| 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 161.35.96.20 |
| --- |

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

| ping 15.199.95.91 = No ICMP Echo  ping 15.199.94.91 = No ICMP Echo  ping 161.35.96.20 = Successful ICMP Echo |
| --- |

1. List of IPs responding to echo requests:

| ping 161.35.96.20 |
| --- |

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

| The pinging command uses ICMP (Internet Control Message Protocol), which is a protocol hosted on the Network layer (Layer 3) of the OSI Model. |
| --- |

1. Mitigation recommendations (if needed):

| One way the Public IP address can be risk mitigated, is by disabling ICMP or Ping in the firewall. By disabling this feature, ICMP cannot be used to ping the network. The firewall is a device that monitors network traffic at the network layer (layer 3) and as such, can be utilized to block all ICMP echo requests and replies over the public IP. |
| --- |

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

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

| sudo nmap -sS 161.35.96.20  [sudo] password for sysadmin:  Starting Nmap 7.80 ( https://nmap.org ) at 2023-07-29 11:09 UTC  Nmap scan report for 161.35.96.20  Host is up (0.22s latency).  Not shown: 999 closed ports  PORT STATE SERVICE  22/tcp open ssh  1 open port, Port 22 open SSH, 999 other ports closed. |
| --- |

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

| Syn scans are conducted over the Transport layer (Layer 4) as data is transmitted over TCP connections. |
| --- |

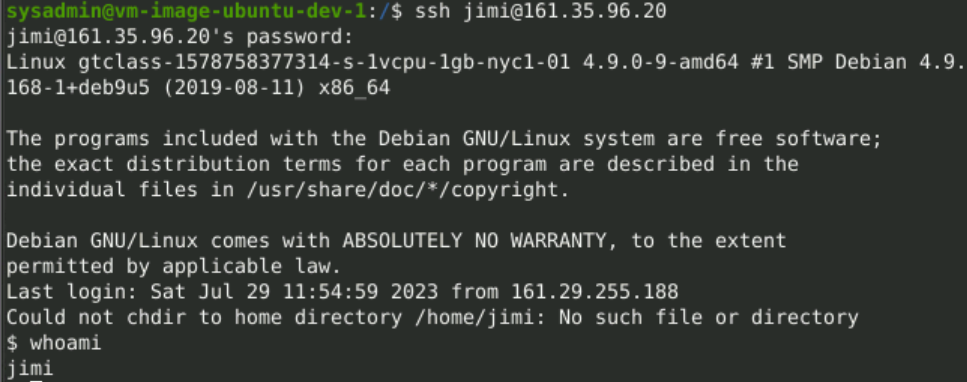
* 1. Explain how you determined which layer:

| The transport layer is in charge of end-to-end transmission and as such, sends data over the Transmission Control Protocol and User Datagram Protocol. Syn scans use a three way handshake over TCP to send a synchronization request to the server to establish a connection. |
| --- |

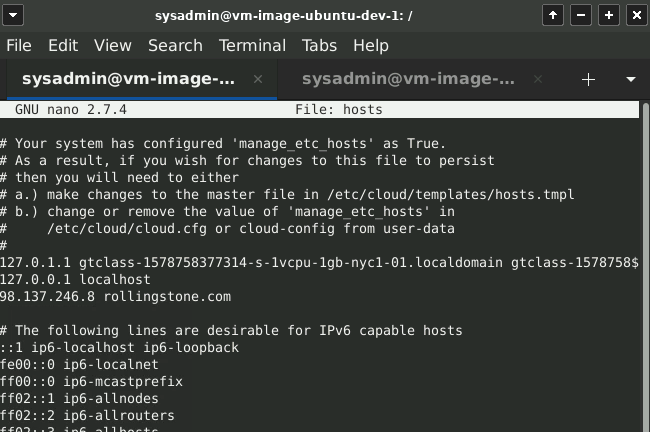
1. Mitigation suggestions (if needed):

| Nmap revealed port 22 (SSH) is open. Port 22 is the default SSH port and as such, it is highly recommended this to be changed to a seemingly random port between 1024 and 65535. Port 22 is susceptible to many hackers, as the default ports are commonly targeted during enumeration.  Additionally, if Rockstar Corp decide, they can additionally disable Port 22 in their sshd\_config file, to avoid any risk over ssh connections. |
| --- |

