

# Penetration Testing a pfSense Firewall (3e)

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

Student:

Christian Barba

Email:

christianbarba527@gmail.com

Time on Task:

14 hours, 38 minutes

Progress:

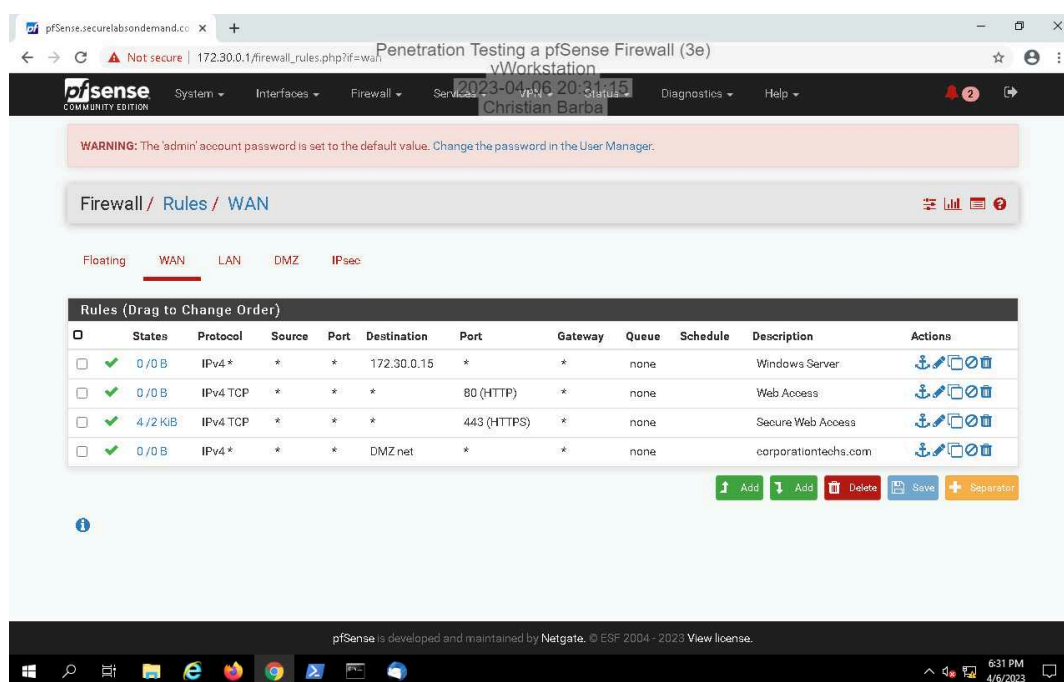
100%

Report Generated: Monday, April 10, 2023 at 5:33 PM

## Section 1: Hands-On Demonstration

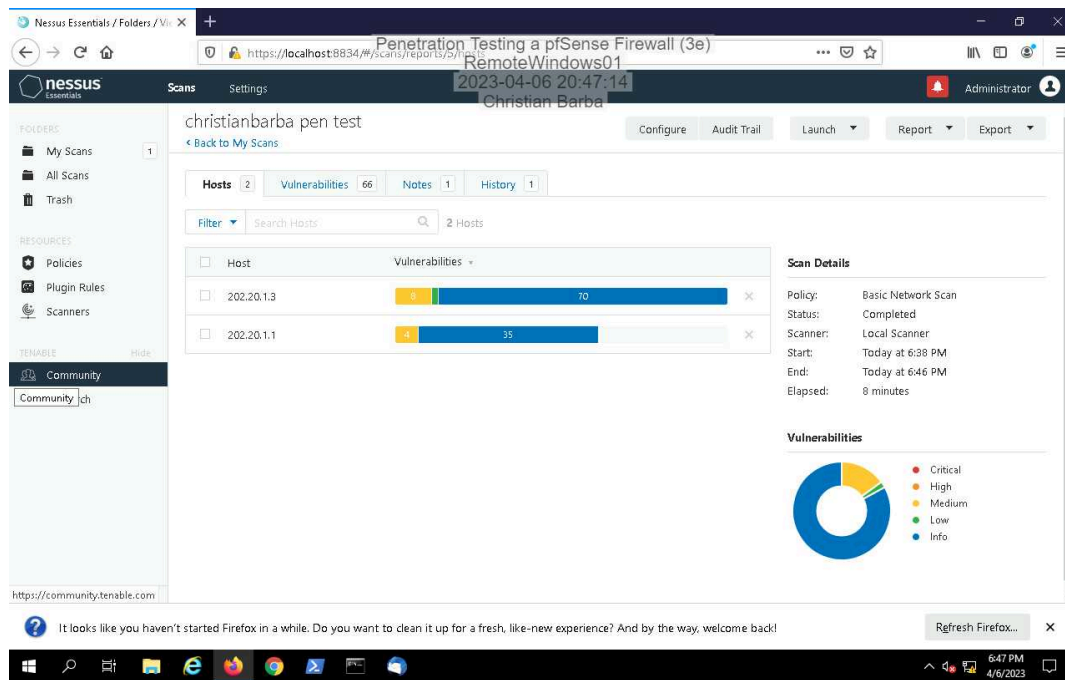
### Part 1: Examine a pfSense Firewall Configuration

