

# Penetration Testing a pfSense Firewall (3e)

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

Student:

Belizaire Bassette II

Email:

bebasset@syr.edu

Time on Task:

57 hours, 52 minutes

Progress:

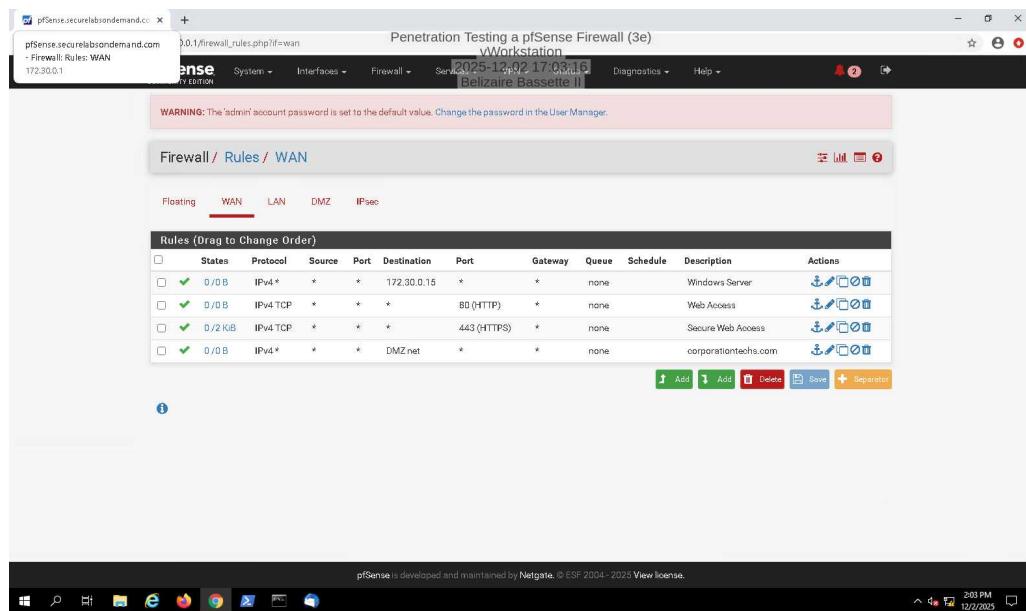
100%

Report Generated: Wednesday, December 3, 2025 at 6:48 PM

## Section 1: Hands-On Demonstration

### Part 1: Examine a pfSense Firewall Configuration

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



The screenshot shows the pfSense Firewall configuration interface. The title bar indicates the URL is `pfSense.securelabondemand.com` and the page is `0.0.1/firewall_rules.php?if=wan`. The top navigation bar includes tabs for Firewall, System, Interfaces, and Diagnostics. The Firewall tab is selected. The main content area is titled "Firewall / Rules / WAN". Below this, there are tabs for Floating, WAN, LAN, DMZ, and IPsec. The WAN tab is selected. The main table is titled "Rules (Drag to Change Order)" and lists the following rules:

Index	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions			
1	0 / 0 B	IPv4 *	*	*	172.30.0.15	*	*	none		Windows Server				
2	0 / 0 B	IPv4 TCP	*	*	*	80 (HTTP)	*	none		Web Access				
3	0 / 2 KB	IPv4 TCP	*	*	*	443 (HTTPS)	*	none		Secure Web Access				
4	0 / 0 B	IPv4 *	*	*	DMZ net	*	*	none		corporationtechs.com				

