Penetration Testing a pfSense Firewall (3e)

Network Security, Firewalls, and VPNs, Third Edition - Lab 10

Student:	Email:
Vidhi Kadakia	jinsukrishna108@gmail.com

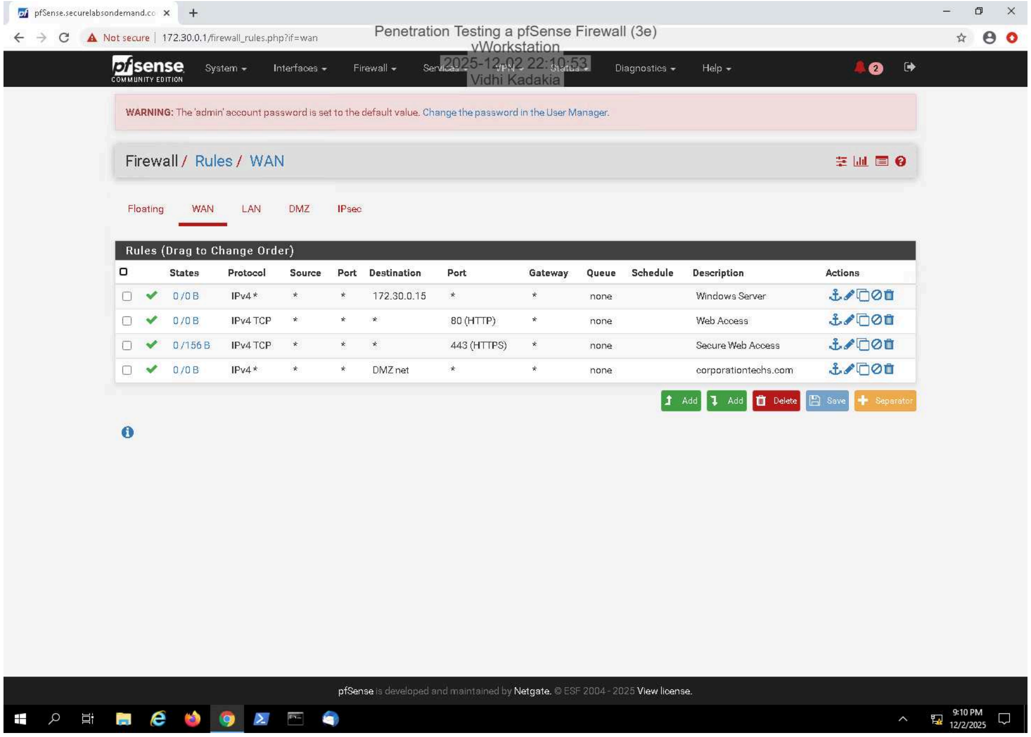
Time on Task:	Progress:
4 hours, 33 minutes	100%

Report Generated: Wednesday, December 3, 2025 at 5:03 PM

Section 1: Hands-On Demonstration

Part 1: Examine a pfSense Firewall Configuration

12. **Make a screen capture** showing the **WAN rules table**.



pfSense.securelabsondemand.co
172.30.0.1/firewall_rules.php?if=wan
Penetration Testing a pfSense Firewall (3e)
vWorkstation
2025-12-02 22:10:53
Vidhi Kadakia
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Firewall / Rules / WAN

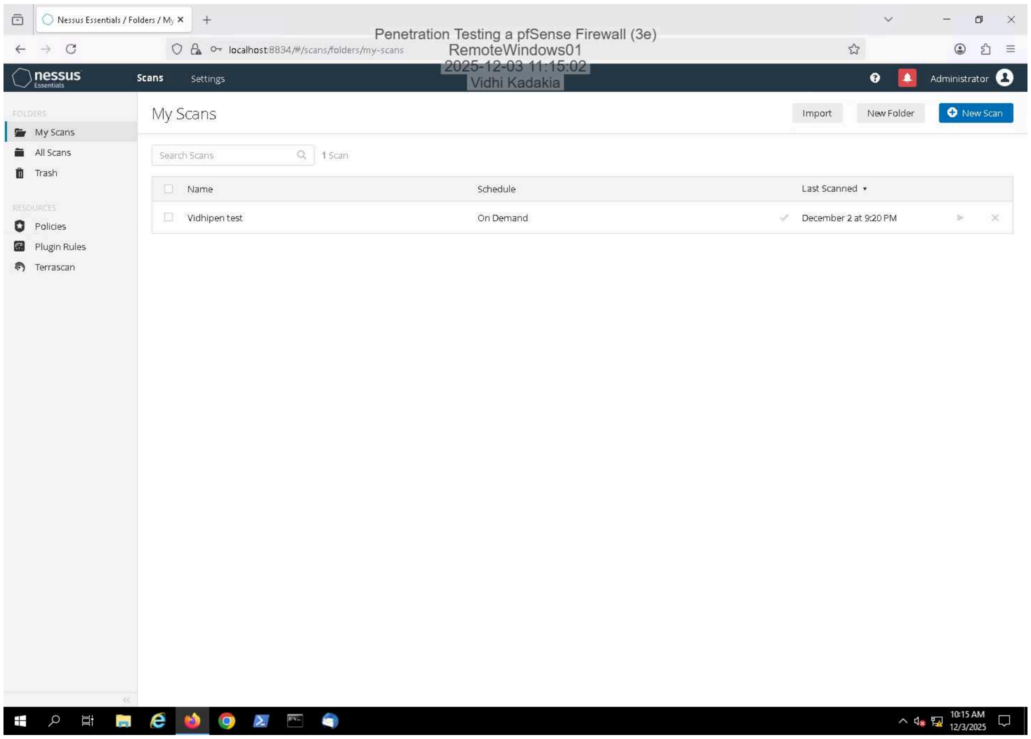
Rules (Drag to Change Order)

