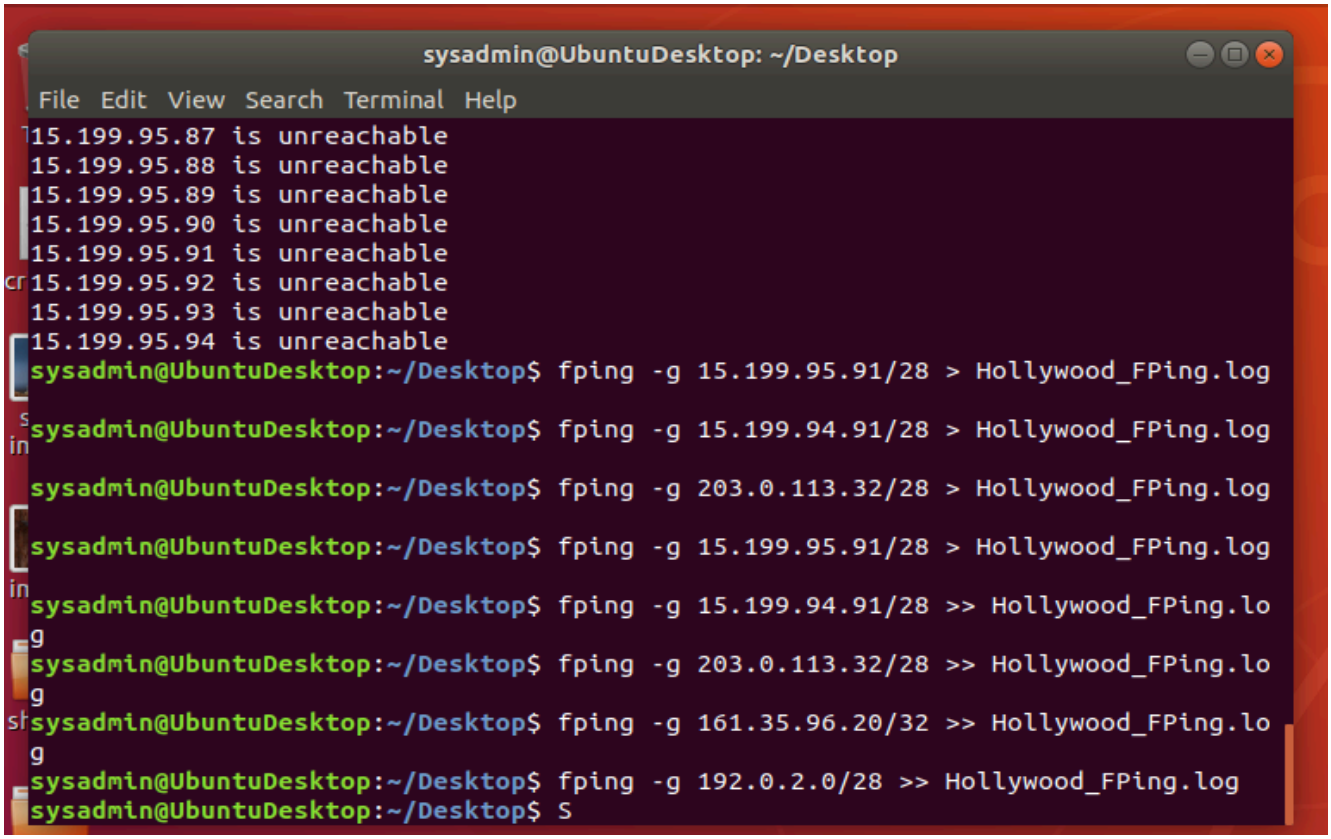
Phase 1: I'd like to teach the world PING

