Task 1:

From looking at the PCAP files, the Honeypot has the private IP address of 172.31.20.47 and there is a router on the same subnet with the private IP address of 172.31.16.1. To aid analysis, the pcap files are merged together by Month. This can be done by first isolating all the separate pcap files for a certain month, then run *mergecap *.pcap -w merged.pcap* to create the merged file called *merged.pcap*.

SubTask 1. This subtask is to show statistics for the month of October 2017 in the Country of Singapore, the merged pcap file is called *sgmerged.pcap*. A quick analysis of the merged pcap files showed that most of the packets were interacting with the Honeypot's SSH service. Hence a decision was made to focus and extract details of the protocols and services interacted with. Using python libraries Scapy to read the individual packet details, these details were used as statistics for matplotlib to create both the graph and table which helps to visualise the data in the pcap files. Based on the graph below (Fig 1), we can see that during the month of October most of the network traffic captured by the Honeypot is SSH traffic sent. The amount of traffic sent through SSH is 3 times more than the next service, HTTP. An explanation for this could be that a critical SSH vulnerability was released in 2017. CVE-2017-6542 was a critical vulnerability in the ssh and telnet client PuTTY. Further analysis of the Top 10 IP addresses which sent the most number of Packets can also be found in a table Appendix A, with details such as Protocol, Service, Packet Count and Country of Origin.

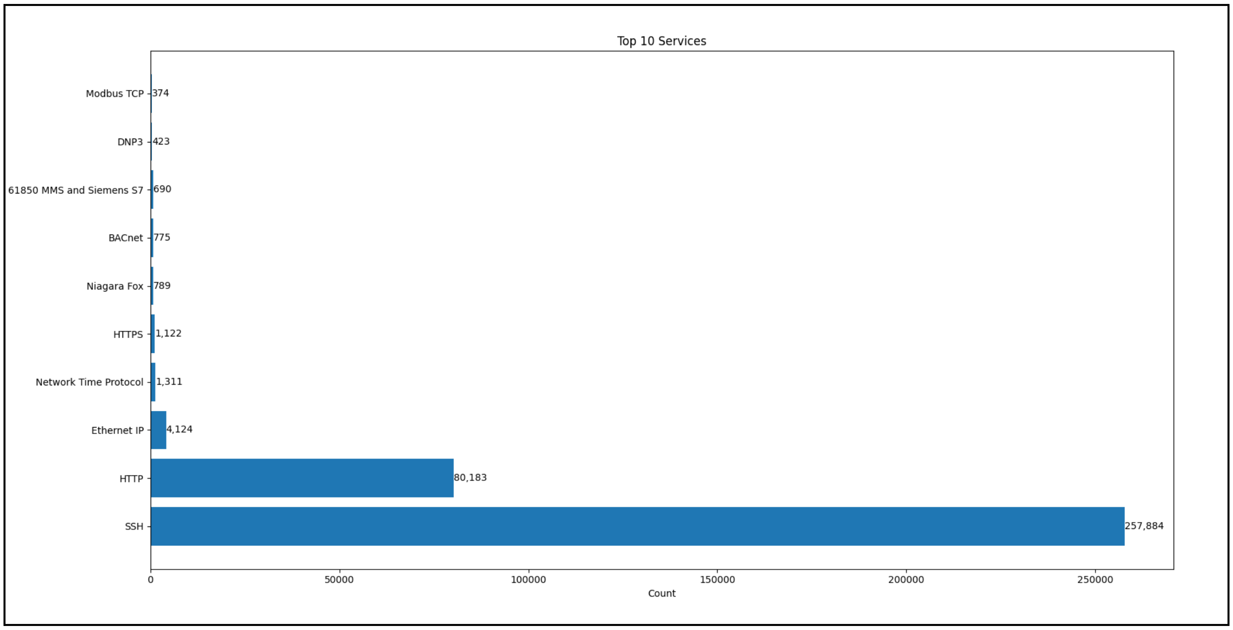


Fig 1. Top 10 services captured by Honeypot on 2017 October

SubTask 2. For this subtask, a comparison between Brazil and Singapore for the month of October 2017 will be made. Daily packet count and daily packet size histograms which shows both countries together have been made. A note that the IP addresses of the Honeypot and Router in Brazil are *172.31.42.31* and *172.31.32.1* respectively. From Fig 2 and Fig 3, we can see that on most days, the honeypot in Brazil and Singapore receive similar amounts of packets. However, the highest amount of packets received by Brazil was about 16,000 packets more than the highest amount of packets received by Singapore for the month of October. Looking at the 11th of October, Brazil's honeypot has the most amount of packets received at 76235 packets, compared to Singapore's honeypot at 25162 packets. Although this is 3 times more, comparing the total packet size on that day, it is only less than 1.5 times more. This could indicate that on that day, although Singapore's honeypot might receive less packets, the data per packet was much more than Brazil.