☐		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☐	✓	0 / 0 B	IPv4 *	*	*	172.30.0.15	*	*	none		Windows Server	
☐	✓	0 / 0 B	IPv4 TCP	*	*	*	80 (HTTP)	*	none		Web Access	
☐	✓	0 / 156 B	IPv4 TCP	*	*	*	443 (HTTPS)	*	none		Secure Web Access	
☐	✓	0 / 0 B	IPv4 *	*	*	DMZ net	*	*	none		corporationtechs.com	

Add
Add
Delete
Save
Separator
pfSense is developed and maintained by Netgate. © ESF 2004 - 2025 View license.
9:10 PM
12/2/2025

Part 2: Conduct a Penetration Test on the Network

11. **Make a screen capture** showing the ***yourname*** **pen test scan results**.



Penetration Testing a pfSense Firewall (3e)
RemoteWindows01
2025-12-03 11:15:02
Vidhi Kadakia

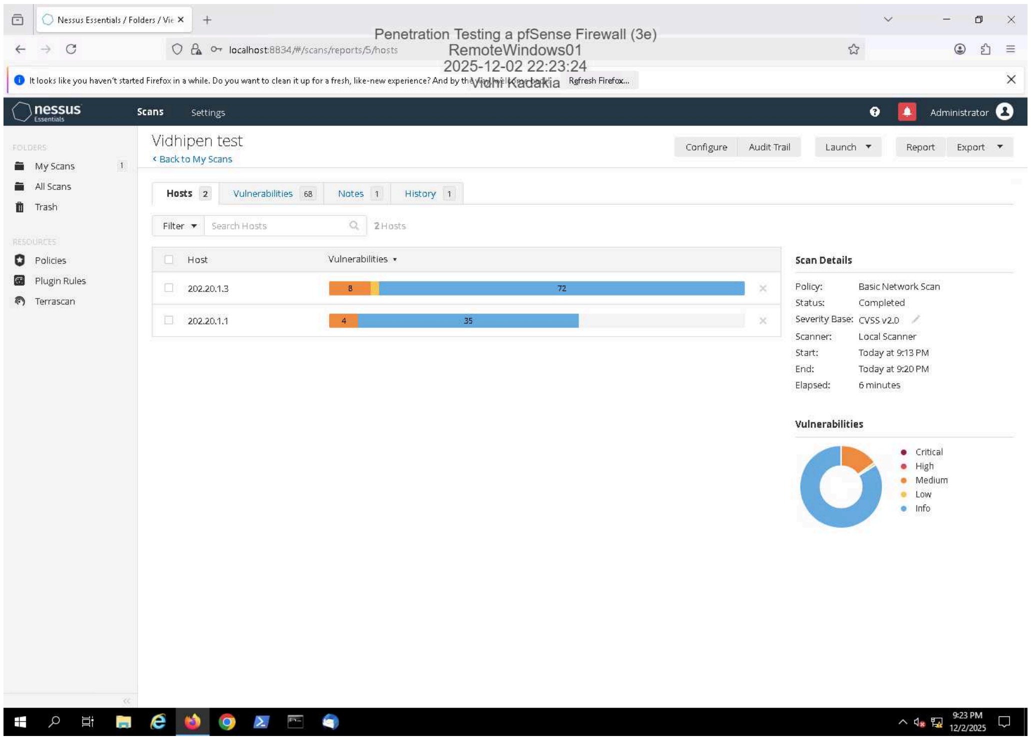
localhost:8834/#/scans/folders/my-scans

My Scans

1 Scan

Name	Schedule	Last Scanned ▾
Vidhipen test	On Demand	December 2 at 9:20 PM

13. **Make a screen capture** showing the **list of vulnerabilities**.



