

Penetration Testing a pfSense Firewall (3e)

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

Student:	Email:
Dillen Dela Cruz	dillen.delacruz@my.utsa.edu

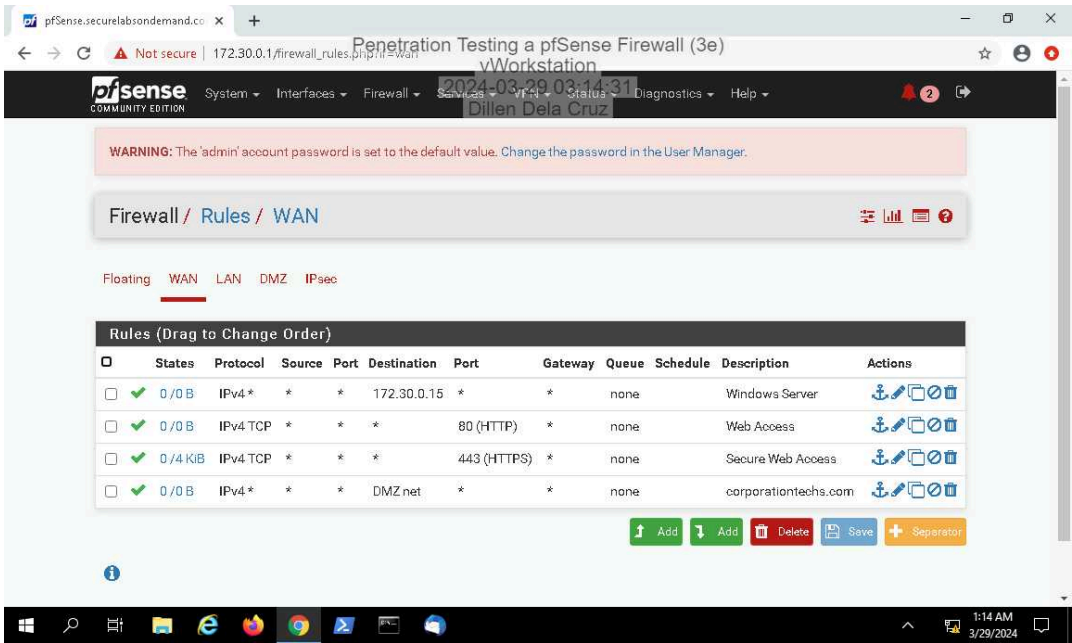
Time on Task:	Progress:
12 hours, 32 minutes	100%

Report Generated: Saturday, March 30, 2024 at 1:38 AM

Section 1: Hands-On Demonstration

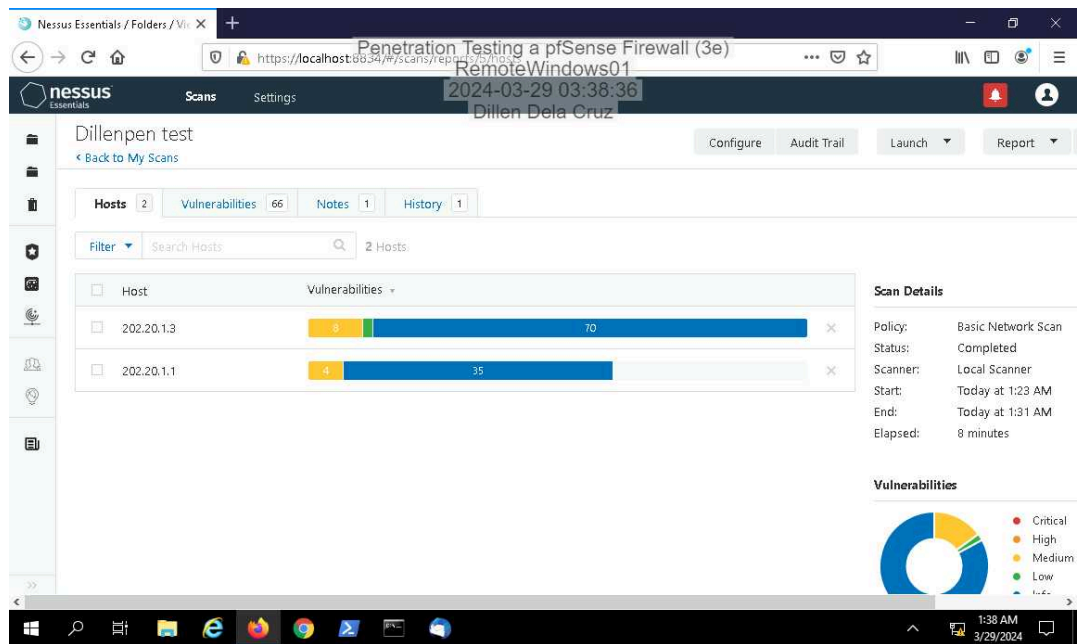
Part 1: Examine a pfSense Firewall Configuration

