**Homework 8: Networking Fundamentals**

|  |
| --- |
| **Network Vulnerability Assessment**  **Company:** RockStar Corporation, Hollywood, California |

**Phase I: Ping the Network Assets of the Hollywood Office**

To ping the subnet, the syntax I used was: **fping -g <CIDRIP>**

fping -g 15.199.95.91/28

fping -g 15.199.94.91/28

fping -g 11.199.158.91/28

fping -g 167.172.144.11/32

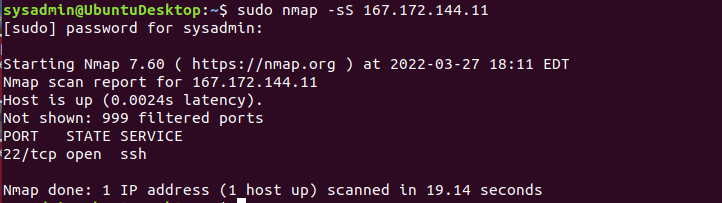
fping -g 11.199.141.91/28

The only IP accepting connections at the time of pinging was **167.172.144.11**. Since RockStar Corporation doesn’t want a vulnerability of anyone being able to ping any server, they should restrict ICMP Echo requests to all of their servers including 167.172.144.11.

The OSI Layer I found the results are in the **Network Layer (Layer 3)** since this is where IP addresses live.

**Phase II: Perform a SYN SCAN**

To perform a SYN SCAN against the IP, I ran **nmap -sS 167.172.144.11**

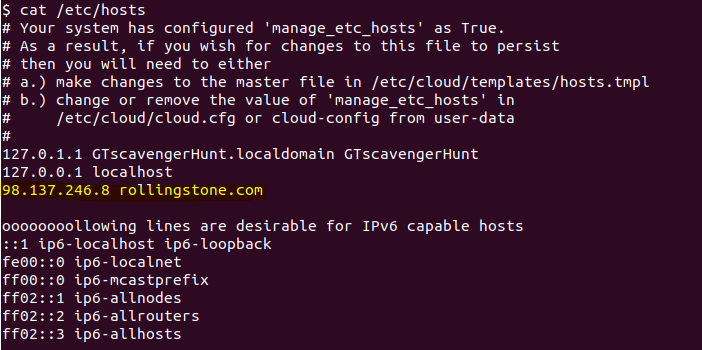
****

The only open port is **Port 22**, which is used by the SSH service. Since this is open, RockStar Corp should also filter out SSH traffic to prevent unauthorized access into their server.

SYN SCAN happens on the **Transport Layer (Layer 4)**.

**Phase III: Perform an NS Lookup**

I ran **cat /etc/hosts** to figure out what is causing a redirection when trying to access rollingstone.com. It displayed a **98.137.246.8** IP address.

****

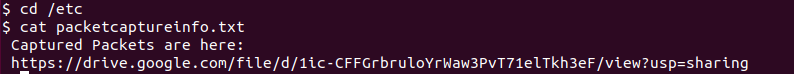
To figure out the domain of this IP, I ran **nslookup 98.137.246.8** which indicates that the domain is owned by **Yahoo.com**.



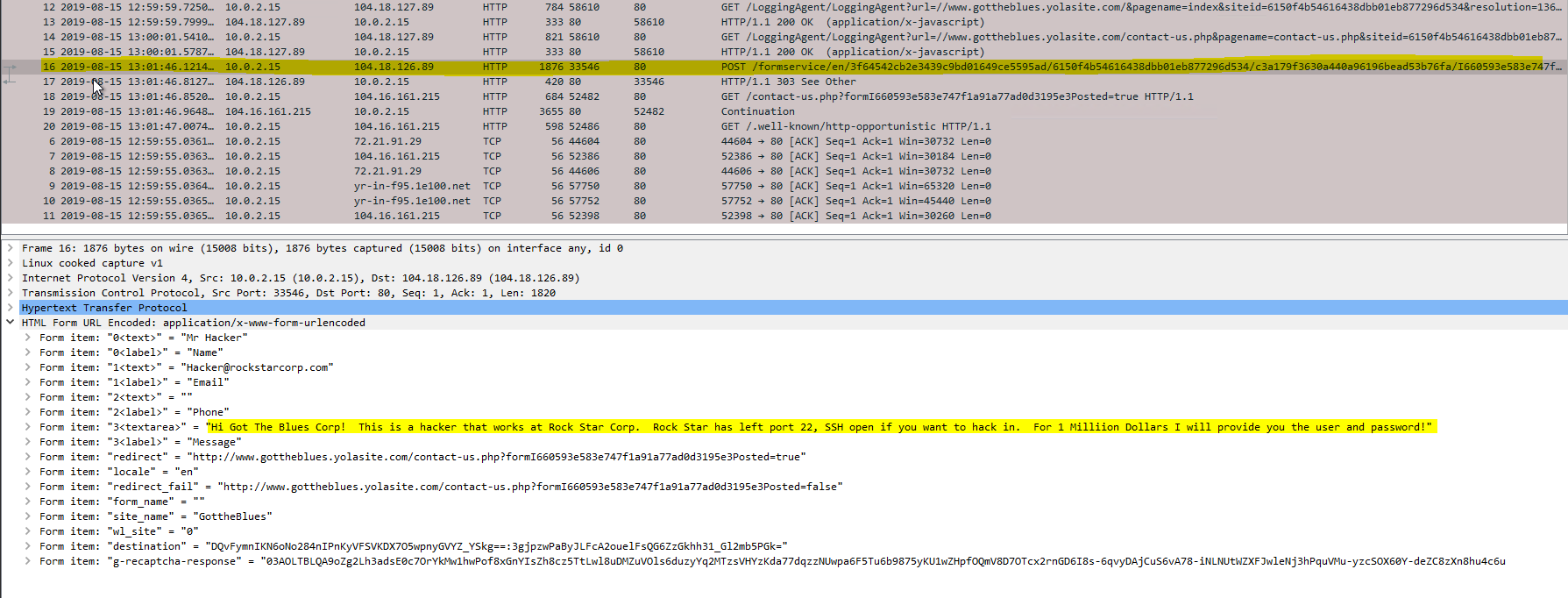
DNS is found in the **Application Layer (Layer 7)**.

