Iptables Attack Visualization

Michael Rash
Security Architect
Enterasys Networks, Inc.

http://www.cipherdyne.org/

OSCON
2007-07-26

Agenda

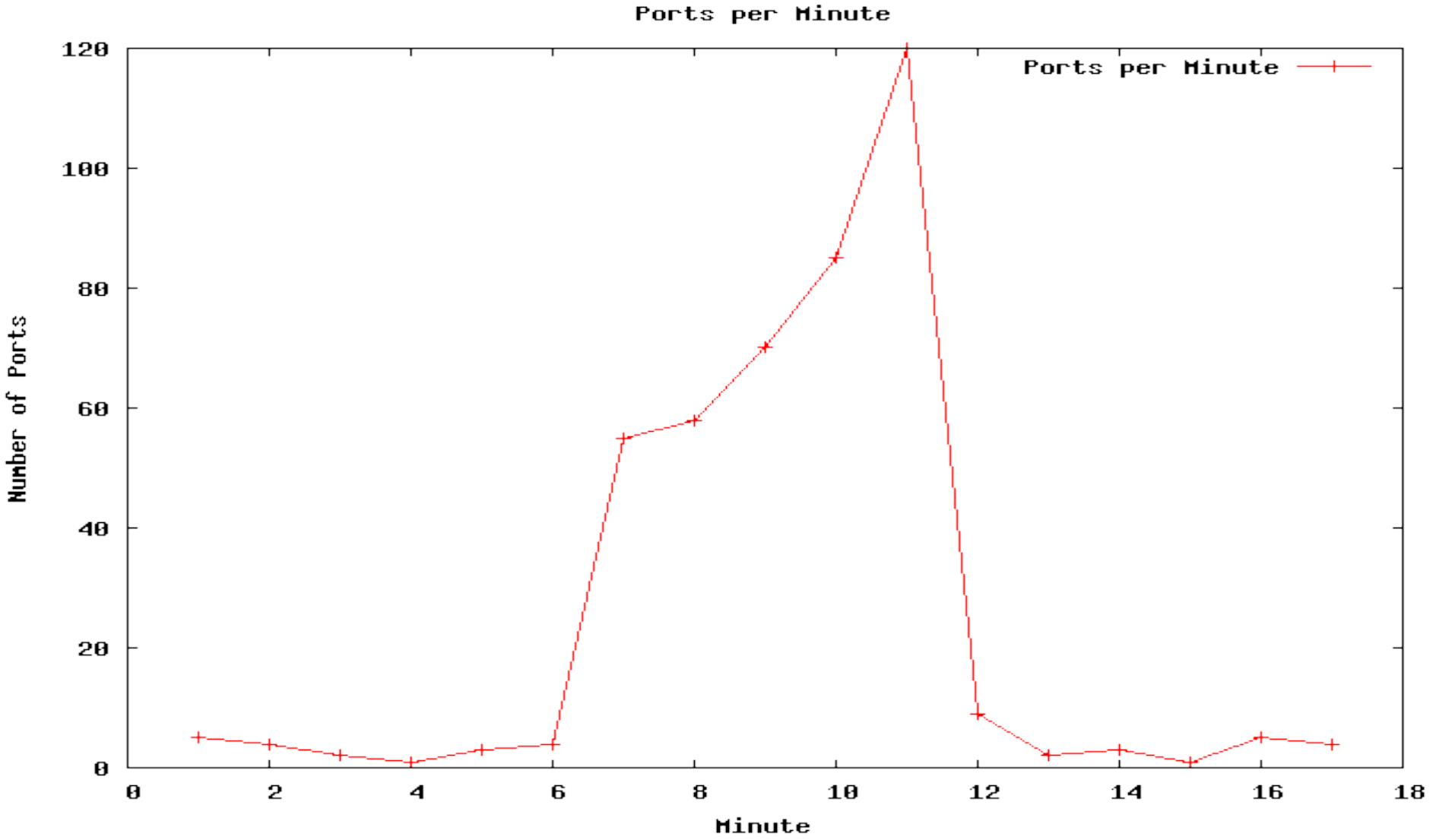
- Why visualize iptables log data?
  - ***context*** and ***change***
  - iptables log message formats and data completeness
- New psad-2.0.8 release with Gnuplot interface
- Honeynet Project Scan34 iptables visualizations (see http://www.honeynet.org)
  - Gnuplot
  - AfterGlow

Why Visualize Data?

- Consider the following set of values (each value represents the number of packets to unique TCP ports per minute):

```
5, 4, 2, 1, 3, 4, 55, 58, 70,
85, 120, 9, 2, 3, 1, 5, 4
```

Seeing the Trend



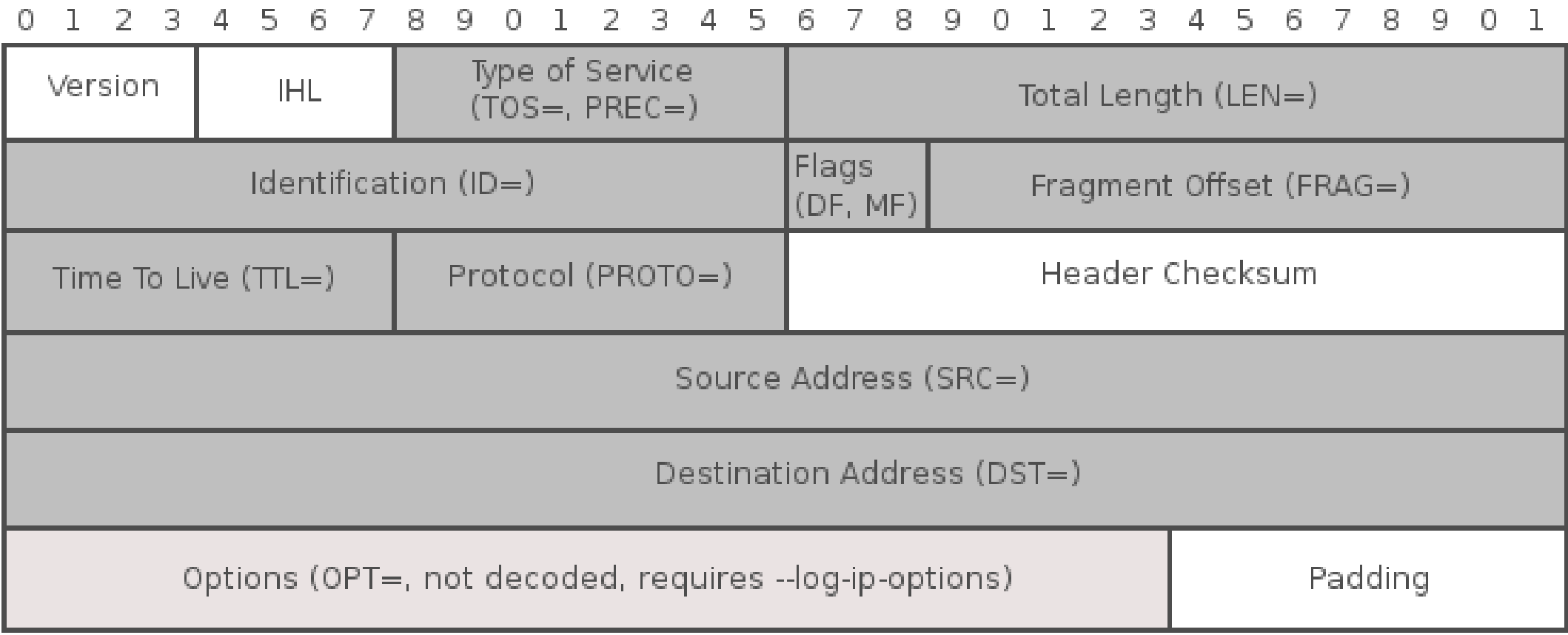
Graph Types

- Gnuplot
  - Dots, points, lines through points – Good at seeing trends and relationships in large data sets (> 100,000 points)
  - 3D mode with interactive viewing
- AfterGlow
  - Link Graphs – Good at expressing network relationships with IP addresses

