

Penetration Testing a pfSense Firewall (3e)

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

Student:

Saliman Zadran

Email:

sz2740@email.vccs.edu

Time on Task:

4 hours, 12 minutes

Progress:

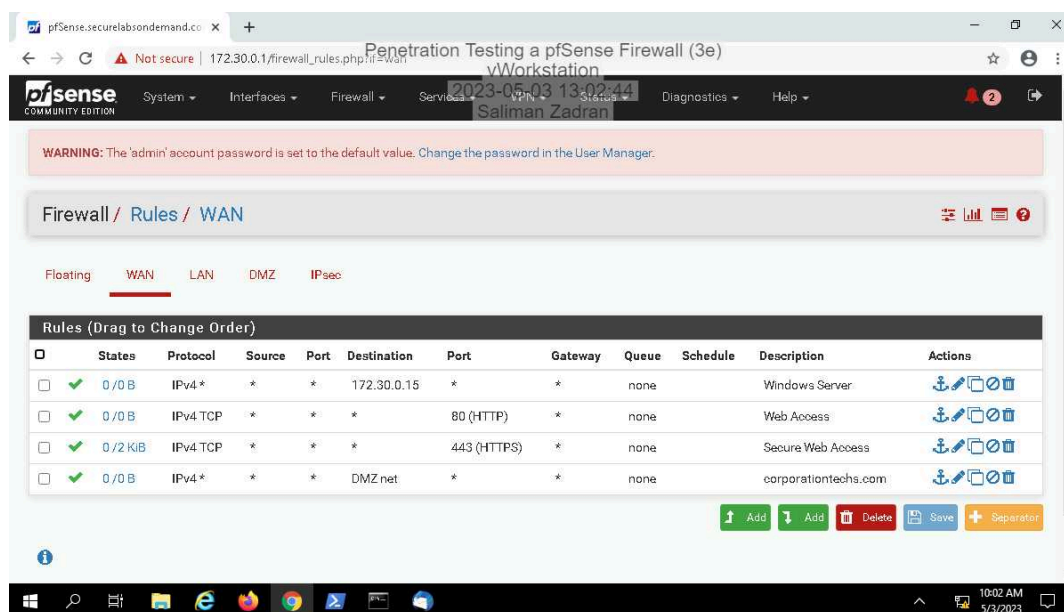
100%

Report Generated: Wednesday, May 3, 2023 at 2:56 PM

Section 1: Hands-On Demonstration

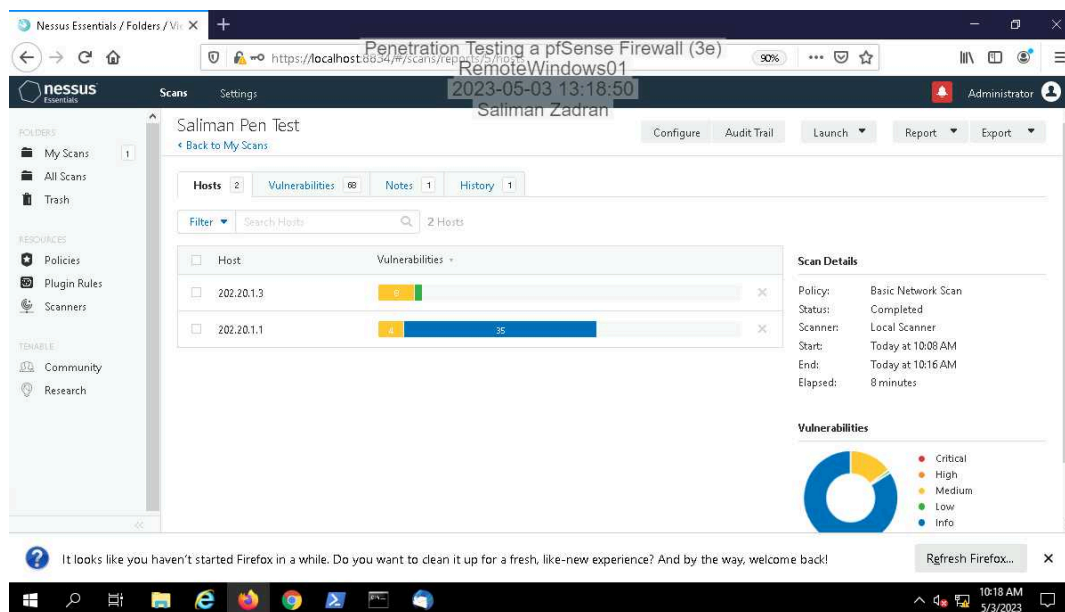
Part 1: Examine a pfSense Firewall Configuration

