PHASE 1

1. I already had fping install, but the command to do so was sudo apt install fping
2. I used the command fping15.199.95.91/28 15.199.94.91/28 and so on until I got to 167.172.144.11/32 and it came back “alive” all others came back “unreachable”
3. I then used the command fping -s -g 167.172.144.11/32 and got back

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

51.3 ms (min round trip time)

51.3 ms (avg round trip time)

51.3 ms (max round trip time)

0.051 sec (elapsed real time)

1. From the results I got back I don’t know for sure about this, but i’d say 167.172.144.11/32 since it is reachable and accepting pings that it might be vulnerable and potentially putting RockStar Corp at risk.
2. I believe it is OSI Layer 3: Network. That layer utilizes ping and traceroute.

Vulnerabilities: The 167.172.144.11 is alive and vulnerable and is a risk to the company. Also from unauthorized users.

Hacker Associations: so far I just see that it is suspicious that it’s alive and there is no proof that it is a hacker.

Recommendations: 167.172.144.11 is accepting pings which I’m sure RockStar Corp doesn’t want to respond to any requests so that’s why it is susceptible to a hacker. It is a huge risk to the company and you don’t want any servers to be “alive” and make sure all ports are closed.

PHASE 2

1. I used the command sudo nmap -sS 167.172.144.11/32 to SYN SCAN on the IP Address that was alive in Phase 1.
2. I got back

Starting Nmap 7.60 ( https://nmap.org ) at 2022-04-19 22:26 EDT

Nmap scan report for 167.172.144.11

Host is up (0.0036s 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 19.46 seconds

1. From what I got back I saw that 22/tcp is open and probably shouldn’t be.
2. OSI Layer 4: Transport. Since Transport does protocols for TCP and UDP and how they establish a connection with the three-way handshake.

Vulnerabilities: Port 22 TCP is open and it shouldn’t be. It should be closed.

Hacker associations: since the Port 22 is open it’s definitely a little suspicious.

Recommendations: Close the port so no one can get into it.

PHASE 3

1. Port 22 is open on 167.172.144.11 so I ssh into it using the default username and password that is on most of their servers. So I used sudo ssh jimi@167.172.144.11 -p22

And the password hendrix.

1. I ran the ls command to list the directors, cd into etc, ls and then cat hosts to get 127.0.1.1 GTscavengerHunt.localdomain GTscavengerHunt

127.0.0.1 localhost

98.137.246.8 rollingstone.com

1. Next I hit ctrl d to exit the ssh and do a nslookup on 98.137.246.8 to determine the real domain of the IP address. nslookup 98.137.246.8

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

Authoritative answers can be found from:

1. OSI Layer 7: Application.

Vulnerabilities: The fact i’m able to ssh into 167.172.144.11 -p22 is a concern. They shouldn’t use default usernames and passwords for their servers.

Hacker associations: hacked the DNS and changed the host to a different website to send us on a chase.

Also it says unknown.yahoo.com and not media.

Recommendations: Change the IP address back to the preferred one. Close the port 22 and make 167.172.144.11 unreachable. Add DNS filter.

PHASE 4:

1. I ran the command sudo ssh jimi@167.172.144.11 -p22

ls

cd etc

ls

Cat packetcaptureinfo.txt

I copied the link that was in there and opened up my mozilla browser and then opened the file with wireshark.

1. Inside wireshark I used http.request.method ==”GET”

And then I got 4 packets and then did http.request.method ==”POST”

I found the hackers information in the HTML and the secret code that said he was asking for 1 million dollars for the username and password.

1. I ran “arp” and found the duplicated IP address which tells me that he changed the MAC address.
2. OSI Layer 7: Application.

Vulnerabilities: I took a screenshot

Hacker associations: I took a screenshot

Recommendations: Don’t use the same username and passwords create some password policies to prevent easy cracking.

Don’t use default admin logins so that you can see who logins specifically.

Monitor logins.

|  |
| --- |

|  |
| --- |