**Intel Report**

**Rockstar Corporation Vulnerability Assessment**

**HW 8.0 November 20, 2020**

### **PREPARED FOR**

**Rockstar Corporation**

Hollywood Division

### **PREPARED BY**

**Sean James**

Security Analyst

**November 20, 2020**

### **Rockstar Corporation**

### Hollywood, CA

Re: Summary of Findings

During the weeklong analysis of the Hollywood location, I believe that there has been a breach of security and that an employee within our organization has in fact created vulnerabilities and is attempting to profit off this unfortunate situation. Within the following pages, you will find a breakdown of the steps taken to track this individual's actions and ultimately what this person intends to do with the vulnerabilities.

If you have questions or would prefer a hands-on demonstration of the actions taken, please let me know at your earliest convenience. Additionally, I am available to travel to the Hollywood location at a moments notice if necessary.

**Sean James**

Security Analyst

Rockstar Corporation

1880 Rockaway Drive

Nashville, TN

450.555.555

**Information Reported**

I was told that the new offices and location in Hollywood would need a network assessment. It was brought to my attention issues that have arised from the potential breach or hack into the servers at the location. Specifically, the Hollywood Application Servers may have been compromised.

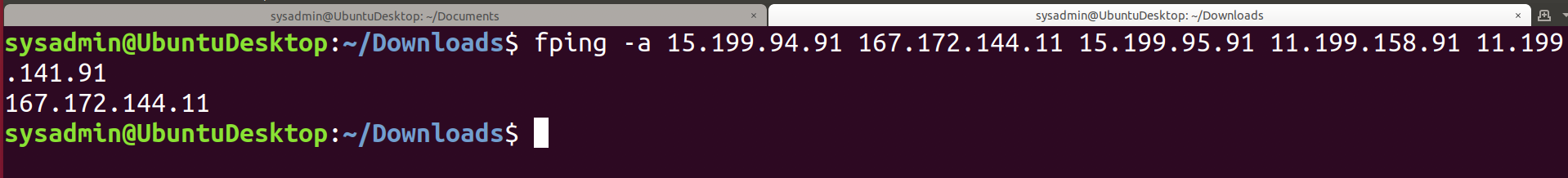
I was given a list of the servers that Rockstar Corporation uses. This was an inclusive list with (5) servers at the new Hollywood location.

I was given a deadline of one week to complete this project. Once a breach or vulnerability was discovered, I was asked to present these findings to your division.

The following is a breakdown of how the breach was discovered, and what tools were used to perform these tasks. Included will be snapshots as well as explanations of the steps taken.

**Phase 1**

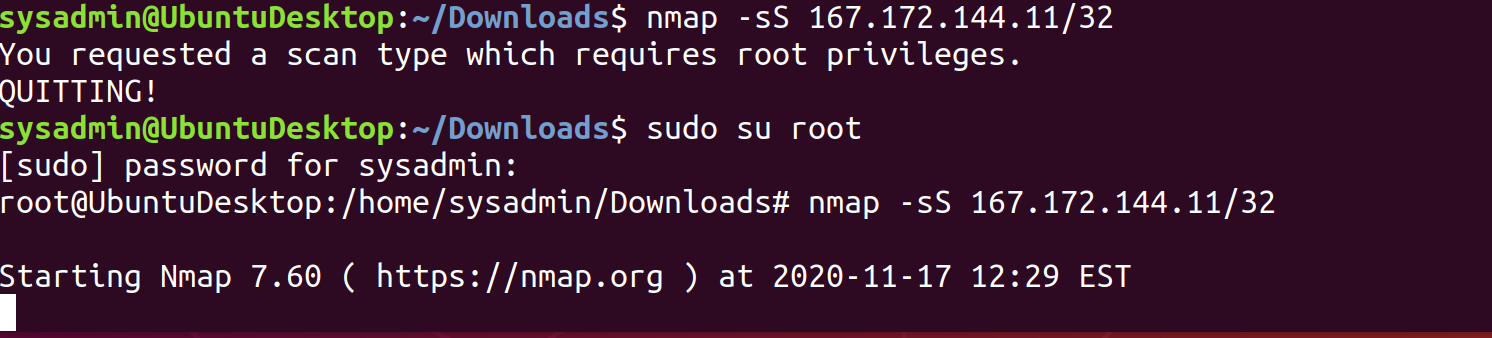
I was asked to determine the IPs for the Hollywood office that are accepting connections. I was told that we don’t want any of the servers, even if they are up, indicating that they are accepting connections.