Penetration Testing a pfSense Firewall (3e)
RemoteWindows01
2025-12-02 22:23:24
Vidhi Kadakia

localhost:8834/#/scans/reports/5/hosts

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

Vidhipen test

2 Hosts

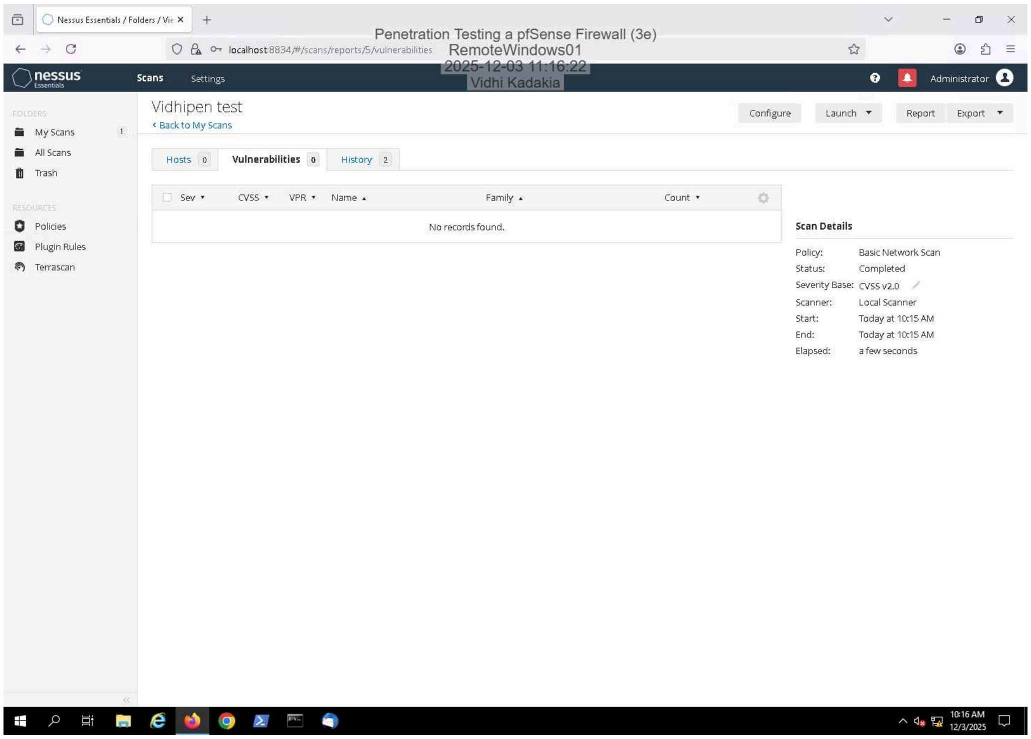
Host	Vulnerabilities ▾
202.20.1.3	8 72
202.20.1.1	4 35

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v2.0
Scanner:	Local Scanner
Start:	Today at 9:13 PM
End:	Today at 9:20 PM
Elapsed:	6 minutes

Vulnerabilities

30. **Make a screen capture** showing the **updated vulnerability report summary**.



Penetration Testing a pfSense Firewall (3e)
RemoteWindows01
2025-12-03 11:16:22
Vidhi Kadakia

Vidhipen test
‹ Back to My Scans

□	Sev	CVSS	VPR	Name	Family	Count
				No records found.		