### 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:



| When logged in as the Jimi user (jimi@161.35.96.20) over ssh, you can analyze the contents within the local hosts file to obtain information regarding DNS entries. Upon checking the /etc/hosts file I uncovered the manual DNS entry of 98.137.246.8 for rollingstone.com. As such, this is why any user signed into RockStar Corp is being redirected to a suspicious website rather than accessing the legitimate site. |
| --- |

1. Command used to query Domain Name System records:

| nslookup 98.137.246.8 |
| --- |

1. Domain name findings:

| Using the suspicious public IP (98.137.246.8) associated with rollingstone.com in the hosts file, the nslookup tool uncovered the domain name of unknown.yahoo.com. |
| --- |

1. Explain what OSI layer DNS runs on:

| The DNS Protocol operates inside the Application Layer (layer 7) as it allows applications to translate an IP address into a Domain Name. Manipulating the hosts configuration file allows applications (chrome, or other web clients) to redirect users to the suspicious website. |
| --- |

1. Mitigation suggestions (if needed):

| Removing the manual entry inside the hosts file and saving the changes will resolve the DNS redirect issue, although this will not resolve the problem entirely, as this file would have been accessed and edited by an internal user at some point. As such, setting up auditing rules to capture file changes by users could capture who the culprit is. If this is the case, disciplinary action could be taken against this user if appropriate. Looking at the hosts file, it is clear to see that only the sudo users have access to read and write, so users editing the file is unlikely, so someone may have needed to edit this file with sudo access. Additionally, updating the read and write access to this file could deter this issue from happening again, as users should not have access to edit this file. |
| --- |



### Phase 4: *“ShARP Dressed Man”*

1. Name of file containing packets:

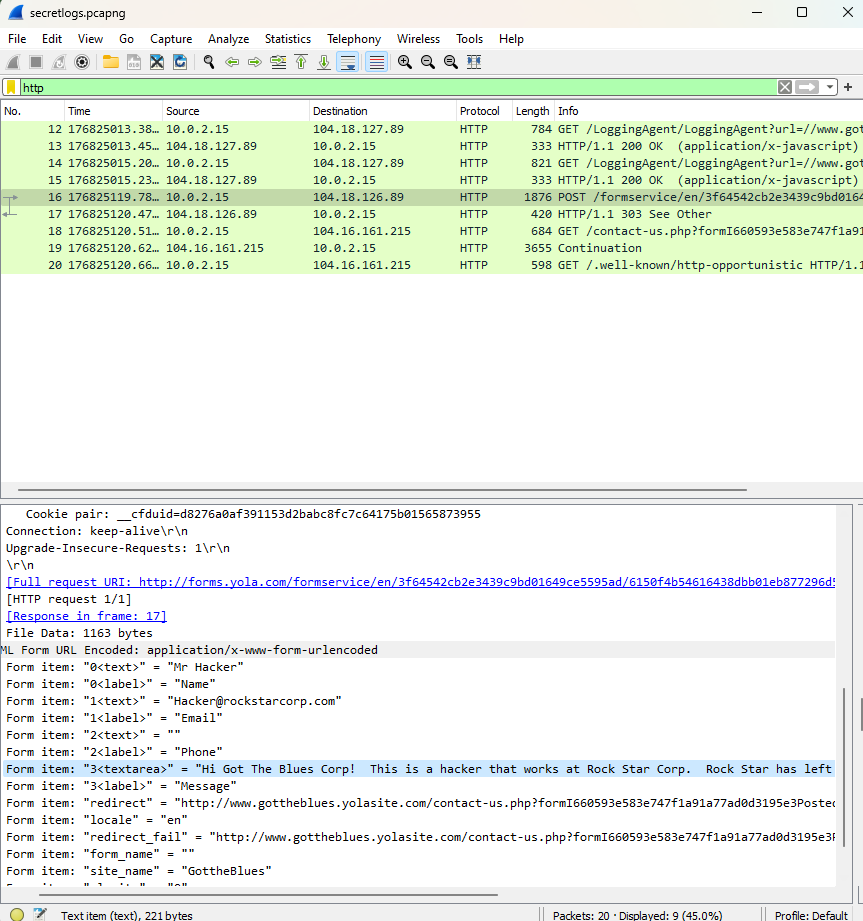
| Located in the /etc directory I was able to identify the file packetcaptureinfo.txt. Opening the contents of the file revealed a unique google drive link: <https://drive.google.com/file/d/1ic-CFFGrbruloYrWaw3PvT71elTkh3eF/view?usp=sharing> |
| --- |