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

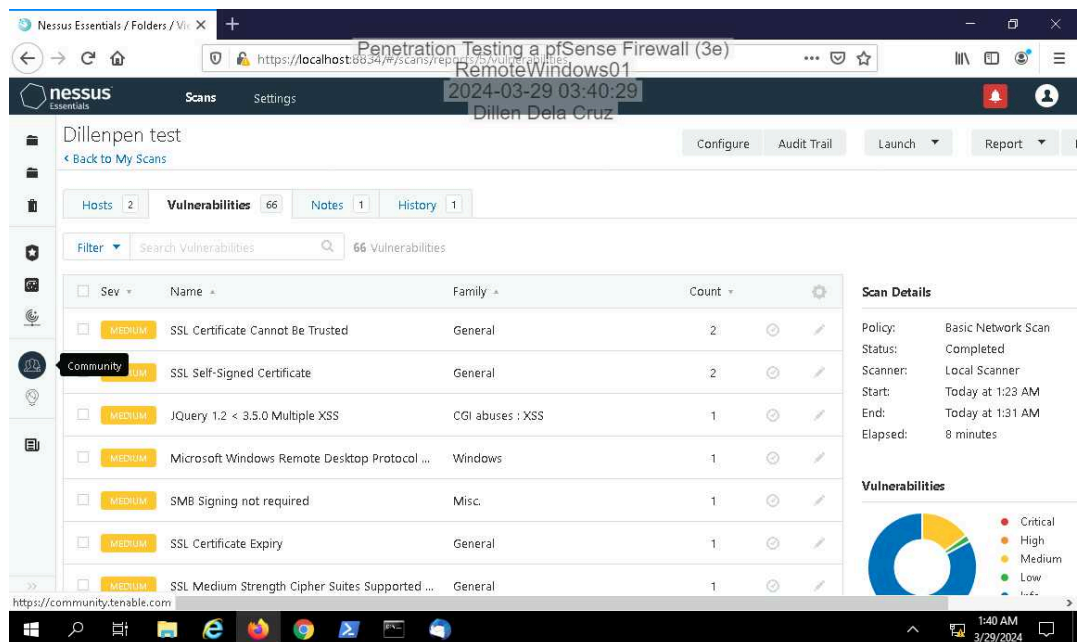


Part 2: Conduct a Penetration Test on the Network

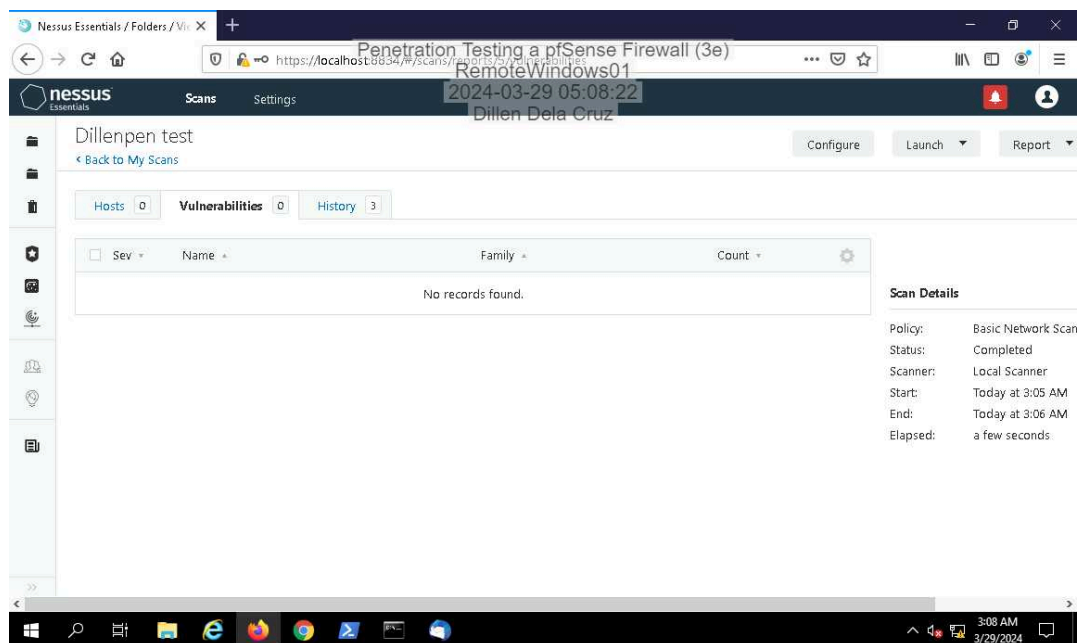
11. Make a screen capture showing the *yourname* pen test scan results.



