**Networking Fundamentals**

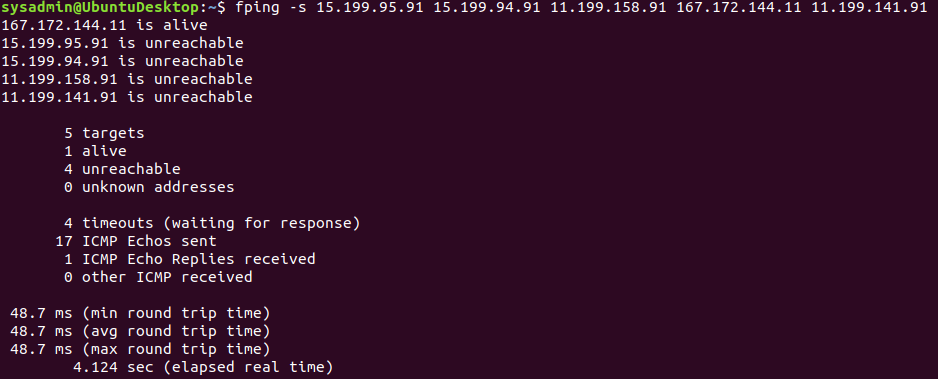
**Phase 1:**

**Network Vulnerability Assessment**

Determine IP ranges to scan and execute fping by using the command below:

* 15.199.95.91
* 15.199.94.91
* 11.199.158.91
* 167.172.144.11
* 11.199.141.91

$ **fping -s 15.199.95.91 15.199.94.91 11.199.158.91 167.172.144.11 11.199.141.91**



**Network Vulnerability Mitigation**

Rockstar IT Policy does not allow any server to indicate they are accepting connections. The following IP violates this policy:

* + 167.172.144.11

The following IP addresses are compliant with Rockstar IT Policy, because they are not accepting connections:

* 15.199.95.91
* 15.199.94.91
* 11.199.158.91
* 11.199.141.91

In order to comply with Rockstar IT Policy and mitigate risk of DOS attack, ICMP echo requests should be restricted against the following IP address to prevent successful responses from PING requests.

* 167.172.144.11

This issue has been identified on the OSI Network Layer. Ping uses IP addresses and IPs are used on the Network Layer.

**Phase 2:**

**Network Vulnerability Assessment**

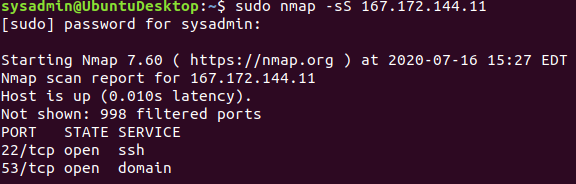
Determine which ports are open and accepting connections.

Execute the following command to run SYN SCAN against IP **167.172.144.11**:

$ **sudo nmap -sS 167.172.144.11**

The results show the following ports are open:

* 22/tcp
* 53/tcp



**Network Vulnerability Mitigation**

**Open port 22/tcp**

In order to mitigate risk of open port 22 for SSH the following action is recommended:

* Configure custom port for use with SSH (below port 1024) to mitigate risk of malicious bots that scan for SSH on standard port 22 and attempt brute force attacks. This will also reduce the impact on log files (use less hard drive space) as there will be less brute force attacks occurring and getting logged.
* Filter the SSH port on the system firewall in order to allow only trusted public static IPs or private LAN connections. This way SSH is closed for any external untrusted connections.
* Enforce security password policy for SSH users to include required length with numbers, upper / lower case letters, and special characters.
* Configure notifications to alert the system administrator via email when there are incoming SSH connections attempted.

**Open port 53/tcp**

In order to mitigate risk of DDOS attacks, cache poisoning, and other malicious activity vulnerable with open port 53 for DNS the following action is recommended:

* Configure a firewall rule to allow DNS with OpenDNS servers and restrict DNS traffic for all other IPs.
* Consider deployment of DNS encryption using DNS Queries over HTTPS. This will secure DNS queries during HTTP communication over TLS.

This occurred on the Transport Layer as SYN SCAN uses IP addresses to determine which ports are open and accepting TCP connections such as SSH and DNS.

