Sasha Shahidi

Week 8 Homework: Networking Fundamentals Homework: Rocking your Network!

Phase 1:

The steps and commands used to complete the tasks:

Used Rockstar Corps' list of network assets to fping their Hollywood office IP's

```
fping -g 15.199.95.91/28
fping -g 15.199.94.91/28
fping -g 11.199.158.91/28
fping -g 167.172.144.11/32
fping -g 11.199.141.91/28
```

A summary of your findings for each testing phase:

I found that each IP is unreachable, except 167.172.144.11, which is alive.

Any network vulnerabilities discovered:

The 167.172.144.11 IP is a network vulnerability since RockStar Corp doesn't want any servers indicating that they're accepting connections, and this IP is indicating it's alive.

Findings associated with a hacker:

There is no evidence.

Recommended mitigation strategy:

Close the 167.172.144.11 IP so that all IP's are unreachable.

Document the OSI layer where the findings were found:

The findings were found in the Layer 3 Network layer (IP's).

Phase 2:

The steps and commands used to complete the tasks:

```
sudo nmap -sS 167.172.144.11
```

A summary of your findings for each testing phase:

Among the 6 ports that were found, I found Port 22 to be the only one open.

Any network vulnerabilities discovered:

Port 22 being open is a big network vulnerability.

Findings associated with a hacker:

There is no evidence.

Recommended mitigation strategy:

Close Port 22 so that no ports are open.

Document the OSI layer where the findings were found:

The findings were found in the Layer 4 Transport layer (ports).

Phase 3:

The steps and commands used to complete the tasks:

ssh jimi@167.172.144.11
Enter password: hendrix
cat /etc/hosts
exit
nslookup rollingstone.com
nslookup 98.137.246.8

A summary of your findings for each testing phase:

The IP address was changed to 98.137.246.8. The real domain of the 98.137.246.8 IP is unknown.yahoo.com.

Any network vulnerabilities discovered:

RockStar Corp using the same username and password for most servers is a network vulnerability. It allows the possibility of hackers to gain access.

Findings associated with a hacker:

A hacker gained access and changed the IP address to 98.137.246.8 and the rollingstone.com domain to unknown.yahoo.com.

Recommended mitigation strategy:

Put different usernames and passwords for all servers.

Document the OSI layer where the findings were found:

The findings were found in the Layer 7 Application layer (SSH and DNS).

Phase 4:

The steps and commands used to complete the tasks:

ssh jimi@167.172.144.11
Enter password: hendrix
cd /etc/
ls
cat packetcaptureinfo.txt
Open the link in Wireshark
Filter: arp
Filter: http

A summary of your findings for each testing phase:

With the ARP protocol, I found suspicious activity in Packet 5, as it reveals a duplicate IP address was detected. With the HTTP protocol, I found suspicious activity in Packet 16, as it reveals that a hacker who works at RockStar Corp sent an email, stating that Port 22 was left open and they will provide the username and password for $1 million.

Any network vulnerabilities discovered:

Leaving Port 22 open and hiring criminal hackers who hack the company network are network vulnerabilities.

Findings associated with a hacker:

A hacker created a duplicate IP address and sent an email revealing Port 22 was open and that they're willing to sell the username and password in exchange for $1 million.

Recommended mitigation strategy:

Close Port 22 and don't hire criminal hackers to the company.

Document the OSI layer where the findings were found:

The findings were found in the Layer 2 Data Link layer (ARP) and the Layer 7 Application layer (HTTP).