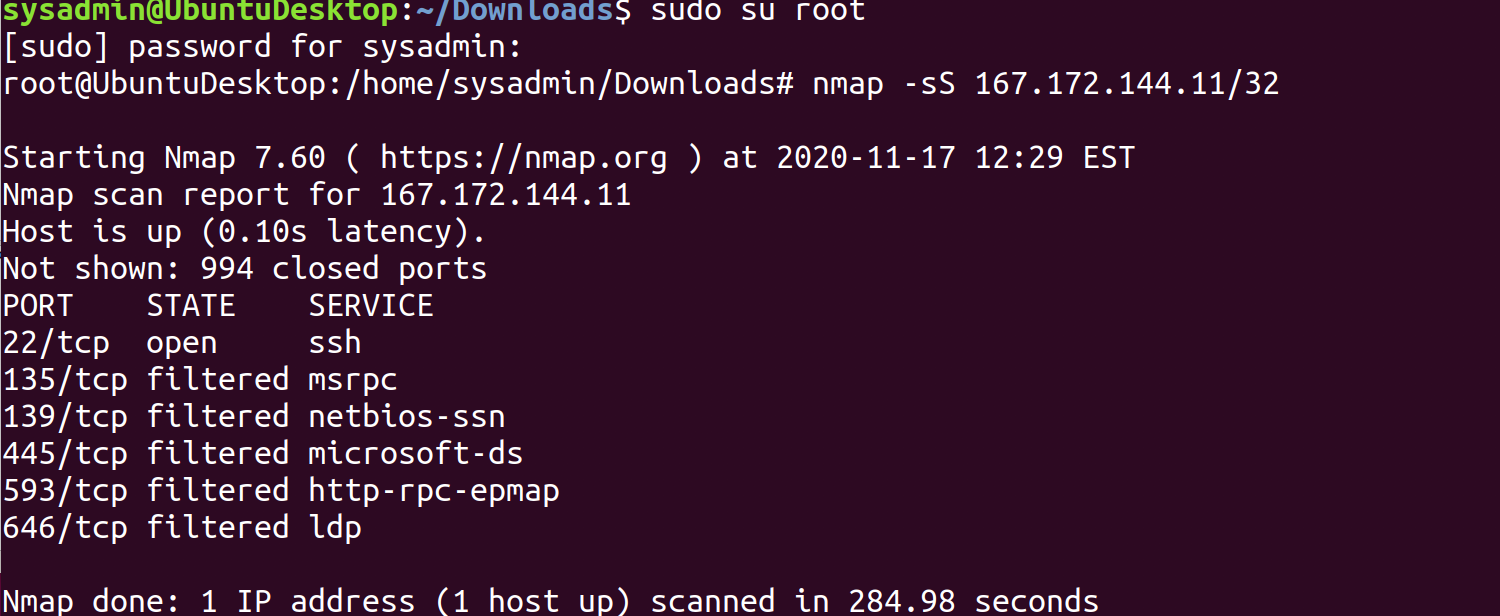
In the above snapshot, you can see that I used: <fping -a 15.199.94.91 167.172.144.11 15.199.95.91 11.199.158.91 11.199.141.91> to search through the Hollywood locations as instructed. In the network layer (Layer 3 of the OSI) the only IP that was alive in all five of the Hollywood locations was the Hollywood Application Servers of: <167.172.144.11/32>. This was verified by using the <-a> option, or asking the command to show only the results of IPs that are alive. The others all read unreachable. It should also be noted that the only IP that was alive was within the Class B network.

This being an Application Server, it should be secured and filtered. I would recommend that the settings be changed on this to and the port be changed to filtered. Since this is most-likely a Microsoft Server, I recommend a Group Policy Object to address this and not allow this server to react to pings.