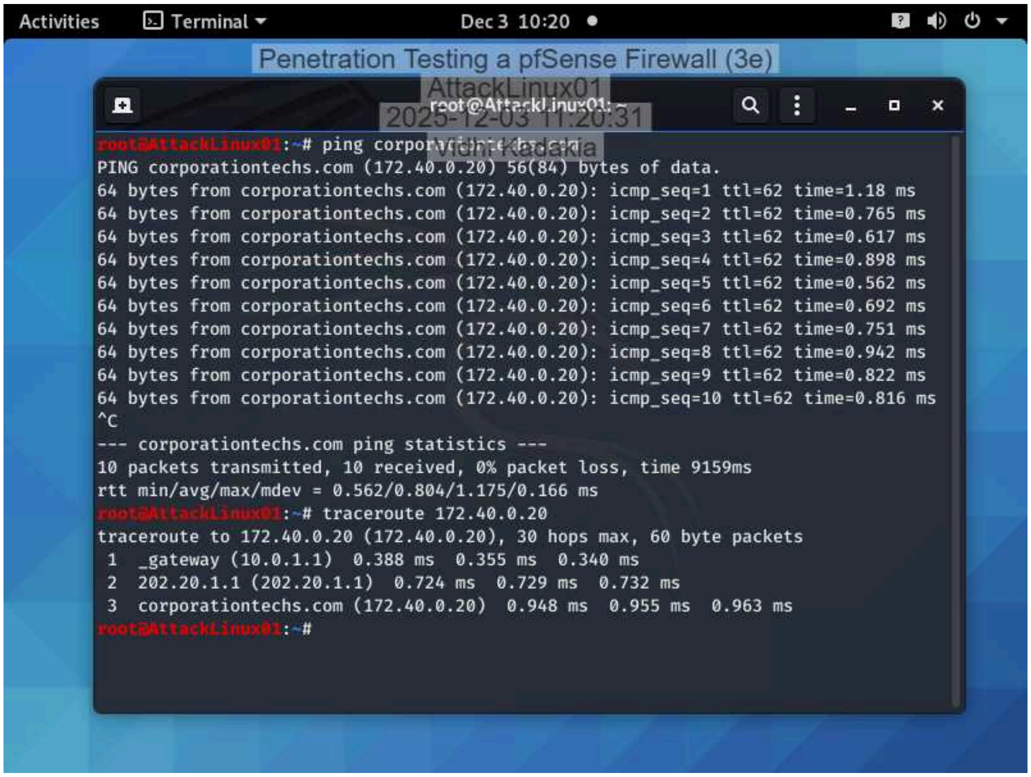
Scan Details

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v2.0
Scanner:	Local Scanner
Start:	Today at 10:15 AM
End:	Today at 10:15 AM
Elapsed:	a few seconds

Section 2: Applied Learning

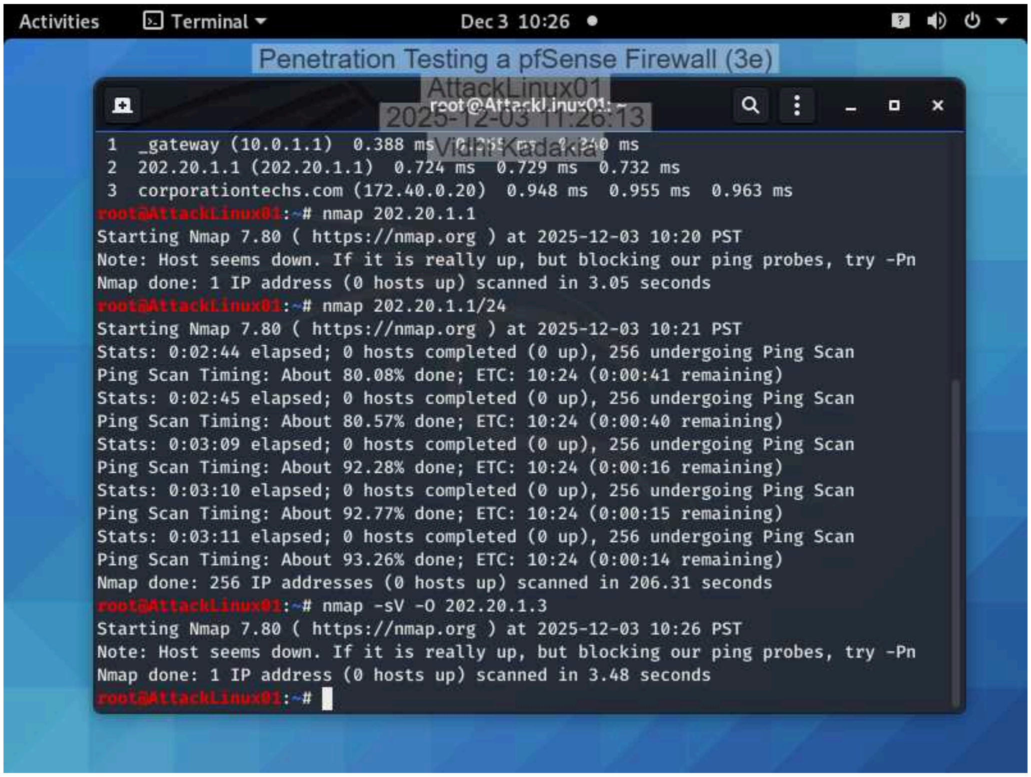
Part 1: Conduct a Port Scan on the Network

7. **Make a screen capture** showing the **results of the traceroute command**.



```
root@AttackLinux01:~# ping corporationtechs.com
PING corporationtechs.com (172.40.0.20) 56(84) bytes of data.
64 bytes from corporationtechs.com (172.40.0.20): icmp_seq=1 ttl=62 time=1.18 ms
64 bytes from corporationtechs.com (172.40.0.20): icmp_seq=2 ttl=62 time=0.765 ms
64 bytes from corporationtechs.com (172.40.0.20): icmp_seq=3 ttl=62 time=0.617 ms
64 bytes from corporationtechs.com (172.40.0.20): icmp_seq=4 ttl=62 time=0.898 ms
64 bytes from corporationtechs.com (172.40.0.20): icmp_seq=5 ttl=62 time=0.562 ms
64 bytes from corporationtechs.com (172.40.0.20): icmp_seq=6 ttl=62 time=0.692 ms
64 bytes from corporationtechs.com (172.40.0.20): icmp_seq=7 ttl=62 time=0.751 ms
64 bytes from corporationtechs.com (172.40.0.20): icmp_seq=8 ttl=62 time=0.942 ms
64 bytes from corporationtechs.com (172.40.0.20): icmp_seq=9 ttl=62 time=0.822 ms
64 bytes from corporationtechs.com (172.40.0.20): icmp_seq=10 ttl=62 time=0.816 ms
^C
--- corporationtechs.com ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9159ms
rtt min/avg/max/mdev = 0.562/0.804/1.175/0.166 ms
root@AttackLinux01:~# traceroute 172.40.0.20
traceroute to 172.40.0.20 (172.40.0.20), 30 hops max, 60 byte packets
 1  _gateway (10.0.1.1)  0.388 ms  0.355 ms  0.340 ms
 2  202.20.1.1 (202.20.1.1)  0.724 ms  0.729 ms  0.732 ms
 3  corporationtechs.com (172.40.0.20)  0.948 ms  0.955 ms  0.963 ms
root@AttackLinux01:~#
```