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

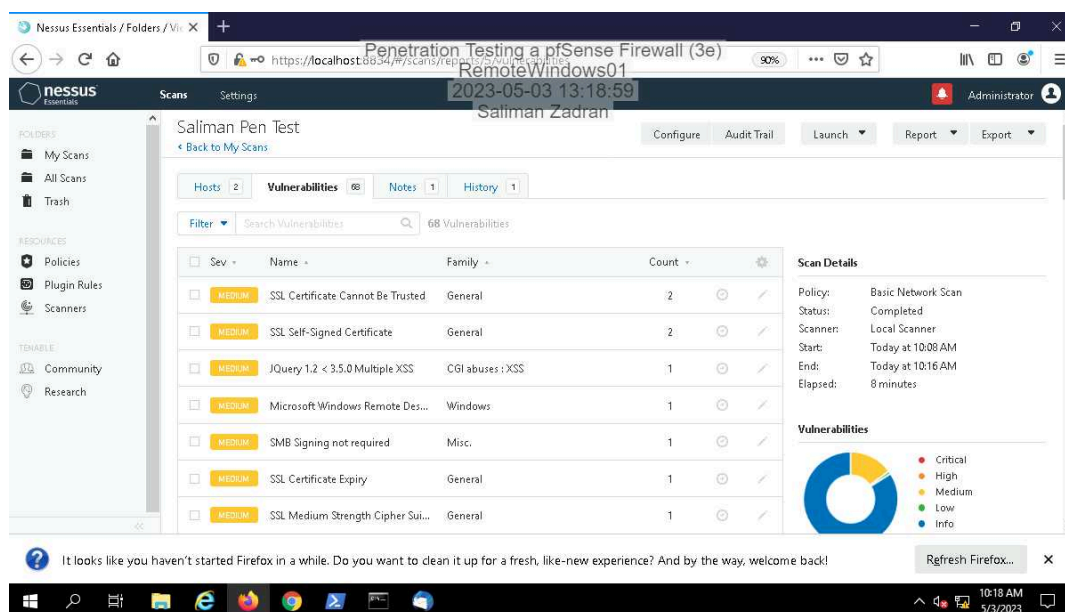


Part 2: Conduct a Penetration Test on the Network

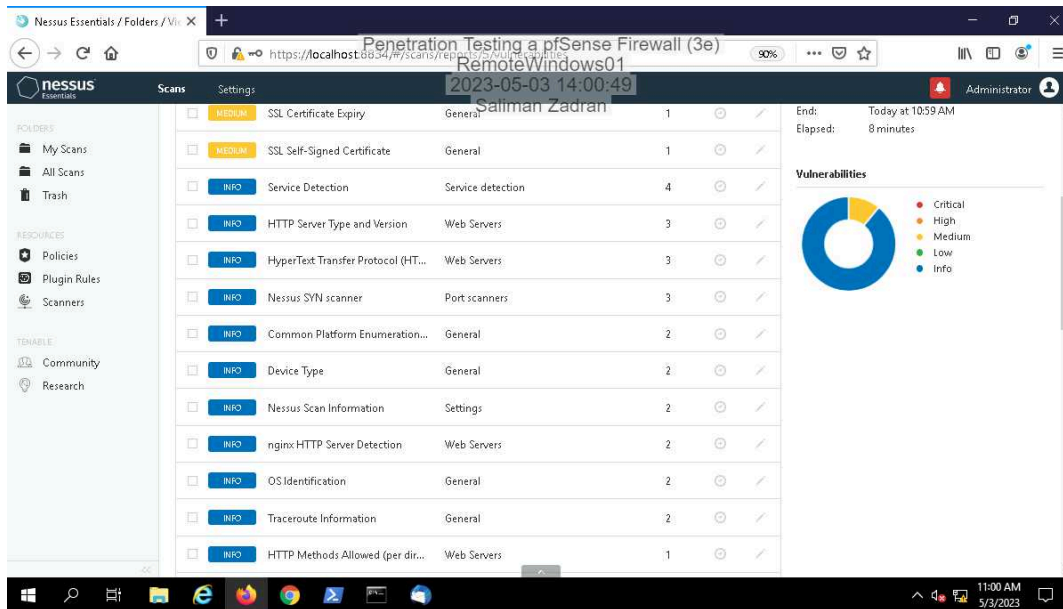
11. Make a screen capture showing the *yourname* pen test scan results.



