Cybersecurity

Networking Challenge Submission File

Networking Fundamentals: Rocking your Network

Make a copy of this document to work in. For each phase, add the solution below the prompt. Save and submit this completed file as your Challenge deliverable.

Phase 1: *"I'd like to Teach the World to `ping`"*

1. Command(s) used to run `ping` against the IP ranges:

```
ping 15.199.95.91
ping 15.199.94.91
ping 203.0.113.32
ping 161.35.96.20
ping 192.0.2.0
```

2. Summarize the results of the `ping` command(s):

```
15.199.95.91, 15.199.94.91 and 203.0.113.32 replied with 'Destination net
unreachable'. This error message may indicate that the specified destination
network or IP address is unreachable due to network misconfigurations,
routing issues, or firewall rules blocking access.

161.35.96.20 replied with all 4 packets that were sent in an average time of
33ms. This indicates that this server is up and may be accepting
connections.
```

3. List of IPs responding to echo requests:

```
161.35.96.20
```

4. Explain which OSI layer(s) your findings involve:

```
Pinging an IP address operates at the Network Layer – Layer 3 of the OSI
model. Layer 3 is responsible for routing and addressing in a network.
```

5. Mitigation recommendations (if needed):

```
Since RockStar Corp does not want any of its servers, even if they are up,
to indicate that they are accepting connections in response to ping
requests, they should implement firewall rules or security group policies to
block ICMP Echo Requests. They can also disable ICMP responses at the server
level, and regularly patch and update servers.
```

Phase 2: *"Some SYN for Nothin'"*

1. Which ports are open on the RockStar Corp server?

```
sudo nmap -sS 161.35.96.20

Port 22 is open and running SSH
```

2. Which OSI layer do SYN scans run on?
    a. OSI layer:

```
SYN scans run on the Transport Layer (Layer 4) of the OSI model.
```

    b. Explain how you determined which layer:

```
SYN scans, which use TCP SYN packets to identify open ports on target
systems, operate at the Transport Layer (Layer 4) of the OSI model due to
their reliance on TCP's port-based communication management. Additionally,
the TCP handshake, a procedure for establishing reliable connections between
devices, involves Device X initiating a connection by sending a SYN request
to Device Z, which responds with a SYN/ACK request, followed by Device X
confirming the connection with an ACK message, all occurring within the
Transport Layer (The Seven Layer OSI Model, 2008-2017).
```

3. Mitigation suggestions (if needed):

```
The Nmap scan report for IP address 161.35.96.20 indicates an active server with an open SSH port, potentially allowing SSH connections. To safeguard against revealing open ports, the company can take steps like configuring firewalls, changing default ports, implementing port knocking, and ensuring regular server security updates and monitoring. These measures, alongside access controls, network segmentation, and adherence to security best practices, contribute to a comprehensive security strategy for protecting servers while maintaining functionality (What is an Open Port & What are the Security Implications, 2022).
```

Phase 3: *"I Feel a DNS Change Comin' On"*

1. Summarize your findings about why access to rollingstone.com is not working as expected from the RockStar Corp Hollywood office:

```
After logging in to the server using SSH command, a review of the /etc/hosts file revealed that the IP address associated with rollingstone.com was showing 98.137.246.8 and not 161.35.96.20. This is as a result of DNS poisoning. The IP address 98.137.246.8 was revealed to be connected to the domain unknown.yahoo.com after further investigation using the nslookup command.
```

2. Command used to query Domain Name System records:

```
nslookup 98.137.246.8
nslookup -type=2A 98.137.246.8
nslookup -type=NS 98.137.246.8
nslookup -type=MX 98.137.246.8
```