I downloaded a document that contained the ip ranges and used the command fping on the list of ips given for the Hollywood offices

fping -g <ip address>
fping -g 203.0.113.32/28 > Hollywood_FPing.log

```
 269  fping -g 15.199.95.91/28 > Hollywood_FPing.log
 270  fping -g 15.199.94.91/28 >> Hollywood_FPing.log
 271  fping -g 203.0.113.32/28 >> Hollywood_FPing.log
 272  fping -g 161.35.96.20/32 >> Hollywood_FPing.log
 273  fping -g 192.0.2.0/28 >> Hollywood_FPing.log
```



cat Hollywood_FPing.log
cat Hollywood_FPing.log | grep alive

The only **IP** that was found was: 161.35.96.20 while the other IPs were labeled unreachable

```
sysadmin@UbuntuDesktop:~/Desktop$ cat Hollywood_FPing.log | grep alive
161.35.96.20 is alive
```

Since we are using the **Fping** utility and it uses the ICMP which operates on Layer 3 networking. (Echo/echo reply messages are used by the well-known PING command, which allows a user to send an echo to a receiving host, which sends an echo reply if echo is received)

Sources: https://www.pcwdld.com/what-is-icmp-and-port
https://stackoverflow.com/questions/67094784/osi-model-layer

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

Sudo nmap -sS 161.35.96.20

```
sysadmin@UbuntuDesktop: ~/Desktop
File  Edit  View  Search  Terminal  Help
sysadmin@UbuntuDesktop:~/Desktop$ nmap -sS 161.35.96.20
You requested a scan type which requires root privileges.
QUITTING!
sysadmin@UbuntuDesktop:~/Desktop$ sudo nmap -sS 161.35.96.20
[sudo] password for sysadmin:

Starting Nmap 7.60 ( https://nmap.org ) at 2023-02-06 14:15 EST
Nmap scan report for 161.35.96.20
Host is up (0.00055s latency).
Not shown: 990 filtered ports
PORT     STATE  SERVICE
22/tcp   open   ssh
80/tcp   closed http
110/tcp  closed pop3
111/tcp  closed rpcbind
587/tcp  closed submission
995/tcp  closed pop3s
1025/tcp closed NFS-or-IIS
3389/tcp closed ms-wbt-server
```

The SSH port was open with the **IP 161.35.96.20**

The **transport layer (layer 4)** is used for things like **SYN scans**, and to detect which ports are open. Sequence number detection, which happens at layer 4 is important to OS detection.

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

Sudo ssh jimi@161.35.96.20 -22 -p 22
password : hendrix

```
$ cat 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 gtclass-1578758377314-s-1vcpu-1gb-nyc1-01.localdomain gtclass-1578758377314-s-1vcp
u-1gb-nyc1-01
127.0.0.1 localhost
98.137.246.8 rollingstone.com

# The following lines are desirable for IPv6 capable hosts
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts

$
```

The ip received was 98.134.246.8 rollingstonde.com
Then exited the the /etc/hosts and used the exit command to end session.

The main reason that /etc/hosts (or the windows equivalent %SYSTEMROOT%\system32\drivers\etc\hosts) are used by attackers is to redirect user traffic to sites under their control. It's important to note that hosts files are used in preference to DNS servers, so even if the user has a good entry in DNS for a specific system, hosts will still take precedence

```
sysadmin@UbuntuDesktop:~/Desktop$ nslookup 98.137.246.8
8.246.137.98.in-addr.arpa       name = unknown.yahoo.com.

Authoritative answers can be found from:

sysadmin@UbuntuDesktop:~/Desktop$ sudo nslookup 98.137.246.8
[sudo] password for sysadmin:
8.246.137.98.in-addr.arpa       name = unknown.yahoo.com.

Authoritative answers can be found from:
```

