Scan of the Month #28

Submitted by Rick Hayes

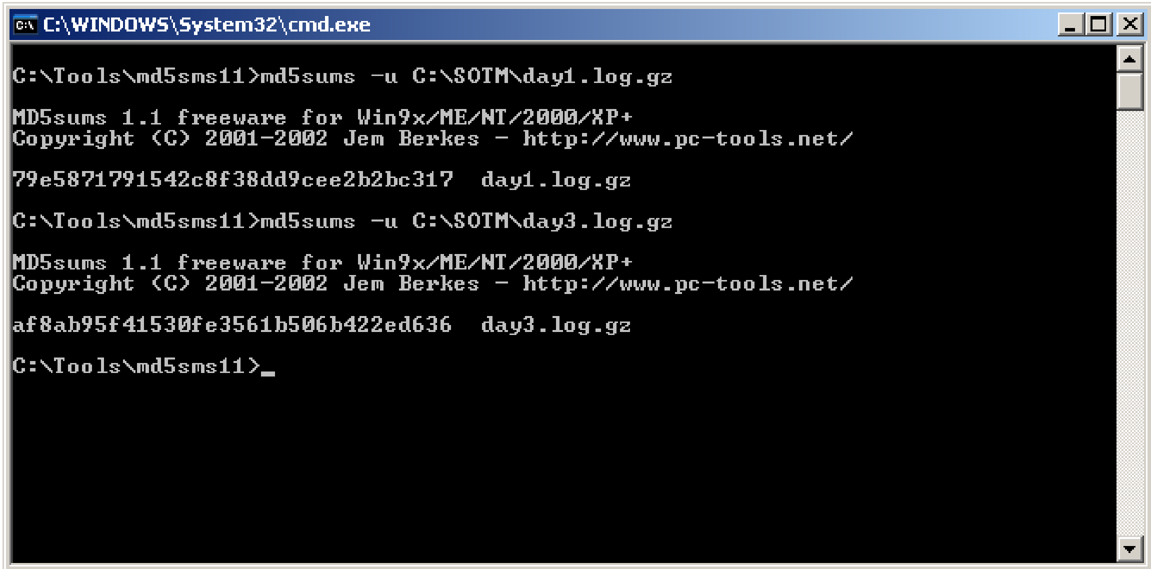
The Challenge

Members of the AT&T Mexico Honeynet captured a unique attack. As common, what is interesting is not how the attackers broke in, but what they did afterwards. Your mission is to analyze the network capture of the attacker's activity and decode the attacker's actions. There are two binary log files. Day1 captured the break in; Day3 captures some unique activity following the compromise. The honeypot in question is IP 192.168.100.28.

Analysis

Verification of the log signature

Analysis was performed entirely on a Windows XP machine. To begin the analysis, first it was necessary to download the log and verify its authenticity. I then had to extract the actual log must be from the compressed archive:



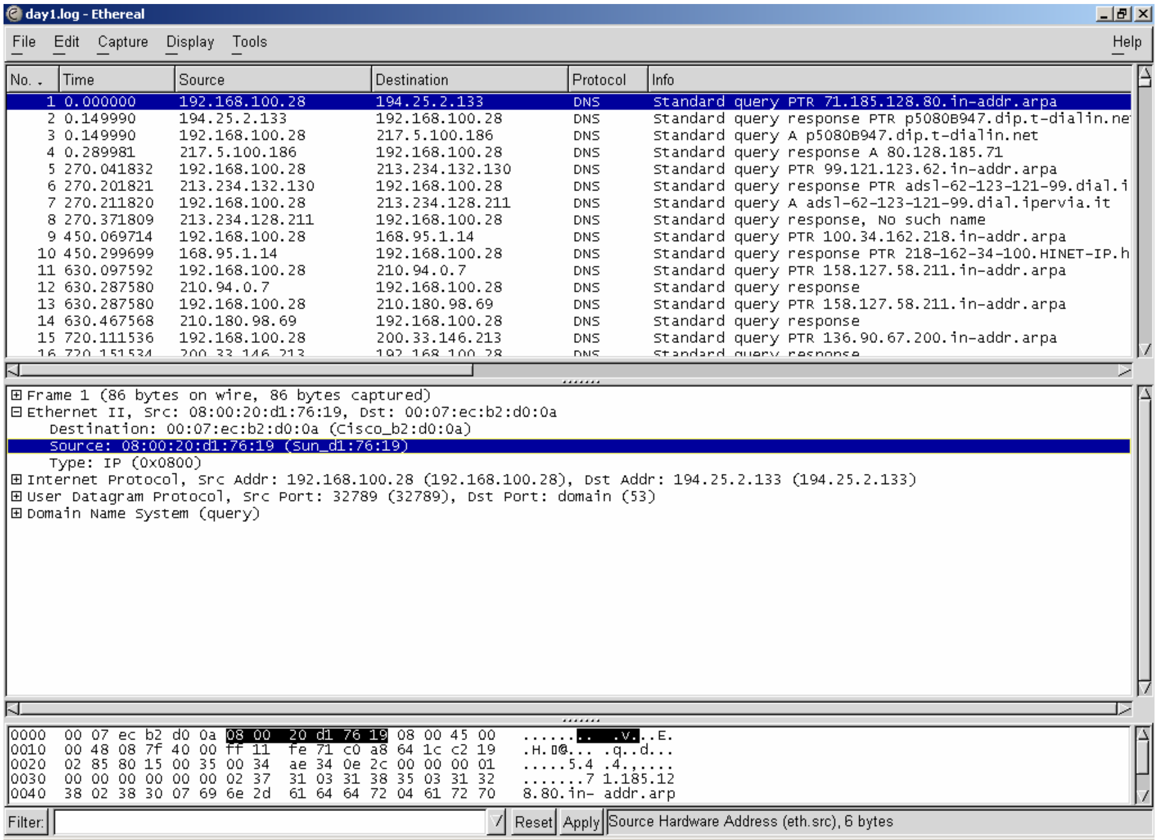
Tools Used

During the analysis of this scan, we used the following tools:

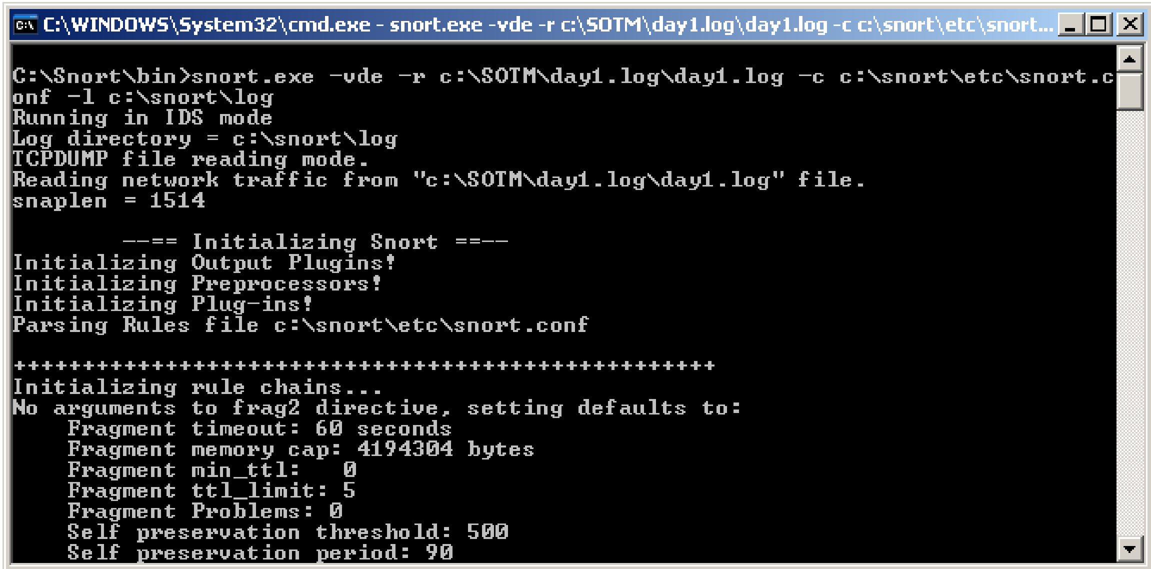
Tool	Description	Location
md5sum	Calculates a checksum of a file. Often used to verify downloads.	http://www.pc-tools.net/win32/freeware/md5sums/
windump	Used to capture packets from the network, or to read previously saved packets.	http://windump.polito.it/
ethereal	Similar to tcpdump, but has a GUI frontend, and several helpful features.	http://www.ethereal.com
snort	A network based intrusion detection system.	http://www.snort.org

Process

First, I opened the log with Ethereal to begin the process of checking for the operating system of the victim.



This yielded some information about the source and destinations. It also allowed me to be able to see the TTL, window size, etc. I used this information along with the Passive Fingerprinting Default TTL values whitepaper to conclude the operating system of the honeypot. After looking through Ethereal it became apparent that several of these attempts were simply DNS queries and responses. Several interesting frames were found that indicated more than DNS queries were being performed. Two rather interesting packets were attempts to perform NetBIOS queries. I decided to take the two logs and run them through snort.



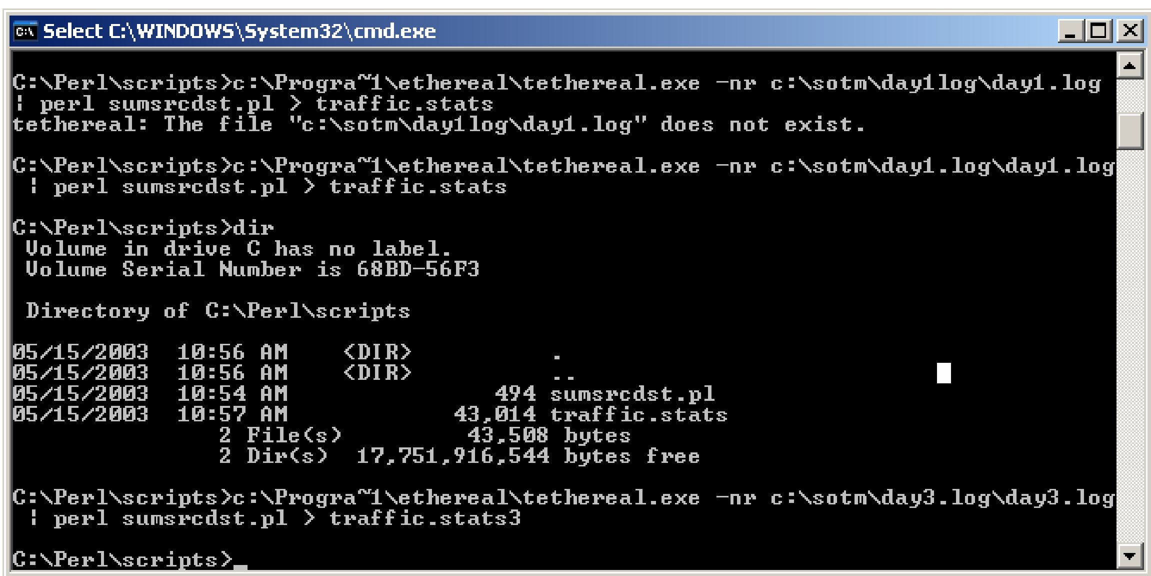
```
C:\WINDOWS\System32\cmd.exe - snort.exe -vde -r c:\SOTM\day1.log\day1.log -c c:\snort\etc\snort...

C:\Snort\bin>snort.exe -vde -r c:\SOTM\day1.log\day1.log -c c:\snort\etc\snort.c
onf -l c:\snort\log
Running in IDS mode
Log directory = c:\snort\log
TCPDUMP file reading mode.
Reading network traffic from "c:\SOTM\day1.log\day1.log" file.
snaplen = 1514

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file c:\snort\etc\snort.conf

+++++++++++++++++++++++++++++++++++++++++++++++++++
Initializing rule chains...
No arguments to frag2 directive, setting defaults to:
    Fragment timeout: 60 seconds
    Fragment memory cap: 4194304 bytes
    Fragment min_ttl:   0
    Fragment ttl_limit: 5
    Fragment Problems: 0
    Self preservation threshold: 500
    Self preservation period: 90
```

This provided some assurances that what was visible with Ethereal was certainly suspicious activity. Now I needed to see who the primary participants were. So, I then ran the logs through tethereal to determine this.



```
Select C:\WINDOWS\System32\cmd.exe

C:\Perl\scripts>c:\Progra~1\ethereal\tethereal.exe -nr c:\sotm\day1log\day1.log
| perl sumsrcdst.pl > traffic.stats
tethereal: The file "c:\sotm\day1log\day1.log" does not exist.

C:\Perl\scripts>c:\Progra~1\ethereal\tethereal.exe -nr c:\sotm\day1.log\day1.log
 | perl sumsrcdst.pl > traffic.stats

C:\Perl\scripts>dir
 Volume in drive C has no label.
 Volume Serial Number is 68BD-56F3

 Directory of C:\Perl\scripts

05/15/2003  10:56 AM    <DIR>          .
05/15/2003  10:56 AM    <DIR>          ..
05/15/2003  10:54 AM               494 sumsrcdst.pl
05/15/2003  10:57 AM            43,014 traffic.stats
               2 File(s)         43,508 bytes
               2 Dir(s)  17,751,916,544 bytes free

C:\Perl\scripts>c:\Progra~1\ethereal\tethereal.exe -nr c:\sotm\day3.log\day3.log
 | perl sumsrcdst.pl > traffic.stats3

C:\Perl\scripts>_
```