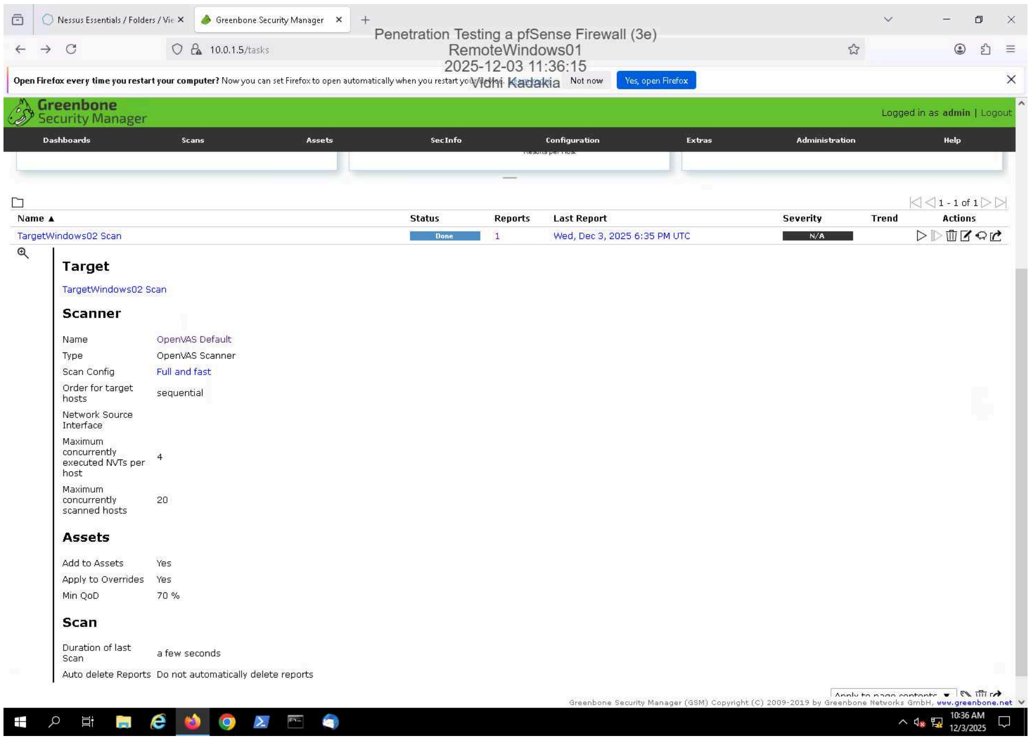
11. **Make a screen capture** showing the result of the **nmap scan with OS detection activated**.



```
 1  _gateway (10.0.1.1)  0.388 ms  0.355 ms  0.340 ms
 2  202.20.1.1 (202.20.1.1)  0.724 ms  0.729 ms  0.732 ms
 3  corporationtechs.com (172.40.0.20)  0.948 ms  0.955 ms  0.963 ms
root@AttackLinux01:~# nmap 202.20.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2025-12-03 10:20 PST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.05 seconds
root@AttackLinux01:~# nmap 202.20.1.1/24
Starting Nmap 7.80 ( https://nmap.org ) at 2025-12-03 10:21 PST
Stats: 0:02:44 elapsed; 0 hosts completed (0 up), 256 undergoing Ping Scan
Ping Scan Timing: About 80.08% done; ETC: 10:24 (0:00:41 remaining)
Stats: 0:02:45 elapsed; 0 hosts completed (0 up), 256 undergoing Ping Scan
Ping Scan Timing: About 80.57% done; ETC: 10:24 (0:00:40 remaining)
Stats: 0:03:09 elapsed; 0 hosts completed (0 up), 256 undergoing Ping Scan
Ping Scan Timing: About 92.28% done; ETC: 10:24 (0:00:16 remaining)
Stats: 0:03:10 elapsed; 0 hosts completed (0 up), 256 undergoing Ping Scan
Ping Scan Timing: About 92.77% done; ETC: 10:24 (0:00:15 remaining)
Stats: 0:03:11 elapsed; 0 hosts completed (0 up), 256 undergoing Ping Scan
Ping Scan Timing: About 93.26% done; ETC: 10:24 (0:00:14 remaining)
Nmap done: 256 IP addresses (0 hosts up) scanned in 206.31 seconds
root@AttackLinux01:~# nmap -sV -O 202.20.1.3
Starting Nmap 7.80 ( https://nmap.org ) at 2025-12-03 10:26 PST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.48 seconds
root@AttackLinux01:~# 
```

Part 2: Conduct a Vulnerability Scan on the Network

12. **Make a screen capture** showing the **OpenVAS scan report**.



