Home Work #8

Phase 1:

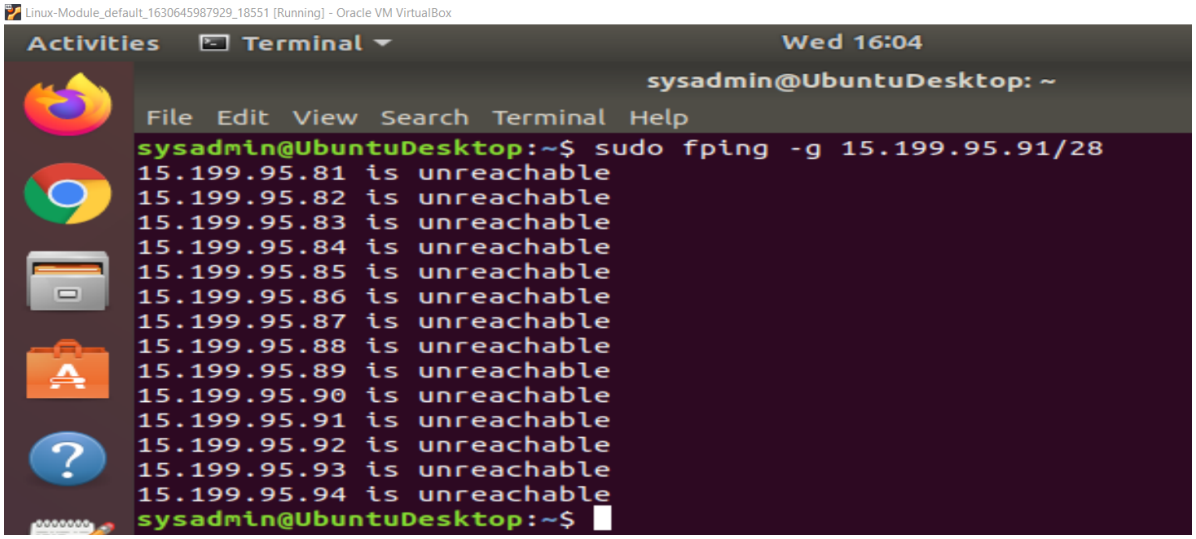
Rock Star

IP Range	Location+Server Type	Response
12.205.151.91/24	New York Database Servers	Unreachable
15.199.151.91/24	New York Web Servers	Unreachable
15.199.158.91/28	New York Web Servers	Unreachable
15.199.141.91/28	New York Web Servers	Unreachable
15.199.131.91/28	New York Application Servers	Unreachable
15.199.121.91/28	New York Application Servers	Unreachable
15.199.111.91/28	Chicago Database Servers	Unreachable
15.199.100.91/28	Chicago Web Servers	Unreachable
15.199.99.91/28	Chicago Web Servers	Unreachable
15.199.98.91/28	Chicago Web Servers	Unreachable
15.199.97.91/28	Chicago Application Servers	Unreachable
15.199.96.91/28	Chicago Application Servers	Unreachable
15.199.95.91/28	**Hollywood Database Servers**	**Unreachable**
15.199.94.91/28	**Hollywood Web Servers**	**Unreachable**
11.199.158.91/28/28	**Hollywood Web Servers**	**Unreachable**
167.172.144.11/32	**Hollywood Application Servers**	**Alive**
11.199.141.91/28	**Hollywood Application Servers**	**Unreachable**
11.199.131.91/28	Miami Database servers	Unreachable
11.199.121.91/29	Miami Web Servers	Unreachable
11.199.111.91/28	Miami Web Servers	Unreachable
11.199.100.91/32	Miami Web Servers	Unreachable
11.199.99.91/24	Miami Application Servers	Unreachable
11.199.98.91/28	Miami Database Servers	Unreachable