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



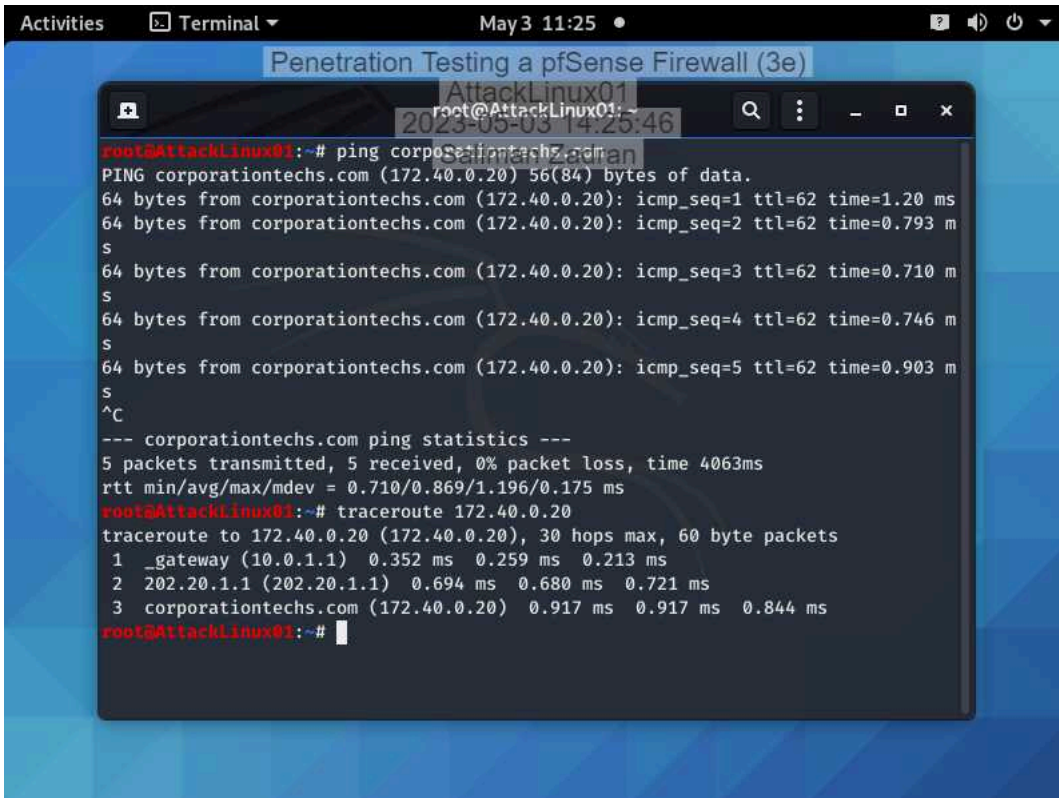
30. Make a screen capture showing the **updated vulnerability report summary**.



