Edwin Sierra

Homework #8

***Phase 1***

Using the tool located at <https://www.ipaddressguide.com/cidr> I was able to get the following IP address ranges. I then ran the command **fping <ip address>** for each one to determine which one was accepting connections.

Range 15.199.95.80 – 15.199.95.95

Range 15.199.94.80 – 15.199.94.95

Range 11.199.141.80 – 11.199.141.95

Range 11.199.158.80 – 11.199.158.95

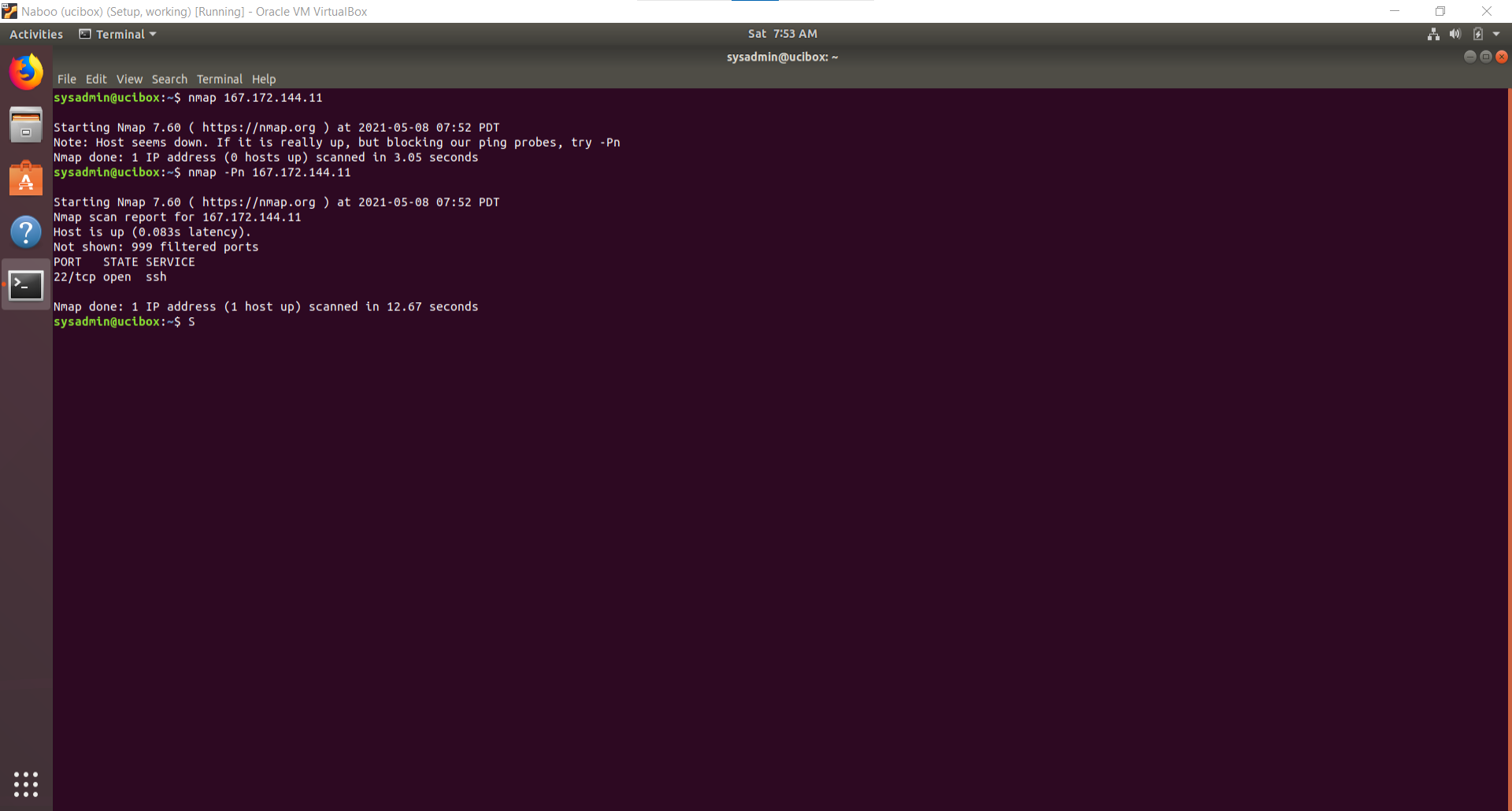
All IP addresses in these ranges are not accepting connections.