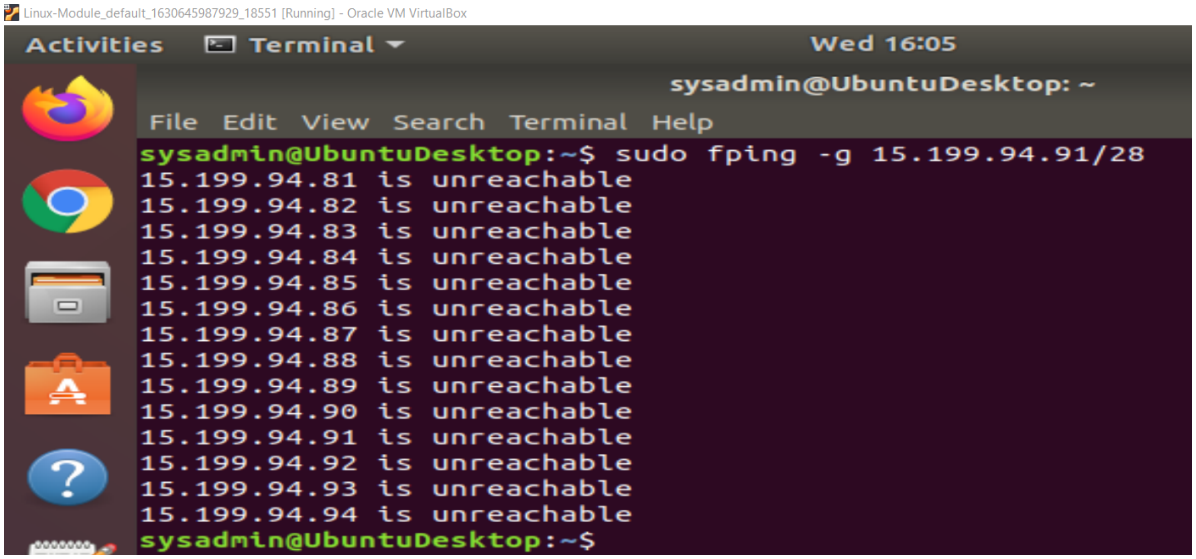
1. The command used for the connection is: fping -g <IP Address>

1.a: fping -g 15.199.95.91/28 ←----------**(Hollywood Database Servers)**
1.b: fping -g 15.199.94.91/28 ←----------**(Hollywood Web Servers)**
1.c: fping -g 11.199.158.91/28 ←----------**(Hollywood Web Servers)**
1.d: fping -g 167.172.144.11/32 ←----------**(Hollywood Application Servers)**
1.e: fping -g 11.199.141.91/28 ←----------**(Hollywood Application Servers)**

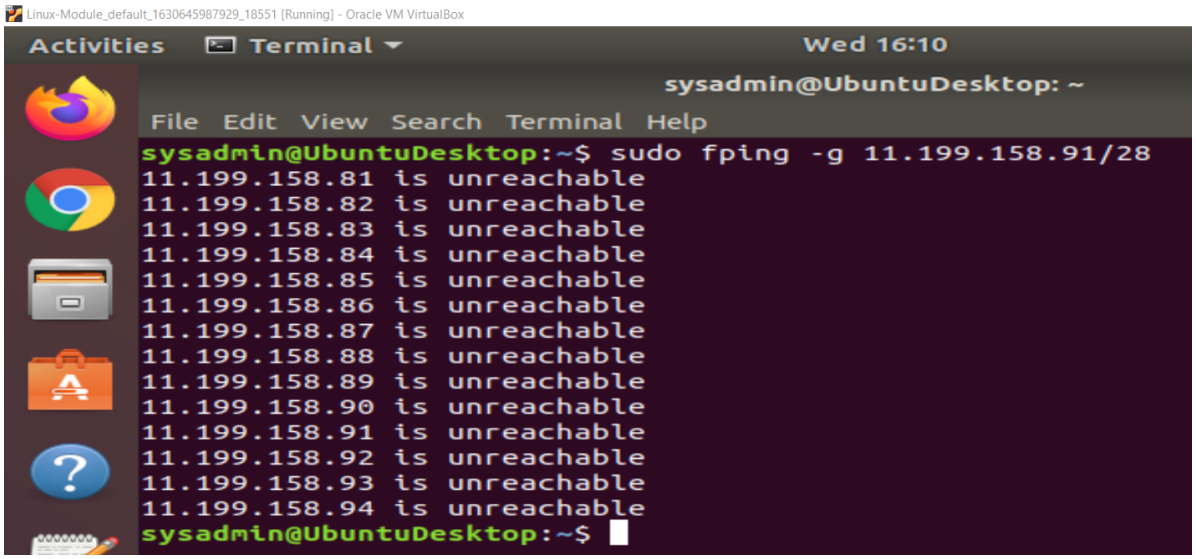
1.a:



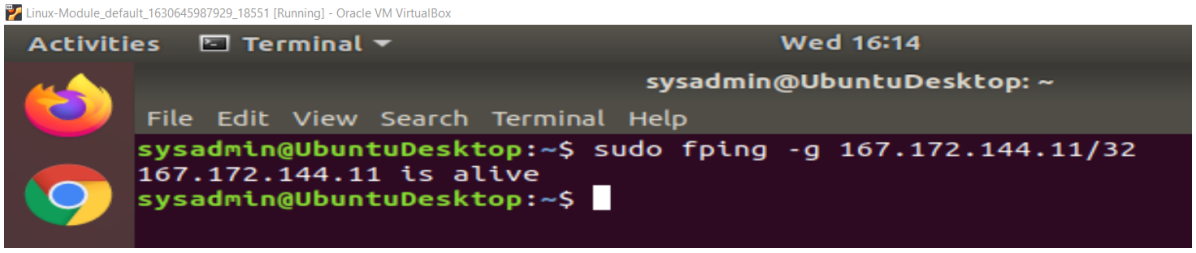
1.b:



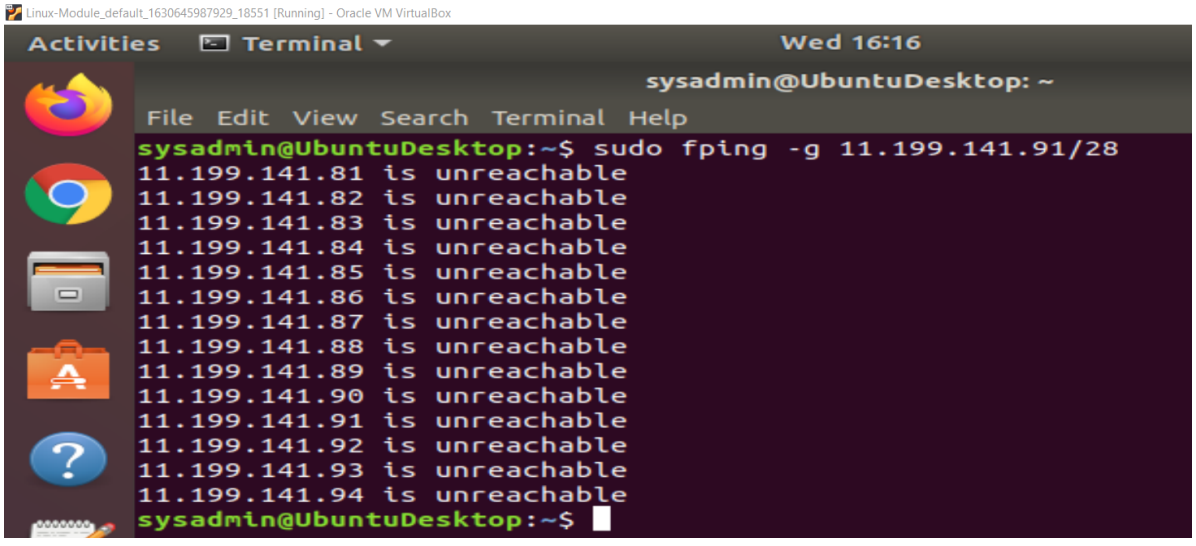
1C:


Linux-Module_default_1630645987929_18551 [Running] - Oracle VM VirtualBox
Activities
Terminal
Wed 16:10
sysadmin@UbuntuDesktop: ~
File Edit View Search Terminal Help
sysadmin@UbuntuDesktop:~$ sudo fping -g 11.199.158.91/28
11.199.158.81 is unreachable
11.199.158.82 is unreachable
11.199.158.83 is unreachable
11.199.158.84 is unreachable
11.199.158.85 is unreachable
11.199.158.86 is unreachable
11.199.158.87 is unreachable
11.199.158.88 is unreachable
11.199.158.89 is unreachable
11.199.158.90 is unreachable
11.199.158.91 is unreachable
11.199.158.92 is unreachable
11.199.158.93 is unreachable
11.199.158.94 is unreachable
sysadmin@UbuntuDesktop:~$

1d:


Linux-Module_default_1630645987929_18551 [Running] - Oracle VM VirtualBox
Activities
Terminal
Wed 16:14
sysadmin@UbuntuDesktop: ~
File Edit View Search Terminal Help
sysadmin@UbuntuDesktop:~$ sudo fping -g 167.172.144.11/32
167.172.144.11 is alive
sysadmin@UbuntuDesktop:~$

1e:


Linux-Module_default_1630645987929_18551 [Running] - Oracle VM VirtualBox
Activities
Terminal
Wed 16:16
sysadmin@UbuntuDesktop: ~
File Edit View Search Terminal Help
sysadmin@UbuntuDesktop:~$ sudo fping -g 11.199.141.91/28
11.199.141.81 is unreachable
11.199.141.82 is unreachable
11.199.141.83 is unreachable
11.199.141.84 is unreachable
11.199.141.85 is unreachable
11.199.141.86 is unreachable
11.199.141.87 is unreachable
11.199.141.88 is unreachable
11.199.141.89 is unreachable
11.199.141.90 is unreachable
11.199.141.91 is unreachable
11.199.141.92 is unreachable
11.199.141.93 is unreachable
11.199.141.94 is unreachable
sysadmin@UbuntuDesktop:~$

2. The only IP address that is accepting connection, is IP address number 167.172.144.11/32 which belongs to Hollywood Application Servers (see step 1.d).

3. Recommend to restrict ICMP echo requests against 167.172.144.11/32 to prevent successful responses from PING requests.

4. Since Rock Star Corp doesn't want to respond to any requests, that will be considered as a vulnerability.

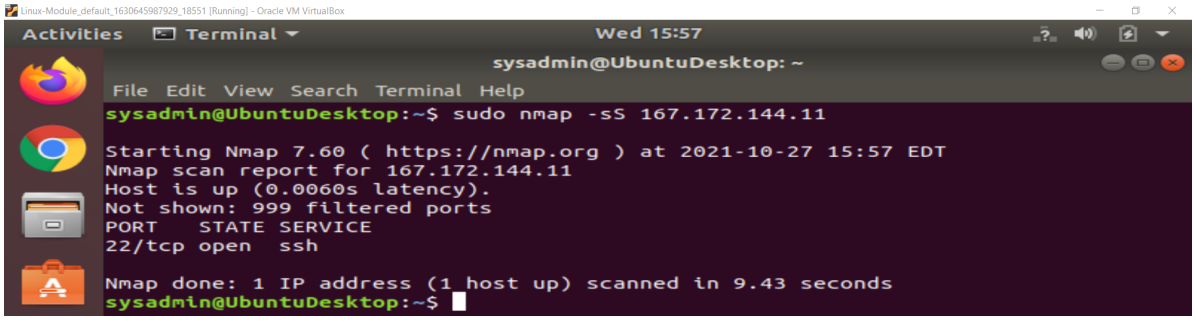
5. The IP (internet protocol) addresses in the OSI model are found in the Network layer.

phase 2:

1. The command used to run nmap with a SYN SCAN is:
   sudo nmap -sS 167.172.144.11
   for the IP address (alive) found from **phase 1**.

2. The scan results are as follow:
   port number: 22/tcp
   state of port: open
   service/protocol: ssh

3. Closed ports report are as follow:
   not shown: 999



4. The ports that are opened are as follow:
Port open: port number 22
OSI SYN SCAN 167.172.144.11/32

layer: Transportation layer

5. My recommendation is to protect/restrict access to port 22 with a firewall.

Phase 3:

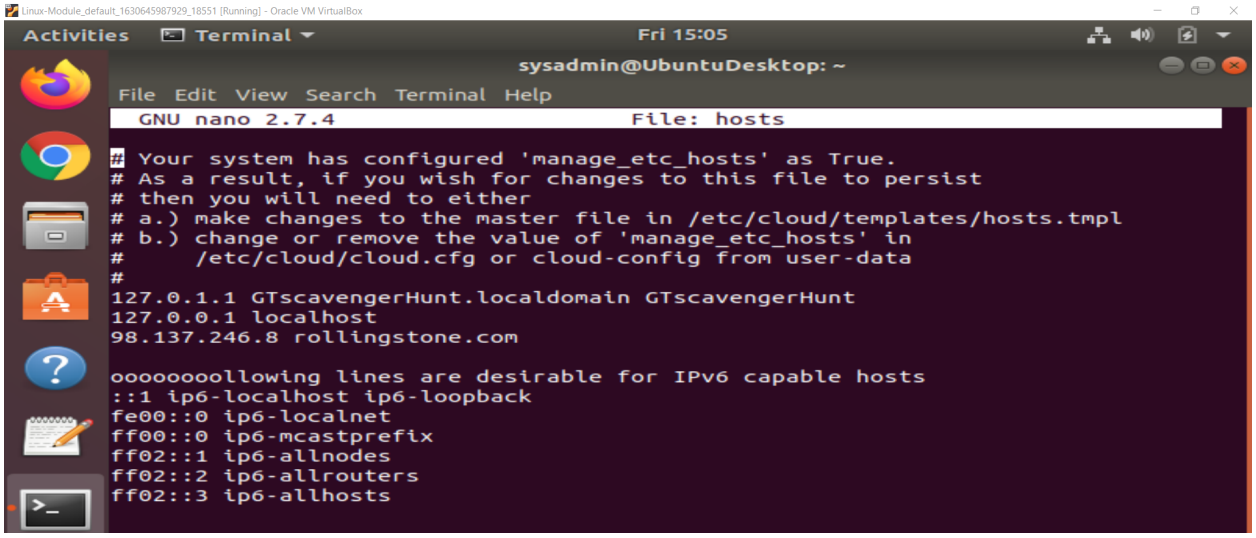
1. sudo ssh jimi@167.172.144.11 -p22
password: hendrix