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



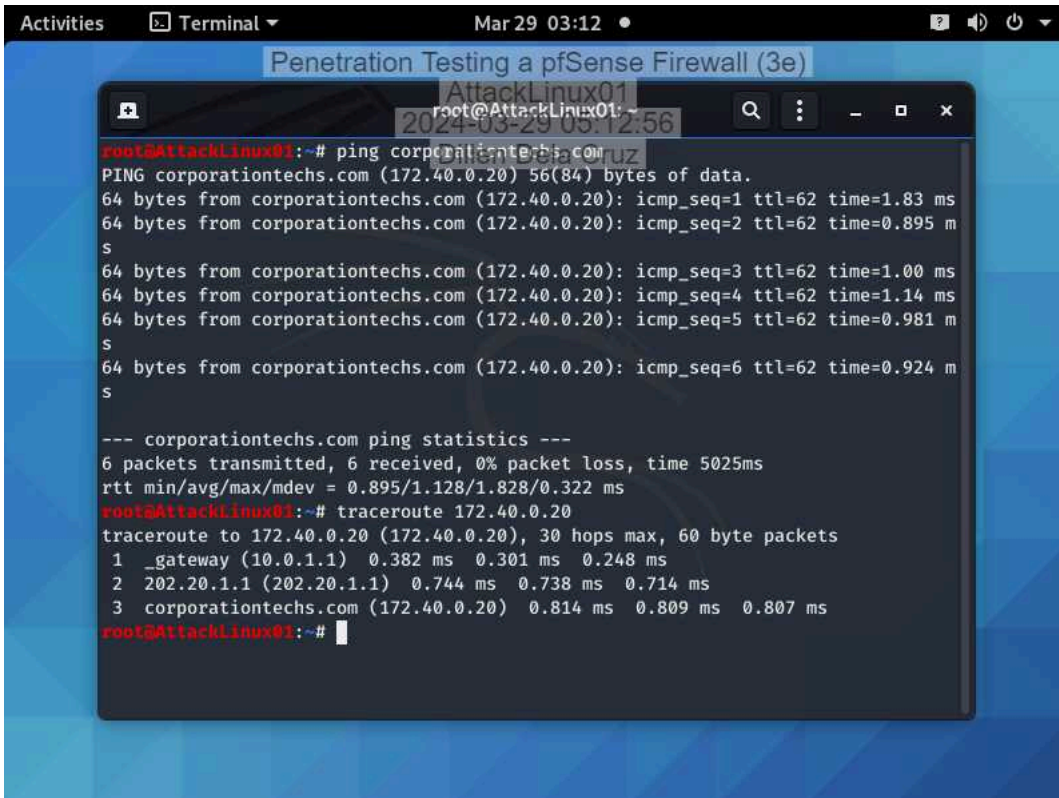
30. Make a screen capture showing the **updated vulnerability report summary**.



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.

