

# Penetration Testing a pfSense Firewall (3e)

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

Student:

Roman Cassman

Email:

rcassman0001@kctcs.edu

Time on Task:

2 hours, 18 minutes

Progress:

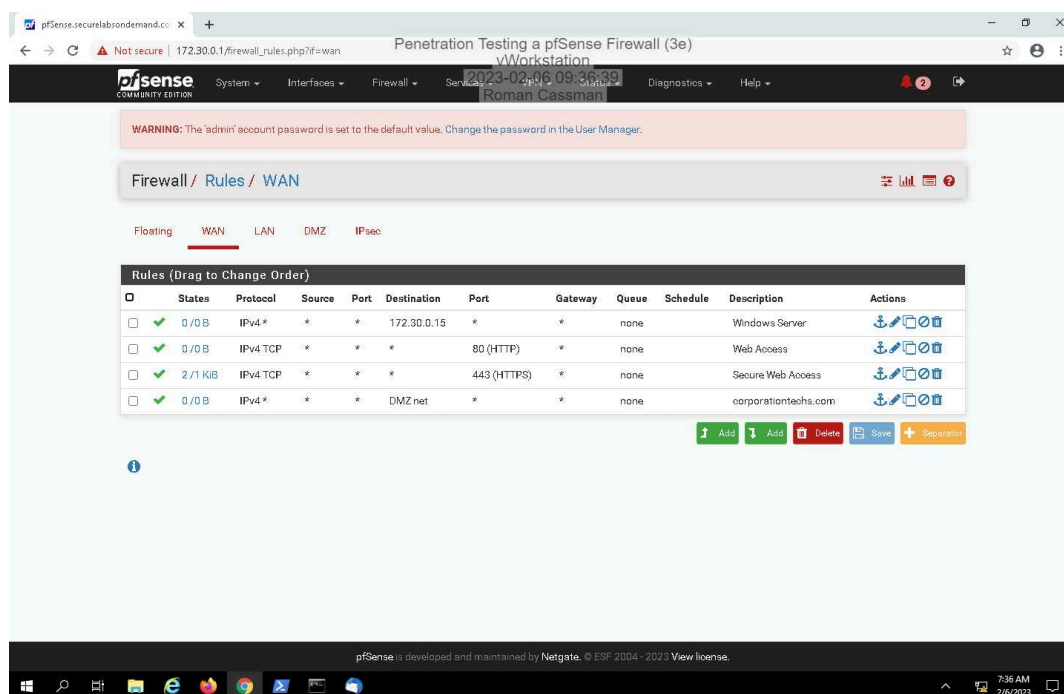
66%

Report Generated: Monday, February 6, 2023 at 11:12 AM

## Section 1: Hands-On Demonstration

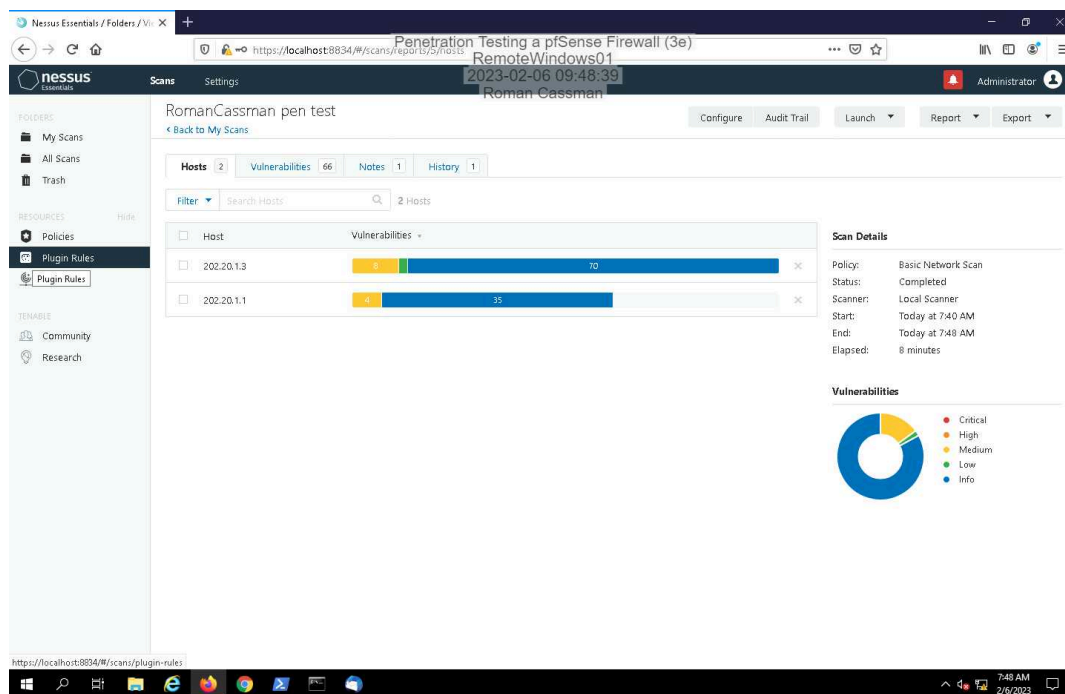
### Part 1: Examine a pfSense Firewall Configuration

