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:

```
fping -sS multiple IP s address
```

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

```
2 IP's alive
```

3. List of IPs responding to echo requests:

```
161.35.96.20 is alive
192.0.2.0 is alive
```

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

```
For IP address 161.35.96.20:
Port 22/tcp is open, indicating that the SSH  service is running on this
host.
For IP address 192.0.2.0:
The output indicates that all 1000 scanned ports are in ignored states, and
1000 filtered TCP ports  are not shown.
```

5. Mitigation recommendations (if needed):

```
For 161.35.96.20's SSH service (Port 22): Enforce robust authentication, like public key authentication. Keep SSH server updated to patch vulnerabilities. Implement firewall rules restricting access to trusted IP addresses for enhanced security.
```

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

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

```
22/tcp open  ssh
```

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

```
Transport
```

    b. Explain how you determined which layer:

```
Using synchronize acknowledge - (-sS)
```

3. Mitigation suggestions (if needed):

```
Implement an ACL to filter all connection to only those pre define
```

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:

```
The issue with access to rollingstone.com from the RockStar Corp Hollywood office stems from a duplicated IP address, leading to redirect to malicious properties.
```

2. Command used to query Domain Name System records:

```
cat /etc/hosts , nslookup 98.137.246.8
```

3. Domain name findings:

```
gtclass-1578758377314-s-1vcpu-1gb-nyc1-01.localdomain
gtclass-1578758377314-s-1vcpu-1gb-nyc1-01
localhost
rollingstone.com
8.246.137.98.in-addr.arpa       name = unknown.yahoo.com.
```

4. Explain what OSI layer DNS runs on:

```
DNS operates at OSI Layer 7 (Application Layer), using TCP and UDP as transport layer protocols for communication between clients and servers.
```

5. Mitigation suggestions (if needed):

```
Enhance security by securing the user home directory, rectifying the hosts file, and reviewing the cloud configuration to address potential vulnerabilities and ensure proper system settings.
```

Phase 4: *"ShARP Dressed Man"*

1. Name of file containing packets:

```
secretlogs.pcapng
```

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

```
Duplicate MAC address for 192.168.47.200 is (00:0c:29:1d:b3:b1)also used by (00:0c:29:0f:71:a3) (frame4)
```

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

```
 [HTTP request 1/1]
    [Response in frame: 17]
    File Data: 1163 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
    Form item: "0<text>" = "Mr Hacker"
    Form item: "0<label>" = "Name"
    Form item: "1<text>" = "Hacker@rockstarcorp.com"
    Form item: "1<label>" = "Email"
    Form item: "2<text>" = ""
    Form item: "2<label>" = "Phone"
    Form item: "3<textarea>" = "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 with the user and
password!"
```

4. Explain the OSI layers for HTTP and ARP.

    a. Layer used for HTTP:

```
HTTP functions at the OSI model's Application Layer 7, focusing on end-user
services
```

    b. Layer used for ARP:

```
ARP operates at the Link Layer 2, managing hardware addresses in the

local network's physical connection between devices.
```

5. Mitigation suggestions (if needed):

```
Remove the newly generated MAC address,Change passwords, especially for port
22,
Isolate the compromised system to prevent unauthorized access. Regularly
back up critical data to mitigate potential data breaches or loss.
```