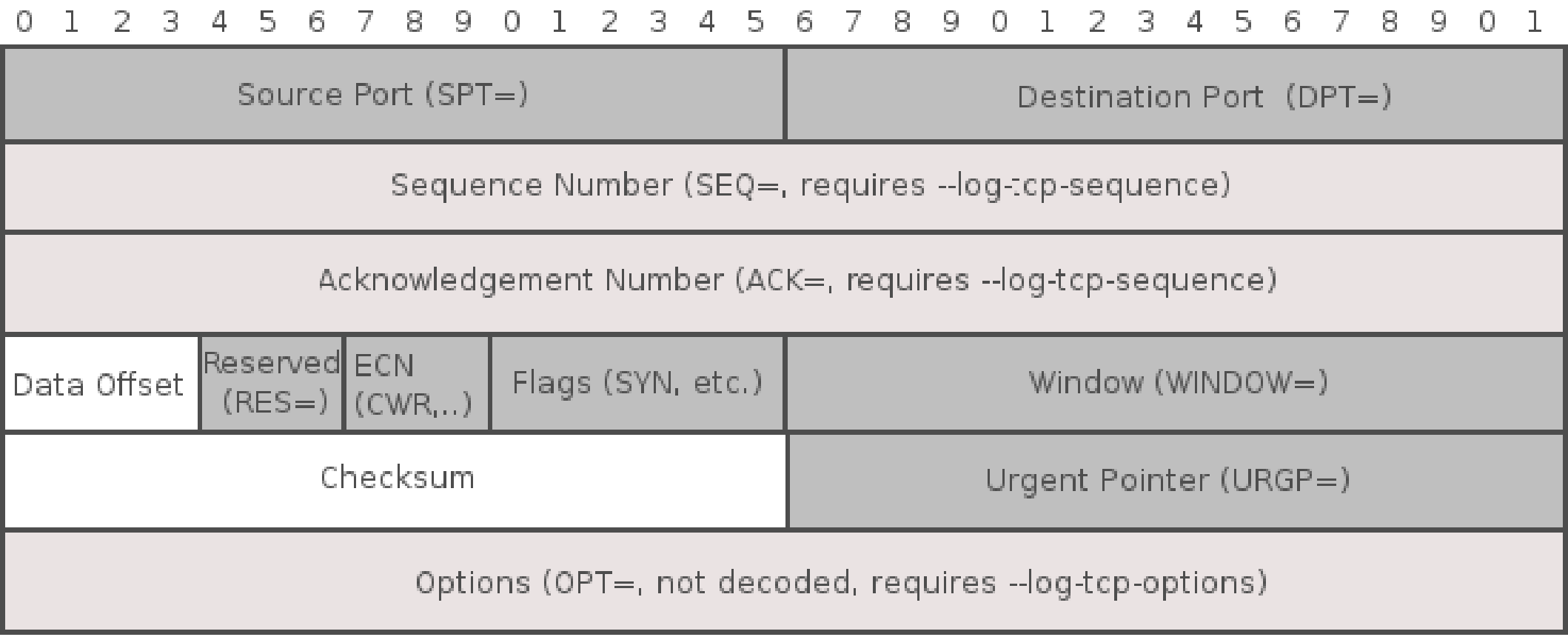
Iptables Log Data

- Graphs will only be as good as the data source permits
- Iptables logs include nearly every interesting field for both the network and transport layer headers – we just need an effective way to parse and then visualize this data
- Iptables log messages can be tied to application layer string matches via the string match extension (see fwsnort)

iptables IP Header Coverage



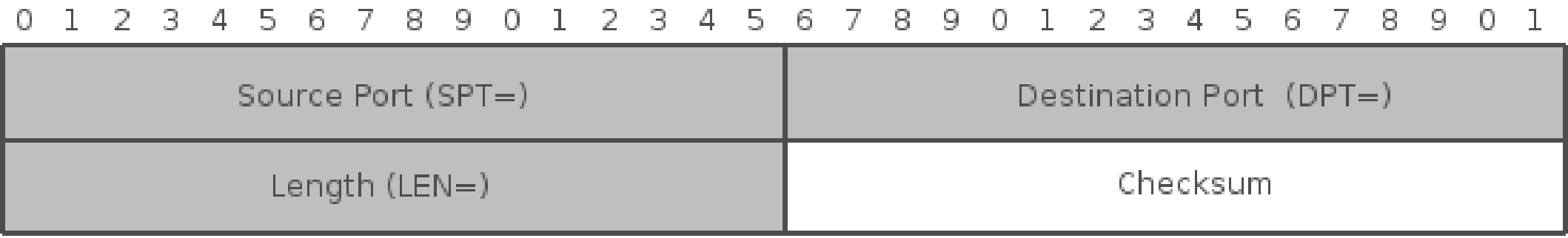
iptables TCP Header Coverage



iptables TCP Log Message

```
Jul 11 20:21:22 minastirith kernel: [199]
SID1361 ESTAB IN=eth1 OUT=
MAC=00:13:d3:38:b6:e4:00:13:46:c2:60:44:08:0
0 SRC=192.168.10.3 DST=192.168.10.1 LEN=60
TOS=0x00 PREC=0x00 TTL=63 ID=11112 DF
PROTO=TCP SPT=28778 DPT=80 WINDOW=5840
RES=0x00 ACK PSH URGP=0 OPT
(0101080A02A041D20CC386B1)
```

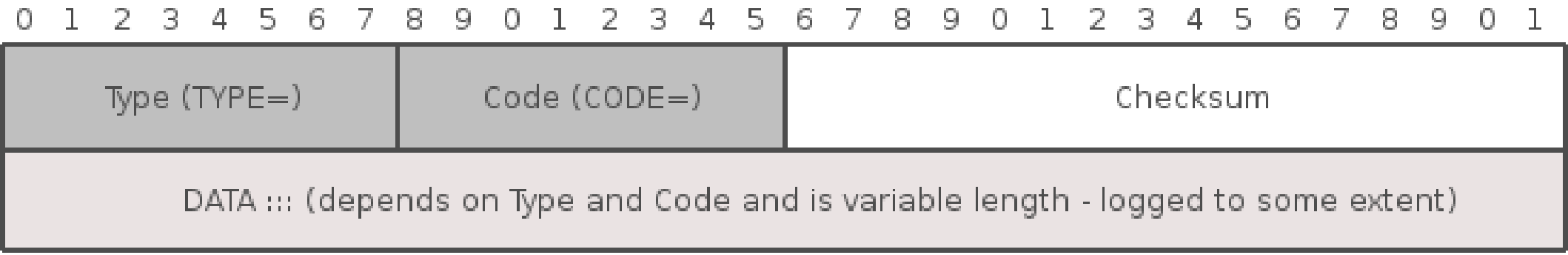
iptables UDP Header Coverage



iptables UDP Log Message

```
Jul 11 20:50:54 minastirith kernel: [153]
SID2001597 IN=eth0 OUT=
MAC=00:13:d3:38:b6:e4:00:13:46:c2:60:44:08:0
0 SRC=192.168.10.3 DST=192.168.10.1 LEN=40
TOS=0x00 PREC=0x00 TTL=63 ID=29758 DF
PROTO=UDP SPT=32046 DPT=61 LEN=20
```

iptables ICMP Header Coverage



iptables ICMP Log Message

```
Jul 11 20:57:18 minastirith kernel: [98]
SID2003294 IN=eth0 OUT=
MAC=00:13:d3:38:b6:e4:00:13:46:c2:60:44:08:0
0 SRC=192.168.10.3 DST=192.168.10.1 LEN=128
TOS=0x00 PREC=0x00 TTL=63 ID=53466
PROTO=ICMP TYPE=8 CODE=0 ID=27459 SEQ=0
```

psad-2.0.8 release

- Interfaces with Gnuplot – parses iptables log data according to header field requirements and builds both a data file and a directives file for Gnuplot
- Various counting modes are supported across different time scales
- Granular requirements on iptables field values (including negation)
- Gnuplot works best with integer data (separated by commas or spaces), so IP addresses need to be translated into integer equivalents

psad-2.0.8 release (cont'd)

