| 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:

| sysadmin@UbuntuDesktop:~$ fping -g 15.199.95.91/28  sysadmin@UbuntuDesktop:~$ fping -g 15.199.94.91/28  sysadmin@UbuntuDesktop:~$ fping -g 203.0.113.32/28  sysadmin@UbuntuDesktop:~$ fping -g 161.35.96.20/32  sysadmin@UbuntuDesktop:~$ fping -g 192.0.2.0/28 |
| --- |

1. Summarize the results of the ping command(s):

| Using ‘fping’ (instead of ‘ping’), we can search multiple IP addresses at once. The only IP address that was alive was IP address 161.35.96.20/32, which is the Hollywood Applications server. All of the other ones were unreachable. This is problematic for RockStar Corp, since they would not want to be accepting any connections to the server, especially any unauthorized ones. |
| --- |

1. List of IPs responding to echo requests:

| 161.35.96.20/32 responds as alive. |
| --- |

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

| The Network Layer (Layer 3) is the OSI Layer that my findings involve because it involves using IP addresses to route data through a physical network. |
| --- |

1. Mitigation recommendations (if needed):

| A risk mitigation recommendation would be to add a firewall device for this server to catch pings and reject them. |
| --- |

### Phase **2:** *“Some SYN for Nothin’”*

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

| sysadmin@UbuntuDesktop:~$ sudo nmap -sS 161.35.96.20  [sudo] password for sysadmin:  Starting Nmap 7.60 ( https://nmap.org ) at 2023-05-25 19:36 EDT  Nmap scan report for 161.35.96.20  Host is up (0.0031s latency).  Not shown: 999 filtered ports  **PORT STATE SERVICE**  **22/tcp open ssh <-open port**  Nmap done: 1 IP address (1 host up) scanned in 18.34 seconds |
| --- |
|  |

1. Which OSI layer do SYN scans run on?
   1. OSI layer:

| SYN scans run on the Transport Layer of the OSI Model (Layer 4). |
| --- |

* 1. Explain how you determined which layer:

| The Transport Layer is not only where data is being transmitted across the network, but this layer also assigns both source and destination ports. The Transmission Control Protocol is a key protocol for this layer and plays a role in sending SYN requests. |
| --- |

1. Mitigation suggestions (if needed):

| We need to ensure that this port is closed and stays closed to prevent unwanted entry by threat actors. |
| --- |

### 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:

| **To gain entry into the system using SSH:**  sysadmin@UbuntuDesktop:~$ ssh jimi@161.35.96.20  jimi@161.35.96.20's password: hendrix  # /etc/cloud/cloud.cfg or cloud-config from user-data  #  127.0.1.1 gtclass-1578758377314-s-1vcpu-1gb-nyc1-01.localdomain gtclass-1578758377314-s-1vcpu-1gb-nyc1-01  127.0.0.1 localhost  98.137.246.8 rollingstone.com  **I have found that rollingstone.com’s IP is 98.137.246.8.**  **However, we cannot access rollingstone.com when we try to ping it in the terminal.**  sysadmin@UbuntuDesktop:~$ ping 98.137.246.8  PING 98.137.246.8 (98.137.246.8) 56(84) bytes of data.  ^C  --- 98.137.246.8 ping statistics ---  162 packets transmitted, 0 received, 100% packet loss, time 164944ms |
| --- |

1. Command used to query Domain Name System records:

| sysadmin@UbuntuDesktop:~$ nslookup rollingstone.com |
| --- |

1. Domain name findings:

| sysadmin@UbuntuDesktop:~$ nslookup rollingstone.com  Server: 8.8.8.8  Address: 8.8.8.8#53  Non-authoritative answer:  Name: rollingstone.com  Address: 192.0.66.114  **I have found that rollingstone.com’s IP address is 192.0.66.114. Both the domain name and the IP address can be ping’d.** |
| --- |

1. Explain what OSI layer DNS runs on:

| The OSI Layer that the Domain Name System runs on is the Application layer (Layer 7). This layer represents data regarding user applications, such as using a browser to access a website, with a key protocol being the DNS. |
| --- |

1. Mitigation suggestions (if needed):

| One could ensure that the DNS is monitored and updated regularly. |
| --- |

### Phase 4: *“ShARP Dressed Man”*

1. Name of file containing packets:

| W**hen you run a ls -l command in the terminal, a file called packetcaptureinfo.txt in the /etc folder grants you access to secretlogs.pcapng and sends you to Wireshark for viewing the packet capture.**  $ cat packetcaptureinfo.txt  My Captured Packets are Here:  https://drive.google.com/file/d/1ic-CFFGrbruloYrWaw3PvT71elTkh3eF/view?usp=sharing |
| --- |

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

| Destination: VMware\_1d:b3:b1 **(00:0c:29:1d:b3:b1) < hacker’s MAC Address** |
| --- |

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

| HTML Form URL Encoded: application/x-www-form-urlencoded  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!"  **The hacker has been trying to post on http://www.gottheblues.yolasite.com/contact-us.php with a ransom message.** |
| --- |

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

| The OSI Layer for HTTP is the Application Layer (Layer 7). This is because HTTP is used for sending packets through the internet and the Application Layer falls under the category of handling communication between the user and the internet. |
| --- |

* 1. Layer used for ARP:

| The OSI Layer for ARP is the Data Link Layer (Layer 2). This layer handles the sending of data between devices on a network, including the connection of an IP address to a MAC address. |
| --- |

1. Mitigation suggestions (if needed):

| One may want to add a Static ARP entry to the highly valuable connections within a network to create a permanent connection between the IP and MAC addresses. |
| --- |

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