Networking Fundamentals Homework: Rocking your Network!

**Phase 1**

The steps and commands used to complete the tasks.

Determined the following IP address are associated with the Hollywood office:

|  |
| --- |
| 15.199.95.91/28 |
| 15.199.94.91/28 |
| 203.0.113.32/28 |
| 161.35.96.20/32 |
| 192.0.2.0/28 |

Used the following commands in terminal:

* fping -g 15.199.95.91/28
* fping -g 15.199.94.91/28
* fping -g 203.0.113.32/28
* fping -g 161.35.96.20/32
* fping -g 192.0.2.0/28

A summary of your findings for each testing phase.

15.199.95.91 - unreachable

15.199.94.91 - unreachable

203.0.113.32 - unreachable

161.35.96.20/32 - alive

192.0.2.0 - unreachable

Any network vulnerabilities discovered & findings associated with a hacker

Given that RockStar Corp has advised that it does not want any open connections, the IP address 161.35.96.20 poses as a potential vulnerability

Recommended mitigation strategy.

It is recommended to restrict all ICMP echo requests from the IP address 161.35.96.20 to prevent further successful ping requests

Document the OSI layer where the findings were found.

This has occurred on the network layer as utilising fping revolves around IP addresses, which is used on the Network Layer 3.

**Phase 2**

The steps and commands used to complete the tasks

Sudo nmap -sS 161.35.96.20/32

A summary of your findings for each testing phase.

Port 22 is the open port and is accepting connections

Document the mitigation recommendations to protect against the discovered vulnerabilities

It is recommended that RockStar Corp looked to block Port 22 as it is a network vulnerability for the company due to possibility of acceptable connections to the network via certain IP addresses

Document the OSI layer where the findings were found.

SYN scans run on transport layer (layer 4)

**Phase 3**

The steps and commands used to complete the tasks

* ssh jimi@161.35.96.20 -22
* Password: hendrix
* ping rollingstone.com
* exit
* nmap rollingstone.com
* ssh jimi@161.35.96.20 -22
* cd etc
* nano hosts

A summary of your findings for each testing phase.

Ping rollingstone.com

* This showcases that the address for connection is 151.101.192.69
* Doing this command while logged into [jimi@161.35.96.20](mailto:jimi@161.35.96.20) -22 shows there is 100% packet loss compared to when logged into sysadmin

Nmap rollingstone.com

* Confirms a number of IP address that will accept connections with 151.101.192.69, 151.101.0.69, 151.101.128.69, and 151.101.64.69 as options

/etc/hosts config file

* Hosts file shows that rollingstone.com is connecting with the IP address 98.137.246.8 which is explains why RockStar Corp while logged into @jimi is unable to access rollingstone.com

Any network vulnerabilities discovered.

* Vulnerability discovered was while logged into [jimi@161.35.96.20](mailto:jimi@161.35.96.20) -22, rollingstone.com is an unreachable connection as confirmed when using ping

Document the OSI layer where the findings were found.

Layer 3 - Network

**Phase 4**

The steps and commands used to complete the tasks.

* ssh [jimi@161.35.96.20](mailto:jimi@161.35.96.20) – 22
* cd etc
* cat packetcaptureinfo.txt
* <https://drive.google.com/file/d/1ic-CFFGrbruloYrWaw3PvT71elTkh3eF/view?usp=sharing>
* Download secretlogs.pcapng
* Open Wireshark and load secretlogs.pcapng
* Filtered Wireshark results via arp.opcode == 1 & http.request.method == "GET"

A summary of your findings for each testing phase & Any network vulnerabilities discovered.

Packetcaptureinfo.txt shows a website url:

* <https://drive.google.com/file/d/1ic-CFFGrbruloYrWaw3PvT71elTkh3eF/view?usp=sharing>
* Url direct us to a file we can download secretlogs.pcapng that we can open in Wireshark
* Reviewing the ARP filter requests, we can identify that in line one, the request was made for 192.168.47.1 with the MAC address of 00:0c:29:0f:71:a3
* However on line 5, there is a duplicate IP address detected and the hacker has provided another MAC addresses 00:0c:29:1d:b3:b1 which is a spoofed MAC address to try and gain access

Findings associated with a hacker

* When looking to filter HTTP results in Wirehark, we can identify text from the hacker has been posted on the website
* Form item: "0<text>" = "Mr Hacker" Form item: "0<label>" = "Name" Form item: "1<text>" = "Hacker@rockstarcorp.com" Form item: "1<label>" = "Email" Form item: "2<text>" = "" Form item: "2<label>" = "Phone" 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!" Form item: "3<label>" = "Message" Form item: "redirect" = "http://www.gottheblues.yolasite.com/contact-us.php?formI660593e583e747f1a91a77ad0d3195e3Posted=true" Form item: "locale" = "en" Form item: "redirect\_fail" = "http://www.gottheblues.yolasite.com/contact-us.php?formI660593e583e747f1a91a77ad0d3195e3Posted=false" Form item: "form\_name" = "" Form item: "site\_name" = "GottheBlues" Form item: "wl\_site" = "0" Form item: "destination" = "DQvFymnIKN6oNo284nIPnKyVFSVKDX7O5wpnyGVYZ\_YSkg==:3gjpzwPaByJLFcA2ouelFsQG6ZzGkhh31\_Gl2mb5PGk=" Form item: "g-recaptcha-response" = "03AOLTBLQA9oZg2Lh3adsE0c7OrYkMw1hwPof8xGnYIsZh8cz5TtLwl8uDMZuVOls6duzyYq2MTzsVHYzKda77dqzzNUwpa6F5Tu6b9875yKU1wZHpfOQmV8D7OTcx2rnGD6I8s-6qvyDAjCuS6vA78-iNLNUtWZXFJwleNj3hPquVMu-yzcSOX60Y-deZC8zXn8hu4c6u

Document the OSI layer where the findings were found.

Layer 4 - Transport