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

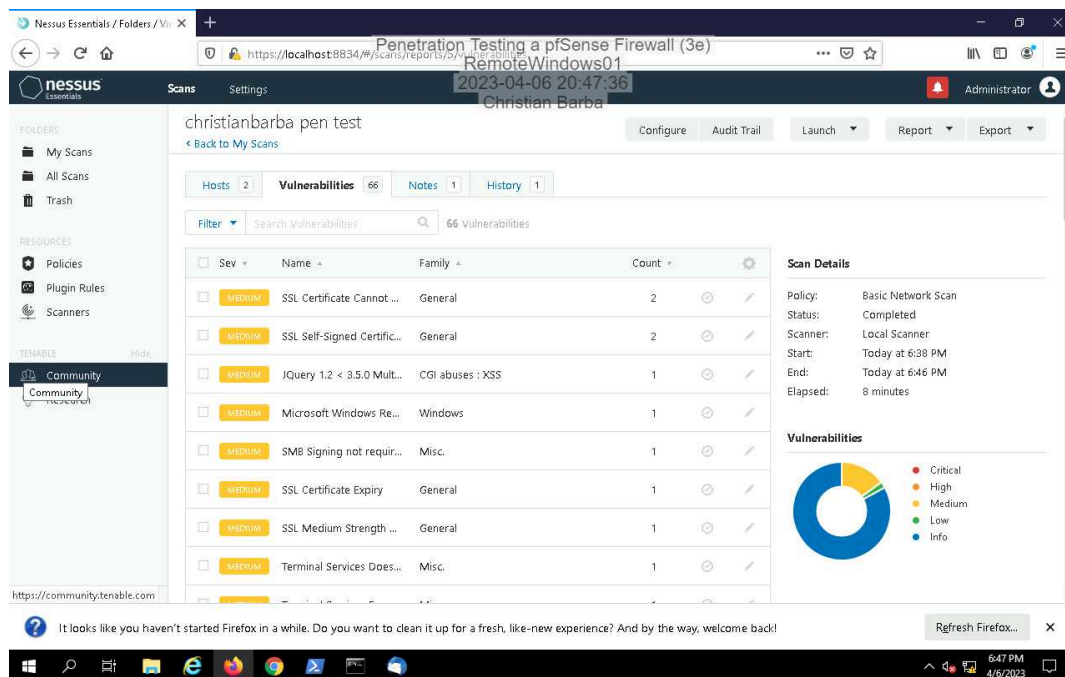


### Part 2: Conduct a Penetration Test on the Network

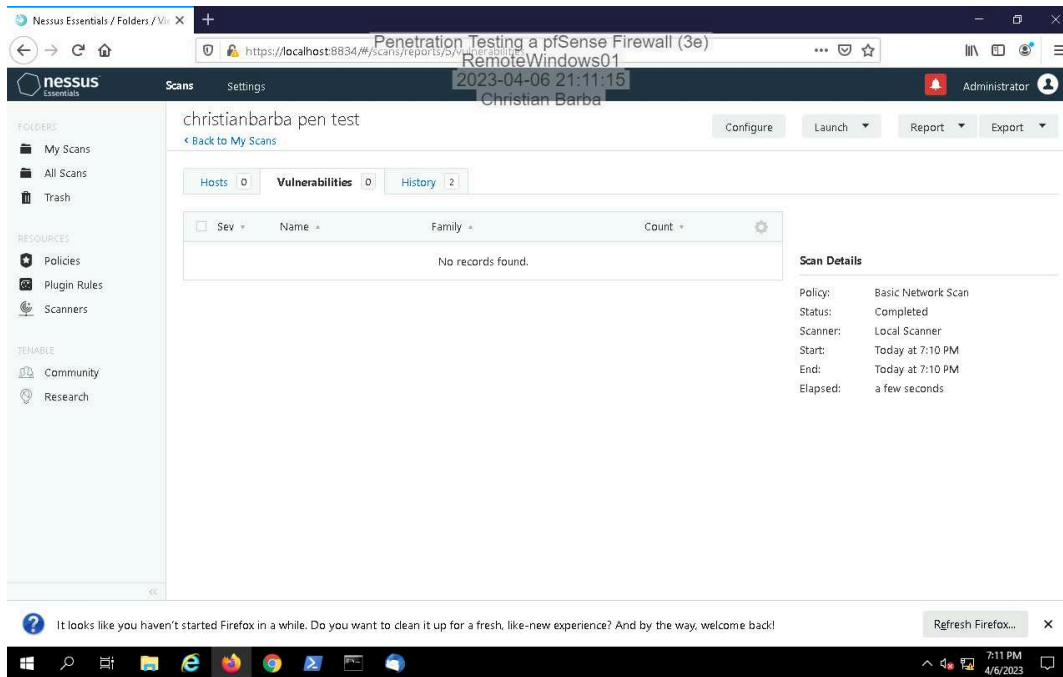
