**Networking Fundamentals Homework: Rocking your Network!**

**Phase 1:**

Hollywood servers:

| 15.199.95.91/28 | Hollywood Database Servers |
| --- | --- |
| 15.199.94.91/28 | Hollywood Web Servers |
| 11.199.158.91/28 | Hollywood Web Servers |
| 167.172.144.11/32 | Hollywood Application Servers |
| 11.199.141.91/28 | Hollywood Application Servers |

fping results on each subnet:

sysadmin@UbuntuDesktop:~$ fping -s -g 15.199.95.91/28

15.199.95.81 is unreachable

15.199.95.82 is unreachable

15.199.95.83 is unreachable

15.199.95.84 is unreachable

15.199.95.85 is unreachable

15.199.95.86 is unreachable

15.199.95.87 is unreachable

15.199.95.88 is unreachable

15.199.95.89 is unreachable

15.199.95.90 is unreachable

15.199.95.91 is unreachable

15.199.95.92 is unreachable

15.199.95.93 is unreachable

15.199.95.94 is unreachable

14 targets

0 alive

14 unreachable

0 unknown addresses

14 timeouts (waiting for response)

56 ICMP Echos sent

0 ICMP Echo Replies received

0 other ICMP received

0.00 ms (min round trip time)

0.00 ms (avg round trip time)

0.00 ms (max round trip time)

4.253 sec (elapsed real time)

sysadmin@UbuntuDesktop:~$ fping -s -g 15.199.94.91/28

15.199.94.81 is unreachable

15.199.94.82 is unreachable

15.199.94.83 is unreachable

15.199.94.84 is unreachable

15.199.94.85 is unreachable

15.199.94.86 is unreachable

15.199.94.87 is unreachable

15.199.94.88 is unreachable

15.199.94.89 is unreachable

15.199.94.90 is unreachable

15.199.94.91 is unreachable

15.199.94.92 is unreachable

15.199.94.93 is unreachable

15.199.94.94 is unreachable

14 targets

0 alive

14 unreachable

0 unknown addresses

14 timeouts (waiting for response)

56 ICMP Echos sent

0 ICMP Echo Replies received

0 other ICMP received

0.00 ms (min round trip time)

0.00 ms (avg round trip time)

0.00 ms (max round trip time)

4.350 sec (elapsed real time)

sysadmin@UbuntuDesktop:~$ fping -s -g 11.199.158.91/28

11.199.158.81 is unreachable

11.199.158.82 is unreachable

11.199.158.83 is unreachable

11.199.158.84 is unreachable

11.199.158.85 is unreachable

11.199.158.86 is unreachable

11.199.158.87 is unreachable

11.199.158.88 is unreachable

11.199.158.89 is unreachable

11.199.158.90 is unreachable

11.199.158.91 is unreachable

11.199.158.92 is unreachable

11.199.158.93 is unreachable

11.199.158.94 is unreachable

14 targets

0 alive

14 unreachable

0 unknown addresses

14 timeouts (waiting for response)

56 ICMP Echos sent

0 ICMP Echo Replies received

0 other ICMP received

0.00 ms (min round trip time)

0.00 ms (avg round trip time)

0.00 ms (max round trip time)

4.334 sec (elapsed real time)

sysadmin@UbuntuDesktop:~$ fping -s -g 167.172.144.11/32

167.172.144.11 is alive

1 targets

1 alive

0 unreachable

0 unknown addresses

0 timeouts (waiting for response)

1 ICMP Echos sent

1 ICMP Echo Replies received

0 other ICMP received

237 ms (min round trip time)

237 ms (avg round trip time)

237 ms (max round trip time)

0.238 sec (elapsed real time)

sysadmin@UbuntuDesktop:~$ fping -s -g 11.199.141.91/28

11.199.141.81 is unreachable

11.199.141.82 is unreachable

11.199.141.83 is unreachable

11.199.141.84 is unreachable

11.199.141.85 is unreachable

11.199.141.86 is unreachable

11.199.141.87 is unreachable

11.199.141.88 is unreachable

11.199.141.89 is unreachable

11.199.141.90 is unreachable

11.199.141.91 is unreachable

11.199.141.92 is unreachable

11.199.141.93 is unreachable

11.199.141.94 is unreachable

14 targets

0 alive

14 unreachable

0 unknown addresses

14 timeouts (waiting for response)