Penetration Testing a pfSense Firewall (3e)
RemoteWindows01
2025-12-03 11:36:15
Vidhi Kadakia

10.0.1.5/tasks

Open Firefox every time you restart your computer? Now you can set Firefox to open automatically when you restart your device.

Logged in as admin | Logout

Name ▲	Status	Reports	Last Report	Severity	Trend	Actions
TargetWindows02 Scan	Done	1	Wed, Dec 3, 2025 6:35 PM UTC	N/A		

Target

TargetWindows02 Scan

Scanner

Name	OpenVAS Default
Type	OpenVAS Scanner
Scan Config	Full and fast
Order for target hosts	sequential
Network Source Interface	
Maximum concurrently executed NVTs per host	4
Maximum concurrently scanned hosts	20

Assets

Add to Assets	Yes
Apply to Overrides	Yes
Min QoD	70 %

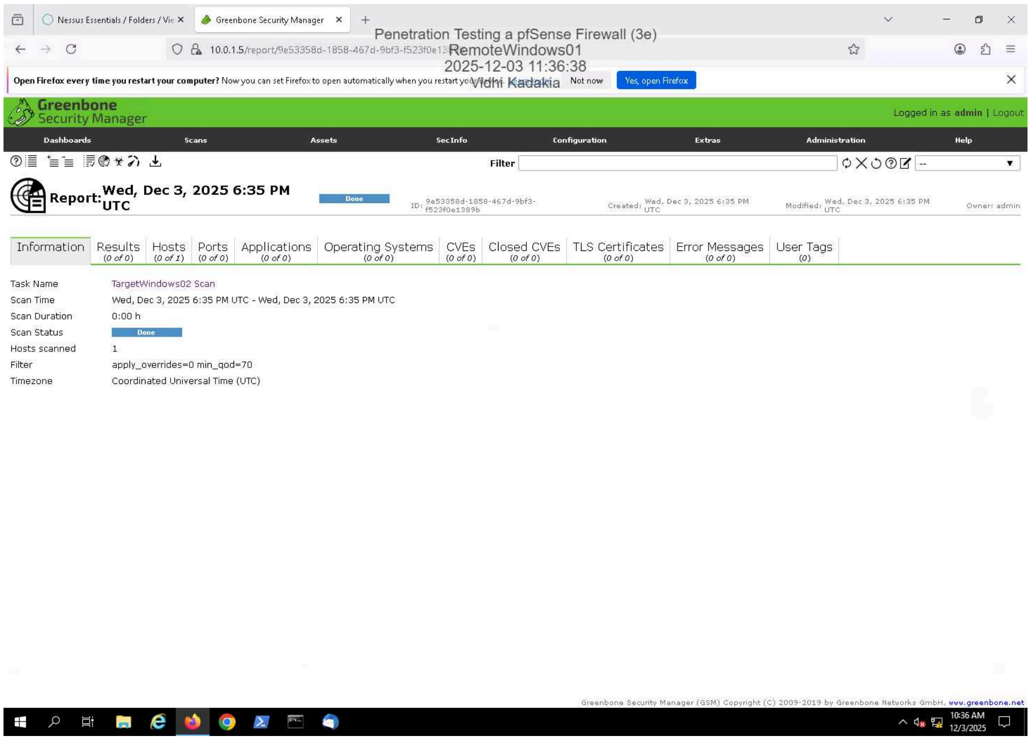
Scan

Duration of last Scan	a few seconds
Auto delete Reports	Do not automatically delete reports

Greenbone Security Manager (GSM) Copyright (C) 2009-2019 by Greenbone Networks GmbH, www.greenbone.net

10:36 AM
12/3/2025

14. **Make a screen capture** showing the **detailed OpenVAS scan results**.



Penetration Testing a pfSense Firewall (3e)
RemoteWindows01
2025-12-03 11:36:38
Vidhi Kadakia

10.0.1.5/report/9e53358d-1858-467d-9bf3-f523f0e13

Open Firefox every time you restart your computer? Now you can set Firefox to open automatically when you restart your device.