- psad --gnuplot command line arguments:

  --gnuplot-graph-style - “points”, “dots”, “linespoints”

  --gnuplot-file-prefix - <file>.gnu, <file>.dat, <file>.png

  --gnuplot-title – Graph title (used for psad command line)

  --gnuplot-sort-style – time sorting vs. value sorting

  --gnuplot-3D – Use “splot” for three-dimensional viewing

  --gnuplot-view – Set viewing angle

The Honeynet Scan34 Data Set

- The goal of a Honeynet is to collect data on real compromises – packet traces and log data is an excellent learning tool
- Over 170,000 lines of iptables log data in the Scan34 challenge – covers a five week period
- Contains evidence of port scans, port sweeps, worm traffic (Slammer, Nachi), and an outright compromise of a system – we will visualize these graphically
- All IP addresses are sanitized to 11.11.0.0/16
- http://www.honeynet.org/

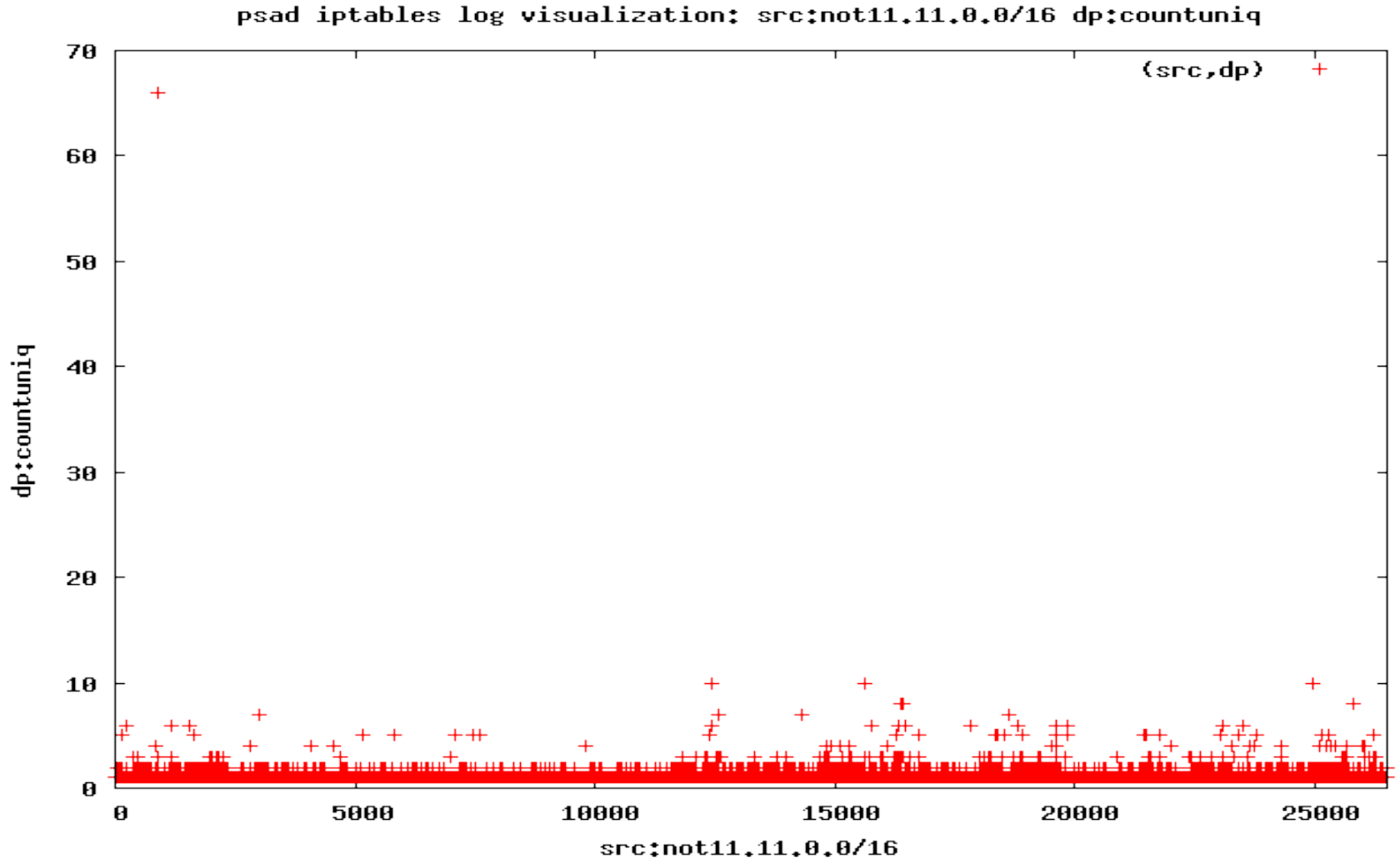
Port Scans

- Packets to many different ports from a single source address
- Not just SYN packets, think of Nmap -sF, -sN, -sX, -sA, (also -sU for UDP)
- Visualize with IP address vs. the number of packets to unique ports

psad Command

```
psad -m iptables.data --gnuplot --
CSV-fields "src:not11.11.0.0/16
dp:countuniq" --gnuplot-graph points
--gnuplot-xrange 0:26500 -gnuplot-
file-prefix portscan
```

Visualizing Port Scans (IP vs. Packet Count to Unique Ports)



psad Gnuplot data files

Generated by psad v2.0.8 (file revision: 2092)

Command line: 'psad -m iptables.data --gnuplot --CSV-fields src:not11.11.0.0/16 dp:countuniq --gnuplot-graph points --gnuplot-xrange 0:26500 --gnuplot-file-prefix portscan --use-store portscan.store'

