HW8 RockStar Network Vulnerability Assessment

Ralph Pursifull
Network Security Analyst

Summary by Phase

1. Hollywood Office IPs and PING
    a. A RockStar **server responds to ICMP** echo req, violating RockStar policy. **Later investigation shows this to be a backdoor with access for sale at $1M.**
    b. Use of **publicly routable IPv4 addresses on systems with no apparent firewall**, and that do not need to be publicly accessible, is a very high risk. Review designs of all RockStar site networks.

2. Open ports on 167.172.144.11
    a. SSH port is open on 167.172.144.11 in violation of RockStar network policy.
    b. NMAP shows many ports are “FILTERED”. These should be converted to “CLOSED” by a properly configured hardware firewall. The firewall will be an additional level of protection in the network, independent of the server configuration. If possible, they should be administered by different people.

3. SSH and NSLOOKUP
    a. Erroneous changes to the network configuration of 167.172.144.11 may be part of a man in the middle attack working to spy on communications with rollingstone.com. It could also be a way to obscure unauthorized data transfers to RollingStone. Investigation is underway to see how this is actually being used.

4. Packets and WIRESHARK
    a. The SSH backdoor is confirmed. An internal actor is attempting to sell credentials and access for $1M.
    b. A duplicate IP situation could be an attempt to intercept data intended for another system. This is still under investigation.

Phase 1. Hollywood Office IPs and PING

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

STEPS TAKEN

Reviewed the list of RockStar servers and ran this script.

```
#!/bin/bash
for i in 15.199.95.91/28 15.199.94.91/28 11.199.158.91/28 \
     167.172.144.11/32 11.199.141.91/28 ;
do
  echo $i
  fping -c 2 -a -g ${i}   # scan all Hollywood IP addresses
  echo
done
```

RESULTS

A. One IPv4 address: 168.172.144.11 responded to ICMP echo requests.

B. All other listed Hollywood IP addresses (15.199.95.91/28 15.199.94.91/28 11.199.158.91/28 11.199.141.91/28) did not respond to ICMP echo requests, but they do have externally routable IP addresses for no known reason.

VULNERABILITIES DISCOVERED

A. RockStar Corp does not want servers to indicate they are accepting connections. The ICMP response from 168.172.144.11 violates that. So this is a vulnerability.

B. All RockStar Corp servers are documented as having externally routable IPv4 addresses. This is a missed opportunity to use Network Address Translation with private iPv4 addresses hidden from the public internet. NAT configuration would make incoming backdoor access more difficult for hackers to configure, as they need to breach both the server and the network firewall/router.

HACKER / SECURITY IMPLICATIONS

A. ICMP response is not part of the design so perhaps a hacker has reconfigured the network for evil purposes.

B. Potential hackers do not need to breach and reconfigure a firewall to knock on the door of RockStar servers. One accidental service installation on a server or one malicious act by a hacker on an internal system can provide ongoing access.

RECOMMENDED MITIGATIONS

A. After this study is complete, install a physical firewall and configure it to block ICMP from all external IP addresses. If ICMP requests are needed internally to facilitate network monitoring and troubleshooting, review RockStar policy and consider these recommendations from blog.Paessler.com. Scroll down to: “How to use ICMP and SNMP while maintaining a focus on security”. If needed for WAN troubleshooting, RockStar could consider adopting a policy where ICMP

responses from the router's IPv4 address are acceptable.

B. Review the design of all RockStar site neworks. Place any servers that need to be accessed from the public internet, behind a firewall in a DMZ. Place servers that do not need to be accessed from the public internet in an internal network that is also protected by a firewall.

OSI Layer
Fping is a utility running at OSI Application Layer 7 used to verify operation of the ICMP protocols at OSI Network Layer 3. The recommendations provided include changes from the Physical Layer 1 (firewall installation), Network Layer 3 (NAT), and Transport Layer 4 (internal IP Addresses).

Phase 2. Open ports on 167.172.144.11

We want to find open ports on 167.172.144.11, so we will use this Linux command:

STEPS TAKEN

```
sudo nmap -sS 167.172.144.11
```

RESULTS
Output of the TCP SYN Scan:

```
Starting Nmap 7.60 ( ... ) at 2021-10-31 18:44 PDT
Nmap scan report for 167.172.144.11
Host is up (0.0052s latency).
Not shown: 999 filtered ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 17.32 seconds
```

IP address 167.172.144.11 has SSH open on port 22, It can be accessed from the public internet. The other 999 ports examined are "filtered".