**Phase 2**

****

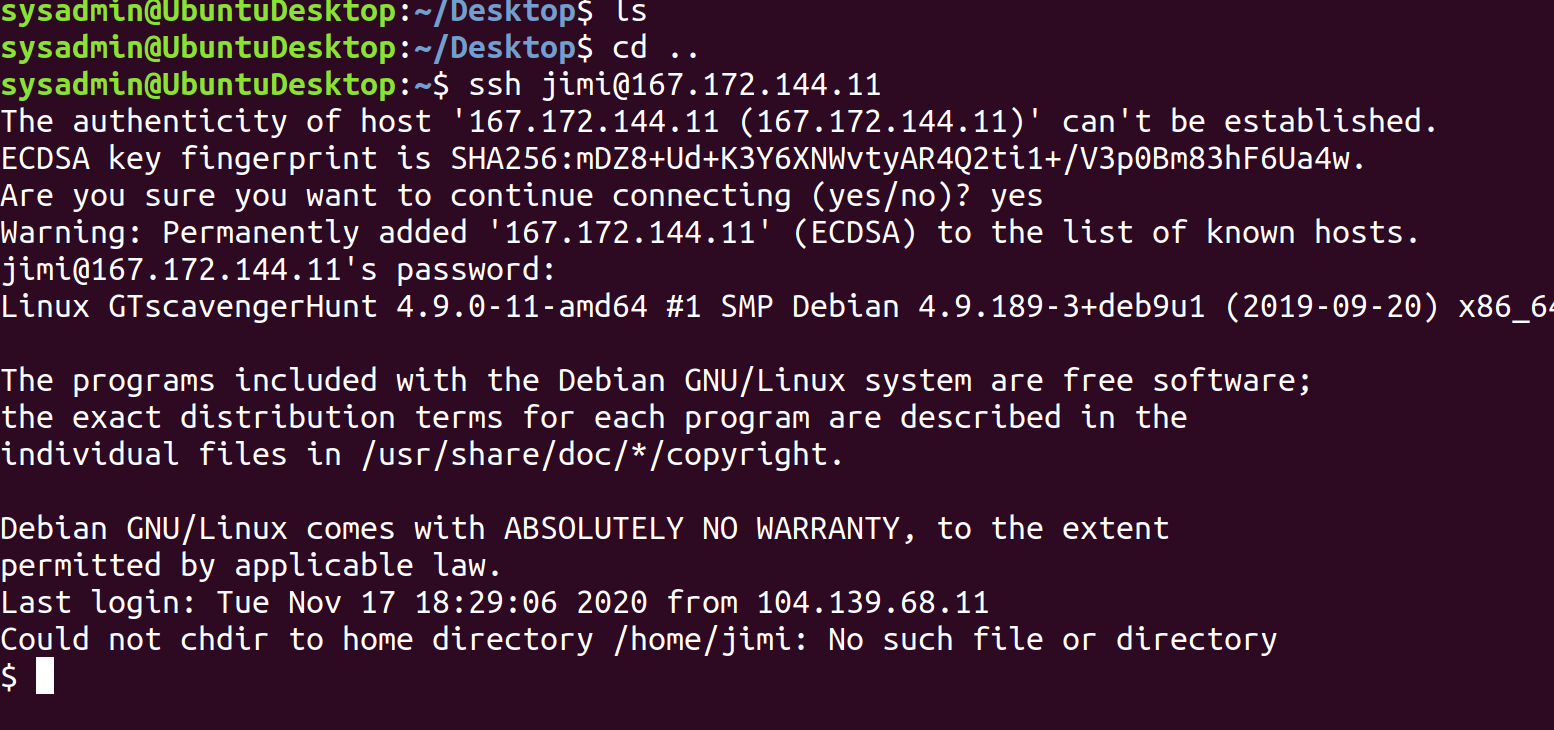
The above is my attempt to run the nmap command to see which ports are open on the IP address that is alive (layer 3 of OSI). As you can see, I learned that it needed to be run as root. After I changed that, you can see the following results.