56 ICMP Echos sent

0 ICMP Echo Replies received

0 other ICMP received

0.00 ms (min round trip time)

0.00 ms (avg round trip time)

0.00 ms (max round trip time)

4.272 sec (elapsed real time)

In the above fping command, if -a switch is used along with others, it would just show the live hosts instead of listing all the hosts.

As per the objective of the task it is determined that all server subnets need to be scanned with fping. As demonstrated above, the command usage is fping -s -g 11.199.158.91/28

**Observation**:

The /32 subnet would have a single host so the command could be either fping -s 167.172.144.11 or fping -s -g 167.172.144.11/32.

**Vulnerabilities**:

As per the above results, it seems that the application server with IP address 167.172.144.11 is the only server that is accepting connections. Since RockStar Corp doesn’t want to respond to any requests, this is a vulnerability.

**Mitigation**:

* It is recommended to restrict the application server 167.172.144.11 from responding to ICMP requests.

**OSI Layers:**

* As fping is using ICMP protocol to determine if the host is alive and responding, it is working in the Network layer which is layer 3 in OSI model.

**Phase 2:**

sysadmin@UbuntuDesktop:~$ sudo nmap -sS 167.172.144.11

[sudo] password for sysadmin:

Starting Nmap 7.60 ( https://nmap.org ) at 2021-07-31 03:00 EDT

Nmap scan report for 167.172.144.11

Host is up (0.017s latency).

Not shown: 997 filtered ports

PORT STATE SERVICE

22/tcp open ssh

1723/tcp closed pptp

5060/tcp closed sip

Nmap done: 1 IP address (1 host up) scanned in 15.90 seconds

As per the objective of the task, it is determined that the ip address to scan is 167.172.144.11 using nmap for any open ports.

As per the result above, only port 22 is open for ssh connections. Since RockStar Corp don’t want any server responding to any requests, this is a vulnerability.

**Mitigation:**

* It is recommended to close port 22 to prevent this server from responding.

**OSI Layers:**

* As nmap uses tcp, udp, sctp and icmp which are transport layer protocols, this operates at layer 4 of the OSI model.

**Phase 3:**

sysadmin@UbuntuDesktop:~$ ssh jimi@167.172.144.11

jimi@167.172.144.11's password:

Linux GTscavengerHunt 4.9.0-11-amd64 #1 SMP Debian 4.9.189-3+deb9u1 (2019-09-20) x86\_64

The programs included with the Debian GNU/Linux system are free software;

the exact distribution terms for each program are described in the

individual files in /usr/share/doc/\*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent

permitted by applicable law.

Last login: Sat Jul 31 06:58:41 2021 from 122.148.220.47

Could not chdir to home directory /home/jimi: No such file or directory

$ cat /etc/hosts

# Your system has configured 'manage\_etc\_hosts' as True.

# As a result, if you wish for changes to this file to persist

# then you will need to either

# a.) make changes to the master file in /etc/cloud/templates/hosts.tmpl

# b.) change or remove the value of 'manage\_etc\_hosts' in

# /etc/cloud/cloud.cfg or cloud-config from user-data

#

127.0.1.1 GTscavengerHunt.localdomain GTscavengerHunt

127.0.0.1 localhost

98.137.246.8 rollingstone.com

oooooooollowing lines are desirable for IPv6 capable hosts

::1 ip6-localhost ip6-loopback

fe00::0 ip6-localnet

ff00::0 ip6-mcastprefix

ff02::1 ip6-allnodes

ff02::2 ip6-allrouters

ff02::3 ip6-allhosts

$ id

uid=1010(jimi) gid=1010(jimi) groups=1010(jimi)

$ ls -l /etc/hosts

-rw-r--r-- 1 root root 648 Mar 18 2020 /etc/hosts

$ ls -l /etc/hosts

-rw-r--r-- 1 root root 648 Mar 18 2020 /etc/hosts

$ vi /etc/hosts

jimi@GTscavengerHunt:/$ id

uid=1010(jimi) gid=1010(jimi) groups=1010(jimi)

jimi@GTscavengerHunt:/$ nano /etc/hosts

Unable to create directory /home/jimi/.nano: No such file or directory

It is required for saving/loading search history or cursor positions.

