### **Your Submission: *"Its the End of the Assessment as We Know It, and I Feel Fine"***

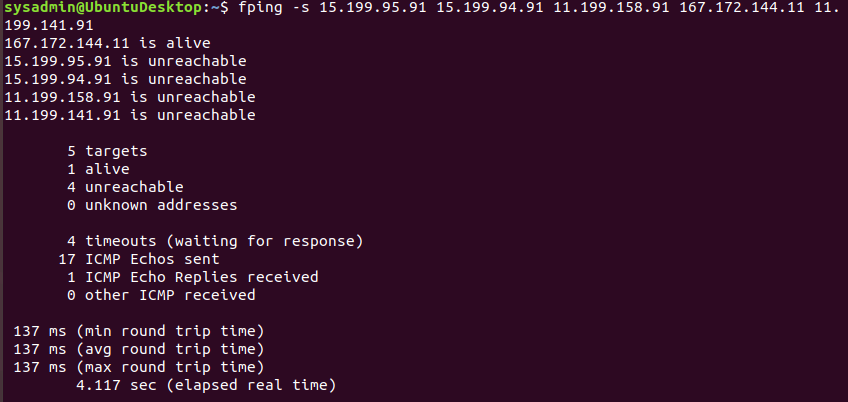
#### **Guidelines for your Submission:**

Provide the following for each phase:

* List the steps and commands used to complete the tasks.
* List any vulnerabilities discovered.
* List any findings associated to a hacker.
* Document the mitigation recommendations to protect against the discovered vulnerabilities.
* Document the OSI layer where the findings were found.

**Phase 1: "I'd like to Teach the World to Ping"**

* Determined the IP ranges to scan for Hollywood offices are 15.199.95.91 15.199.94.91 11.199.158.91 167.172.144.11 and 11.199.141.91, then ran fping against 15.199.95.91 15.199.94.91 11.199.158.91 167.172.144.11 and 11.199.141.91
  + Used the following commands to run fping:  
    - **fping -s 15.199.95.91 15.199.94.91 11.199.158.91 167.172.144.11 11.199.141.91**
      * **167.172.144.11 is alive**
      * **15.199.95.91 is unreachable**
      * **15.199.94.91 is unreachable**
      * **11.199.158.91 is unreachable**
      * **11.199.141.91 is unreachable**



* Determined a potential vulnerability that IP **167.172.144.11** is responding.  
  + Since RockStar Corp doesn't want to respond to any requests, this is a vulnerability.
* Recommend to restrict allowing ICMP echo requests against IP 167.172.144.11 to prevent successful responses from PING requests.

**sudo traceroute -I 167.172.144.11**

**[sudo] password for sysadmin:**

**traceroute to 167.172.144.11 (167.172.144.11), 30 hops max, 60 byte packets**

**1 \_gateway (10.0.2.2) 0.179 ms 0.145 ms 0.139 ms**

**2 192.168.1.1 (192.168.1.1) 3.244 ms 3.389 ms 3.390 ms**

**3 99.244.170.1 (99.244.170.1) 16.349 ms 16.398 ms 19.034 ms**

**4 69.63.243.49 (69.63.243.49) 19.054 ms 26.582 ms 26.603 ms**

**5 69.63.250.13 (69.63.250.13) 28.716 ms 28.794 ms 28.904 ms**

**6 209.148.235.218 (209.148.235.218) 28.583 ms 19.421 ms 19.374 ms**

**7 ix-ae-13-0.tcore1.tnk-toronto.as6453.net (64.86.33.5) 40.615 ms 41.248 ms 41.232 ms**

**8 if-ae-2-2.tcore2.tnk-toronto.as6453.net (64.86.33.90) 41.543 ms 42.490 ms 42.581 ms**

**9 if-ae-8-2.tcore1.ct8-chicago.as6453.net (66.110.48.2) 42.605 ms 42.617 ms 42.629 ms**

**10 if-ae-26-2.tcore3.nto-newyork.as6453.net (216.6.81.28) 53.339 ms 53.368 ms 53.364 ms**

**11 if-ae-2-2.tcore1.n75-newyork.as6453.net (66.110.96.62) 41.264 ms 41.267 ms 44.872 ms**

**12 \* \* \***

**13 \* \* \***

**14 \* \* \***

**15 \* \* \***

**16 \* \* \***

**17 167.172.144.11 (167.172.144.11) 54.351 ms 50.598 ms 44.320 ms**

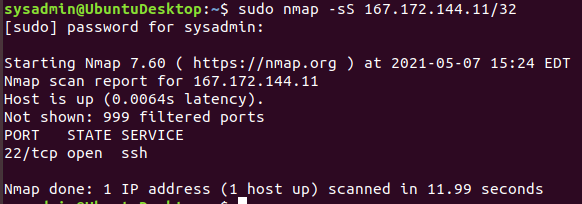
**Disabling ICMP can cause network issues**

**All servers from Hollywood office are not responding, except the 167.172.144.11/32 Hollywood Application Servers which is vulnerability as per RockStar Corp.**

* This occurred on the network layer as Ping uses IP addresses and IPs are used on the **Network Layer number 3**.