## 11. Make a screen capture showing the *yourname* pen test scan results.



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



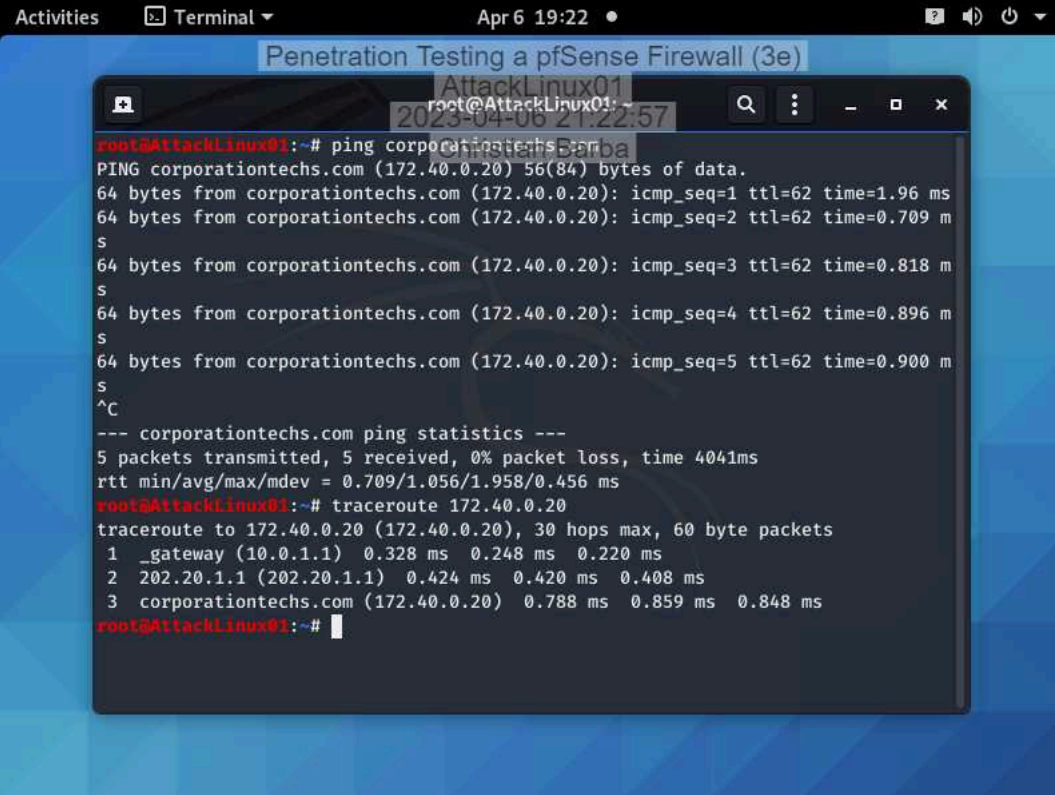
## 30. Make a screen capture showing the updated vulnerability report summary.