Time stamp: Sun Jul 8 13:43:28 2007

905, 66 ### 905=60.248.80.102

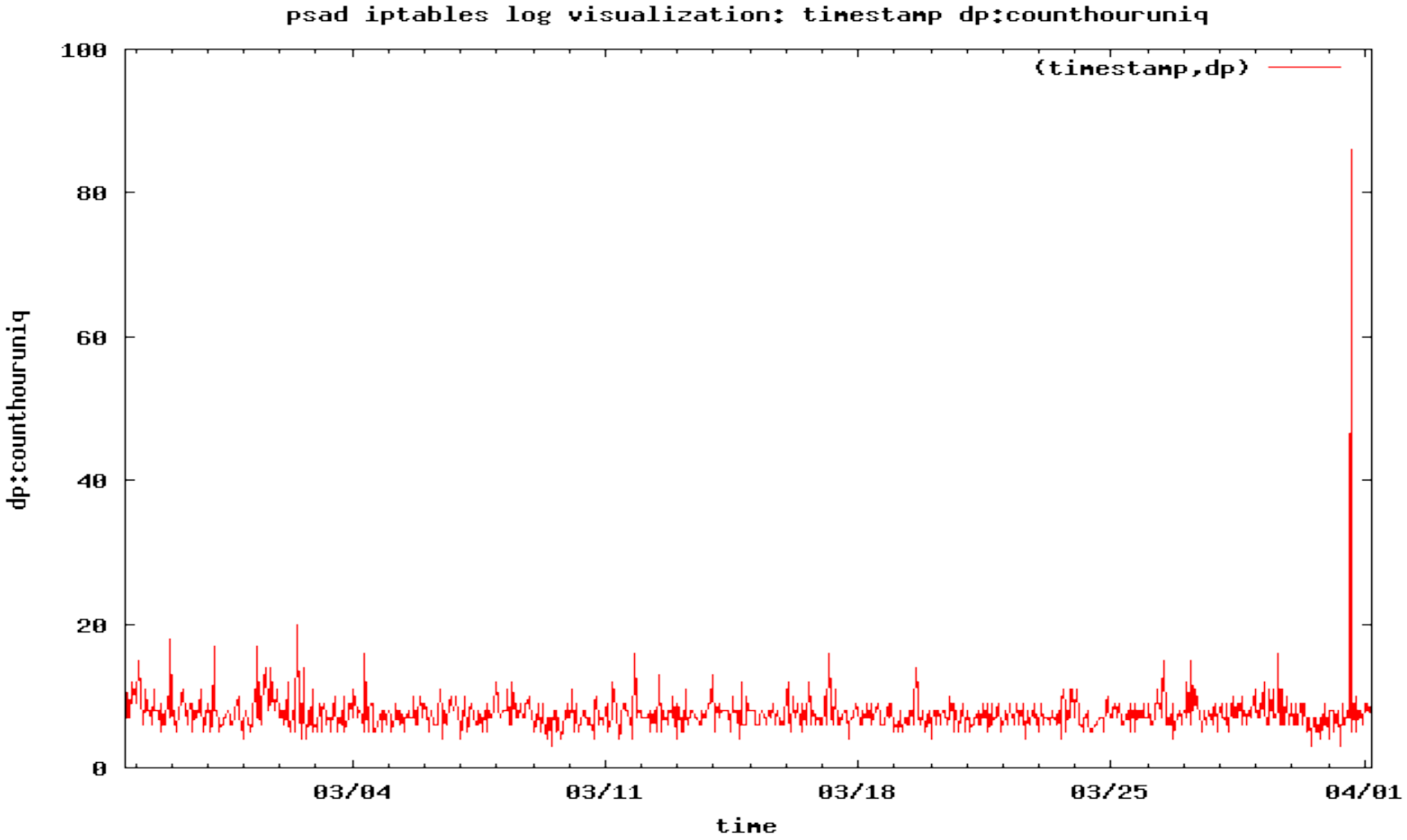
12415, 10 ### 12415=63.135.2.15

15634, 10 ### 15634=63.186.32.94

24950, 10 ### 24950=218.85.9.143

16374, 8 ### 16374=63.204.104.150

When Did the Heaviest Scan Occur?



psad Analysis of Scanner: 60.248.80.102

psad -m iptables.data -A --analysis-fields "**src:60.248.80.102**"

SRC: 60.248.80.102, DL: 2, Dsts: 1, Pkts: 67, Unique sigs: 3

DST: 11.11.79.125

Scanned ports: UDP 7-43981, Pkts: 53, Chain: FORWARD, Intf: br0

Scanned ports: TCP 68-32783, Pkts: 14, Chain: FORWARD, Intf: br0

Signature match: "POLICY vncviewer Java applet download attempt"

TCP, Chain: FORWARD, Count: 1, DP: 5802, SYN, Sid: 1846

Signature match: "PSAD-CUSTOM Slammer communication attempt"

UDP, Chain: FORWARD, Count: 1, DP: 1434, Sid: 100208

Signature match: "RPC portmap listing UDP 32771"

UDP, Chain: FORWARD, Count: 1, DP: 32771, Sid: 1281

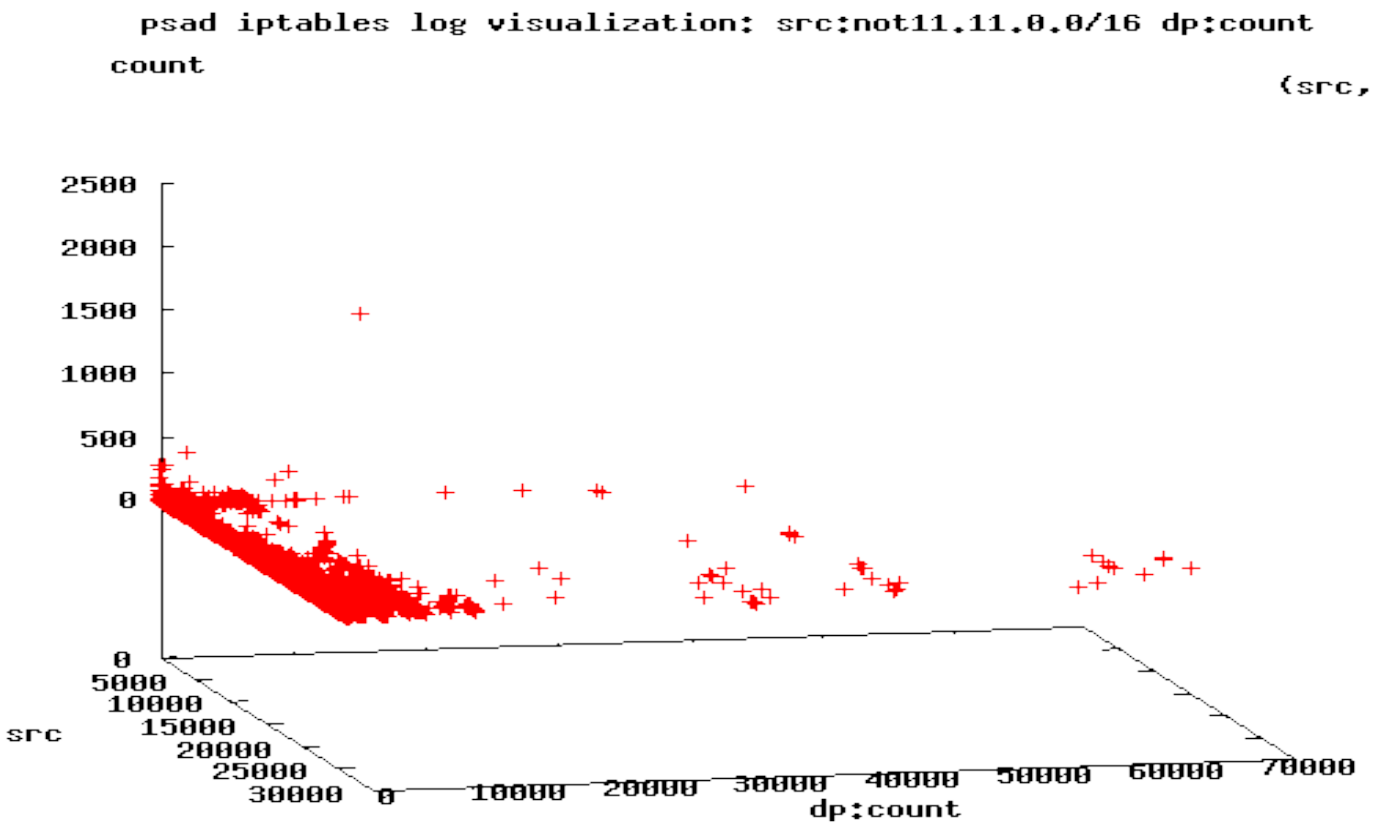
Port Sweeps

- Packets to a single port number across many hosts
- Good evidence of an automated worm (or human) that can exploit a specific vulnerability in a particular service
- Visualize with external IP addresses vs. destination ports vs. packet count