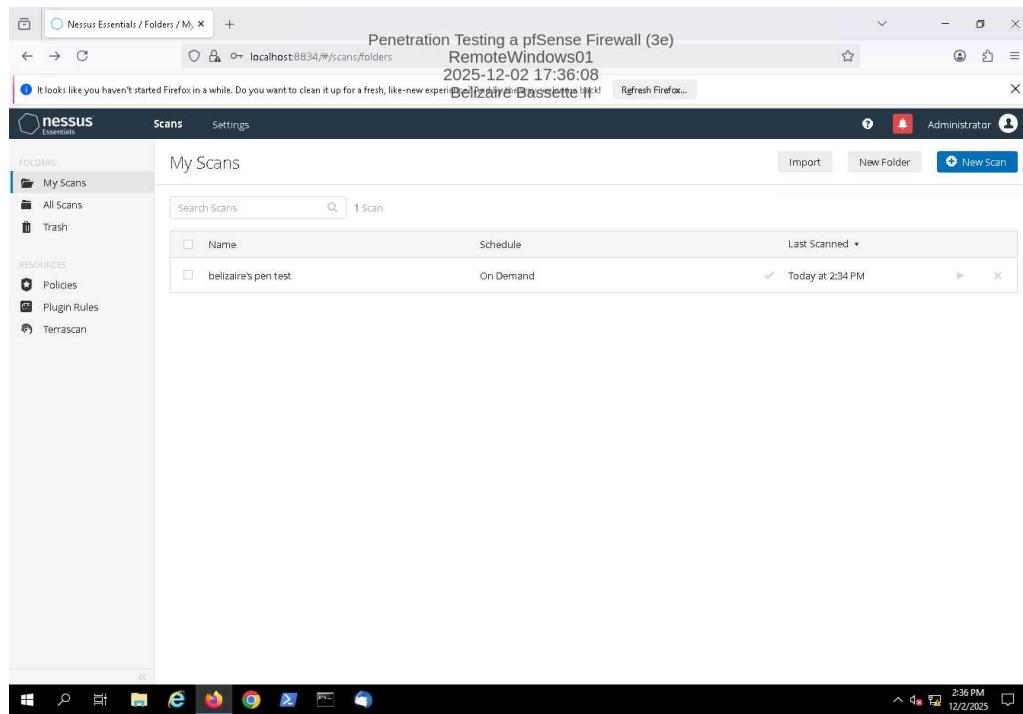
At the bottom of the table are buttons for Add, Add, Delete, Save, and Separator. The pfSense footer at the bottom of the screen indicates it is developed and maintained by Netgate, © ESF 2004-2025 View license.

### Part 2: Conduct a Penetration Test on the Network

# Penetration Testing a pfSense Firewall (3e)

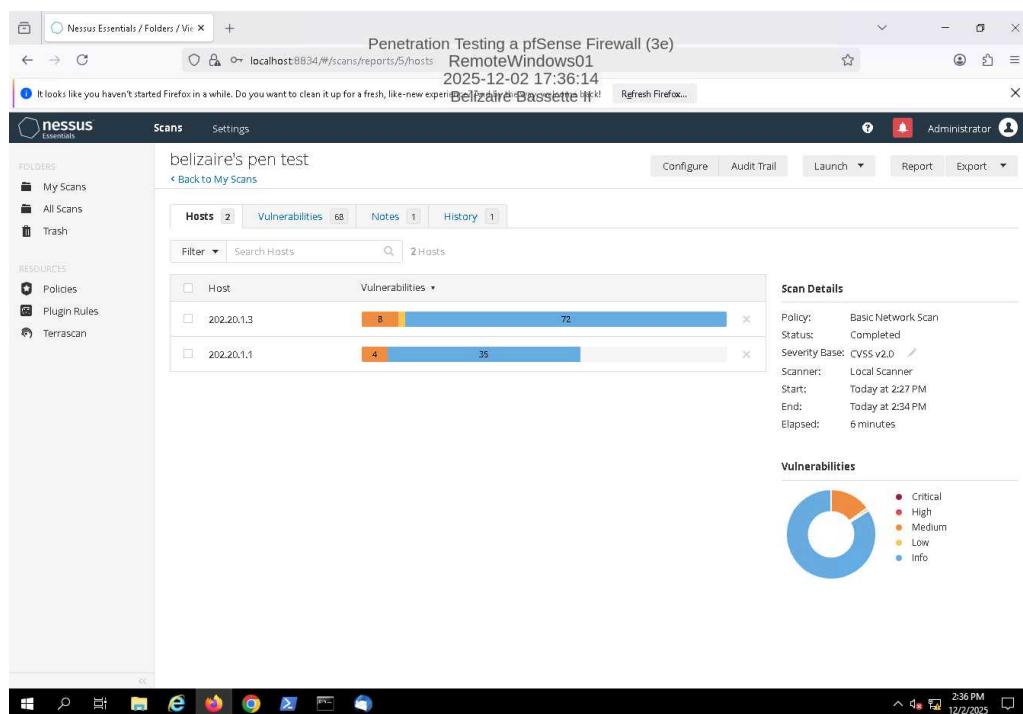
Network Security, Firewalls, and VPNs, Third Edition - Lab 10