**Phase 2: "Some Syn for Nothin`"**

* **sudo nmap -sS 167.172.144.11/32**

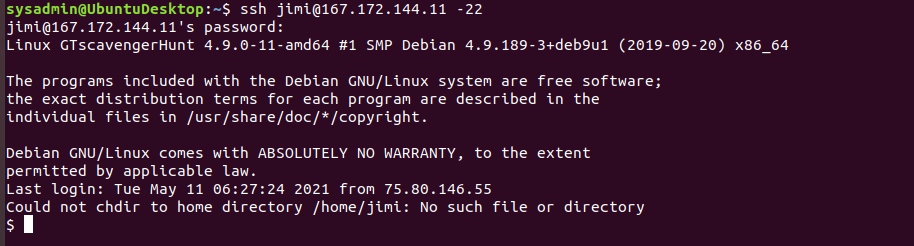
****

**Port 22 is accepting connections.**

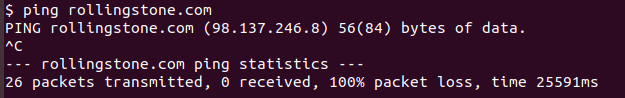
* This occurred on the transport layer as SYN uses **TCP which is connection-oriented** on the **Network Layer number 4**.

**Phase 3: "I Feel a DNS Change Comin' On"**

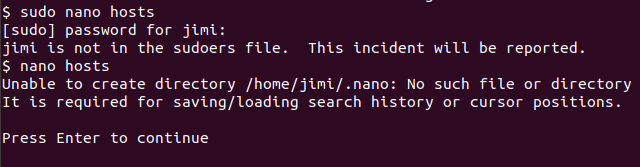
* To login **ssh jimi@167.172.144.11 -22**



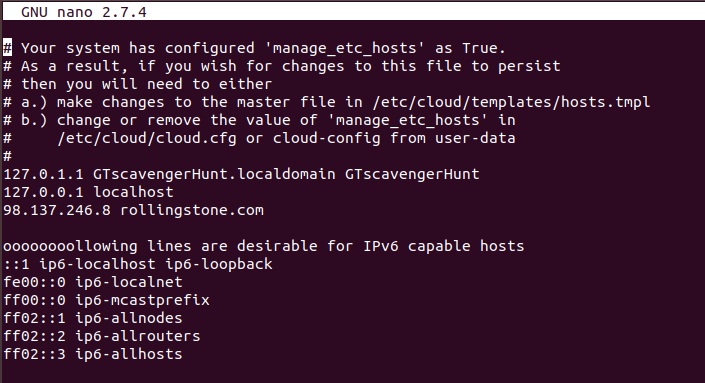
**ping rollingstone.com**



**sudo nano hosts**

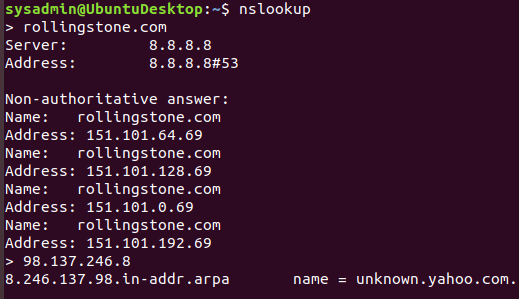
****

**nano hosts**

****

**add to the file ---> 98.137.246.8 rollingstone.com**

**nslookup**

****

****

**This occurred on the application layer as DNS runs in parallel to HTTP in the Application Layer (layer 7). DNS is in effect an application that is invoked to help out the HTTP application, and therefore does not sit "below" HTTP in the OSI stack.**