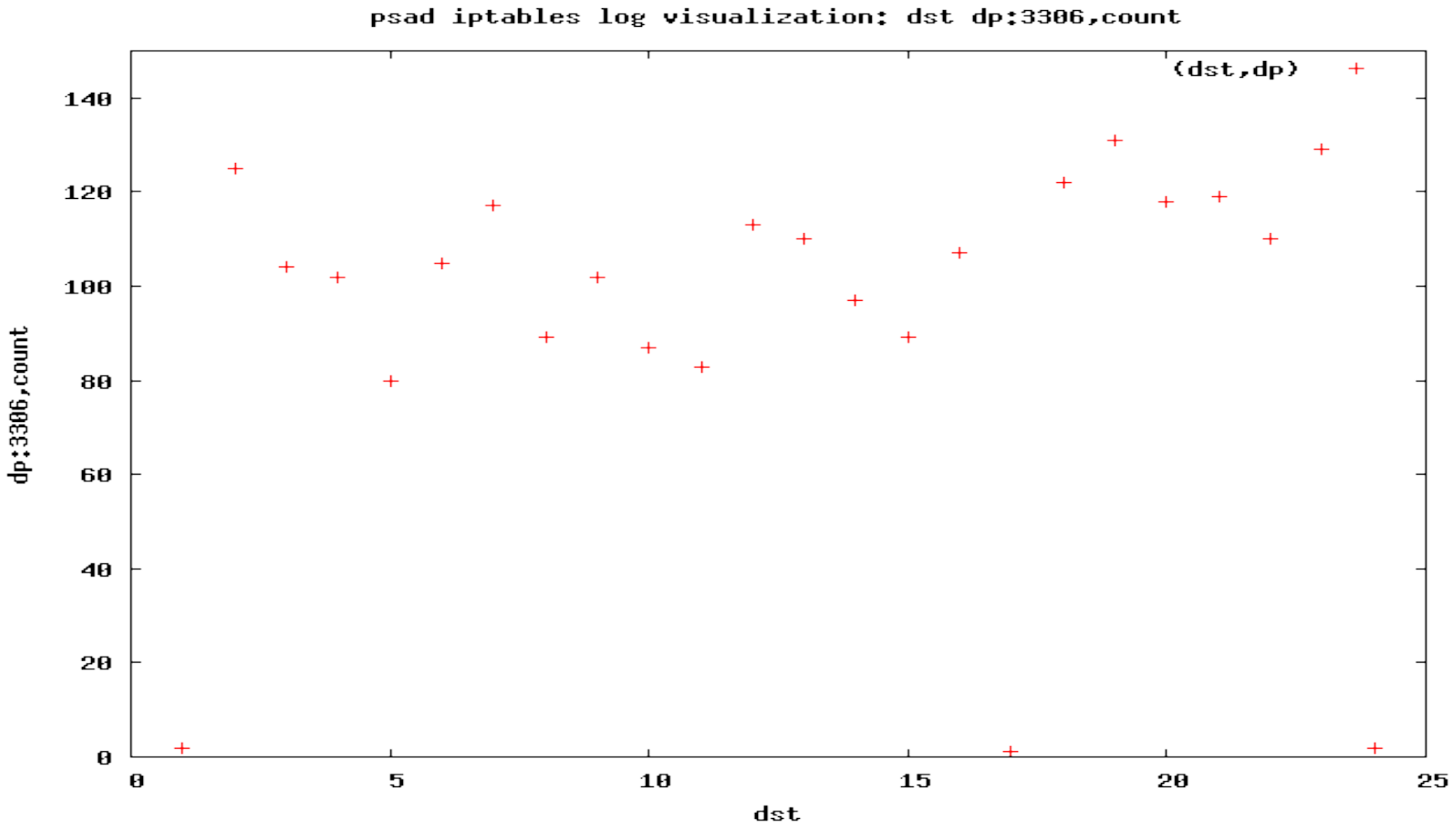
psad Command

```
psad -m iptables.data --gnuplot --
CSV-fields "src:not11.11.0.0/16
dp:count" --gnuplot-graph points --
gnuplot-3d --gnuplot-view 74,77 --
gnuplot-file-prefix portsweep
```

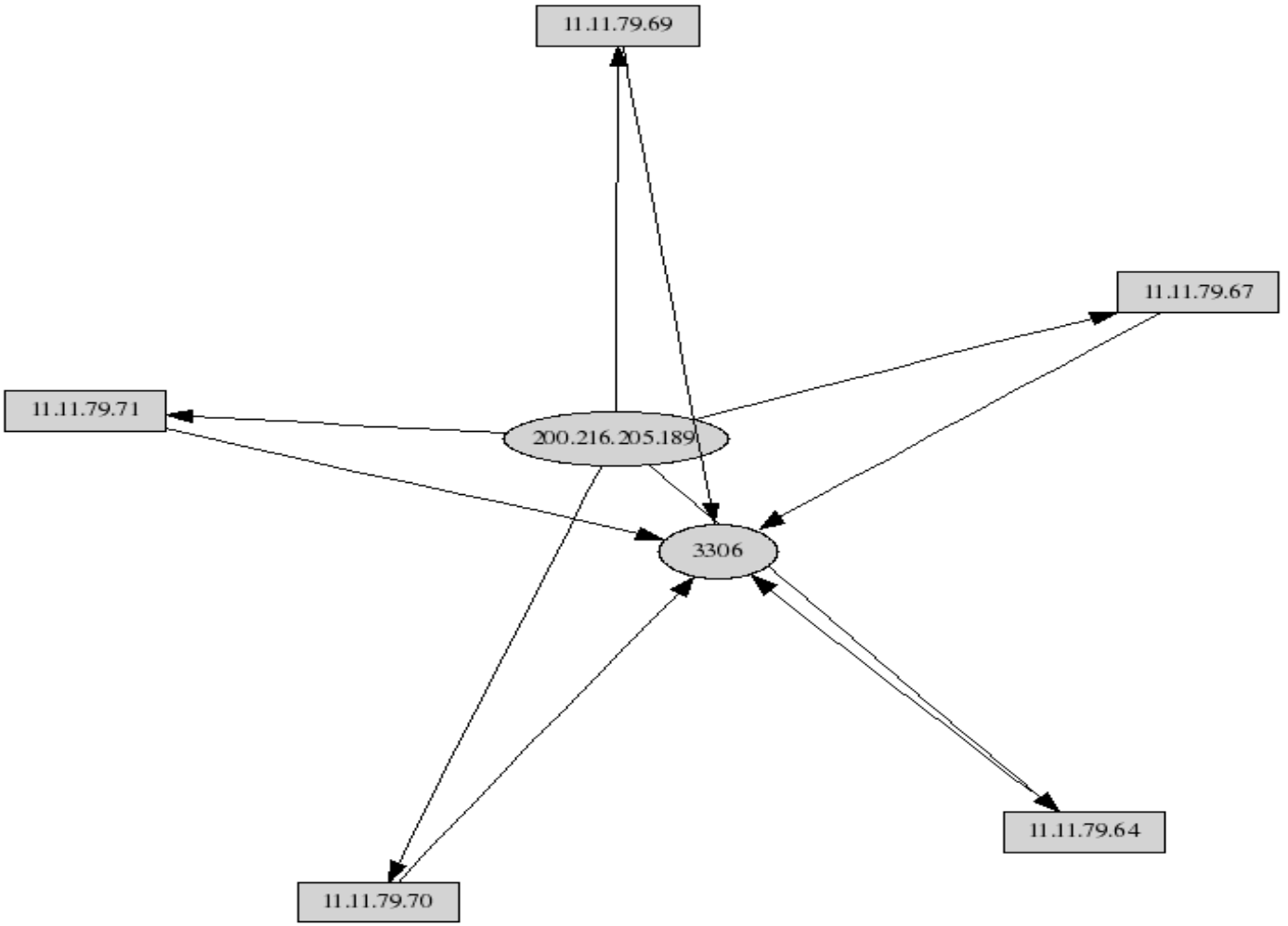
Visualizing Port Sweeps (IP vs. Destination Port vs. Packet Count)