Press Enter to continue

jimi@GTscavengerHunt:/$ nano /etc/hosts

Unable to create directory /home/jimi/.nano: No such file or directory

It is required for saving/loading search history or cursor positions.

Press Enter to continue

jimi@GTscavengerHunt:/$ vi /etc/hosts

jimi@GTscavengerHunt:/$ id

uid=1010(jimi) gid=1010(jimi) groups=1010(jimi)

jimi@GTscavengerHunt:/$ visudoers

bash: visudoers: command not found

jimi@GTscavengerHunt:/$ sudo visudoers

[sudo] password for jimi:

jimi is not in the sudoers file. This incident will be reported.

jimi@GTscavengerHunt:/$ useradd jimi -g sudo

bash: useradd: command not found

jimi@GTscavengerHunt:/$ man adduser

bash: man: command not found

jimi@GTscavengerHunt:/$ exit

exit

shell returned 127

Press ENTER or type command to continue

jimi@GTscavengerHunt:/$ exit

exit

Press ENTER or type command to continue

$ exit

Connection to 167.172.144.11 closed.

sysadmin@UbuntuDesktop:~$ nslookup rollingstone.com

Server: 8.8.8.8

Address: 8.8.8.8#53

Non-authoritative answer:

Name: rollingstone.com

Address: 151.101.128.69

Name: rollingstone.com

Address: 151.101.64.69

Name: rollingstone.com

Address: 151.101.0.69

Name: rollingstone.com

Address: 151.101.192.69

sysadmin@UbuntuDesktop:~$ nslookup 98.137.246.8

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

Authoritative answers can be found from:

sysadmin@UbuntuDesktop:~$

As observed in the previous phase, port 22 is open for ssh communication and we can access it by using the given credentials in this phase. The command to use is ssh jimi@167.172.144.11 as demonstrated above.

It looks like the /etc/hosts file has been modified as we can see the entry for rollingstone.com on line 10 of the file. Also the nslookup tool indicates that the ip addresses for rollingstone.com is/are different from what was saved under /etc/hosts file as demonstrated above. This explains the random web pages being displayed when trying to access this domain.

The real domain of the set ip address 98.137.246.8 seems to be unknown.yahoo.com as per the nslookup output above.

The possibilities of the entry under hosts file could be:

1. An administrator might have done intentionally/unintentionally
2. A hacker might have modified the file to redirect all users who are accessing the aforementioned website to a compromised site.

**Observations:**

* Same default password being used on all servers
* hosts file is modified with the entry for rollingstone.com
* Users are being redirected to an unknown site when they are trying to access rollingstone.com
* It seems the default account don’t have root access to edit the hosts file, so obviously the attacker has gained root access and might still hold it.
* As we didn’t see any other domain entries in the hosts file, it is safe to assume that DNS server is in operation on the network.

**Vulnerabilities:**

* As it is known that a default password is used on all servers and it looks like this application server is hacked, there are chances that others might have been compromised as well. Even if there is no known indication of being compromised, there is a possibility of dormant threat.
* As the hosts file is modified and the default account don’t have

**Mitigation:**

* Should change the account passwords
* Prune the accounts for old employees
* Prune users with sudo access
* Monitoring and restoring unwanted system file changes at regular intervals.
* As it seems that a DNS server is in use, unless company have a habit of changing hosts files on the clients, it might be worth making a daily routine to restore hosts file on all the clients.
* Log file monitoring to trace the user who did the changes and following up the purpose of the change.