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



The screenshot shows the Nessus Essentials interface. The title bar reads "Penetration Testing a pfSense Firewall (3e) RemoteWindows01 2025-12-02 17:36:08". The main content area is titled "My Scans" and shows a table with one scan entry: "belizaire's pen test" (On Demand, Last Scanned: Today at 2:34 PM). The left sidebar includes sections for FOLDERS (My Scans, All Scans, Trash), RESOURCES (Policies, Plugin Rules, Terrascan), and a "Scans" tab. The bottom status bar shows the date and time as 12/2/2025 2:36 PM.

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

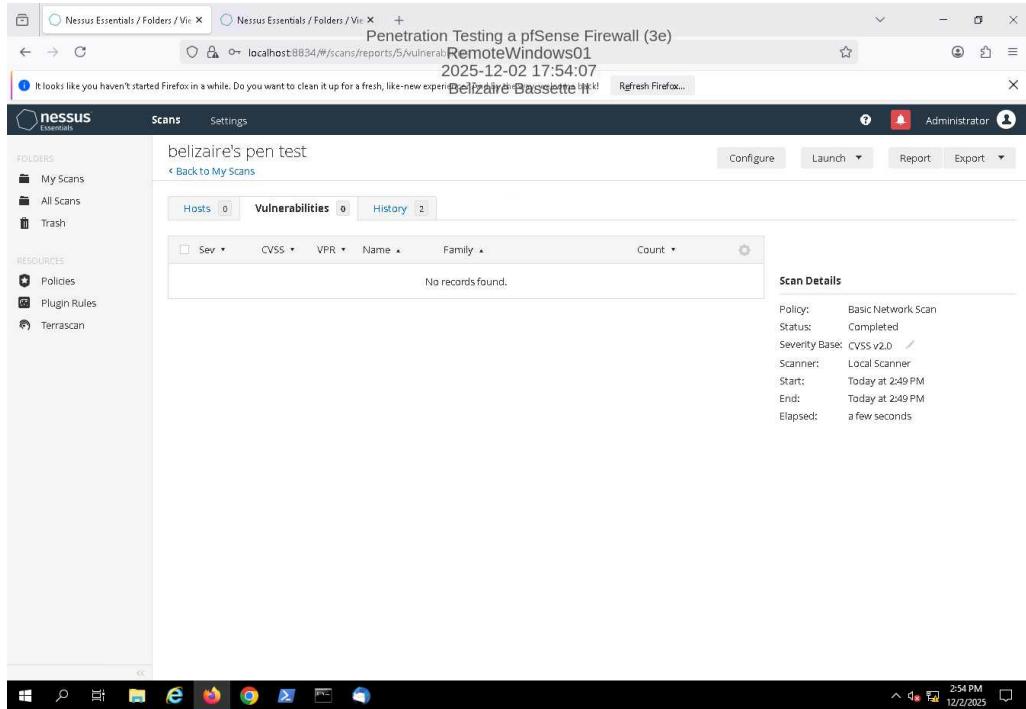


The screenshot shows the Nessus Essentials interface for the "belizaire's pen test" scan. The title bar is the same as the previous screenshot. The main content area shows a table of hosts: "202.20.1.3" with 8 critical and 72 medium vulnerabilities, and "202.20.1.1" with 4 critical and 35 medium vulnerabilities. To the right, the "Scan Details" panel provides information: Policy: Basic Network Scan, Status: Completed, Severity Base: CVSS v2.0, Scanner: Local Scanner, Start: Today at 2:27 PM, End: Today at 2:34 PM, and Elapsed: 6 minutes. Below the table is a "Vulnerabilities" section with a pie chart showing the distribution of severity levels: Critical (orange), High (red), Medium (yellow), Low (light blue), and Info (light blue).