From the NMAP Reference Guide, Chapter 15

> The state is either open, filtered, closed, or unfiltered. **Open means that an application on the target machine is listening for connections/packets on that port. Filtered means that a firewall, filter, or other network obstacle is blocking the port so that Nmap cannot tell whether it is open or closed.** Closed ports have no application listening on them, though they could open up at any time. Ports are classified as unfiltered when they are responsive to Nmap's probes, but Nmap cannot determine whether they are open or closed. Nmap

reports the state combinations open|filtered and closed|filtered when it cannot determine which of the two states describe a port.

VULNERABILITIES DISCOVERED

RockStar Corp does not want to indicate they are accepting connections.

A. SSH is running, accepting connections on port 22 of 167.172.144.11. This is a vulnerability as it provides access that was not part of the network requirements.

B. The other 999 ports scanned on 167.172.144.11 are filtered, meaning they respond to SYN in a way that is not clear to Nmap. An RST response from a firewall on behalf of RockStar servers would represent a clear refusal to establish a connection, and prevent the SYN request from reaching the server..

HACKER / SECURITY IMPLICATIONS

A. If SSH was not authorized and officially enabled by RockStar IT, then it could be a backdoor for unauthorized logins and malicious activity.

B. The lack of a firewall presenting closed ports to the public internet is another missed opportunity to establish a significant hurdle to hacker access from the public network. Accidental configuration of a service on an internal server with an externally routable IP address could be enough to open that service to the public internet.

RECOMMENDED MITIGATIONS

A. After this study is complete, if internal use of SSH is required, then configure the firewall to CLOSE port 22 for 167.172.144.11 preventing logins from the public internet. If internal use of SSH is not required, then disable the service on that server. Investigate further to see if this path has been used for malicious purposes. In particular, look for IP addresses that have connected via SSH.

B. After this study is complete, take steps to configure the firewall to present CLOSED ports (instead of filtered) using RST to the public internet for TCP “private” ports between 1 and 1023. Review business needs and consider closing “registered” ports 1024 to 49151, and “dynamic” ports 49152 to 65535. Review RockStar policy for UDP connections and ensure the firewall provides appropriate security. If possible, the servers should be administered by one group, and the firewall should be administered by another group. This separation of duties makes it more difficult for individual hackers to configure access.

OSI Layer

SYN / ACK and RST are part of TCP. So the scan performed is looking for TCP activity in the OSI Transport Layer 4.

Phase 3. SSH and NSLOOKUP

SSH runs on port 22, which is commonly used for system administration and is open on 167.172.144.11.

STEPS TAKEN
We will try to connect to the open port with this command:

```
ssh jimi@167.172.144.11
```

It is successful, so we are IN and have a command line on the host: **GTscavengerHunt**.

Since the Hollywood site is having trouble with access to rollingstone.com. Let's try nslookup and dig. Then let's look at **`/etc/hosts`** on that computer.

```
nslookup rollingstone.com
dig rollingstone.com
less /etc/hosts
grep -i rollingstone /etc/hosts
```

RESULTS
The nslookup and dig commands are not found. That's unusual.
The less and grep commands find this line in **`/etc/hosts`**

```
98.137.246.8 rollingstone.com
```

FURTHER STEPS TAKEN
So, let's exit from 167.172.144.11, and see if we can verify that IP <> Hostname combination with public DNS as provided by Google DNS service at 8.8.8.8.
Using the nslookup command on my VM, we see:

```
$ nslookup rollingstone.com  8.8.8.8
Server:         8.8.8.8
Address:   8.8.8.8#53

Non-authoritative answer:
Name: rollingstone.com
Address: 151.101.64.69
Name: rollingstone.com
Address: 151.101.0.69
Name: rollingstone.com
```

```
Address: 151.101.128.69
Name: rollingstone.com
Address: 151.101.192.69
```

So we get 4 IP addresses, none of which match the value we see in the Hollywood Office. So this is suspicious. Let's see what the IP we found has another name. We get:

```
$ nslookup 98.137.246.8
8.246.137.98.in-addr.arpa  name = unknown.yahoo.com.
```

FURTHER RESULTS
The changes made to /etc/hosts are ERRONEOUS.

VULNERABILITIES DISCOVERED
Someone has changed **/etc/hosts** on this Hollywood Server. They configured a line "**`98.137.246.8 rollingstone.com`**" in that file that could be interpreted in two ways, both suspicious. The vulnerability is that the RockStar server is running with system configuration files that have been erroneously modified to reroute connections.

HACKER / SECURITY IMPLICATIONS

A. This could be a man-in-the-middle attack -- We see a system change that redirects connection attempts intended for rollingstone.com over to a different, suspect server. Perhaps the system at 98.137.246.8 records the communications and then forwards it on to the real rollingstone.com server. This would let hackers spy on possibly sensitive communications with rollingstone.com.