3. Domain name findings:

```
The following information was found using the nslookup command:
Server: 8.8.8.8
Address: 8.8.8.8#53
Non-authoritative answer:
8.246.137.98.in-addr.arpa     name = unknown.yahoo.com.
```

```
The findings of the nslookup revealed that the hacker is using one of
Google's public DNS servers and is listening on port 53. The IP address
98.137.246.8 is linked to unknown.yahoo.com. This might not be the final
authoritative answer for that IP address.

Further to the above, the hosts file in the /etc folder was modified on the
server and is therefore affecting viewing rollingstone.com in the browser.
The IP address is supposed to be 161.35.96.20 for this Hollywood office
server, but is instead showing 98.137.246.8. The IP address 98.137.246.8 is
associated with unknown.yahoo.com. This indicates that the DNS was poisoned.
DNS poisoning is a malicious technique in which an attacker corrupts or
manipulates the DNS cache to redirect legitimate domain name resolutions to
malicious IP addresses.
```

4. Explain what OSI layer DNS runs on:

```
DNS runs on the Application Layer (Layer 7) of the OSI model, responsible
for translating human-readable domain names into IP addresses. It
facilitates the conversion of domain names to IP addresses, crucial for
internet communication, and uses protocols associated with the Application
Layer for data exchange.
```

5. Mitigation suggestions (if needed):

```
RockStar Corp should correct DNS poisoning caused by the modified hosts file
in the /etc folder, by editing the hosts file and removing the unauthorized
entry, optionally flushing the DNS cache, and restarting networking. To
prevent future DNS poisoning, the company should regularly monitor and
secure the hosts file, keep software up to date, and educate users about
potential risks. They can also consider using DNSSEC for added security.
```

Phase 4: *"ShARP Dressed Man"*

1. Name of file containing packets:

```
packetcaptureinfo.txt

The following subsequent steps were taken:
ssh jimi@161.35.96.20
cd /etc
```

```
cat packetcaptureinfo.txt
In this file, is a link to the PCAP files ‘secretlogs.pcapng’
```

2. ARP findings identifying the hacker’s MAC address:

```
After reviewing the PCAP files, specifically the ARP protocol, there are two devices trying to use the same IP address 192.168.47.200. One device has the MAC address 00:0c:29:1d:b3:b1 and the other has 00:0c:29:0f:71:a3. This is a problem because each device on a network should have a unique IP address to work properly, and having two devices with the same IP can cause network issues. This suspicious activity can be attributed to the hacker from MAC address 00:0c:29:1d:b3:b1.
```

3. HTTP findings, including the message from the hacker:

```
After reviewing the PCAP files, specifically the HTTP protocol, I found a suspicious POST request to a specific URL. After further investigation, it was revealed that the hacker sent message to gottheblues.yoloasite.com via the Contact US form: “Hi Got The Blues Corp! This is a hacker that works at Rock Star Corp. Rock Star has left port 22, SSH open if you want to hack in. For 1 Million Dollars I will provide you the user and password!”.
```

4. Explain the OSI layers for HTTP and ARP.
    a. Layer used for HTTP:

```
HTTP operates at the Application Layer (Layer 7) of the OSI model, facilitating communication between web browsers and servers on the internet.
```

    b. Layer used for ARP:

```
ARP operates at the Data Link Layer (Layer 2) of the OSI model and resolves IP addresses to physical MAC addresses within a local network.
```

5. Mitigation suggestions (if needed):

```
To address the issue of unauthorized access attempts and prevent future incidents, first, RockStar Corp should identify and isolate the rogue device
```

```
causing the duplicate IP address alert (identified via ARP protocol in
Wireshark). Immediately change SSH credentials and review access logs for
suspicious activity. For long-term prevention, implement network access
controls, port security, intrusion detection/prevention systems, and
regularly update and patch systems. Additionally, educate users, segment the
network, and have an incident response plan in place while considering legal
action against the hacker who attempted to sell login credentials.
```


References

The Seven Layer OSI Model (2008-2017). *Flylib.com*
https://flylib.com/books/en/4.283.1.79/1/

What is an Open Port & What are the Security Implications (2022). *BeyondTrust*
https://www.beyondtrust.com/blog/entry/what-is-an-open-port-what-are-the-security-implications