# Penetration Testing a pfSense Firewall (3e)

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

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



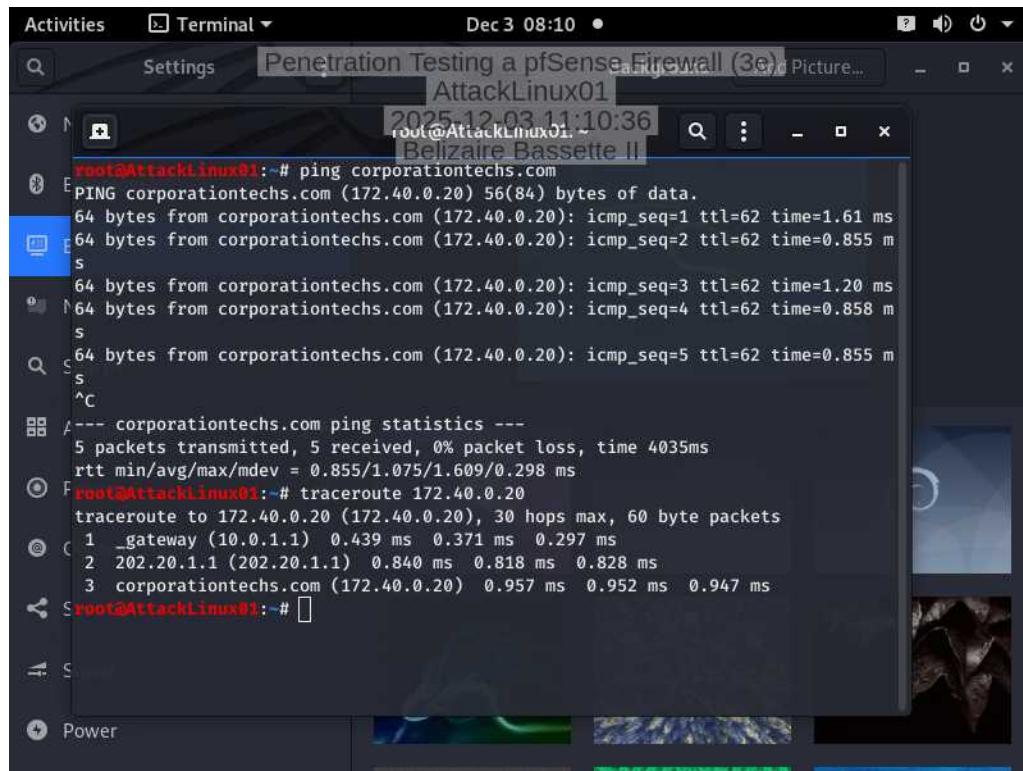
The screenshot shows the Nessus Essentials interface with the following details:

- Scan Title:** belizaire's pen test
- Scan Status:** Completed
- Scan Details:**
  - Policy: Basic Network Scan
  - Status: Completed
  - Severity Base: CVSS v2.0
  - Scanner: Local Scanner
  - Start: Today at 2:49 PM
  - End: Today at 2:49 PM
  - Elapsed: a few seconds
- Vulnerabilities:** 0 (No records found)

