**### \*\*Phase 1\*\*:** *\_"I'd like to Teach the World to `Ping`"\_*

﻿

**fping 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

**OSI Layer 3** – **Network**

**### \*\*Phase 2\*\*:** *\_"Some `Syn` for Nothin`"\_*

**sudo nmap -sS 167.172.144.11**

﻿Nmap scan report for 167.172.144.11

Host is up (1.4s latency).

Not shown: 994 closed ports

PORT STATE SERVICE

22/tcp open ssh

**OSI Layer 4** – **Transport**

**### Phase 3:** *\_"I Feel a `DNS` Change Comin' On"\_*

﻿**nslookup rollingstone.com**

Server: 8.8.8.8

Address: 8.8.8.8#53

Non-authoritative answer:

Name: rollingstone.com

Address: 151.101.192.69

Name: rollingstone.com

Address: 151.101.128.69

Name: rollingstone.com

Address: 151.101.0.69

Name: rollingstone.com

Address: 151.101.64.69

**ssh** [**jimi@167.172.144.11**](mailto:jimi@167.172.144.11) **;** *password* **hendrix**

**﻿$ cat /etc/hosts**

# Your system has configured 'manage\_etc\_hosts' as True.

# As a result, if you wish for changes to this file to persist

# then you will need to either

# a.) make changes to the master file in /etc/cloud/templates/hosts.tmpl

# b.) change or remove the value of 'manage\_etc\_hosts' in

# /etc/cloud/cloud.cfg or cloud-config from user-data

#

127.0.1.1 GTscavengerHunt.localdomain GTscavengerHunt

127.0.0.1 localhost

98.137.246.8 rollingstone.com

$ exit

**nslookup 98.137.246.8**

﻿8.246.137.98.in-addr.arpa name = unknown.yahoo.com.

Authoritative answers can be found from:

**OSI Layer 7** – **Application**

**### Phase 4:** *\_"Sh`ARP` Dressed Man"\_*

**ssh** [**jimi@167.172.144.11**](mailto:jimi@167.172.144.11) **;** *password* **hendrix**

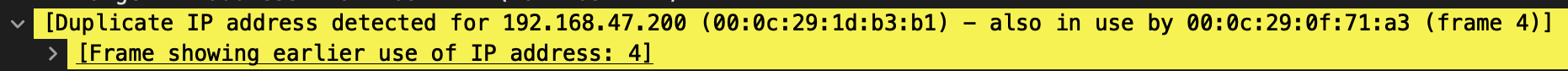
**ls /etc**

**cat /etc/packetcaptureinfo.txt**

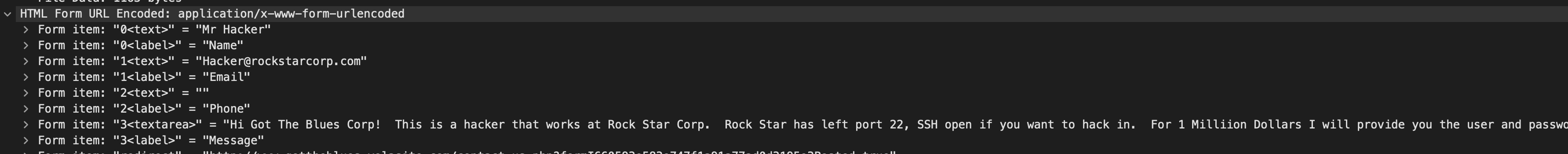
﻿Captured Packets are here:

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

MAC address of the hacker is at (00:0c:29:1d:b3:b1)



Hacker is found on POST /formservice/



**OSI Layer 6 - Presentation**