## Section 2: Applied Learning

### Part 1: Conduct a Port Scan on the Network

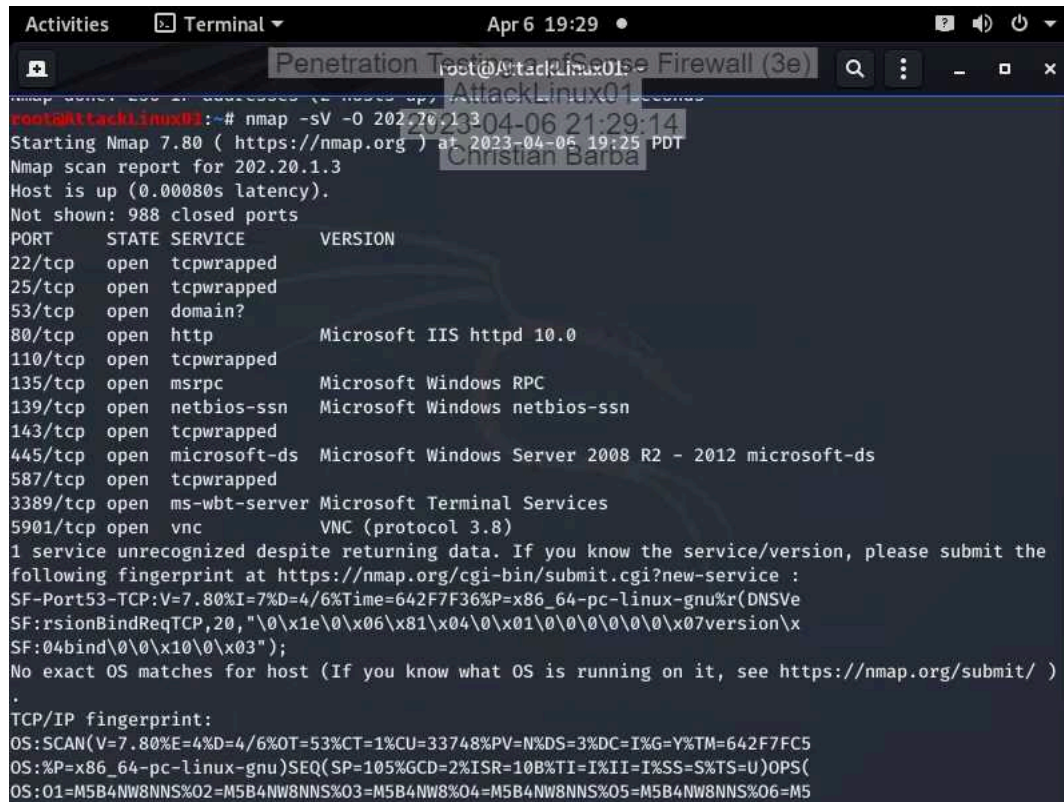
7. Make a screen capture showing the results of the traceroute command.