## 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.



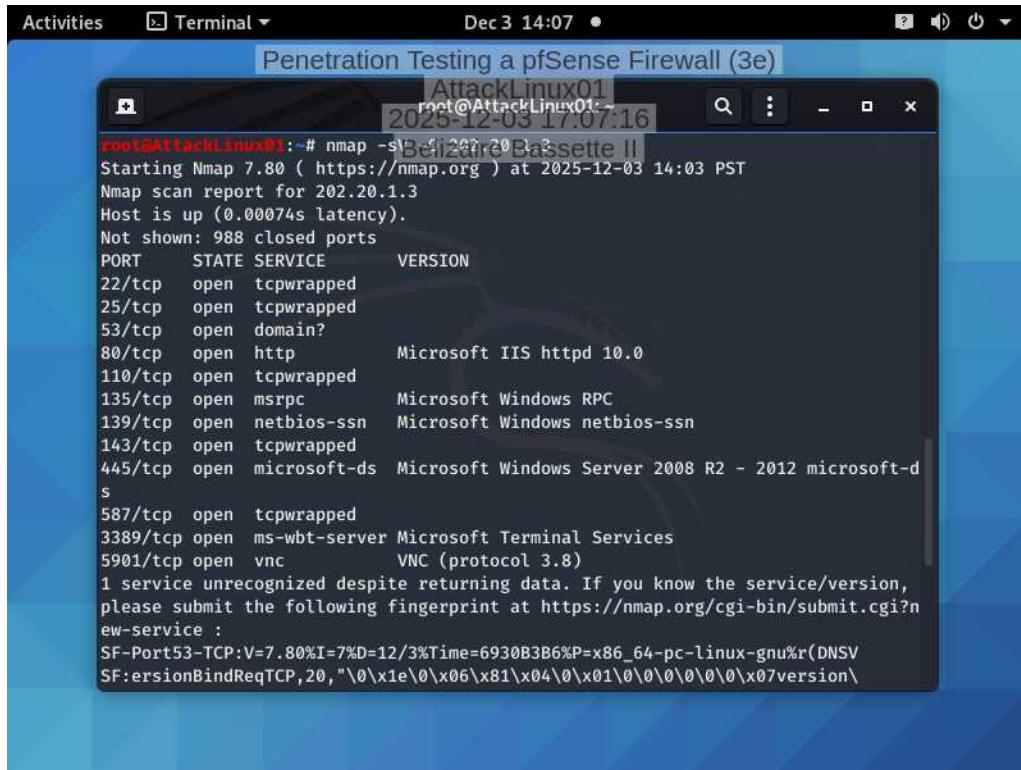
The screenshot shows a terminal window on a Linux desktop environment. The terminal window title is "Penetration Testing a pfSense Firewall (3e)". The terminal content shows the following commands and their output:

```
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=1.61 ms
64 bytes from corporationtechs.com (172.40.0.20): icmp_seq=2 ttl=62 time=0.855 ms
64 bytes from corporationtechs.com (172.40.0.20): icmp_seq=3 ttl=62 time=1.20 ms
64 bytes from corporationtechs.com (172.40.0.20): icmp_seq=4 ttl=62 time=0.858 ms
64 bytes from corporationtechs.com (172.40.0.20): icmp_seq=5 ttl=62 time=0.855 ms
^C
--- corporationtechs.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4035ms
rtt min/avg/max/mdev = 0.855/1.075/1.609/0.298 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)  0.439 ms  0.371 ms  0.297 ms
 2  202.20.1.1 (202.20.1.1)  0.840 ms  0.818 ms  0.828 ms
 3  corporationtechs.com (172.40.0.20)  0.957 ms  0.952 ms  0.947 ms
root@AttackLinux01:~#
```

