#### **Todd Peralta**

#### **Week 8 Submission Homework**

#### **Network Vulnerability Assessment**

**Phase 1**: *"I'd like to Teach the World to Ping"*

#### **Step 1: fping - g**

Create a summary file in a word document that lists out the fping command used, as well as a summary of the results.

Use fping -g on the following IP:

12.205.151.91/24 -Unreachable

15.199.151.91/24 -Unreachable

15.199.158.91/28 -Unreachable

15.199.141.91/28q -Unreachable

15.199.131.91/28 -Unreachable

15.199.121.91/28 -Unreachable

15.199.111.91/28 -Unreachable

15.199.100.91/28 -Unreachable

15.199.99.91/28 -Unreachable

15.199.98.91/28 -Unreachable

15.199.97.91/28 -Unreachable

15.199.96.91/28 -Unreachable

15.199.95.91/28 -Unreachable

15.199.94.91/28 -Unreachable

11.199.158.91/28 -Unreachable

167.172.144.11/32 -Alive

11.199.141.91/28 -Unreachable

11.199.131.91/28 -Unreachable

11.199.121.91/29 -Unreachable

11.199.111.91/28 -Unreachable

11.199.100.91/32 -Unreachable

11.199.99.91/24 -Unreachable

11.199.98.91/28 -Unreachable

1. Also indicate at which OSI layer your findings are found:

Layer 3: Network Layer

1. Document the mitigation recommendations to protect against the discovered vulnerabilities:  
   Update firewall protocols to disable to prevent ping requests from passing through the firewall. Since RockStar Corp doesn't want to respond to any requests, this is a vulnerability.
2. Mitigations include: Recommend to restrict allowing ICMP echo requests against IP 167.172.144.11/32 to prevent successful responses from PING requests and scanning ports for potential vulnerabilities.

#### **Step 2: *"Some Syn for Nothin`"***

#### **Guidelines for your Submission:**

Provide the following for each phase:

* List the steps and commands used to complete the tasks.  
  1) Use nmap -sS for SYN SCAN

2) nmap -sS 167.172.144.11/32

Finding output: PORT STATE SERVICE

List any vulnerabilities discovered:

Starting Nmap 7.60 ( https://nmap.org ) at 2021-05-07 22:21 EDT

Nmap scan report for 167.172.144.11

Host is up (0.0058s latency).

Not shown: 998 filtered ports

PORT STATE SERVICE

22/tcp open ssh

53/tcp open domain

Nmap done: 1 IP address (1 host up) scanned in 8.98 seconds

1. Document the mitigation recommendations to protect against the discovered vulnerabilities:  
   You can scan for and close open ports that are exchanging information on their networks. If an organization has more open ports than the average organization in its industry, it’s more likely to experience a data breach.
2. Document the OSI layer where the findings were found.  
   Transport Layer - when using SYN you are using the 3-way handshake.

**Phase 3: *"I Feel a DNS Change Comin' On"***

**Step 1: SSH Into Jimi’s account**

$ ssh jimi@167.172.144.11

Password: hendrix

**Step 2: Look through files to find the configuration file, record the entry that is set to rollingstone.com.**

$ cd etc

(optional) $cd ssh

$cat hosts

Found output:

$98.137.246.8 rollingstone.com

Step 2a)

$cd etc

$more packetcaptureinfo.txt

Found output:

https://drive.google.com/file/d/1ic-CFFGrbruloYrWaw3PvT71elTkh3eF/view?usp=sharing

**Step 3: Terminate your ssh session to the rollingstone server, and use nslookup to determine the real domain of the IP address you found from the previous step.**

$ exit (terminate ssh)

$ nslookup 98.137.246.8

Output: 8.246.137.98.in-addr.arpa name = unknown.yahoo.com.

1. List any vulnerabilities discovered:  
   RockStar typically uses the same default usernames and passwords for most of their servers. I would change this so there are no default usernames and passwords that are the same and this effect will be more secure for their servers.

1. Document the mitigation recommendations to protect against the discovered vulnerabilities.  
   The username and passwords should be changed to be unique for each server. Being able to ssh into port 22 should be a concern for Rock Star Corp.

1. Document the OSI layer where the findings were found.

Application Layer 7

### **Phase 4: *"ShARP Dressed Man"***

Within the RockStar server that you SSH'd into, and in the same directory as the configuration file from **Phase 3**, the hacker left a note as to where he stored away some packet captures.

* View the file to find where to recover the packet captures.
* These are packets that were captured from the activity in the Hollywood Office.
* Use Wireshark to analyze this pcap file and determine if there was any suspicious activity that could be attributed to a hacker.  
  + **Hint**: Focus on the ARP and HTTP protocols. Recall the different types of HTTP request methods and be sure to thoroughly examine the contents of these packets.
* Add your findings in your summary and be sure to indicate at which OSI layer they were found.

**Packet Capture Findings:**

Filters used:

http.request.method == GET

http.request.method == POST

HTTP capture:

* Visited www.gottheblues.yolasite.com
* Packet 16 has chat logs: = "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!"

ARP Capture:

* Duplicate IP addresses on packet 5

**Packet Capture Findings:**

1. List any vulnerabilities discovered.  
   Looks like the hacker got into Rock Star Corps systems and requested $1 million from their competitor Got The Blues Corp. The hacker exploited port 22 and created multiple problems for the company.
2. List any findings associated with a hacker.  
   Listed in ARP and HTTP Captures above.
3. Document the mitigation recommendations to protect against the discovered vulnerabilities.  
   Scan and secure their ports and scan for any irregular traffic in their networks. Look through packet captures and monitor irregular behaviour.

1. Document the OSI layer where the findings were found.

Layer 2: Data Link