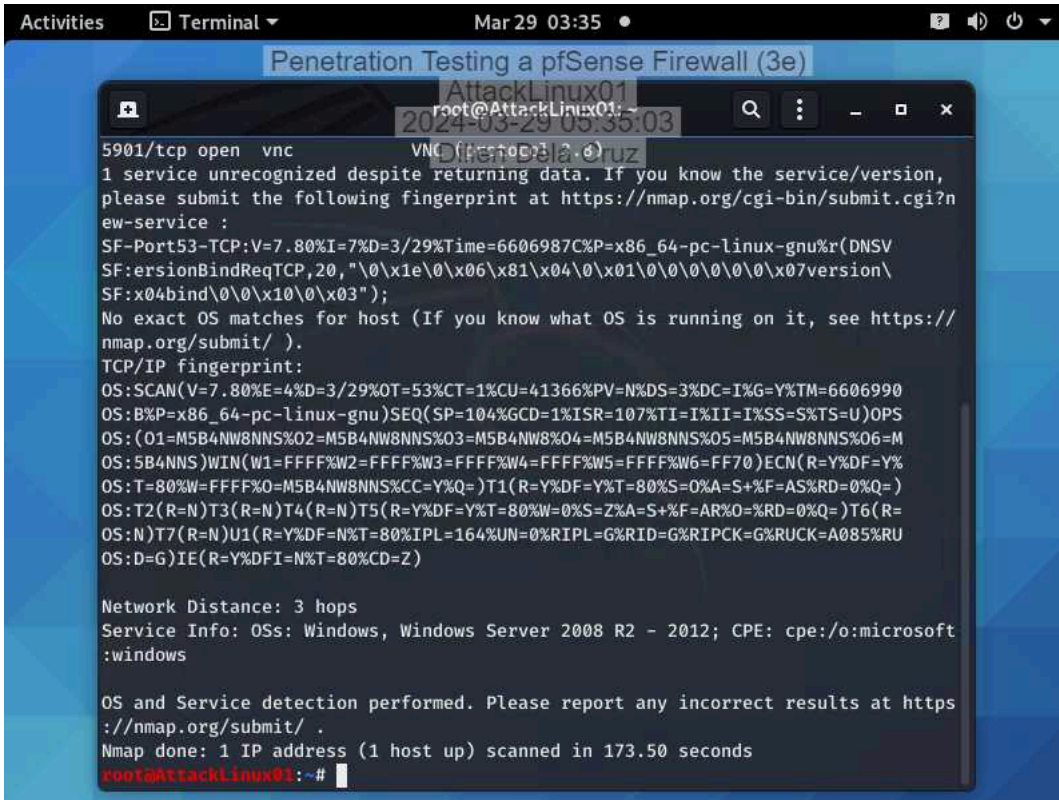


The screenshot shows a terminal window titled "Penetration Testing a pfSense Firewall (3e)" with a subtitle "AttackLinux01". The terminal output shows the results of a ping and traceroute command. The ping command was run against corporationtechs.com (172.40.0.20) and the traceroute command was run to 172.40.0.20. The traceroute shows three 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=1.83 ms
64 bytes from corporationtechs.com (172.40.0.20): icmp_seq=2 ttl=62 time=0.895 ms
64 bytes from corporationtechs.com (172.40.0.20): icmp_seq=3 ttl=62 time=1.00 ms
64 bytes from corporationtechs.com (172.40.0.20): icmp_seq=4 ttl=62 time=1.14 ms
64 bytes from corporationtechs.com (172.40.0.20): icmp_seq=5 ttl=62 time=0.981 ms
64 bytes from corporationtechs.com (172.40.0.20): icmp_seq=6 ttl=62 time=0.924 ms