Logged in as admin | Logout

Report: Wed, Dec 3, 2025 6:35 PM UTC Done

ID: 9e53358d-1858-467d-9bf3-f523f0e1389b Created: Wed, Dec 3, 2025 6:35 PM UTC Modified: Wed, Dec 3, 2025 6:35 PM UTC Owner: admin

Information	Results	Hosts	Ports	Applications	Operating Systems	CVEs	Closed CVEs	TLS Certificates	Error Messages	User Tags
	(0 of 0)	(0 of 1)	(0 of 0)	(0 of 0)	(0 of 0)	(0 of 0)	(0 of 0)	(0 of 0)	(0 of 0)	(0)

Task Name	TargetWindows02 Scan
Scan Time	Wed, Dec 3, 2025 6:35 PM UTC - Wed, Dec 3, 2025 6:35 PM UTC
Scan Duration	0:00 h
Scan Status	Done
Hosts scanned	1
Filter	apply_overrides=0 min_qod=70
Timezone	Coordinated Universal Time (UTC)

Greenbone Security Manager (GSM) Copyright (C) 2009-2019 by Greenbone Networks GmbH, www.greenbone.net

10:36 AM
12/3/2025

Section 3: Challenge and Analysis

Part 1: Research DMZ Deployment Best Practices

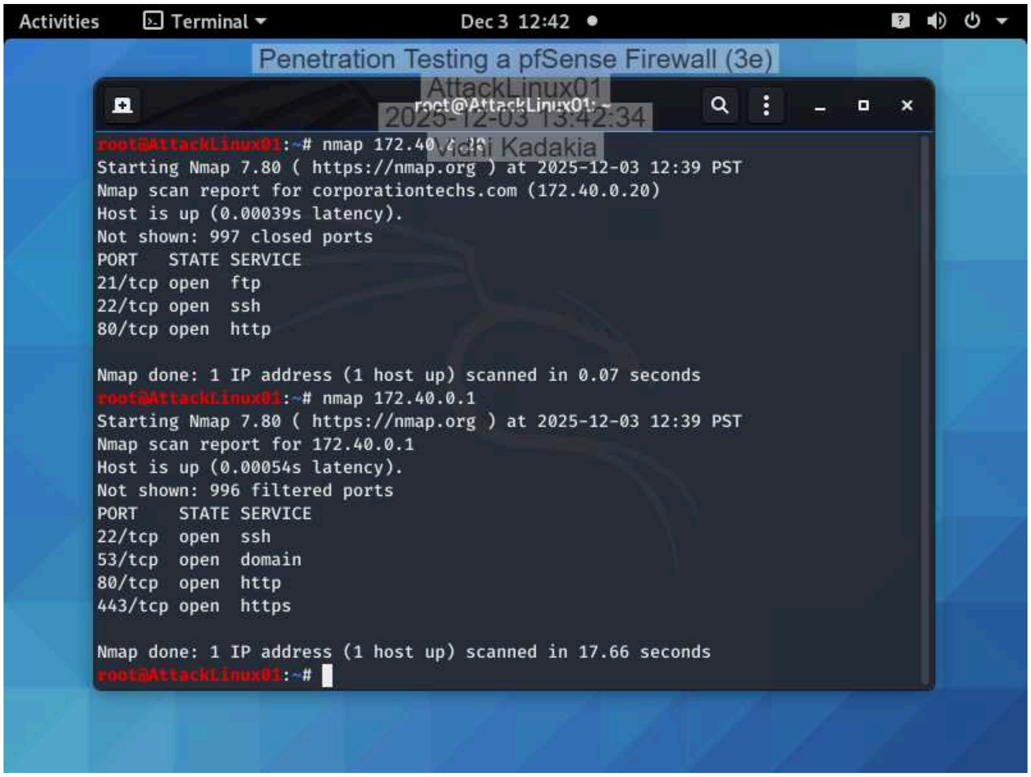
Before beginning the technical portion of your penetration test, you decide to spend some time brushing up on best practices and common mistakes for DMZ deployments - both the network aspect and the servers located therein. Use the Internet to **research** DMZ deployments, then **identify** three best practices and one potential mistake or vulnerability.

1. Keep the DMZ separate: Put public facing servers in a separate network zone so attackers cannot reach internal systems easily. Use firewalls to strictly control traffic in and out of the DMZ

2. Allow only necessary traffic: Open only the exact ports and services that DMZ servers need. Block everything else to reduce attack paths.
3. Harden and monitor DMZ servers: Keep DMZ servers patched, remove unused software and enable logging. Watch them closely since they face the internet.

Part 2: Conduct a Penetration Test on the DMZ

Make a screen capture showing the **open ports on the corporationtechs.com web server and the DMZ firewall interface**.

