Rayshaun McIntosh

Homework 8

## Phase 1

My initial Ping

I started by pinging all the IP addresses of the Hollywood office using the following syntax: fping -g [Beginning range IP Address] [Ending range IP Address] Example: fping -g 15.199.95.28 15.199.95.91

I did this to find out which IP Addresses were alive and which ones were unreachable. The results were as follows:

15.199.95.28/91 Hollywood Database Servers were **Unreachable**.

15.199.94.28/91 Hollywood Web Servers were **Unreachable**.

11.199.158.28/91 Hollywood Web Servers were **Unreachable**.

11.199.141.28/91 Hollywood Application Servers were **Unreachable**.

167.172.144.11/18 Hollywood Application Servers were **Alive**.

167.172.144.19 Hollywood Application Servers were **Unreachable**.

167.172.144.20/24 Hollywood Application Servers were **Alive**.

167.172.144.25 Hollywood Application Servers were **Unreachable**.

167.172.144.26/32 Hollywood Application Servers were **Alive**.

When referring to the OSI Model, Layer 3 Network is where this process would fall under.

## Phase 2

The syntax I used to obtain this information was 'sudo nmap -sS [IP Address] [ IP Address] [IP Address]'

I initially tried to scan all the ports at once but it was taking a long time so I decided to scan them 3 at a time.

| IP Address | Ports Open | Services |
|---|---|---|
| 167.172.144.11 | 22/TCP | SSH |
| 167.172.144.12 | 22,80,443/TCP | SSH, HTTP, HTTPS |
| 167.172.144.13 | 22/TCP | SSH |
| 167.172.144.14 | 22,80,443/TCP | SSH, HTTP, HTTPS |
| 167.172.144.15 | 22,80,81,443/TCP | SSH, HTTP, HOSTS2-NS, HTTPS |
| 167.172.144.16 | 22,80,443/TCP | SSH, HTTP, HTTPS |
| 167.172.144.17 | 22,80/TCP | SSH, HTTP |
| 167.172.144.18 | 22,80,9090/TCP | SSH, HTTP, ZEUS-ADMIN |
| 167.172.144.20 | 22,80,3306/TCP | SSH, HTTP, MYSQL |
| 167.172.144.21 | 22,80,443/TCP | SSH, HTTP, HTTPS |

| | | |
|---|---|---|
| 167.172.144.22 | 22,80,443/TCP | SSH, HTTP, HTTPS |
| 167.172.144.23 | 22,80,443/TCP | SSH, HTTP, HTTPS |
| 167.172.144.24 | 22,80,443/TCP | SSH, HTTP, HTTPS |
| 167.172.144.26 | 22/TCP | SSH |
| 167.172.144.27 | 22/TCP | SSH |
| 167.172.144.28 | 22,80,443/TCP | SSH, HTTP, HTTPS |
| 167.172.144.29 | 80,443/TCP | HTTP, HTTPS |
| 167.172.144.30 | 21,22,53,80,106,110,143, 443,465,993,995,8443 | FTP,SSH,DOMAIN,HTTP, POP3PW,POP3,IMAP,HTTPS, SMTPS,IMAPS,POP3S, HTTPS-ALT |
| 167.172.144.31 | 22/TCP | SSH |
| 167.172.144.32 | 22/TCP | SSH |

Red highlighted = suspecious ports, could be vulnerable to an attack if not already being attacked. I would recommend closing all ports that are not needed.

I looked up a list of TCP and UDP port numbers to confirm open ports and what they should be compared to what they actually are. (Wikipedia, 2022)

The OSI Model would be Layer 4 Transport.

## Phase 3

For me to gain remote access I had to use the command 'ssh jimi@167.172.144.11-p 80'.

After submitting the password I wanted to see what rights the user had, so I used the command 'id' to see of jimi had sudo priveledges, which he did not.

Once I knew the rights I had under the user I used the command 'ls' to list the directory I was in. I immediately noticed the etc directory so I used the 'cd etc' command so I could access the directory.

I seen the hosts file and use the command 'cat hosts' to read the file. There I found the rollingstone.com was being redirected to a 98.137.246.8 IP address. I made a copy of the IP address, exited the ssh use this command to see who this IP address belong to using 'nslookup 98.137.246.8'. The results were 'name = unknown.yahoo.com'.