Phase 4: *"ShARP Dressed Man"*

ssh jimi@161.35.96.20 -22

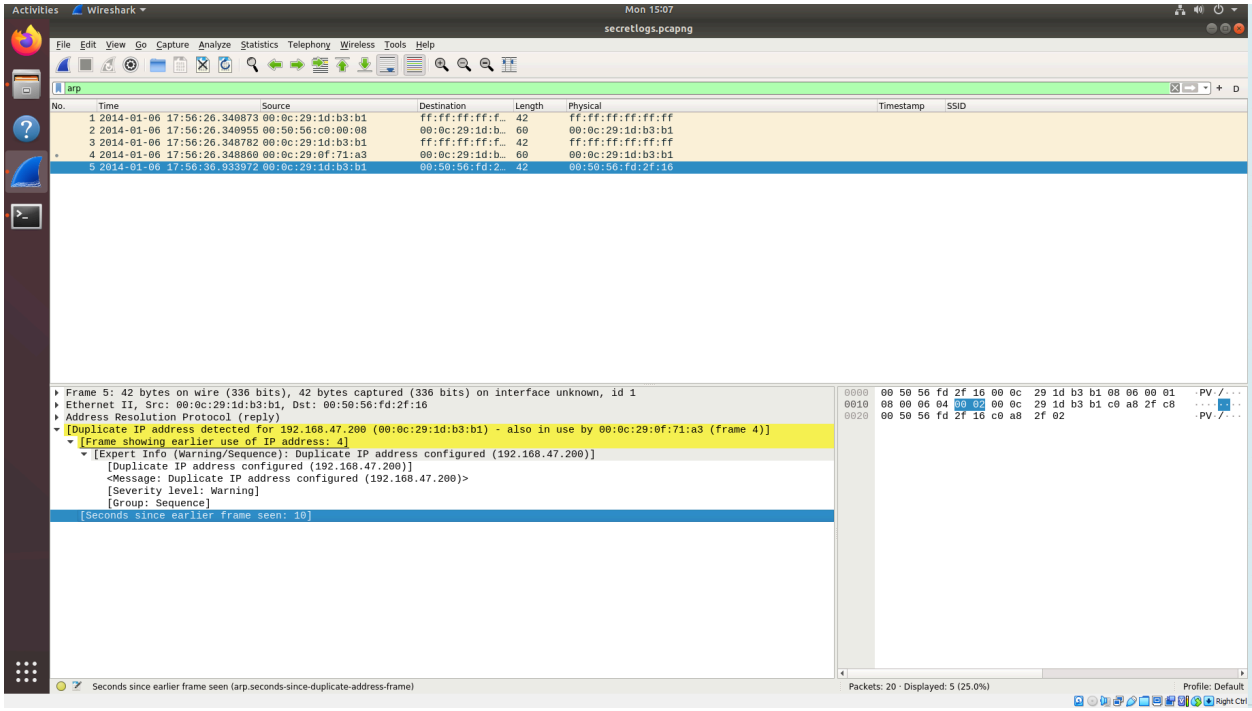
Then moved to the /etc/

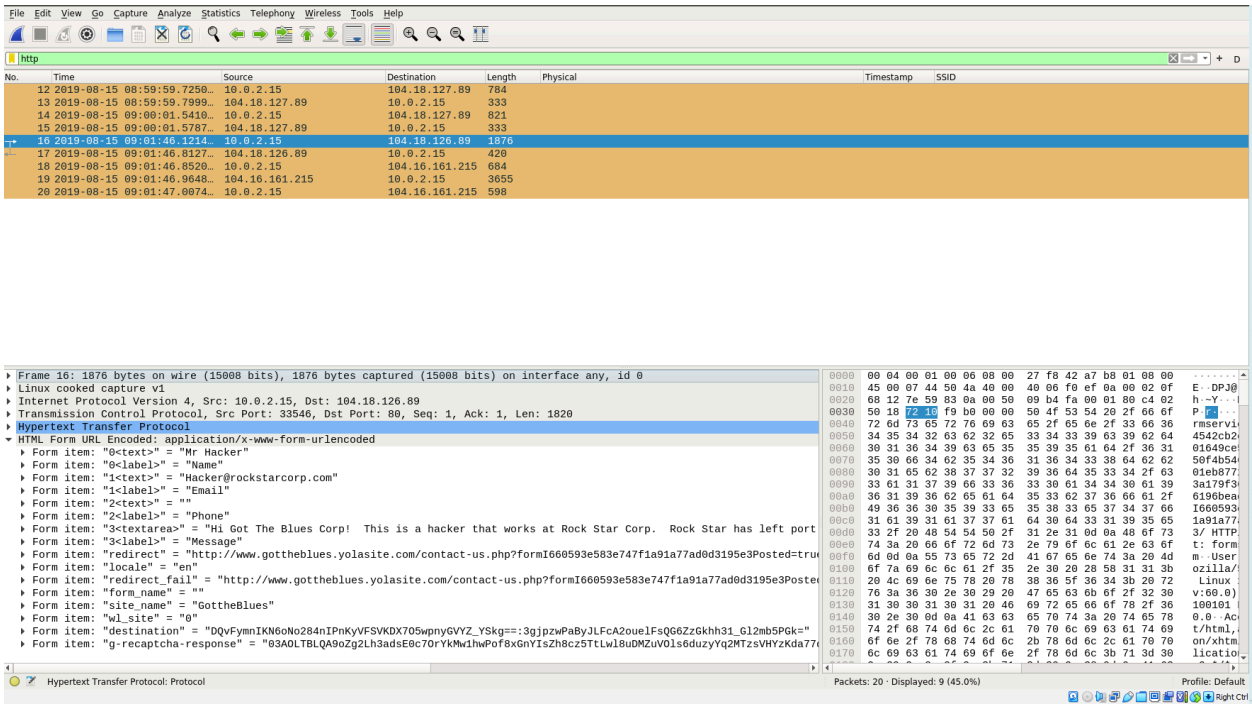
The next command I used was ls -lah

I then found the packectcaptureinfo.txt

Then used cat and found a link:
https://drive.google.com/file/d/1ic-CFFGrbruloYrWaw3PvT71elTkh3eF/view

Then downloaded the file and used Wireshark to inspect ARP and HTTP


Activities
Wireshark
Mon 15:07
secretlogs.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
arp
No. Time Source Destination Length Physical Timestamp SSID
1 2014-01-06 17:56:26.340873 00:0c:29:1d:b3:b1 ff:ff:ff:ff:f… 42 ff:ff:ff:ff:ff:ff
2 2014-01-06 17:56:26.340955 00:50:56:c0:00:08 00:0c:29:1d:b… 60 00:0c:29:1d:b3:b1
3 2014-01-06 17:56:26.348782 00:0c:29:1d:b3:b1 ff:ff:ff:ff:f… 42 ff:ff:ff:ff:ff:ff
4 2014-01-06 17:56:26.348860 00:0c:29:0f:71:a3 00:0c:29:1d:b… 60 00:0c:29:1d:b3:b1