Day 1: Protocol Statistics

```
206.252.192.195 -> 192.168.100.28 TCP     2162
192.168.100.28 -> 206.252.192.195 TCP     1928
61.219.90.180 -> 192.168.100.28 TCP      1879
192.168.100.28 -> 61.219.90.180 TCP      1853
62.211.66.53 -> 192.168.100.28 HTTP      1291
192.168.100.28 -> 61.134.3.11 ICMP        846
192.168.100.28 -> 217.116.38.10 ICMP      846
192.168.100.28 -> 62.211.66.53 TCP        819
192.18.99.122 -> 192.168.100.28 FTP-DATA      784
192.168.100.28 -> 192.18.99.122 TCP       707
```

```
148.244.153.91 -> 192.168.100.28 DNS      454
192.168.100.28 -> 148.244.153.91 DNS      405
192.168.100.28 -> 80.117.14.44 Gryphon      257
80.117.14.44 -> 192.168.100.28 TCP        255
62.211.66.16 -> 192.168.100.28 FTP-DATA      174
80.117.14.44 -> 192.168.100.28 Gryphon      163
192.168.100.28 -> 80.117.14.44 TCP        146
192.168.100.28 -> 62.211.66.16 TCP        140
192.168.100.28 -> 200.33.146.213 DNS       53
200.33.146.213 -> 192.168.100.28 DNS       52
192.12.94.30 -> 192.168.100.28 DNS         52
192.168.100.28 -> 192.12.94.30 DNS         52
192.168.100.28 -> 192.31.80.30 DNS         51
192.31.80.30 -> 192.168.100.28 DNS         51
192.168.100.28 -> 140.135.18.25 DNS        44
192.168.100.28 -> 200.33.146.217 DNS       38
200.33.146.217 -> 192.168.100.28 DNS       37
192.168.100.28 -> 192.5.6.30 DNS           36
192.5.6.30 -> 192.168.100.28 DNS           36
140.135.18.25 -> 192.168.100.28 DNS        34
200.33.213.66 -> 192.168.100.28 DNS        32
192.168.100.28 -> 200.33.213.66 DNS        32
62.211.66.16 -> 192.168.100.28 TCP         30
192.35.51.30 -> 192.168.100.28 DNS         29
192.168.100.28 -> 192.35.51.30 DNS         29
63.250.206.138 -> 192.168.100.28 DNS       26
192.168.100.28 -> 63.250.206.138 DNS       26
192.168.100.196 -> 192.168.100.28 DNS       25
192.168.100.28 -> 192.168.100.196 DNS       25
192.18.99.122 -> 192.168.100.28 FTP        24
192.41.162.30 -> 192.168.100.28 DNS        21
192.100.59.110 -> 192.168.100.28 DNS       21
192.168.100.28 -> 192.26.92.30 DNS         21
192.168.100.28 -> 192.41.162.30 DNS        21
192.26.92.30 -> 192.168.100.28 DNS         21
192.168.100.28 -> 192.33.14.30 DNS         21
192.168.100.28 -> 192.100.59.110 DNS       21
192.33.14.30 -> 192.168.100.28 DNS         21
192.42.93.30 -> 192.168.100.28 DNS         20
192.168.100.28 -> 192.42.93.30 DNS         20
192.54.112.30 -> 192.168.100.28 DNS        18
192.168.100.28 -> 192.54.112.30 DNS        18
206.98.114.20 -> 192.168.100.28 DNS        18
62.211.66.16 -> 192.168.100.28 FTP         18
192.168.100.28 -> 206.98.114.20 DNS        18
192.52.178.30 -> 192.168.100.28 DNS        17
192.168.100.28 -> 200.33.148.193 DNS       17
192.168.100.28 -> 205.152.0.5 DNS          17
192.168.100.28 -> 192.52.178.30 DNS        17
192.168.100.28 -> 210.180.98.69 DNS        17
210.180.98.69 -> 192.168.100.28 DNS        17
205.152.0.5 -> 192.168.100.28 DNS          17
192.168.100.28 -> 210.94.0.7 DNS           17
200.33.148.193 -> 192.168.100.28 DNS       17
210.94.0.7 -> 192.168.100.28 DNS           17
192.168.100.28 -> 198.133.199.110 DNS       16
192.168.100.28 -> 62.211.66.16 FTP         15
```

```
192.168.100.28 -> 200.23.1.1 DNS           15
148.244.153.82 -> 192.168.100.28 DNS       15
200.23.1.1 -> 192.168.100.28 DNS           15
192.168.100.28 -> 192.18.99.122 FTP        14
206.98.114.10 -> 192.168.100.28 DNS        14
192.18.99.122 -> 192.168.100.28 TCP        14
192.168.100.28 -> 206.98.114.10 DNS        14
192.168.100.28 -> 128.63.2.53 DNS          13
192.168.100.28 -> 206.252.192.195 IRC       13
204.176.88.5 -> 192.168.100.28 ICMP        13
192.168.100.28 -> 66.28.255.130 ICMP       13
192.168.100.28 -> 64.15.251.198 ICMP       13
192.168.100.28 -> 148.244.153.82 DNS       13
128.63.2.53 -> 192.168.100.28 DNS          13
64.0.96.12 -> 192.168.100.28 ICMP          13
192.168.100.28 -> 213.61.6.2 ICMP          13
192.168.100.28 -> 212.62.17.145 ICMP       13
192.168.100.72 -> 192.168.100.28 DNS       13
64.14.117.10 -> 192.168.100.28 ICMP        13
213.61.6.2 -> 192.168.100.28 ICMP          13
192.168.100.28 -> 208.185.54.14 ICMP       13
63.218.7.130 -> 192.168.100.28 ICMP        13
192.168.100.28 -> 64.14.117.10 ICMP        13
64.15.251.198 -> 192.168.100.28 ICMP       13
192.168.100.28 -> 63.218.7.130 ICMP        13
192.168.100.28 -> 213.234.132.130 DNS       13
192.168.100.28 -> 192.168.100.72 DNS       13
208.185.54.14 -> 192.168.100.28 ICMP       13
66.28.255.130 -> 192.168.100.28 ICMP       13
192.168.100.28 -> 64.0.96.12 ICMP          13
213.234.132.130 -> 192.168.100.28 DNS       13
192.168.100.28 -> 204.176.88.5 ICMP        13
212.62.17.145 -> 192.168.100.28 ICMP       13
205.152.0.20 -> 192.168.100.28 DNS         12
192.168.100.28 -> 200.23.242.193 DNS       12
198.133.199.110 -> 192.168.100.28 DNS       12
192.168.100.28 -> 204.176.177.10 DNS       12
192.168.100.28 -> 205.152.0.20 DNS         12
200.23.242.193 -> 192.168.100.28 DNS       12
128.242.107.15 -> 192.168.100.28 DNS       12
204.176.177.10 -> 192.168.100.28 DNS       11
192.168.100.28 -> 204.70.57.242 DNS        11
204.70.57.242 -> 192.168.100.28 DNS        11
192.168.100.28 -> 192.58.128.30 DNS        11
132.248.253.1 -> 192.168.100.28 DNS        11
192.58.128.30 -> 192.168.100.28 DNS        11
192.168.100.28 -> 213.234.128.211 DNS       10
192.168.100.28 -> 193.0.0.193 DNS          10
193.0.0.193 -> 192.168.100.28 DNS          10
66.28.47.162 -> 192.168.100.28 ICMP        10
192.168.100.28 -> 66.28.47.162 ICMP        10
213.234.128.211 -> 192.168.100.28 DNS       10
192.168.100.28 -> 192.43.172.30 DNS        10
192.168.100.28 -> 168.95.1.14 DNS          10
168.95.1.14 -> 192.168.100.28 DNS          10
64.0.96.22 -> 192.168.100.28 DNS           10
192.168.100.28 -> 64.0.96.22 DNS           10
```

```
192.43.172.30 -> 192.168.100.28 DNS        10
200.33.146.201 -> 192.168.100.28 DNS       10
192.168.100.28 -> 200.33.146.201 DNS       10
192.168.100.28 -> 216.73.82.10 ICMP         9
63.210.142.26 -> 192.168.100.28 DNS         9
216.73.82.10 -> 192.168.100.28 ICMP         9
192.168.100.28 -> 61.144.145.243 TCP        9
192.48.79.30 -> 192.168.100.28 DNS          9
192.168.100.28 -> 64.14.76.206 DNS          9
192.168.100.28 -> 63.210.142.26 DNS         9
63.121.106.134 -> 192.168.100.28 DNS        9
192.168.100.28 -> 63.121.106.134 DNS        9
64.14.76.206 -> 192.168.100.28 DNS          9
61.144.145.243 -> 192.168.100.28 TCP        9
192.168.100.28 -> 192.48.79.30 DNS          9
206.79.230.10 -> 192.168.100.28 DNS         8
192.41.162.32 -> 192.168.100.28 DNS         8
192.168.100.28 -> 140.135.18.15 DNS         8
192.168.100.28 -> 192.168.100.198 DNS        8
192.168.100.28 -> 211.216.50.150 DNS        8
192.168.100.28 -> 64.15.251.221 DNS         8
192.168.100.28 -> 192.41.162.32 DNS         8
192.168.100.198 -> 192.168.100.28 DNS        8
192.168.100.28 -> 151.164.1.1 DNS           8
192.168.100.28 -> 206.79.230.10 DNS         8
151.164.1.1 -> 192.168.100.28 DNS           8
211.216.50.150 -> 192.168.100.28 DNS        8
64.15.251.221 -> 192.168.100.28 DNS         8
168.95.192.14 -> 192.168.100.28 DNS         8
192.168.100.28 -> 168.95.192.14 DNS         8
64.58.77.85 -> 192.168.100.28 DNS           8
192.168.100.28 -> 64.58.77.85 DNS           8
192.168.100.28 -> 211.216.50.130 DNS        7
192.168.100.28 -> 132.248.253.1 DNS         7
216.32.120.21 -> 192.168.100.28 DNS         7
192.168.100.28 -> 216.32.120.21 DNS         7
199.2.117.66 -> 192.168.100.28 DNS          7
140.135.18.15 -> 192.168.100.28 DNS         7
192.168.100.28 -> 209.132.1.28 DNS          7
192.168.100.28 -> 199.2.117.66 DNS          7
192.55.83.30 -> 192.168.100.28 DNS          7
209.132.1.28 -> 192.168.100.28 DNS          7
211.216.50.130 -> 192.168.100.28 DNS        7
192.168.100.28 -> 192.55.83.30 DNS          7
192.168.100.28 -> 65.54.248.222 DNS         7
65.54.248.222 -> 192.168.100.28 DNS         7
192.168.100.28 -> 210.81.13.179 DNS         6
206.252.192.195 -> 192.168.100.28 IRC        6
216.32.126.150 -> 192.168.100.28 DNS        6
192.168.100.28 -> 12.129.72.181 DNS         6
207.82.198.150 -> 192.168.100.28 DNS        6
192.168.100.28 -> 216.32.65.14 DNS          6
216.32.65.14 -> 192.168.100.28 DNS          6
206.252.192.5 -> 192.168.100.28 DNS         6
12.129.72.181 -> 192.168.100.28 DNS         6
192.168.100.28 -> 207.82.198.150 DNS        6
192.168.100.28 -> 206.252.192.5 DNS         6
```

```
192.168.100.28 -> 216.239.38.10 DNS         6
216.239.38.10 -> 192.168.100.28 DNS         6
192.168.100.28 -> 216.32.126.150 DNS        6
192.168.100.28 -> 207.248.240.42 DNS        5
192.168.100.28 -> 167.216.196.131 DNS        5
192.168.100.28 -> 192.115.106.11 DNS        5
192.168.100.28 -> 203.255.234.103 DNS        5
192.168.100.28 -> 63.123.77.194 ICMP        5
192.168.100.28 -> 66.28.255.153 DNS         5
192.115.106.11 -> 192.168.100.28 DNS        5
167.216.196.131 -> 192.168.100.28 DNS        5
192.168.100.28 -> 205.138.3.20 DNS          5
203.255.234.103 -> 192.168.100.28 DNS        5
63.123.77.194 -> 192.168.100.28 ICMP        5
192.168.100.28 -> 206.252.192.6 DNS         5
205.138.3.20 -> 192.168.100.28 DNS          5
66.28.255.153 -> 192.168.100.28 DNS         5
206.252.192.6 -> 192.168.100.28 DNS         5
207.248.240.42 -> 192.168.100.28 DNS        5
210.81.13.179 -> 192.168.100.28 DNS         5
192.168.100.28 -> 208.211.225.10 DNS        4
200.34.163.34 -> 192.168.100.28 DNS         4
192.168.100.28 -> 211.47.45.22 DNS          4
207.46.138.20 -> 192.168.100.28 DNS         4
192.168.100.28 -> 192.115.106.10 DNS        4
192.168.100.28 -> 151.164.1.7 DNS           4
63.218.7.158 -> 192.168.100.28 DNS          4
151.164.1.7 -> 192.168.100.28 DNS           4
192.168.100.28 -> 169.158.128.136 DNS        4
212.62.17.141 -> 192.168.100.28 DNS         4
192.168.100.28 -> 209.185.188.14 DNS        4
213.199.144.151 -> 192.168.100.28 DNS        4
200.23.242.201 -> 192.168.100.28 DNS        4
192.168.100.28 -> 212.62.17.141 DNS         4
211.47.45.22 -> 192.168.100.28 DNS          4
192.168.100.28 -> 64.14.117.6 DNS           4
64.24.196.50 -> 192.168.100.28 TCP          4
192.168.100.28 -> 208.254.75.130 ICMP        4
64.14.117.6 -> 192.168.100.28 DNS           4
151.99.125.2 -> 192.168.100.28 DNS          4
192.168.100.28 -> 208.185.54.23 DNS         4
192.168.100.28 -> 200.23.242.201 DNS        4
192.168.100.28 -> 207.46.138.20 DNS         4
192.168.100.28 -> 64.24.196.50 TCP          4
192.168.100.28 -> 209.1.235.120 DNS         4
192.168.100.28 -> 213.199.144.151 DNS        4
209.1.235.120 -> 192.168.100.28 DNS         4
209.185.188.14 -> 192.168.100.28 DNS        4
204.253.104.10 -> 192.168.100.28 DNS        4
208.211.225.10 -> 192.168.100.28 DNS        4
192.115.106.10 -> 192.168.100.28 DNS        4
192.168.100.28 -> 204.253.104.10 DNS        4
192.168.100.28 -> 63.218.7.158 DNS          4
192.168.100.28 -> 194.25.0.125 DNS          4
192.168.100.28 -> 151.99.125.2 DNS          4
208.185.54.23 -> 192.168.100.28 DNS         4
192.168.100.28 -> 200.34.163.34 DNS         4
```

```
192.168.100.28 -> 192.149.252.21 DNS        4
208.254.75.130 -> 192.168.100.28 ICMP        4
192.168.100.28 -> 169.158.128.156 DNS        4
203.248.240.31 -> 192.168.100.28 DNS        3
203.199.107.187 -> 192.168.100.28 ICMP        3
192.168.100.28 -> 202.130.158.130 ICMP        3
137.39.1.3 -> 192.168.100.28 DNS            3
193.205.245.5 -> 192.168.100.28 DNS         3
64.124.186.66 -> 192.168.100.28 ICMP        3
200.33.148.201 -> 192.168.100.28 DNS        3
216.39.69.65 -> 192.168.100.28 ICMP         3
62.211.66.53 -> 192.168.100.28 TCP          3
192.168.100.163 -> 192.168.100.28 DNS        3
192.168.100.28 -> 67.195.152.135 TCP        3
192.168.100.28 -> 66.218.71.63 DNS          3
192.168.100.28 -> 192.83.166.11 DNS         3
192.168.100.28 -> 203.197.173.129 ICMP        3
204.248.36.130 -> 192.168.100.28 DNS        3
192.168.100.28 -> 63.215.198.79 DNS         3
193.0.0.237 -> 192.168.100.28 DNS           3
192.168.100.28 -> 216.21.234.73 DNS         3
192.168.100.28 -> 202.12.28.131 DNS         3
192.168.100.28 -> 203.248.240.31 DNS        3
64.160.228.206 -> 192.168.100.28 TCP        3
128.8.10.90 -> 192.168.100.28 DNS           3
192.168.100.28 -> 193.0.0.237 DNS           3
66.236.129.66 -> 192.168.100.28 ICMP        3
192.168.100.28 -> 195.20.224.98 DNS         3
24.167.44.129 -> 192.168.100.28 TCP         3
192.168.100.28 -> 128.8.10.90 DNS           3
192.168.100.28 -> 129.70.132.100 DNS        3
192.36.125.2 -> 192.168.100.28 DNS          3
192.168.100.28 -> 202.54.111.72 ICMP        3
202.54.111.72 -> 192.168.100.28 ICMP        3
192.168.100.28 -> 203.239.31.60 TCP         3
203.197.173.129 -> 192.168.100.28 ICMP        3
192.168.100.28 -> 64.124.186.66 ICMP        3
192.168.100.28 -> 217.12.4.104 DNS          3
216.21.234.73 -> 192.168.100.28 DNS         3
202.12.28.131 -> 192.168.100.28 DNS         3
192.168.100.28 -> 64.160.228.206 TCP        3
64.231.37.135 -> 192.168.100.28 TCP         3
211.214.125.74 -> 192.168.100.28 TCP        3
207.46.245.230 -> 192.168.100.28 DNS        3
192.168.100.28 -> 65.203.232.2 ICMP         3
211.14.0.99 -> 192.168.100.28 ICMP          3
192.168.100.28 -> 192.31.80.32 DNS          3
192.168.100.28 -> 203.199.107.187 ICMP        3
192.168.100.28 -> 209.10.34.55 DNS          3
192.168.100.28 -> 192.168.100.158 Syslog        3
192.168.100.28 -> 192.36.125.2 DNS          3
216.34.88.17 -> 192.168.100.28 ICMP         3
67.36.28.116 -> 192.168.100.28 TCP          3
192.168.100.28 -> 217.5.100.185 DNS         3
212.113.82.90 -> 192.168.100.28 DNS         3
192.168.100.28 -> 137.39.1.3 DNS            3
192.168.100.28 -> 66.236.129.66 ICMP        3
```

```
203.239.31.60 -> 192.168.100.28 TCP         3
216.74.133.194 -> 192.168.100.28 ICMP        3
192.168.100.28 -> 24.167.44.129 TCP         3
192.149.252.21 -> 192.168.100.28 DNS        3
195.20.224.98 -> 192.168.100.28 DNS         3
202.130.158.130 -> 192.168.100.28 ICMP        3
192.168.100.28 -> 203.89.210.82 ICMP        3
192.168.100.28 -> 193.205.245.5 DNS         3
64.14.42.16 -> 192.168.100.28 ICMP          3
192.168.100.28 -> 216.34.88.17 ICMP         3