1.A. cd /etc

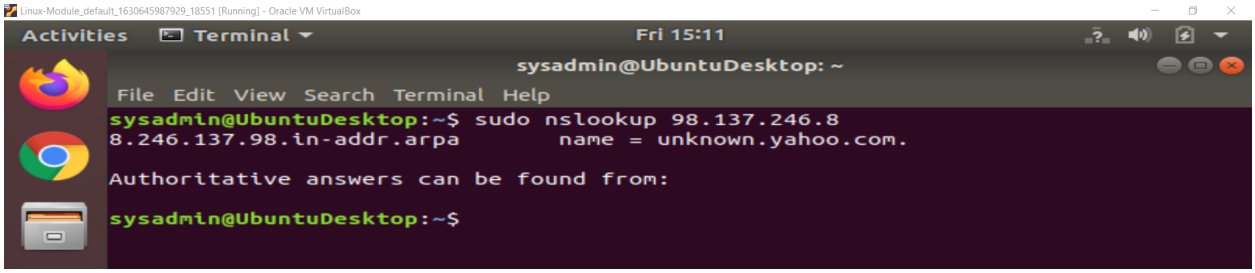
1.B. dir

1.C. nano hosts

It looks like someone **modified** the real rollingstone.com IP address **to** 98.137.246.8, which will redirect the access/view from rollingstone.com web page, to a different web page (see phase 3, step 2).



2. After exiting back to Sysadmin, I ran the command:
sudo nslookup 98.137.246.8 with the **modified** IP address (98.137.246.8) for rollingstone.com, I used the command above to discover the real domain of this IP, which is: unknown.yahoo.com

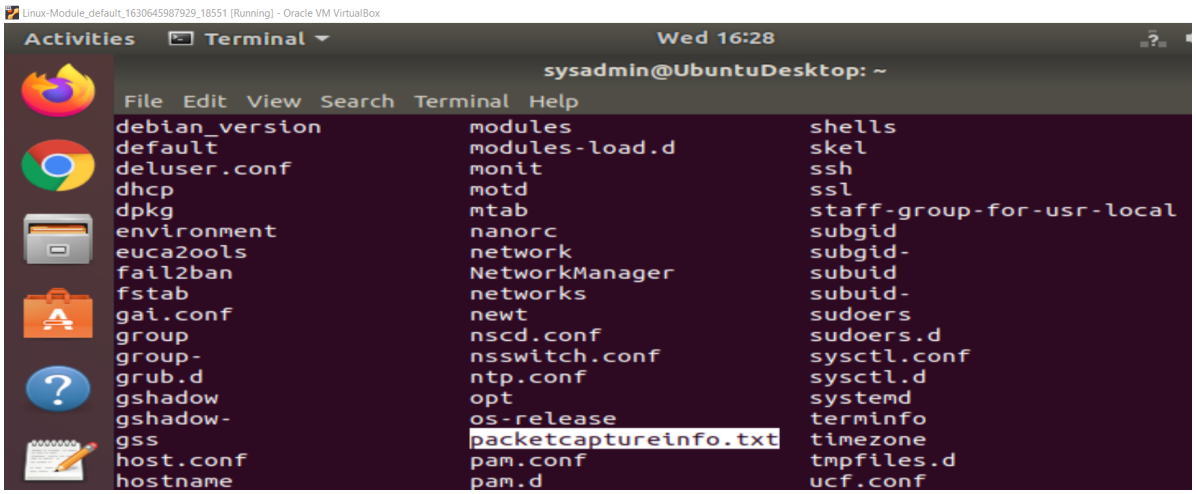


3. The OSI layer the unknown.yahoo.com domain was found, and where the command nslookup <domain name> can be run on is the application layer