**OSI Layer:**

* SSH is a layer 7 protocol
* DNS is a layer 7 protocol

**Phase 4:**

jimi@GTscavengerHunt:/home/matt.ryan/falcons$ ls -l /etc/ | grep 'pack'

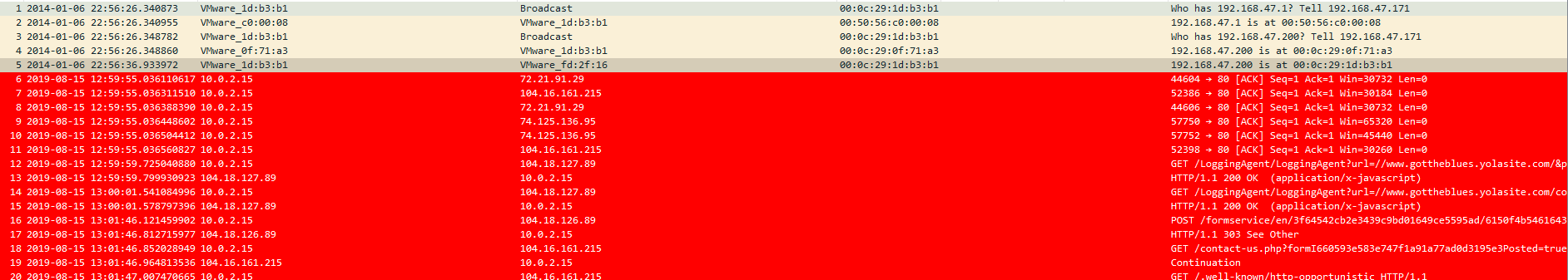
-rw-r--r-- 1 root root 112 Mar 18 2020 packetcaptureinfo.txt

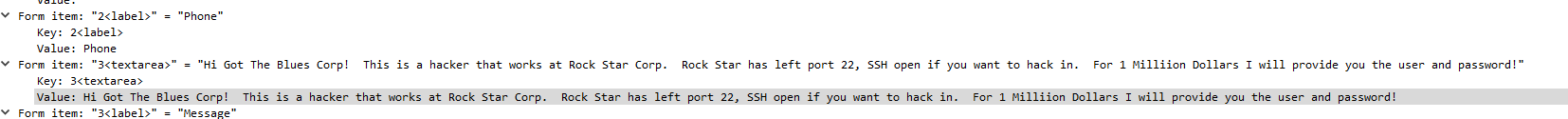
jimi@GTscavengerHunt:/home/matt.ryan/falcons$ cat /etc/packetcaptureinfo.txt

Captured Packets are here:

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

jimi@GTscavengerHunt:/home/matt.ryan/falcons$





**Observations:**

* It looks like the hacker have stored the packet capture on google drive on 16th Aug 2019 @ 12:16AM (not sure of the timezone, guessing it’s local timezone)
* Upon analysing the packet capture, it seems the packet capture has some old and some new information.
  + There was ARP poisoning done back in 2014 and
  + HTTP traffic with form submission about the hacking and open ssh port recently in 2019.
  + Also, the machine that advertised that it’s ip address as 192.168.47.200, never asked by any machine or by the destination computer that it sent the communication to.
  + Additionally, both the subnets are different
* It doesn’t make sense why the hacker would have saved packet capture of his own communication and saved the information about it on the same server..

**Vulnerabilities:**

* As per the message in form submission, Mr Hacker’s is an employee who has ill intentions.
* His Intention was to give unsolicited access to RockStar Corp in return for the money.
* Leaving port 22 open for intruders could lead to unexpected visitors.

**Mitigation:**

* Port monitoring
* Closure of any unwanted ports, in this case port 22
* Log file monitoring to trace the user who did the changes and following up the purpose of the change.

**OSI Layer:** in this phase, the transactions are done on

* Packet capture - Layer 7
* File Upload to google drive - Layer 7
* ARP poisoning - ARP operates between Layer 2 and 3
* HTTP - Layer 7