192.168.100.28 -> 67.36.28.116 TCP          3
192.168.100.28 -> 64.231.37.135 TCP         3
192.168.100.28 -> 192.168.100.163 DNS        3
217.12.4.104 -> 192.168.100.28 DNS          3
192.168.100.28 -> 211.214.125.74 TCP        3
192.31.80.32 -> 192.168.100.28 DNS          3
65.203.232.2 -> 192.168.100.28 ICMP         3
67.195.152.135 -> 192.168.100.28 TCP        3
192.168.100.28 -> 204.248.36.130 DNS        3
192.168.100.28 -> 216.21.226.73 DNS         3
192.168.100.28 -> 64.14.42.16 ICMP          3
192.168.100.28 -> 216.74.133.194 ICMP        3
192.168.100.28 -> 212.113.82.90 DNS         3
203.89.210.82 -> 192.168.100.28 ICMP        3
192.168.100.28 -> 216.39.69.65 ICMP         3
192.168.100.28 -> 193.205.245.8 DNS         3
63.215.198.79 -> 192.168.100.28 DNS         3
192.168.100.28 -> 211.14.0.99 ICMP          3
192.168.100.28 -> 200.33.148.201 DNS        3
217.5.100.185 -> 192.168.100.28 DNS         3
192.168.100.28 -> 207.46.245.230 DNS        3
193.205.245.8 -> 192.168.100.28 ICMP        3
129.70.132.100 -> 192.168.100.28 DNS        3
66.218.71.63 -> 192.168.100.28 DNS          3
192.83.166.11 -> 192.168.100.28 DNS         2
192.168.100.28 -> 64.12.51.132 DNS          2
216.136.155.4 -> 192.168.100.28 DNS         2
192.168.100.28 -> 192.149.252.22 DNS        2
192.168.100.28 -> 209.164.7.66 ICMP         2
192.168.100.28 -> 216.73.83.10 ICMP         2
192.168.100.28 -> 216.35.213.248 DNS        2
192.168.100.28 -> 12.110.133.131 DNS        2
128.121.101.11 -> 192.168.100.28 DNS        2
192.168.100.28 -> 203.248.240.141 DNS        2
192.168.100.28 -> 64.37.246.2 ICMP          2
192.168.100.28 -> 213.61.6.5 DNS            2
63.241.199.50 -> 192.168.100.28 DNS         2
192.168.100.28 -> 148.244.240.195 DNS        2
192.94.163.152 -> 192.168.100.28 DNS        2
192.5.5.241 -> 192.168.100.28 DNS           2
192.168.100.28 -> 209.41.31.13 DNS          2
206.65.191.194 -> 192.168.100.28 ICMP        2
192.168.100.28 -> 148.244.153.69 DNS        2
213.133.105.2 -> 192.168.100.28 DNS         2
192.168.100.28 -> 203.73.24.8 DNS           2
192.168.100.28 -> 63.215.198.78 DNS         2
207.44.0.1 -> 192.168.100.28 DNS            2
```

```
134.106.1.7 -> 192.168.100.28 DNS              2
192.109.42.4 -> 192.168.100.28 DNS             2
210.65.0.28 -> 192.168.100.28 DNS              2
192.168.100.28 -> 202.30.50.50 DNS             2
63.209.5.253 -> 192.168.100.28 DNS             2
192.168.100.28 -> 209.209.37.11 DNS            2
195.20.225.40 -> 192.168.100.28 DNS            2
192.168.100.28 -> 164.124.101.31 DNS           2
192.168.100.28 -> 210.65.0.28 DNS              2
192.168.100.28 -> 38.8.50.2 DNS                2
206.65.170.100 -> 192.168.100.28 DNS           2
192.168.100.28 -> 200.10.202.3 DNS             2
152.163.159.232 -> 192.168.100.28 DNS           2
192.168.100.28 -> 213.133.105.2 DNS            2
205.188.157.232 -> 192.168.100.28 DNS           2
64.28.86.226 -> 192.168.100.28 ICMP            2
192.168.100.28 -> 207.68.128.151 DNS           2
192.168.100.28 -> 62.211.66.53 HTTP            2
63.215.198.78 -> 192.168.100.28 DNS            2
192.168.100.28 -> 206.65.183.71 DNS            2
192.149.252.22 -> 192.168.100.28 DNS           2
207.158.192.40 -> 192.168.100.28 DNS           2
192.168.100.28 -> 64.215.170.28 DNS            2
200.73.172.25 -> 192.168.100.28 DNS            2
209.164.7.66 -> 192.168.100.28 ICMP            2
206.65.183.71 -> 192.168.100.28 DNS            2
205.180.85.6 -> 192.168.100.28 DNS             2
192.168.100.28 -> 216.73.84.10 ICMP            2
194.85.119.1 -> 192.168.100.28 DNS             2
192.168.100.28 -> 207.158.192.40 DNS           2
159.226.6.178 -> 192.168.100.28 DNS            2
192.168.100.28 -> 216.136.217.67 DNS           2
192.168.100.28 -> 216.239.36.10 DNS            2
192.168.100.28 -> 200.73.172.25 DNS            2
62.53.3.68 -> 192.168.100.28 DNS               2
192.168.100.28 -> 205.180.85.6 DNS             2
209.10.34.55 -> 192.168.100.28 DNS             2
203.73.24.8 -> 192.168.100.28 DNS              2
192.168.100.28 -> 63.241.199.50 DNS            2
192.168.100.28 -> 205.188.157.232 DNS           2
128.9.0.107 -> 192.168.100.28 DNS              2
141.1.27.248 -> 192.168.100.28 DNS             2
216.239.32.10 -> 192.168.100.28 DNS            2
209.209.37.11 -> 192.168.100.28 DNS            2
192.168.100.28 -> 134.106.1.7 DNS              2
204.69.234.1 -> 192.168.100.28 DNS             2
192.168.100.28 -> 217.32.247.132 DNS           2
192.168.100.28 -> 194.246.96.49 DNS            2
192.168.100.28 -> 192.168.100.71 DNS           2
63.236.5.157 -> 192.168.100.28 DNS             2
204.74.101.1 -> 192.168.100.28 DNS             2
192.168.100.28 -> 168.95.192.2 DNS             2
192.168.100.28 -> 192.112.36.4 DNS             2
192.203.230.10 -> 192.168.100.28 DNS           2
192.168.100.28 -> 194.246.96.79 DNS            2
4.2.49.2 -> 192.168.100.28 DNS                 2
192.168.100.28 -> 207.44.0.1 DNS               2
```

```
192.168.100.28 -> 148.244.249.75 DNS        2
192.168.100.28 -> 192.203.230.10 DNS        2
192.168.100.28 -> 128.121.101.11 DNS        2
192.168.100.28 -> 192.5.5.241 DNS           2
216.136.217.67 -> 192.168.100.28 DNS        2
200.33.246.1 -> 192.168.100.28 DNS          2
38.8.50.2 -> 192.168.100.28 DNS             2
192.168.100.28 -> 202.12.29.60 DNS          2
192.168.100.28 -> 211.216.50.160 DNS        2
192.168.100.28 -> 151.99.125.138 DNS        2
216.35.213.248 -> 192.168.100.28 DNS        2
194.246.96.79 -> 192.168.100.28 DNS         2
192.168.100.28 -> 64.95.61.36 DNS           2
192.168.100.28 -> 63.236.5.157 DNS          2
192.168.100.28 -> 192.36.148.17 DNS         2
66.135.207.138 -> 192.168.100.28 DNS        2
192.168.100.28 -> 216.136.155.4 DNS         2
192.168.100.28 -> 192.33.4.12 DNS           2
192.168.100.28 -> 216.136.217.66 DNS        2
192.168.100.28 -> 159.226.6.178 DNS         2
205.188.132.235 -> 192.168.100.28 DNS        2
164.124.101.31 -> 192.168.100.28 DNS        2
209.41.31.13 -> 192.168.100.28 DNS          2
192.168.100.28 -> 192.94.163.152 DNS        2
148.244.153.69 -> 192.168.100.28 DNS        2
192.168.100.28 -> 206.65.191.194 ICMP        2
192.168.100.28 -> 150.100.2.3 DNS           2
192.168.100.28 -> 4.2.49.2 DNS              2
192.168.100.28 -> 204.69.234.1 DNS          2
192.168.100.28 -> 165.193.217.2 ICMP        2
168.95.192.2 -> 192.168.100.28 DNS          2
192.168.100.28 -> 128.9.0.107 DNS           2
192.168.100.28 -> 141.1.27.248 DNS          2
192.168.100.28 -> 195.20.225.40 DNS         2
64.215.170.28 -> 192.168.100.28 DNS         2
203.248.240.141 -> 192.168.100.28 DNS        2
150.100.2.3 -> 192.168.100.28 DNS           2
192.168.100.28 -> 209.209.37.6 DNS          2
192.168.100.28 -> 128.242.107.15 DNS        2
66.135.207.137 -> 192.168.100.28 DNS        2
192.168.100.28 -> 192.109.42.4 DNS          2
192.168.100.28 -> 205.188.132.235 DNS        2
192.168.100.28 -> 151.99.250.2 DNS          2
213.61.6.5 -> 192.168.100.28 DNS            2
195.129.12.74 -> 192.168.100.28 DNS         2
202.12.29.60 -> 192.168.100.28 DNS          2
192.168.100.28 -> 62.53.3.68 DNS            2
192.168.100.28 -> 209.10.66.55 DNS          2
207.68.128.151 -> 192.168.100.28 DNS        2
64.95.61.36 -> 192.168.100.28 DNS           2
216.136.217.66 -> 192.168.100.28 DNS        2
192.168.100.28 -> 152.163.159.232 DNS        2
12.110.133.131 -> 192.168.100.28 DNS        2
192.168.100.28 -> 208.225.197.194 ICMP        2
192.168.100.28 -> 66.135.207.138 DNS        2
165.193.217.2 -> 192.168.100.28 ICMP        2
192.36.148.17 -> 192.168.100.28 DNS         2
```

```
12.47.217.11 -> 192.168.100.28 DNS          2
192.168.100.28 -> 66.135.207.137 DNS        2
192.168.100.28 -> 206.65.170.100 DNS        2
216.64.158.11 -> 192.168.100.28 DNS         2
148.244.153.69 -> 192.168.100.28 ICMP        2
217.32.247.132 -> 192.168.100.28 DNS        2
4.22.49.75 -> 192.168.100.28 DNS            2
192.168.100.28 -> 12.47.217.11 DNS          2
192.168.100.28 -> 130.206.1.2 DNS           2
192.168.100.28 -> 216.64.158.11 DNS         2
64.12.51.132 -> 192.168.100.28 DNS          2
151.99.125.138 -> 192.168.100.28 DNS        2
192.168.100.28 -> 200.33.246.1 DNS          2
192.168.100.28 -> 4.22.49.75 DNS            2
192.168.100.28 -> 195.129.12.74 DNS         2
192.168.100.28 -> 63.209.5.253 DNS          2
151.99.250.2 -> 192.168.100.28 DNS          2
192.33.4.12 -> 192.168.100.28 DNS           2
211.216.50.160 -> 192.168.100.28 DNS        2
148.244.249.75 -> 192.168.100.28 DNS        2
209.10.66.55 -> 192.168.100.28 DNS          2
216.239.36.10 -> 192.168.100.28 DNS         2
194.246.96.49 -> 192.168.100.28 DNS         2
148.244.240.195 -> 192.168.100.28 DNS        2
192.168.100.28 -> 204.74.101.1 DNS          2
192.168.100.28 -> 198.6.1.181 DNS           2
209.209.37.6 -> 192.168.100.28 DNS          2
216.73.84.10 -> 192.168.100.28 ICMP         2
130.206.1.2 -> 192.168.100.28 DNS           2
64.37.246.2 -> 192.168.100.28 ICMP          2
216.73.83.10 -> 192.168.100.28 ICMP         2
200.10.202.3 -> 192.168.100.28 DNS          2
198.6.1.181 -> 192.168.100.28 DNS           2
192.168.100.28 -> 194.85.119.1 DNS          2
208.225.197.194 -> 192.168.100.28 ICMP        2
192.168.100.28 -> 64.28.86.226 ICMP         2
192.168.100.71 -> 192.168.100.28 DNS        2
192.168.100.28 -> 216.239.32.10 DNS         2
192.168.100.28 -> 195.145.119.189 DNS        1
193.205.245.66 -> 192.168.100.28 DNS        1
192.168.100.28 -> 213.61.5.28 DNS           1
216.32.65.105 -> 192.168.100.28 DNS         1
64.226.28.33 -> 192.168.100.28 DNS          1
192.168.100.28 -> 200.4.48.13 DNS           1
192.168.100.28 -> 204.253.104.11 DNS        1
207.227.117.2 -> 192.168.100.28 DNS         1
192.168.100.28 -> 193.205.245.66 DNS        1
192.168.100.28 -> 216.218.131.2 DNS         1
12.129.11.44 -> 192.168.100.28 DNS          1
192.168.100.28 -> 10.12.9.141 ICMP          1
63.209.29.138 -> 192.168.100.28 DNS         1
192.168.100.28 -> 212.172.60.17 DNS         1
192.168.100.28 -> 63.98.240.201 DNS         1
128.32.206.9 -> 192.168.100.28 DNS          1
209.126.152.242 -> 192.168.100.28 DNS        1
192.168.100.28 -> 212.109.58.202 DNS        1
65.206.228.71 -> 192.168.100.28 DNS         1
```

```
194.237.107.6 -> 192.168.100.28 DNS         1
192.168.100.28 -> 128.32.206.9 DNS          1
64.26.0.23 -> 192.168.100.28 DNS            1
192.168.100.28 -> 212.53.64.30 DNS          1
192.168.100.28 -> 203.136.232.67 DNS        1
200.52.132.83 -> 192.168.100.28 DNS         1
192.168.100.28 -> 213.133.104.2 DNS         1
192.168.100.28 -> 209.133.1.96 DNS          1
192.168.100.28 -> 65.163.234.133 DNS        1
192.168.100.28 -> 193.79.163.118 ICMP        1
192.168.100.28 -> 151.99.125.3 DNS          1
213.152.145.16 -> 192.168.100.28 DNS        1
192.168.100.28 -> 139.130.4.5 DNS           1
192.168.100.28 -> 64.39.29.212 DNS          1
192.168.100.28 -> 63.71.94.5 DNS            1
192.168.100.28 -> 207.235.16.2 DNS          1
192.168.100.28 -> 200.52.66.125 DNS         1
192.168.100.28 -> 192.134.0.49 DNS          1
192.168.100.28 -> 12.129.11.44 DNS          1
209.249.55.102 -> 192.168.100.28 DNS        1
192.168.100.28 -> 198.6.1.114 DNS           1
192.168.100.28 -> 194.109.218.36 DNS        1
209.68.217.194 -> 192.168.100.28 ICMP        1
151.99.125.3 -> 192.168.100.28 DNS          1
192.168.100.28 -> 216.113.128.58 DNS        1
208.172.80.140 -> 192.168.100.28 DNS        1
206.65.183.21 -> 192.168.100.28 DNS         1
16.1.0.18 -> 192.168.100.28 DNS             1
192.168.100.28 -> 202.144.78.2 ICMP         1
192.168.100.28 -> 207.248.240.41 DNS        1
192.168.100.28 -> 200.171.38.61 ICMP        1
63.211.121.147 -> 192.168.100.28 DNS        1
192.168.100.28 -> 193.108.91.3 DNS          1
192.109.42.5 -> 192.168.100.28 DNS          1
192.168.100.28 -> 61.221.179.26 TCP         1
192.168.100.28 -> 66.111.73.173 DNS         1
192.168.100.28 -> 168.95.192.10 DNS         1
192.168.100.28 -> 65.206.228.71 DNS         1
192.168.100.28 -> 209.225.41.200 DNS        1
192.168.100.28 -> 216.136.225.202 DNS        1
210.155.137.2 -> 192.168.100.28 DNS         1
192.168.100.28 -> 213.152.145.16 DNS        1
192.168.100.28 -> 207.182.224.10 DNS        1
202.12.29.59 -> 192.168.100.28 DNS          1
192.168.100.28 -> 210.8.213.35 DNS          1
212.77.231.12 -> 192.168.100.28 DNS         1
216.218.131.2 -> 192.168.100.28 DNS         1
192.168.100.28 -> 218.17.158.135 ICMP        1
192.168.100.28 -> 212.49.128.65 DNS         1
216.52.244.144 -> 192.168.100.28 DNS        1
192.168.100.28 -> 195.20.224.95 DNS         1
152.163.209.129 -> 192.168.100.28 DNS        1
209.133.1.96 -> 192.168.100.28 DNS          1
213.244.173.25 -> 192.168.100.28 DNS        1
211.13.227.66 -> 192.168.100.28 ICMP        1
192.168.100.28 -> 216.32.65.105 DNS         1
192.168.100.28 -> 158.43.193.80 DNS         1
```

```
212.49.128.65 -> 192.168.100.28 DNS         1
207.248.240.41 -> 192.168.100.28 DNS        1
216.239.34.10 -> 192.168.100.28 DNS         1
192.168.100.28 -> 216.34.88.151 DNS         1
192.168.100.28 -> 204.59.144.222 DNS        1
210.117.65.2 -> 192.168.100.28 DNS          1
192.168.100.28 -> 64.152.2.36 DNS           1
63.71.94.5 -> 192.168.100.28 DNS            1
192.168.100.28 -> 204.74.112.1 DNS          1
192.168.100.28 -> 137.189.6.21 DNS          1
192.168.100.28 -> 165.76.0.98 DNS           1
192.168.100.28 -> 211.75.30.52 TCP          1
64.39.29.212 -> 192.168.100.28 DNS          1
192.168.100.28 -> 193.171.255.34 DNS        1
212.38.191.82 -> 192.168.100.28 DNS         1
209.216.124.211 -> 192.168.100.28 DNS        1
216.221.162.111 -> 192.168.100.28 DNS        1
216.156.2.3 -> 192.168.100.28 DNS           1
192.168.100.28 -> 217.5.100.186 DNS         1
62.4.74.66 -> 192.168.100.28 ICMP           1
193.0.14.129 -> 192.168.100.28 DNS          1
195.20.225.36 -> 192.168.100.28 DNS         1
192.168.100.28 -> 207.227.117.2 DNS         1
192.168.100.28 -> 209.68.217.194 ICMP        1
192.168.100.28 -> 212.121.130.5 DNS         1
192.168.100.28 -> 132.235.64.1 DNS          1
168.95.192.1 -> 192.168.100.28 DNS          1