The OSI Model would be Layer 6 Presentation

## Phase 4

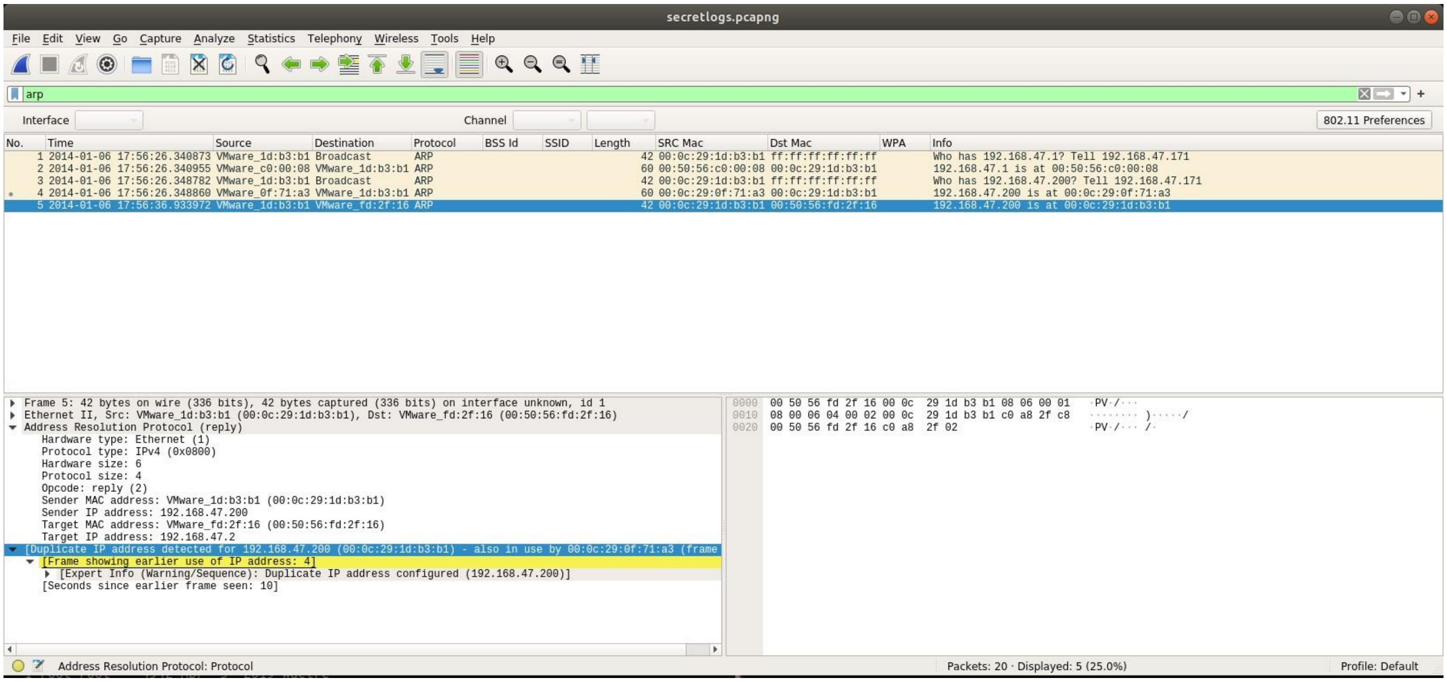
For me to gain remote access I used the command 'ssh jimi@167.172.144.11-p 80' again. I went back to the etc directory and discovered an unusual txt document named packetcaptureinfo.txt. The command I used to take a look at the file was 'cat packetcaptureinfo.txt'. When I did that a google drive link was present. https://drive.google.com/file/d/1ic-CFFGrbruloYrWaw3PvT71elTkh3eF/view?usp=sharing .

Once I open the link a secretlogs.pcapng file was present. I downloaded the file and opened it in wireshark to check the file.

The first thing I did was filter the packets by arp. I was left with 5 displayed packets. The first four packets seemed normal but the fifth packet had an Duplication IP address detected alert

192.168.47.200 and different Mac address 00:0c:29:0f:71:a3. This shows signs of a Man in the Middle attack.