****

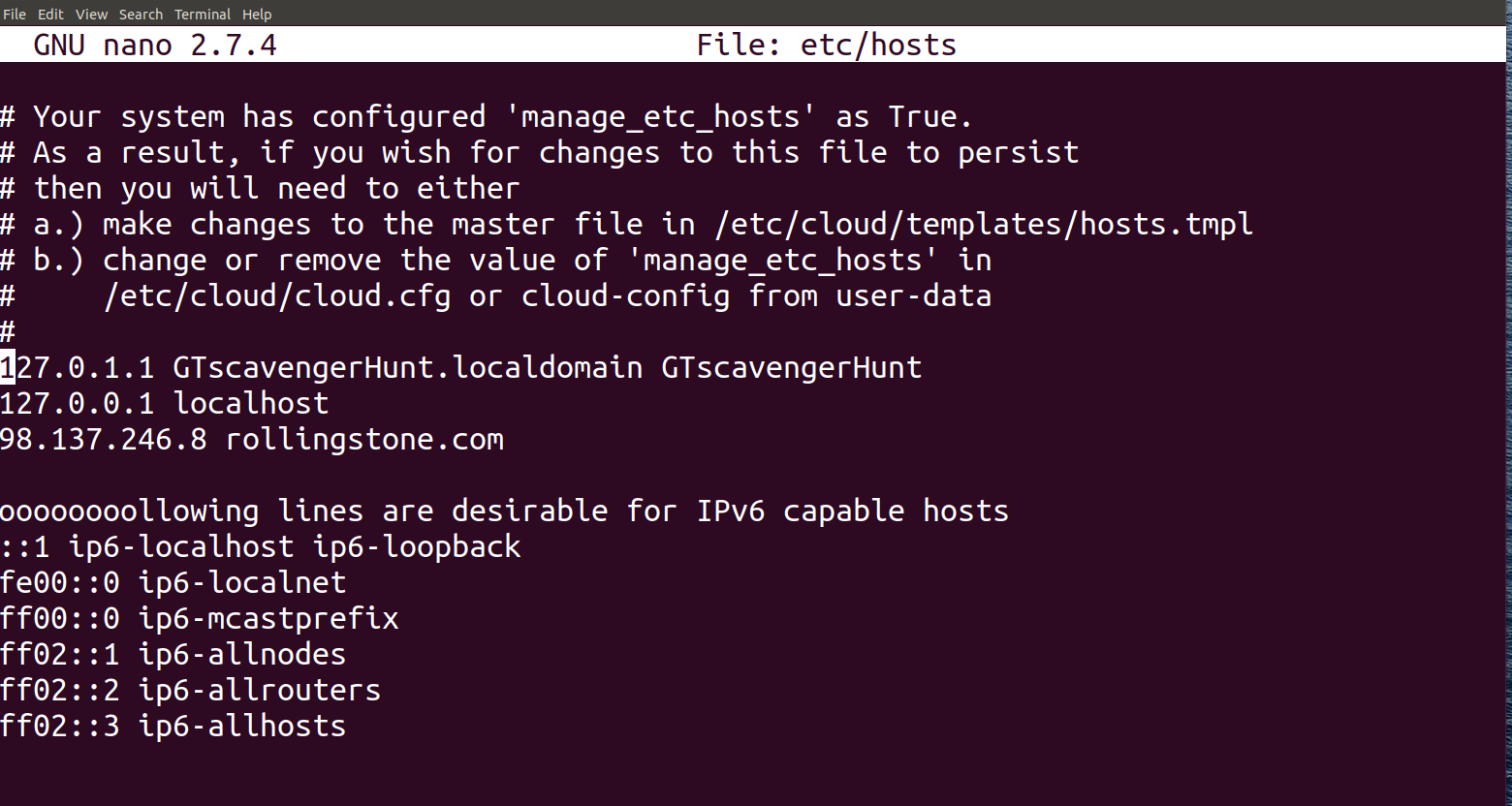
Of the 1,000 most frequently used ports; 994 are closed. Port 22 commonly used for ssh is open. Ports 135, 139, 445, 593, 646 are filtered or stopped by a firewall.

Since port 22 is often used for ssh (OSI Layer 7) or remote logins at the application layer, just a strong password is often not enough to prevent a brute force or other attacks from gaining access to the server. It is recommended that a public and private access key be used and the private key installed on those machines that would need remote access to this server. If you insist port 22 remain open, I again suggest having it filtered since it is being used at the application level (OSI Layer 7).

**Phase 3**

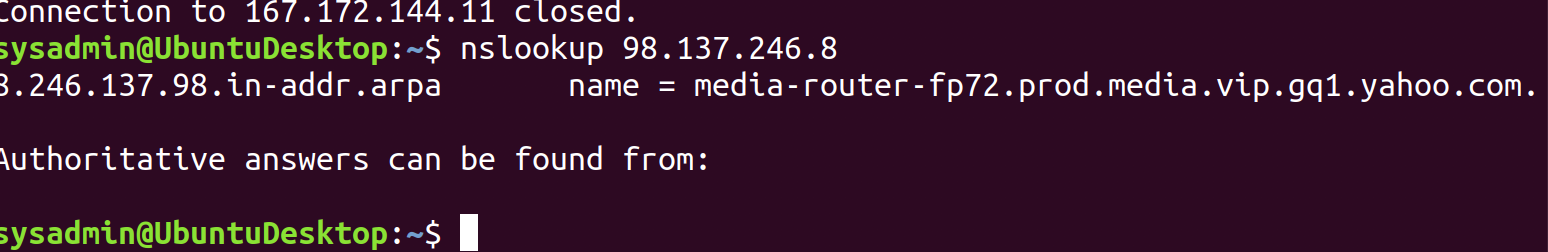


Since this is an internal server, I was given both the name and password for login. By using the command <ssh jimi@167.172.144.1>, I was able to remote into this server.