193.171.255.34 -> 192.168.100.28 DNS        1
216.113.128.58 -> 192.168.100.28 DNS        1
192.9.9.3 -> 192.168.100.28 DNS             1
194.69.254.2 -> 192.168.100.28 DNS          1
192.168.100.28 -> 12.127.16.70 DNS          1
192.168.100.28 -> 63.150.183.46 DNS         1
192.168.100.28 -> 212.74.64.34 DNS          1
213.61.5.28 -> 192.168.100.28 DNS           1
192.168.100.28 -> 200.73.183.198 DNS        1
66.28.34.130 -> 192.168.100.28 ICMP         1
192.168.100.28 -> 203.69.233.93 TCP         1
198.6.1.65 -> 192.168.100.28 DNS            1
192.168.100.28 -> 217.29.76.4 DNS           1
202.32.86.139 -> 192.168.100.28 DNS         1
4.2.49.3 -> 192.168.100.28 DNS              1
200.160.0.5 -> 192.168.100.28 DNS           1
192.168.100.28 -> 202.186.13.228 DNS        1
140.111.1.2 -> 192.168.100.28 DNS           1
192.168.100.28 -> 199.202.200.2 DNS         1
207.235.16.2 -> 192.168.100.28 DNS          1
192.168.100.28 -> 206.20.254.33 DNS         1
193.158.124.130 -> 192.168.100.28 DNS        1
213.86.246.21 -> 192.168.100.28 DNS         1
198.6.1.114 -> 192.168.100.28 DNS           1
192.168.100.28 -> 192.5.6.32 DNS            1
154.32.105.90 -> 192.168.100.28 DNS         1
63.209.170.136 -> 192.168.100.28 DNS        1
200.52.66.125 -> 192.168.100.28 DNS         1
194.25.2.130 -> 192.168.100.28 DNS          1
200.33.246.3 -> 192.168.100.28 DNS          1
```

```
192.168.100.28 -> 63.209.29.138 DNS         1
200.171.38.61 -> 192.168.100.28 NBNS        1
61.221.179.26 -> 192.168.100.28 TCP         1
200.33.146.193 -> 192.168.100.28 DNS        1
192.168.100.28 -> 193.158.124.130 DNS        1
209.225.41.200 -> 192.168.100.28 DNS        1
194.109.218.36 -> 192.168.100.28 DNS        1
193.108.91.93 -> 192.168.100.28 DNS         1
194.25.0.125 -> 192.168.100.28 DNS          1
218.17.158.135 -> 192.168.100.28 NBNS        1
192.168.100.28 -> 4.2.49.3 DNS              1
192.168.100.28 -> 192.9.9.3 DNS             1
212.172.60.17 -> 192.168.100.28 DNS         1
192.168.100.28 -> 204.248.36.131 DNS        1
207.228.252.101 -> 192.168.100.28 DNS        1
192.168.100.28 -> 81.19.67.2 DNS            1
192.168.100.28 -> 193.125.152.3 DNS         1
63.71.94.4 -> 192.168.100.28 DNS            1
63.219.179.130 -> 192.168.100.28 ICMP        1
192.168.100.28 -> 194.25.2.133 DNS          1
192.168.100.28 -> 216.39.68.40 DNS          1
192.168.100.28 -> 160.45.10.13 DNS          1
200.4.48.13 -> 192.168.100.28 DNS           1
192.168.100.28 -> 146.20.43.251 DNS         1
192.168.100.28 -> 129.70.4.55 DNS           1
192.168.100.28 -> 140.111.1.2 DNS           1
192.168.100.28 -> 200.33.246.3 DNS          1
209.247.108.228 -> 192.168.100.28 DNS        1
192.168.100.28 -> 193.108.91.159 DNS        1
192.168.100.28 -> 209.249.55.102 DNS        1
192.168.100.28 -> 64.124.186.252 DNS        1
192.168.100.28 -> 63.208.48.42 DNS          1
148.245.244.157 -> 192.168.100.28 DNS        1
192.168.100.28 -> 63.209.170.136 DNS        1
193.159.170.187 -> 192.168.100.28 DNS        1
163.138.96.11 -> 192.168.100.28 DNS         1
192.168.100.28 -> 134.75.30.1 DNS           1
203.50.0.137 -> 192.168.100.28 DNS          1
194.67.57.4 -> 192.168.100.28 DNS           1
199.202.200.2 -> 192.168.100.28 DNS         1
207.171.171.132 -> 192.168.100.28 DNS        1
192.168.100.28 -> 209.126.152.242 DNS        1
216.52.1.33 -> 192.168.100.28 DNS           1
213.133.104.11 -> 192.168.100.28 DNS        1
12.127.16.70 -> 192.168.100.28 DNS          1
192.168.100.28 -> 198.6.1.182 DNS           1
192.168.100.28 -> 213.86.246.21 DNS         1
206.20.254.33 -> 192.168.100.28 DNS         1
192.168.100.28 -> 193.110.128.201 DNS        1
192.168.100.28 -> 64.226.28.33 DNS          1
192.168.100.28 -> 198.186.202.136 DNS        1
213.133.104.2 -> 192.168.100.28 DNS         1
216.148.227.68 -> 192.168.100.28 DNS        1
192.168.100.28 -> 63.71.94.4 DNS            1
192.168.100.28 -> 194.25.2.130 DNS          1
132.235.64.1 -> 192.168.100.28 DNS          1
192.168.100.28 -> 203.37.255.97 DNS         1
```

```
192.168.100.28 -> 202.160.241.130 ICMP        1
195.13.2.13 -> 192.168.100.28 DNS          1
192.168.100.28 -> 64.26.0.23 DNS           1
192.168.100.28 -> 62.13.128.20 DNS         1
212.53.64.30 -> 192.168.100.28 DNS         1
192.168.100.28 -> 163.138.96.11 DNS        1
149.174.211.8 -> 192.168.100.28 DNS        1
192.168.100.28 -> 152.163.209.129 DNS       1
192.168.100.28 -> 194.98.19.1 DNS          1
216.39.68.40 -> 192.168.100.28 DNS         1
192.168.100.28 -> 213.133.104.11 DNS       1
192.168.100.28 -> 208.172.80.140 DNS       1
65.163.234.133 -> 192.168.100.28 DNS       1
192.168.100.28 -> 128.242.107.5 DNS        1
64.58.79.83 -> 192.168.100.28 DNS          1
202.144.78.2 -> 192.168.100.28 ICMP        1
192.168.100.28 -> 216.35.213.247 DNS       1
204.59.144.222 -> 192.168.100.28 DNS       1
192.168.100.28 -> 216.221.162.111 DNS       1
192.168.100.28 -> 207.228.252.101 DNS       1
192.134.0.49 -> 192.168.100.28 DNS         1
192.168.100.28 -> 64.58.79.83 DNS          1
207.44.96.129 -> 192.168.100.28 DNS        1
192.168.100.28 -> 168.144.68.8 DNS         1
195.66.240.130 -> 192.168.100.28 DNS       1
192.168.100.28 -> 207.171.171.132 DNS       1
192.168.100.28 -> 216.169.161.225 DNS       1
128.242.107.5 -> 192.168.100.28 DNS        1
209.41.31.14 -> 192.168.100.28 DNS         1
202.160.241.130 -> 192.168.100.28 ICMP        1
210.81.97.184 -> 192.168.100.28 DNS        1
203.136.232.67 -> 192.168.100.28 DNS       1
192.168.100.28 -> 63.219.179.130 ICMP       1
195.167.217.34 -> 192.168.100.28 DNS       1
192.168.100.28 -> 200.160.0.5 DNS          1
192.168.100.28 -> 202.12.27.33 DNS         1
192.168.100.28 -> 16.1.0.18 DNS            1
192.168.100.28 -> 63.211.121.147 DNS       1
63.215.198.86 -> 192.168.100.28 DNS        1
192.168.100.28 -> 192.76.144.16 DNS        1
192.76.144.16 -> 192.168.100.28 DNS        1
192.5.6.32 -> 192.168.100.28 DNS           1
192.168.100.28 -> 194.168.4.237 DNS        1
192.168.100.28 -> 212.38.191.82 DNS        1
169.158.128.136 -> 192.168.100.28 DNS       1
192.168.100.28 -> 193.159.170.187 DNS       1
192.168.100.28 -> 206.65.183.21 DNS        1
192.168.100.28 -> 62.4.74.66 ICMP          1
208.138.153.11 -> 192.168.100.28 DNS       1
192.168.100.28 -> 212.77.231.12 DNS        1
64.152.2.36 -> 192.168.100.28 DNS          1
192.168.100.28 -> 192.188.72.21 DNS        1
192.168.100.28 -> 192.35.51.32 DNS         1
192.168.100.28 -> 148.245.244.157 DNS       1
202.12.27.33 -> 192.168.100.28 DNS         1
192.168.100.28 -> 208.184.139.82 ICMP       1
192.168.100.28 -> 216.148.227.68 DNS       1
```

```
192.35.51.34 -> 192.168.100.28 DNS         1
195.5.64.2 -> 192.168.100.28 DNS           1
192.168.100.28 -> 216.239.34.10 DNS        1
64.124.186.252 -> 192.168.100.28 DNS       1
66.28.103.87 -> 192.168.100.28 TCP         1
192.168.100.28 -> 149.174.211.8 DNS        1
192.168.100.28 -> 195.167.217.34 DNS       1
203.37.255.97 -> 192.168.100.28 DNS        1
63.210.142.65 -> 192.168.100.28 DNS        1
130.59.211.10 -> 192.168.100.28 DNS        1
200.73.183.198 -> 192.168.100.28 DNS       1
192.168.100.28 -> 128.86.1.20 DNS          1
81.19.67.2 -> 192.168.100.28 DNS           1
139.130.4.5 -> 192.168.100.28 DNS          1
192.168.100.28 -> 130.59.211.10 DNS        1
160.45.10.13 -> 192.168.100.28 DNS         1
168.95.192.10 -> 192.168.100.28 DNS        1
210.8.213.35 -> 192.168.100.28 DNS         1
192.168.100.28 -> 195.66.240.130 DNS       1
192.168.100.197 -> 192.168.100.28 DNS       1
202.186.13.228 -> 192.168.100.28 DNS       1
192.168.100.28 -> 211.13.227.66 ICMP       1
192.168.100.28 -> 194.237.107.6 DNS        1
168.144.1.177 -> 192.168.100.28 DNS        1
192.168.100.28 -> 194.69.254.2 DNS         1
192.168.100.28 -> 202.32.86.139 DNS        1
192.168.100.28 -> 65.214.50.130 ICMP       1
193.108.91.159 -> 192.168.100.28 DNS       1
212.111.32.38 -> 192.168.100.28 DNS        1
206.65.183.70 -> 192.168.100.28 DNS        1
212.3.247.25 -> 192.168.100.28 DNS         1
192.168.100.28 -> 200.52.132.83 DNS        1
192.168.100.28 -> 209.247.108.228 DNS       1
192.168.100.28 -> 203.178.136.63 DNS       1
192.168.100.28 -> 212.3.247.25 DNS         1
192.168.100.28 -> 202.12.29.59 DNS         1
202.30.50.50 -> 192.168.100.28 DNS         1
192.168.100.28 -> 210.155.137.2 DNS        1
192.168.100.28 -> 64.73.138.71 DNS         1
192.168.100.28 -> 193.108.91.93 DNS        1
216.249.24.15 -> 192.168.100.28 DNS        1
192.112.36.4 -> 192.168.100.28 DNS         1
209.66.103.20 -> 192.168.100.28 DNS        1
204.253.104.11 -> 192.168.100.28 DNS       1
192.168.100.28 -> 194.67.57.4 DNS          1
192.168.100.28 -> 206.65.183.70 DNS        1
203.69.233.93 -> 192.168.100.28 TCP        1
194.168.4.237 -> 192.168.100.28 DNS        1
212.121.130.5 -> 192.168.100.28 DNS        1
192.168.100.28 -> 207.44.96.129 DNS        1
212.109.58.202 -> 192.168.100.28 DNS       1
218.14.182.224 -> 192.168.100.28 NBNS       1
198.186.202.136 -> 192.168.100.28 DNS       1
217.5.100.186 -> 192.168.100.28 DNS        1
193.214.57.194 -> 192.168.100.28 ICMP       1
192.168.100.28 -> 66.28.103.87 TCP         1
193.108.91.3 -> 192.168.100.28 DNS         1
```

```
192.168.100.28 -> 205.138.3.243 DNS         1
192.168.100.28 -> 204.127.198.33 DNS        1
212.74.64.34 -> 192.168.100.28 DNS          1
193.232.212.12 -> 192.168.100.28 DNS        1
129.70.4.55 -> 192.168.100.28 DNS           1
192.168.100.28 -> 192.35.51.34 DNS          1
216.52.1.1 -> 192.168.100.28 DNS            1
192.168.100.28 -> 216.52.244.144 DNS        1
192.168.100.28 -> 66.35.250.12 DNS          1
192.168.100.28 -> 216.147.1.120 DNS         1
165.76.0.98 -> 192.168.100.28 DNS           1
192.168.100.28 -> 203.120.14.5 DNS          1
203.178.136.63 -> 192.168.100.28 DNS        1
192.168.100.28 -> 203.133.1.8 DNS           1
63.98.240.201 -> 192.168.100.28 DNS         1
216.34.88.151 -> 192.168.100.28 DNS         1
192.168.100.28 -> 154.32.105.90 DNS         1
212.80.175.2 -> 192.168.100.28 DNS          1
198.6.1.182 -> 192.168.100.28 DNS           1
216.220.40.243 -> 192.168.100.28 DNS        1
206.132.160.36 -> 192.168.100.28 DNS        1
63.150.183.46 -> 192.168.100.28 DNS         1
168.144.68.8 -> 192.168.100.28 DNS          1
204.248.36.131 -> 192.168.100.28 DNS        1
66.111.73.173 -> 192.168.100.28 DNS         1
192.168.100.28 -> 195.13.2.13 DNS           1
192.168.100.28 -> 212.111.32.38 DNS         1
192.168.100.28 -> 212.66.160.8 DNS          1
204.174.223.1 -> 192.168.100.28 DNS         1
192.168.100.28 -> 208.138.153.11 DNS        1
192.168.100.28 -> 209.41.31.14 DNS          1
192.168.100.28 -> 216.156.2.3 DNS           1
195.145.119.189 -> 192.168.100.28 DNS        1
216.35.213.247 -> 192.168.100.28 DNS        1
194.67.35.252 -> 192.168.100.28 DNS         1
62.13.128.20 -> 192.168.100.28 DNS          1
192.168.100.28 -> 213.199.1.132 DNS         1
192.168.100.28 -> 198.6.1.65 DNS            1
212.66.160.8 -> 192.168.100.28 DNS          1
65.214.50.130 -> 192.168.100.28 ICMP        1
64.73.138.71 -> 192.168.100.28 DNS          1
192.168.100.28 -> 209.216.124.211 DNS        1
192.168.100.28 -> 216.249.24.15 DNS         1
63.209.5.254 -> 192.168.100.28 DNS          1
192.168.100.28 -> 212.227.58.206 DNS        1
63.208.48.42 -> 192.168.100.28 DNS          1
192.168.100.28 -> 195.5.64.2 DNS            1
192.168.100.28 -> 216.220.40.243 DNS        1
192.168.100.28 -> 200.33.146.193 DNS        1
207.182.224.10 -> 192.168.100.28 DNS        1
192.168.100.28 -> 210.117.65.2 DNS          1
66.35.250.12 -> 192.168.100.28 DNS          1
192.168.100.28 -> 192.168.100.197 DNS        1
192.168.100.28 -> 63.210.142.65 DNS         1
212.227.58.206 -> 192.168.100.28 DNS        1
192.168.100.28 -> 63.209.5.254 DNS          1
137.189.6.21 -> 192.168.100.28 DNS          1
```

```
192.168.100.28 -> 193.232.212.12 DNS           1
216.136.225.199 -> 192.168.100.28 DNS          1
216.136.225.202 -> 192.168.100.28 DNS          1
203.120.14.5 -> 192.168.100.28 DNS             1
192.168.100.28 -> 218.14.182.224 ICMP          1
193.79.163.118 -> 192.168.100.28 NBNS          1
128.86.1.20 -> 192.168.100.28 DNS              1
158.43.193.80 -> 192.168.100.28 DNS            1
192.188.72.21 -> 192.168.100.28 DNS            1
192.168.100.28 -> 216.136.225.199 DNS          1
192.168.100.28 -> 63.215.198.86 DNS            1
194.25.2.133 -> 192.168.100.28 DNS             1
213.199.1.132 -> 192.168.100.28 DNS            1
10.12.9.141 -> 192.168.100.28 NBNS             1
192.168.100.28 -> 203.50.0.137 DNS             1
192.168.100.28 -> 216.52.1.1 DNS               1
192.168.100.28 -> 209.66.103.20 DNS            1
192.168.100.28 -> 216.52.1.33 DNS              1
211.75.30.52 -> 192.168.100.28 TCP             1
192.168.100.28 -> 168.95.192.1 DNS             1
193.110.128.201 -> 192.168.100.28 DNS          1
192.168.100.28 -> 168.144.1.177 DNS            1
192.168.100.28 -> 210.81.97.184 DNS            1
192.168.100.28 -> 66.28.34.130 ICMP            1
192.168.100.28 -> 213.244.173.25 DNS           1
203.133.1.8 -> 192.168.100.28 DNS              1
192.168.100.28 -> 204.174.223.1 DNS            1
194.98.19.1 -> 192.168.100.28 DNS              1
195.20.224.95 -> 192.168.100.28 DNS            1
217.29.76.4 -> 192.168.100.28 DNS              1
205.138.3.243 -> 192.168.100.28 DNS            1
192.168.100.28 -> 192.109.42.5 DNS             1
192.168.100.28 -> 194.67.35.252 DNS            1
192.35.51.32 -> 192.168.100.28 DNS             1
192.168.100.28 -> 206.132.160.36 DNS           1
146.20.43.251 -> 192.168.100.28 DNS            1
216.169.161.225 -> 192.168.100.28 DNS          1
193.125.152.3 -> 192.168.100.28 DNS            1
192.168.100.28 -> 212.80.175.2 DNS             1
192.168.100.28 -> 195.20.225.36 DNS            1
192.168.100.28 -> 193.214.57.194 ICMP          1
204.74.112.1 -> 192.168.100.28 DNS             1
208.184.139.82 -> 192.168.100.28 ICMP          1
192.168.100.28 -> 193.0.14.129 DNS             1
204.127.198.33 -> 192.168.100.28 DNS           1
216.147.1.120 -> 192.168.100.28 DNS            1

Total:                                     18843
```