To prevent such an attack in the future make sure you are using high-security web browsers and ensure all sensitive online transactions or logins are secured with HTTPS. You can also install IDS (Intrusion Detection System) to monitor you network and alert you of suspecious activity. (System, 2022)


secretlogs.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Interface
Channel
802.11 Preferences

```
arp
```

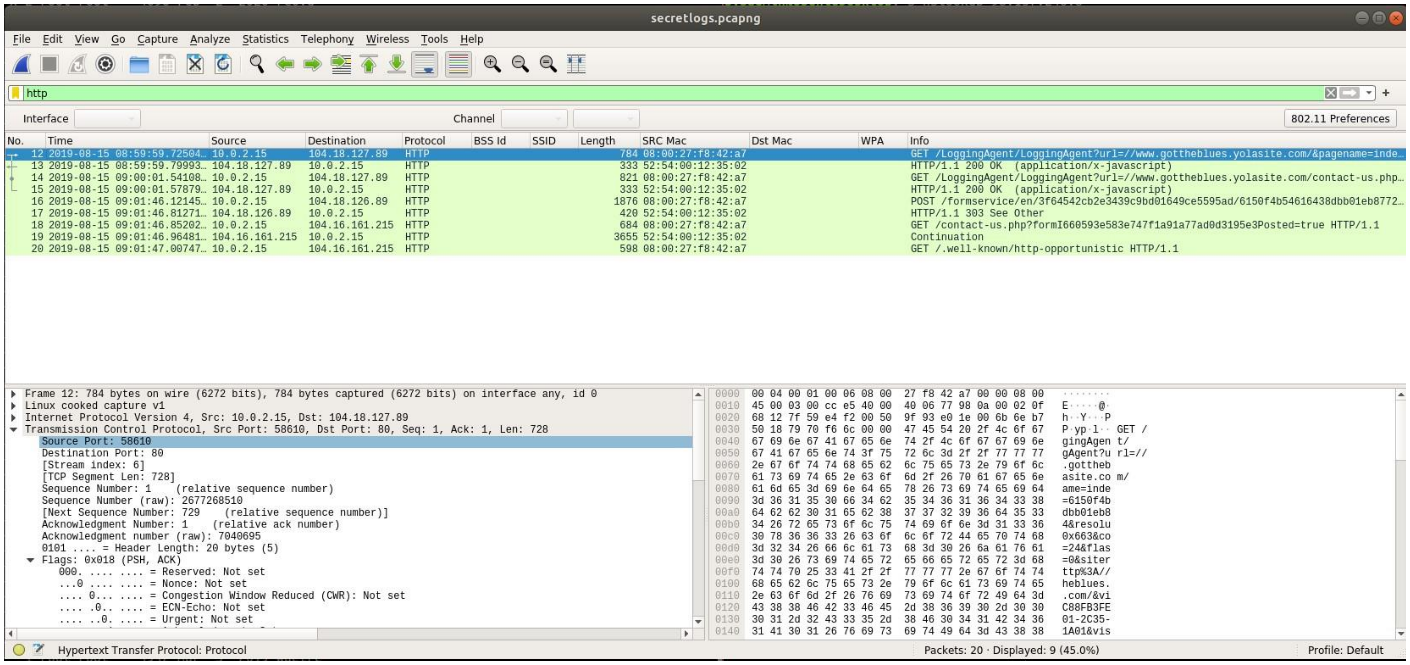
```
No.  Time                       Source            Destination       Protocol  BSS Id  SSID  Length  SRC Mac            Dst Mac            WPA  Info
  1 2014-01-06 17:56:26.340873 VMware_1d:b3:b1 Broadcast       ARP                            42 00:0c:29:1d:b3:b1 ff:ff:ff:ff:ff:ff      Who has 192.168.47.1? Tell 192.168.47.171
  2 2014-01-06 17:56:26.340955 VMware_c0:00:08 VMware_1d:b3:b1 ARP                            60 00:50:56:c0:00:08 00:0c:29:1d:b3:b1      192.168.47.1 is at 00:50:56:c0:00:08
  3 2014-01-06 17:56:26.348782 VMware_1d:b3:b1 Broadcast       ARP                            42 00:0c:29:1d:b3:b1 ff:ff:ff:ff:ff:ff      Who has 192.168.47.200? Tell 192.168.47.171
  4 2014-01-06 17:56:26.348860 VMware_0f:71:a3 VMware_1d:b3:b1 ARP                            60 00:0c:29:0f:71:a3 00:0c:29:1d:b3:b1      192.168.47.200 is at 00:0c:29:0f:71:a3
  5 2014-01-06 17:56:36.933972 VMware_1d:b3:b1 VMware_fd:2f:16 ARP                            42 00:0c:29:1d:b3:b1 00:50:56:fd:2f:16      192.168.47.200 is at 00:0c:29:1d:b3:b1
```

```
▸ Frame 5: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface unknown, id 1
▸ Ethernet II, Src: VMware_1d:b3:b1 (00:0c:29:1d:b3:b1), Dst: VMware_fd:2f:16 (00:50:56:fd:2f:16)
▾ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: VMware_1d:b3:b1 (00:0c:29:1d:b3:b1)
    Sender IP address: 192.168.47.200
    Target MAC address: VMware_fd:2f:16 (00:50:56:fd:2f:16)
    Target IP address: 192.168.47.2
▾ [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
  ▾ [Frame showing earlier use of IP address: 4]
    ▸ [Expert Info (Warning/Sequence): Duplicate IP address configured (192.168.47.200)]
    [Seconds since earlier frame seen: 10]
```

```
0000  00 50 56 fd 2f 16 00 0c  29 1d b3 b1 08 06 00 01   ·PV·/···
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                     ·PV·/··· /·
```

```
Address Resolution Protocol: Protocol          Packets: 20 · Displayed: 5 (25.0%)          Profile: Default
```