**Phase IV: Examine HTTP and ARP**

To view the file to recover the packet captures, I ran **cd /etc** and then opened it with cat **packetcaptureinfo.txt** to find the location of the hacker’s packet captures.

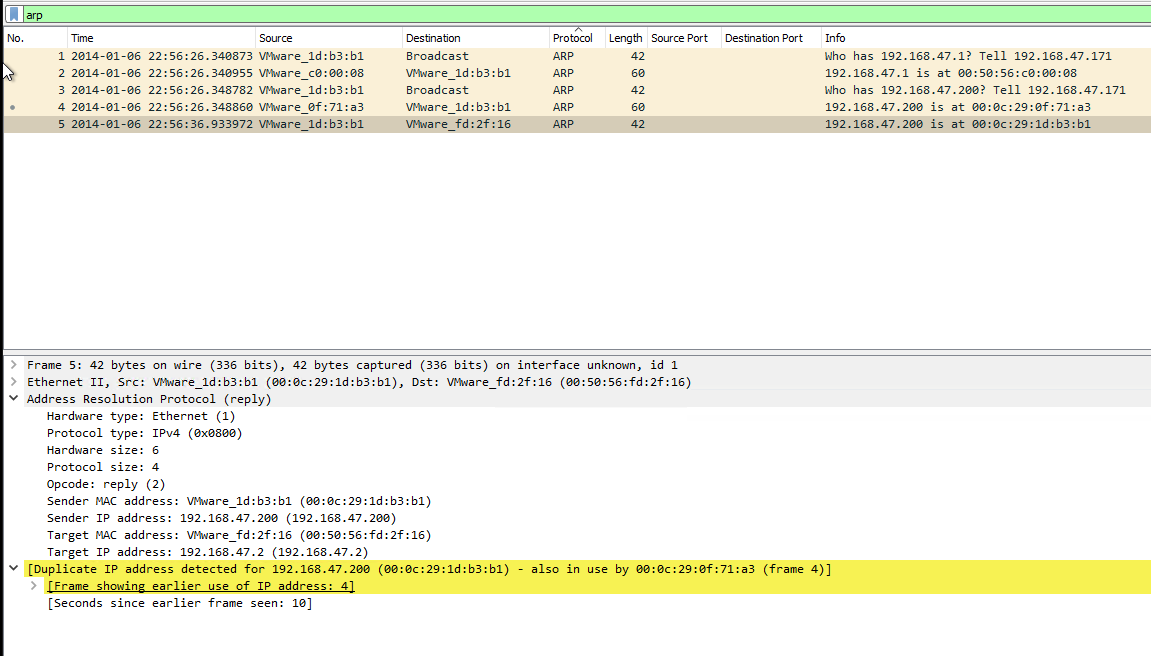


**HTTP Finding:**



HTTP runs on the **Application Layer (Layer 7)**.

**ARP Finding:**



ARP runs on the **Data Link Layer (Layer 2)**. With the duplicate IP address detected, this could be an indicator a potential **ARP poisoning attack** where a hacker can send a spoof ARP message to the LAN, and intercept all traffic originally intended for the good host to instead send to the hacker’s malicious MAC address instead. A possible mitigation method to protect against this would be creating static ARP entries rather than dynamic ones to ensure that permanent IP-address-to-MAC-address mappings are created in the local ARP cache and cannot be changed.