Day 3: Protocol Statistics

```
192.168.100.28 -> 195.130.233.20 TCP       57978
192.168.100.28 -> 205.177.13.231 TCP       18680
195.130.233.20 -> 192.168.100.28 TCP       11706
192.168.100.28 -> 192.114.144.52 TCP        5196
206.252.192.195 -> 192.168.100.28 TCP       2690
192.168.100.28 -> 206.252.192.195 TCP       2425
```

```
192.168.100.28 -> 195.130.233.20 IP      2319
192.168.100.28 -> 195.130.233.20 UDP     2245
192.168.100.28 -> 195.130.233.20 ICMP     2219
62.211.66.55 -> 192.168.100.28 HTTP      1617
195.130.233.20 -> 192.168.100.28 ICMP     1397
62.101.108.86 -> 192.168.100.28 TCP      1042
192.168.100.28 -> 61.134.3.11 ICMP       1036
192.168.100.28 -> 62.211.66.55 TCP       1021
192.168.100.28 -> 62.101.108.86 TCP       913
2001:6b8:0:400::5d0e -> 2001:750:2:0:202:a5ff:fef0:aac7 IRC      912
2001:750:2:0:202:a5ff:fef0:aac7 -> 2001:6b8:0:400::5d0e TCP      896
12.122.12.62 -> 192.168.100.28 ICMP       881
2001:750:2:0:202:a5ff:fef0:aac7 -> 2001:6b8:0:400::5d0e IRC      853
192.168.100.28 -> 217.116.38.10 ICMP      760
61.134.3.11 -> 192.168.100.28 ICMP        757
80.117.14.222 -> 192.168.100.28 TCP       735
2001:6b8:0:400::5d0e -> 2001:750:2:0:202:a5ff:fef0:aac7 TCP      673
205.177.13.231 -> 192.168.100.28 TCP      519
192.168.100.28 -> 80.117.14.222 Gryphon      476
192.168.100.28 -> 80.117.14.222 TCP       471
192.114.144.52 -> 192.168.100.28 TCP      280
80.117.14.222 -> 192.168.100.28 Gryphon      203
12.123.17.57 -> 192.168.100.28 ICMP       156
12.122.2.226 -> 192.168.100.28 ICMP       111
148.244.153.91 -> 192.168.100.28 DNS       95
192.168.100.28 -> 148.244.153.91 DNS       85
192.168.100.28 -> 192.168.100.158 Syslog       63
192.168.100.28 -> 140.135.18.25 DNS        28
140.135.18.25 -> 192.168.100.28 DNS        24
12.122.2.225 -> 192.168.100.28 ICMP        24
192.58.128.30 -> 192.168.100.28 DNS        19
192.168.100.28 -> 192.5.6.30 DNS           18
192.168.100.28 -> 200.33.146.213 DNS       18
192.41.162.30 -> 192.168.100.28 DNS        18
200.33.146.213 -> 192.168.100.28 DNS       18
193.0.0.193 -> 192.168.100.28 DNS          18
192.5.6.30 -> 192.168.100.28 DNS           18
12.122.12.13 -> 192.168.100.28 ICMP        17
192.26.92.30 -> 192.168.100.28 DNS         17
192.168.100.28 -> 192.26.92.30 DNS         17
192.168.100.28 -> 192.41.162.30 DNS        17
192.168.100.28 -> 200.33.213.66 DNS        16
200.33.213.66 -> 192.168.100.28 DNS        16
192.168.100.28 -> 192.58.128.30 DNS        16
192.31.80.30 -> 192.168.100.28 DNS         15
200.33.148.193 -> 192.168.100.28 DNS       15
128.63.2.53 -> 192.168.100.28 DNS          15
192.168.100.28 -> 128.63.2.53 DNS          15
192.42.93.30 -> 192.168.100.28 DNS         14
192.168.100.28 -> 193.0.0.193 DNS          14
12.122.10.73 -> 192.168.100.28 ICMP        14
12.122.12.45 -> 192.168.100.28 ICMP        14
192.168.100.28 -> 192.42.93.30 DNS         14
192.168.100.28 -> 192.31.80.30 DNS         14
206.98.114.20 -> 192.168.100.28 DNS        13
192.168.100.28 -> 200.33.148.193 DNS       13
192.168.100.28 -> 206.98.114.20 DNS        13
```

```
192.168.100.28 -> 210.180.98.69 DNS        12
210.94.0.7 -> 192.168.100.28 DNS           12
192.168.100.28 -> 192.43.172.30 DNS        12
210.180.98.69 -> 192.168.100.28 DNS        12
192.168.100.28 -> 206.98.114.10 DNS        12
192.168.100.28 -> 210.94.0.7 DNS           12
192.43.172.30 -> 192.168.100.28 DNS        12
192.100.59.110 -> 192.168.100.28 DNS       11
211.216.50.150 -> 192.168.100.28 DNS       11
205.152.0.5 -> 192.168.100.28 DNS          11
192.168.100.28 -> 192.48.79.30 DNS         11
192.168.100.28 -> 192.168.100.72 DNS       11
206.98.114.10 -> 192.168.100.28 DNS        11
192.48.79.30 -> 192.168.100.28 DNS         11
192.168.100.28 -> 211.216.50.150 DNS       11
192.168.100.28 -> 192.100.59.110 DNS       11
192.168.100.28 -> 205.152.0.5 DNS          11
205.152.0.20 -> 192.168.100.28 DNS         10
12.122.10.77 -> 192.168.100.28 ICMP        10
192.168.100.28 -> 205.152.0.20 DNS         10
192.168.100.72 -> 192.168.100.28 DNS       10
192.168.100.28 -> 213.234.132.130 DNS        9
213.234.132.130 -> 192.168.100.28 DNS        9
192.168.100.28 -> 198.133.199.110 DNS        8
192.168.100.28 -> 64.0.96.12 ICMP           8
192.35.51.30 -> 192.168.100.28 DNS          8
64.0.96.12 -> 192.168.100.28 ICMP           8
192.168.100.28 -> 200.23.242.193 DNS        8
192.168.100.28 -> 192.35.51.30 DNS          8
198.133.199.110 -> 192.168.100.28 DNS        8
132.248.253.1 -> 192.168.100.28 DNS         8
202.12.28.131 -> 192.168.100.28 DNS         7
192.42.93.32 -> 192.168.100.28 DNS          7
213.234.128.211 -> 192.168.100.28 DNS        7
192.168.100.28 -> 213.234.128.211 DNS        7
192.168.100.28 -> 168.95.192.14 DNS         7
168.95.192.14 -> 192.168.100.28 DNS         7
200.33.146.217 -> 192.168.100.28 DNS        7
211.47.45.22 -> 192.168.100.28 DNS          7
192.168.100.28 -> 211.47.45.22 DNS          7
192.41.162.32 -> 192.168.100.28 DNS         7
192.168.100.28 -> 202.12.28.131 DNS         7
200.23.242.193 -> 192.168.100.28 DNS        7
192.168.100.28 -> 192.42.93.32 DNS          7
192.168.100.28 -> 200.33.146.217 DNS        7
192.168.100.28 -> 206.252.192.6 DNS         7
192.168.100.28 -> 192.41.162.32 DNS         7
206.252.192.6 -> 192.168.100.28 DNS         7
64.15.251.198 -> 192.168.100.28 ICMP        6
192.33.14.30 -> 192.168.100.28 DNS          6
192.168.100.28 -> 213.61.6.2 ICMP           6
192.168.100.28 -> 192.33.14.30 DNS          6
192.168.100.28 -> 64.14.117.10 ICMP         6
62.101.108.86 -> 192.168.100.28 ICMP        6
192.168.100.28 -> 64.15.251.198 ICMP        6
63.218.7.130 -> 192.168.100.28 ICMP         6
192.168.100.28 -> 168.95.1.14 DNS           6
```

```
192.168.100.28 -> 208.185.54.14 ICMP        6
192.168.100.28 -> 63.218.7.130 ICMP         6
204.176.88.5 -> 192.168.100.28 ICMP         6
192.54.112.30 -> 192.168.100.28 DNS         6
212.62.17.145 -> 192.168.100.28 ICMP        6
192.168.100.28 -> 204.176.88.5 ICMP         6
213.61.6.2 -> 192.168.100.28 ICMP           6
192.168.100.28 -> 212.62.17.145 ICMP        6
192.168.100.28 -> 192.54.112.30 DNS         6
208.185.54.14 -> 192.168.100.28 ICMP        6
168.95.1.14 -> 192.168.100.28 DNS           6
64.14.117.10 -> 192.168.100.28 ICMP         6
192.168.100.28 -> 132.248.253.1 DNS         6
192.168.100.28 -> 206.252.192.5 DNS         5
192.168.100.28 -> 192.52.178.30 DNS         5
192.168.100.28 -> 192.12.94.32 DNS          5
203.255.234.103 -> 192.168.100.28 DNS        5
192.168.100.28 -> 216.73.82.10 ICMP         5
192.12.94.32 -> 192.168.100.28 DNS          5
206.252.192.5 -> 192.168.100.28 DNS         5
192.52.178.30 -> 192.168.100.28 DNS         5
192.168.100.28 -> 163.162.170.173 ICMP        5
12.122.9.157 -> 192.168.100.28 ICMP         5
192.168.100.28 -> 66.28.255.130 ICMP        5
66.28.255.130 -> 192.168.100.28 ICMP        5
192.114.144.52 -> 192.168.100.28 ICMP        5
192.168.100.28 -> 203.255.234.103 DNS        5
216.73.82.10 -> 192.168.100.28 ICMP         5
192.168.100.28 -> 198.41.0.4 DNS            4
200.23.1.1 -> 192.168.100.28 DNS            4
198.41.0.4 -> 192.168.100.28 DNS            4
192.168.100.28 -> 166.130.113.157 TCP        4
151.99.125.138 -> 192.168.100.28 DNS        4
164.124.101.31 -> 192.168.100.28 DNS        4
192.168.100.28 -> 151.99.125.138 DNS        4
192.115.106.10 -> 192.168.100.28 DNS        4
192.168.100.28 -> 192.115.106.10 DNS        4
192.168.100.28 -> 192.115.106.11 DNS        4
192.115.106.11 -> 192.168.100.28 DNS        4
192.168.100.28 -> 200.23.1.1 DNS            4
192.168.100.28 -> 164.124.101.31 DNS        4
192.168.100.28 -> 140.135.18.15 DNS         4
192.168.100.28 -> 192.168.100.71 DNS        4
166.130.113.157 -> 192.168.100.28 TCP        4
140.111.1.2 -> 192.168.100.28 DNS           4
192.168.100.71 -> 192.168.100.28 DNS        4
64.14.76.206 -> 192.168.100.28 DNS          3
192.168.100.28 -> 131.154.1.3 DNS           3
192.168.100.28 -> 192.12.94.30 DNS          3
192.168.100.28 -> 195.130.233.20 RX         3
192.168.100.28 -> 204.70.57.242 DNS         3
192.168.100.28 -> 151.99.125.2 DNS          3
192.168.100.28 -> 151.164.1.1 DNS           3
200.23.242.201 -> 192.168.100.28 DNS        3
192.168.100.28 -> 128.9.0.107 DNS           3
192.12.94.30 -> 192.168.100.28 DNS          3
66.135.207.138 -> 192.168.100.28 DNS        3
```

```
192.168.100.28 -> 66.135.207.138 DNS        3
192.168.100.28 -> 200.23.242.201 DNS        3
128.8.10.90 -> 192.168.100.28 DNS           3
62.211.66.55 -> 192.168.100.28 TCP          3
131.154.1.3 -> 192.168.100.28 DNS           3
151.164.1.7 -> 192.168.100.28 DNS           3
12.122.9.158 -> 192.168.100.28 ICMP         3
192.168.100.28 -> 192.55.83.30 DNS          3
209.132.221.43 -> 192.168.100.28 DNS        3
128.9.0.107 -> 192.168.100.28 DNS           3
192.55.83.30 -> 192.168.100.28 DNS          3
151.99.125.2 -> 192.168.100.28 DNS          3
192.168.100.28 -> 209.132.221.43 DNS        3
192.168.100.28 -> 151.164.1.7 DNS           3
192.168.100.28 -> 128.8.10.90 DNS           3
148.244.249.75 -> 192.168.100.28 DNS        3
151.164.1.1 -> 192.168.100.28 DNS           3
192.168.100.28 -> 148.244.249.75 DNS        3
204.70.57.242 -> 192.168.100.28 DNS         3
192.168.100.28 -> 64.14.76.206 DNS          3
140.135.18.15 -> 192.168.100.28 DNS         3
192.168.100.28 -> 151.99.250.2 DNS          2
192.168.100.28 -> 211.216.50.160 DNS        2
192.149.252.22 -> 192.168.100.28 DNS        2
192.168.100.28 -> 198.32.64.12 DNS          2
192.168.100.28 -> 193.205.245.8 DNS         2
192.168.100.197 -> 192.168.100.28 DNS        2
192.168.100.28 -> 192.36.148.17 DNS         2
192.168.100.164 -> 192.168.100.28 DNS        2
192.168.100.28 -> 207.82.198.150 DNS        2
192.168.100.28 -> 216.32.120.21 DNS         2
209.10.66.55 -> 192.168.100.28 DNS          2
192.168.100.28 -> 192.149.252.22 DNS        2
192.168.100.28 -> 64.15.251.221 DNS         2
192.220.125.10 -> 192.168.100.28 DNS        2
192.168.100.28 -> 192.5.6.32 DNS            2
168.95.192.2 -> 192.168.100.28 DNS          2
fe80::c0a8:641c -> ff02::1:fff8:e01c ICMPv6        2
192.168.100.28 -> 148.244.153.69 DNS        2
193.205.245.8 -> 192.168.100.28 DNS         2
192.168.100.28 -> 140.111.1.2 DNS           2
192.168.100.28 -> 192.220.125.10 DNS        2
64.28.86.226 -> 192.168.100.28 ICMP         2
151.92.2.34 -> 192.168.100.28 DNS           2
63.215.198.78 -> 192.168.100.28 DNS         2
198.32.64.12 -> 192.168.100.28 DNS          2
151.99.250.2 -> 192.168.100.28 DNS          2
192.168.100.28 -> 192.168.100.197 DNS        2
192.168.100.28 -> 66.28.47.162 ICMP         2
fe80::206:5bff:fe04:5e95 -> ff02::1:ff00:5d0f ICMPv6        2
194.25.2.130 -> 192.168.100.28 DNS          2
211.216.50.130 -> 192.168.100.28 DNS        2
192.168.100.28 -> 192.168.100.164 DNS        2
192.168.100.28 -> 194.25.2.130 DNS          2
209.10.34.55 -> 192.168.100.28 DNS          2
216.239.36.10 -> 192.168.100.28 DNS         2
192.168.100.28 -> 203.73.24.8 DNS           2
```

```
192.168.100.28 -> 64.14.117.6 DNS           2
192.168.100.28 -> 202.12.29.60 DNS          2
202.12.27.33 -> 192.168.100.28 DNS          2
192.168.100.28 -> 63.215.198.78 DNS         2
203.73.24.8 -> 192.168.100.28 DNS           2
200.33.148.201 -> 192.168.100.28 DNS        2
192.168.100.28 -> 62.101.108.86 ICMP        2
203.37.255.97 -> 192.168.100.28 DNS         2
193.0.14.129 -> 192.168.100.28 DNS          2
64.14.117.6 -> 192.168.100.28 DNS           2
203.133.1.8 -> 192.168.100.28 DNS           2
200.33.146.201 -> 192.168.100.28 DNS        2
192.168.100.28 -> 203.248.240.141 DNS        2
64.15.251.221 -> 192.168.100.28 DNS         2
192.168.100.28 -> 64.37.246.2 ICMP          2
202.12.29.60 -> 192.168.100.28 DNS          2
192.168.100.28 -> 217.42.126.229 TCP        2
203.248.240.141 -> 192.168.100.28 DNS        2