## Penetration Testing a pfSense Firewall (3e)

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

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



```
root@AttackLinux01:~# nmap -sS -O 202.20.1.3
Starting Nmap 7.80 ( https://nmap.org ) at 2025-12-03 14:03 PST
Nmap scan report for 202.20.1.3
Host is up (0.00074s latency).

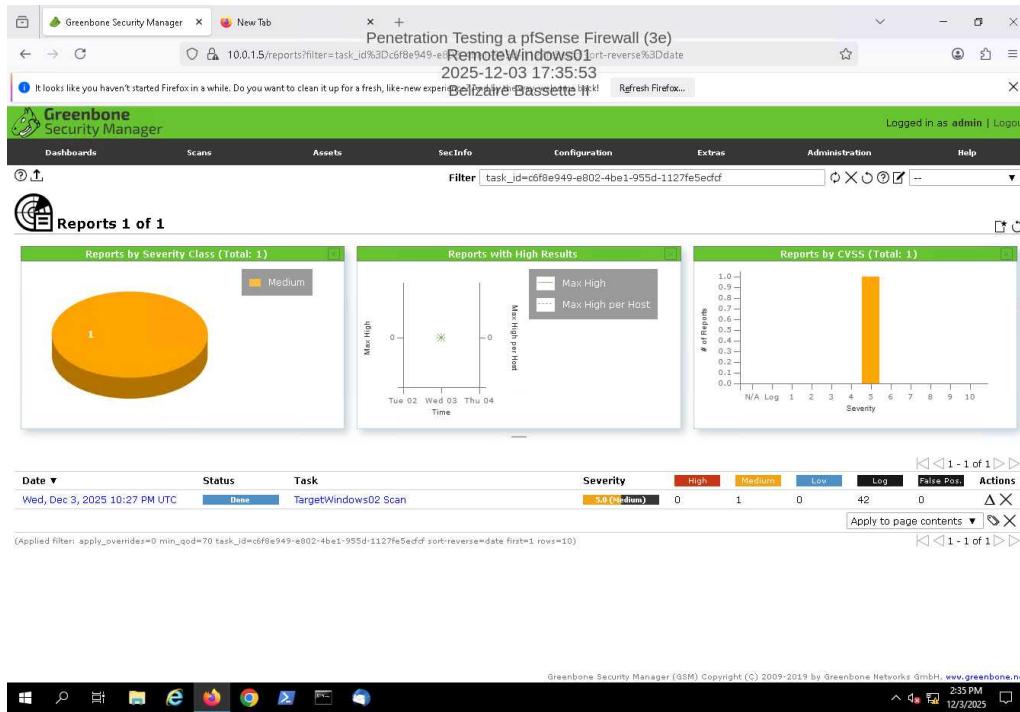
Not shown: 988 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  tcpwrapped
25/tcp    open  tcpwrapped
53/tcp    open  domain?
80/tcp    open  http         Microsoft IIS httpd 10.0
110/tcp   open  tcpwrapped
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
143/tcp   open  tcpwrapped
445/tcp   open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
587/tcp   open  tcpwrapped
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
5901/tcp  open  vnc          VNC (protocol 3.8)
1 service unrecognized despite returning data. If you know the service/version,
please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.80%I=7%D=12/3%Time=6930B3B6%P=x86_64-pc-linux-gnu%r(DNSV
SF:ersi0nBindReqTCP,20,"%0\x1e\0\x06\x81\x04\0\x01\0\0\0\0\0\x07version\
```

## Part 2: Conduct a Vulnerability Scan on the Network

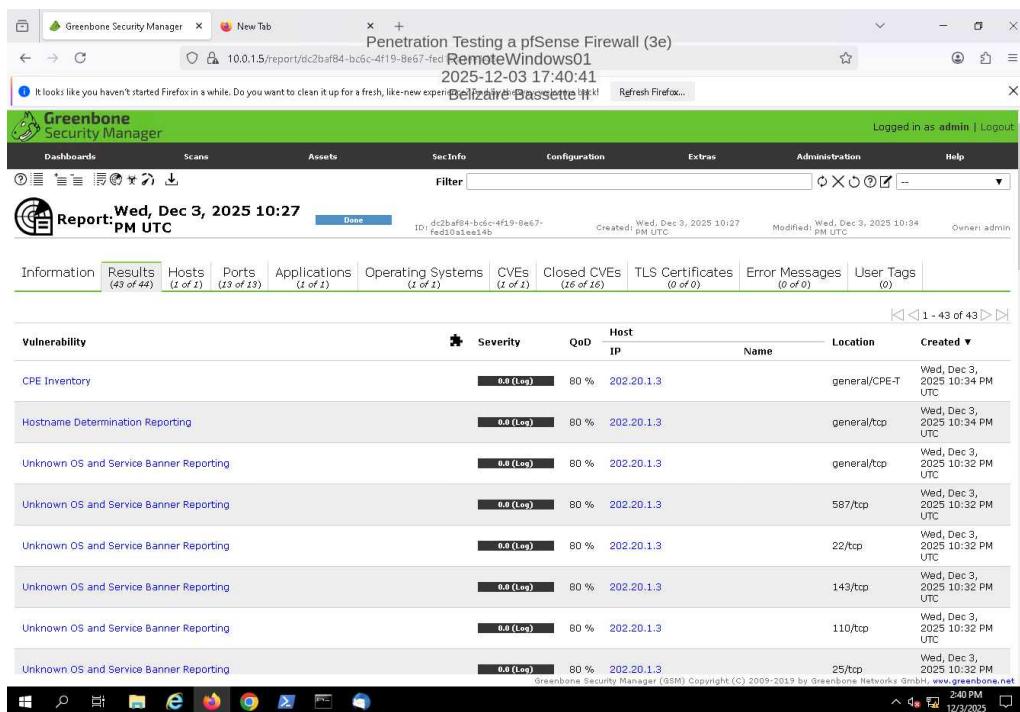
# Penetration Testing a pfSense Firewall (3e)

