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 -g]
```

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

```
[15.199.95.91/28: unreachable
15.199.94.91/28: unreachable
203.0.113.32/28: unreachable
161.35.96.20/32: alive
192.0.2.0/28: unreachable]
```

3. List of IPs responding to echo requests:

```
[161.35.96.20 is alive]
```

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

```
[Network]
```

5. Mitigation recommendations (if needed):

```
[Block ping requests against subnets]
```

Phase 2: *“Some SYN for Nothin’”*

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

```
[port 22]
```

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

```
[Transport]
```

    b. Explain how you determined which layer:

```
[Dealing with network traffic]
```

3. Mitigation suggestions (if needed):

```
[monitoring ssh traffic]
```

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:

```
[IP is attached to the wrong website, IP in host file is connected to an
unknown yahoo website.]
```

2. Command used to query Domain Name System records:

```
[nslookup 98.137.246.8]
```

3. Domain name findings:

```
[With nslookup we found the IP address was connected to unknown.yahoo.com,
instead of the rolling stone website]
```

4. Explain what OSI layer DNS runs on:

```
[Application]
```

5. Mitigation suggestions (if needed):

```
[Putting the correct IP address from rolling stone in the host file]
```

Phase 4: *"ShARP Dressed Man"*

1. Name of file containing packets:

```
[Packetcaptureinfo.txt]
```

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

```
[Duplicate ARP response, 00:0c:29:1d:b3:b1]
```

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

```
[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 Milliion Dollars I will provide you the user and
password!"]
```

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

```
[Application]
```

    b. Layer used for ARP:

```
[Data Link]
```

5. Mitigation suggestions (if needed):

```
[Static ARP entries, find the owner of the MAC address]
```

© 2023 edX Boot Camps LLC. Confidential and Proprietary. All Rights Reserved.