B. An attempt to disguise leaks of sensitive information -- A hacker has likely gained access to this RockStar host. That access could be used to open connections and transfer information to **unknown.yahoo.com** while making it appear to be normal connections to rollingstone.com. If logging systems on the breached RockStar host log only DNS hostnames as provided by the user, then the logs would record hacker activity as innocent connections to rollingstone.com. Also, a watchful system administrator using `ps -ef` (or similar) to view activity on the system, would see processes connecting to rollingstone.com.

RECOMMENDED MITIGATIONS

A+B. Immediately start packet capturing traffic with **98.137.246.8** to learn more. Immediately review logs on the RockStar server and increase internal logging with a particular initial focus on SSH networking and SUDO. Correlate packet captures and enhanced logging to answer the question "who is running what programs that use the bad rollingstone.com IP address?".
Inform RockStar management of a possible breach in progress. Engage them in discussion to understand how best to manage the tradeoff of (a) learning who is

doing what, vs. (b) stopping the malicious activity more quickly.
Remove the invalid line from /etc/hosts.

OSI Layer
DNS is an Application Layer 7 service that normally uses UDP (transport layer 4) to get results. In this case, the /etc/hosts file on the server overrides the UDP lookup process. This is a typical default Linux behavior and is controlled by /etc/nsswitch.conf.

Phase 4. Packets and WIRESHARK

STEPS TAKEN
We go back to the breached RockStar system 167.172.144.11, In /etc, where the suspicious line in /etc/hosts was found, we also discover the file named `/etc/packetcaptureinfo.txt`

It tells us:
`Captured Packets are here: https://drive.google.com/file/d/1ic-CFFGrbruloYrWaw3PvT71elTkh3eF/view?usp=sharing`

So we load that file into WIreshark and find 20 packets, including 5 ARP, 6 TCP ACKs to port 80, and 9 HTTP,

RESULTS

1. Packet 4 sent Jan 6, 2014,
   ARP reply shows IP 192.168.47.200 used by VMware-00:0c:29:0f:71:a3.
   Packet 5 sent 10 seconds later, detects DUPLICATE IP
   ARP reply shows IP 192.168.47.200 now used by VMware-00:0c:29:1d:b3:b1.

   Could be a case of arp cache poisoning aka arp spoofing.
   Where we believe VMware-00:0c:29:0f:71:a3 is the good MAC address, but VMware-00:0c:29:1d:b3:b1 is trying to intercept traffic for that IP.

2. Packets 6 through 11
   Six TCP ACK packets from 10.0.2.15 to port 80 (HTTP) of three IP addresses 72.21.91.29 (twice), 104.16.161.215 (twice), 74.125.136.95 (twice).

   ACK is confirmation that the client 10.0.2.15 has established a TCP connection to the HTTP servers. None of those HTTP server IP addresses are known RockStar Corp systems or suspected by other parts of this analysis.

3. Packets 12 through 20 show an HTTP session between client 10.0.2.15 and webserver 104.18.127.89 opening URL http://www.gottheblues.yolasite.com.

Packet 16 sent 2019-Aug-15 is the only HTTP POST of data from client to server. It contains the following:

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"

This text shows an insider at RockStar Corp attempting to sell SSH access to a RockStar server for $1M. It is not clear who will receive this offer.

VULNERABILITIES DISCOVERED

A. A person with access to RockStar systems would like to sell credentials necessary for SSH access that he/she configured, to someone for one million dollars. The open SSH port discovered in earlier phases is in fact, a backdoor.

B. Possible case of arp cache poisoning (aka. arp spoofing). It is possible that VMware-00:0c:29:0f:71:a3 is the good MAC address, but VMware-00:0c:29:1d:b3:b1

HACKER / SECURITY IMPLICATIONS

A. Insiders selling access to RockStar computing systems is a significant threat and likely illegal.

B. ARP cache poisoning could be an attempt to intercept traffic for another system. There is also a chance this is an accidental misconfiguration of a VMware virtual machine.

RECOMMENDED MITIGATIONS

A. Change passwords on all accounts on 167.172.144.11. Check all accounts for access via public key encryption. Look for $HOME/.ssh/authorized_keys. Review and

B. Attempt to locate the two MAC addresses that produced the duplicate IP. This will involve review of ARP caches in network switches. Narrow it down then assess the possibility this was malicious vs. accidental. If likely malicious, gather evidence. If likely accidental, then work with the system owner to properly configure IP addresses of virtual machines. If it is unclear, then capture more packets to see if this is recurring.

OSI Layer

ARP is a Data Link Layer 2 protocol. TCP is a Transport Layer 4 protocol. HTTP is an Application Layer 7 protocol.