--- corporationtechs.com ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5025ms
rtt min/avg/max/mdev = 0.895/1.128/1.828/0.322 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) 0.382 ms 0.301 ms 0.248 ms
 2 202.20.1.1 (202.20.1.1) 0.744 ms 0.738 ms 0.714 ms
 3 corporationtechs.com (172.40.0.20) 0.814 ms 0.809 ms 0.807 ms
root@AttackLinux01:~#
```

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



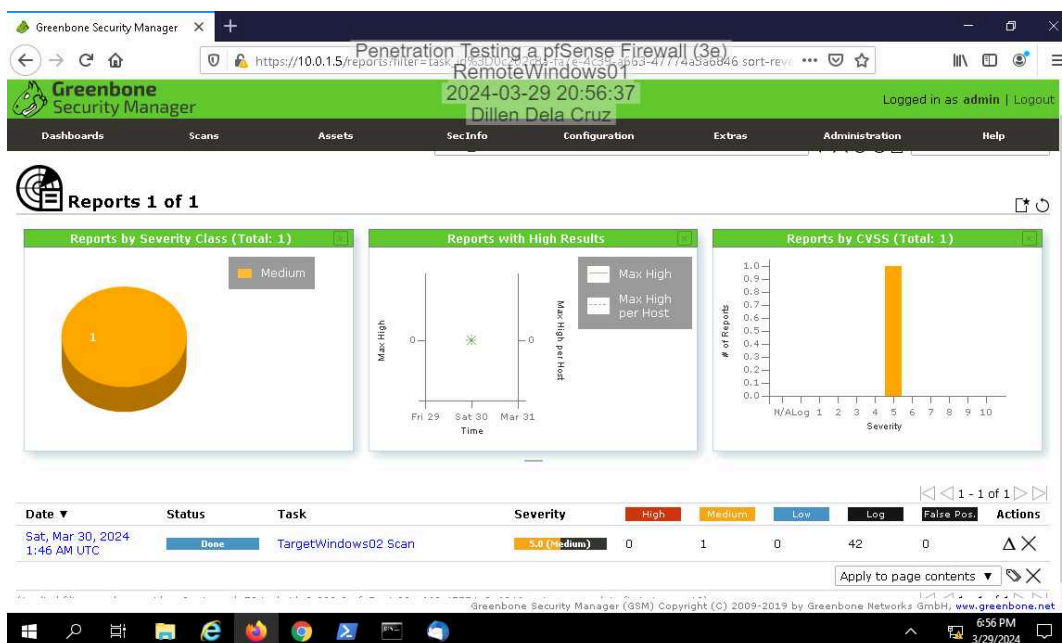
```
Penetration Testing a pfSense Firewall (3e)
root@AttackLinux01:~# nmap -i 10.0.1.12 -oN nmap.txt
5901/tcp open  vnc
1 service unrecognized despite returning data. If you know the service/version,
please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?n
ew-service :
SF-Port53-TCP:V=7.80%I=7%D=3/29%T=6606987C%P=x86_64-pc-linux-gnu%r(DNSV
SF:ersionBindReqTCP,20,"\\0\\x1e\\0\\x06\\x81\\x04\\0\\x01\\0\\0\\0\\0\\x07version\\
SF:x04bind\\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=3/29%OT=53%CT=1%CU=41366%PV=N%DS=3%DC=I%G=Y%TM=6606990
OS:B%P=x86_64-pc-linux-gnu)SEQ(SP=104%GCD=1%ISR=107%TI=I%II=I%SS=S%TS=U)OPS
OS:(O1=M5B4NW8NNS%O2=M5B4NW8NNS%O3=M5B4NW8%O4=M5B4NW8NNS%O5=M5B4NW8NNS%O6=M
OS:5B4NNS)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF70)ECN(R=Y%DF=Y%
OS:T=80%W=FFFF%O=M5B4NW8NNS%CC=Y%Q=)T1(R=Y%DF=Y%T=80%S=0%A=S+F=AS%RD=0%Q=)
OS:T2(R=N)T3(R=N)T4(R=N)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+F=AR%O=RD=0%Q=)T6(R=
OS:N)T7(R=N)U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=A085%RU
OS:D=G)IE(R=Y%DFI=N%T=80%CD=Z)

Network Distance: 3 hops
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; 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 173.50 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.

The screenshot displays the Greenbone Security Manager (GSM) web interface. The browser address bar shows the URL `https://10.0.1.5/report/4e29bdc1-1382-4f00-b44f-7c0d9e90e041`. The interface is logged in as 'admin'. The main navigation bar includes tabs for Dashboards, Scans, Assets, SecInfo, Configuration, Extras, Administration, and Help. The 'Scans' tab is active, showing a report for 'RemoteWindows01' dated '2024-03-29 20:59:18'. The report details include ID '4e29bdc1-1382-4f00-b44f-7c0d9e90e041', created on 'Sat, Mar 30, 2024 1:47 AM UTC', and modified on 'Sat, Mar 30, 2024 1:54 AM UTC'. The report is categorized under 'Information' and 'Results (43 of 44)'. The 'Vulnerability' section is expanded, showing a table of results:

Vulnerability	Severity	QoD	Host IP	Name	Location	Created
CPE Inventory	0.0 (Log)	80 %	202.20.1.3		general/CPE-T	Sat, Mar 30, 2024 1:53 AM UTC
Hostname Determination Reporting	0.0 (Log)	80 %	202.20.1.3		general/tcp	Sat, Mar 30, 2024 1:53 AM UTC
Unknown OS and Service Banner Reporting	0.0 (Log)	80 %	202.20.1.3		25/tcp	Sat, Mar 30, 2024 1:51 AM UTC
Unknown OS and Service Banner Reporting	0.0 (Log)	80 %	202.20.1.3		general/tcp	Sat, Mar 30, 2024 1:51 AM UTC
Unknown OS and Service Banner Reporting	0.0 (Log)	80 %	202.20.1.3		587/tcp	Sat, Mar 30, 2024 1:51 AM UTC
Unknown OS and Service Banner Reporting	0.0 (Log)	80 %	202.20.1.3		22/tcp	Sat, Mar 30, 2024 1:51 AM UTC

The footer of the interface shows the copyright notice: 'Greenbone Security Manager (GSM) Copyright (C) 2009-2019 by Greenbone Networks GmbH, www.greenbone.net'.

