| Cybersecurity |
| --- |
| Module 8 Challenge Submission File |

## 

## **Networking Fundamentals: Rocking your Network**

Make a copy of this document to work in, and then 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 fping against the IP ranges:

| fping -asg -c 4 15.199.95.91/28  fping -asg -c 4 15.199.94.91/28  fping -asg -c 4 11.199.158.91/28  fping -asg -c 4 161.35.96.20/32  fping -asg -c 4 11.199.141.91/28  fping == stands for fast ping, and allows the ability to scan a list of hosts whereas ping just allows for one -a == output option to show targets that are alive  -s == output option to show final stats  -g == probing option to allow the use of CIDR (or to do a range of IPs)  -c == probing option to specify the number of pings sent to the target (in this case, 4) |
| --- |

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

| For the IP ranges which were provided for the Hollywood branch, almost all did not return a ping result. However, the one that did was **161.35.96.20**. |
| --- |

1. List of IPs responding to echo requests:

| The only IP that responded to an echo (ping) was:   * 161.35.96.20 |
| --- |

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

| Ping utilizes the Network layer (or Layer 3) of the OSI model, since it is utilizing IP addresses. |
| --- |

1. Mitigation recommendations (if needed):

| I would suggest that you configure your firewall to block ICMP pings, much as has been done for the other Hollywood servers. Additionally, you might want to consider looking at your router configuration and having it look for and drop any suspicious packets. While this may cause some false positives, if you are wanting to keep your server out of ping, it might be worth it. You can always white-list those IPs which are valid to let them in. |
| --- |

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

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

| 161.35.96.20:22  Port 22/tcp is in a state of Open |
| --- |

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

| Layer 4 (Transport) is where SYN scan scans are done |
| --- |

* 1. Explain how you determined which layer:

| SYN is part of the TCP 3way-handshake. Infact, it is the first step of the 3way. Since TCP is found on the Transport Layer, then the SYN Scan would be a part of the Transport Layer |
| --- |

1. Mitigation suggestions (if needed):

| Unless you have employees who regularly SSH into your network, I would suggest turning off port 22. If you do have employees who need SSH access, then I would suggest configuring it to a different port, and require a VPN and MFA in order to gain access into the system. |
| --- |

### 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:

| After SSHing into 161.35.96.20 as jimi…  cat /etc/hosts  This shows that rollingstone.com is set to go to the ip 98.137.246.8. Doing a reverse IP lookup on this, it appears to go to a website called: unknown.yahoo.com |
| --- |

1. Command used to query Domain Name System records:

| There are multiple options to do this. Just to name a few, there are:   * dig * nslookup * host   You can also do a reverse IP lookup via various different websites.  Below is a screenshot of all three and the information they provide, without any flags: |
| --- |

1. Domain name findings:

| As stated previously, when an employee at RockStar tries to go to rollingstone.com, it is sending them to the IPaddress of 98.137.246.8, which resolves to unknown.yahoo.com.  If you wanted rollingstone.com, the IPaddress is 192.0.66.114 |
| --- |

1. Explain what OSI layer DNS runs on:

| DNS operates on the Application (Layer 7) level. As stated by dnsfilter.com, “Simply put, when a client application requests that a domain name be converted into an IP address, the task is completed within the application layer by DNS”. |
| --- |

1. Mitigation suggestions (if needed):

| First, I would remove the redirect for rollingstone.com from the hosts file. Then, using the information gathered (in the next steps), continue to monitor the IP/MAC of the insider until enough information is gathered which warrants direct action with them.  If you feel that you already have enough information, then I would block that MAC on the server(s) and shutdown their access across the network. |
| --- |

### Phase 4: *“ShARP Dressed Man”*

1. Name of file containing packets:

| cat /etc/packetcaptureinfo.txt    The downloaded file is called: secretlogs.pcapng |
| --- |

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

| After opening the .pcapng file into Wireshark, I narrowed down the information to those items which gave an ARP response (arp.opcode == 2).  This allowed me to filter through things a bit more easily, whereupon I found one line which had a duplicate IP. This let me know someone had spoofed the IP, and what their MAC was.  In this case, the hacker’s MAC is: 00:0c:29:1c:b3:b1 |
| --- |

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

| Changing the filter to look at HTTP requests for POST, we are able to find a form which the hacker filled out, trying to get 1 million dollar in order to provide credentials to log in for a competitor. |
| --- |

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

| HTTP is on the Application (Layer 7) level |
| --- |

* 1. Layer used for ARP:

| ARP is used on the Data Link (Layer 2) level, where it is used to map MAC addresses to IP addresses |
| --- |

1. Mitigation suggestions (if needed):

| As stated previously, I would suggest continued monitoring of the IP/MAC of the insider until enough information is gathered which warrants direct action with them.  If you feel that you already have enough information, then I would block that MAC on the server(s) and shutdown their access across the network. |
| --- |

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.