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

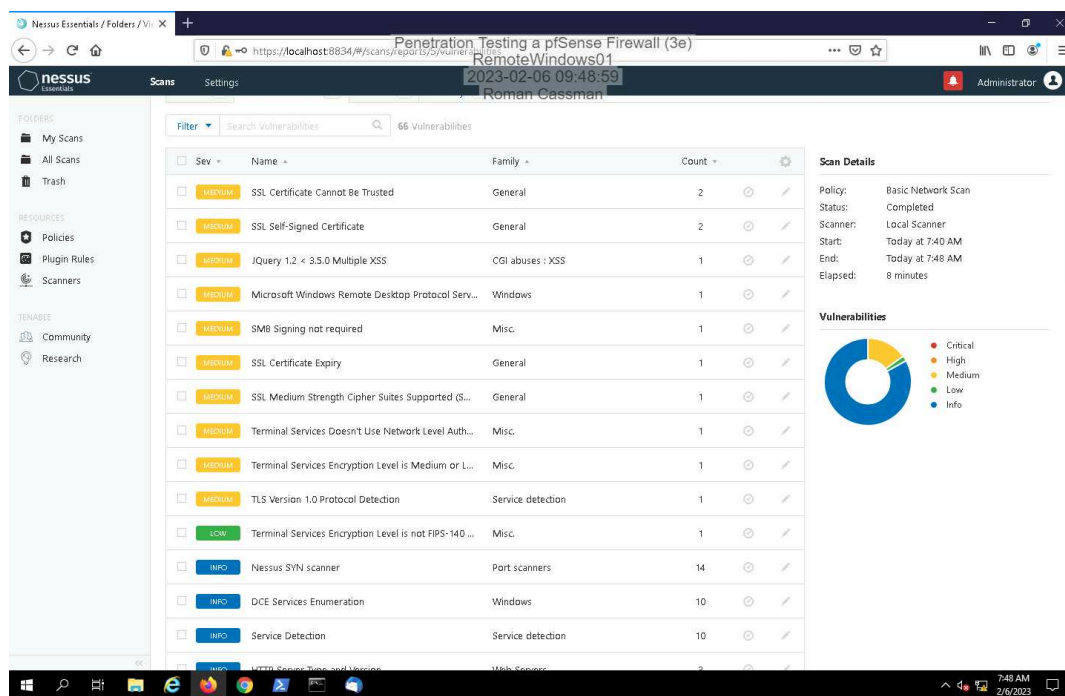


### Part 2: Conduct a Penetration Test on the Network

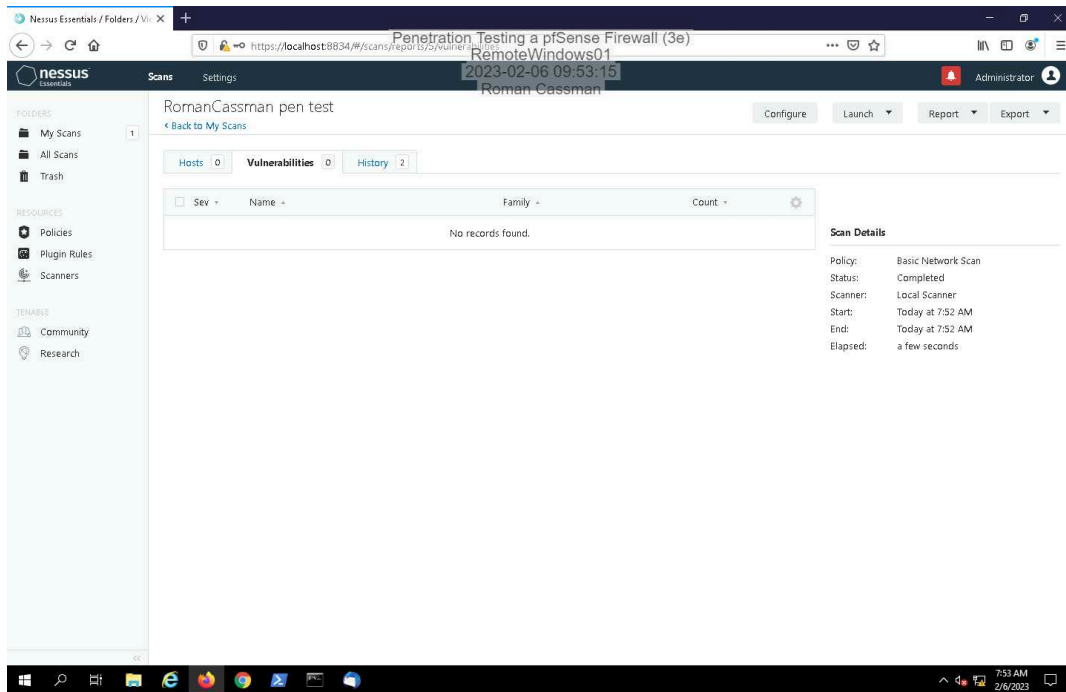
## 11. Make a screen capture showing the *yourname* pen test scan results.