**167.172.144.11** is accepting connections and is a vulnerability.

Fping uses the network layer of the OSI model.

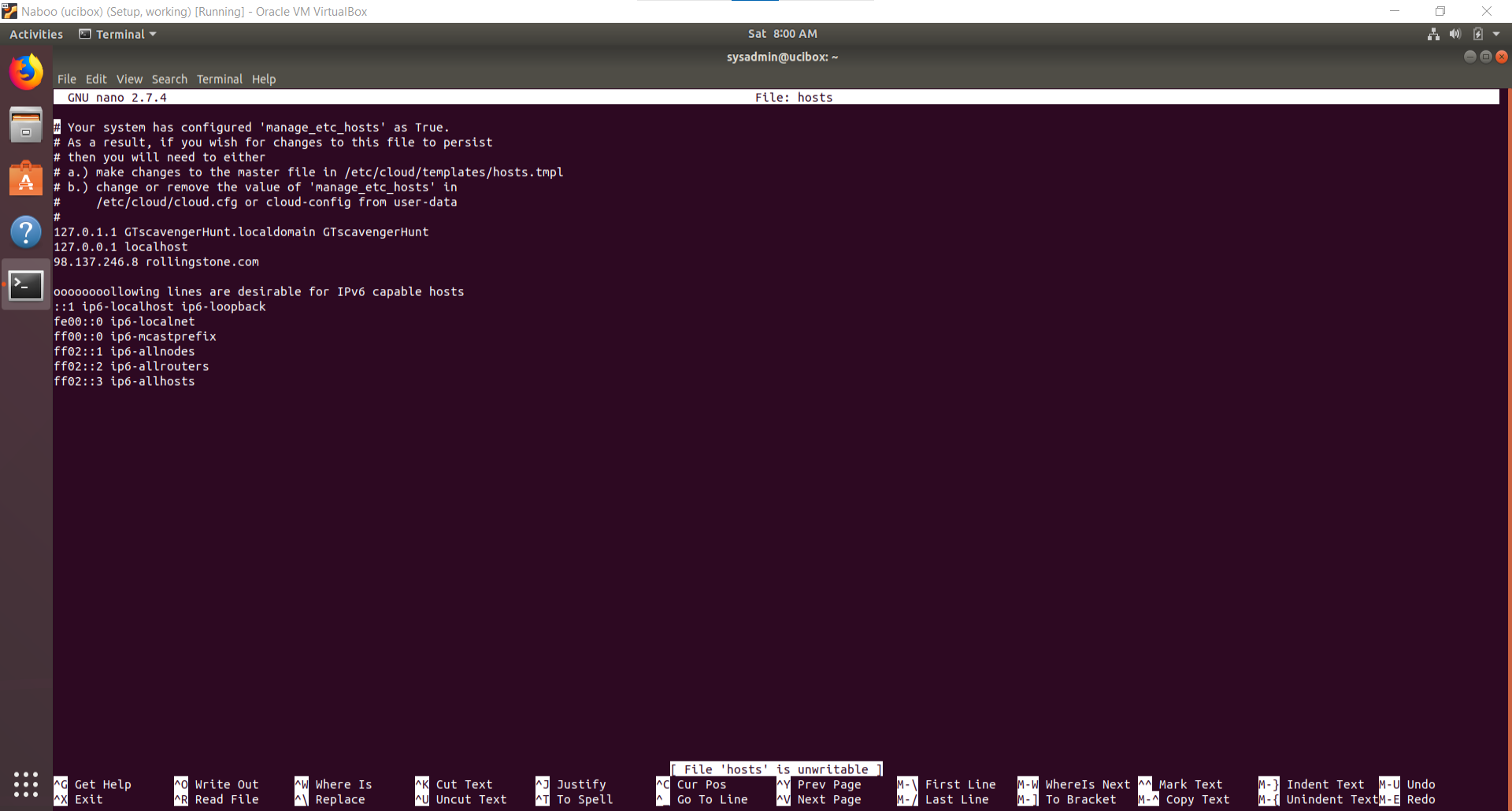
***Phase 2***

Next did a SYN scan to check for open ports. The command **nmap -sS 167.172.144.11** took over 1.5 hours to complete and didn’t complete properly. I ran the suggested command **nmap -Pnann 167.172.144.11.**  This determined that the SSH port 22 was open and accepting connections. **nmap runs on the transport layer of the OSI model.**

