Unit 8 Homework

Glenn Parnell

# PHASE 1

## INVESTIGATION

The provided xls suggested that the Hollywood Servers to scan were the IPs/Ranges:

15.199.94.91/28 - Hollywood Web Servers

11.199.158.91/28 - Hollywood Web Servers

167.172.144.11/32 - Hollywood Application Server

11.199.141.91/28 - Hollywood Application Servers

**sysadmin@UbuntuDesktop:~$** fping -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

**sysadmin@UbuntuDesktop:~$** fping -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

**sysadmin@UbuntuDesktop:~$** fping -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

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

167.172.144.11 is alive

**sysadmin@UbuntuDesktop:~$** fping -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

## SUMMARY

I appears that the only host responding to ping is 167.172.144.11

ICMP packets are technically Layer3 in the OSI model, however there is some conjecture as to if they overlap into Layer4.

## MITIGATION

Simplest mitigation for this exposure is to block ICMP at the firewall. Alternatively, required domains could be whitelisted.

# PHASE 2

## INVESTIGATION

**sysadmin@UbuntuDesktop**:~$ sudo nmap 167.172.144.11 -sS

Starting Nmap 7.60 ( https://nmap.org ) at 2021-07-18 00:51 EDT

Nmap scan report for 167.172.144.11

Host is up (0.00019s latency).

Not shown: 810 filtered ports, 189 closed ports

PORT STATE SERVICE

22/tcp open ssh

Nmap done: 1 IP address (1 host up) scanned in 1329.81 seconds

## SUMMARY

TCP communicates via the flags SYN, ACK & FIN. The confirmation we receive that port 22 is ‘open’ is via these flags therefore the results of our SYN SCAN are bound to Layer4 of the OSI model.

## MITIGATION

Port 22 for SSH should never really be left open to the public. Whitelisting the SRC domains required is an option.

# PHASE 3

## INVESTIGATION

**sysadmin@UbuntuDesktop:~$** ssh jimi@167.172.144.11

The authenticity of host '167.172.144.11 (167.172.144.11)' can't be established.

ECDSA key fingerprint is SHA256:mDZ8+Ud+K3Y6XNWvtyAR4Q2ti1+/V3p0Bm83hF6Ua4w.

Are you sure you want to continue connecting (yes/no)? yes

Warning: Permanently added '167.172.144.11' (ECDSA) to the list of known hosts.

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 17 21:44:06 2021 from 98.194.104.91

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

**$** exit

Connection to 167.172.144.11 closed.

**sysadmin@UbuntuDesktop:~$** nslookup 98.137.245.8

8.245.137.98.in-addr.arpa name = new-netdb-ng-hv02.netops.gq1.yahoo.com.

## SUMMARY

The cause of requests to rollingstone.com being redirected was that the hosts file had been adjusted, bypassing the network assigned DNS server with a locally defined IP address for the domain to resolve to.

DNS resides in Layer7 within the OSI model, as it is involved with applications making queries.

## MITIGATION

Changes to this file should be prevented by the employ of suitable access controls. Further monitoring should also be done to ensure the integrity of the file.

# PHASE 4

## INVESTIGATION

**$** ls -la /etc | grep packet

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

**$** cat /etc/packetcaptureinfo.txt

Captured Packets are here:

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

Analysis of the packet capture showed that a 'hacker' used a HTTP POST action to send infromation to an external source:

"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!"

The ARP records showed that there was a host on the network with a duplicate IP address, possibly a malicious entity.

## SUMMARY

The hacker has notified an external source that SSH on port 22 is open. Furthermore they are attempting to sell credentials for a price. This notification was performed via an application, using HTTP which is a Layer7 component.

## MITIGATION

Available mitigations of this communication itself are fairly minimal. Whilst ‘blacklisting’ of certain domains could be employed, the transmission of data from within the network to an external source is usually based around the type data. In this case a simple text message would be extremely hard to mitigate.

Two possible mitigations for the duplicate IP issue are adjusting DHCP settings and whitelisting MAC addresses .