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.

Best Practices:

1. Segmentation and Access Control:

- Implement strict segmentation between the DMZ and the internal network using firewalls or similar devices.
- Enforce access controls to allow only necessary traffic between the DMZ and internal networks, minimizing the attack surface.

2. Multi-Layered Security:

- Deploy multiple layers of security mechanisms within the DMZ, such as intrusion detection/prevention systems (IDS/IPS) and antivirus software to detect and mitigate different types of attacks.
- Employ strong authentication and encryption protocols to protect sensitive data and communications within the DMZ.

3. Regular Monitoring and Patch Management:

- Implement continuous monitoring of network traffic, system logs, and security events within the DMZ to detect and respond to potential threats promptly.
- Establish a strong patch management process to ensure that servers and applications within the DMZ are regularly updated with the latest security patches and fixes which will reduce the risk of known vulnerabilities being exploited.

Potential Mistake or Vulnerability:

1. Failing to care for Regular Security Audits and Updates:

- Failing to conduct regular security audits and updates within the DMZ can lead to the accumulation of unpatched vulnerabilities over time, making it easier for attackers to exploit weaknesses.
- Not staying informed about emerging threats and failing to update security measures accordingly can leave the DMZ susceptible to new attack vectors and techniques.
- Overlooking the importance of periodically re-evaluating access controls and firewall rules may result in misconfigurations that could potentially expose the DMZ to unauthorized access or data breaches.

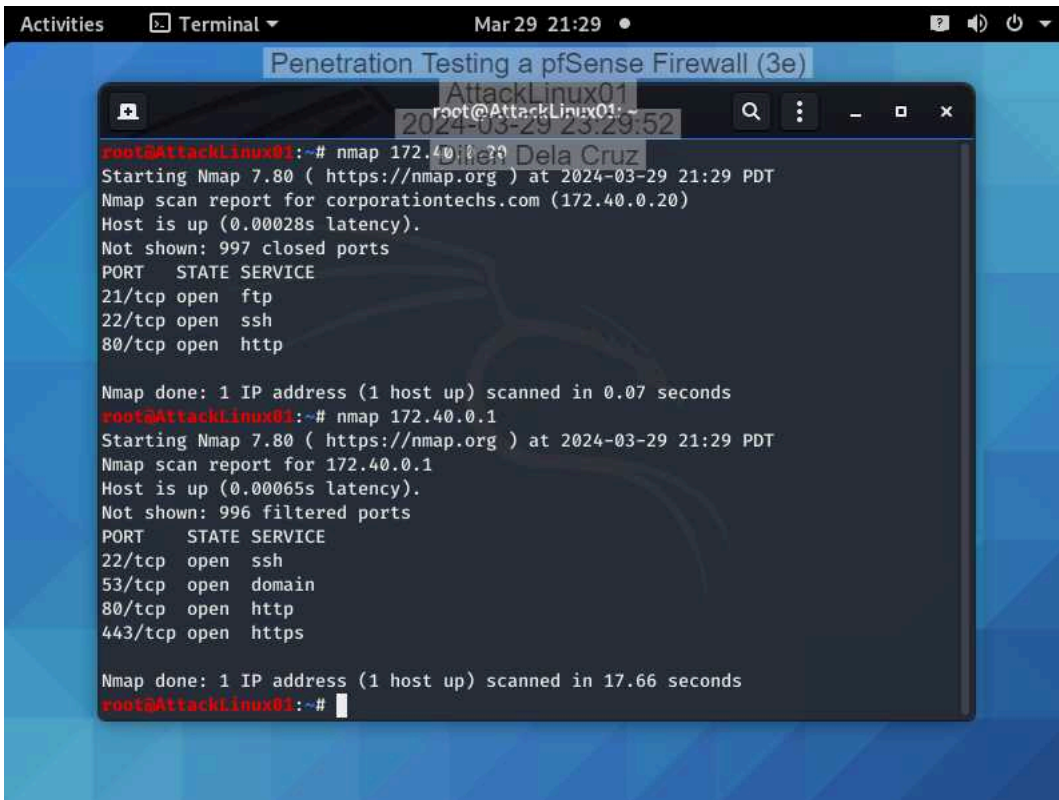
Works Cited LinkedIn. Wikipedia, <https://www.linkedin.com/pulse/strengthening-network-security-firewall-dmz-hardening-denisov-ms/>. Accessed 29 March 2024. Secure Works. Wikipedia, <https://www.secureworks.com/blog/incident-response-teams-find-common-pitfalls-in-network-security>. Accessed 29 March 2024.

