# Phase 1

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **IP Range** | **Location** | **Fping command** | **Fping command Output** | **IPs Accepting connections** |
| 15.199.95.91/28 | Hollywood Database Servers | fping -s -g 15.199.95.80 15.199.95.95 | 16 targets  0 alive  16 unreachable  0 unknown addresses | None |
| 15.199.94.91/28 | Hollywood Web Servers | fping -s -g 15.199.94.80 15.199.94.95 | 16 targets  0 alive  16 unreachable  0 unknown addresses | None |
| 11.199.158.91/28 | Hollywood Web Servers | fping -s -g 11.199.158.80 11.199.158.95 | 16 targets  0 alive  16 unreachable  0 unknown addresses | None |
| 167.172.144.11/32 | Hollywood Application Servers | fping -s 167.172.144.11 | 1 targets  1 alive  0 unreachable  0 unknown addresses | 167.172.144.11 |
| 11.199.141.91/28 | Hollywood Application Servers | fping -s -g 11.199.141.80 11.199.141.95 | 16 targets  0 alive  16 unreachable  0 unknown addresses | None |

## Phase 1 findings summary:

Determined a potential vulnerability that IP 167.172.144.11 is responding to Ping ICMP echo requests. Since RockStar Corp doesn't want to respond to any requests, this is a vulnerability.

Recommend to restrict allowing ICMP echo requests against IP 167.172.144.11 to prevent successful responses from PING requests.

This occurred on the network layer (Layer 3 of OSI Model) as Ping uses IP addresses and IPs are used on the Network Layer.

# Phase 2

|  |  |  |
| --- | --- | --- |
| **IPs Accepting connections** | **SYN SCAN Command** | **SYN SCAN Results** |
| 167.172.144.11 | sudo nmap -sS 167.172.144.11 | sysadmin@UbuntuDesktop:~$ sudo nmap -sS 167.172.144.11  Starting Nmap 7.60 ( https://nmap.org ) at 2020-11-01 14:34 EST  Nmap scan report for 167.172.144.11  Host is up (0.011s latency).  Not shown: 999 filtered ports  PORT STATE SERVICE  22/tcp open ssh  Nmap done: 1 IP address (1 host up) scanned in 5.60 seconds |

## Phase 2 findings summary:

Determined a potential vulnerability that Port 22 is open on IP 167.172.144.11

From Syn Scan, it appears like this port is for SSH and is accepting SSH connections. This is a vulnerability because it provides SSH terminal access to anyone over a Public IP address.

Recommend closing this port 22 or if access to this port is required then put this server inside an internal network with a private IP.

This occurred on the transport layer (Layer 4 of OSI Model) as SSH uses TCP.

# Phase 3

|  |  |  |
| --- | --- | --- |
| **IPs and Port Accepting connections** | **Login Command** | **SYN SCAN Results** |
| 167.172.144.11 22 | ssh jimi@167.172.144.11  (port is not required explicitly since ssh uses port 22 by default)  OR  ssh jimi@167.172.144.11 -p 22 | sysadmin@UbuntuDesktop:~$ ssh jimi@167.172.144.11 -p 22  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: Sun Nov 1 19:56:28 2020 from 73.223.89.101  Could not chdir to home directory /home/jimi: No such file or directory  $ |

## Phase 3 findings summary:

Determined from /etc/hosts file on RockStar Corp server (167.172.144.11) that it had an entry as below:

98.137.246.8 rollingstone.com

From the above entry, it appears like the hacker modified the hosts file to redirect requests going to rollingstone.com to 98.137.246.8

On doing nslookup on 98.137.246.8 , it resolves to media-router-fp72.prod.media.vip.gq1.yahoo.com

sysadmin@UbuntuDesktop:~$ nslookup 98.137.246.8

8.246.137.98.in-addr.arpa name = media-router-fp72.prod.media.vip.gq1.yahoo.com.

Authoritative answers can be found from:

However, when doing nslookup on rollingstone.com from outside RockStar Corp server (167.172.144.11) , it resolves to addresses as listed below:

sysadmin@UbuntuDesktop:~$ nslookup rollingstone.com

Server: 127.0.0.53

Address: 127.0.0.53#53

Non-authoritative answer:

Name: rollingstone.com

Address: 151.101.64.69

Name: rollingstone.com

Address: 151.101.192.69

Name: rollingstone.com

Address: 151.101.128.69

Name: rollingstone.com

Address: 151.101.0.69

This is a vulnerability because it redirects users to an unintended website.

Recommend fixing the /etc/hosts file with either the correct IP addresses or removing the entry altogether and rely on Name Server to resolve the name.

The file /etc/hosts can only be modified by a user who has sudo privilege, thus it looks like the hacker either has sudo privilege or root access or is using the account of a user who has sudo privilege.

This occurred on the application layer (Layer 7 of OSI Model) as the change in /etc/hosts affects DNS which is an application and thus runs on layer 7.

# Phase 4

Command to find file to view capture packets

$ cat packetcaptureinfo.txt

Captured Packets are here:

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

## Phase 4 findings summary:

Findings from secretlogs.pcapng

* Wireshark Filter : arp && arp.duplicate-address-detected
  + 1 packet identified
    - [Duplicate IP address detected for 192.168.47.200 (00:0c:29:1d:b3:b1) - also in use by 00:0c:29:0f:71:a3 (frame 4)]
    - This means that the hacker has potentially executed ARP spoofing
* Wireshark Filter : http && http.request.method==POST
  + 1 packet identified
    - Under HTML Form URL Encoded: application/x-www-form-urlencoded, we can view Form Data which says:

HTML Form URL Encoded: application/x-www-form-urlencoded

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

This is a vulnerability because the hacker has executed ARP spoofing and is also planning to sell access information to RockStar Corp server.

Recommend fixing as below:

* ARP spoofing can be fixed by a network administrator who can create Static ARP entries which map permanent IP-to-MAC addresses
* Close port 22 on identified server
* Change default username and password for RockStar Corp servers

ARP spoofing occurred on the Data link layer (Layer 2 of OSI Model) as the hacker sent a spoof ARP message to the LAN, directing all traffic intended for the good host to the hacker’s MAC address.