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

| Opening the packet capture in wireshark revealed a series of packets capture. Searching by ‘arp’ in the filter revealed 5 ARP entries. The 5th ARP Frame identifies the Hacker has associated an additional mac address to the IP 192.168.47.200. The hacker’s Mac address appears to be 00:0c:29:1d:b3:b1.  Frame 5: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface unknown, id 1  Ethernet II, Src: VMware\_1d:b3:b1 (00:0c:29:1d:b3:b1), Dst: VMware\_fd:2f:16 (00:50:56:fd:2f:16)  Address Resolution Protocol (reply)  [Duplicate IP address detected for 192.168.47.200 (**00:0c:29:1d:b3:b1**) - also in use by 00:0c:29:0f:71:a3 (frame 4)]  [Frame showing earlier use of IP address: 4]  [Expert Info (Warning/Sequence): Duplicate IP address configured (192.168.47.200)]  [Duplicate IP address configured (192.168.47.200)]  [Severity level: Warning]  [Group: Sequence]  [Seconds since earlier frame seen: 10] |
| --- |

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

| Using the http filter, I was able to isolate the traffic using HTTP. Looking through all 9 Frames (Frame 12 - 20), I was able to find a form completion capture. In this form, I was able to locate a hidden message by the Hacker in the form items, with the below message:  "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!"  In these captures, I was also able to Identify that the hacker has an email [Hacker@rockstarcorp.com](mailto:Hacker@rockstarcorp.com), and had entered the name Mr hacker. |
| --- |



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

| HTTP resides within the Application layer (Layer 7) of the OSI Model as it is used to transmit data from a web server to a client. In this situation, the Hacker has completed a form hosted on the web application gottheblues.yoalsite.com. As such, this HTTP packet was captured allowing us to detect the information of the Hacker. If the hacker was using HTTPS (or HTTP + TLS) then the contents of the packet capture would be encrypted and difficult to read. |
| --- |

* 1. Layer used for ARP:

| ARP resides within the Data Link Layer (Layer 2) of the OSI model. The Data Link layer is in charge of establishing links between nodes using MAC addresses to send data to the correct node. ARP uses devices on the network to determine the Mac Address of nodes based on their IP Address. In this situation, ARP was used to identify that 2 devices, each with different MAC Addresses, were sharing the same IP address 192.168.47.200 on the network. |
| --- |

1. Mitigation suggestions (if needed):

| Now that we have determined the activity of the hacker, we are able to determine which device has the MAC address **00:0c:29:1d:b3:b1** and which devices are using the IP 192.168.47.200. Additionally, it may be recommended to blacklist or block this IP address so the hacker cannot pursue further with their attack. Once the culprit is found, further investigation can be conducted to determine the means of the attack, the nature of the hacker, and the outcome of the hack. |
| --- |

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