The Top Port Sweeper: 200.216.205.189 vs. TCP/3306



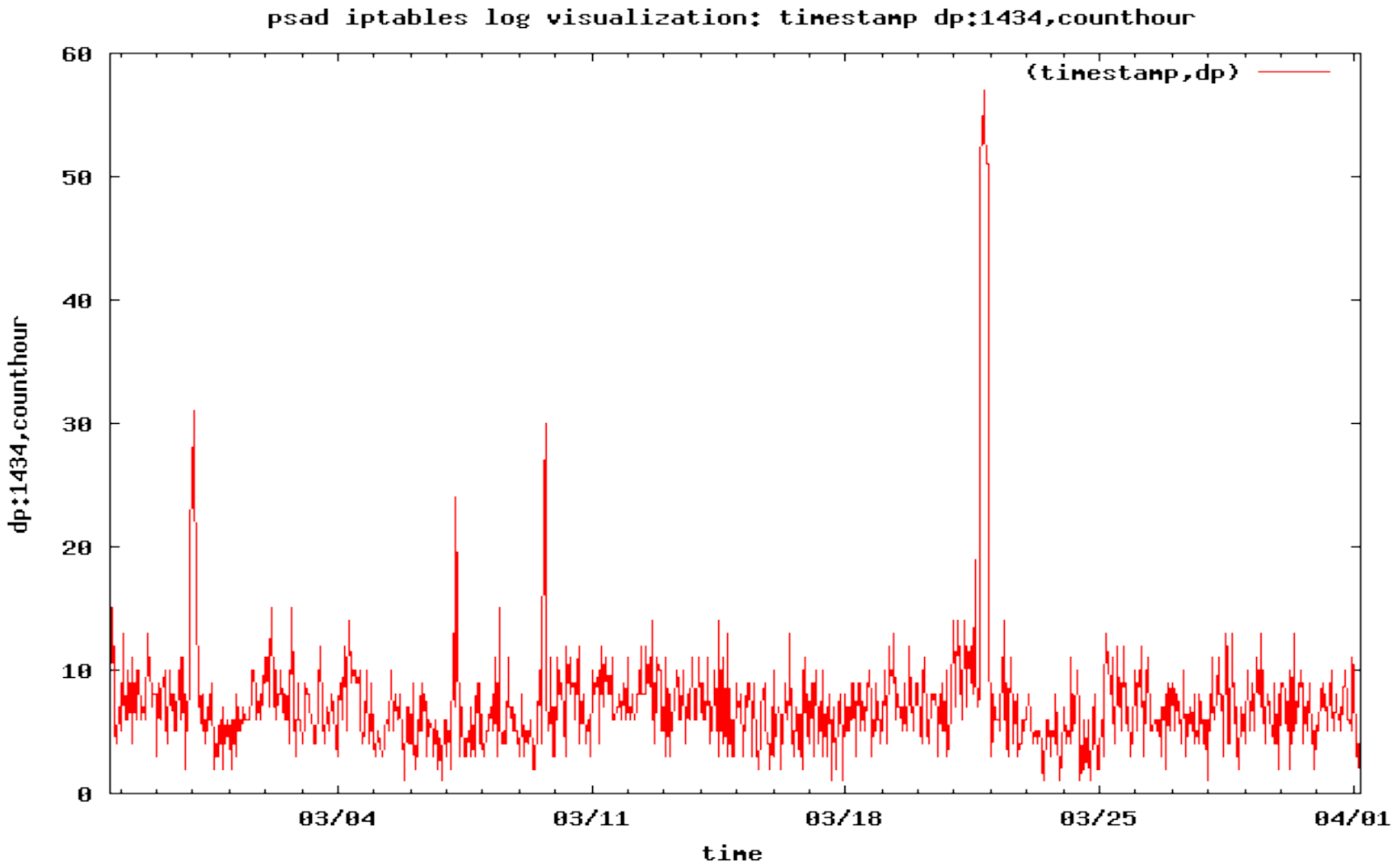
The Top Port Sweeper (Link Graph)



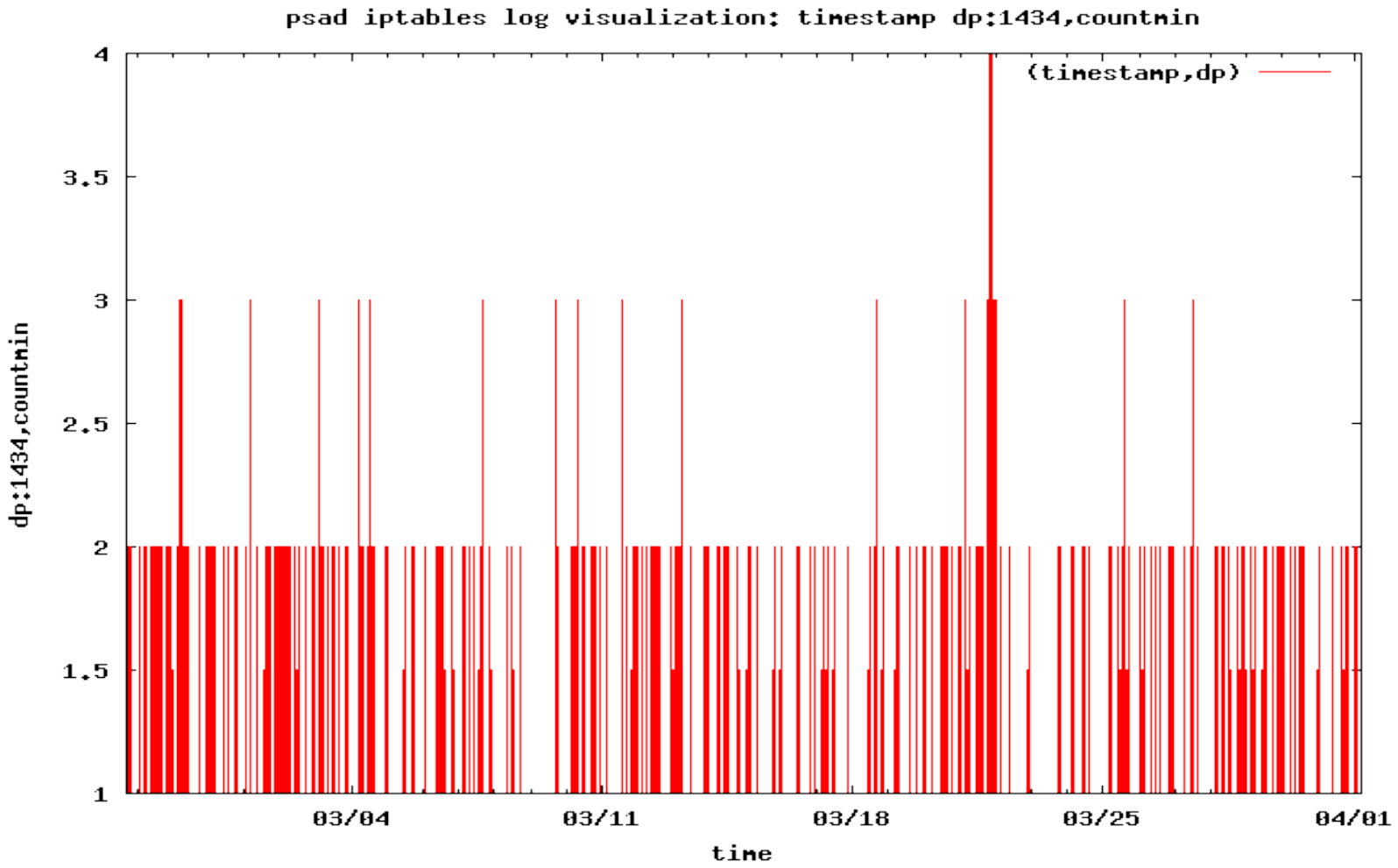
Slammer Worm

- Exploited a vulnerability in MS SQL Server 2000
- Single 404-byte UDP packet to port 1434
- One of the fastest spreading worms in history
- Can easily be spoofed – useless to return ICMP port unreachable with your IDS; need to block the packet with an IPS and patch the vulnerability

Visualizing the Slammer Worm (UDP 404-byte Packets vs. Hours)



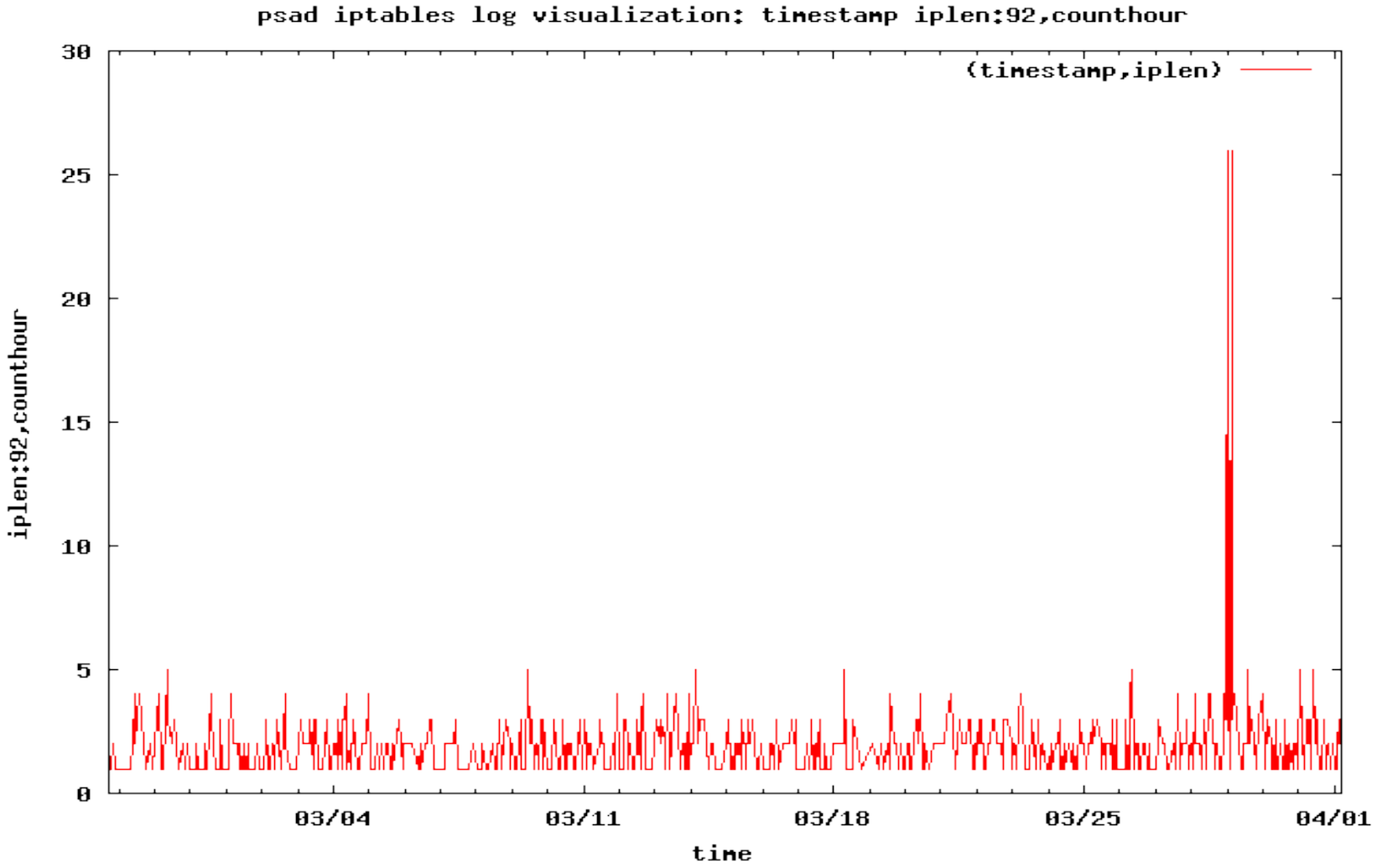
Visualizing the Slammer Worm (UDP 404-byte Packets vs. Minutes)

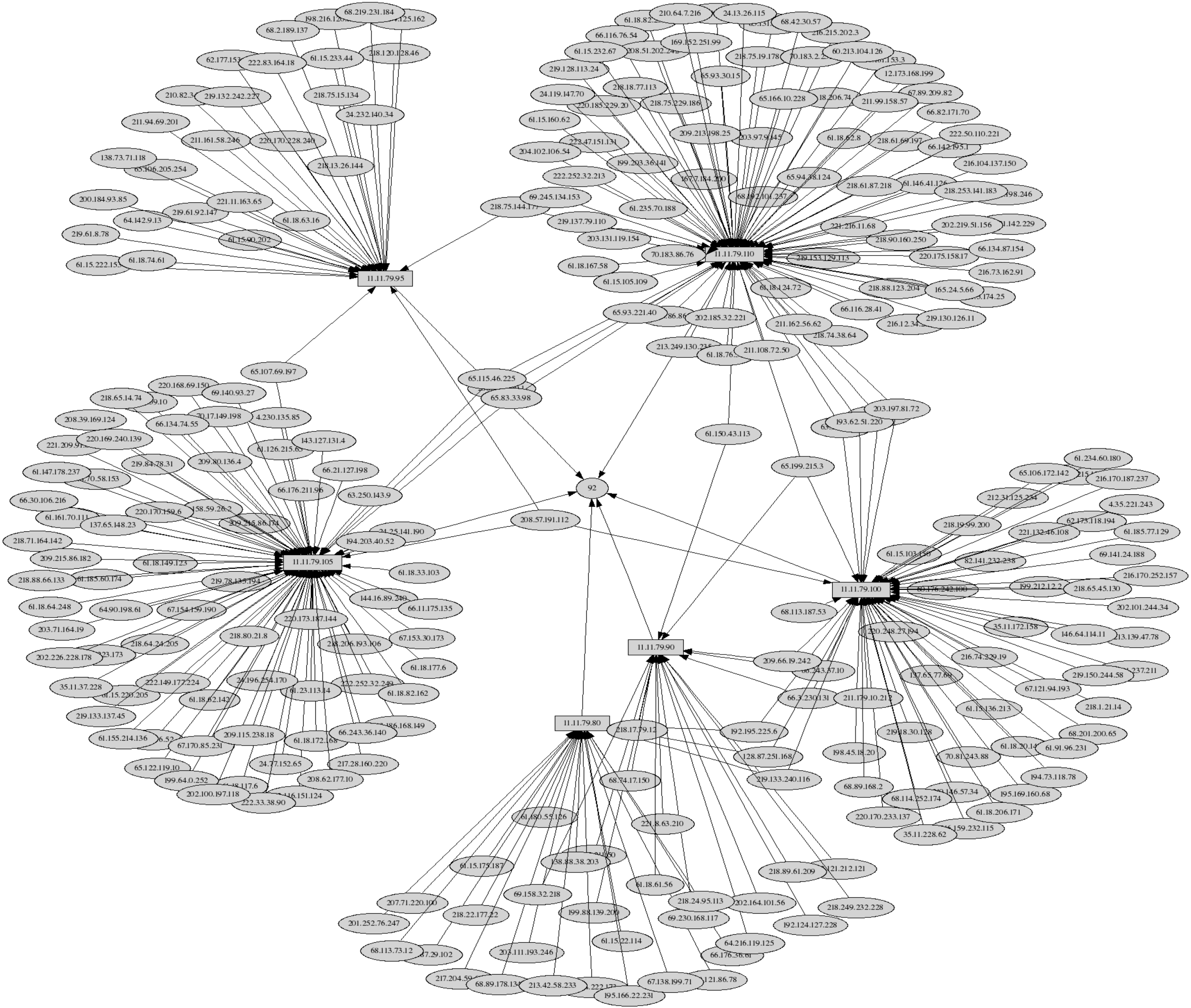


Nachi Worm

- Exploits Windows 2000 and XP systems that are not patched against the MS03-026 vulnerability
- Always sends a 92-byte ICMP echo request to a target system before attempting to exploit the vulnerability
- This ICMP packet makes the worm easy to detect