5 2014-01-06 17:56:36.933972 00:0c:29:1d:b3:b1 00:50:56:fd:2… 42 00:50:56:fd:2f:16
Frame 5: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface unknown, id 1
Ethernet II, Src: 00:0c:29:1d:b3:b1, Dst: 00:50:56:fd:2f:16
Address Resolution Protocol (reply)
[Duplicate IP address detected for 192.168.47.200 (00:0c:29:1d:b3:b1) - also in use by 00:0c:29:0f:71:a3 (frame 4)]
[Frame showing earlier use of IP address: 4]
[Expert Info (Warning/Sequence): Duplicate IP address configured (192.168.47.200)]
[Duplicate IP address configured (192.168.47.200)]
<Message: Duplicate IP address configured (192.168.47.200)>
[Severity level: Warning]
[Group: Sequence]
[Seconds since earlier frame seen: 10]
0000 00 50 56 fd 2f 16 00 0c 29 1d b3 b1 08 06 00 01
0010 08 00 06 04 00 02 00 0c 29 1d b3 b1 c0 a8 2f c8
0020 00 50 56 fd 2f 16 c0 a8 2f 02
Seconds since earlier frame seen (arp.seconds-since-duplicate-address-frame)
Packets: 20 · Displayed: 5 (25.0%)
Profile: Default