After that I took a look at the http packets by filtering http to see what I could find there. I found something very interesting there as well. All the http packets we push and acknowledgment packets. Next I did research on ack-psh flood to find out that this is a possible DDoS attack. (Mazebolt, 2022) To prevent these type of attacks you can lower your threshold for SYN, ICMP and UDP floods. You can also drop spoofed packets as early as possible. (DataDome, 2022)


secretlogs.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Interface
Channel
802.11 Preferences

```
http
```

```
No.  Time                     Source          Destination     Protocol  BSS Id  SSID  Length  SRC Mac            Dst Mac  WPA  Info
 12 2019-08-15 08:59:59.72504… 10.0.2.15      104.18.127.89   HTTP                       784 08:00:27:f8:42:a7               GET /LoggingAgent/LoggingAgent?url=//www.gottheblues.yolasite.com/&pagename=inde…
 13 2019-08-15 08:59:59.79993… 104.18.127.89  10.0.2.15       HTTP                       333 52:54:00:12:35:02               HTTP/1.1 200 OK  (application/x-javascript)
 14 2019-08-15 09:00:01.54108… 10.0.2.15      104.18.127.89   HTTP                       821 08:00:27:f8:42:a7               GET /LoggingAgent/LoggingAgent?url=//www.gottheblues.yolasite.com/contact-us.php…
 15 2019-08-15 09:00:01.57879… 104.18.127.89  10.0.2.15       HTTP                       333 52:54:00:12:35:02               HTTP/1.1 200 OK  (application/x-javascript)
 16 2019-08-15 09:01:46.12145… 10.0.2.15      104.18.126.89   HTTP                      1876 08:00:27:f8:42:a7               POST /formservice/en/3f64542cb2e3439c9bd01649ce5595ad/6150f4b54616438dbb01eb8772…
 17 2019-08-15 09:01:46.81271… 104.18.126.89  10.0.2.15       HTTP                       420 52:54:00:12:35:02               HTTP/1.1 303 See Other
 18 2019-08-15 09:01:46.85202… 10.0.2.15      104.16.161.215  HTTP                       684 08:00:27:f8:42:a7               GET /contact-us.php?formI660593e583e747f1a91a77ad0d3195e3Posted=true HTTP/1.1
 19 2019-08-15 09:01:46.96481… 104.16.161.215 10.0.2.15       HTTP                      3655 52:54:00:12:35:02               Continuation
 20 2019-08-15 09:01:47.00747… 10.0.2.15      104.16.161.215  HTTP                       598 08:00:27:f8:42:a7               GET /.well-known/http-opportunistic HTTP/1.1
```

```
▸ Frame 12: 784 bytes on wire (6272 bits), 784 bytes captured (6272 bits) on interface any, id 0
▸ Linux cooked capture v1
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 104.18.127.89
▾ Transmission Control Protocol, Src Port: 58610, Dst Port: 80, Seq: 1, Ack: 1, Len: 728
    Source Port: 58610
