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

### **Phase 1: *“I’d like to Teach the World to ping”***

1. Command(s) used to run fping against the IP ranges:

|  |
| --- |
| fping -g -a 15.199.95.91/28  fping -g -a 15.199.94.91/28  fping -g -a 203.0.113.32/28  fping -g -a 161.35.96.20/32  fping -g -a 192.0.2.0/28 |

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

|  |
| --- |
| fping command uses ICMP echo to figure out what the host is responding to. Fping is similar to ping but is better when pinging more than one host.  Option -g scans through the whole subnet. Option -a displays which host is alive. |

1. List of IPs responding to echo requests:

|  |
| --- |
| 161.35.96.20 |

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

|  |
| --- |
| ICMP that is used to diagnose network communication lives in layer 3 of the OSI model |

1. Mitigation recommendations (if needed):

|  |
| --- |
| Disable ICMP or have a firewall |

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

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

|  |
| --- |
| ports 21 & 22 |

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

|  |
| --- |
| Layer 4 |

* 1. Explain how you determined which layer:

|  |
| --- |
| I used the port scanning method which analyzes which ports are open and closed. It can also help analyze risks to those specific ports. |

1. Mitigation suggestions (if needed):

|  |
| --- |
| Make sure the ports are closed that are not being used |

### **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:

|  |
| --- |
| 98.137.246.8 is not reachable even after using proper credentials |

1. Command used to query Domain Name System records:

|  |
| --- |
| isnslookup rollingstone.comand |

1. Domain name findings:

|  |
| --- |
| There are no issues found in 192.0.66.114 |

1. Explain what OSI layer DNS runs on:

|  |
| --- |
| layer 7 |

1. Mitigation suggestions (if needed):

|  |
| --- |
| Make sure the DNS server is up to date and install software like BIND. |

### **Phase 4: *“ShARP Dressed Man”***

1. Name of file containing packets:

|  |
| --- |
| packetcaptureinfo.txt |

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

|  |
| --- |
| 00:0c:29:1d:b3:b1 |

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

|  |
| --- |
| The hacker was trying to send a 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 Million 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 |

* 1. Layer used for ARP:

|  |
| --- |
| Layer 2 |

1. Mitigation suggestions (if needed):

|  |
| --- |
| Scan for unused open ports and close them on a regular basis |