Section 2: Applied Learning

Part 1: Conduct a Port Scan on the Network

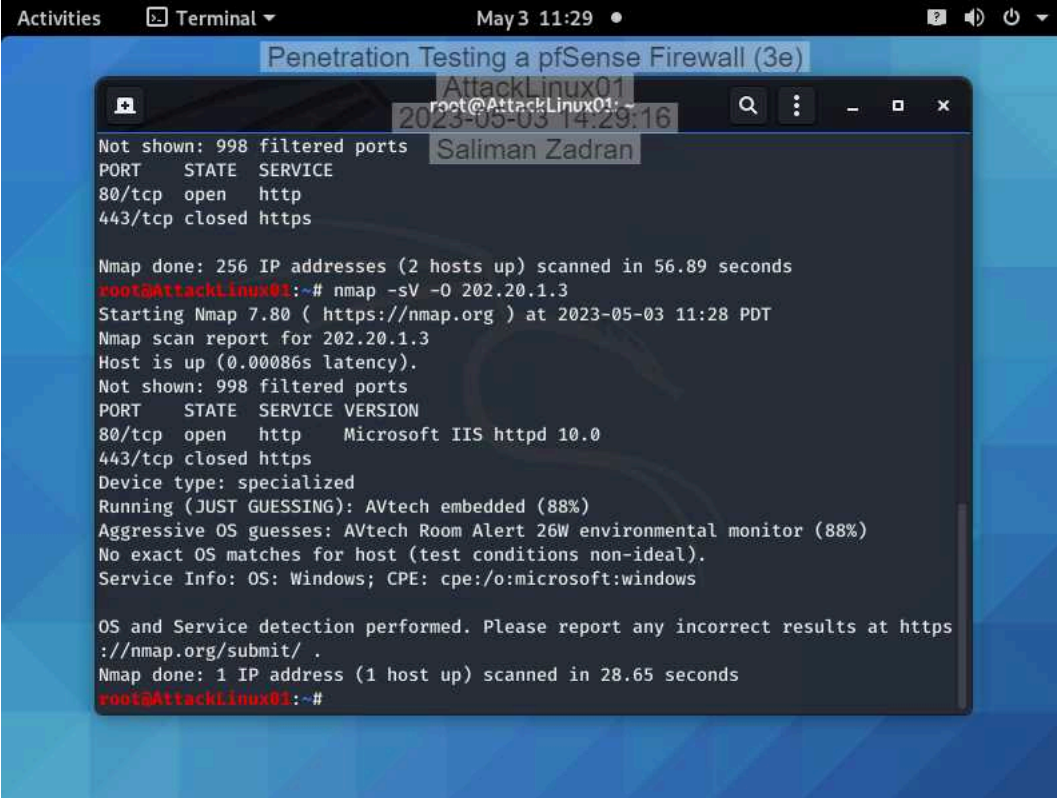
7. Make a screen capture showing the results of the traceroute command.



The screenshot shows a terminal window titled "Penetration Testing a pfSense Firewall (3e)" with a subtitle "AttackLinux01". The terminal output shows a ping command to corporationtechs.com (172.40.0.20) and a subsequent traceroute to the same IP. The ping results show 5 successful packets with varying times. The traceroute shows 3 hops: gateway (10.0.1.1), 202.20.1.1, and corporationtechs.com (172.40.0.20).

```
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=1.20 ms
64 bytes from corporationtechs.com (172.40.0.20): icmp_seq=2 ttl=62 time=0.793 ms
64 bytes from corporationtechs.com (172.40.0.20): icmp_seq=3 ttl=62 time=0.710 ms
64 bytes from corporationtechs.com (172.40.0.20): icmp_seq=4 ttl=62 time=0.746 ms
64 bytes from corporationtechs.com (172.40.0.20): icmp_seq=5 ttl=62 time=0.903 ms
^C
--- corporationtechs.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4063ms
rtt min/avg/max/mdev = 0.710/0.869/1.196/0.175 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) 0.352 ms 0.259 ms 0.213 ms
 2 202.20.1.1 (202.20.1.1) 0.694 ms 0.680 ms 0.721 ms
 3 corporationtechs.com (172.40.0.20) 0.917 ms 0.917 ms 0.844 ms
root@AttackLinux01:~#
```