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



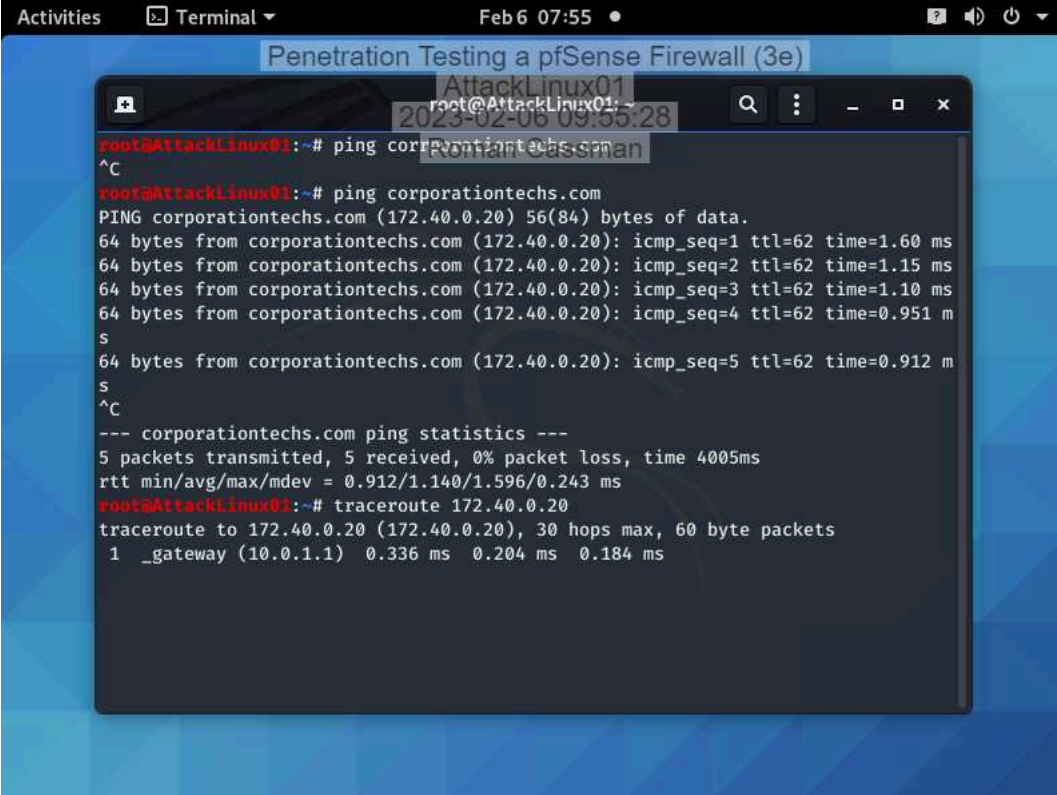
## 30. Make a screen capture showing the updated vulnerability report summary.