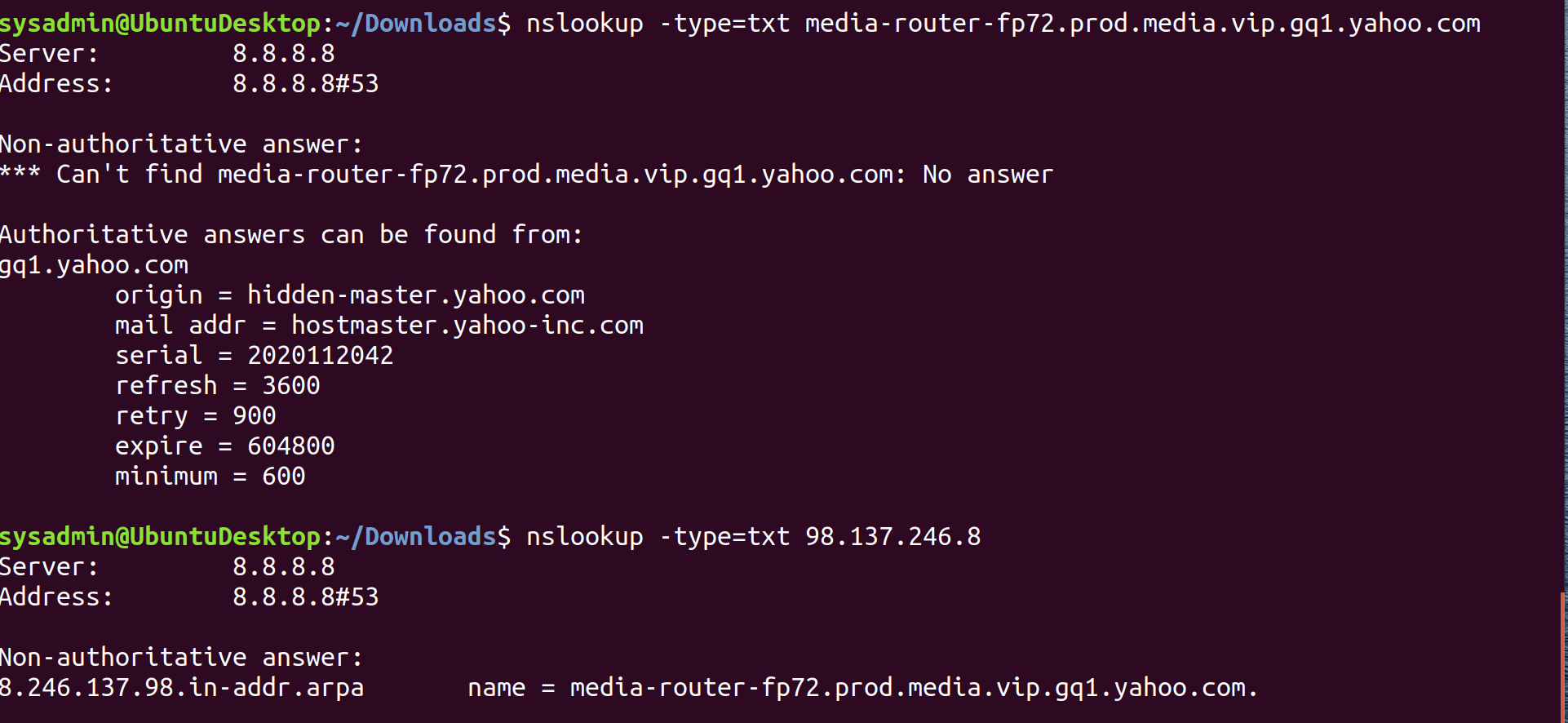
****

Once there, I could see that the text file had some edits to it. Specifically, that the IP address was added for rollingstone.com to be that of <98.137.246.8>. This is re-directing those that attempt to enter that domain to another site that is not owned by Rolling Stone.

The changes to the file can be seen above, with the specific change to the IP address added to the rollingstone.com domain. This can be viewed once gaining access to the Hollywood server in a few ways. I went into this by changing into the etc folder, then using <cat hosts> to view the file. This can also be done under a text editor approach (above) where the file can be edited by using a text editor such as nano (presumably what the hacker did).