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

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



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



### 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 Use multiple firewalls (layered security) - use two separate firewalls: one between the Internet -> DMZ- One between the DMZ -> internal network

#2 Strict, Minimal Access Rules Inbound: Allow only required ports (ex: HTTP/HTTPS for a web server)

Outbound: Restrict DMZ servers so they cannot initiate arbitrary connections

East/West: Limit DMZ server-to-server communication  
Why: Reduces the attack surface and prevents lateral movement.

#3 Continuous Monitoring and Logging

DMZ systems are exposed to the internet and they must be heavily monitored.

Implement:

IDS/IPS

SIEM log forwarding

Real-time alerting

Vulnerability scans and patching

Benefit: You detect attacks early and reduce the chance of unnoticed breaches.

A Common Mistake/Vulnerability — Overtrusting the DMZ (Too Much Internal Access)

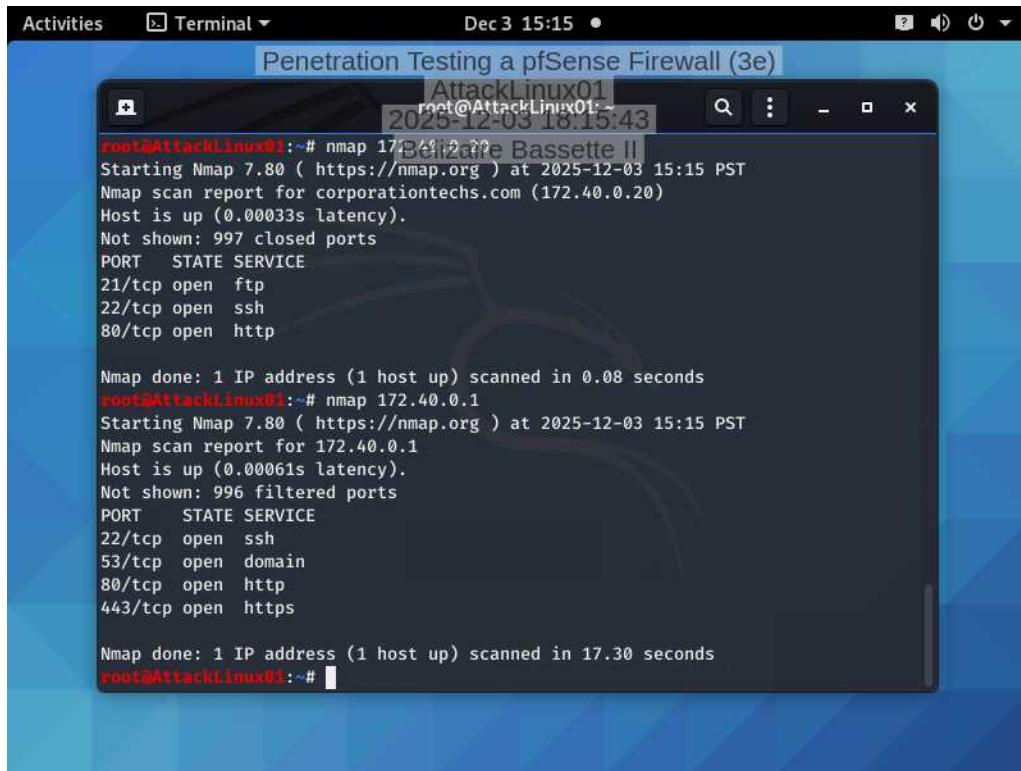
The biggest mistake: Allowing DMZ systems to directly access internal networks or sensitive databases.

#### Part 2: Conduct a Penetration Test on the DMZ

## Penetration Testing a pfSense Firewall (3e)

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

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



The screenshot shows a terminal window titled "Penetration Testing a pfSense Firewall (3e)" running on "AttackLinux01". The terminal displays two Nmap scan sessions. The first session scans the IP 172.40.0.20 (corporationtechs.com) and finds open ports 21/tcp (FTP), 22/tcp (SSH), and 80/tcp (HTTP). The second session scans the IP 172.40.0.1 (DMZ interface) and finds open ports 22/tcp (SSH), 53/tcp (DNS), 80/tcp (HTTP), and 443/tcp (HTTPS). Both scans were completed in under 18 seconds.

```
root@AttackLinux01:~# nmap 172.40.0.20 Basette II
Starting Nmap 7.80 ( https://nmap.org ) at 2025-12-03 15:15 PST
Nmap scan report for corporationtechs.com (172.40.0.20)
Host is up (0.00033s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http

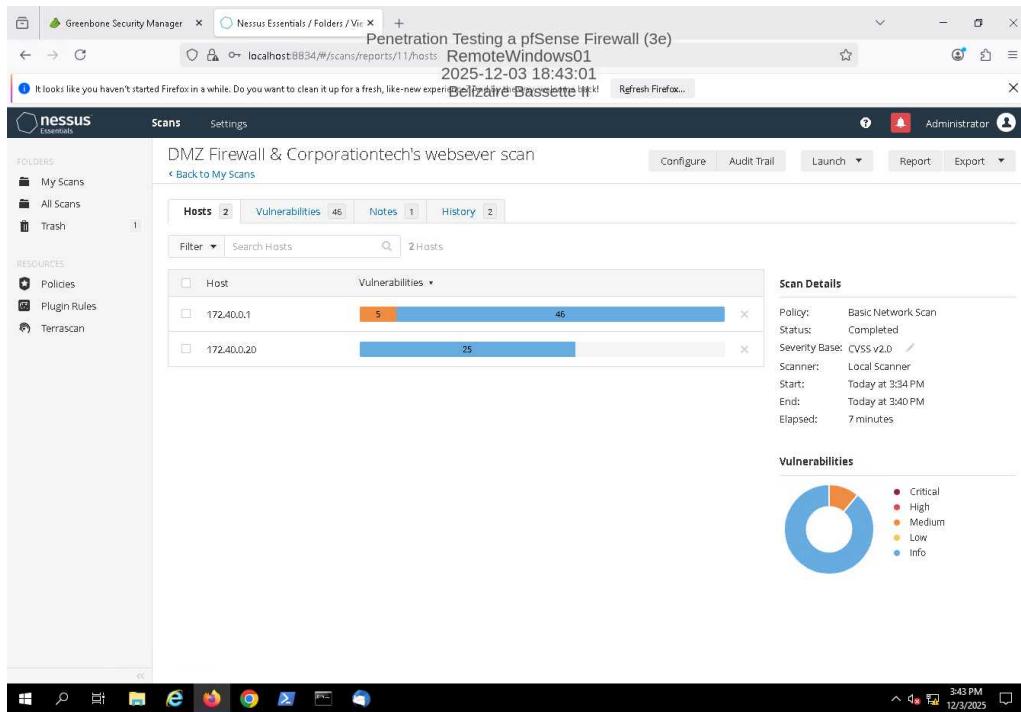
Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
root@AttackLinux01:~# nmap 172.40.0.1
Starting Nmap 7.80 ( https://nmap.org ) at 2025-12-03 15:15 PST
Nmap scan report for 172.40.0.1
Host is up (0.00061s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 17.30 seconds
root@AttackLinux01:~#
```

# Penetration Testing a pfSense Firewall (3e)

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

Make a screen capture showing the vulnerability scan results.



## 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.

Strict, Minimal Access Rules

Only allow exactly what's needed — nothing more.

Rules should be:

Inbound: Allow only required ports (ex: HTTP/HTTPS for a web server)

Outbound: Restrict DMZ servers so they cannot initiate arbitrary connections

East/West: Limit DMZ server-to-server communication