## 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.

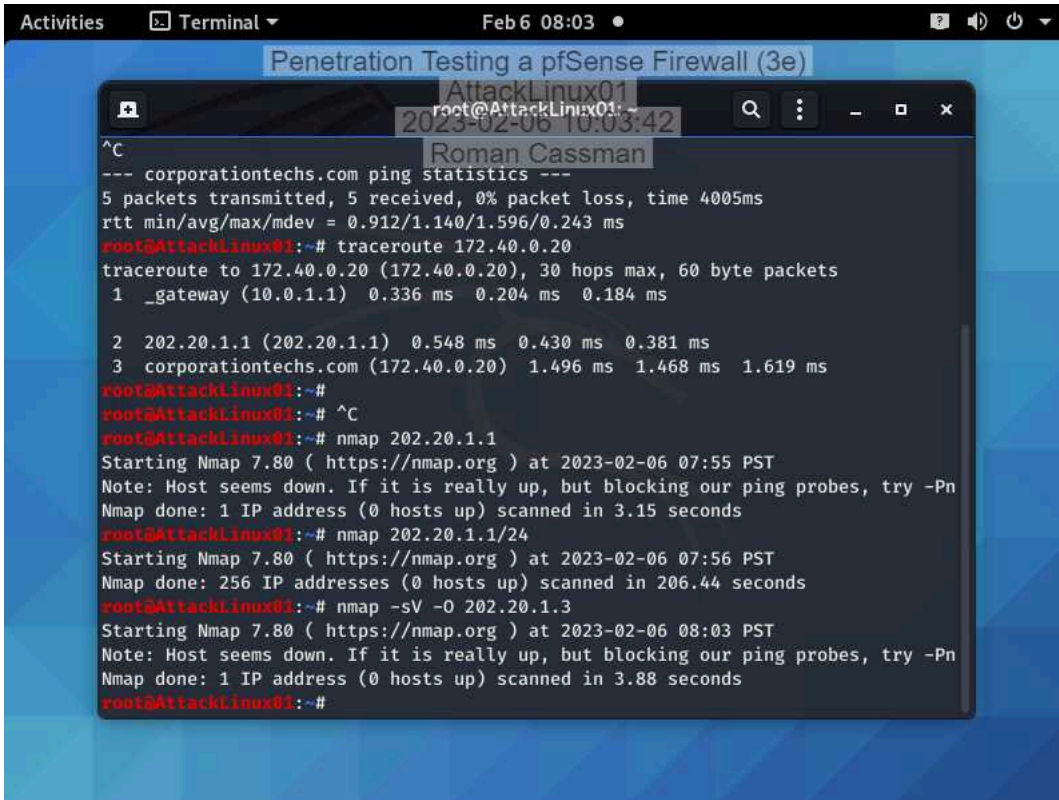


The screenshot shows a terminal window titled "Penetration Testing a pfSense Firewall (3e)" with a dark background. The terminal displays the following commands and output:

```
root@AttackLinux01:~# ping corporationtechs.com
^C
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=1.60 ms
64 bytes from corporationtechs.com (172.40.0.20): icmp_seq=2 ttl=62 time=1.15 ms
64 bytes from corporationtechs.com (172.40.0.20): icmp_seq=3 ttl=62 time=1.10 ms
64 bytes from corporationtechs.com (172.40.0.20): icmp_seq=4 ttl=62 time=0.951 m
s
64 bytes from corporationtechs.com (172.40.0.20): icmp_seq=5 ttl=62 time=0.912 m
s
^C
--- corporationtechs.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 0.912/1.140/1.596/0.243 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) 0.336 ms 0.204 ms 0.184 ms
```

The terminal window is part of a desktop environment with a blue background. The top bar shows "Activities", "Terminal", and the date/time "Feb 6 07:55". There are also icons for help, volume, and power. The terminal window has a title bar with "AttackLinux01" and a timestamp "2023-02-06 09:55:28".