The screenshot shows a terminal window titled "Penetration Testing a pfSense Firewall (3e)" with a subtitle "AttackLinux01". The terminal output shows a successful ping to corporationtechs.com (172.40.0.20) and a traceroute to the same destination. The traceroute shows three hops: a gateway at 10.0.1.1, an intermediate hop at 202.20.1.1, and the destination at 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=1.96 ms
64 bytes from corporationtechs.com (172.40.0.20): icmp_seq=2 ttl=62 time=0.709 ms
64 bytes from corporationtechs.com (172.40.0.20): icmp_seq=3 ttl=62 time=0.818 ms
64 bytes from corporationtechs.com (172.40.0.20): icmp_seq=4 ttl=62 time=0.896 ms
64 bytes from corporationtechs.com (172.40.0.20): icmp_seq=5 ttl=62 time=0.900 ms
^C
--- corporationtechs.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4041ms
rtt min/avg/max/mdev = 0.709/1.056/1.958/0.456 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) 0.328 ms 0.248 ms 0.220 ms
 2 202.20.1.1 (202.20.1.1) 0.424 ms 0.420 ms 0.408 ms
 3 corporationtechs.com (172.40.0.20) 0.788 ms 0.859 ms 0.848 ms
root@AttackLinux01:~#
```

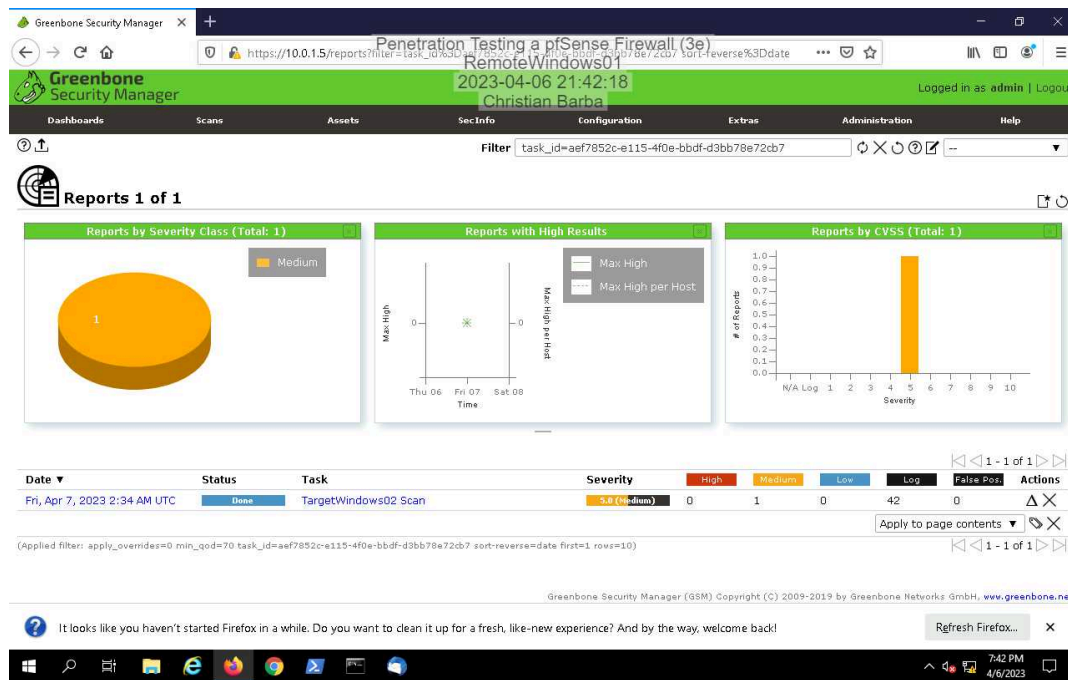
11. Make a screen capture showing the result of the **nmap** scan with OS detection activated.



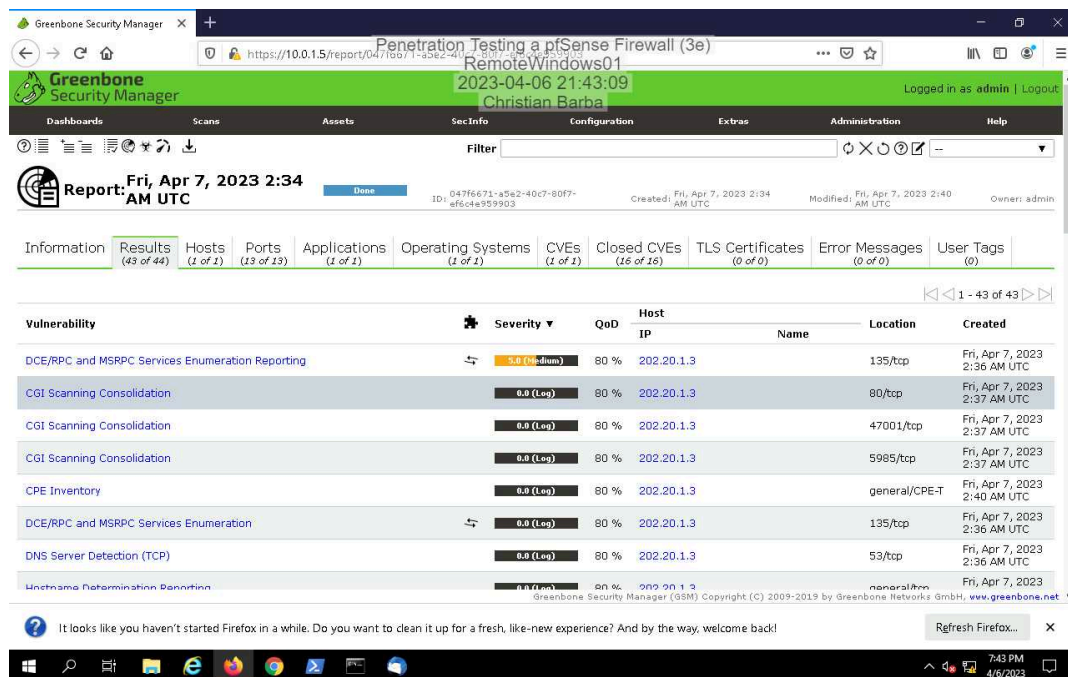
```
root@AttackLinux01:~# nmap -sV -O 202.20.1.3