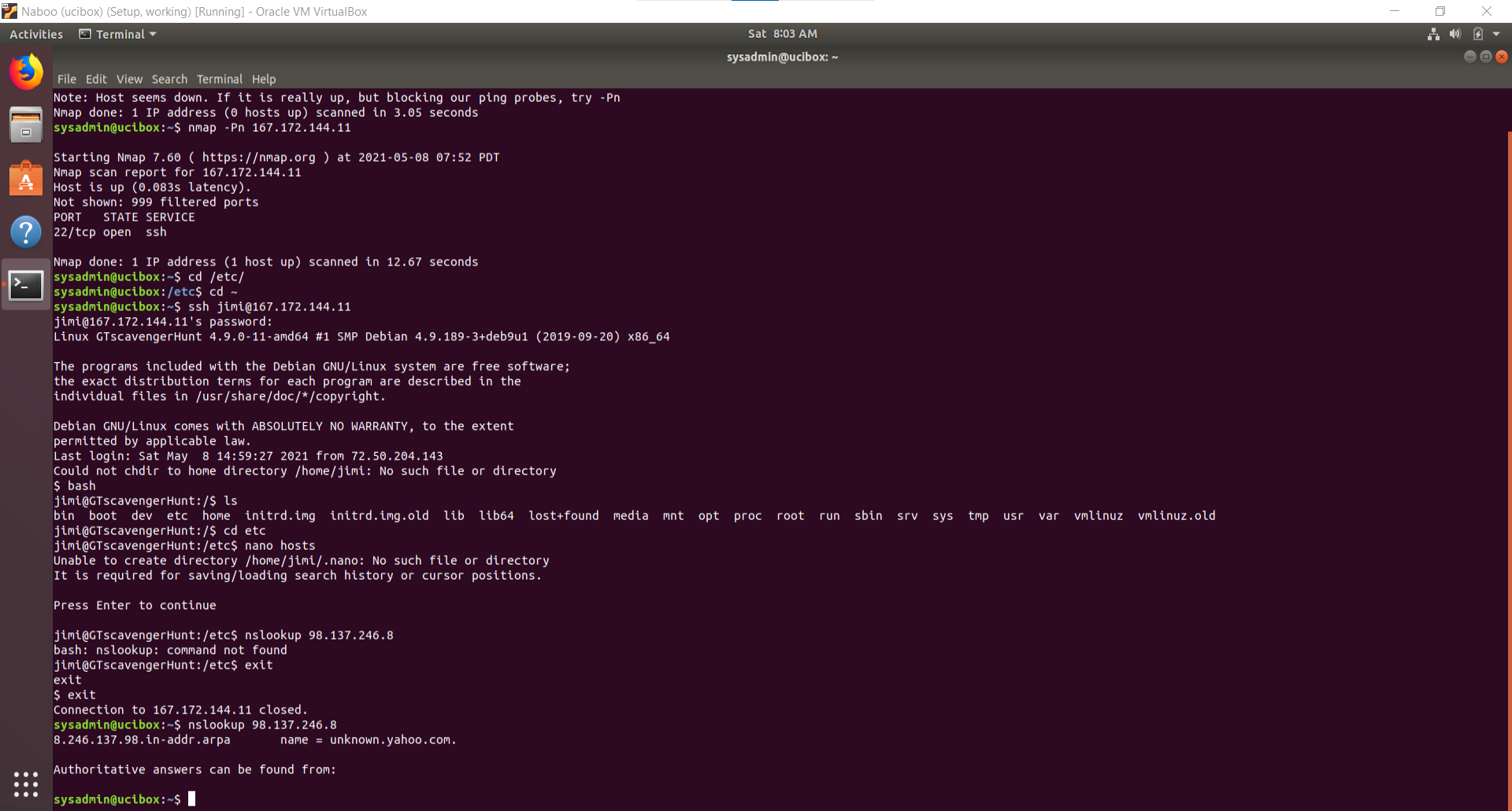


***Phase 3***

Next, I tried to see if I could connect to the IP address via SSH by running **ssh** [**jimi@167.172.144.11**](mailto:jimi@167.172.144.11) **-p 22**. I was able to log on using the password **hendix.** Next step was to verify the hosts file to see if there were any DNS re-directing. This file is located by using **cd /etc/hosts**. Using **nano /etc/hosts** showed that [www.rollingstone.com](http://www.rollingstone.com) was being redirected to **98.137.246.8**.



We were able to determine the correct domain by using **nslookup 98.137.246.8** which showed that the domain was unknown.yahoo.com. **nslookup runs on the application layer of the OSI model**.