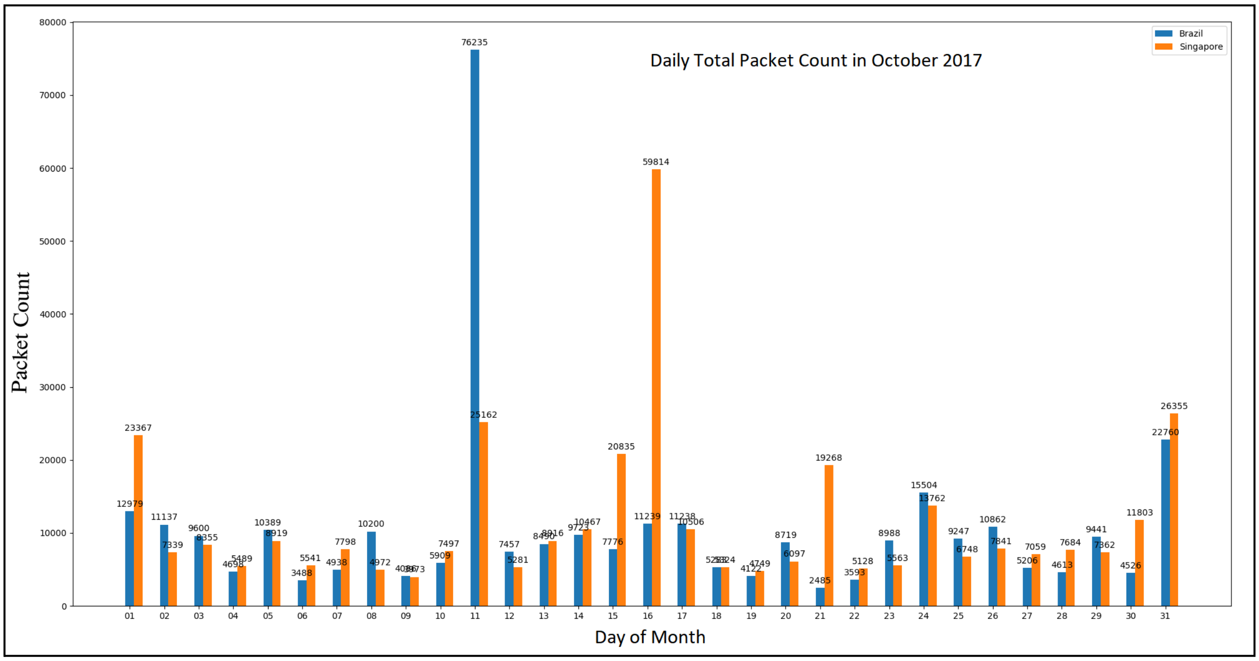


Fig 2. Comparing daily packet count for October 2017 between Brazil and Singapore

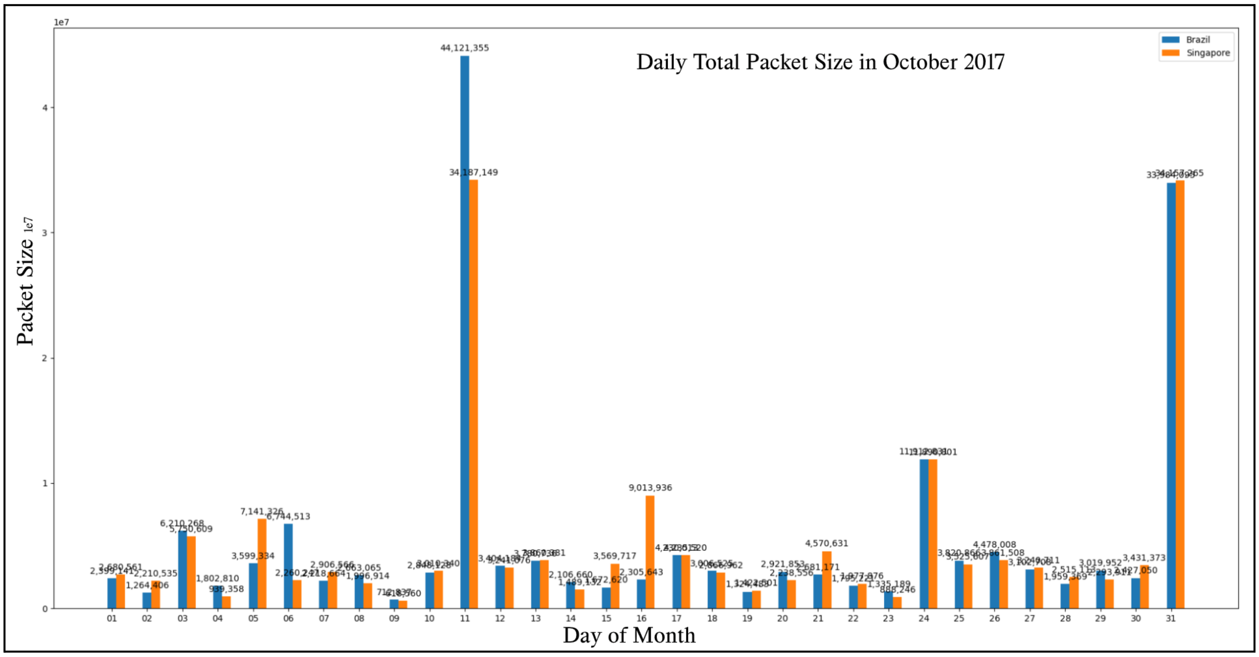
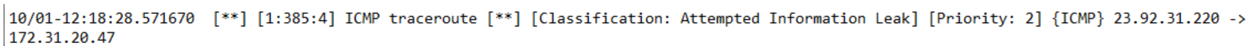


Fig 3. Comparing daily packet size received for October 2017 between Brazil and Singapore

Another important note is that a total of 1090 IP addresses appeared for both Honeypots. This is a significant amount as it shows that many of the sources which interact or probe the geographically different honeypots are the same. This gives confidence that any cybersecurity tools configuration can be generalised globally.

SubTask 3. For this subtask, the Singapore dataset for the month of October will be of focus. Using an open-source IDS called Snort to check the file sgmerged.pcap. Going through the report given by Snort, there are a few concerning alerts. These alerts are given a priority of 2 (Fig 4), and have a classification of the supposed attack that is happening.



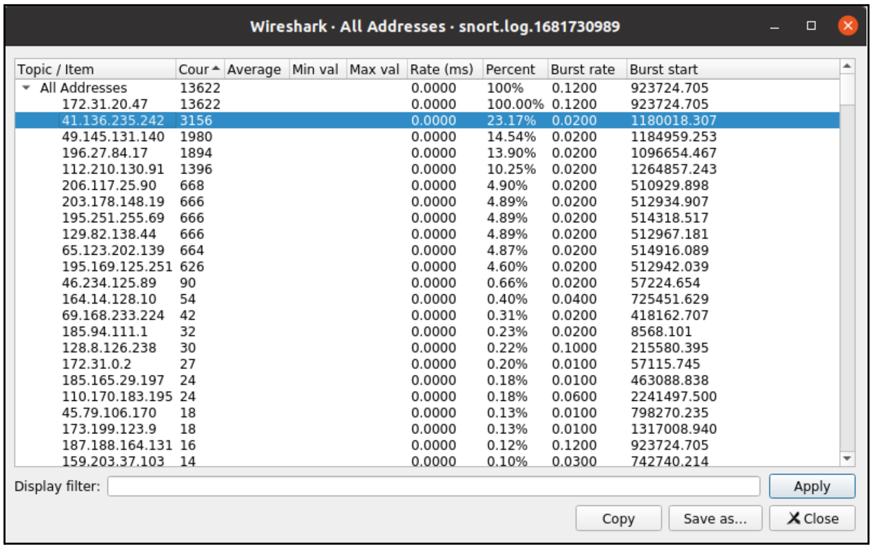
```
10/01-12:18:28.571670  [**] [1:385:4] ICMP traceroute [**] [Classification: Attempted Information Leak] [Priority: 2] {ICMP} 23.92.31.220 ->
172.31.20.47
```

Fig 4. Example of a Priority 2 alert by Snort report

Going through the report, a total of 4 activities can be found

Classification	**Activity**	**Explanation**
Attempted Information Leak	ICMP traceroute	Traceroute can be used to determine the network topology using TTL values. TTL values less than the required amount will receive a ICMP Time Exceeded Message from the source to provide a trace of the path the packet took to reach the destination. TTL value is incremented by one until the destination address specified in the traceroute command is reached.
Attempted Information Leak	ICMP PING NMAP	Popular network scanner NMAP can use ICMP or TCP pings, depending on the attacker's privileges, to perform host discovery reconnaissance. The ICMP pings received here are usually indicated by ICMP ping packets with 0 data, as seen in the pcap file
Potentially Bad Traffic	DNS SPOOF query response with TTL of 1 min. and no authority	A DNS spoof query has been detected. DNS spoofing aims to alter DNS records which will then redirect traffic to a fraudulent website that resembles its intended destination.
Potentially Bad Traffic	ICMP redirect host	Through ICMP redirects, a host can find out which networks can be accessed from within the local network, and which are the routers to be used for each such network. The attacker can then basically alter your host's routing tables and divert traffic towards external hosts on a path of his/her choice.

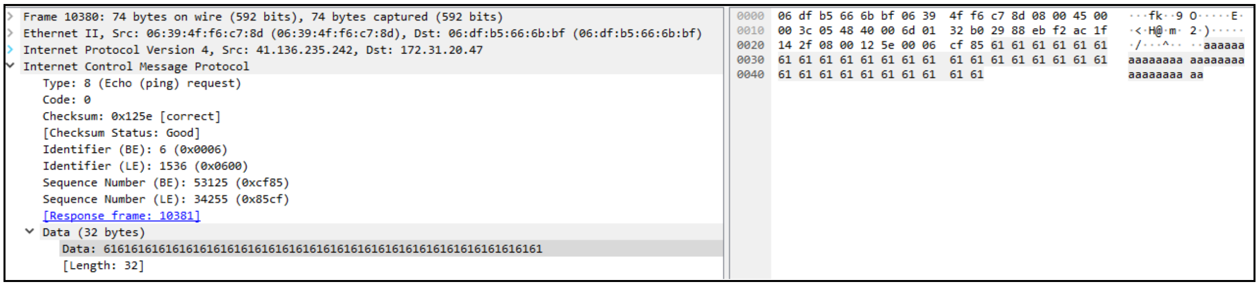
With a more thorough analysis of the Snort logs in Wireshark, the packets that trigger the alerts are properly verified. In Wireshark, the packets are mostly ICMP packets, with occasional DNS packets and this information further strengthens the validity of results given by SNORT. Moreover, as seen in Fig 5, Wireshark statistics show that the address *41.136.235.242* from the country Mauritius has sent the most amount of packets. The packets sent from this IP address are ICMP ping requests with 32 bytes of data corresponding to the ascii character 'a' (Fig 6).



Wireshark · All Addresses · snort.log.1681730989

Topic / Item	Cour	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
All Addresses	13622				0.0000	100%	0.1200	923724.705
172.31.20.47	13622				0.0000	100.00%	0.1200	923724.705
41.136.235.242	3156				0.0000	23.17%	0.0200	1180018.307
49.145.131.140	1980				0.0000	14.54%	0.0200	1184959.253
196.27.84.17	1894				0.0000	13.90%	0.0200	1096654.467
112.210.130.91	1396				0.0000	10.25%	0.0200	1264857.243
206.117.25.90	668				0.0000	4.90%	0.0200	510929.898
203.178.148.19	666				0.0000	4.89%	0.0200	512934.907
195.251.255.69	666				0.0000	4.89%	0.0200	514318.517
129.82.138.44	666				0.0000	4.89%	0.0200	512967.181
65.123.202.139	664				0.0000	4.87%	0.0200	514916.089
195.169.125.251	626				0.0000	4.60%	0.0200	512942.039
46.234.125.89	90				0.0000	0.66%	0.0200	57224.654
164.14.128.10	54				0.0000	0.40%	0.0400	725451.629
69.168.233.224	42				0.0000	0.31%	0.0200	418162.707
185.94.111.1	32				0.0000	0.23%	0.0200	8568.101
128.8.126.238	30				0.0000	0.22%	0.1000	215580.395
172.31.0.2	27				0.0000	0.20%	0.0100	57115.745
185.165.29.197	24				0.0000	0.18%	0.0100	463088.838
110.170.183.195	24				0.0000	0.18%	0.0600	2241497.500
45.79.106.170	18				0.0000	0.13%	0.0100	798270.235
173.199.123.9	18				0.0000	0.13%	0.0100	1317008.940
187.188.164.131	16				0.0000	0.12%	0.1200	923724.705
159.203.37.103	14				0.0000	0.10%	0.0300	742740.214

Fig 5. IP addresses and packet count from snort alert log



```
> Frame 10380: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
> Ethernet II, Src: 06:39:4f:f6:c7:8d (06:39:4f:f6:c7:8d), Dst: 06:df:b5:66:6b:bf (06:df:b5:66:6b:bf)
> Internet Protocol Version 4, Src: 41.136.235.242, Dst: 172.31.20.47
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x125e [correct]
    [Checksum Status: Good]
    Identifier (BE): 6 (0x0006)
    Identifier (LE): 1536 (0x0600)
    Sequence Number (BE): 53125 (0xcf85)
    Sequence Number (LE): 34255 (0x85cf)
    [Response frame: 10381]
  v Data (32 bytes)
      Data: 6161616161616161616161616161616161616161616161616161616161616161
      [Length: 32]
```

```
0000  06 df b5 66 6b bf 06 39  4f f6 c7 8d 08 00 45 00   ···fk··9 O·····E·
0010  00 3c 05 48 40 00 6d 01  32 b0 29 88 eb f2 ac 1f   ·<·H@·m· 2·)·····
0020  14 2f 08 00 12 5e 00 06  cf 85 61 61 61 61 61 61   ·/···^·· ··aaaaaa
0030  61 61 61 61 61 61 61 61  61 61 61 61 61 61 61 61   aaaaaaaa aaaaaaaa
0040  61 61 61 61 61 61 61 61  61 61                     aaaaaaaa aa
```

Fig 6. Example ICMP ping packet sent from *41.136.235.242*

SubTask 4. The findings above can be very crucial in configuring and tuning cybersecurity tools since the above findings shed a light on the real life attack trends. The collected IP addresses, especially those IP addresses alerted by Snort, are extremely useful in helping configure firewall rules. These attacker IP addresses could be considered to be added to a black-list filter, to permanently filter out these IP addresses. Moreover, from subtask 1, we can see the amount of traffic directed at certain services. This could act as a signal to focus on properly configuring these services better. For example, in Singapore, a strong consideration is to configure the SSH servers to include a white-list from only approved sources. Moreover, an attempt at security through obscurity could be to configure the SSH server to avoid port 22 for the SSH service. From subtask 3, knowing how network reconnaissance is done, we can also aim to configure the firewall to not reply to traceroute or NMAP attempts to fingerprint the network. Overall, these findings are useful information for cybersecurity experts to know the current cyber threat landscape and how to configure their tools like firewalls or IDS to properly defend against these threats.

Task 2:

SubTask 1. Using a python script, the ip addresses which are not internal ip addresses are extracted. Then the python module `python-whois` was run for each of the external ip addresses, along with a virus total check.

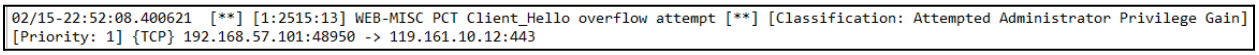
IP Address	Domain Name	State and Country	Virus Total
104.16.0.0/12 104.22.36.221 104.22.37.221 104.26.2.27 104.26.3.27 104.26.9.198	Cloudflare, Inc	CA US	Clean
104.69.0.0/18 104.69.38.163 104.69.42.238 104.69.44.74	Akamai Technologies, Inc.	MA US	Clean
106.10.128.0/17 106.10.218.137 106.10.236.141 106.10.236.37 106.10.236.40 106.10.248.157	YAHOO.COM	VA US	BitDefender - Phishing G-Data - Phishing Xcitium Verdict Cloud - Malware
119.161.10.0/23 119.161.10.11 119.161.10.12	KR3 Service Co,.Ltd.	KR	Clean
13.96.0.0/13, 13.104.0.0/14, 13.64.0.0/11 13.107.4.50	Microsoft Corporation	WA US	Antiy-AVL - Malicious BitDefender - Malware CRDF - Malicious CyRadar - Malicious G-Data - Malware VIPRE - Malicious Webroot - Malicious Xcitium Verdict Cloud - Malware Criminal IP - Suspicious
142.250.0.0/15 172.217.0.0/16 172.253.0.0/16 34.128.0.0/10 216.239.32.0/20 74.125.0.0/16 142.250.181.35 142.250.4.100 142.250.4.101 142.250.4.102 142.250.4.104 142.250.4.109 142.250.4.113 142.250.4.138 142.250.4.139 142.250.4.94 142.250.4.99 142.251.10.100 142.251.10.101 142.251.10.102 142.251.10.108 142.251.10.113 142.251.10.138 142.251.10.139 142.251.10.19	Google LLC fonts.gstatic.com id.google.com play.google.com pop.gmail.com smtp.gmail.com ssl.gstatic.com www.google.com www.googleapis.com www3.l.google.com	CA US	Clean

142.251.10.94 142.251.12.100 142.251.12.101 142.251.12.102 142.251.12.103 142.251.12.104 142.251.12.105 142.251.12.106 142.251.12.113 142.251.12.139 142.251.12.147 142.251.12.84 142.251.12.94 142.251.12.99 172.217.194.100 172.217.194.102 172.217.194.103 172.217.194.105 172.217.194.138 172.217.194.17 172.217.194.83 172.217.194.94 172.253.118.101 172.253.118.103 172.253.118.106 172.253.118.84 172.253.118.94 34.160.122.198 216.239.32.29 216.239.32.55 74.125.130.102 74.125.130.94 74.125.200.100 74.125.200.101 74.125.200.139 74.125.200.94 74.125.24.100 74.125.24.101 74.125.24.102 74.125.24.113 74.125.24.138 74.125.24.139 74.125.24.94 74.125.68.103 74.125.68.105 74.125.68.106 74.125.68.139 74.125.68.147 74.125.68.95 74.125.68.99			
172.64.0.0/13 172.67.69.99 172.67.7.19	Cloudflare, Inc	CA US	Clean
185.125.188.0/22 185.125.188.55 185.125.188.58 185.125.188.59 185.125.190.28	Canonical Group Limited	GB	Clean
185.199.108.0/22 185.199.109.133	GitHub, Inc	CA US	Xcitium Verdict Cloud - Malware
20.33.0.0/16 20.128.0.0/16 20.40.0.0/13 20.34.0.0/15 20.64.0.0/10 20.36.0.0/14 20.48.0.0/12 20.192.0.0/10 4.240.0.0/12 40.80.0.0/12 40.112.0.0/13	Microsoft Corporation	WA US	Clean

40.124.0.0/16 40.120.0.0/14 40.125.0.0/17 40.76.0.0/14 40.74.0.0/15 40.96.0.0/12 52.96.0.0/12 52.112.0.0/14 20.103.253.93 20.50.73.9 20.205.243.166 4.246.174.31 40.79.150.120 52.109.52.148			
202.165.104.0/22 202.165.107.50 202.165.107.57	Yahoo SG3 Data Center	SG	Clean
204.79.197.0/24 204.79.197.203 204.79.197.219	ECN-NETWORK Microsoft Corporation	WA US	Xcitium Verdict Cloud - Malware
212.166.96.0/19 212.166.100.13	T-Systems Austria GesmbH	AT	Clean
23.0.0.0/12, 23.64.0.0/14, 23.32.0.0/11, 23.72.0.0/13 23.15.147.56 23.64.122.82 23.72.44.106	Akamai Technologies, Inc.	MA US	Clean
54.208.0.0/13 54.220.0.0/15 54.144.0.0/12 54.192.0.0/12 54.160.0.0/11 54.216.0.0/14 54.217.10.153	Amazon Technologies Inc.	WA US	Clean
69.147.64.0/18 74.6.0.0/16 69.147.80.15 74.6.143.25 74.6.143.26	Oath Holdings Inc	NY US	CMC Threat Intelligence - Malware Xcitium Verdict Cloud - Malware
74.208.0.0/16 74.208.236.166	IONOS Inc	PA US	Clean
8.8.8.0/24 8.8.8.8	dns.google	CA US	CRDF - Malicious Xcitium Verdict Cloud - Malware CrowdSec - Suspicious

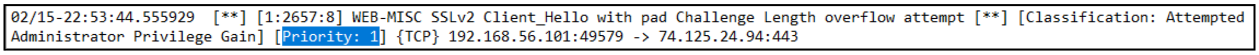
SubTask 2. I believe that the machine with the internal IP address *192.168.57.101* is compromised by malware. The other local machines have normal network traffic such as normal google searches which are not found in *192.168.57.101.*

Moreover, the analysis which Snort provides shows multiple Priority 1 attack attempts all conducted by the IP address 192.168.56.101, as shown in the figures below (Fig 7,8,9).



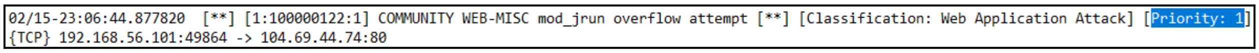
```
02/15-22:52:08.400621  [**] [1:2515:13] WEB-MISC PCT Client_Hello overflow attempt [**] [Classification: Attempted Administrator Privilege Gain]
[Priority: 1] {TCP} 192.168.57.101:48950 -> 119.161.10.12:443
```

Fig 7. Buffer overflow in PCT allows remote attackers to execute arbitrary code via PCT 1.0 handshake packets



```
02/15-22:53:44.555929  [**] [1:2657:8] WEB-MISC SSLv2 Client_Hello with pad Challenge Length overflow attempt [**] [Classification: Attempted
Administrator Privilege Gain] [Priority: 1] {TCP} 192.168.56.101:49579 -> 74.125.24.94:443
```

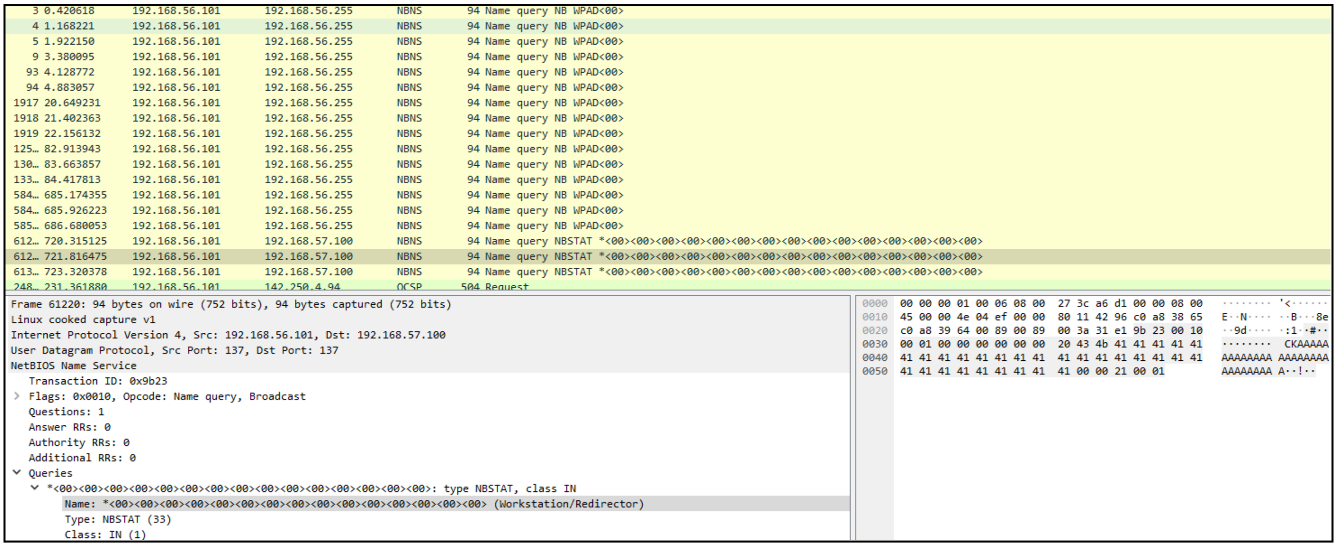
Fig 8. Heap-based buffer overflow in NSS library to execute arbitrary code via modified record length field in an SSLv2 client hello message



```
02/15-23:06:44.877820  [**] [1:100000122:1] COMMUNITY WEB-MISC mod_jrun overflow attempt [**] [Classification: Web Application Attack] [Priority: 1]
{TCP} 192.168.56.101:49864 -> 104.69.44.74:80
```

Fig 9. Buffer overflow in the JRun 3.0 allows remote attackers to execute arbitrary code via a long HTTP header Content-Type field

Moreover, a huge indicator can be seen from Fig 10 where multiple NBNS queries perform NetBios browse master calls. This could be suspicious why the host machine wants to query for all using ‘*’.



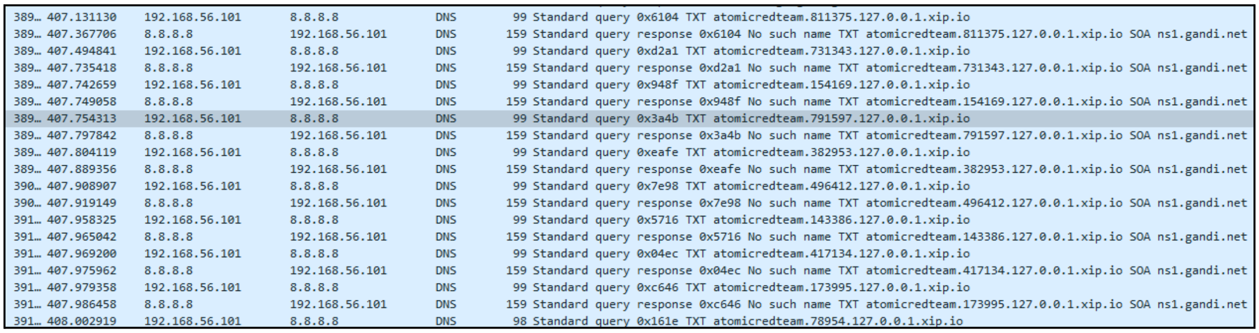
```
     3 0.420618     192.168.56.101     192.168.56.255     NBNS      94 Name query NB WPAD<00>
     4 1.168221     192.168.56.101     192.168.56.255     NBNS      94 Name query NB WPAD<00>
     5 1.922150     192.168.56.101     192.168.56.255     NBNS      94 Name query NB WPAD<00>
     9 3.380095     192.168.56.101     192.168.56.255     NBNS      94 Name query NB WPAD<00>
    93 4.128772     192.168.56.101     192.168.56.255     NBNS      94 Name query NB WPAD<00>
    94 4.883057     192.168.56.101     192.168.56.255     NBNS      94 Name query NB WPAD<00>
  1917 20.649231    192.168.56.101     192.168.56.255     NBNS      94 Name query NB WPAD<00>
  1918 21.402363    192.168.56.101     192.168.56.255     NBNS      94 Name query NB WPAD<00>
  1919 22.156132    192.168.56.101     192.168.56.255     NBNS      94 Name query NB WPAD<00>
  125… 82.913943    192.168.56.101     192.168.56.255     NBNS      94 Name query NB WPAD<00>
  130… 83.663857    192.168.56.101     192.168.56.255     NBNS      94 Name query NB WPAD<00>
  133… 84.417813    192.168.56.101     192.168.56.255     NBNS      94 Name query NB WPAD<00>
  584… 685.174355   192.168.56.101     192.168.56.255     NBNS      94 Name query NB WPAD<00>
  584… 685.926223   192.168.56.101     192.168.56.255     NBNS      94 Name query NB WPAD<00>
  585… 686.680053   192.168.56.101     192.168.56.255     NBNS      94 Name query NB WPAD<00>
  612… 720.315125   192.168.56.101     192.168.57.100     NBNS      94 Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><00><00><00><00>
  612… 721.816475   192.168.56.101     192.168.57.100     NBNS      94 Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><00><00><00><00>
  613… 723.320378   192.168.56.101     192.168.57.100     NBNS      94 Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><00><00><00><00>
  248… 231.361880   192.168.56.101     142.250.4.94       OCSP     504 Request
```

```
Frame 61220: 94 bytes on wire (752 bits), 94 bytes captured (752 bits)
Linux cooked capture v1
Internet Protocol Version 4, Src: 192.168.56.101, Dst: 192.168.57.100
User Datagram Protocol, Src Port: 137, Dst Port: 137
NetBIOS Name Service
   Transaction ID: 0x9b23
 > Flags: 0x0010, Opcode: Name query, Broadcast
   Questions: 1
   Answer RRs: 0
   Authority RRs: 0
   Additional RRs: 0
 v Queries
   v *<00><00><00><00><00><00><00><00><00><00><00><00><00><00><00>: type NBSTAT, class IN
        Name: *<00><00><00><00><00><00><00><00><00><00><00><00><00><00><00> (Workstation/Redirector)
        Type: NBSTAT (33)
        Class: IN (1)
```

```
0000  00 00 00 01 00 06 08 00  27 3c a6 d1 00 00 08 00   ········ '<······
0010  45 00 00 4e 04 ef 00 00  80 11 42 96 c0 a8 38 65   E··N···· ··B···8e
0020  c0 a8 39 64 00 89 00 89  00 3a 31 e1 9b 23 00 10   ··9d···· ·:1··#··
0030  00 01 00 00 00 00 00 00  20 43 4b 41 41 41 41 41   ········  CKAAAAA
0040  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41   AAAAAAAA AAAAAAAA
0050  41 41 41 41 41 41 41 41  41 00 00 21 00 01         AAAAAAAA A··!··
```

Fig 10. NetBios query for all (‘*’)

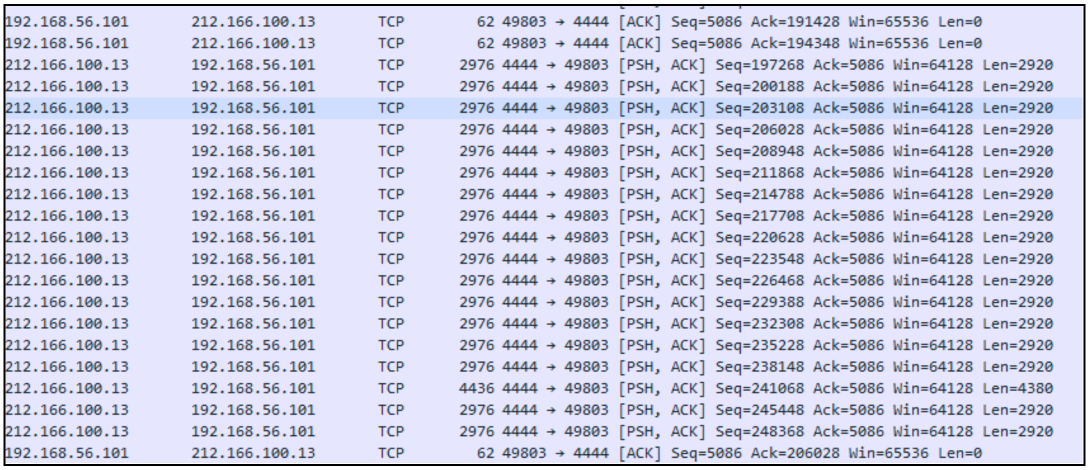
The infected IP address also has numerous DNS queries to which all do not return a response as well (Fig 11).



```
389… 407.131130   192.168.56.101     8.8.8.8            DNS      99 Standard query 0x6104 TXT atomicredteam.811375.127.0.0.1.xip.io
389… 407.367706   8.8.8.8            192.168.56.101     DNS     159 Standard query response 0x6104 No such name TXT atomicredteam.811375.127.0.0.1.xip.io SOA ns1.gandi.net
389… 407.494841   192.168.56.101     8.8.8.8            DNS      99 Standard query 0xd2a1 TXT atomicredteam.731343.127.0.0.1.xip.io
389… 407.735418   8.8.8.8            192.168.56.101     DNS     159 Standard query response 0xd2a1 No such name TXT atomicredteam.731343.127.0.0.1.xip.io SOA ns1.gandi.net
389… 407.742659   192.168.56.101     8.8.8.8            DNS      99 Standard query 0x948f TXT atomicredteam.154169.127.0.0.1.xip.io
389… 407.749058   8.8.8.8            192.168.56.101     DNS     159 Standard query response 0x948f No such name TXT atomicredteam.154169.127.0.0.1.xip.io SOA ns1.gandi.net
389… 407.754313   192.168.56.101     8.8.8.8            DNS      99 Standard query 0x3a4b TXT atomicredteam.791597.127.0.0.1.xip.io
389… 407.797842   8.8.8.8            192.168.56.101     DNS     159 Standard query response 0x3a4b No such name TXT atomicredteam.791597.127.0.0.1.xip.io SOA ns1.gandi.net
389… 407.804119   192.168.56.101     8.8.8.8            DNS      99 Standard query 0xeafe TXT atomicredteam.382953.127.0.0.1.xip.io
389… 407.889356   8.8.8.8            192.168.56.101     DNS     159 Standard query response 0xeafe No such name TXT atomicredteam.382953.127.0.0.1.xip.io SOA ns1.gandi.net
390… 407.908907   192.168.56.101     8.8.8.8            DNS      99 Standard query 0x7e98 TXT atomicredteam.496412.127.0.0.1.xip.io
390… 407.919149   8.8.8.8            192.168.56.101     DNS     159 Standard query response 0x7e98 No such name TXT atomicredteam.496412.127.0.0.1.xip.io SOA ns1.gandi.net
391… 407.958325   192.168.56.101     8.8.8.8            DNS      99 Standard query 0x5716 TXT atomicredteam.143386.127.0.0.1.xip.io
391… 407.965042   8.8.8.8            192.168.56.101     DNS     159 Standard query response 0x5716 No such name TXT atomicredteam.143386.127.0.0.1.xip.io SOA ns1.gandi.net
391… 407.969200   192.168.56.101     8.8.8.8            DNS      99 Standard query 0x04ec TXT atomicredteam.417134.127.0.0.1.xip.io
391… 407.975962   8.8.8.8            192.168.56.101     DNS     159 Standard query response 0x04ec No such name TXT atomicredteam.417134.127.0.0.1.xip.io SOA ns1.gandi.net
391… 407.979358   192.168.56.101     8.8.8.8            DNS      99 Standard query 0xc646 TXT atomicredteam.173995.127.0.0.1.xip.io
391… 407.986458   8.8.8.8            192.168.56.101     DNS     159 Standard query response 0xc646 No such name TXT atomicredteam.173995.127.0.0.1.xip.io SOA ns1.gandi.net
391… 408.002919   192.168.56.101     8.8.8.8            DNS      98 Standard query 0x161e TXT atomicredteam.78954.127.0.0.1.xip.io
```

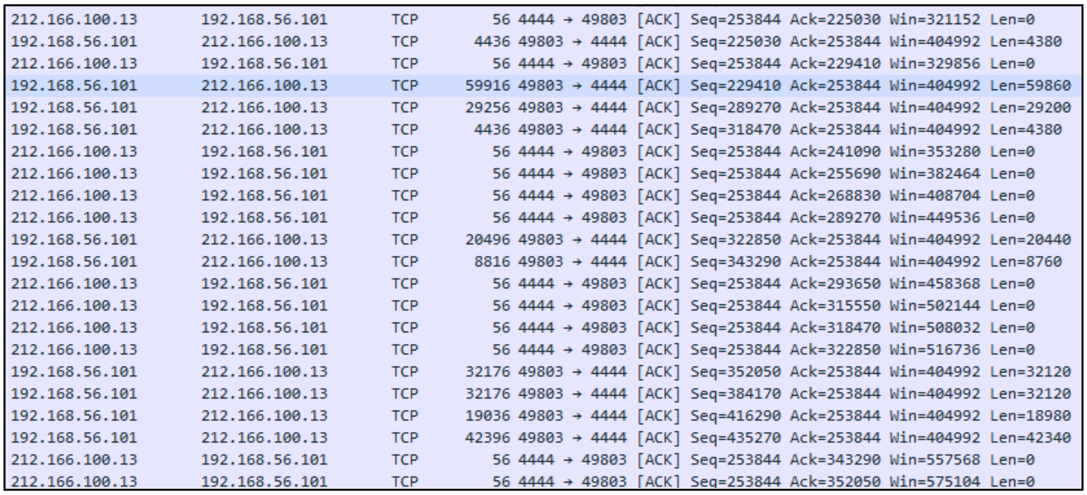
Fig 11. Suspicious DNS queries

SubTask 3. The malware seems to be scanning laterally to other machines on the local subnet through its NetBios queries to find other machines on the private/internal network as a step to fingerprint the internal network. Communication done over TCP to a suspicious IP 212.166.10.13 which the infected host first receives a lot of information while usually only sending ACK messages back (Fig 12), to then later the roles being flipped where the infected host is the one sending back large amounts of data to the same connection (Fig 13).



```
192.168.56.101      212.166.100.13      TCP        62 49803 → 4444 [ACK] Seq=5086 Ack=191428 Win=65536 Len=0
192.168.56.101      212.166.100.13      TCP        62 49803 → 4444 [ACK] Seq=5086 Ack=194348 Win=65536 Len=0
212.166.100.13      192.168.56.101      TCP      2976 4444 → 49803 [PSH, ACK] Seq=197268 Ack=5086 Win=64128 Len=2920
212.166.100.13      192.168.56.101      TCP      2976 4444 → 49803 [PSH, ACK] Seq=200188 Ack=5086 Win=64128 Len=2920
212.166.100.13      192.168.56.101      TCP      2976 4444 → 49803 [PSH, ACK] Seq=203108 Ack=5086 Win=64128 Len=2920
212.166.100.13      192.168.56.101      TCP      2976 4444 → 49803 [PSH, ACK] Seq=206028 Ack=5086 Win=64128 Len=2920
212.166.100.13      192.168.56.101      TCP      2976 4444 → 49803 [PSH, ACK] Seq=208948 Ack=5086 Win=64128 Len=2920
212.166.100.13      192.168.56.101      TCP      2976 4444 → 49803 [PSH, ACK] Seq=211868 Ack=5086 Win=64128 Len=2920
212.166.100.13      192.168.56.101      TCP      2976 4444 → 49803 [PSH, ACK] Seq=214788 Ack=5086 Win=64128 Len=2920
212.166.100.13      192.168.56.101      TCP      2976 4444 → 49803 [PSH, ACK] Seq=217708 Ack=5086 Win=64128 Len=2920
212.166.100.13      192.168.56.101      TCP      2976 4444 → 49803 [PSH, ACK] Seq=220628 Ack=5086 Win=64128 Len=2920
212.166.100.13      192.168.56.101      TCP      2976 4444 → 49803 [PSH, ACK] Seq=223548 Ack=5086 Win=64128 Len=2920
212.166.100.13      192.168.56.101      TCP      2976 4444 → 49803 [PSH, ACK] Seq=226468 Ack=5086 Win=64128 Len=2920
212.166.100.13      192.168.56.101      TCP      2976 4444 → 49803 [PSH, ACK] Seq=229388 Ack=5086 Win=64128 Len=2920
212.166.100.13      192.168.56.101      TCP      2976 4444 → 49803 [PSH, ACK] Seq=232308 Ack=5086 Win=64128 Len=2920
212.166.100.13      192.168.56.101      TCP      2976 4444 → 49803 [PSH, ACK] Seq=235228 Ack=5086 Win=64128 Len=2920
212.166.100.13      192.168.56.101      TCP      2976 4444 → 49803 [PSH, ACK] Seq=238148 Ack=5086 Win=64128 Len=2920
212.166.100.13      192.168.56.101      TCP      4436 4444 → 49803 [PSH, ACK] Seq=241068 Ack=5086 Win=64128 Len=4380
212.166.100.13      192.168.56.101      TCP      2976 4444 → 49803 [PSH, ACK] Seq=245448 Ack=5086 Win=64128 Len=2920
212.166.100.13      192.168.56.101      TCP      2976 4444 → 49803 [PSH, ACK] Seq=248368 Ack=5086 Win=64128 Len=2920
192.168.56.101      212.166.100.13      TCP        62 49803 → 4444 [ACK] Seq=5086 Ack=206028 Win=65536 Len=0
```

Fig 12. C2 sending host information



```
212.166.100.13      192.168.56.101      TCP        56 4444 → 49803 [ACK] Seq=253844 Ack=225030 Win=321152 Len=0
192.168.56.101      212.166.100.13      TCP      4436 49803 → 4444 [ACK] Seq=225030 Ack=253844 Win=404992 Len=4380
212.166.100.13      192.168.56.101      TCP        56 4444 → 49803 [ACK] Seq=253844 Ack=229410 Win=329856 Len=0
192.168.56.101      212.166.100.13      TCP     59916 49803 → 4444 [ACK] Seq=229410 Ack=253844 Win=404992 Len=59860
192.168.56.101      212.166.100.13      TCP     29256 49803 → 4444 [ACK] Seq=289270 Ack=253844 Win=404992 Len=29200
192.168.56.101      212.166.100.13      TCP      4436 49803 → 4444 [ACK] Seq=318470 Ack=253844 Win=404992 Len=4380
212.166.100.13      192.168.56.101      TCP        56 4444 → 49803 [ACK] Seq=253844 Ack=241090 Win=353280 Len=0
212.166.100.13      192.168.56.101      TCP        56 4444 → 49803 [ACK] Seq=253844 Ack=255690 Win=382464 Len=0
212.166.100.13      192.168.56.101      TCP        56 4444 → 49803 [ACK] Seq=253844 Ack=268830 Win=408704 Len=0
212.166.100.13      192.168.56.101      TCP        56 4444 → 49803 [ACK] Seq=253844 Ack=289270 Win=449536 Len=0
192.168.56.101      212.166.100.13      TCP     20496 49803 → 4444 [ACK] Seq=322850 Ack=253844 Win=404992 Len=20440
192.168.56.101      212.166.100.13      TCP      8816 49803 → 4444 [ACK] Seq=343290 Ack=253844 Win=404992 Len=8760
212.166.100.13      192.168.56.101      TCP        56 4444 → 49803 [ACK] Seq=253844 Ack=293650 Win=458368 Len=0
212.166.100.13      192.168.56.101      TCP        56 4444 → 49803 [ACK] Seq=253844 Ack=315550 Win=502144 Len=0
212.166.100.13      192.168.56.101      TCP        56 4444 → 49803 [ACK] Seq=253844 Ack=318470 Win=508032 Len=0
212.166.100.13      192.168.56.101      TCP        56 4444 → 49803 [ACK] Seq=253844 Ack=322850 Win=516736 Len=0
192.168.56.101      212.166.100.13      TCP     32176 49803 → 4444 [ACK] Seq=352050 Ack=253844 Win=404992 Len=32120
192.168.56.101      212.166.100.13      TCP     32176 49803 → 4444 [ACK] Seq=384170 Ack=253844 Win=404992 Len=32120
192.168.56.101      212.166.100.13      TCP     19036 49803 → 4444 [ACK] Seq=416290 Ack=253844 Win=404992 Len=18980
192.168.56.101      212.166.100.13      TCP     42396 49803 → 4444 [ACK] Seq=435270 Ack=253844 Win=404992 Len=42340
212.166.100.13      192.168.56.101      TCP        56 4444 → 49803 [ACK] Seq=253844 Ack=343290 Win=557568 Len=0
212.166.100.13      192.168.56.101      TCP        56 4444 → 49803 [ACK] Seq=253844 Ack=352050 Win=575104 Len=0
```

Fig 13. Infected host replying C2 with large amounts of information

This could possibly be the C2 server communicating with the infected host on the things to do and later could be when the infected host replies with the collected data. Moreover, the multiple attack attempts from Fig 7-9 could be that this infected machine is now part of a bot network to perform remote attacks on other servers, controlled by the C2.

Appendix A

Table of Top 10 IP Addresses by Packets sent

IP Address	Protocol	Service	Count	Country , City
198.98.53.156	TCP	SSH	63932	Cheyenne, Wyoming, US
54.179.137.100	TCP	HTTP	45454	Seattle, Washington, US
211.23.4.210	TCP	SSH	13064	South Brisbane, Queensland, Australia
199.195.248.31	TCP	SSH	11200	Cheyenne, Wyoming, US
54.169.117.133	TCP	HTTP	10519	Seattle, Washington, US
158.85.76.3	TCP	SSH	9773	Dallas, Texas, US
52.172.202.136	TCP	SSH	8394	Redmond, Washington, US
54.169.144.212	TCP	HTTP	8165	Seattle, Washington, US
54.179.187.123	TCP	HTTP	6914	Seattle, Washington, US
198.98.61.180	TCP	SSH	4984	Cheyenne, Wyoming, US