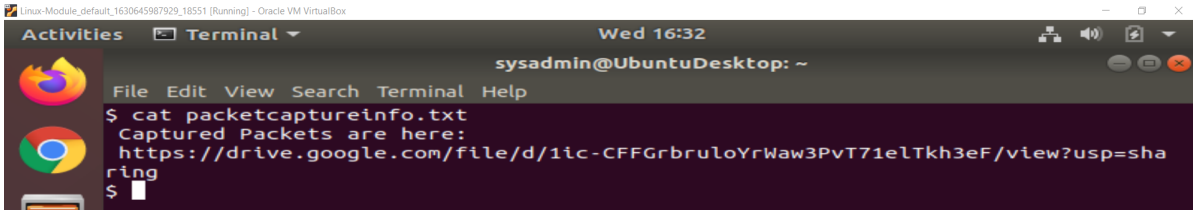
4. My recommendation is to erase the false IP address in the hosts file, and restore to real IP address (167.172.144.11) for rollingstone.com, and protect the hosts file with a password.

phase 4:

1. sudo ssh jimi@167.172.144.11
2. Password: hendrix
2. cd /etc
3. dir
4. Finding packetcaptureinfo.txt file within: /etc directory

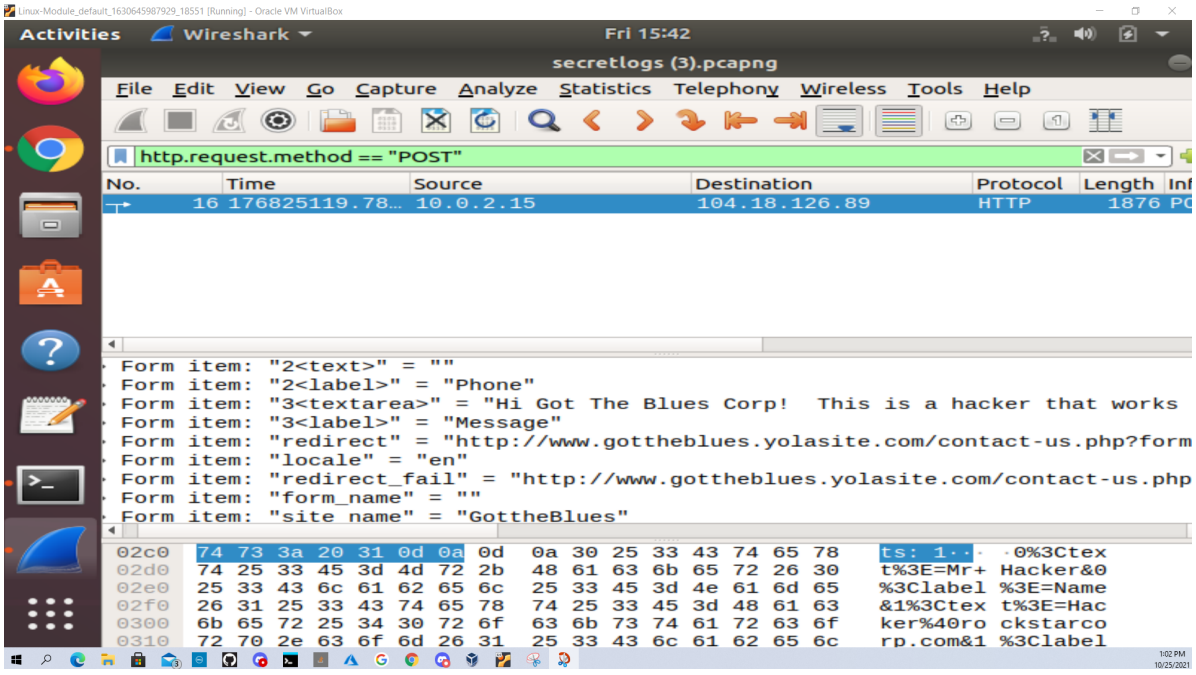


5. cat packetcaptureinfo.txt



6. Right click with mouse on the link, and press open link in the VM. Press download, and open with wireshark. In the filter bar type:
http.request.method == "post"

7. Under HTML Form URL encoded 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 Million dollars I will provide you the user and password!"



8. My recommendation is to protect and/or restrict access to port 22 with a firewall.

9. The OSI layer is the Data link layer, since the hacker used port 22, and it is on the Data link layer.