| 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   * The request timed out. (100% loss)   ping 15.199.94.91   * The request timed out. (100% loss)   ping 203.0.113.32   * The request timed out. (100% loss)   ping 161.35.96.20   * Sent and Received 4 replies (0% loss)   ping 192.0.2.0 |
| --- |

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

| After pinging all of the IP addresses for the Hollywood office, there was only one that had a reply. The IP address that replied correctly was the Hollywood Application Server 1 - 161.35.96.20. The other IP addresses were a 100% loss after 4 attempts. |
| --- |

1. List of IPs responding to echo requests:

| 161.35.96.20 |
| --- |

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

| The findings primarily involve the network layer (Layer 3) of the OSI model, as ping operates at this layer to test connectivity between devices. |
| --- |

1. Mitigation recommendations (if needed):

| - Monitor network activity for any anomalies or unauthorized access.  - Create strong firewall rules to restrict access to only necessary IP addresses. |
| --- |

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

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

| sysadmin@vm-image-ubuntu-dev-1:~$ sudo nmap -sS 161.35.96.20  Starting Nmap 7.80 ( https://nmap.org ) at 2024-02-22 22:09 UTC  Nmap scan report for 161.35.96.20  Host is up (0.079s latency).  Not shown: 999 closed ports  PORT STATE SERVICE  22/tcp open ssh  From my results, port 22 is open. |
| --- |

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

| Transport layer (Layer 4) - TCP protocol for SYN scan |
| --- |

* 1. Explain how you determined which layer:

| The SYN scan operates at the Transport Layer (Layer 4) of the OSI model because it’s using the TCP protocol (Transmission Control Protocol).It specifically uses the TCP process to check the state of ports on the targeted system. |
| --- |

1. Mitigation suggestions (if needed):

| - Use access control lists (ACLs) to restrict access to specific ports based on necessity.  - Regularly update and patch server software to fix any known vulnerabilities. |
| --- |

### 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:

| -I did an **ls** to see **etc**  -Then **cd /etc/**  -Then did **ls** again to see “hosts”  -I did **cat hosts**  -That revealed 98.137.246.8 rollingstone.com  -I signed out of jimi and while in sysadmin, I did:  **nslookup 98.137.246.8**  sysadmin@vm-image-ubuntu-dev-1:~$ nslookup 98.137.246.8  8.246.137.98.in-addr.arpa name = unknown.yahoo.com.  Summary:  Successfully logged into the server using SSH.  - Identified that port 22 is used for SSH.  - Found that rollingstone.com was redirected to a different website (unknown.yahoo.com) in the configuration file.  - Terminated the SSH session (**exit**).  - Used nslookup to determine the real domain associated with the IP address.  Findings:  - Port 22 (SSH) is used for remote system administration.  - rollingstone.com was redirected to a different website.  - The real domain associated with the IP(98.137.246.8) address is (unknown.yahoo.com). |
| --- |

1. Command used to query Domain Name System records:

| nslookup 98.137.246.8 |
| --- |

1. Domain name findings:

| http://unknown.yahoo.com/ |
| --- |

1. Explain what OSI layer DNS runs on:

| DNS operates at the application layer (Layer 7) of the OSI model.DNS provides a service that translates domain names into IP addresses and vice versa. |
| --- |

1. Mitigation suggestions (if needed):

| -Default credentials were used for SSH access, which is a security risk.  -Unauthorized modification of DNS settings could lead to potential security issues.  -Change default credentials and enforce strong password policies.  -Audit and monitor DNS configurations for any unauthorized changes.  -Implement access controls to restrict modifications to critical configuration files. |
| --- |

### Phase 4: *“ShARP Dressed Man”*

1. Name of file containing packets:

| secretlogs.pcapng |
| --- |

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

| The hackers MAC address in the ARP appears to be 192.168.47.200 (**00:0c:29:1d:b3:b1**) as it highlights in yellow that there is a duplicate IP address detected. It says: -also in use by 00:0c:29:0f:71:as (frame 4) |
| --- |

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

| The hacker is attempting to sell the username and password to the open port for 1 million dollars. There’s a hidden message in the 16th packet of HTTP:  Message from hacker: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! |
| --- |

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

| Layer 7, Application of the OSI model, HTTP is a key protocol used in this layer. |
| --- |

* 1. Layer used for ARP:

| Layer 2, Date Link Level, of the OSI model. ARP maps MAC addresses to IP addresses. |
| --- |

1. Mitigation suggestions (if needed):

| Close Port 22 for ssh and reassign to another port Port 22 is indeed closed and reassigned to another Port |
| --- |

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