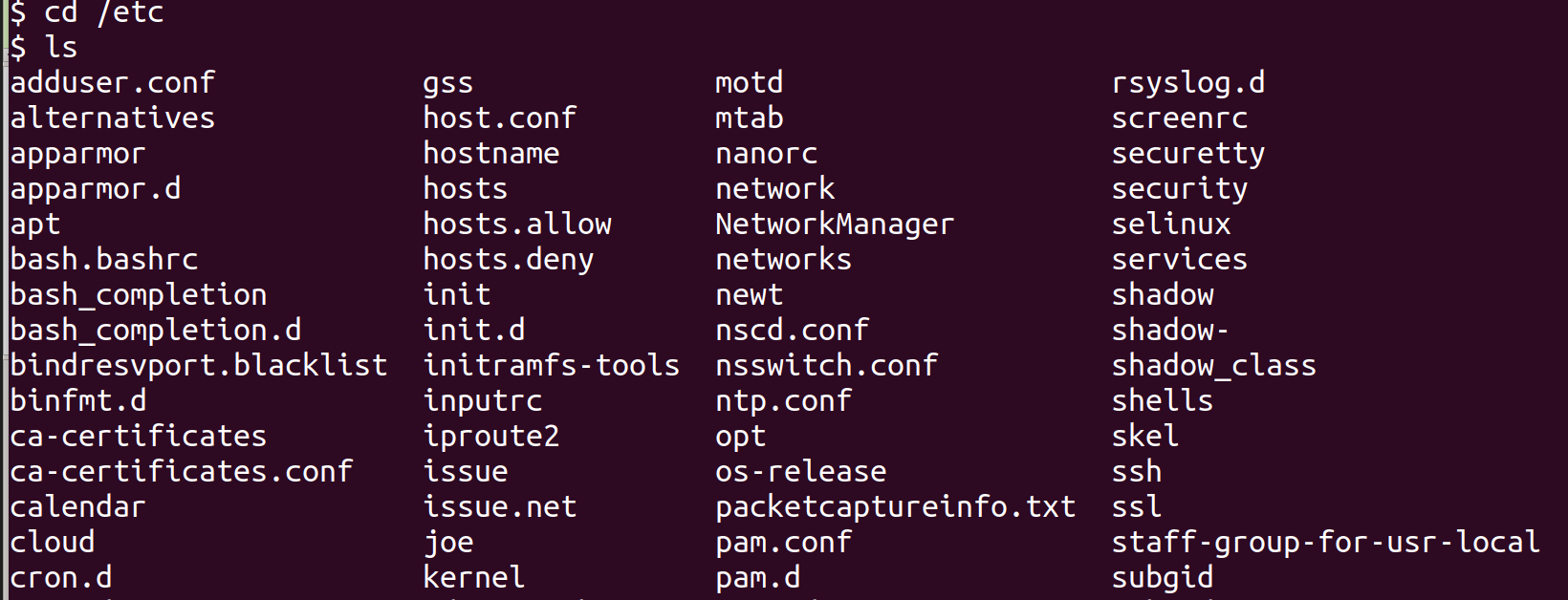
I then used the <nslookup> command to see if I could gather information on the DNS to where these packets were sent (OSI Layer 7). I did that with the basic <nslookup> command above.



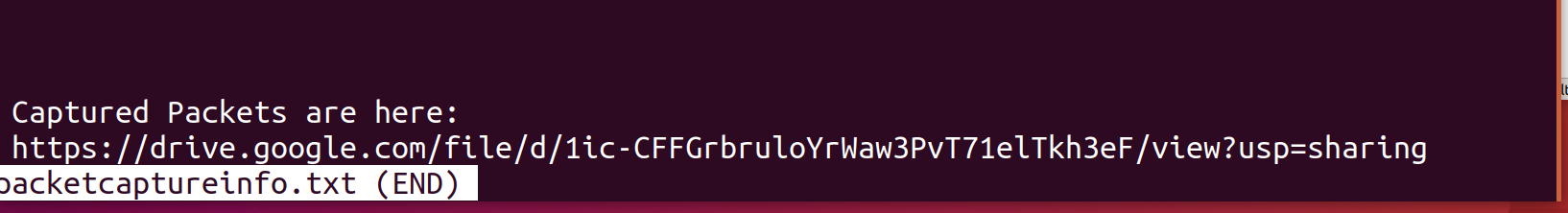
Once I was able to determine that the domain’s IP was spoofed, I used the above command <nslookup -type=txt 98.137.246.8> This yielded the above result. That is commonly referred to as a reverse DNS lookup since I had the IP only. I then ran it with the domain name. I noticed that this was coming from server <8.8.8.8> which is a server owned by Google and is commonly used in pings by those tasked with looking for indicators of compromise. The domain users are being redirected to is the above starting with name = media-router.