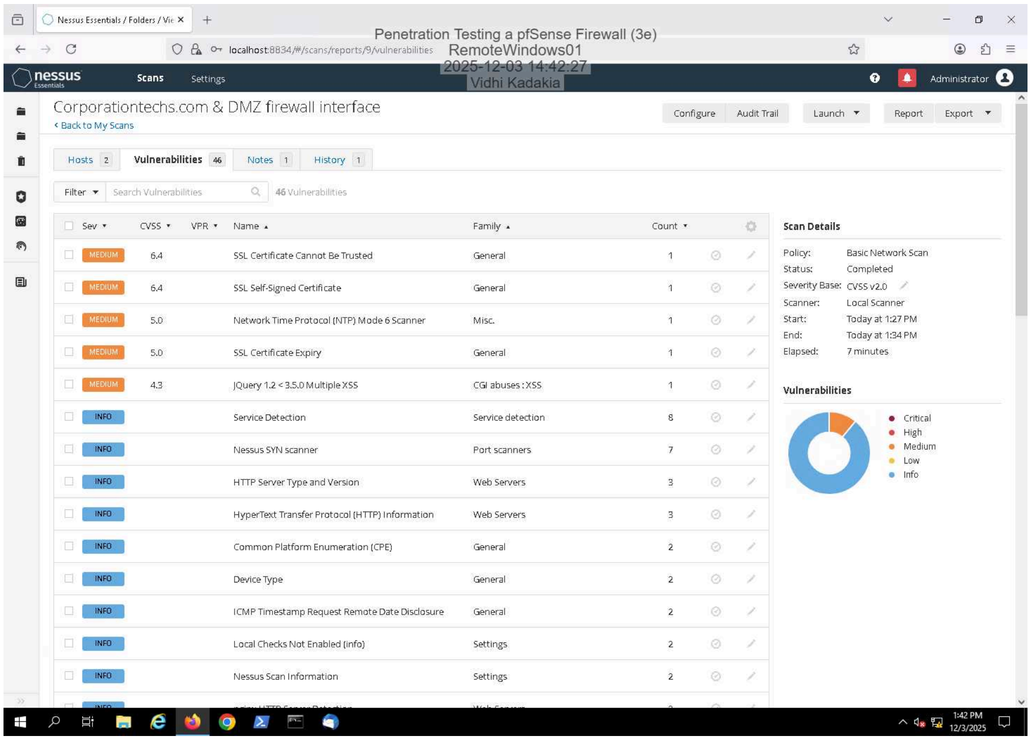


```
root@AttackLinux01:~# nmap 172.40.0.20
Starting Nmap 7.80 ( https://nmap.org ) at 2025-12-03 12:39 PST
Nmap scan report for corporationtechs.com (172.40.0.20)
Host is up (0.00039s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
root@AttackLinux01:~# nmap 172.40.0.1
Starting Nmap 7.80 ( https://nmap.org ) at 2025-12-03 12:39 PST
Nmap scan report for 172.40.0.1
Host is up (0.00054s latency).
Not shown: 996 filtered ports
PORT    STATE SERVICE
22/tcp  open  ssh
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 17.66 seconds
root@AttackLinux01:~# 
```

Make a screen capture showing the **vulnerability scan results**.



Penetration Testing a pfSense Firewall (3e)
RemoteWindows01
2025-12-03 14:42:27
Vidhi Kadakia

Corporationtechs.com & DMZ firewall interface
‹ Back to My Scans

46 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count
MEDIUM	6.4		SSL Certificate Cannot Be Trusted	General	1
MEDIUM	6.4		SSL Self-Signed Certificate	General	1
MEDIUM	5.0		Network Time Protocol (NTP) Mode 6 Scanner	Misc.	1
MEDIUM	5.0		SSL Certificate Expiry	General	1
MEDIUM	4.3		JQuery 1.2 < 3.5.0 Multiple XSS	CGI abuses : XSS	1
INFO			Service Detection	Service detection	8
INFO			Nessus SYN scanner	Port scanners	7
INFO			HTTP Server Type and Version	Web Servers	3
INFO			HyperText Transfer Protocol (HTTP) Information	Web Servers	3
INFO			Common Platform Enumeration (CPE)	General	2
INFO			Device Type	General	2
INFO			ICMP Timestamp Request Remote Date Disclosure	General	2
INFO			Local Checks Not Enabled (info)	Settings	2
INFO			Nessus Scan Information	Settings	2

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v2.0
Scanner:	Local Scanner
Start:	Today at 1:27 PM
End:	Today at 1:34 PM
Elapsed:	7 minutes

Vulnerabilities

Part 3: Recommend Changes to the DMZ

Based on your research in Part 1 and your findings in Part 2, **prepare a brief summary** of recommended changes that Secure Labs on Demand should make to their DMZ deployment. Remember, your recommendations should apply to both the network configuration and the web server.

Secure Labs on Demand should improve their DMZ by fixing the SSL problems first, since the scan shows self-signed and expired certificates. They should replace these with a trusted certificate and only allow newer TLS versions. The web server also needs updates, including fixing the old jQuery version and installing all security patches. They should close or disable any services that don’t need to be open, like NTP mode 6, extra information the web server gives out, and ICMP timestamp replies. The firewall rules should be tightened so only required ports are open, and the DMZ has limited access back to the internal network. Finally, the servers in the DMZ should be better protected with logging, monitoring, and host firewalls to reduce risk and detect issues quickly.