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-06 19:25 PDT
Nmap scan report for 202.20.1.3
Host is up (0.00080s latency).
Not shown: 988 closed ports
PORT      STATE SERVICE          VERSION
22/tcp    open  tcpwrapped
25/tcp    open  tcpwrapped
53/tcp    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=4/6%T=642F7F36P=x86_64-pc-linux-gnu%r(DNSVe
SF:rsionBindReqTCP,20,"\0\x1e\0\x06\x81\x04\0\x01\0\0\0\0\0\0\x07version\x
SF:04bind\0\0\x10\0\x03");
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ )
.
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=4/6%OT=53%CT=1%CU=33748%PV=N%DS=3%DC=I%G=Y%TM=642F7FC5
OS:%P=x86_64-pc-linux-gnu)SEQ(SP=105%GCD=2%ISR=10B%TI=I%II=I%SS=S%TS=U)OPPS(
OS:O1=M5B4NW8NNS%O2=M5B4NW8NNS%O3=M5B4NW8%O4=M5B4NW8NNS%O5=M5B4NW8NNS%O6=M5
```

## 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.

When using the internet to research more about the DMZ deployments, I came across multiple sources that explained some of the best practices to use. these practices include but are not limited to: enforce separation of duties and ensure that only the specific people that are trusted are the only ones able to monitor the system, make sure that the firewall is isolated, and regularly audit the firewall to ensure the functionality. Firstly, by letting only a few members of the organization