**Phase 4: "ShARP Dressed Man"**

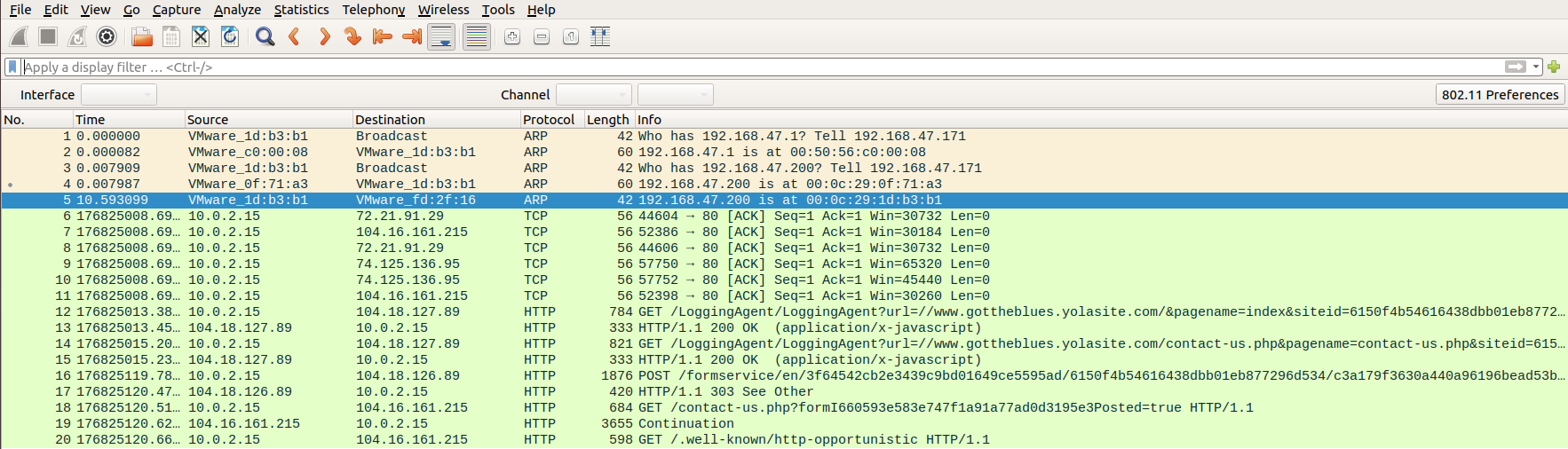
**The file left by hacker was in the etc folder: packetcaptureinfo.txt**