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



A terminal window titled "Penetration Testing a pfSense Firewall (3e)" showing the output of an nmap scan. The window has a title bar with "Activities", "Terminal", and a clock showing "May 3 11:29". The terminal output is as follows:

```
root@AttackLinux01:~# nmap -sV -O 202.20.1.3
Starting Nmap 7.80 ( https://nmap.org ) at 2023-05-03 11:28 PDT
Nmap scan report for 202.20.1.3
Host is up (0.00086s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   closed https

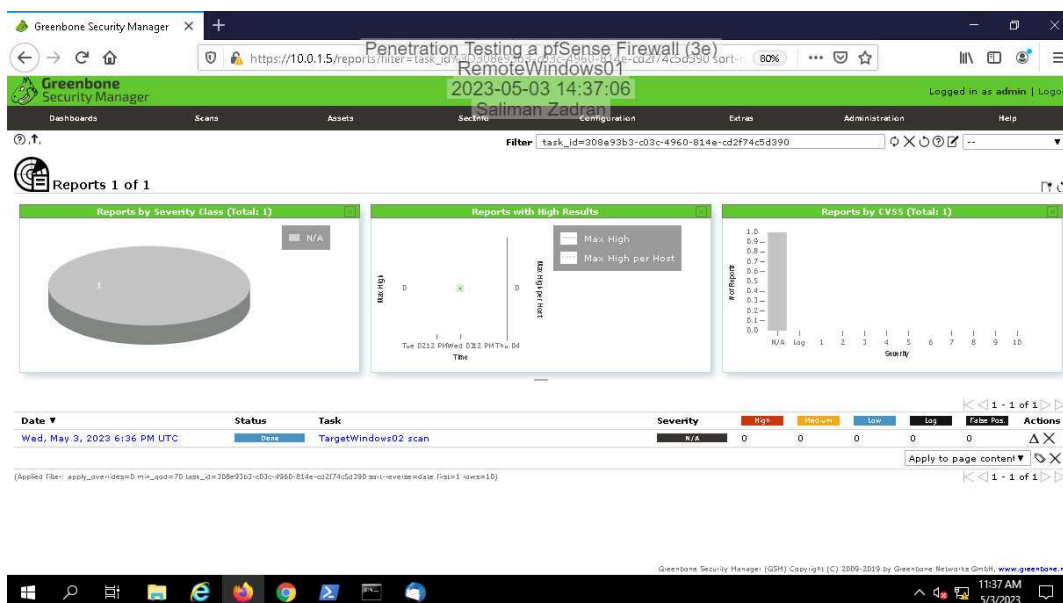
Nmap done: 256 IP addresses (2 hosts up) scanned in 56.89 seconds
root@AttackLinux01:~# nmap -sV -O 202.20.1.3
Starting Nmap 7.80 ( https://nmap.org ) at 2023-05-03 11:28 PDT
Nmap scan report for 202.20.1.3
Host is up (0.00086s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http      Microsoft IIS httpd 10.0
443/tcp   closed https

Device type: specialized
Running (JUST GUESSING): AVtech embedded (88%)
Aggressive OS guesses: AVtech Room Alert 26W environmental monitor (88%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

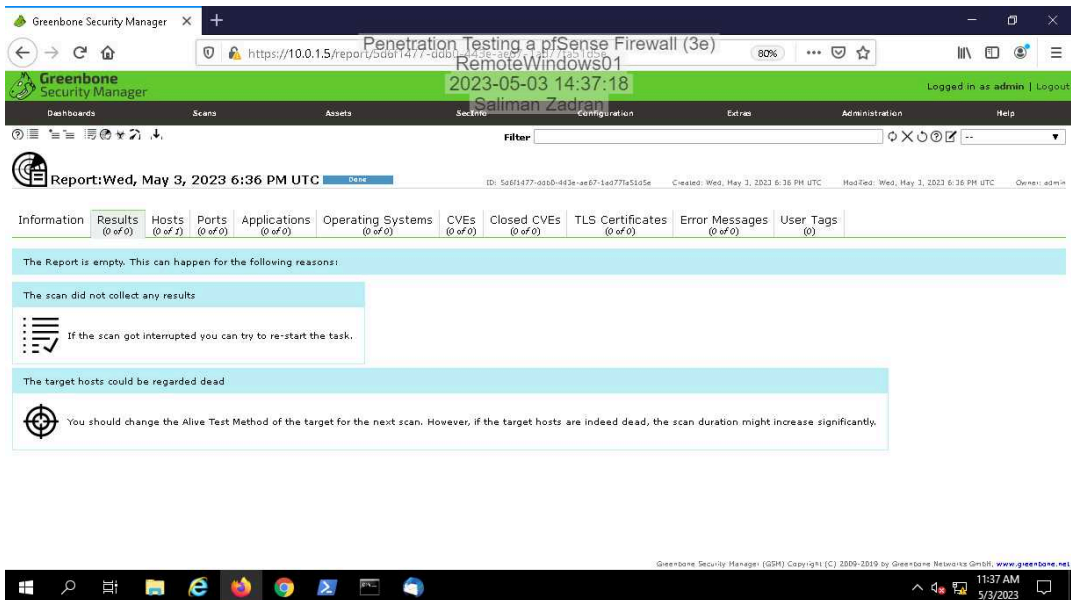
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.65 seconds
root@AttackLinux01:~#
```