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Length Physical Timestamp SSID
12 2019-08-15 08:59:59.7250… 10.0.2.15 104.18.127.89 784
13 2019-08-15 08:59:59.7999… 104.18.127.89 10.0.2.15 333
14 2019-08-15 09:00:01.5410… 10.0.2.15 104.18.127.89 821
15 2019-08-15 09:00:01.5787… 104.18.127.89 10.0.2.15 333
16 2019-08-15 09:01:46.1214… 10.0.2.15 104.18.126.89 1876
17 2019-08-15 09:01:46.8127… 104.18.126.89 10.0.2.15 420
18 2019-08-15 09:01:46.8520… 10.0.2.15 104.16.161.215 684
19 2019-08-15 09:01:46.9648… 104.16.161.215 10.0.2.15 3655
20 2019-08-15 09:01:47.0074… 10.0.2.15 104.16.161.215 598
Frame 16: 1876 bytes on wire (15008 bits), 1876 bytes captured (15008 bits) on interface any, id 0
Linux cooked capture v1
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 104.18.126.89
Transmission Control Protocol, Src Port: 33546, Dst Port: 80, Seq: 1, Ack: 1, Len: 1820
Hypertext Transfer Protocol
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
Form item: "3<label>" = "Message"
Form item: "redirect" = "http://www.gottheblues.yolasite.com/contact-us.php?formI660593e583e747f1a91a77ad0d3195e3Posted=tru
Form item: "locale" = "en"
Form item: "redirect_fail" = "http://www.gottheblues.yolasite.com/contact-us.php?formI660593e583e747f1a91a77ad0d3195e3Poste
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" = "03AOLTBLQA9oZg2Lh3adsE0c7OrYkMw1hwPof8xGnYIsZh8cz5TtLwl8uDMZuVOls6duzyYq2MTzsVHYzKda77
0000 00 04 00 01 00 06 08 00 27 f8 42 a7 b8 01 08 00
0010 45 00 07 44 50 4a 40 00 40 06 f0 ef 0a 00 02 0f
0020 68 12 7e 59 83 0a 00 50 09 b4 fa 00 01 80 c4 02
0030 50 18 72 1c f9 b0 00 00 50 4f 53 54 20 2f 66 6f
0040 72 6d 73 65 72 76 69 63 65 2f 65 6e 2f 33 66 36
0050 34 35 34 32 63 62 32 65 33 34 33 39 63 39 62 64
0060 30 31 36 34 39 63 65 35 35 39 35 61 64 2f 36 31
0070 35 30 66 34 62 35 34 36 31 36 34 33 38 64 62 62
0080 30 31 65 62 38 37 37 32 39 36 64 35 33 34 2f 63
0090 33 61 31 37 39 66 33 36 33 30 61 34 34 30 61 39
00a0 36 31 39 36 62 65 61 64 35 33 62 37 36 66 61 2f
00b0 49 36 36 30 35 39 33 65 35 38 33 65 37 34 37 66
00c0 31 61 39 31 61 37 37 61 64 30 64 33 31 39 35 65
00d0 33 2f 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73
00e0 74 3a 20 66 6f 72 6d 73 2e 79 6f 6c 61 2e 63 6f
00f0 6d 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d
0100 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 58 31 31 3b
0110 20 4c 69 6e 75 78 20 78 38 36 5f 36 34 3b 20 72
0120 76 3a 36 30 2e 30 29 20 47 65 63 6b 6f 2f 32 30
0130 31 30 30 31 30 31 20 46 69 72 65 66 6f 78 2f 36
0140 30 2e 30 0d 0a 41 63 63 65 70 74 3a 20 74 65 78
0150 74 2f 68 74 6d 6c 2c 61 70 70 6c 69 63 61 74 69
0160 6f 6e 2f 78 68 74 6d 6c 2b 78 6d 6c 2c 61 70 70
0170 6c 69 63 61 74 69 6f 6e 2f 78 6d 6c 3b 71 3d 30
Hypertext Transfer Protocol: Protocol
Packets: 20 · Displayed: 9 (45.0%)
Profile: Default