monitor the firewall, there are less opportunities for someone to gain unnecessary access to the firewall. Limiting the amount of people with access will limit the accounts that could be hacked into, and there will be a small group of people to look at when things go wrong. Secondly, by isolating the firewall and ensuring there are no backdoors to the company's servers, there will be more complications for the malicious actor to go to in order to try to get on the protected servers. Since the firewall will not directly jump to the servers, there shouldn't be a way a for hackers to figure out the real IP address that the company uses. Lastly, checking the logs and making sure there are no threats will prove that the firewall is actually working. This could also be a potential mistake firewall managers run into because they put too much trust in the firewall to stop everything that gets thrown at it. There must be changes and updates to the firewall when they are needed and the only way to figure this out is to properly monitor it.

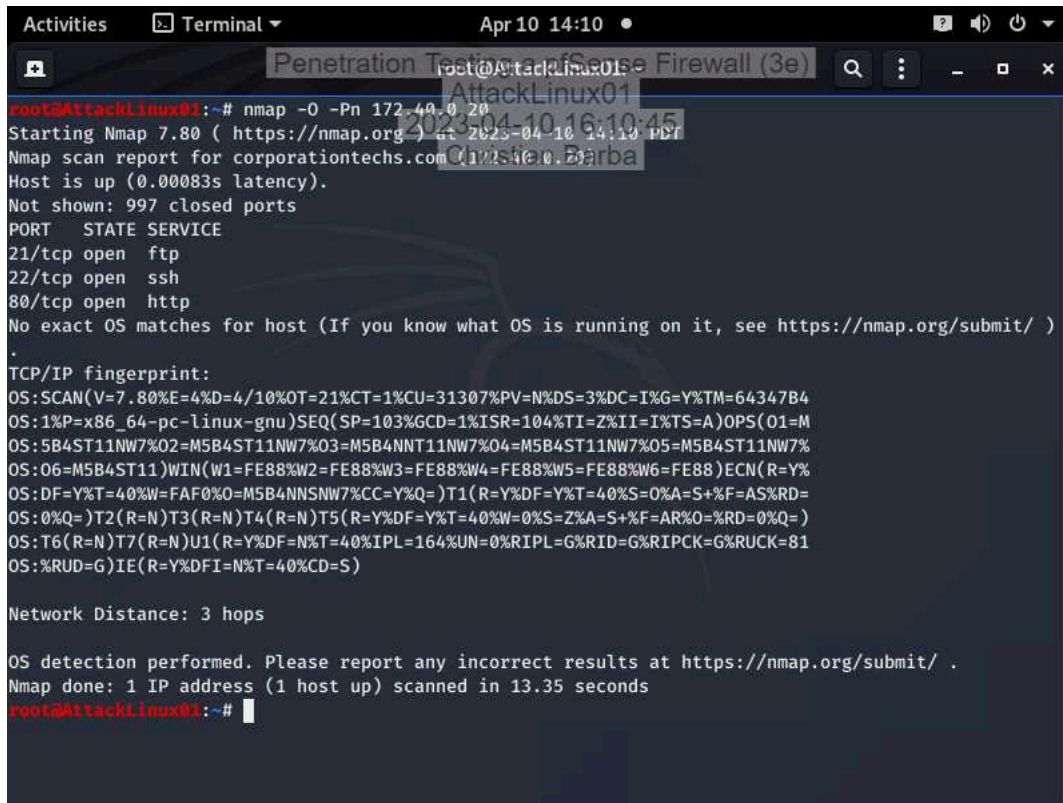
#### Part 2: Conduct a Penetration Test on the DMZ



# Penetration Testing a pfSense Firewall (3e)

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

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

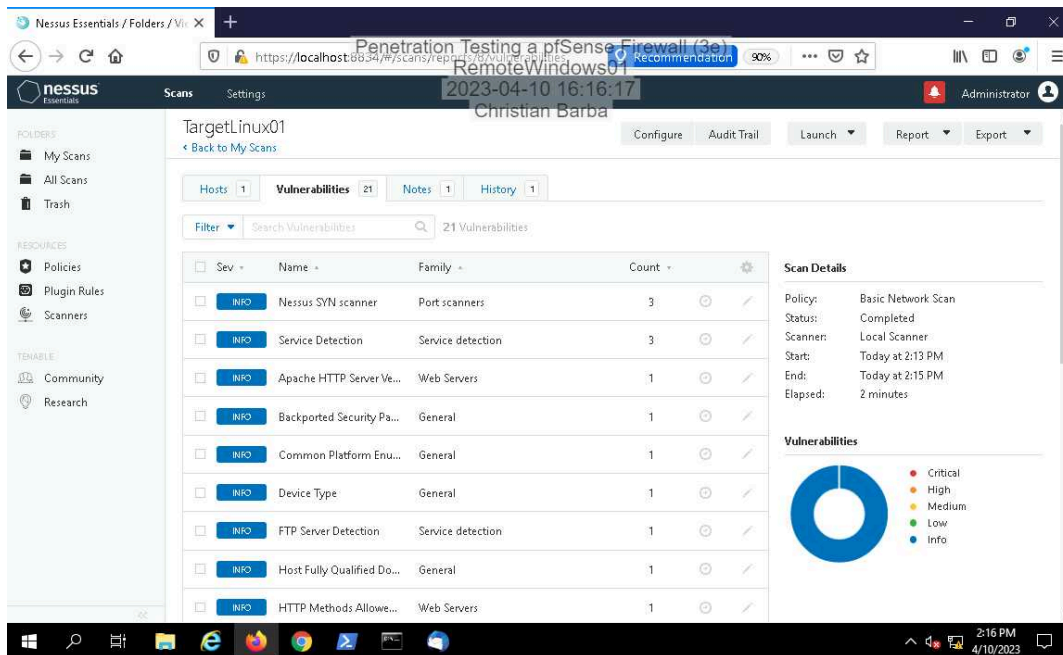