**cat packetcaptureinfo.txt**

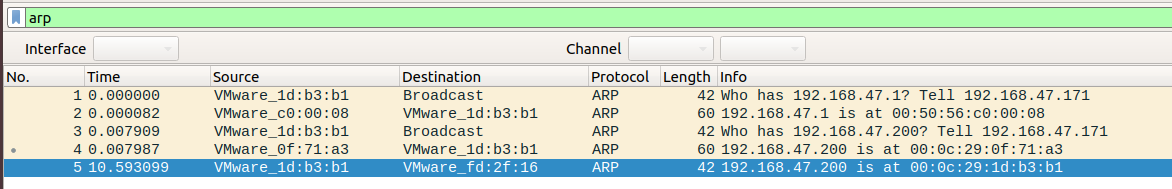
****

**From the Firefox web browser downloaded the file: secretlogs.pcapng file.**

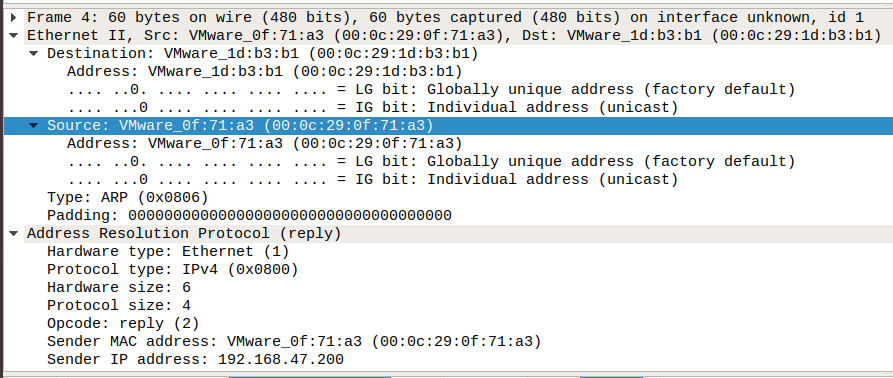
**Opened in Wireshark.**

****

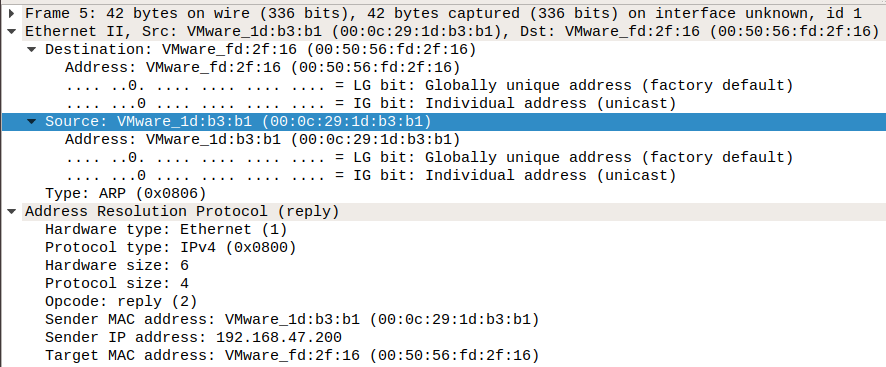
**Filtered the ARP**

****

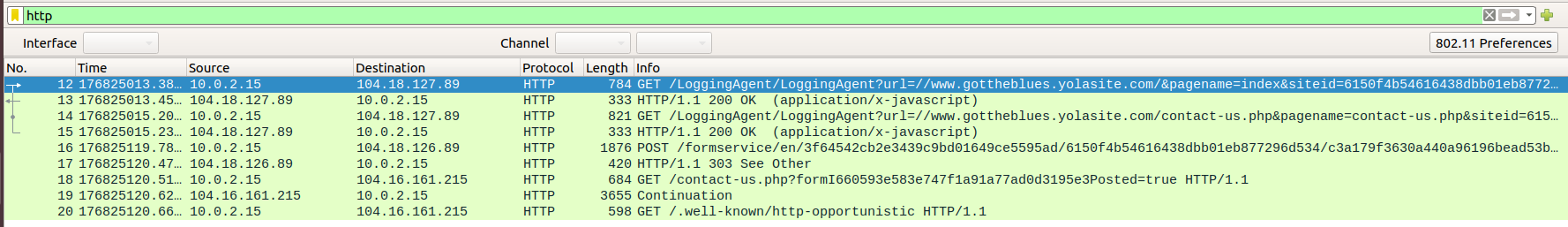
**Looking at the ARP filters request is made for the 192.168.47.1 in line one, and response on line 4 is showing the correct MAC address 00:0c:29:0f:71:a3**

****

**On line 5 the hacker has provided another MAC address 00:0c:29:1d:b3:b1 which is a spoofed MAC address to get the access.**

****

**Filtered http:**

****

**Looking at the info of the http traffic it all looks ok until line 16 where the POST from the hacker is on the website.**

**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"**

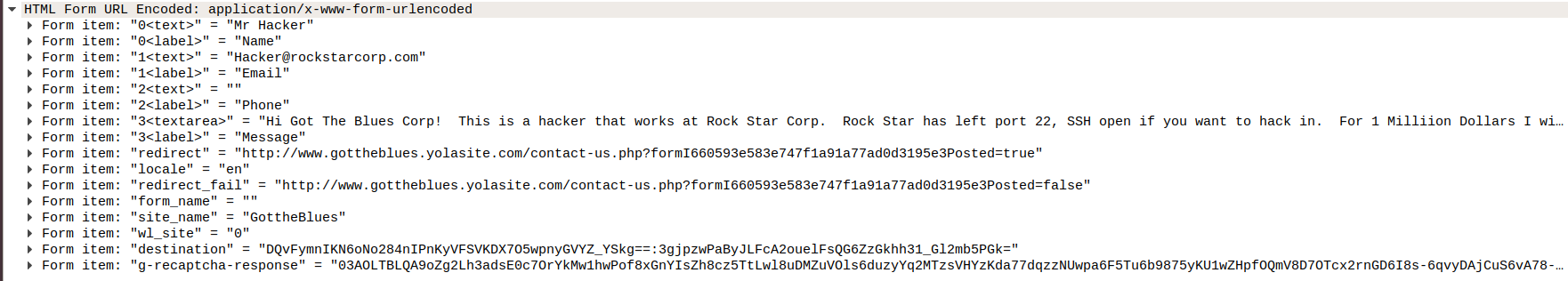
**Form item: "form\_name" = ""**

**Form item: "site\_name" = "GottheBlues"**

**Form item: "wl\_site" = "0"**

**Form item: "destination" = "DQvFymnIKN6oNo284nIPnKyVFSVKDX7O5wpnyGVYZ\_YSkg==:3gjpzwPaByJLFcA2ouelFsQG6ZzGkhh31\_Gl2mb5PGk="**

**Form item: "g-recaptcha-response" = "03AOLTBLQA9oZg2Lh3adsE0c7OrYkMw1hwPof8xGnYIsZh8cz5TtLwl8uDMZuVOls6duzyYq2MTzsVHYzKda77dqzzNUwpa6F5Tu6b9875yKU1wZHpfOQmV8D7OTcx2rnGD6I8s-6qvyDAjCuS6vA78-iNLNUtWZXFJwleNj3hPquVMu-yzcSOX60Y-deZC8zXn8hu4c6u**

****

**This occurred on the application layer as the input on the website is used on the Application Layer 7.**

© 2020 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.