    Destination Port: 80
    [Stream index: 6]
    [TCP Segment Len: 728]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 2677268510
    [Next Sequence Number: 729    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 7040695
    0101 .... = Header Length: 20 bytes (5)
  ▾ Flags: 0x018 (PSH, ACK)
       000. .... .... = Reserved: Not set
       ...0 .... .... = Nonce: Not set
       .... 0... .... = Congestion Window Reduced (CWR): Not set
       .... .0.. .... = ECN-Echo: Not set
       .... ..0. .... = Urgent: Not set
```

```
0000  00 04 00 01 00 06 08 00  27 f8 42 a7 00 00 08 00   ········
0010  45 00 03 00 cc e5 40 00  40 06 77 98 0a 00 02 0f   E·····@·
0020  68 12 7f 59 e4 f2 00 50  9f 93 e0 1e 00 6b 6e b7   h··Y···P
0030  50 18 79 70 f6 6c 00 00  47 45 54 20 2f 4c 6f 67   P·yp·l·· GET /
0040  67 69 6e 67 41 67 65 6e  74 2f 4c 6f 67 67 69 6e   gingAgen t/
0050  67 41 67 65 6e 74 3f 75  72 6c 3d 2f 2f 77 77 77   gAgent?u rl=//
0060  2e 67 6f 74 74 68 65 62  6c 75 65 73 2e 79 6f 6c   .gottheb
0070  61 73 69 74 65 2e 63 6f  6d 2f 26 70 61 67 65 6e   asite.co m/
0080  61 6d 65 3d 69 6e 64 65  78 26 73 69 74 65 69 64   ame=inde
0090  3d 36 31 35 30 66 34 62  35 34 36 31 36 34 33 38   =6150f4b
00a0  64 62 62 30 31 65 62 38  37 37 32 39 36 64 35 33   dbb01eb8
00b0  34 26 72 65 73 6f 6c 75  74 69 6f 6e 3d 31 33 36   4&resolu
00c0  30 78 36 36 33 26 63 6f  6c 6f 72 44 65 70 74 68   0x663&co
00d0  3d 32 34 26 66 6c 61 73  68 3d 30 26 6a 61 76 61   =24&flas
00e0  3d 30 26 73 69 74 65 72  65 66 65 72 65 72 3d 68   =0&siter
00f0  74 74 70 25 33 41 2f 2f  77 77 77 2e 67 6f 74 74   ttp%3A//
0100  68 65 62 6c 75 65 73 2e  79 6f 6c 61 73 69 74 65   heblues.
0110  2e 63 6f 6d 2f 26 76 69  73 69 74 6f 72 49 64 3d   .com/&vi
0120  43 38 38 46 42 33 46 45  2d 38 36 39 30 2d 30 30   C88FB3FE
0130  30 31 2d 32 43 33 35 2d  38 46 30 34 31 42 34 36   01-2C35-
0140  31 41 30 31 26 76 69 73  69 74 49 64 3d 43 38 38   1A01&vis
```

```
Hypertext Transfer Protocol: Protocol          Packets: 20 · Displayed: 9 (45.0%)          Profile: Default
```

The OSI Model would be Layer 7 Application.

## References

DataDome. (2022, Feb 13). *DataDome*. Retrieved from DataDome: https://datadome.co/resources/how-to-stop-ddos-attacks/#prevent

Mazebolt. (2022, Feb 13). *Mazebolt*. Retrieved from Mazebolt: https://kb.mazebolt.com/knowledgebase/ack-psh-flood/

System, S. S. (2022, Feb 13). *Solid State System*. Retrieved from Solid State System: http://solidsystemsllc.com/prevent-man-in-the-middle-attacks/

Wikipedia. (2022, January 31). *Wikipedia*. Retrieved from https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers