Honeynet Challenge of the month scan 30

Submitted by

Sabyasachi Chakrabarty

Basudev Saha

basu_sachi@yahoo.com

The challenge

This month's challenge is different. Traditional SotM challenges have been about analyzing specific attacks against specific honeypots. This time we are going to take a step back and look at the bigger picture. Your job is to analyze a months worth of connection activity to and from a honeynet by analyzing the firewall logs.

a. Honeynet IPs sanitized to: 11.11.11.*
b. Our DNS server IPs sanitized to: 22.22.22.* and 23.23.23.*

Download the image

- **Download the image from project.honeypoy.net to local machine.**

```
  # wget  http://www.honeynet.org/scans/scan30/honeynet-Feb1_FebXX.log.gz
```

- **Verify the md5 checksum of downloaded file.**

```
# md5sum –c honeynet-Feb1_FebXX.log.gz e002b1013f18dd42e17be919c2870081
```

- **Unzip the downloaded file.**

```
  # gunzip honeynet-Feb1_FebXX.log.gz
```

- **Verify the md5 checksum of log file.**

```
# md5sum –c honeynet-Feb1_FebXX.log 8c0070ef51f6f764fde0551fa60da11b
```

Analysis

Example of a iptables/Netfilter log file :

```
Feb 1 00:00:02 bridge kernel: INBOUND TCP: IN=br0 PHYSIN=eth0 OUT=br0 PHYSOUT=eth1
SRC=192.150.249.87 DST=11.11.11.84 LEN=40 TOS=0x00 PREC=0x00 TTL=110 ID=12973
PROTO=TCP SPT=220 DPT=6129 WINDOW=16384 RES=0x00 SYN URGP=0
```

Fields in iptables / Netfilter log file:

Feb 1 00:00:02 bridge kernel:	syslog prefix.
INBOUND TCP:	user defined log prefix
IN=br0	Bridge Interface the packet was received from.
PHYSIN=eth0	Physical interface the packet was received from
OUT=br0	Bridge Interface the packet was sent to
PHYSOUT=eth1	Physical Interface the packet was sent to
MAC=	Destination MAC
SRC=192.150.249.87	Source IP address
DST=11.11.11.84	Destination IP address
LEN=40	Total length of IP packet in bytes
TOS=0x00	Type Of Service, "Type" field.
PREC=0x00	Type Of Service, "Precedence" field.
TTL=110	Remaining Time To Live is 110 hops.

ID=12973	Unique ID for this IP datagram, shared by all fragments if fragmented.
CE	Presumably the "ECN CE" flag (Congestion Experienced).
DF	"Don't Fragment" flag.
PROTO=TCP	Protocol name or number. TCP, UDP etc
SPT=220	Source port (TCP and UDP)
DPT=6129	Destination port (TCP and UDP)
SEQ	Receive Sequence number.
WINDOW=16384	The TCP Receive Window size.
RES=0x00	Reserved bits.
SYN	SYN flag, only exchanged at TCP connection establishment.
ACK	Acknowledgement flag.
PSH	Push flag.
RST	RST (Reset) flag.
FIN	FIN flag, only exchanged at TCP disconnection.
URGP=0	The Urgent Pointer allows for urgent, "out of band" data transfer

Fig: Format of iptables/Netfilter log format

Analyzing/Parsing/quering Netfilter logs:

Netfilter logs are intuitive, easy and provides a lot of information. However, there are several issues involving consistency, efficiency and parsing issues in the iptables/netfilter logs.

Simple extractor commands like the one below are defeated by the variable number of fields.

```
awk '/DPT=111 /{printf("%s %s\n", $10, $15)} logfile'
```

There are several log viewers and analyzers like Sawmill, fwanalog, adcfw-log etc. available for analyzing iptables log files. A SQL database can also be used to query the logs. We used a combination of several analyzers to arrive at the results.

Using adcfw-log:

```
grep 11.11.11.67 honeynet-Feb1_FebXX.log | adcfw-log -protocol ICMP
```

will extract all ICMP packets exchanged by the host 11.11.11.67

```
cat honeynet-Feb1_FebXX.log | adcfw-log -IN-interface eth1
```

will extract all packets on the In interface eth1

Using Sawmill:

Sawmill is a commercial log analyzer. Sawmill can analyze firewall, proxy, and cache log files. We have used Sawmill mainly for statistical analysis of the logs. It makes graphical representation of the data analysis.

Using SQL database (MySQL, MS SQL etc) :

This involves importing the log file (space delimited) to the database and querying it to select a particular set of records

e.g.- (we want to list all records containing source IP as 11.11.11.75 and destination IP as 81.53.86.15)

Select * from table_name where SourceIP like '%11.11.11.75' and DestIP like '%81.53.86.15%'

Using fwanalog

fwanalog also can be used for statistical analysis and it produces graphical representations.

There are many other log analyzers available, both freeware and commercial. Log analyzers like **psad, snortalog, trollhunter** are available which can even detect port scans/attacks from the iptables/netfilter logs.

Answers

1. What are the high-level trends in connectivity to/from the honeynet ? What was growing/decreasing? How does that match global statistics from DShield and other sources?

The high level trends in activity noticed in the Honeynet logs are as follows:

The activity noticed in the Honeynet was highest in the following ports, in descending order.

Destination Port	Packets	Explanation
135	88157	DCE Endpoint resolution
445	46439	Win 2K Server Message Block
443	26444	SSL
3127	25781	W32.MyDoom, W32.Novarg.A backdoor
53	18156	DNS
139	15000	NetBIOS Session, Windows File & Printer Sharing
80	13310	WWW
137	8752	NetBIOS Name Service
1434	5909	Microsoft-SQL-Server
138	3819	NetBIOS datagram

The following Honeynet servers received the highest traffic.

HONEYNET IP	Packets
11.11.11.75	30130
11.11.11.80	13255
11.11.11.67	12381
11.11.11.100	11417
11.11.11.90	11359
11.11.11.71	11062
11.11.11.87	10994
11.11.11.105	10915
11.11.11.115	10842
11.11.11.110	10839

Highest traffic originated from the following IP addresses.

Source IP	Packets	Packets (%)
11.11.11.67	22815	7.92%
66.60.166.84	21829	7.58%
66.186.83.178	10197	3.54%
63.13.135.27	8121	2.82%
127.0.0.1	6394	2.22%
63.123.70.166	4018	1.40%
63.125.10.7	3794	1.32%
63.126.133.117	2801	0.97%
67.123.234.132	2334	0.81%
63.126.133.8	2087	0.72%

The following were the changes in activity (growing/decreasing) during the observed period.

The traffic directed at ports 135 was constant throughout the observed period.

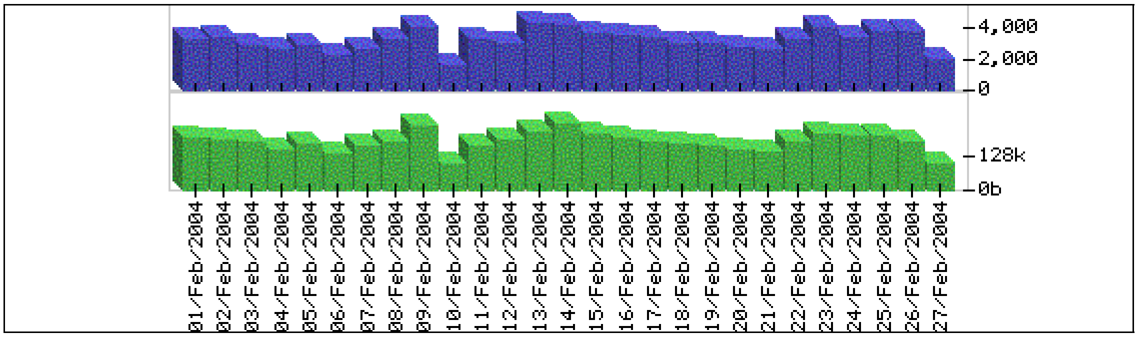


Fig: Destination Port 135

🟦 Packets 🟩 Bandwidth

There was a surge in traffic directed at ports 445 on Feb. 3, Feb. 4, Feb 11 and Feb. 26. During the rest of the observed time-period, the traffic was almost constant.

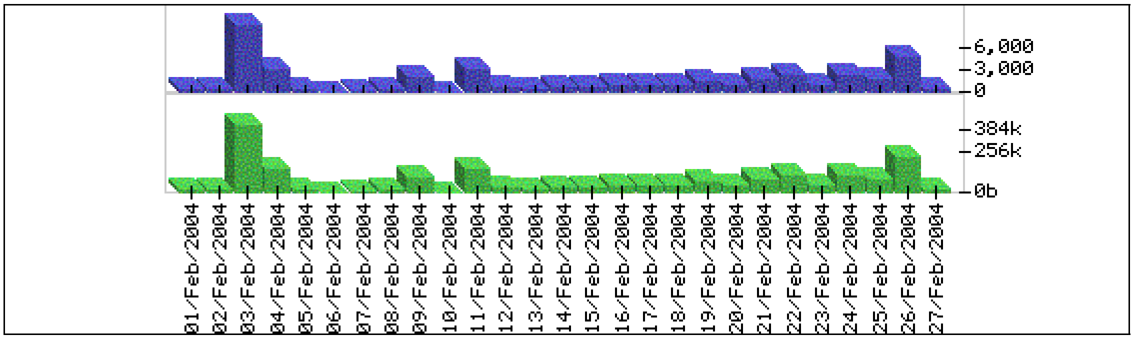


Fig: Destination Port 445 🟦 Packets 🟩 Bandwidth

There was a surge in traffic directed at ports 443 on Feb. 7 and Feb. 8,. During the rest of the observed time-period, there was very little traffic.

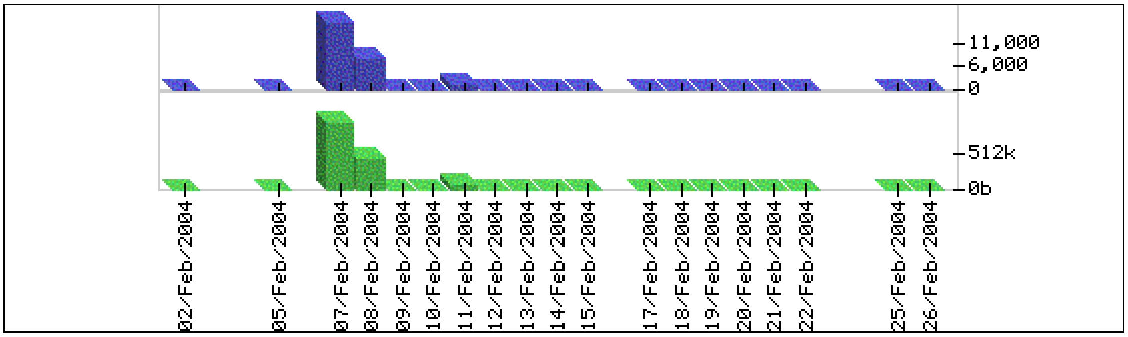


Fig: Destination Port 443 🟦 Packets 🟩 Bandwidth

The activity on port 3127 slowly picked up till it almost followed a constant level from around 09 Feb. There was a surge in traffic directed at ports 3127 on Feb. 21.

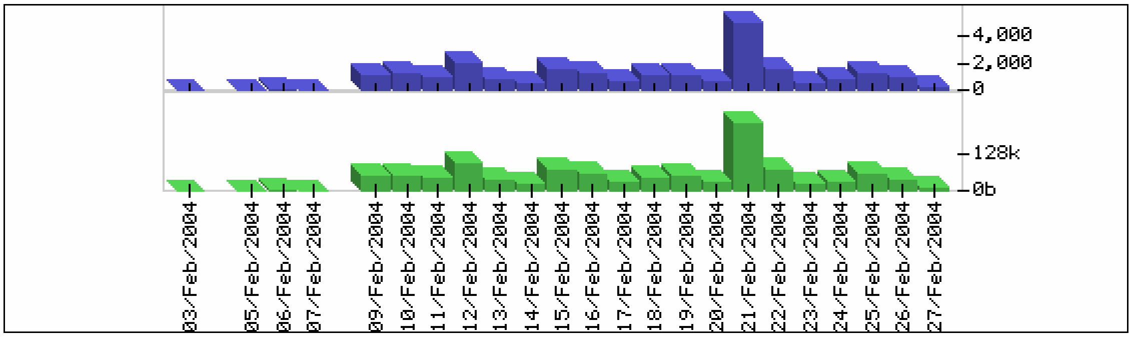
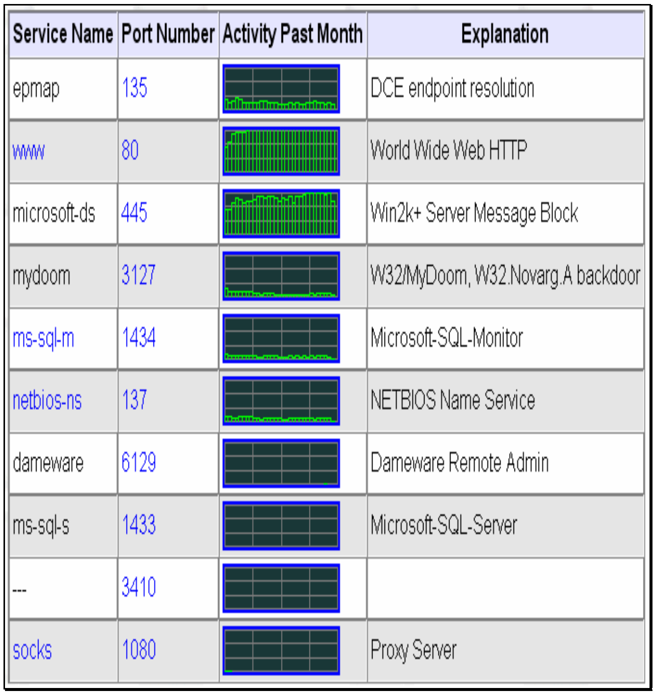
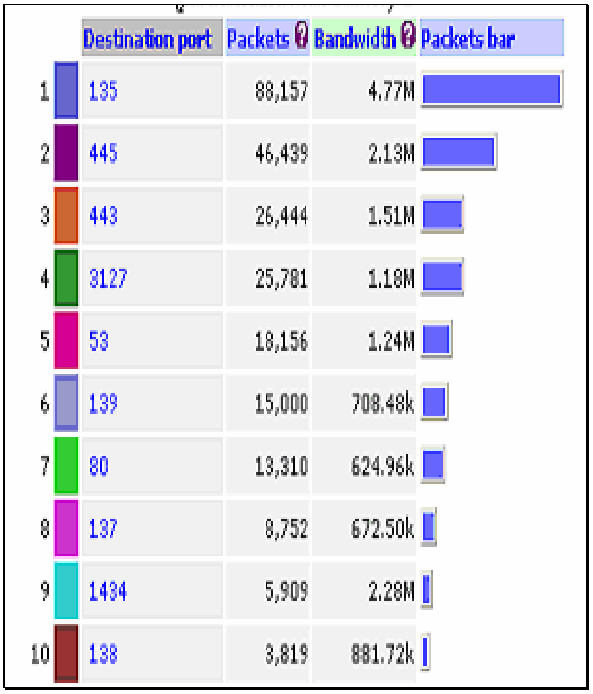


Fig: Destination Port 3127 🟦 Packets 🟩 Bandwidth

The trends of traffic are consistent with the traffic reports of global statistics at that time. A comparison is shown below between activity on D-shield and on the honeynet servers.



Service Name	Port Number	Activity Past Month	Explanation
epmap	135		DCE endpoint resolution
www	80		World Wide Web HTTP
microsoft-ds	445		Win2k+ Server Message Block
mydoom	3127		W32/MyDoom, W32.Novarg.A backdoor
ms-sql-m	1434		Microsoft-SQL-Monitor
netbios-ns	137		NETBIOS Name Service
dameware	6129		Dameware Remote Admin
ms-sql-s	1433		Microsoft-SQL-Server
---	3410		
socks	1080		Proxy Server



		Destination port	Packets	Bandwidth	Packets bar
1		135	88,157	4.77M	
2		445	46,439	2.13M	
3		443	26,444	1.51M	
4		3127	25,781	1.18M	
5		53	18,156	1.24M	
6		139	15,000	708.48k	
7		80	13,310	624.96k	
8		137	8,752	672.50k	
9		1434	5,909	2.28M	
10		138	3,819	881.72k	

DSHIELD **HONEYNET**

The most active port in both DShield and the honeynet logs was the same. It was port 135. This shows there was a great deal of similarity in the the traffic pattern.

While port 80 is in the second position in the DShield logs, it is seventh in the honeynet logs. The second highest active port on honeynet logs is port 445 which is third highest most active port on DShield.

Port 443 (SSL) occupies the third position in the honeynet logs and is entirely absent from DShield. The volume of activity of activity on port 443 is unusual. Besides more than 80% of SSL originated from a single IP address and on two days.

Interestingly, the 4th position in both DShield and honeynet logs is on port 3127. This resulted from the after effects of the MyDoom worm.

2. What possible evidence of Malware is there? What types? What are the Malware trends you can observe?

Possible evidence of Malware is seen from the lines of logs as given below.

Some logs indicate the possibility of the presence of Mydoom and MS Blaster worm in the Honeynet machines. **W32/MyDoom Virus** leaves a backdoor in an affected system. The backdoor works on TCP port 3128.

A Honeynet Machine **11.11.11.73** is found to be listening on port **3128,** This is a possible indication of infection by Mydoom virus.

```
Feb     24      15:22:05        bridge   kernel:  OUTG_CONN      TCP:     br0     eth1
        OUT=br0         =eth0   11.11.11.73      DST=218.18.131.79       LEN=552
        TOS=0x00        PREC=0x00       TTL=64  ID=28918        PROTO=TCP       SPT=3128
        DPT=24775       WINDOW=5840  RES=0x00         ACK     URGP=0


Feb     24      15:22:05        bridge   kernel:  OUTG_CONN      TCP:     br0     eth1
        OUT=br0         =eth0   11.11.11.73      DST=218.18.131.79       LEN=552
        TOS=0x00        PREC=0x00       TTL=64  ID=28918        PROTO=TCP       SPT=3128
        DPT=24775       WINDOW=5840  RES=0x00         ACK     URGP=0
```

Large number of packets as source ip 127.0.0.1 and source port 80

The traffic above was probably a result of the MsBlaster worm.

```
Feb     23      19:40:01        bridge   kernel:  INBOUND        TCP:     IN=br0  PHYSIN=eth0
        OUT=br0         PHYSOUT=eth1  SRC=127.0.0.1   DST=11.11.11.64         LEN=40
        TOS=0x00        PREC=0x00       TTL=119         ID=28945        PROTO=TCP
        SPT=80  DPT=1089        WINDOW=0      RES=0x00        ACK     RST     URGP=0
Feb     23      19:40:25        bridge   kernel:  INBOUND        TCP:     IN=br0  PHYSIN=eth0
        OUT=br0         PHYSOUT=eth1  SRC=127.0.0.1   DST=11.11.11.67         LEN=40
        TOS=0x00        PREC=0x00       TTL=119         ID=64330        PROTO=TCP
        SPT=80  DPT=1055        WINDOW=0      RES=0x00        ACK     RST     URGP=0
Feb     23      18:48:09        bridge   kernel:  INBOUND        TCP:     IN=br0  PHYSIN=eth0
        OUT=br0         PHYSOUT=eth1  SRC=127.0.0.1   DST=11.11.11.125        LEN=40
        TOS=0x00        PREC=0x00       TTL=119         ID=31298        PROTO=TCP
        SPT=80  DPT=1172        WINDOW=0      RES=0x00        ACK     RST     URGP=0
Feb     23      18:51:40        bridge   kernel:  INBOUND        TCP:     IN=br0  PHYSIN=eth0
        OUT=br0         PHYSOUT=eth1  SRC=127.0.0.1   DST=11.11.11.73         LEN=40
        TOS=0x00        PREC=0x00       TTL=119         ID=58641        PROTO=TCP
        SPT=80  DPT=1332        WINDOW=0      RES=0x00        ACK     RST     URGP=0
Feb     23      19:00:55        bridge   kernel:  INBOUND        TCP:     IN=br0  PHYSIN=eth0
        OUT=br0         PHYSOUT=eth1  SRC=127.0.0.1   DST=11.11.11.64         LEN=40
        TOS=0x00        PREC=0x00       TTL=119         ID=42071        PROTO=TCP
        SPT=80  DPT=1062        WINDOW=0      RES=0x00        ACK     RST     URGP=0
Feb     23      19:08:22        bridge   kernel:  INBOUND        TCP:     IN=br0  PHYSIN=eth0
        OUT=br0         PHYSOUT=eth1  SRC=127.0.0.1   DST=11.11.11.89         LEN=40
        TOS=0x00        PREC=0x00       TTL=119         ID=26523        PROTO=TCP
        SPT=80  DPT=1116        WINDOW=0      RES=0x00        ACK     RST     URGP=0
Feb     23      17:59:44        bridge   kernel:  INBOUND        TCP:     IN=br0  PHYSIN=eth0
        OUT=br0         PHYSOUT=eth1  SRC=127.0.0.1   DST=11.11.11.64         LEN=40
        TOS=0x00        PREC=0x00       TTL=119         ID=11056        PROTO=TCP
        SPT=80  DPT=1261        WINDOW=0        RES=0x00        ACK     RST     URGP=0
Feb     23      18:06:52        bridge  kernel: INBOUND         TCP:    IN=br0  PHYSIN=eth0
        OUT=br0         PHYSOUT=eth1    SRC=127.0.0.1   DST=11.11.11.90         LEN=40
        TOS=0x00        PREC=0x00       TTL=119         ID=13899        PROTO=TCP
        SPT=80  DPT=1215        WINDOW=0        RES=0x00        ACK     RST     URGP=0
```

Types of Malware

Malware traffic was noticed both from within the Honeynet and also to the Honeynet from outside. The attacks included the W32/Blaster worm which exploits the Micorsoft RPC DCOM vulnerability and works on port 135. This can also be co-related from the extract of the logs shown above and also from the huge amount of traffic on port 135, 139, 445. The other types of Malware included the MyDoom and its variants and the affects can be seen in the extract of codes above. Most of the other types of Malware noticed were scans from outside by other Malware for backdoors left behind.

Malware trends

A large scale scan on backdoor ports opened by recent Viruses/Worms/Trojans were observed. Lot of these scans are run by other Malware. (e.g. the DoomJuice scans for the backdoors left behind by Mydoom). The Malware identified included both mass mailing worm/virus (Mydoom) and other worms/virus like Blaster. Some of the trends of the malware observed are as below-

Mydoom 3127, 1080, (Mydoom.b, MyDoom.f – h), 3128 (Mydoom.b), 10080 (MyDoom.b)

```
Feb     27      10:53:06        bridge  kernel: INBOUND         TCP:    IN=br0  PHYSIN=eth0
        OUT=br0         PHYSOUT=eth1    SRC=24.44.129.105       DST=11.11.11.64
        LEN=48  TOS=0x00        PREC=0x00       TTL=111         ID=3105         DF
        PROTO=TCP       SPT=1362        DPT=3127        WINDOW=64240 RES=0x00           SYN
        URGP=0
```

Port 12345 NetBUS (Italk chat system also uses this port)

```
Feb     24      22:57:18        bridge  kernel: INBOUND         TCP:    IN=br0  PHYSIN=eth0
        OUT=br0         PHYSOUT=eth1    SRC=68.20.10.54         DST=11.11.11.72
        LEN=52  TOS=0x00        PREC=0x00       TTL=50  ID=33394        DF      PROTO=TCP
        SPT=1222        DPT=12345       WINDOW=60352 RES=0x00           SYN     URGP=0
```

Port 8866 Beagle.B (used by ultima online messenger)

```
Feb     18      22:00:19        bridge  kernel: INBOUND         TCP:    IN=br0  PHYSIN=eth0
        OUT=br0         PHYSOUT=eth1    SRC=149.159.54.170      DST=11.11.11.125
        LEN=48  TOS=0x00        PREC=0x00       TTL=114         ID=5815         DF
        PROTO=TCP       SPT=1522        DPT=8866        WINDOW=16384 RES=0x00           SYN
        URGP=0
```

Port 17300 Kuang2 (not registered port)

```
Feb     24      21:22:47        bridge  kernel: INBOUND         TCP:    IN=br0  PHYSIN=eth0
        OUT=br0         PHYSOUT=eth1    SRC=81.250.182.138      DST=11.11.11.75
        LEN=48  TOS=0x00        PREC=0x00       TTL=111         ID=41732        DF
        PROTO=TCP       SPT=1149        DPT=17300       WINDOW=16384 RES=0x00           SYN
        URGP=0
```

Port 27374 SubSeven (not registered port)

```
Feb     24      22:57:17        bridge   kernel:  INBOUND        TCP:     IN=br0  PHYSIN=eth0
        OUT=br0         PHYSOUT=eth1     SRC=68.20.10.54         DST=11.11.11.72
        LEN=52  TOS=0x00        PREC=0x00        TTL=50  ID=33392        DF       PROTO=TCP
        SPT=1221        DPT=27374        WINDOW=60352 RES=0x00           SYN      URGP=0
```

Port 31789 Hackatack UDP (windows remote administration)

```
Feb     18      04:18:17        bridge   kernel:  INBOUND        UDP:     br0     eth0
        OUT=br0         =eth1   80.109.15.181    DST=11.11.11.64          LEN=29  TOS=0x00
        PREC=0x00       TTL=108          ID=42686        PROTO=UDP        SPT=31790
        DPT=31789       LEN=9
```

Port 135 – MS Blaster worm

```
Feb     27      13:55:07        bridge   kernel:  INBOUND        TCP:     IN=br0  PHYSIN=eth0
        OUT=br0         PHYSOUT=eth1     SRC=83.33.180.234       DST=11.11.11.85
        LEN=48  TOS=0x00        PREC=0x00        TTL=113         ID=46797         DF
        PROTO=TCP       SPT=2340         DPT=135         WINDOW=65535 RES=0x00            SYN
        URGP=0
```

Port 445 DeLoder , mIRC

```
Feb     27      14:00:45        bridge   kernel:  INBOUND        TCP:     IN=br0  PHYSIN=eth0
        OUT=br0         PHYSOUT=eth1     SRC=68.148.254.54       DST=11.11.11.87
        LEN=48  TOS=0x00        PREC=0x00        TTL=116         ID=13734         DF
        PROTO=TCP       SPT=2741         DPT=445         WINDOW=16384 RES=0x00            SYN
        URGP=0
```

Port 443 Slapper worm

```
Feb     26      12:34:18        bridge   kernel:  INBOUND        TCP:     IN=br0  PHYSIN=eth0
        OUT=br0         PHYSOUT=eth1     SRC=212.202.235.4       DST=11.11.11.120         LEN=60
        TOS=0x00        PREC=0x00        TTL=47  ID=35030        DF       PROTO=TCP
        SPT=2866        DPT=443          WINDOW=32120 RES=0x00            SYN      URGP=0
```

3. What types of reconnaissance activity you notice? What do you think they were looking for? What are some of the notorious sources of such activity in the files?

A common network reconnaissance involves

- Finding machines that are up on the network
- Determining the ports that are open
- Determining network architecture
- Locating Firewall Misconfigurations
- DNS Zone transfer attemps

In the Honeynet logs the following reconnaissance activities were noticed

Ping sweep Attempt: Source IP 63.125.10.7

```
Feb     1       00:15:12        bridge  kernel: INBOUND         ICMP:   br0     eth0
        OUT=br0         =eth1   63.125.10.7     DST=11.11.11.64         LEN=92  TOS=0x00
        PREC=0x00       TTL=121         ID=61143        PROTO=ICMP      TYPE=8  CODE=0 ID=512

Feb     1       00:15:12        bridge  kernel: INBOUND         ICMP:   br0     eth0
        OUT=br0         =eth1   63.125.10.7     DST=11.11.11.67         LEN=92  TOS=0x00
        PREC=0x00       TTL=121         ID=61147        PROTO=ICMP      TYPE=8  CODE=0 ID=512

Feb     1       00:15:12        bridge  kernel: INBOUND         ICMP:   br0     eth0
        OUT=br0         =eth1   63.125.10.7     DST=11.11.11.69         LEN=92  TOS=0x00
        PREC=0x00       TTL=121         ID=61150        PROTO=ICMP      TYPE=8  CODE=0 ID=512

Feb     1       00:15:13        bridge  kernel: INBOUND         ICMP:   br0     eth0
        OUT=br0         =eth1   63.125.10.7     DST=11.11.11.70         LEN=92  TOS=0x00
        PREC=0x00       TTL=121         ID=61152        PROTO=ICMP      TYPE=8  CODE=0 ID=512
```

DNS Zone Transfer Attempt

```
Feb     18      13:21:55        bridge  kernel: INBOUND         TCP:    br0     eth0
        OUT=br0         =eth1   218.64.117.195  DST=11.11.11.69         LEN=64  TOS=0x00
        PREC=0x00       TTL=44  ID=7123         PROTO=TCP       SPT=3047        DPT=53
        WINDOW=34064 RES=0x00           SYN     URGP=0

Feb     18      13:21:56        bridge  kernel: INBOUND         TCP:    br0     eth0
        OUT=br0         =eth1   218.64.117.195  DST=11.11.11.70         LEN=64  TOS=0x00
        PREC=0x00       TTL=44  ID=7157         PROTO=TCP       SPT=3067        DPT=53
        WINDOW=34064 RES=0x00           SYN     URGP=0

Feb     18      13:21:57        bridge  kernel: INBOUND         TCP:    br0     eth0
        OUT=br0         =eth1   218.64.117.195  DST=11.11.11.71         LEN=64  TOS=0x00
        PREC=0x00       TTL=44  ID=7189         PROTO=TCP       SPT=3085        DPT=53
        WINDOW=34064 RES=0x00           SYN     URGP=0

Feb     18      13:21:38        bridge  kernel: INBOUND         TCP:    br0     eth0
        OUT=br0         =eth1   218.64.117.195  DST=11.11.11.64         LEN=64  TOS=0x00
        PREC=0x00       TTL=44  ID=6932         PROTO=TCP       SPT=4844        DPT=53
        WINDOW=34064 RES=0x00           SYN     URGP=0

Feb     18      13:21:45        bridge  kernel: INBOUND         TCP:    br0     eth0
        OUT=br0         =eth1   218.64.117.195  DST=11.11.11.67         LEN=64  TOS=0x00
        PREC=0x00       TTL=44  ID=7050         PROTO=TCP       SPT=3008        DPT=53
        WINDOW=34064 RES=0x00           SYN     URGP=0

Feb     18      07:45:59        bridge  kernel: INBOUND         TCP:    br0     eth0
        OUT=br0         =eth1   200.208.28.39   DST=11.11.11.85         LEN=40  TOS=0x08
        PREC=0x00       TTL=116         ID=11540        PROTO=TCP       SPT=80  DPT=53897
        WINDOW=65535 RES=0x00           ACK_SYN         URGP=0
```

Probe on port 135 followed by ICMP echo requests Source IP 63.123.70.166

```
Feb             9       19:28:20        bridge   kernel:  INBOUND         ICMP:    IN=br0
        PHYSIN=eth0     OUT=br0         PHYSOUT=eth1  SRC=63.123.70.166       DST=11.11.11.72
        LEN=92  TOS=0x00        PREC=0x00       TTL=118         ID=30829        PROTO=ICMP
        TYPE=8  CODE=0 ID=768  SEQ=52538

Feb             9       19:28:20        bridge   kernel:  INBOUND         TCP:     IN=br0
        PHYSIN=eth0     OUT=br0         PHYSOUT=eth1  SRC=63.123.70.166       DST=11.11.11.69
        LEN=48  TOS=0x00        PREC=0x00       TTL=117         ID=30830        DF
        PROTO=TCP       SPT=3435        DPT=135         WINDOW=16384

Feb             9       19:28:20        bridge   kernel:  INBOUND         ICMP:    IN=br0
        PHYSIN=eth0     OUT=br0         PHYSOUT=eth1  SRC=63.123.70.166       DST=11.11.11.73
        LEN=92  TOS=0x00        PREC=0x00       TTL=117         ID=30831        PROTO=ICMP
        TYPE=8  CODE=0 ID=768  SEQ=52794

Feb             9       19:28:20        bridge   kernel:  INBOUND         TCP:     IN=br0
        PHYSIN=eth0     OUT=br0         PHYSOUT=eth1  SRC=63.123.70.166       DST=11.11.11.70
        LEN=48  TOS=0x00        PREC=0x00       TTL=117         ID=30832        DF
        PROTO=TCP       SPT=3436        DPT=135         WINDOW=16384

Feb             9       19:28:20        bridge   kernel:  INBOUND         TCP:     IN=br0
        PHYSIN=eth0     OUT=br0         PHYSOUT=eth1  SRC=63.123.70.166       DST=11.11.11.71
        LEN=48  TOS=0x00        PREC=0x00       TTL=118         ID=30834        DF
        PROTO=TCP       SPT=3437        DPT=135         WINDOW=16384
```

Scan for open proxy ports 80, 8080, 3128: Source IP 64.0.66.213

```
Feb     2       13:39:09        bridge   kernel:  INBOUND        TCP:     IN=br0  PHYSIN=eth0
        OUT=br0         PHYSOUT=eth1  SRC=64.0.66.213         DST=11.11.11.64
        LEN=48  TOS=0x00        PREC=0x00       TTL=114         ID=52821        DF
        PROTO=TCP       SPT=4630        DPT=8080        WINDOW=65535 RES=0x00        SYN
        URGP=0

Feb     2       13:39:10        bridge   kernel:  INBOUND        TCP:     IN=br0  PHYSIN=eth0
        OUT=br0         PHYSOUT=eth1  SRC=64.0.66.213         DST=11.11.11.64
        LEN=48  TOS=0x00        PREC=0x00       TTL=114         ID=52822        DF
        PROTO=TCP       SPT=4631        DPT=80  WINDOW=65535 RES=0x00        SYN
        URGP=0

Feb     2       13:39:11        bridge   kernel:  INBOUND        TCP:     IN=br0  PHYSIN=eth0
        OUT=br0         PHYSOUT=eth1  SRC=64.0.66.213         DST=11.11.11.64
        LEN=48  TOS=0x00        PREC=0x00       TTL=114         ID=52823        DF
        PROTO=TCP       SPT=4632        DPT=3128        WINDOW=65535 RES=0x00        SYN
        URGP=0

Feb     2       13:39:11        bridge   kernel:  INBOUND        TCP:     IN=br0  PHYSIN=eth0
        OUT=br0         PHYSOUT=eth1  SRC=64.0.66.213         DST=11.11.11.67
        LEN=48  TOS=0x00        PREC=0x00       TTL=114         ID=52830        DF
        PROTO=TCP       SPT=4639        DPT=8080        WINDOW=65535 RES=0x00        SYN
        URGP=0

Feb     2       13:39:11        bridge   kernel:  INBOUND        TCP:     IN=br0  PHYSIN=eth0
        OUT=br0         PHYSOUT=eth1  SRC=64.0.66.213         DST=11.11.11.67
        LEN=48  TOS=0x00        PREC=0x00       TTL=114         ID=52831        DF
        PROTO=TCP       SPT=4640        DPT=80  WINDOW=65535 RES=0x00        SYN
        URGP=0
```

Probe on port 6129 source port is 220

TCP port 6129 is used by DameWare Mini Remote Control. DameWare is a Windows Remote Admin tool. The attacker is using a program to scan blocks of IP addresses for systems running DameWare on this port. The program always uses source port as 220.

```
Feb       1         00:00:02            bridge    kernel:   INBOUND             TCP:      br0       eth0
          OUT=br0             =eth1     192.150.249.87      DST=11.11.11.84               LEN=40    TOS=0x00
          PREC=0x00           TTL=110             ID=12973            PROTO=TCP           SPT=220
          DPT=6129            WINDOW=16384        RES=0x00            SYN       URGP=0


Feb       1         00:00:02            bridge    kernel:   INBOUND             TCP:      br0       eth0
          OUT=br0             =eth1     24.17.237.70        DST=11.11.11.95               LEN=40    TOS=0x00
          PREC=0x00           TTL=113             ID=27095            PROTO=TCP           SPT=220
          DPT=6129            WINDOW=16384        RES=0x00            SYN       URGP=0


Feb       1         00:00:07            bridge    kernel:   INBOUND             TCP:      br0       eth0
          OUT=br0             =eth1     192.150.249.87      DST=11.11.11.85               LEN=40    TOS=0x00
          PREC=0x00           TTL=110             ID=13801            PROTO=TCP           SPT=220
          DPT=6129            WINDOW=16384        RES=0x00            SYN       URGP=0


Feb       1         00:00:17            bridge    kernel:   INBOUND             TCP:      br0       eth0
          OUT=br0             =eth1     192.150.249.87      DST=11.11.11.87               LEN=40    TOS=0x00
          PREC=0x00           TTL=110             ID=15432            PROTO=TCP           SPT=220
          DPT=6129            WINDOW=16384        RES=0x00            SYN       URGP=0


Feb       1         00:00:24            bridge    kernel:   INBOUND             TCP:      br0       eth0
          OUT=br0             =eth1     24.17.237.70        DST=11.11.11.100              LEN=40    TOS=0x00
          PREC=0x00           TTL=113             ID=31168            PROTO=TCP           SPT=220
          DPT=6129            WINDOW=16384        RES=0x00            SYN       URGP=0
```

Slow and regular Probe on port UDP port 135 and 1026
Probe for Microsoft windows messenger service vulnerability

```
Feb       3         04:28:06            bridge    kernel:   INBOUND             UDP:      br0       eth0
          OUT=br0             =eth1     64.156.39.12        DST=11.11.11.64               LEN=574
          TOS=0x00            PREC=0x00           TTL=117             ID=36844            PROTO=UDP
          SPT=666             DPT=135             LEN=554
Feb       3         04:28:07            bridge    kernel:   INBOUND             UDP:      br0       eth0
          OUT=br0             =eth1     64.156.39.12        DST=11.11.11.64               LEN=574
          TOS=0x00            PREC=0x00           TTL=117             ID=36845            PROTO=UDP
          SPT=666             DPT=1026            LEN=554
Feb       3         04:28:07            bridge    kernel:   INBOUND             UDP:      br0       eth0
          OUT=br0             =eth1     64.156.39.12        DST=11.11.11.67               LEN=574
          TOS=0x00            PREC=0x00           TTL=117             ID=36850            PROTO=UDP
          SPT=666             DPT=135             LEN=554
Feb       3         04:28:09            bridge    kernel:   INBOUND             UDP:      br0       eth0
          OUT=br0             =eth1     64.156.39.12        DST=11.11.11.67               LEN=574
          TOS=0x00            PREC=0x00           TTL=117             ID=36851            PROTO=UDP
          SPT=666             DPT=1026            LEN=554
Feb       3         04:28:09            bridge    kernel:   INBOUND             UDP:      br0       eth0
          OUT=br0             =eth1     64.156.39.12        DST=11.11.11.69               LEN=574
          TOS=0x00            PREC=0x00           TTL=117             ID=36854            PROTO=UDP
          SPT=666             DPT=135             LEN=554
Feb       3         04:28:09            bridge    kernel:   INBOUND             UDP:      br0       eth0
          OUT=br0             =eth1     64.156.39.12        DST=11.11.11.69               LEN=574
          TOS=0x00            PREC=0x00           TTL=117             ID=36855            PROTO=UDP
          SPT=666             DPT=1026            LEN=554
```

The different reconnaissance activity were aimed at Finding

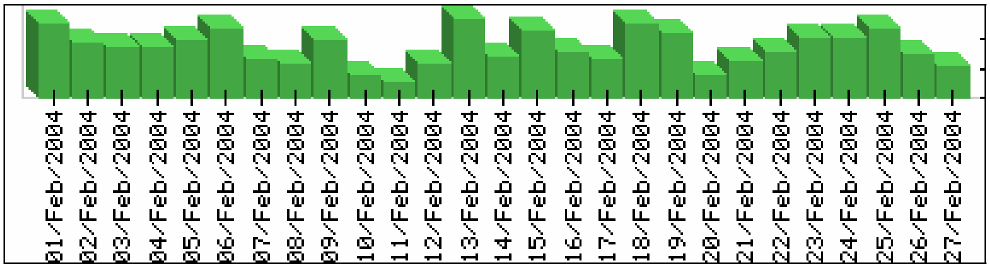
- DNS zone transfer attempts for list of internal machines
- Ping sweep to detect Machines that were up

- Port scan to detect Open ports on these machines
- Detecting any open proxy ports

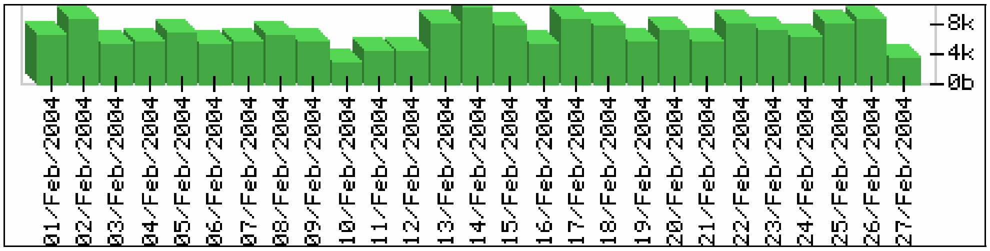
Some Sources of such activity are as seen in the extracts of the logs given above

Day wise activities of some of this IPs are given below.

63.123.70.166

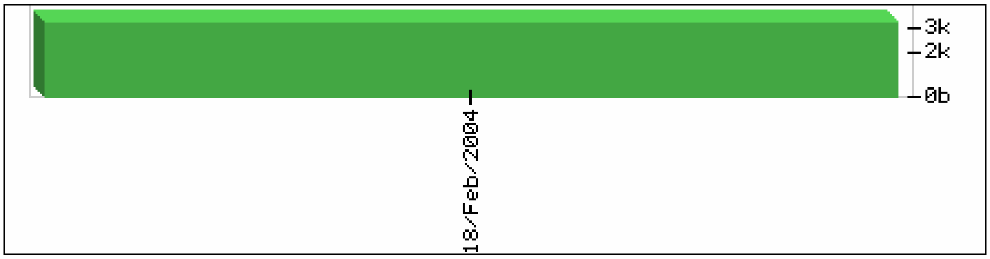


63.125.10.7



218.64.117.195

From this source there was activity on 18th Feb only and scanned to a defined set of ports



Similarly the following IP addresses also had shown such activity

64.0.66.213, 192.150.249.87, 64.156.39.12

4. What are the different scan patterns (sequential, etc) you can notice? Do you think all come from different attack tools? Any long term ("low and slow") scanning activity?

From the details given in answer to question no 2 the following distinct scan patterns were observed

- As observed from the log file, majority of the scan attempts were targeted to specific ports like 137, 139, 443 and 445.
- Sequential ICMP sweep scan was observed from source IP 63.123.70.166.
- A scan of combination of ICMP echo request and then TCP probe on 135 was noticed from some IPs.
- Sequential Scan for open proxy ports (80, 8080, 3128) were also noticed
- High level scan were observed towards backdoor ports left open by common worms/viruses/Trojans.

Attack tools

The scan patterns indicate that the scans originated from different scanning tools. This can be observed from the scans which followed a pattern, generally observed in scans/attacks done with common attack tools.

Long term slow scanning activity

ICMP and TCP/Syn packet to random ip addresses, evenly distributed across the days: Source IP **63.123.70.166, 63.125.10.7**

Probe on port 135 followed by ICMP echo requests Source IP 63.123.70.166

```
Feb         9       19:28:20        bridge   kernel:  INBOUND        ICMP:    IN=br0
        PHYSIN=eth0     OUT=br0         PHYSOUT=eth1   SRC=63.123.70.166
        DST=11.11.11.72         LEN=92 TOS=0x00       PREC=0x00      TTL=118
        ID=30829        PROTO=ICMP      TYPE=8  CODE=0 ID=768  SEQ=52538

Feb         9       19:28:20        bridge   kernel:  INBOUND        TCP:     IN=br0
        PHYSIN=eth0     OUT=br0         PHYSOUT=eth1   SRC=63.123.70.166
        DST=11.11.11.69         LEN=48 TOS=0x00       PREC=0x00      TTL=117
        ID=30830        DF      PROTO=TCP       SPT=3435       DPT=135
        WINDOW=16384

Feb         9       19:28:20        bridge   kernel:  INBOUND        ICMP:    IN=br0
        PHYSIN=eth0     OUT=br0         PHYSOUT=eth1   SRC=63.123.70.166
        DST=11.11.11.73         LEN=92 TOS=0x00       PREC=0x00      TTL=117
        ID=30831        PROTO=ICMP      TYPE=8  CODE=0 ID=768  SEQ=52794

Feb         9       19:28:20        bridge   kernel:  INBOUND        TCP:     IN=br0
        PHYSIN=eth0     OUT=br0         PHYSOUT=eth1   SRC=63.123.70.166
        DST=11.11.11.70         LEN=48 TOS=0x00       PREC=0x00      TTL=117
        ID=30832        DF      PROTO=TCP       SPT=3436       DPT=135
        WINDOW=16384

Feb         9       19:28:20        bridge   kernel:  INBOUND        TCP:     IN=br0
        PHYSIN=eth0     OUT=br0         PHYSOUT=eth1   SRC=63.123.70.166
        DST=11.11.11.71         LEN=48 TOS=0x00       PREC=0x00      TTL=118
        ID=30834        DF      PROTO=TCP       SPT=3437       DPT=135
        WINDOW=16384
```

SYN Scan to port 135 and 445 on almost everyday for a small period of time: Source IP 63.126.133.8

```
Feb     2       21:55:42        bridge  kernel:  INBOUND        TCP:    br0     eth0
        OUT=br0         =eth1   63.126.133.8     DST=11.11.11.95        LEN=48  TOS=0x00
        PREC=0x00       TTL=122         ID=47723        PROTO=TCP       SPT=2952
        DPT=135         WINDOW=16384 RES=0x00           SYN     URGP=0


Feb     2       21:55:42        bridge  kernel:  INBOUND        TCP:    br0     eth0
        OUT=br0         =eth1   63.126.133.8     DST=11.11.11.95        LEN=48  TOS=0x00
        PREC=0x00       TTL=122         ID=47725        PROTO=TCP       SPT=2954
        DPT=135         WINDOW=16384 RES=0x00           SYN     URGP=0


Feb     2       21:55:42        bridge  kernel:  INBOUND        TCP:    br0     eth0
        OUT=br0         =eth1   63.126.133.8     DST=11.11.11.95        LEN=48  TOS=0x00
        PREC=0x00       TTL=122         ID=47735        PROTO=TCP       SPT=2964
        DPT=135         WINDOW=16384 RES=0x00           SYN     URGP=0


Feb     2       21:55:42        bridge  kernel:  INBOUND        TCP:    br0     eth0
        OUT=br0         =eth1   63.126.133.8     DST=11.11.11.95        LEN=48  TOS=0x00
        PREC=0x00       TTL=122         ID=47743        PROTO=TCP       SPT=2972
        DPT=135         WINDOW=16384 RES=0x00           SYN     URGP=0


Feb     2       21:55:42        bridge  kernel:  INBOUND        TCP:    br0     eth0
        OUT=br0         =eth1   63.126.133.8     DST=11.11.11.95        LEN=48  TOS=0x00
        PREC=0x00       TTL=122         ID=47789        PROTO=TCP       SPT=2954
        DPT=135         WINDOW=16384 RES=0x00           SYN     URGP=0
```

Slow and regular Probe on UDP port 135 and 1026
Probe for Microsoft windows messenger service vulnerability

```
Feb     3       04:28:06        bridge  kernel:  INBOUND        UDP:    br0     eth0
        OUT=br0         =eth1   64.156.39.12     DST=11.11.11.64        LEN=574
        TOS=0x00        PREC=0x00       TTL=117         ID=36844       PROTO=UDP
        SPT=666         DPT=135         LEN=554
Feb     3       04:28:07        bridge  kernel:  INBOUND        UDP:    br0     eth0
        OUT=br0         =eth1   64.156.39.12     DST=11.11.11.64        LEN=574
        TOS=0x00        PREC=0x00       TTL=117         ID=36845       PROTO=UDP
        SPT=666         DPT=1026        LEN=554
Feb     3       04:28:07        bridge  kernel:  INBOUND        UDP:    br0     eth0
        OUT=br0         =eth1   64.156.39.12     DST=11.11.11.67        LEN=574
        TOS=0x00        PREC=0x00       TTL=117         ID=36850       PROTO=UDP
        SPT=666         DPT=135         LEN=554
Feb     3       04:28:09        bridge  kernel:  INBOUND        UDP:    br0     eth0
        OUT=br0         =eth1   64.156.39.12     DST=11.11.11.67        LEN=574
        TOS=0x00        PREC=0x00       TTL=117         ID=36851       PROTO=UDP
        SPT=666         DPT=1026        LEN=554
Feb     3       04:28:09        bridge  kernel:  INBOUND        UDP:    br0     eth0
        OUT=br0         =eth1   64.156.39.12     DST=11.11.11.69        LEN=574
        TOS=0x00        PREC=0x00       TTL=117         ID=36854       PROTO=UDP
        SPT=666         DPT=135         LEN=554
Feb     3       04:28:09        bridge  kernel:  INBOUND        UDP:    br0     eth0
        OUT=br0         =eth1   64.156.39.12     DST=11.11.11.69        LEN=574
        TOS=0x00        PREC=0x00       TTL=117         ID=36855       PROTO=UDP
        SPT=666         DPT=1026        LEN=554
```

Symptom of Spoofed Packet: Logs with INBLOCK message

```
Feb     10      14:06:52        bridge  kernel:  INBLOCK:       eth1    OUT=
        MAC=00:02:b3:65:c9:71:00:b0:d0:87:85:c3:08:00  11.11.11.69      DST=11.11.11.65
        LEN=89  TOS=0x00        PREC=0x00       TTL=64  ID=0    PROTO=UDP       SPT=1025
        DPT=514         LEN=69
```

Incoming traffic from Private IP address were also noticed, which would indicate an attack on the destination IP addresses.

172.17.0.0

```
Feb     13      12:39:04        bridge  kernel:  INBOUND        TCP:    br0     eth0
        OUT=br0         =eth1   172.17.3.59      DST=11.11.11.64        LEN=44  TOS=0x00
        PREC=0xA0       TTL=113         ID=24039        PROTO=TCP       SPT=2006
        DPT=3127        WINDOW=8192  RES=0x00           SYN     URGP=0

Feb     13      12:39:07        bridge  kernel:  INBOUND        TCP:    br0     eth0
        OUT=br0         =eth1   172.17.3.59      DST=11.11.11.64        LEN=44  TOS=0x00
        PREC=0xA0       TTL=113         ID=23528        PROTO=TCP       SPT=2006
        DPT=3127        WINDOW=8192  RES=0x00           SYN     URGP=6656
```

192.168.0.0

```
Feb     26      17:05:14        bridge  kernel:  INBOUND        ICMP:   br0     eth0
        OUT=br0         =eth1   192.168.1.99     DST=11.11.11.110       LEN=92  TOS=0x00
        PREC=0x00       TTL=112         ID=50664        PROTO=ICMP      TYPE=8  CODE=0
        ID=512  SEQ=33720

Feb     26      03:55:50        bridge  kernel:  INBOUND        ICMP:   br0     eth0
        OUT=br0         =eth1   192.168.35.100   DST=11.11.11.105       LEN=92  TOS=0x00
        PREC=0x00       TTL=108         ID=58531        PROTO=ICMP      TYPE=8  CODE=0
        ID=768  SEQ=33066
```

10.0.0.0

```
        Feb     25      17:18:43        bridge  kernel:  INBOUND        TCP:    br0     eth0
        OUT=br0         =eth1   10.30.101.157    DST=11.11.11.115       LEN=48  TOS=0x00
        PREC=0x00       TTL=113         ID=13937        PROTO=TCP       SPT=2878
        DPT=445         WINDOW=64240 RES=0x00           SYN     URGP=0

        Feb     25      17:18:47        bridge  kernel:  INBOUND        TCP:    br0     eth0
        OUT=br0         =eth1   10.30.101.157    DST=11.11.11.115       LEN=48  TOS=0x00
        PREC=0x00       TTL=113         ID=13987        PROTO=TCP       SPT=2878
        DPT=445         WINDOW=64240 RES=0x00           SYN     URGP=0
```

5. What other common internet noise types do you see?

Network traffic connections that are commonly considered noise:

TCP 113 - ident; used when an *incoming* connection comes in, servers may make an *outgoing* 113 request of the source IP to try and get a username behind the incoming connection.

UDP 137,138 - NetBIOS name lookup over TCP/IP; MS Windows based systems commonly broadcast this type of traffic. They don't only use DNS in some versions of Windows, they also try NetBIOS name looks as well. This type of UDP traffic is considered noise.

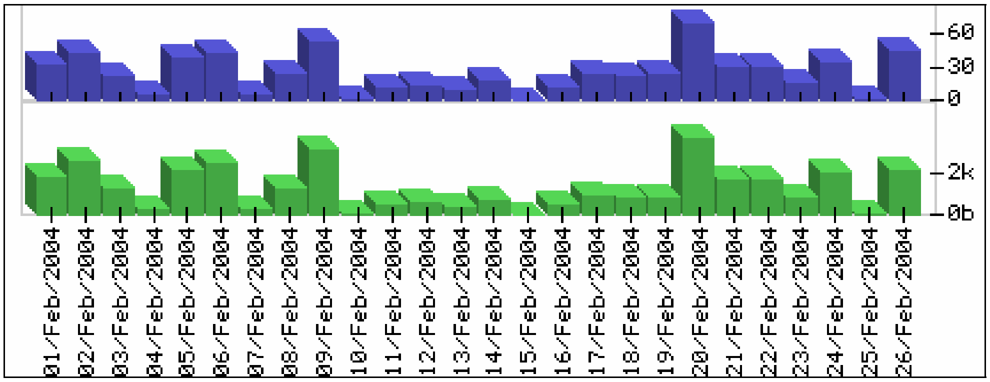
ICMP echo request/reply - (ICMPTYPES 8 and 0) PING. Some are noise, however they are used for certain attacks/scans. The recent MS worms used this to see whether a system/host was online before trying to connect to its TCP 135.

UDP 33400-33500 – These nominally are for services, but the biggest cause of them turning up in firewall logs is traceroute This is for Unix traceroute;

Noise generated due to Malware traffic: Activities of the different worms create a lot of internet activity… which is essentially noise.

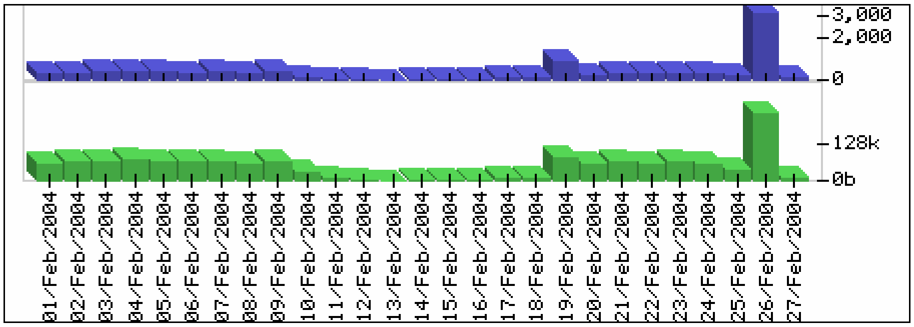
Some of the Internet noises noticed in the Honeynet logs are as:

Port 113



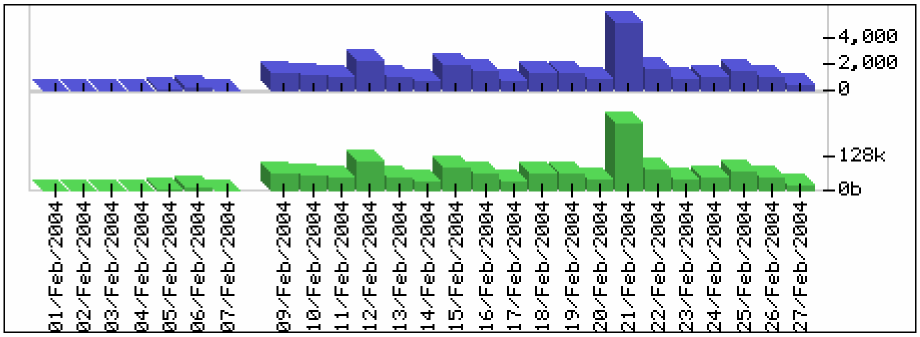
```
Feb     26      20:07:53        bridge   kernel:  INBOUND      TCP:    IN=br0  PHYSIN=eth0
        OUT=br0         PHYSOUT=eth1     SRC=63.199.242.48     DST=11.11.11.64         LEN=48
        TOS=0x00        PREC=0x00        TTL=111      ID=29533         DF      PROTO=TCP
        SPT=4152        DPT=113          WINDOW=65535 RES=0x00         SYN     URGP=0

Feb     26      20:07:53        bridge   kernel:  INBOUND      TCP:    IN=br0  PHYSIN=eth0
        OUT=br0         PHYSOUT=eth1     SRC=63.199.242.48     DST=11.11.11.67         LEN=48
        TOS=0x00        PREC=0x00        TTL=111      ID=29536         DF      PROTO=TCP
        SPT=4155        DPT=113          WINDOW=65535 RES=0x00         SYN     URGP=0

Feb     26      20:07:53        bridge   kernel:  INBOUND      TCP:    IN=br0  PHYSIN=eth0
        OUT=br0         PHYSOUT=eth1     SRC=63.199.242.48     DST=11.11.11.69         LEN=48
        TOS=0x00        PREC=0x00        TTL=111      ID=29538         DF      PROTO=TCP
        SPT=4157        DPT=113          WINDOW=65535 RES=0x00         SYN     URGP=0

Feb     26      20:07:53        bridge   kernel:  INBOUND      TCP:    IN=br0  PHYSIN=eth0
        OUT=br0         PHYSOUT=eth1     SRC=63.199.242.48     DST=11.11.11.70         LEN=48
        TOS=0x00        PREC=0x00        TTL=111      ID=29539         DF      PROTO=TCP
        SPT=4158        DPT=113          WINDOW=65535 RES=0x00         SYN     URGP=0

Feb     26      20:07:53        bridge   kernel:  INBOUND      TCP:    IN=br0  PHYSIN=eth0
        OUT=br0         PHYSOUT=eth1     SRC=63.199.242.48     DST=11.11.11.71         LEN=48
        TOS=0x00        PREC=0x00        TTL=111      ID=29540         DF      PROTO=TCP
        SPT=4159        DPT=113          WINDOW=65535 RES=0x00         SYN     URGP=0

Feb     26      20:07:53        bridge   kernel:  INBOUND      TCP:    IN=br0  PHYSIN=eth0
        OUT=br0         PHYSOUT=eth1     SRC=63.199.242.48     DST=11.11.11.72         LEN=48
        TOS=0x00        PREC=0x00        TTL=111      ID=29541         DF      PROTO=TCP
        SPT=4160        DPT=113          WINDOW=65535 RES=0x00         SYN     URGP=0
```

UDP 137,138



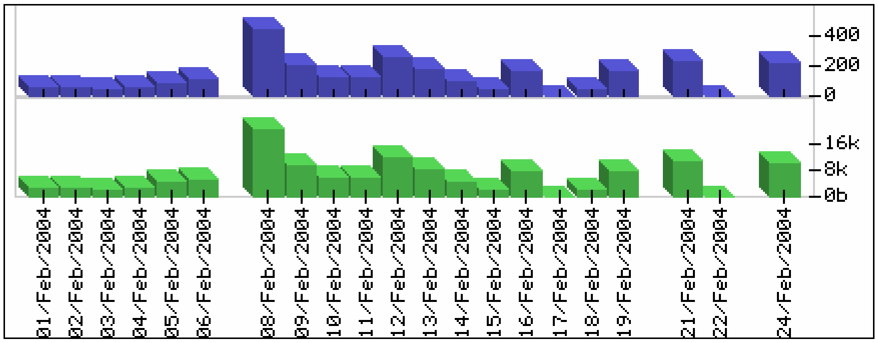
```
Feb   25    13:53:58     bridge    kernel:  OUTG    CONN    UDP:    IN=br0  PHYSIN=eth1
      OUT=br0           PHYSOUT=eth0  SRC=11.11.11.67         DST=62.181.161.36
      LEN=257           TOS=0x00      PREC=0x00       TTL=64  ID=0    DF      PROTO=UDP
      SPT=137           DPT=3159      LEN=237

Feb   25    13:53:59     bridge    kernel:  OUTG    CONN    UDP:    IN=br0  PHYSIN=eth1
      OUT=br0           PHYSOUT=eth0  SRC=11.11.11.67         DST=62.181.161.36
      LEN=257           TOS=0x00      PREC=0x00       TTL=64  ID=0    DF      PROTO=UDP
      SPT=137           DPT=3160      LEN=237

Feb   25    13:54:03     bridge    kernel:  OUTG    CONN    UDP:    IN=br0  PHYSIN=eth1
      OUT=br0           PHYSOUT=eth0  SRC=11.11.11.67         DST=62.181.161.36
      LEN=257           TOS=0x00      PREC=0x00       TTL=64  ID=0    DF      PROTO=UDP
      SPT=137           DPT=3170      LEN=237

Feb   25    13:58:43     bridge    kernel:  Legal   Broadcast:      IN=br0  PHYSIN=eth1
      OUT=br0           PHYSOUT=eth0  SRC=11.11.11.67         DST=11.11.11.255
      LEN=241           TOS=0x00      PREC=0x00       TTL=64  ID=0    DF      PROTO=UDP
      SPT=138           DPT=138       LEN=221

Feb   25    13:58:43     bridge    kernel:  Legal   Broadcast:      IN=br0  PHYSIN=eth1
      OUT=br0           PHYSOUT=eth0  SRC=11.11.11.67         DST=11.11.11.255
      LEN=232           TOS=0x00      PREC=0x00       TTL=64  ID=0    DF      PROTO=UDP
      SPT=138           DPT=138       LEN=212

Feb   25    13:46:39     bridge    kernel:  Legal   Broadcast:      IN=br0  PHYSIN=eth1
      OUT=br0           PHYSOUT=eth0  SRC=11.11.11.67         DST=11.11.11.255
      LEN=241           TOS=0x00      PREC=0x00       TTL=64  ID=0    DF      PROTO=UDP
      SPT=138           DPT=138       LEN=221
```

Noise due to all the variants of Mydoom 3127, 3128, 1080, 10080



Noise due to other Malware like Beagle.B (port 8866), Kuang2 (port 17300), SubSeven (port 27374), hackatack (port 31789)

The samples of the logs due to these are given above in response to question number 2.
The activity noticed which were probably due to the above mentioned Malware is shown below in graphical representation.



6. Any unidentified/anomalous traffic observed? Please suggest hypothesis for why it is there and what it indicates.

Large number of packets as source ip 127.0.0.1 and source port 80

```
Feb     23      19:40:01        bridge  kernel: INBOUND         TCP:    IN=br0  PHYSIN=eth0
        OUT=br0         PHYSOUT=eth1    SRC=127.0.0.1   DST=11.11.11.64         LEN=40
        TOS=0x00        PREC=0x00       TTL=119         ID=28945        PROTO=TCP
        SPT=80  DPT=1089        WINDOW=0        RES=0x00        ACK     RST     URGP=0

Feb     23      19:40:25        bridge  kernel: INBOUND         TCP:    IN=br0  PHYSIN=eth0
        OUT=br0         PHYSOUT=eth1    SRC=127.0.0.1   DST=11.11.11.67         LEN=40
        TOS=0x00        PREC=0x00       TTL=119         ID=64330        PROTO=TCP
        SPT=80  DPT=1055        WINDOW=0        RES=0x00        ACK     RST     URGP=0
```

```
Feb       23        18:48:09            bridge    kernel:   INBOUND             TCP:      IN=br0    PHYSIN=eth0
          OUT=br0             PHYSOUT=eth1        SRC=127.0.0.1       DST=11.11.11.125              LEN=40
          TOS=0x00            PREC=0x00           TTL=119             ID=31298            PROTO=TCP
          SPT=80    DPT=1172            WINDOW=0            RES=0x00            ACK       RST       URGP=0

Feb       23        18:51:40            bridge    kernel:   INBOUND             TCP:      IN=br0    PHYSIN=eth0
          OUT=br0             PHYSOUT=eth1        SRC=127.0.0.1       DST=11.11.11.73               LEN=40
          TOS=0x00            PREC=0x00           TTL=119             ID=58641            PROTO=TCP
          SPT=80    DPT=1332            WINDOW=0            RES=0x00            ACK       RST       URGP=0

Feb       23        19:00:55            bridge    kernel:   INBOUND             TCP:      IN=br0    PHYSIN=eth0
          OUT=br0             PHYSOUT=eth1        SRC=127.0.0.1       DST=11.11.11.64               LEN=40
          TOS=0x00            PREC=0x00           TTL=119             ID=42071            PROTO=TCP
          SPT=80    DPT=1062            WINDOW=0            RES=0x00            ACK       RST       URGP=0

Feb       23        19:08:22            bridge    kernel:   INBOUND             TCP:      IN=br0    PHYSIN=eth0
          OUT=br0             PHYSOUT=eth1        SRC=127.0.0.1       DST=11.11.11.89               LEN=40
          TOS=0x00            PREC=0x00           TTL=119             ID=26523            PROTO=TCP
          SPT=80    DPT=1116            WINDOW=0            RES=0x00            ACK       RST       URGP=0

Feb       23        17:59:44            bridge    kernel:   INBOUND             TCP:      IN=br0    PHYSIN=eth0
          OUT=br0             PHYSOUT=eth1        SRC=127.0.0.1       DST=11.11.11.64               LEN=40
          TOS=0x00            PREC=0x00           TTL=119             ID=11056            PROTO=TCP
          SPT=80    DPT=1261            WINDOW=0            RES=0x00            ACK       RST       URGP=0

Feb       23        18:06:52            bridge    kernel:   INBOUND             TCP:      IN=br0    PHYSIN=eth0
          OUT=br0             PHYSOUT=eth1        SRC=127.0.0.1       DST=11.11.11.90               LEN=40
          TOS=0x00            PREC=0x00           TTL=119             ID=13899            PROTO=TCP
          SPT=80    DPT=1215            WINDOW=0            RES=0x00            ACK       RST       URGP=0
```

The traffic above was probably as a result of the MsBlaster worm.