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.**

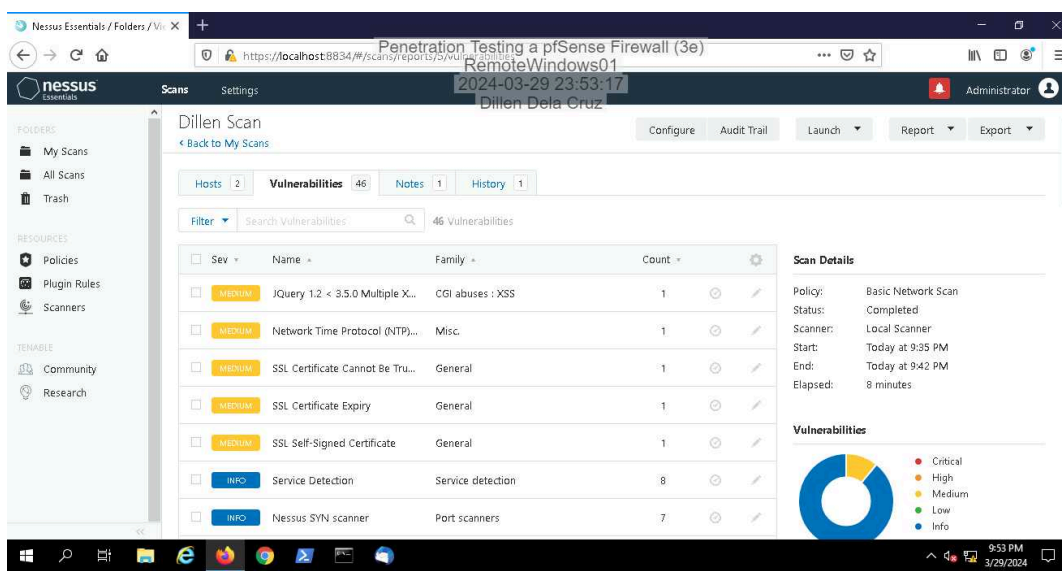


```
root@AttackLinux01:~# nmap 172.40.0.20
Starting Nmap 7.80 ( https://nmap.org ) at 2024-03-29 21:29 PDT
Nmap scan report for corporationtechs.com (172.40.0.20)
Host is up (0.00028s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  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 2024-03-29 21:29 PDT
Nmap scan report for 172.40.0.1
Host is up (0.00065s 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.**



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.

To enhance security, Secure Labs On Demand should focus on improving their network configuration and strengthening web server security. In terms of network configuration, they should review and update firewall rules on both the DMZ and internal network firewalls, restricting access to necessary ports and services while closing unnecessary ones like FTP (port 21). Additionally, implementing strict access controls between the DMZ and internal networks can minimize the risk of unauthorized access or lateral movement by potential attackers. Regarding web server security, they should apply strict security measures to services on open ports (SSH, HTTP/HTTPS) such as enforcing strong authentication, employing encryption protocols like updated SSL/TLS (DMZ has many SSL “medium” vulnerabilities), and regularly updating software to address vulnerabilities (DMZ needs to update JQuery). Deploying a Web Application Firewall (WAF) can provide an additional layer of protection against common web-based attacks, such as SQL injection (Cloud Flare). These measures collectively strengthen the overall security of their DMZ deployment and mitigate potential risks effectively.

Work Cited Cloud Flare. “What is a WAF? | Web Application Firewall explained.” Cloudflare, <https://www.cloudflare.com/learning/ddos/glossary/web-application-firewall-waf/>. Accessed 30 March 2024.