Part 2: Conduct a Vulnerability Scan on the Network

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

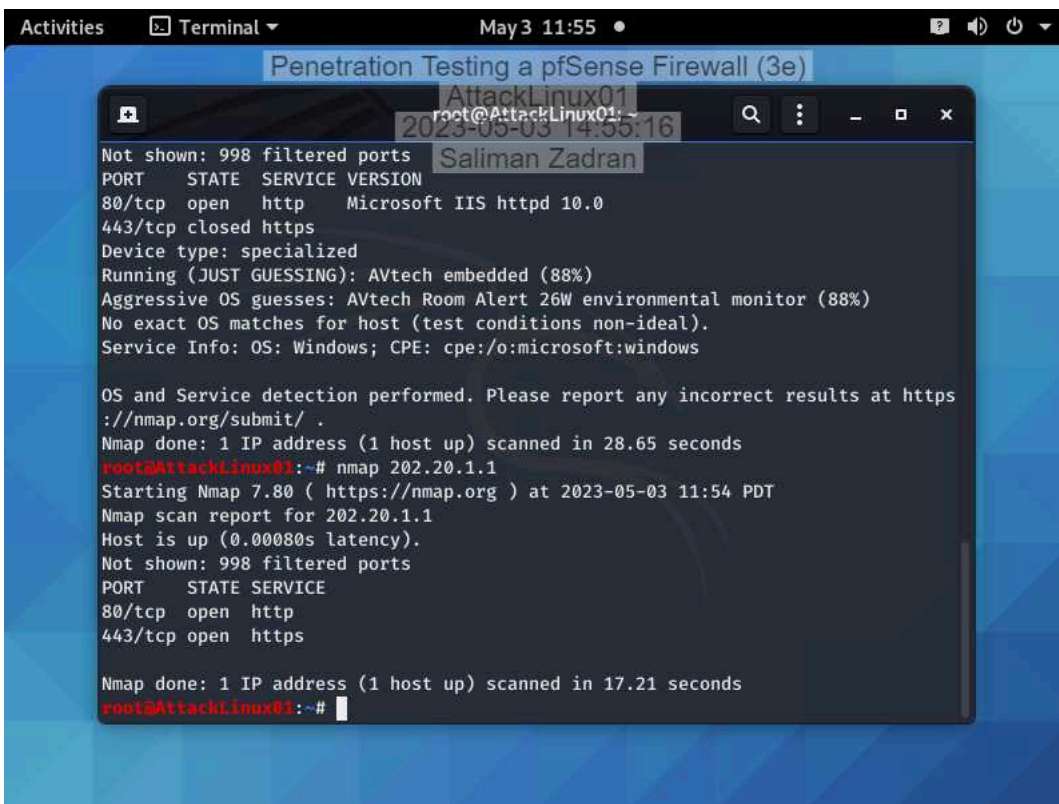
Part 1: Research DMZ Deployment Best Practices

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.

Three best practices include: Hardening and isolating service console, clearly labeling each zone within the DMZ, and regular auditing of the configuration. A mistake would be not auditing the configuration regularly.