192.168.100.28 -> 203.37.255.97 DNS         2
192.168.100.28 -> 209.10.34.55 DNS          2
207.82.198.150 -> 192.168.100.28 DNS        2
192.168.100.28 -> 211.216.50.130 DNS        2
192.168.100.28 -> 193.0.14.129 DNS          2
192.168.100.28 -> 202.12.27.33 DNS          2
192.168.100.28 -> 192.33.4.12 DNS           2
66.28.47.162 -> 192.168.100.28 ICMP         2
192.168.100.28 -> 216.239.36.10 DNS         2
192.36.125.2 -> 192.168.100.28 DNS          2
192.5.6.32 -> 192.168.100.28 DNS            2
192.168.100.28 -> 198.41.3.39 DNS           2
148.244.153.69 -> 192.168.100.28 DNS        2
129.70.132.100 -> 192.168.100.28 DNS        2
192.168.100.28 -> 192.36.125.2 DNS          2
192.168.100.28 -> 65.203.232.2 ICMP         2
66.28.34.130 -> 192.168.100.28 ICMP         2
192.168.100.28 -> 200.33.148.201 DNS        2
192.33.4.12 -> 192.168.100.28 DNS           2
192.168.100.28 -> 209.10.66.55 DNS          2
192.5.5.241 -> 192.168.100.28 DNS           2
192.168.100.28 -> 151.92.2.34 DNS           2
192.168.100.28 -> 129.70.132.100 DNS        2
64.37.246.2 -> 192.168.100.28 ICMP          2
217.42.126.229 -> 192.168.100.28 TCP        2
fe80::c0a8:641c -> ff02::1:ff00:5d0e ICMPv6         2
192.168.100.28 -> 66.28.34.130 ICMP         2
192.168.100.28 -> 62.211.66.55 HTTP         2
211.216.50.160 -> 192.168.100.28 DNS        2
65.203.232.2 -> 192.168.100.28 ICMP         2
192.168.100.28 -> 203.133.1.8 DNS           2
216.32.120.21 -> 192.168.100.28 DNS         2
198.41.3.39 -> 192.168.100.28 DNS           2
192.168.100.28 -> 200.33.146.201 DNS        2
192.168.100.28 -> 64.28.86.226 ICMP         2
192.33.14.32 -> 192.168.100.28 DNS          2
192.168.100.28 -> 192.33.14.32 DNS          2
192.168.100.28 -> 168.95.192.2 DNS          2
192.168.100.28 -> 192.5.5.241 DNS           2
```

```
192.168.100.28 -> 203.50.0.137 DNS          1
143.248.1.177 -> 192.168.100.28 DNS         1
200.34.163.34 -> 192.168.100.28 DNS         1
192.168.100.28 -> 208.129.201.10 DNS        1
192.168.100.28 -> 216.130.214.82 DNS        1
192.168.100.28 -> 203.197.173.129 ICMP        1
192.168.100.28 -> 193.214.57.194 ICMP       1
192.168.100.28 -> 192.31.80.34 DNS          1
192.168.100.28 -> 64.226.28.33 DNS          1
216.239.32.10 -> 192.168.100.28 DNS         1
192.168.100.28 -> 65.206.228.70 DNS         1
192.168.100.28 -> 195.130.233.20 SRVLOC        1
192.168.100.28 -> 213.61.5.28 DNS           1
202.160.241.130 -> 192.168.100.28 ICMP        1
193.205.245.66 -> 192.168.100.28 DNS        1
64.226.28.33 -> 192.168.100.28 DNS          1
209.225.31.197 -> 192.168.100.28 DNS        1
192.168.100.28 -> 205.158.108.194 ICMP        1
192.168.100.28 -> 195.130.233.20 SliMP3        1
192.168.100.28 -> 66.28.255.153 DNS         1
192.168.100.28 -> 209.185.188.14 DNS        1
198.5.148.6 -> 192.168.100.28 ICMP          1
205.158.108.194 -> 192.168.100.28 ICMP        1
209.185.188.14 -> 192.168.100.28 DNS        1
192.168.100.28 -> 199.191.128.105 DNS       1
192.168.100.28 -> 193.205.245.66 DNS        1
192.168.100.28 -> 64.154.81.20 DNS          1
216.21.234.73 -> 192.168.100.28 DNS         1
192.168.100.28 -> 202.160.241.130 ICMP        1
192.168.100.28 -> 192.76.144.16 DNS         1
207.46.245.230 -> 192.168.100.28 DNS        1
192.168.100.28 -> 216.151.111.83 ICMP       1
192.76.144.16 -> 192.168.100.28 DNS         1
65.206.228.71 -> 192.168.100.28 DNS         1
192.168.100.28 -> 204.70.128.1 DNS          1
194.25.2.132 -> 192.168.100.28 DNS          1
195.129.12.74 -> 192.168.100.28 DNS         1
192.168.100.28 -> 139.130.4.5 DNS           1
192.168.100.28 -> 211.14.0.99 ICMP          1
207.248.240.42 -> 192.168.100.28 DNS        1
192.168.100.28 -> 204.74.101.1 DNS          1
216.32.126.150 -> 192.168.100.28 DNS        1
00000000.0000 -> 00000000.0000 Vines        1
192.168.100.28 -> 152.163.209.129 DNS       1
209.73.164.76 -> 192.168.100.28 DNS         1
208.172.128.158 -> 192.168.100.28 DNS       1
192.168.100.28 -> 192.203.230.10 DNS        1
192.168.100.28 -> 198.6.1.83 DNS            1
192.168.100.28 -> 192.106.1.31 DNS          1
63.211.121.147 -> 192.168.100.28 DNS        1
192.168.100.28 -> 202.175.245.2 ICMP        1
192.168.100.28 -> 216.148.227.68 DNS        1
192.168.100.28 -> 61.221.179.26 TCP         1
64.12.51.132 -> 192.168.100.28 DNS          1
192.168.100.28 -> 65.206.228.71 DNS         1
192.168.100.28 -> 203.133.1.6 DNS           1
192.168.100.28 -> 192.168.100.198 DNS       1
```

```
192.168.100.28 -> 200.34.163.34 DNS         1
204.176.88.1 -> 192.168.100.28 DNS          1
192.168.100.28 -> 194.25.0.125 DNS          1
204.70.49.234 -> 192.168.100.28 DNS         1
192.168.100.28 -> 206.228.179.10 DNS        1
199.2.117.66 -> 192.168.100.28 DNS          1
192.168.100.28 -> 216.239.32.10 DNS         1
192.168.100.28 -> 213.157.130.12 TCP        1
192.168.100.28 -> 199.2.117.66 DNS          1
192.168.100.28 -> 200.160.0.5 DNS           1
192.168.100.28 -> 212.62.17.141 DNS         1
192.168.100.28 -> 64.12.51.132 DNS          1
207.46.72.123 -> 192.168.100.28 DNS         1
192.168.100.28 -> 63.210.142.26 DNS         1
63.218.7.158 -> 192.168.100.28 DNS          1
192.168.100.28 -> 63.211.121.147 DNS        1
192.168.100.28 -> 216.74.57.197 DNS         1
192.168.100.28 -> 209.104.33.252 DNS        1
152.163.209.129 -> 192.168.100.28 DNS        1
199.191.128.105 -> 192.168.100.28 DNS        1
192.168.100.28 -> 209.73.164.76 DNS         1
212.111.32.38 -> 192.168.100.28 DNS         1
198.6.1.83 -> 192.168.100.28 DNS            1
65.206.228.70 -> 192.168.100.28 DNS         1
192.168.100.28 -> 195.130.233.20 MGCP        1
62.4.74.66 -> 192.168.100.28 ICMP           1
64.35.7.130 -> 192.168.100.28 ICMP          1
192.168.100.28 -> 216.32.126.150 DNS        1
147.28.0.39 -> 192.168.100.28 DNS           1
192.168.100.28 -> 206.25.8.69 DNS           1
213.61.5.28 -> 192.168.100.28 DNS           1
192.18.99.5 -> 192.168.100.28 DNS           1
209.104.33.252 -> 192.168.100.28 DNS        1
192.168.100.28 -> 217.29.76.4 DNS           1
134.75.30.1 -> 192.168.100.28 DNS           1
192.168.100.28 -> 193.108.91.42 DNS         1
fe80::206:5bff:fe04:5e95 -> ff02::1:ff04:5e95 ICMPv6        1
216.74.57.197 -> 192.168.100.28 DNS         1
192.168.100.28 -> 66.7.130.1 DNS            1
192.168.100.28 -> 217.5.100.186 DNS         1
192.168.100.28 -> 216.21.234.73 DNS         1
206.228.179.10 -> 192.168.100.28 DNS        1
203.133.1.6 -> 192.168.100.28 DNS           1
192.168.100.28 -> 217.116.224.1 DNS         1
192.168.100.28 -> 212.31.251.66 ICMP        1
203.50.5.200 -> 192.168.100.28 DNS          1
192.168.100.28 -> 143.248.1.177 DNS         1
218.90.41.105 -> 192.168.100.28 NBNS        1
193.214.57.194 -> 192.168.100.28 ICMP        1
212.31.251.66 -> 192.168.100.28 ICMP        1
168.95.192.1 -> 192.168.100.28 DNS          1
64.154.81.20 -> 192.168.100.28 DNS          1
192.168.100.28 -> 62.4.74.66 ICMP           1
192.168.100.28 -> 195.130.233.20 DDTP        1
192.168.100.28 -> 209.73.176.204 DNS        1
192.168.100.28 -> 202.30.50.50 DNS          1
206.25.8.69 -> 192.168.100.28 DNS           1
```

```
200.160.0.5 -> 192.168.100.28 DNS          1
192.168.100.28 -> 65.54.248.222 DNS        1
211.14.0.99 -> 192.168.100.28 ICMP         1
213.200.82.49 -> 192.168.100.28 ICMP       1
192.36.148.17 -> 192.168.100.28 DNS        1
129.70.4.55 -> 192.168.100.28 DNS          1
208.211.225.10 -> 192.168.100.28 DNS       1
202.175.245.2 -> 192.168.100.28 NBNS       1
192.168.100.28 -> 204.253.104.10 DNS       1
61.221.179.26 -> 192.168.100.28 TCP        1
12.122.12.58 -> 192.168.100.28 ICMP        1
206.79.230.10 -> 192.168.100.28 DNS        1
63.210.142.65 -> 192.168.100.28 DNS        1
192.168.100.28 -> 213.41.76.66 ICMP        1
204.71.116.25 -> 192.168.100.28 DNS        1
192.168.100.28 -> 129.70.4.55 DNS          1
192.168.100.28 -> 216.231.111.14 DNS       1
192.168.100.28 -> 208.211.225.10 DNS       1
192.168.100.28 -> 195.130.233.20 NBNS       1
194.25.0.125 -> 192.168.100.28 DNS         1
139.130.4.5 -> 192.168.100.28 DNS          1
209.21.0.72 -> 192.168.100.28 DNS          1
192.168.100.28 -> 195.130.233.20 RADIUS       1
192.168.100.28 -> 194.25.2.132 DNS         1
64.70.38.180 -> 192.168.100.28 DNS         1
216.130.214.82 -> 192.168.100.28 DNS       1
:: -> ff02::1:ff00:5d0f ICMPv6             1
207.68.128.151 -> 192.168.100.28 DNS       1
192.168.100.28 -> 202.12.29.25 DNS         1
216.151.111.83 -> 192.168.100.28 ICMP       1
192.168.100.28 -> 203.50.5.200 DNS         1
192.168.100.28 -> 198.5.148.6 ICMP         1
192.168.100.28 -> 192.9.9.3 DNS            1
192.168.100.28 -> 208.254.75.130 ICMP       1
209.73.176.204 -> 192.168.100.28 DNS       1
65.54.248.222 -> 192.168.100.28 DNS        1
192.168.100.28 -> 64.35.7.130 ICMP         1
192.168.100.28 -> 204.70.49.234 DNS        1
192.168.100.28 -> 192.18.99.5 DNS          1
206.65.183.70 -> 192.168.100.28 DNS        1
216.231.111.14 -> 192.168.100.28 DNS       1
66.7.130.1 -> 192.168.100.28 DNS           1
192.168.100.28 -> 208.185.54.23 DNS        1
192.168.100.28 -> 207.248.240.42 DNS       1
192.168.100.28 -> 212.111.32.38 DNS        1
192.168.100.28 -> 64.154.80.20 DNS         1
192.168.100.28 -> 204.71.116.25 DNS        1
192.168.100.28 -> 147.28.0.39 DNS          1
213.199.1.132 -> 192.168.100.28 DNS        1
209.132.221.44 -> 192.168.100.28 DNS       1
192.168.100.28 -> 206.79.230.10 DNS        1
204.70.128.1 -> 192.168.100.28 DNS         1
192.168.100.28 -> 63.210.142.65 DNS        1
192.168.100.28 -> 206.65.183.70 DNS        1
192.168.100.28 -> 213.199.1.132 DNS        1
204.253.104.10 -> 192.168.100.28 DNS       1
151.92.2.35 -> 192.168.100.28 DNS          1
```

```
192.168.100.28 -> 207.68.128.151 DNS        1
192.168.100.28 -> 63.218.7.158 DNS          1
208.254.75.130 -> 192.168.100.28 ICMP        1
195.130.233.20 -> 192.168.100.28 UDP        1
192.168.100.28 -> 207.46.72.123 DNS         1
217.5.100.186 -> 192.168.100.28 DNS         1
192.168.100.28 -> 209.132.221.44 DNS        1
192.168.100.28 -> 218.90.41.105 ICMP        1
204.74.101.1 -> 192.168.100.28 DNS          1
64.0.96.22 -> 192.168.100.28 DNS            1
192.168.100.28 -> 195.130.233.20 AODV6        1
217.116.224.1 -> 192.168.100.28 DNS         1
212.62.17.141 -> 192.168.100.28 DNS         1
192.168.100.28 -> 207.46.245.230 DNS        1
213.157.130.12 -> 192.168.100.28 TCP        1
192.168.100.28 -> 168.95.192.1 DNS          1
208.129.201.10 -> 192.168.100.28 DNS        1
192.168.100.28 -> 195.129.12.74 DNS         1
fe80::206:5bff:fe04:5e95 -> ff02::2:d64f:8980 ICMPv6        1
192.168.100.28 -> 134.75.30.1 DNS           1
202.12.29.25 -> 192.168.100.28 DNS          1
66.28.255.153 -> 192.168.100.28 DNS         1
217.29.76.4 -> 192.168.100.28 DNS           1
64.154.80.20 -> 192.168.100.28 DNS          1
203.50.0.137 -> 192.168.100.28 DNS          1
216.148.227.68 -> 192.168.100.28 DNS        1
192.168.100.28 -> 204.176.88.1 DNS          1
192.168.100.28 -> 208.172.128.158 DNS        1
192.168.100.28 -> 209.225.31.197 DNS        1
216.73.84.10 -> 192.168.100.28 ICMP         1
192.31.80.34 -> 192.168.100.28 DNS          1
192.106.1.31 -> 192.168.100.28 DNS          1
192.168.100.28 -> 216.73.84.10 ICMP         1
192.168.100.28 -> 64.0.96.22 DNS            1
203.197.173.129 -> 192.168.100.28 ICMP        1
192.168.100.28 -> 151.92.2.35 DNS           1
208.185.54.23 -> 192.168.100.28 DNS         1
192.168.100.28 -> 64.70.38.180 DNS          1
192.168.100.198 -> 192.168.100.28 DNS        1
193.108.91.42 -> 192.168.100.28 DNS         1
213.41.76.66 -> 192.168.100.28 ICMP         1
192.203.230.10 -> 192.168.100.28 DNS        1
192.168.100.28 -> 195.130.233.20 DLSw        1
192.168.100.28 -> 209.21.0.72 DNS           1

Total:                                 123123
```

