5	5.260056763	PCSSystemtec_74:55:f8	PCSSystemtec_a1:db:16	ARP	42 Who has 192.168.2.19?
6	5.260300884	PCSSystemtec_a1:db:16	PCSSystemtec_74:55:f8	ARP	60 192.168.2.19 is at 00:00:27:01:b6:f2
7	15.184926345	00000000.00002701b6f2	00000000.ffffffffffff	IPX SAP	60 General Query
8	37.659968496	192.168.2.12	192.168.1.12	TCP	74 45168 → 22 [SYN] Seq=0
9	39.704854086	192.168.2.12	192.168.1.12	TCP	74 [TCP Retransmission]
10	39.714112062	192.168.2.12	192.168.1.12	TCP	74 [TCP Retransmission]
11	40.738061639	192.168.2.12	192.168.1.12	TCP	74 [TCP Retransmission]
12	41.773400666	192.168.2.12	192.168.1.12	TCP	74 [TCP Retransmission]
13	42.766984224	192.168.2.12	192.168.1.12	TCP	74 [TCP Retransmission]
14	44.930825074	PCSSystemtec_74:55:f8	PCSSystemtec_a1:db:16	ARP	42 Who has 192.168.2.19?
15	44.931841979	PCSSystemtec_a1:db:16	PCSSystemtec_74:55:f8	ARP	60 192.168.2.19 is at 00:00:27:01:b6:f2
16	49.762591216	192.168.2.12	192.168.1.12	TCP	74 42320 → 88 [SYN] Seq=0
17	50.709886793	192.168.2.12	192.168.1.12	TCP	74 [TCP Retransmission]
18	51.814041285	192.168.2.12	192.168.1.12	TCP	74 [TCP Retransmission]
19	52.846240254	192.168.2.12	192.168.1.12	TCP	74 [TCP Retransmission]
20	53.853035841	192.168.2.12	192.168.1.12	TCP	74 [TCP Retransmission]
21	54.886845598	192.168.2.12	192.168.1.12	TCP	74 [TCP Retransmission]

Figure 21: Web service check: B.1 to A.2

3.6 Allowed Web Services

The web services permitted between different computers in the network are:

- HTTP (port 80) allowed from B.1 to A.1 and A.2
- SSH (port 22) allowed only within Network A
- ICMP requests blocked from B to A, A can still ping to B.

3.7 Differences Between Task-III and Task-V Scans

Key differences observed between the scans conducted in Task-III and Task-V:

- Reduction in exposed open ports due to firewall implementation.
- Blocked ICMP responses after policy enforcement.
- Limited access to certain services that were previously open.

4 Task-VI: Testing Local Router Security Policy

4.1 Local Router Configuration Rules

Below is a screenshot of the firewall rules applied to the local A.1 router and explanations of their functions.

4.2 Wireshark Results: Local Network Web Service Checks

Wireshark captures demonstrating web service interactions within the local network:

```
vboxuser@Ubuntu:~$ sudo ufw status verbose
Status: inactive
vboxuser@Ubuntu:~$ sudo ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
vboxuser@Ubuntu:~$ sudo ufw default deny outgoing
Default outgoing policy changed to 'deny'
(be sure to update your rules accordingly)
vboxuser@Ubuntu:~$ sudo ufw allow proto tcp from 192.168.1.12 to any port 22
Rules updated
vboxuser@Ubuntu:~$ sudo ufw allow proto tcp from 192.168.1.12 to any port 80
Rules updated
vboxuser@Ubuntu:~$ sudo ufw allow proto tcp from 192.168.1.12 to any port 44
3
Rules updated
vboxuser@Ubuntu:~$ sudo ufw allow out 53
Rules updated
Rules updated (v6)
vboxuser@Ubuntu:~$ sudo ufw allow out proto icmp to any
ERROR: Unsupported protocol 'icmp'
vboxuser@Ubuntu:~$ sudo ufw allow out proto icmp to any
ERROR: Unsupported protocol 'icmp'
vboxuser@Ubuntu:~$ sudo ufw enable
Firewall is active and enabled on system startup
vboxuser@Ubuntu:~$ ufw status
\ERROR: You need to be root to run this script
vboxuser@Ubuntu:~$ sudo ufw status
Status: active
```

Figure 22: Local Router Rules on A.1

4.3 Allowed Web Services

Updated list of allowed web services between computers:

- HTTP (port 80) remains accessible within permitted nodes.
- SSH (port 22) still limited to specific network segments.
- Additional restrictions on unauthorized access to classified data.

4.4 Differences Between Task-V and Task-VI Scans

Comparison of security policy enforcement between Task-V and Task-VI:

- Strengthened access controls in Task-VI.
- Stricter policy enforcement leading to fewer detected open ports.
- Enhanced logging and tracking mechanisms in Task-VI implementation.

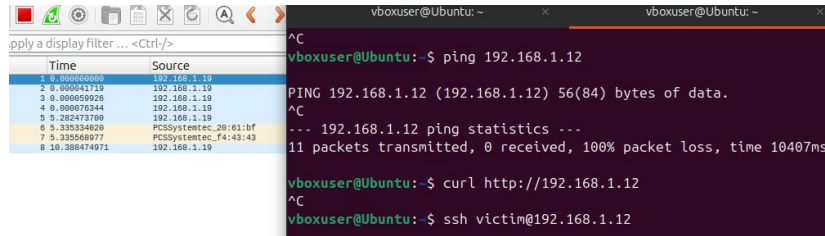


Figure 23: Web service check: B.1 to B.2

1	0.000000000	00000000.00002701b6f2	00000000.ffffffff	IPX SAP	60 Nearest Query
2	2.353933564	192.168.2.12	192.168.1.12	ICMP	98 Echo (ping) request id=0x045a, seq=1/256,
3	3.424486505	192.168.2.12	192.168.1.12	ICMP	98 Echo (ping) request id=0x045a, seq=2/512,
4	4.443136064	192.168.2.12	192.168.1.12	ICMP	98 Echo (ping) request id=0x045a, seq=3/768,
5	5.457835164	192.168.2.12	192.168.1.12	ICMP	98 Echo (ping) request id=0x045a, seq=4/1024,
6	6.487845342	192.168.2.12	192.168.1.12	ICMP	98 Echo (ping) request id=0x045a, seq=5/1280,
7	7.478500223	PCSSystemtec_74:55:f8	PCSSystemtec_a1:db:16	ARP	42 Who has 192.168.2.10? Tell 192.168.2.12
8	7.478764714	PCSSystemtec_a1:db:16	PCSSystemtec_74:55:f8	ARP	60 192.168.2.10 is at 08:00:27:a1:db:16
9	5.088949303	192.168.2.12	192.168.1.12	TCP	74 55770 - 80 [SYN] Seq=0 Win=64240 Len=0 MSS=
10	10.116634395	192.168.2.12	192.168.1.12	TCP	74 [TCP Retransmission] 55770 - 80 [SYN] Seq=0
11	17.4169391896	192.168.2.12	192.168.1.12	TCP	74 [TCP Retransmission] 55770 - 80 [SYN] Seq=0
12	18.194323647	192.168.2.12	192.168.1.12	TCP	74 [TCP Retransmission] 55770 - 80 [SYN] Seq=0
13	19.238205518	192.168.2.12	192.168.1.12	TCP	74 [TCP Retransmission] 55770 - 80 [SYN] Seq=0
14	40.901376602	192.168.2.12	192.168.1.12	TCP	74 45006 - 22 [SYN] Seq=0 Win=64240 Len=0 MSS=
15	41.993702165	192.168.2.12	192.168.1.12	TCP	74 [TCP Retransmission] 45006 - 22 [SYN] Seq=0
16	42.993946659	192.168.2.12	192.168.1.12	TCP	74 [TCP Retransmission] 45006 - 22 [SYN] Seq=0
17	44.018136423	192.168.2.12	192.168.1.12	TCP	74 [TCP Retransmission] 45006 - 22 [SYN] Seq=0
18	45.051535918	192.168.2.12	192.168.1.12	TCP	74 [TCP Retransmission] 45006 - 22 [SYN] Seq=0
19	46.123332653	PCSSystemtec_74:55:f8	PCSSystemtec_a1:db:16	ARP	42 Who has 192.168.2.10? Tell 192.168.2.12
20	46.130421213	PCSSystemtec_a1:db:16	PCSSystemtec_74:55:f8	ARP	60 192.168.2.10 is at 08:00:27:a1:db:16
21	59.992427939	00000000.00002701b6f2	00000000.ffffffff	IPX SAP	60 General Query

Figure 24: Web service check: B.1 to A.1 (Local Network)

1	0.000000000	192.168.2.12	192.168.1.19	ICMP	98 Echo (ping) request
2	1.018688160	192.168.2.12	192.168.1.19	ICMP	98 Echo (ping) request
3	2.042282640	192.168.2.12	192.168.1.19	ICMP	98 Echo (ping) request
4	3.098455975	192.168.2.12	192.168.1.19	ICMP	98 Echo (ping) request
5	4.122073440	192.168.2.12	192.168.1.19	ICMP	98 Echo (ping) request
6	5.146136084	192.168.2.12	192.168.1.19	ICMP	98 Echo (ping) request
7	9.146606419	PCSSystemtec_74:55:f8	PCSSystemtec_a1:db:16	ARP	42 Who has 192.168.2.10?
8	9.146801776	PCSSystemtec_a1:db:16	PCSSystemtec_74:55:f8	ARP	60 192.168.2.10 is at 08
9	10.575956566	192.168.2.12	192.168.1.12	TCP	74 47052 - 80 [SYN] Seq=
10	11.066193251	192.168.2.12	192.168.1.12	TCP	74 [TCP Retransmission]
11	12.630079904	192.168.2.12	192.168.1.12	TCP	74 [TCP Retransmission]
12	13.654454281	192.168.2.12	192.168.1.12	TCP	74 [TCP Retransmission]
13	14.761309221	192.168.2.12	192.168.1.12	TCP	74 [TCP Retransmission]
14	15.704294186	192.168.2.12	192.168.1.12	TCP	74 [TCP Retransmission]
15	31.498738356	192.168.2.12	192.168.1.19	TCP	74 57392 - 22 [SYN] Seq=
16	32.515436273	192.168.2.12	192.168.1.19	TCP	74 [TCP Retransmission]
17	33.531620021	192.168.2.12	192.168.1.19	TCP	74 [TCP Retransmission]
18	34.551801875	192.168.2.12	192.168.1.19	TCP	74 [TCP Retransmission]
19	35.574423144	192.168.2.12	192.168.1.19	TCP	74 [TCP Retransmission]
20	36.609327950	192.168.2.12	192.168.1.19	TCP	74 [TCP Retransmission]

Figure 25: Web service check: B.1 to B.2

1	0.000000000	00000000.00002701b6f2	00000000.ffffffff	IPX SAP	60 General Query
2	4.875642054	192.168.2.12	192.168.2.13	ICMP	98 Echo (ping) request
3	4.875802409	PCSSystemtec_01:b6:f2	Broadcast	ARP	60 Who has 192.168.2.12
4	4.875809400	PCSSystemtec_74:55:f8	PCSSystemtec_01:b6:f2	ARP	42 192.168.2.12 is at 6
5	4.875896798	192.168.2.13	192.168.2.12	ICMP	98 Echo (ping) reply
6	5.902710103	192.168.2.12	192.168.2.13	ICMP	98 Echo (ping) request
7	5.902874293	192.168.2.13	192.168.2.12	ICMP	98 Echo (ping) reply
8	6.933710748	192.168.2.12	192.168.2.13	ICMP	98 Echo (ping) request
9	6.933922518	192.168.2.13	192.168.2.12	ICMP	98 Echo (ping) reply
10	9.887823836	PCSSystemtec_74:55:f8	PCSSystemtec_01:b6:f2	ARP	42 Who has 192.168.2.13
11	9.887958814	PCSSystemtec_01:b6:f2	PCSSystemtec_74:55:f8	ARP	60 192.168.2.13 is at 6
12	12.621233588	192.168.2.12	192.168.2.13	TCP	74 43146 - 80 [SYN] Seq=
13	12.621469298	192.168.2.13	192.168.2.12	TCP	60 80 - 43146 [RST, ACK
14	15.68.000025399	192.168.2.12	192.168.2.13	TCP	74 49784 - 80 [SYN] Seq=
15	16.68.000173377	192.168.2.13	192.168.2.12	TCP	60 80 - 49784 [RST, ACK
17	73.906473140	PCSSystemtec_74:55:f8	PCSSystemtec_01:b6:f2	ARP	42 Who has 192.168.2.13
18	73.906706937	PCSSystemtec_01:b6:f2	PCSSystemtec_74:55:f8	ARP	60 192.168.2.13 is at 6

Figure 26: Web service check: B.1 to A.1 (Local Network)

4.5 Security Policy Effectiveness in Protecting Classified Data

The security policy aims to prevent classified data leaks from Computer A.1. However, potential vulnerabilities include:

- Insider threats—authorized users transferring data manually.
- Lack of monitoring on encrypted traffic.
- Missing policies for data loss prevention (DLP) strategies.

Recommendations for stronger enforcement:

- Implement stricter logging and access controls.
- Use encryption for stored and transmitted data.
- Deploy intrusion detection systems (IDS) to monitor abnormal access patterns.

5 Conclusion

This project provided hands-on experience in setting up a virtual sandbox, configuring network security, and analyzing traffic. Challenges faced included network configuration issues and firewall misconfigurations, which were resolved through debugging and testing. The project successfully enforced a security policy to control network traffic between internal and external systems. One of the key takeaways from this project was the importance of layered security. Layered security is incredibly important because simply blocking or allowing traffic through a firewall isn't enough. A well structured security policy must take into consideration for outbound and inbound rules, service restrictions, and any potential attacks. By limiting external access to only essential services (such as HTTP to the web server) and restricting the internal workstations from exposing services, we successfully minimized the attack surface of the network. Seeing how the pre to post security scans were also provided a lot of insight to us as in how a firewall could be manipulated and exposed by attackers. The Access Control Matrix and new router rules helped in creating strong boundaries so there wouldn't be any unauthorized access nor data leaks. Overall this project really helped in strengthening our skills in network security, access control and monitoring traffic. Doing a project like this which can be easily applied in a real life setting taught us the importance of having a secure network. For the future it would be interesting to test attack scenarios and improving our firewall policies