Part 2: Conduct a Penetration Test on the DMZ

Make a screen capture showing the open ports on TargetLinux01 and the DMZ firewall interface.



```
Activities Terminal May 3 11:55
Penetration Testing a pfSense Firewall (3e)
AttackLinux01
root@AttackLinux01:~#
2023-05-03 14:55:16
Saliman Zadrar

Not shown: 998 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http   Microsoft IIS httpd 10.0
443/tcp   closed https
Device type: specialized
Running (JUST GUESSING): AVtech embedded (88%)
Aggressive OS guesses: AVtech Room Alert 26W environmental monitor (88%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

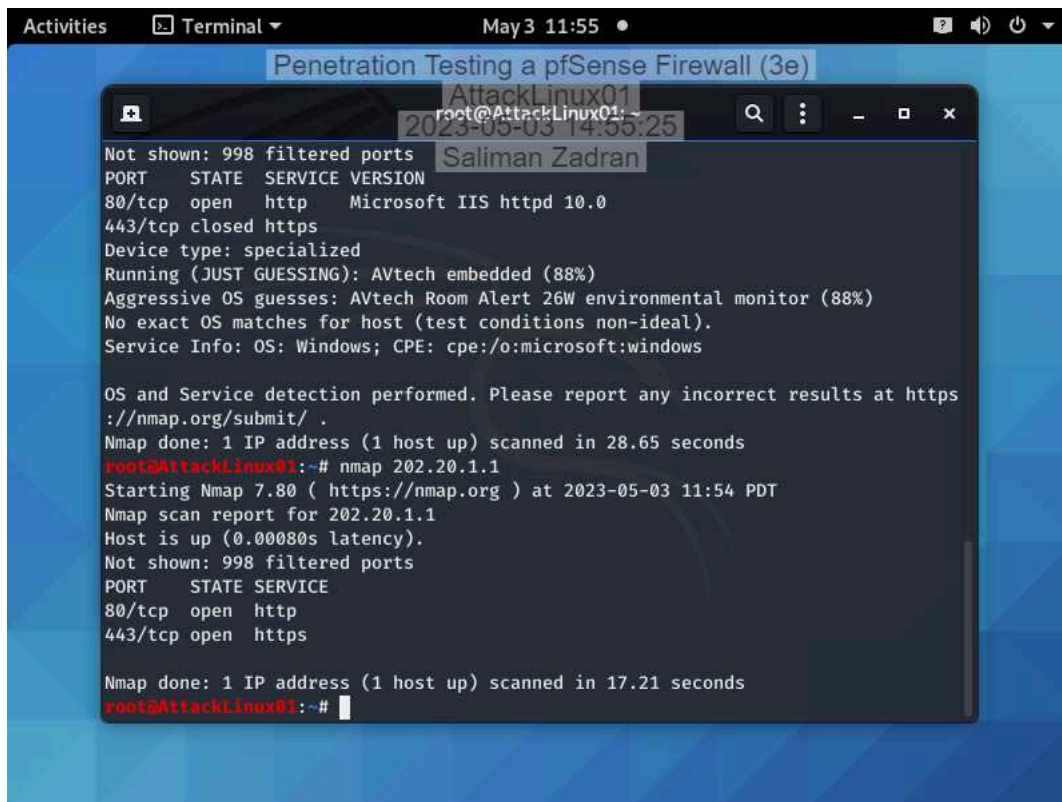
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.65 seconds
root@AttackLinux01:~# nmap 202.20.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2023-05-03 11:54 PDT
Nmap scan report for 202.20.1.1
Host is up (0.00080s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 17.21 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**.



```
Activities Terminal May 3 11:55
Penetration Testing a pfSense Firewall (3e)
AttackLinux01
root@AttackLinux01:~# nmap 202.20.1.1
2023-05-03 14:55:25
Saliman Zadran
Not shown: 998 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http   Microsoft IIS httpd 10.0
443/tcp   closed https
Device type: specialized
Running (JUST GUESSING): AVtech embedded (88%)
Aggressive OS guesses: AVtech Room Alert 26W environmental monitor (88%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.65 seconds
root@AttackLinux01:~# nmap 202.20.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2023-05-03 11:54 PDT
Nmap scan report for 202.20.1.1
Host is up (0.00080s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 17.21 seconds
root@AttackLinux01:~#
```

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.

Unnecessary ports should be closed, ICMP ping requests need to be locked as well. Discoverability of hosts is too easy.