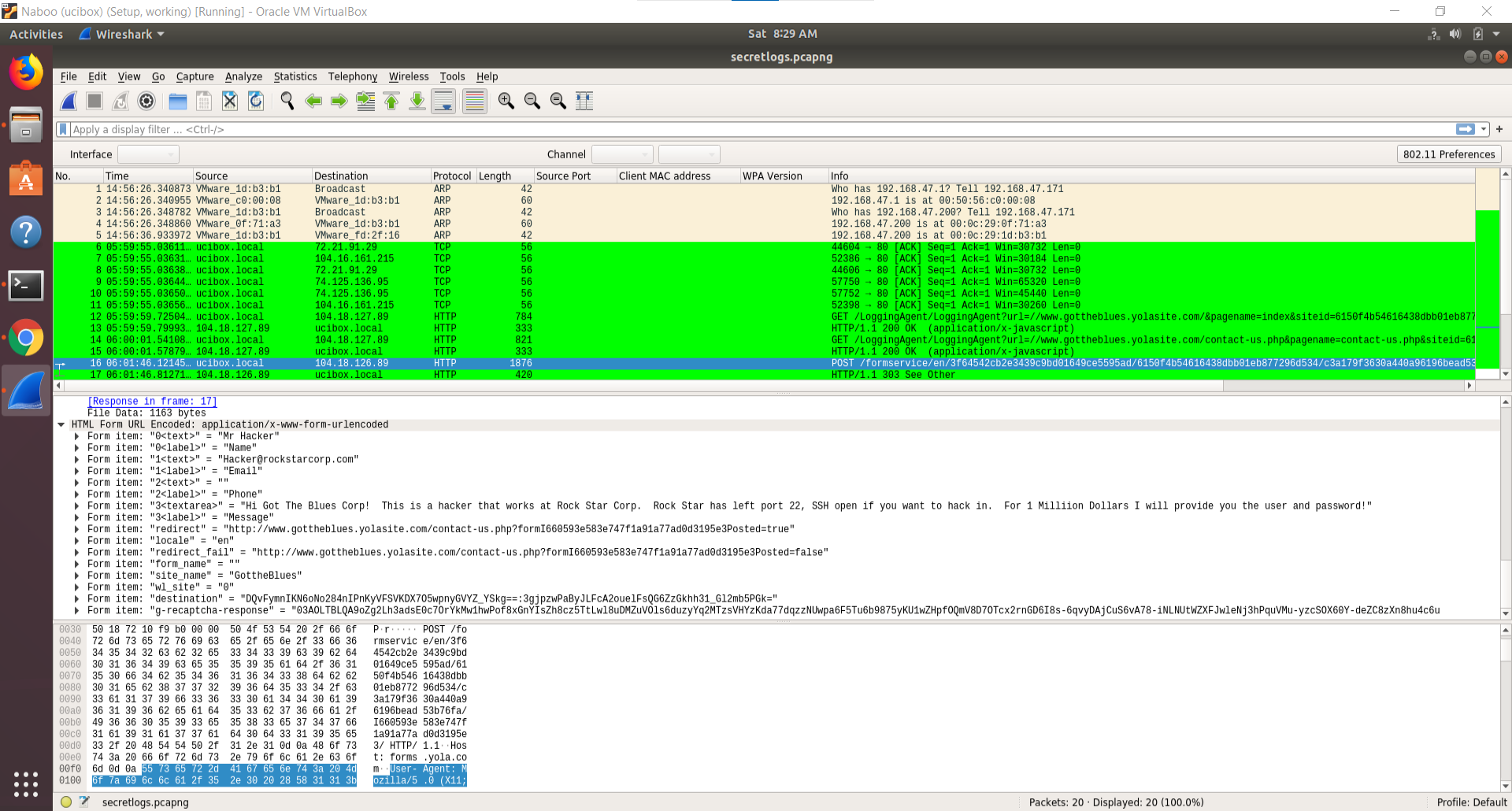


***Phase 4***

Within the **/etc/** directory there was a file called **packetcaptureinfo.txt** that led to google drive pcap file. File was downloaded and opened with wireshark.

**Attacker is spoofing MAC address. Attacker has access to data being sent and received from 192.168.47.200. Attacker’s MAC address likely to be 00:0c:29:1d:b3:b1.**

**Attacker also sent a form to Got the Blues Corp letting them know that an ssh port was open and asking for money to get the user name and password.**

****