With this information I was now able to focus on just a few specific machines. I decided to go back to Ethereal and begin to look for packets that corresponded with the information obtained from Snort. I then noticed the numerous DNS queries and few NBTSTAT queries. These packets were responded to with ICMP "destination unreachable" replies. These packets were followed by some interesting packets sent to port 1433 (ms-sql-s). These reports were responded to with a RST, ACK indicating that the victim did not have the particular port open. As I continued to scan down within Ethereal I noticed the next batch of packets being sent to port 6112. A google search of this port indicated that this port is used for 'dtpcd'. This information combined with the previously obtained about the possible victim's operating system proved to be quite interesting.

Now I moved back to the snort outputs to obtain the information about the "skillz" ICMP packets. This was quite easy since snort indicated that this was a DDOS Stacheldraht agent->handler.

I now attempted to determine the nationality of the attacker and used whois to provide me with the country of origin based upon the owner of the IP blocks.

Q1 Answer

What is the operating system of the honeypot? How did you determine that?

It appears that the honeypot is a Sun Solaris 5.8 system. This is based upon the ethereal analysis of the Source and Destination MAC addresses. This information was validated with the Passive Fingerprinting Default TTL values of both TCP and UDP packets. The TTL value displayed by Ethereal is 255 which correspond to a Solaris system below 7. Ethereal provided the final piece of information between frames 569 and 574 where the operating system is reported to the attacker from the victim as SunOS 5.8.

Q2 Answer

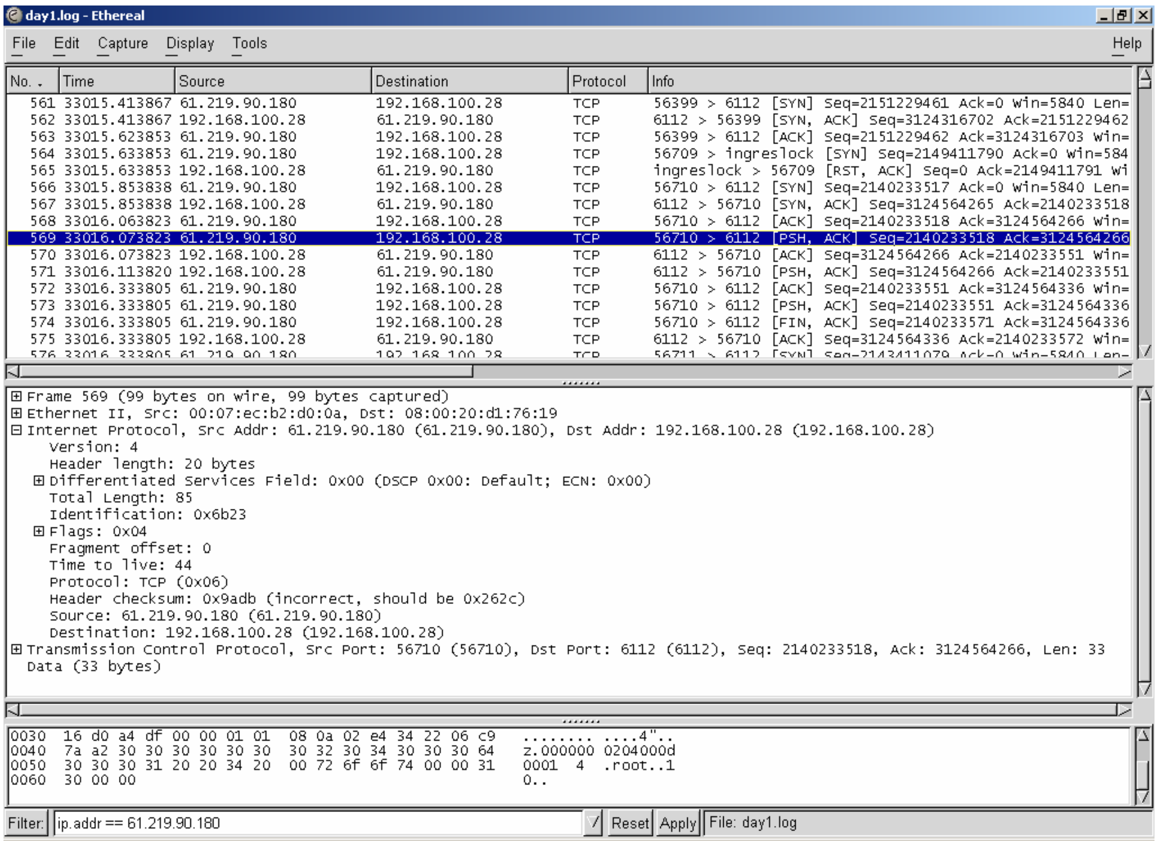
How did the attacker(s) break into the system?

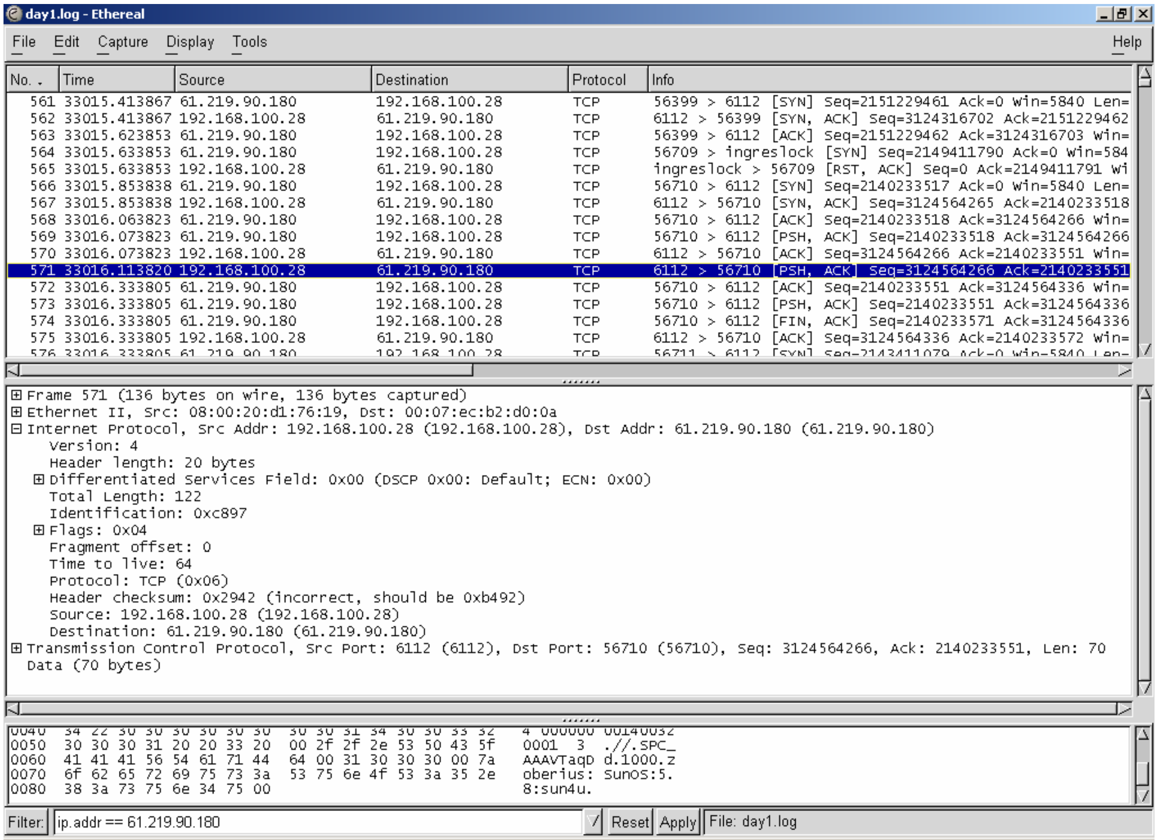
It appears that the attacker(s) gained access to the system using TCP a destination port 6112 which is used for 'dtspcd'. According to the CERT Vulnerability Note VU#172583 (http://www.kb.cert.org/vuls/id/172583) this could affect both SunOS 5.8, 5.8_x86 systems. A remotely exploitable buffer overflow exists in the Common Desktop Environment (CDE) Subprocess Control Service (dtspcd). An attacker who successfully exploits this vulnerability can execute arbitrary code as root.

Q3 Answer

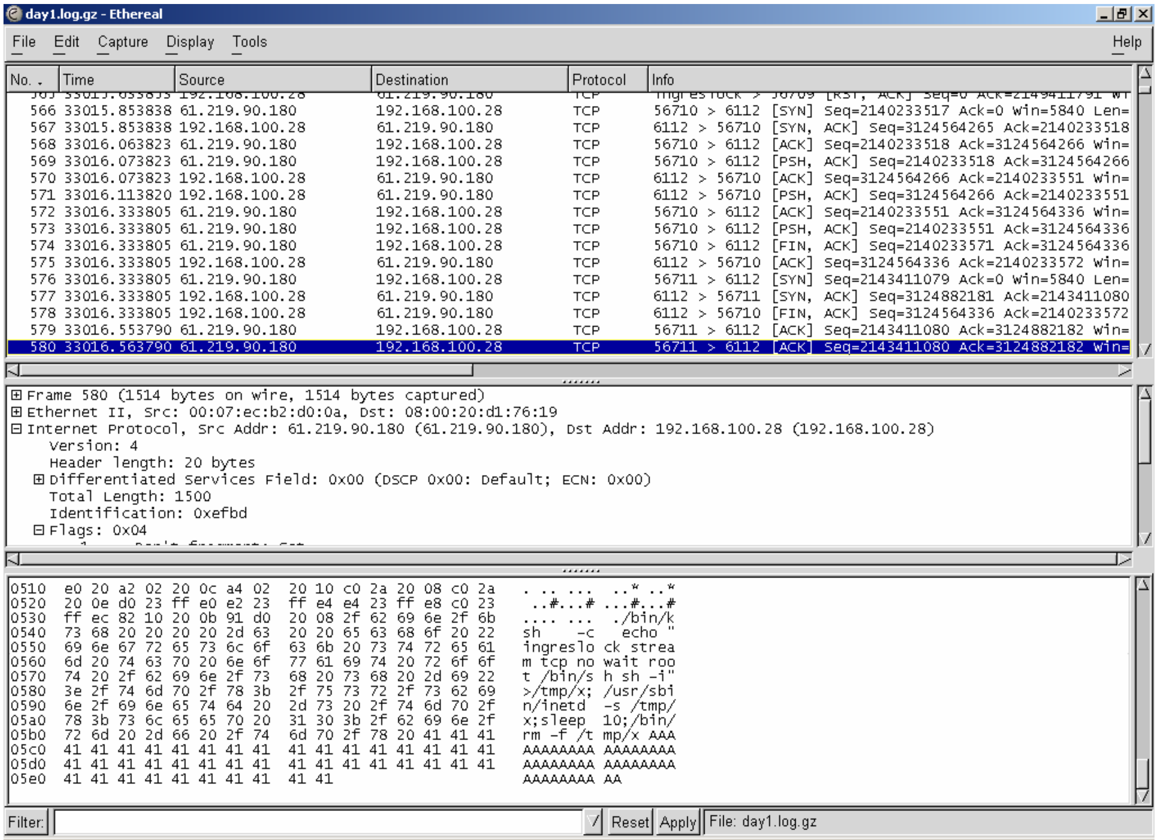
Which systems were used in this attack, and how?

61.219.90.180 – began the attack with SYN packet sent to destination port 6112. Once it received an SYN/ACK, it completed the three way handshake with an ACK. This system then attempted to access the victim via port 1524 (Ingreslock) which is probably an attempt to exploit a root shell exploit using Ingreslock. The system then went back to work on the original dtspcd exploit. As you can see with Frame 569 the attacker now has control of our victim. You can also see the operating system is SunOS 5.8





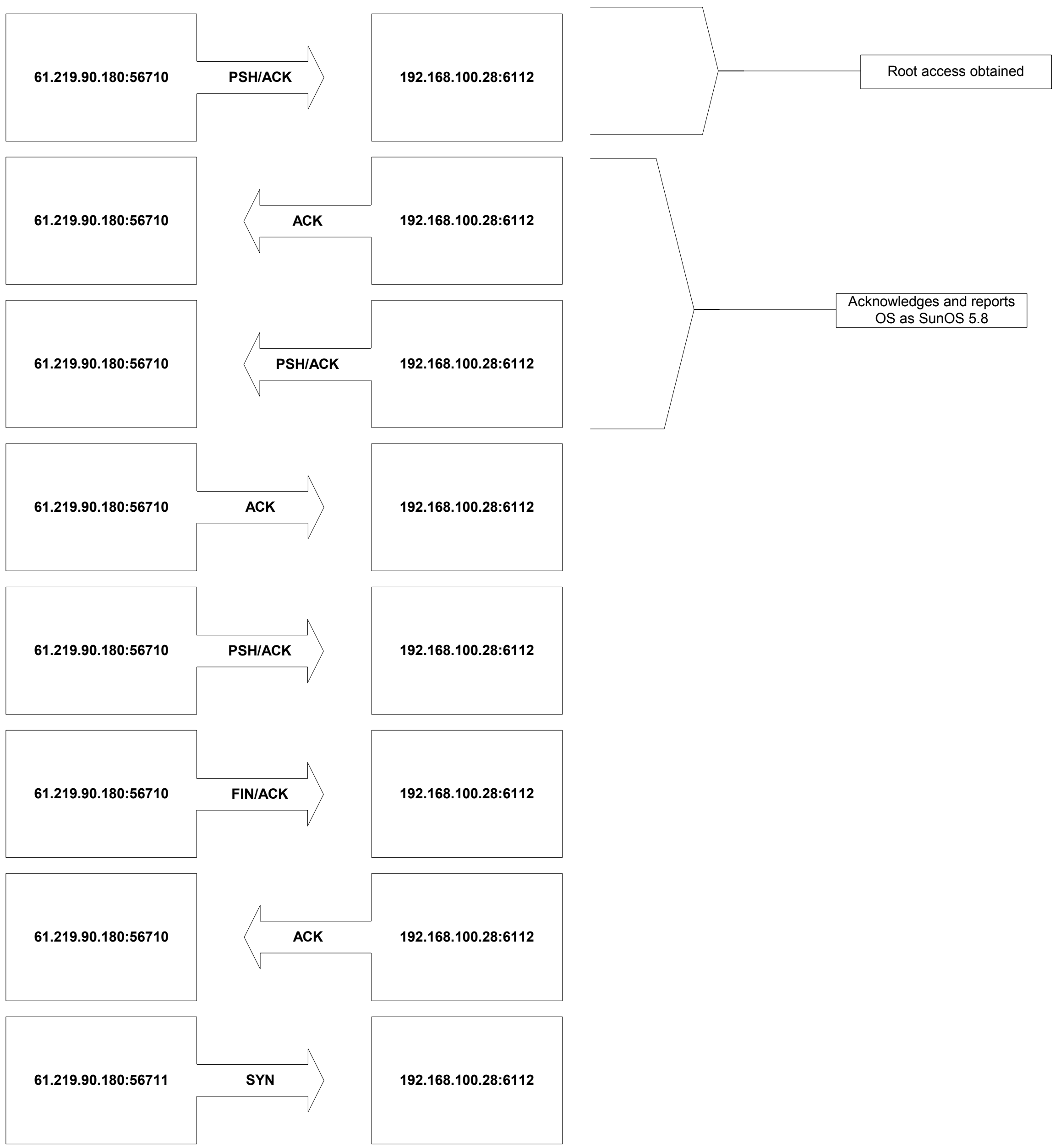
The attacker then added the Ingreslock entry to inetd with the newly acquired shell access.



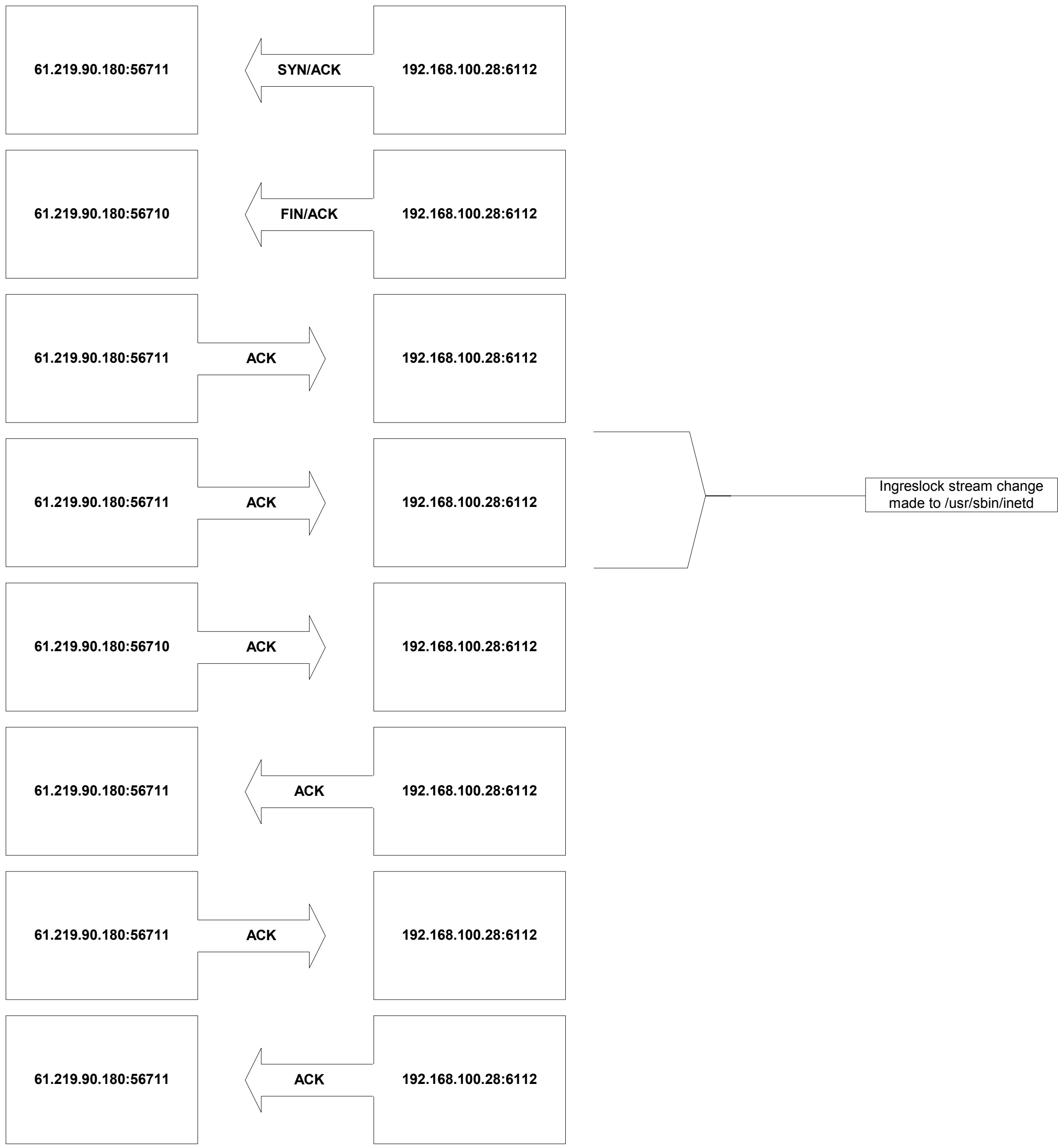
Q4 Answer

Create a diagram that demonstrates the sequences involved in the attack.


61.219.90.180:56399
SYN
192.168.100.28:6112
61.219.90.180:56399
SYN/ACK
192.168.100.28:6112
61.219.90.180:56399
ACK
192.168.100.28:6112
Initial three-way handshake via dtspcd (6112)
61.219.90.180:56709
ACK
192.168.100.28:1542
61.219.90.180:56709
RST/ACK
192.168.100.28:1542
Attempted Ingreslock (port 1542) access.
61.219.90.180:56710
SYN
192.168.100.28:6112
61.219.90.180:56710
SYN/ACK
192.168.100.28:6112
61.219.90.180:56710
ACK
192.168.100.28:6112
Three-way handshake via dtspcd (6112)



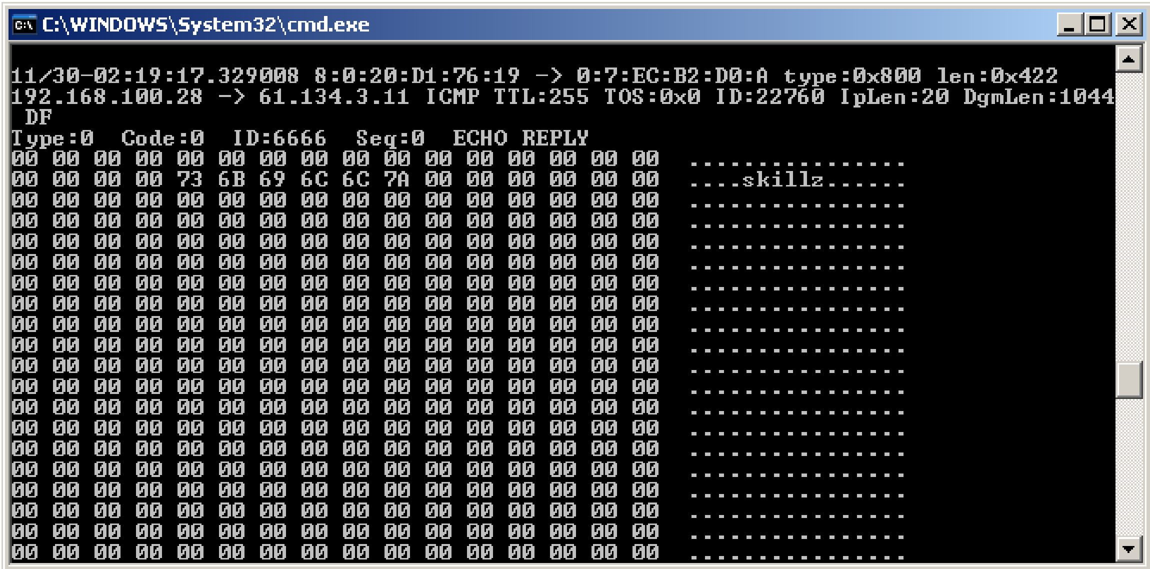
61.219.90.180:56710
PSH/ACK
192.168.100.28:6112
Root access obtained
61.219.90.180:56710
ACK
192.168.100.28:6112
Acknowledges and reports OS as SunOS 5.8
61.219.90.180:56710
PSH/ACK
192.168.100.28:6112
61.219.90.180:56710
ACK
192.168.100.28:6112
61.219.90.180:56710
PSH/ACK
192.168.100.28:6112
61.219.90.180:56710
FIN/ACK
192.168.100.28:6112
61.219.90.180:56710
ACK
192.168.100.28:6112
61.219.90.180:56711
SYN
192.168.100.28:6112



Q5 Answer

What is the purpose/reason of the ICMP packets with 'skillz' in them?

The ICMP packets with 'skillz' in them are an indication of a DDOS Stacheldraht agent->handler (skillz). Stacheldraht were originally found in binary form on a number of Solaris 2.x systems, which were identified as having been compromised by exploitation of buffer overrun bugs in the RPC services "statd", "cmsd" and "ttdbserverd".



```
C:\WINDOWS\System32\cmd.exe
11/30-02:19:17.329008 8:0:20:D1:76:19 -> 0:7:EC:B2:D0:A type:0x800 len:0x422
192.168.100.28 -> 61.134.3.11 ICMP TTL:255 TOS:0x0 ID:22760 IpLen:20 DgmLen:1044
 DF
Type:0  Code:0  ID:6666  Seq:0  ECHO REPLY
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 73 6B 69 6C 6C 7A 00 00 00 00 00 00  ....skillz......
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

Q6 Answer

Following the attack, the attacker(s) enabled a unique protocol that one would not expect to find on an IPv4 network. Can you identify that protocol and why it was used?

Gryphon Communication Protocol was found on day 3 at frame 1188. Dearborn Group's Gryphon product is a device that serves as a gateway between automotive / industrial automation networks and a TCP/IP network. Communication between Gryphon and a user's application takes place over a TCP/IP link. Applications may execute on remote networked nodes or on Gryphon itself. Communication between user applications (clients) and Gryphon (the server) is established via the Gryphon Communication Protocol (http://www.dgtech.com/gryphon/docs/html/GCprotocol/). This is obviously not normal for transmission on the internet. The reason appears to be to communicate with psyBNC 2.2.1 server. A bnc is short for a 'bouncer.' A bnc acts as a proxy for irc, allowing you to hide your real IP address and use a vhost. It was used to connect to other irc servers.

Q7 Answer

Can you identify the nationality of the attacker?

Whois reveals that the 61.216.0.0 - 61.219.255.255 IP address block assignments could indicate that the initial attack came from Taiwan.

Bonus Question Answer

What are the implications of using the unusual IP protocol to the Intrusion Detection industry?

The implications are that obviously the hackers are becoming more aware of unique protocols that exist and in fact choosing to use them as another means of hiding or obscuring there communications. It seems that since the industry is focused primarily on common protocols that perhaps unusual protocols will not be noticed. If you happen to have an IDS that uses canned rules and does not allow you to create your own that you are truly exposed and have no way of resolving the problem.

What tools exist that can decode this protocol?

Ethereal can decode DG Gryphon Protocol (gryphon)