```
root@AttackLinux01:~# nmap -O -Pn 172.40.0.20
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-10 16:10:45
Nmap scan report for corporationtechs.com (172.40.0.20)
Host is up (0.00083s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=4/10%OT=21%CT=1%CU=31307%PV=N%DS=3%DC=I%G=Y%TM=64347B4
OS:1%P=x86_64-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=104%TI=Z%II=I%TS=A)OPS(O1=M
OS:5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O5=M5B4ST11NW7%
OS:06=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN(R=Y%
OS:DF=Y%T=40%W=FAF0%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=
OS:0%Q=)T2(R=N)T3(R=N)T4(R=N)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
OS:T6(R=N)T7(R=N)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=81
OS:%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 3 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.35 seconds
root@AttackLinux01:~#
```

Make a screen capture showing the vulnerability scan results.



Sev	Name	Family	Count
INFO	Nessus SYN scanner	Port scanners	3
INFO	Service Detection	Service detection	3
INFO	Apache HTTP Server Ve...	Web Servers	1
INFO	Backported Security Pa...	General	1
INFO	Common Platform Enu...	General	1
INFO	Device Type	General	1
INFO	FTP Server Detection	Service detection	1
INFO	Host Fully Qualified Do...	General	1
INFO	HTTP Methods Allowe...	Web Servers	1

**Scan Details**

Policy: Basic Network Scan  
Status: Completed  
Scanner: Local Scanner  
Start: Today at 2:13 PM  
End: Today at 2:15 PM  
Elapsed: 2 minutes

**Vulnerabilities**

Donut chart showing vulnerability distribution: Critical (red), High (orange), Medium (yellow), Low (green), Info (blue).



### 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.

By using both nmap on the AttackLinux01 machine and Nessus on the RemoteWindows01 computer, I was able to witness a few vulnerabilities. These vulnerabilities were dealing with open ports and some outdated software. The open ports that were listed happened to be ports 21 (FTP), 22 (SSH), and port 80(HTTP). These ports are highly dangerous to have open because people would be able to attack file transfers and upload and/or steal information that others are sharing through this port. Port 22 is also dangerous because this has to deal with remote access for a machine, so if this port gets exploited, someone could gain full access to this vulnerable computer. Finally port 80 is a port that malicious actors could still use to access data that a host computer may hold. Also, Nessus shows that there are servers that are using these ports to function. My recommendations would be to patch up these ports as they are dangerous to have open, and they should check the firewall logs to see who has been interacting on these ports as well. The administrators should also close these servers only to those that should be allowed to have access to them. Leaving them open is irresponsible and dangerous because hackers could come and tinker with whatever they can find through these open ports. As far as the outdated and misconfigured software goes, the admin of the servers should ensure that the passwords are mandatory and up to date with patches that could be available to ensure security.