I recommend that once again the etc/hosts file be edited, and the entry for redirecting those who search the rollingstone domain be deleted. Furthermore, there should be enhanced restrictions in place regarding who has access to being a root user. I would also request that since I am your new analyst, I should have access to files such as the list of users and the sudoers files.

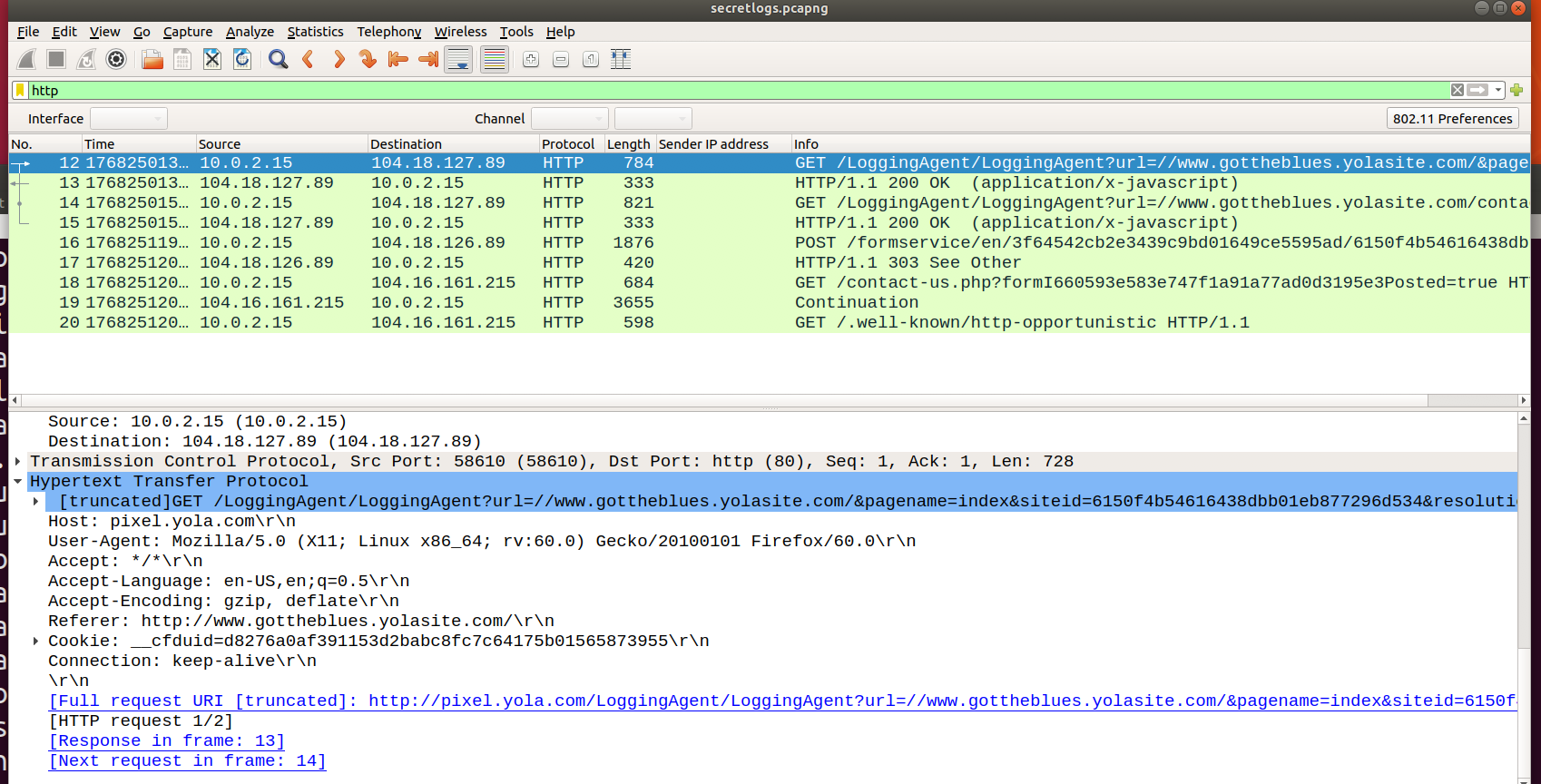
**Phase 4**



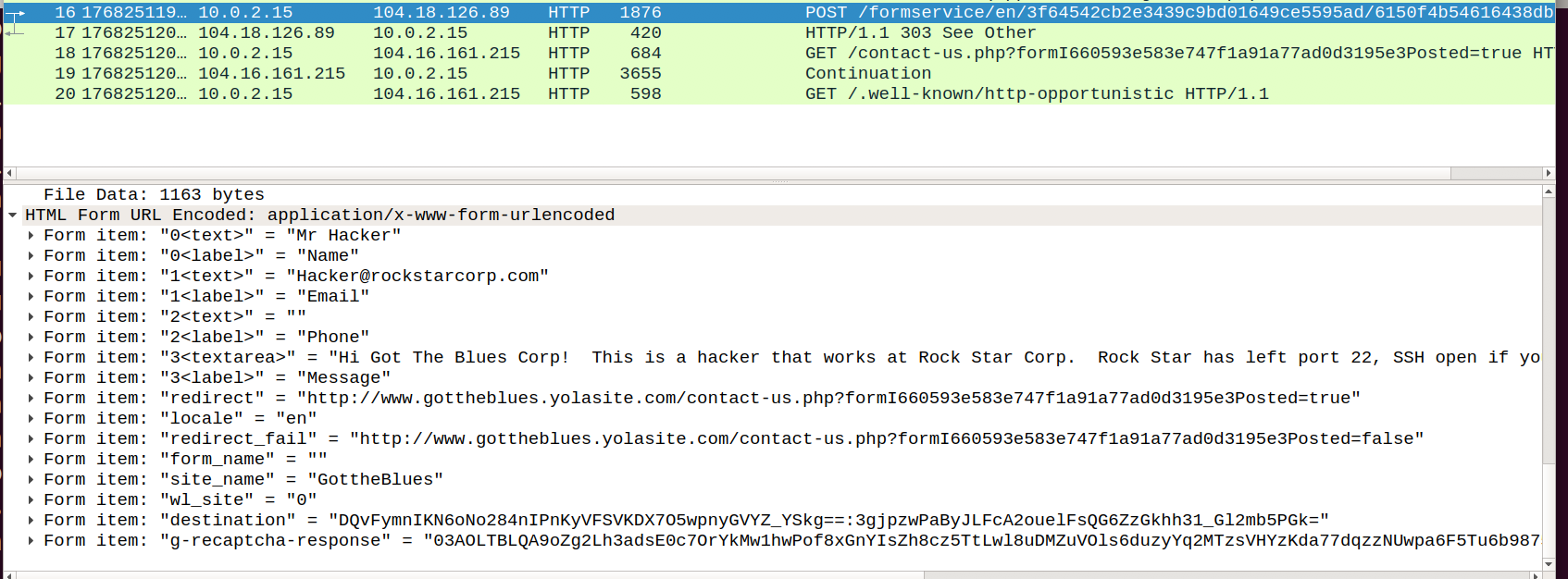
Once in the server, I changed directories and entered the etc folder. Within that I used the <ls> command to take a look around. I noticed the above <packetcaptureinfo.txt>.

****

I used the <less packetcaptureinfo.txt> command to take a look within and found the hyperlink to the Google Drive File. I used that within a browser and had to first download it. Once that was completed, I opened the file with Wireshark.



In the above snapshot, you can see an <http> filter of the packets captured in wireshark. Within this filter, it is clear that within the first filtered capture, the hacker is using a logging agent. These are commonly used to read and send logs to another location.

****

In the above capture, you can see that the hacker is using an HTML form service in an unsecured HTTP transfer. I viewed this by resolving all options under the name resolution and was able to see what was written in plain text. The following highlighted text was extracted from the packet exchanged:

**Arrival Time: Aug 15, 2019 09:01:46.121459902 EDT**

**Src: 10.0.2.15 (10.0.2.15), Dst: 104.18.126.89 (104.18.126.89)**

**Flags: 0x4000, Don't fragment**

**Source: 10.0.2.15 (10.0.2.15)**

**Destination: 104.18.126.89 (104.18.126.89)**

**Form item: "0<text>" = "Mr Hacker"**

**Form item: "0<label>" = "Name"**

**Form item: "1<text>" = "Hacker@rockstarcorp.com"**

**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!"**

Since the hacker used an email address on our local server, we should be able to figure out who this person is with access to the mail exchange information. I attempted to use outside sources within OSINT such as <hunter.io> and was not able to locate that email address.

Additionally, the IP source of <10.0.2.15> is a private class A and internal IP. Since we use VMware, I believe we should be able to locate who had that particular IP assigned to them and at what time it was used. We have the time this was sent and should be able to narrow down who had that IP at that time within our VMware application.

I believe that we have enough evidence to present to authorities to prove a crime has been committed. I recommend that we change our practices in the future to restrict who has access to servers, root commands, and ports. Also, we need to change passwords that are not as obvious or easy to attack. We should be using a two-factor authentication and demand our password policies be revisited.