**Phase 3:**

**Network Vulnerability Assessment**

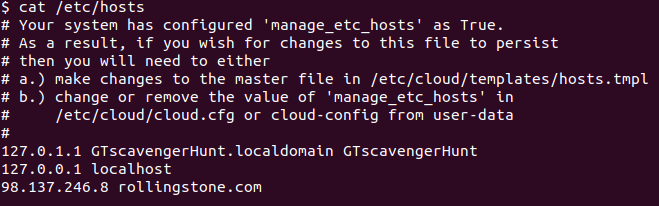
Determine if the server is accepting connections via open port by executing the following command to access the server:

$ **ssh jimi@167.172.144.11 -p22**

$ **password: hendrix**

Determine if any modifications were made to the hosts file by executing the following command:

$ **cat /etc/hosts**

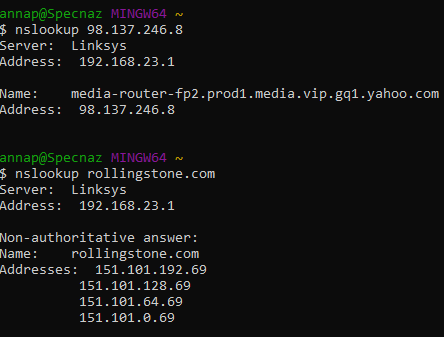


The **/etc/hosts** file has been modified and the IP address of **rollingstone.com** was changed to resolve the following IP address:

* **98.137.246.8**

Determine the real domain of the IP address identified in the **/etc/hosts** file by executing the following command:

$ **nslookup 98.137.246.8**



The actual hostname / domain is the following:

* **media-router-fp2.prod1.media.vip.gq1.yahoo.com**

The actual IP addresses determined for **rollingstone.com** are the following:

* 151.101.64.69
* 151.101.0.69
* 151.101.192.69
* 151.101.128.69

**Network Vulnerability Mitigation**

It appears the DNS server has been poisoned by a hosts file pharming attack.

**Recommendations:**

* Consider using anti-malware software and keeping it up-to date.
* Patch devices and perform regular virus scans and periodic clearing of cache/browser cookies.
* Audit and monitor DNS servers to reduce the chances of them being exploited.
* Educate all users that are granted access to the network regarding safe browsing behaviour, the risk of phishing scams, malware infections, and other viruses.
* Ensure strong password security policy enforced on routers to help prevent drive-by attacks.
* Enable 2FA on SSH in order to improve security by requiring a second form of identification.
* As mentioned in Phase #2 mitigation strategy the following items are also important to consider: Enforcement of strong password policies, monitoring of login attempts over SSH, and custom port assignment for SSH.

This occurred on the Application Layer as DNS is a service that translates host names into IP addresses.

**Phase 4:**

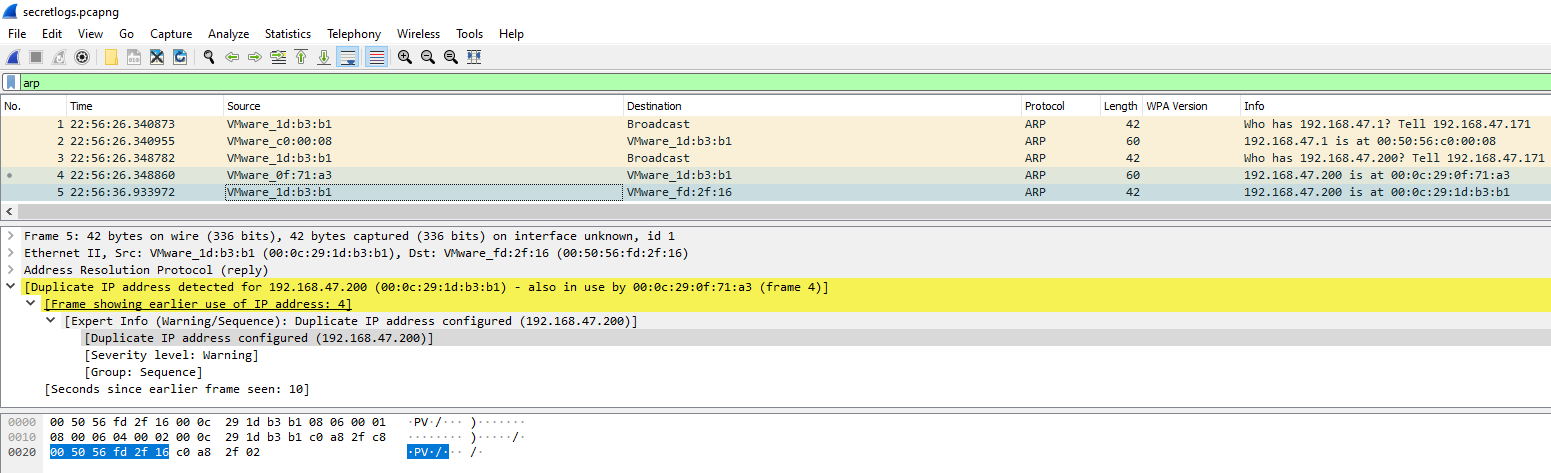
**Network Vulnerability Assessment**

The file **packetcaptureinfo.txt** has been identified in the **/etc** folder. The file contains a link to download a file named **Secretlogs.pcapng**. This file is stored at the following link:

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

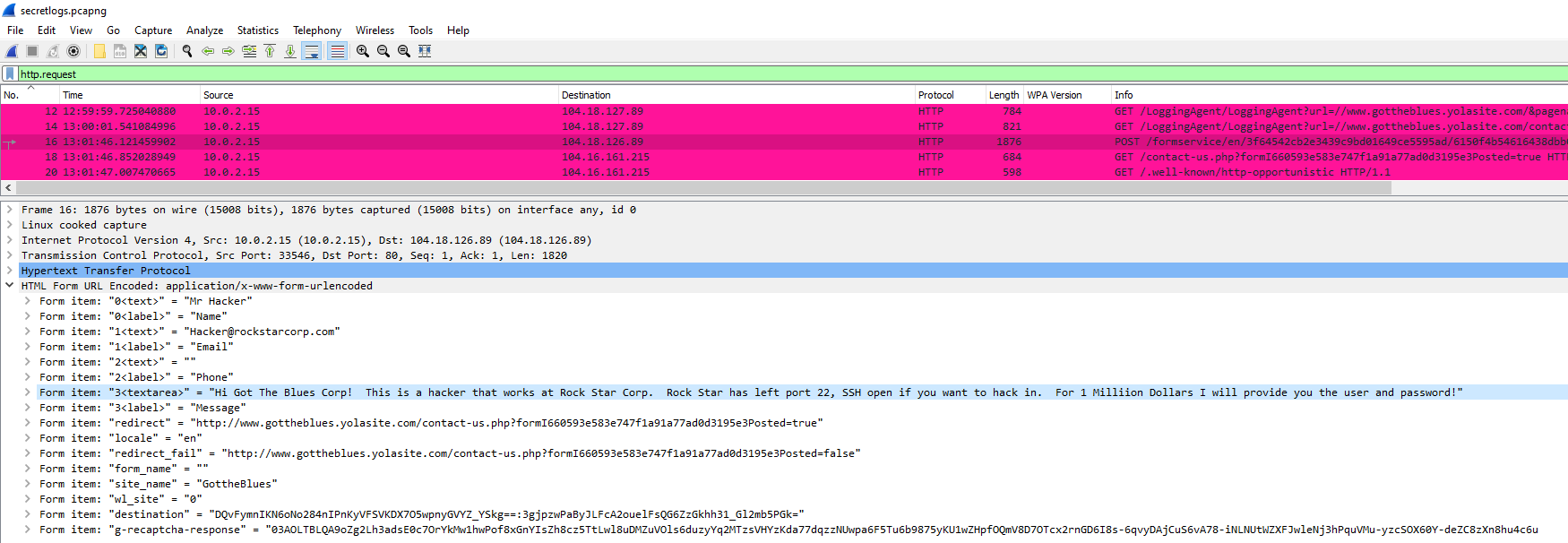
The file is a capture of packets and contains the following suspicious activity:

* ARP poisoning attack identified by finding duplicate IP addresses assigned to 2 different MAC addresses.



* HTML injection has been identified because the hacker has hidden a secret message inside the HTML form which states the following message:

“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!”



**Network Vulnerability Mitigation**

In order to mitigate risk of ARP Poisoning attack the following action is recommended:

* Ensure using VPN to encrypt all the data that going out of the server, to make connections safe.
* Assign static IP and MAC addresses to devices to prevent spoofing attacks.

In order to mitigate risk of HTML Injection attack the following action is recommended:

* Web applications should never connect to the database with accounts that have root privileges. This will help to prevent the executing the code.
* Create an isolated account for each application and deny access to unnecessary files and privileges.
* Ensure to create a set of rules for Web Application Firewall to filter the malicious data and requests. It will prevent cross-site Scripting, session hijacking and code injections.

The ARP poisoning attack occurred on the Data Link Layer, as it used for discovering the link layer address.

The HTML Injection happened on the HTTP Protocol, as being a part of the Application Layer.