Large DNS requests from 11.11.11.67 to DNS Servers

```
Feb       24        14:33:31            bridge    kernel:   Legal     DNS:      IN=br0    PHYSIN=eth1
          OUT=br0             PHYSOUT=eth0        SRC=11.11.11.67               DST=22.22.22.40
          LEN=72    TOS=0x00            PREC=0x00           TTL=64    ID=17291            DF        PROTO=UDP
          SPT=3536            DPT=53    LEN=52

Feb       24        14:33:31            bridge    kernel:   Legal     DNS:      IN=br0    PHYSIN=eth1
          OUT=br0             PHYSOUT=eth0        SRC=11.11.11.67               DST=22.22.22.40
          LEN=72    TOS=0x00            PREC=0x00           TTL=64    ID=17292            DF        PROTO=UDP
          SPT=3537            DPT=53    LEN=52

Feb       24        14:33:31            bridge    kernel:   Legal     DNS:      IN=br0    PHYSIN=eth1
          OUT=br0             PHYSOUT=eth0        SRC=11.11.11.67               DST=22.22.22.40
          LEN=72    TOS=0x00            PREC=0x00           TTL=64    ID=17292            DF        PROTO=UDP
          SPT=3538            DPT=53    LEN=52

Feb       24        14:33:31            bridge    kernel:   Legal     DNS:      IN=br0    PHYSIN=eth1
          OUT=br0             PHYSOUT=eth0        SRC=11.11.11.67               DST=22.22.22.40
          LEN=72    TOS=0x00            PREC=0x00           TTL=64    ID=17293            DF        PROTO=UDP
          SPT=3539            DPT=53    LEN=52

Feb       24        14:33:31            bridge    kernel:   Legal     DNS:      IN=br0    PHYSIN=eth1
          OUT=br0             PHYSOUT=eth0        SRC=11.11.11.67               DST=22.22.22.40
          LEN=72    TOS=0x00            PREC=0x00           TTL=64    ID=17293            DF        PROTO=UDP
          SPT=3540            DPT=53    LEN=52

Feb       24        14:33:31            bridge    kernel:   Legal     DNS:      IN=br0    PHYSIN=eth1
          OUT=br0             PHYSOUT=eth0        SRC=11.11.11.67               DST=22.22.22.40
          LEN=72    TOS=0x00            PREC=0x00           TTL=64    ID=17293            DF        PROTO=UDP
          SPT=3541            DPT=53    LEN=52
```

```
Feb     24      14:33:31        bridge   kernel:  Legal    DNS:     IN=br0  PHYSIN=eth1
        OUT=br0         PHYSOUT=eth0  SRC=11.11.11.67        DST=22.22.22.40
        LEN=72 TOS=0x00       PREC=0x00      TTL=64  ID=17294       DF      PROTO=UDP
        SPT=3542        DPT=53 LEN=52

Feb     24      14:33:31        bridge   kernel:  Legal    DNS:     IN=br0  PHYSIN=eth1
        OUT=br0         PHYSOUT=eth0  SRC=11.11.11.67        DST=22.22.22.40
        LEN=72 TOS=0x00       PREC=0x00      TTL=64  ID=17294       DF      PROTO=UDP
        SPT=3543        DPT=53 LEN=52
```

Large number of SYN/ACK packets from outside sources to internal Honeynet servers.

This was unexplained as no SYN requests were sent from the internal servers to those machines. Further these SYN ACK packets had a source port of 80.

```
Feb     3       07:02:28        bridge   kernel:  INBOUND        TCP:     br0     eth0
        OUT=br0         =eth1   218.22.13.10     DST=11.11.11.85         LEN=48  TOS=0x00
        PREC=0x00       TTL=110         ID=0     PROTO=TCP      SPT=80  DPT=20502
        WINDOW=65535 RES=0x00         ACK_SYN         URGP=0


Feb     3       07:00:27        bridge   kernel:  INBOUND        TCP:     br0     eth0
        OUT=br0         =eth1   202.99.219.185  DST=11.11.11.89         LEN=44  TOS=0x00
        PREC=0x00       TTL=113         ID=52801        PROTO=TCP     SPT=80  DPT=56984
        WINDOW=16616 RES=0x00         ACK_SYN         URGP=0


Feb     3       07:00:31        bridge   kernel:  INBOUND        TCP:     br0     eth0
        OUT=br0         =eth1   202.99.219.185  DST=11.11.11.89         LEN=44  TOS=0x00
        PREC=0x00       TTL=113         ID=28331        PROTO=TCP     SPT=80  DPT=56984
        WINDOW=16616 RES=0x00         ACK_SYN         URGP=0


Feb     3       05:55:59        bridge   kernel:  INBOUND        TCP:     br0     eth0
        OUT=br0         =eth1   218.22.13.10     DST=11.11.11.95         LEN=48  TOS=0x00
        PREC=0x00       TTL=110         ID=0     PROTO=TCP      SPT=80  DPT=16233
        WINDOW=65535 RES=0x00         ACK_SYN         URGP=0


Feb     3       06:05:56        bridge   kernel:  INBOUND        TCP:     br0     eth0
        OUT=br0         =eth1   218.22.13.10     DST=11.11.11.69         LEN=48  TOS=0x00
        PREC=0x00       TTL=110         ID=0     PROTO=TCP      SPT=80  DPT=55259
        WINDOW=65535 RES=0x00         ACK_SYN         URGP=0
```

This can be due to either spoofed internal Honeynet IP addresses being used against the machines which were sending SYN ACK packets. This behavior is also noticed when load balancers are used.

7. Was the honeypot compromised during the observed time period? How do you know?

Some of the Honeypot machines are suspected to have been compromised.

These Honeynet machines were likely to have been compromised.

SRC=11.11.11.73
SRC=11.11.11.67
SRC=11.11.11.75
SRC=11.11.11.80
SRC=11.11.11.71

A Honeypot is usually configured to drops packets from inside IP to outside after a certain number of connections. From the logs, it is observed that the limit was placed at 13. Thus Honeynet machines for which packets were dropped after 13 connections would indicate a possible compromise.

```
Feb     NULL     9        12:44:48         bridge    kernel:   Drop     TCP      after    13       attempts
        IN=br0   PHYSIN=eth1     OUT=br0          PHYSOUT=eth0   SRC=11.11.11.67
        DST=211.185.238.162     LEN=60 TOS=0x00        PREC=0x00       TTL=64  ID=12193
        DF       PROTO=TCP       SPT=1859         DPT=113          WINDOW=5840   RES=0x00
        SYN      URGP=0


Feb     NULL     9        05:42:05         bridge    kernel:   Drop     TCP      after    13       attempts
        IN=br0   PHYSIN=eth1     OUT=br0          PHYSOUT=eth0   SRC=11.11.11.67
        DST=203.190.146.137     LEN=60 TOS=0x00        PREC=0x00       TTL=64  ID=17313
        DF       PROTO=TCP       SPT=1834         DPT=113          WINDOW=5840   RES=0x00
        SYN      URGP=0


Feb     NULL     8        12:01:03         bridge    kernel:   Drop     udp      after    20       attempts
        IN=br0   PHYSIN=eth1     OUT=br0          PHYSOUT=eth0   SRC=11.11.11.67
        DST=11.11.11.65          LEN=157          TOS=0x00         PREC=0x00       TTL=64  ID=0
        DF       PROTO=UDP       SPT=4916         DPT=514          LEN=137          NULL     NULL
        NULL


Feb     NULL     8        11:49:57         bridge    kernel:   Drop     TCP      after    13       attempts
        IN=br0   PHYSIN=eth1     OUT=br0          PHYSOUT=eth0   SRC=11.11.11.67
        DST=207.66.155.21        LEN=60 TOS=0x00        PREC=0x00       TTL=64  ID=24147
        DF       PROTO=TCP       SPT=1765         DPT=80 WINDOW=5840   RES=0x00        SYN
        URGP=0


Feb     NULL     8        10:54:01         bridge    kernel:   Drop     udp      after    20       attempts
        IN=br0   PHYSIN=eth1     OUT=br0          PHYSOUT=eth0   SRC=11.11.11.67
        DST=11.11.11.65          LEN=82 TOS=0x00        PREC=0x00       TTL=64  ID=0     DF
        PROTO=UDP       SPT=4914         DPT=514          LEN=62 NULL     NULL     NULL
```

This activity was noticed in the following period.

SRC=11.11.11.73
SRC=11.11.11.67 (Feb 1, 2, 3, 8, 9)
SRC=11.11.11.75 (Feb 7)
SRC=11.11.11.80 (Feb 11)
SRC=11.11.11.71 (Feb 12)

The Machine with IP address 11.11.11.67 had made connections from date Feb 1 itself. So it is probable that the machine may have been compromised earlier, before the logs being observed.

Further, two more Honeynet machines had also made outgoing connections but the threshold limit of 13 connections had not been reached. The outgoing connections were identified by the message OUTG CONN in the logs.

11.11.11.69
11.11.11.72

```
Feb     NULL     9        22:48:24         bridge    kernel:   OUTG     CONN     TCP:     IN=br0
        PHYSIN=eth1      OUT=br0          PHYSOUT=eth0   SRC=11.11.11.67
        DST=211.222.247.108     LEN=60 TOS=0x00        PREC=0x00       TTL=64  ID=17805
        DF       PROTO=TCP       SPT=1876         DPT=113          WINDOW=5840   RES=0x00
        SYN      URGP=0


Feb     NULL     9        22:48:27         bridge    kernel:   OUTG     CONN     TCP:     IN=br0
        PHYSIN=eth1      OUT=br0          PHYSOUT=eth0   SRC=11.11.11.67
        DST=211.222.247.108    LEN=60 TOS=0x00       PREC=0x00      TTL=64  ID=17806
        DF       PROTO=TCP      SPT=1876        DPT=113         WINDOW=5840  RES=0x00
        SYN      URGP=0

Feb     NULL     9        22:49:04          bridge   kernel:  OUTG     CONN    TCP:     IN=br0
        PHYSIN=eth1     OUT=br0         PHYSOUT=eth0  SRC=11.11.11.71
        DST=211.222.247.108    LEN=60 TOS=0x00       PREC=0x00      TTL=64  ID=39502
        DF       PROTO=TCP      SPT=1878        DPT=113         WINDOW=5840  RES=0x00
        SYN      URGP=0

Feb     NULL     9        22:49:05          bridge   kernel:  OUTG     CONN    TCP:     IN=br0
        PHYSIN=eth1     OUT=br0         PHYSOUT=eth0  SRC=11.11.11.72
        DST=211.222.247.108    LEN=60 TOS=0x00       PREC=0x00      TTL=64  ID=2753
        DF       PROTO=TCP      SPT=1879        DPT=113         WINDOW=5840  RES=0x00
        SYN      URGP=0

Feb     NULL     9        22:49:05          bridge   kernel:  OUTG     CONN    TCP:     IN=br0
        PHYSIN=eth1     OUT=br0         PHYSOUT=eth0  SRC=11.11.11.75
        DST=211.222.247.108    LEN=60 TOS=0x00       PREC=0x00      TTL=64  ID=31014
        DF       PROTO=TCP      SPT=1880        DPT=113         WINDOW=5840  RES=0x00
        SYN      URGP=0
```

8. If you'd obtain such firewall logs from a production system, what source IPs or groups of such IPs you'd focus on as a highest threat?