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



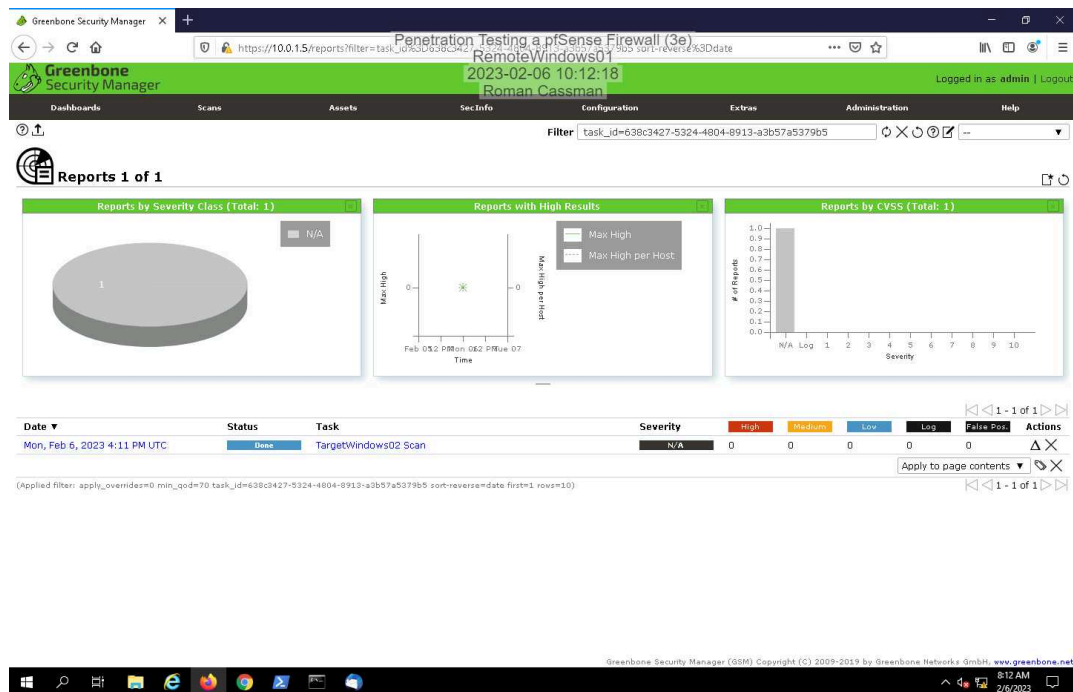
The screenshot shows a terminal window titled "Penetration Testing a pfSense Firewall (3e)" with a dark background. The terminal output includes the following commands and results:

```
^C
--- corporationtechs.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 0.912/1.140/1.596/0.243 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)  0.336 ms  0.204 ms  0.184 ms

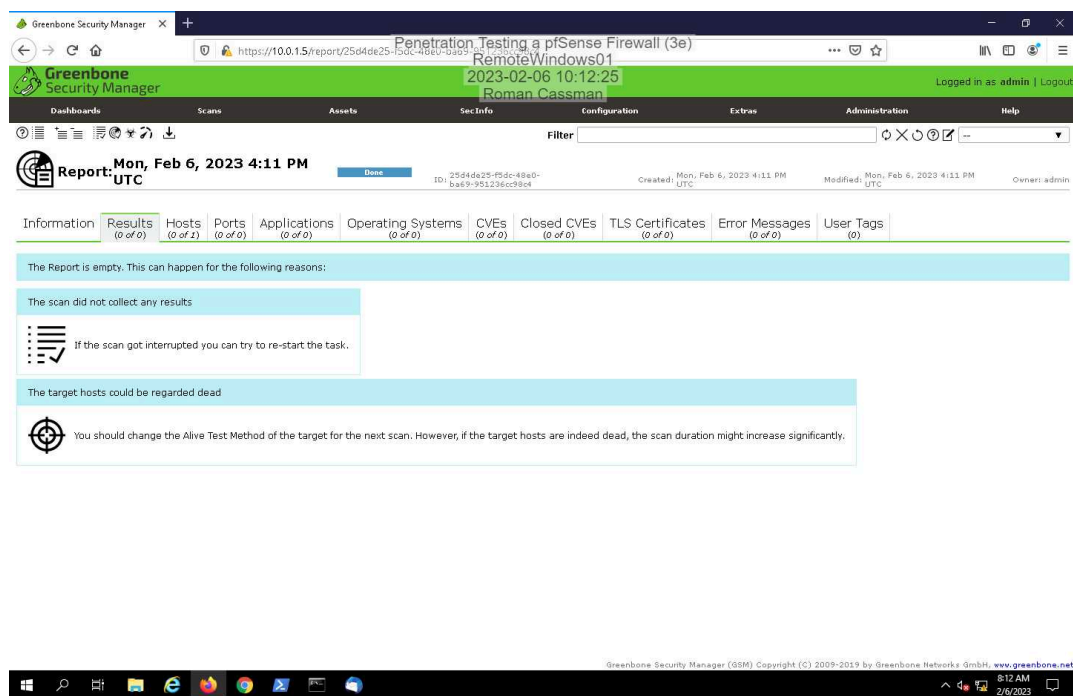
 2 202.20.1.1 (202.20.1.1)  0.548 ms  0.430 ms  0.381 ms
 3 corporationtechs.com (172.40.0.20)  1.496 ms  1.468 ms  1.619 ms
root@AttackLinux01:~#
root@AttackLinux01:~# ^C
root@AttackLinux01:~# nmap 202.20.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2023-02-06 07:55 PST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.15 seconds
root@AttackLinux01:~# nmap 202.20.1.1/24
Starting Nmap 7.80 ( https://nmap.org ) at 2023-02-06 07:56 PST
Nmap done: 256 IP addresses (0 hosts up) scanned in 206.44 seconds
root@AttackLinux01:~# nmap -sV -O 202.20.1.3
Starting Nmap 7.80 ( https://nmap.org ) at 2023-02-06 08:03 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 3.88 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.

Incomplete

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

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

Incomplete

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

Incomplete

#### 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.

Incomplete