Source IP 66.60.166.84

Destination IP	Packets		Destination port	Packets
11.11.11.75	19584		443	21829
11.11.11.69	519			
11.11.11.89	496		**IP flags**	**Packets**
11.11.11.82	478		SYN	21781
11.11.11.87	439		ACK FIN	48
11.11.11.105	311			
11.11.11.73	2			

It shows a clear SYN scan/attack to port 443 and primarily aimed at 11.11.11.75

Source IP 66.186.83.178

Destination IP	Packets		Destination port	Packets
11.11.11.125	647		445	7657
11.11.11.120	638		139	2540
11.11.11.115	637			
11.11.11.110	626		**IP flags**	**Packets**
11.11.11.69	535		SYN	10197
11.11.11.70	533			
11.11.11.67	530			
11.11.11.73	528			
11.11.11.72	526			

11.11.11.75	524			

This IP was targeting ports 139 and 445. It was probably attempting to exploit the Microsoft RPC DCOM vulnerabilities.

Source IP 63.13.135.27

Destination IP	Packets		Destination port	Packets
11.11.11.70	382		445	3330
11.11.11.85	374		137	2588
11.11.11.72	368		139	2177
11.11.11.100	367		113	26
11.11.11.81	367			
11.11.11.95	366		**Protocol**	**Packets**
11.11.11.67	365		TCP	5533
11.11.11.69	361		UDP	2588
11.11.11.83	361			
11.11.11.120	360		Flags	Packets
			SYN	5533

This IP was also targeting port 139 and 445.

Source IP 63.123.70.166

Destination IP	Packets		Flags	Packets
11.11.11.69	261		SYN	4018
11.11.11.67	251			
11.11.11.95	227			
11.11.11.70	224		**Destination port**	**Packets**
11.11.11.100	215		135	4018
11.11.11.73	206			
11.11.11.72	190			
11.11.11.87	185			
11.11.11.89	185			
11.11.11.75	185			

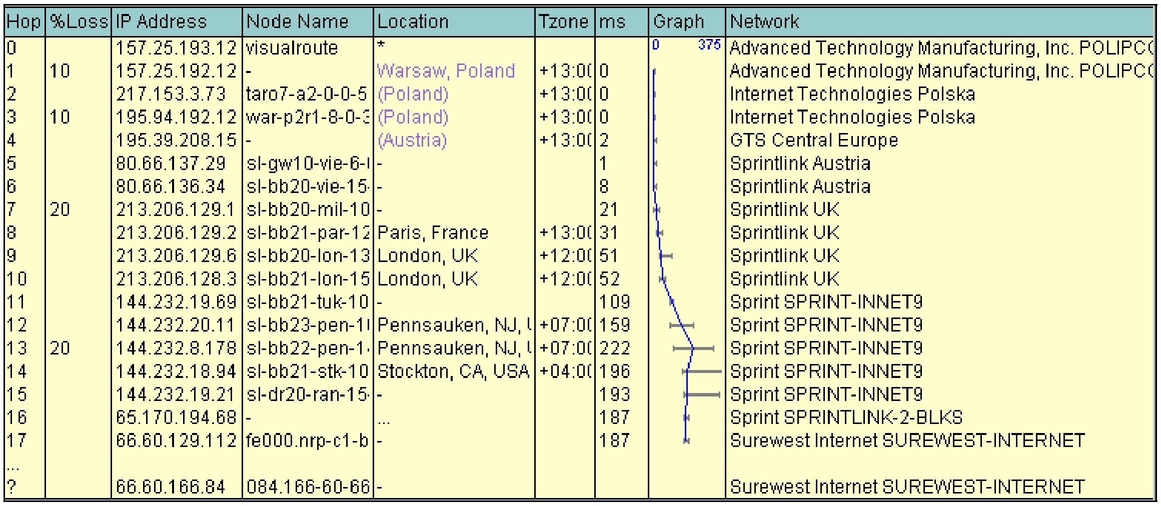
Some Other IPs

63.125.10.7, 218.64.117.195, 63.123.70.166, 64.0.66.213, 192.150.249.87, 64.156.39.12

The whois query to some IPs

66.60.166.84		66.186.83.178	
OrgName:	Surewest Internet	OrgName:	Vianet Internet Solutions
OrgID:	SURW	OrgID:	VIS
Address:	P.O. Box 969	Address:	128 Larch Street
City:	Roseville	Address:	Suite 301
StateProv:	CA	City:	Sudbury
PostalCode:	95678	StateProv:	ON
Country:	US	PostalCode:	P3E-5J8
NetRange:	66.60.128.0 - 66.60.191.255	Country:	CA
		NetRange:	66.186.64.0 - 66.186.95.255
CIDR:	66.60.128.0/18	CIDR:	6.186.64.0/19
NetName:	SUREWEST-INTERNET	NetName:	VIANET-CA3
NetHandle:	NET-66-60-128-0-1	NetHandle:	NET-66-186-64-0-1
Parent:	NET-66-0-0-0-0	Parent:	NET-66-0-0-0-0
		NetType:	Direct Allocation
		NameServer:	ICEWALL.VIANET.CA
		NameServer:	GWN.VIANET.CA

Visual route of 66.60.166.84



Hop	%Loss	IP Address	Node Name	Location	Tzone	ms	Graph	Network
0		157.25.193.12	visualroute	*			0 375	Advanced Technology Manufacturing, Inc. POLIPC
1	10	157.25.192.12	-	Warsaw, Poland	+13:0	0		Advanced Technology Manufacturing, Inc. POLIPC
2		217.153.3.73	taro7-a2-0-0-5	(Poland)	+13:0	0		Internet Technologies Polska
3	10	195.94.192.12	war-p2r1-8-0-3	(Poland)	+13:0	0		Internet Technologies Polska
4		195.39.208.15	-	(Austria)	+13:0	2		GTS Central Europe
5		80.66.137.29	sl-gw10-vie-6-I	-		1		Sprintlink Austria
6		80.66.136.34	sl-bb20-vie-15	-		8		Sprintlink Austria
7	20	213.206.129.1	sl-bb20-mil-10	-		21		Sprintlink UK
8		213.206.129.2	sl-bb21-par-12	Paris, France	+13:0	31		Sprintlink UK
9		213.206.129.6	sl-bb20-lon-13	London, UK	+12:0	51		Sprintlink UK
10		213.206.128.3	sl-bb21-lon-15	London, UK	+12:0	52		Sprintlink UK
11		144.232.19.69	sl-bb21-tuk-10	-		109		Sprint SPRINT-INNET9
12		144.232.20.11	sl-bb23-pen-1	Pennsauken, NJ,	+07:0	159		Sprint SPRINT-INNET9
13	20	144.232.8.178	sl-bb22-pen-1	Pennsauken, NJ,	+07:0	222		Sprint SPRINT-INNET9
14		144.232.18.94	sl-bb21-stk-10	Stockton, CA, USA	+04:0	196		Sprint SPRINT-INNET9
15		144.232.19.21	sl-dr20-ran-15	-		193		Sprint SPRINT-INNET9
16		65.170.194.68	-	...		187		Sprint SPRINTLINK-2-BLKS
17		66.60.129.112	fe000.nrp-c1-b	-		187		Surewest Internet SUREWEST-INTERNET
...								
?		66.60.166.84	084.166-60-66	-				Surewest Internet SUREWEST-INTERNET

9. What honeypot systems were attacked the most? What ports were open on each of them? Why do you think a machines with close IP addresses were attacked differently?

The most attacked Honeynet IPs are

11.11.11.75, 11.11.11.80, 11.11.11.67, 11.11.11.100, 11.11.11.90

Destination IP	Packets received
11.11.11.75	30130
11.11.11.80	13255
11.11.11.67	12381
11.11.11.100	11417
11.11.11.90	11359
11.11.11.71	11062
11.11.11.87	10994
11.11.11.105	10915
11.11.11.115	10842
11.11.11.110	10839

Open Ports

Open ports of a machine were identified by looking for traffic from inside with ACK flag set.

IP	Open Ports
11.11.11.67	443
11.11.11.71	80,443
11.11.11.73	80, 443,3128
11.11.11.80	443,80
11.11.11.69	443
11.11.11.72	443,80
11.11.11.75	443,80

Bonus Question:
10. Provide some high-level metrics about the data (such as most frequently targeted ports, etc) and make some conclusions based on them.

Destination Port	Packets	Protocol	Explanation
135	88157	TCP	DCE Endpoint resolution
445	46439	TCP	Win 2K Server Message Block
443	26444	TCP	SSL
3127	25781	TCP	W32.MyDoom, W32.Novarg.A backdoor
139	15000	TCP	NetBIOS Session, Windows File & Printer Shaaring
1434	5909	TCP	Microsoft-SQL-Server

There is high level traffic flow towards port 135, 139, 445 which essentially indicates attempt on different windows vulnerability.

High traffic for Mydoom backdoor

There are some SYN Attack attempts to port 443

```
Feb     8       07:31:38        bridge  kernel: INBOUND         TCP:    IN=br0  PHYSIN=eth0
        OUT=br0         PHYSOUT=eth1    SRC=66.60.166.84        DST=11.11.11.82
        LEN=60  TOS=0x00        PREC=0x00       TTL=49  ID=33000        DF      PROTO=TCP
        SPT=38843       DPT=443         WINDOW=5840     RES=0x00        SYN     URGP=0

Feb     8       07:31:39        bridge  kernel: INBOUND         TCP:    IN=br0  PHYSIN=eth0
        OUT=br0         PHYSOUT=eth1    SRC=66.60.166.84        DST=11.11.11.82
        LEN=60  TOS=0x00        PREC=0x00       TTL=49  ID=30736        DF      PROTO=TCP
        SPT=38870       DPT=443         WINDOW=5840     RES=0x00        SYN     URGP=0

Feb     8       07:31:39        bridge  kernel: INBOUND         TCP:    IN=br0  PHYSIN=eth0
        OUT=br0         PHYSOUT=eth1    SRC=66.60.166.84        DST=11.11.11.82
        LEN=60  TOS=0x00        PREC=0x00       TTL=49  ID=34628        DF      PROTO=TCP
        SPT=38888       DPT=443         WINDOW=5840     RES=0x00        SYN     URGP=0
```

References

http://www.robertgraham.com/pubs/firewall-seen.html
http://logi.cc/linux/netfilter-log-format.php3
http://www.sawmill.net
http://www.dshield.org
http://www.visualroute.nl
http://www.doshelp.com/trojanports.htm
http://www.keypoint.com.au/knowledge.html?strid=1144