Nachi Worm (92-Byte ICMP Packet vs. Hours)

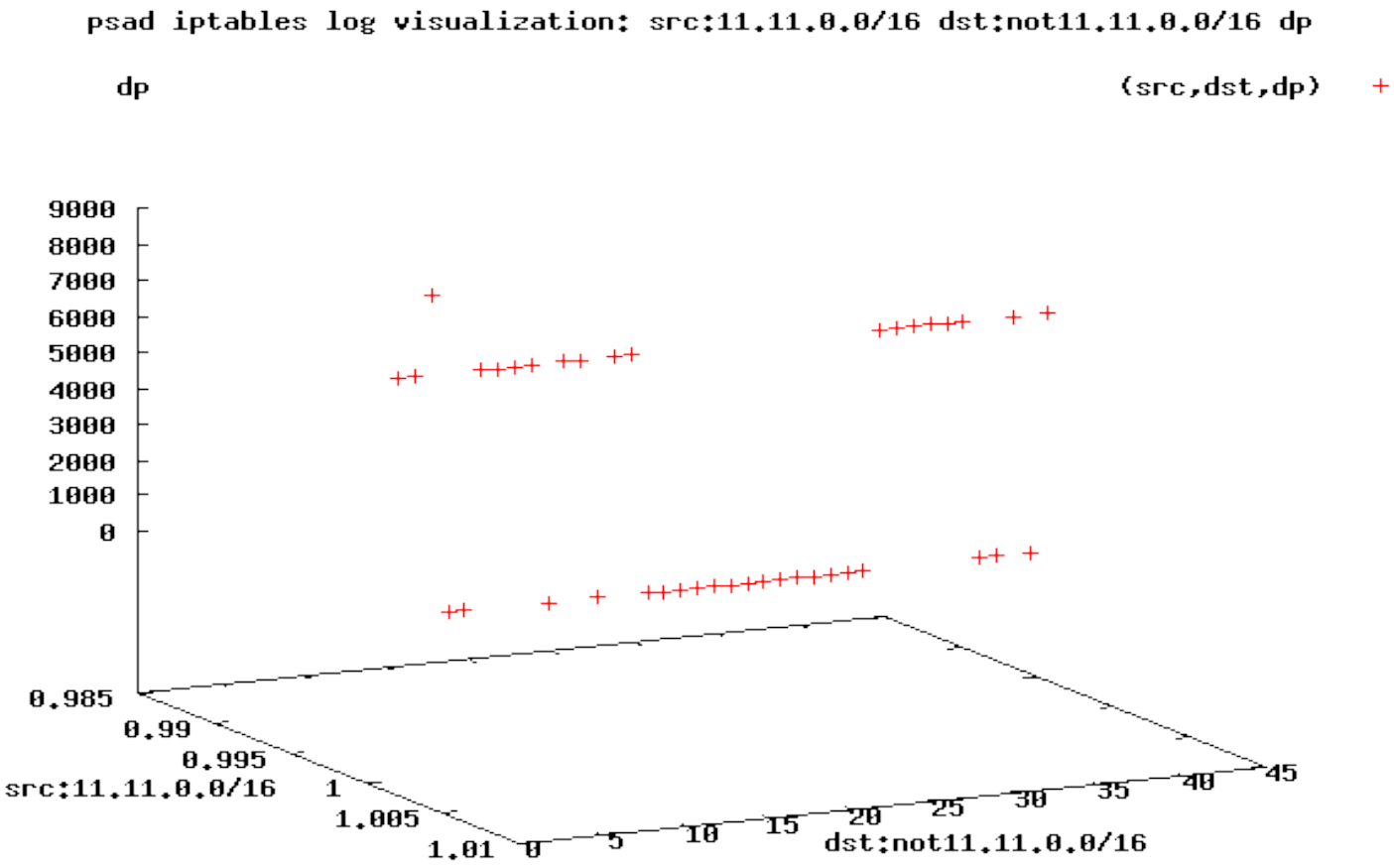


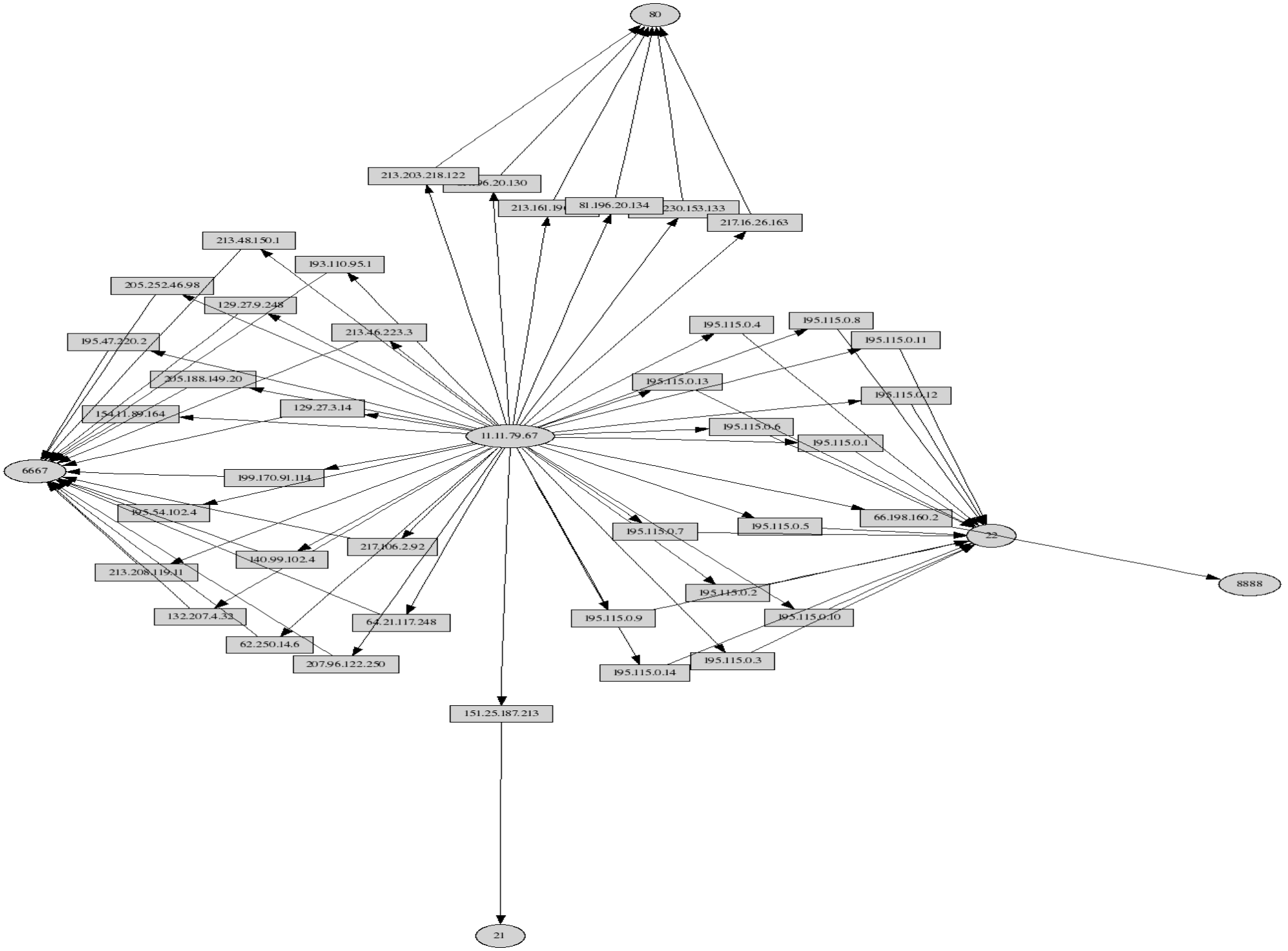

11.11.79.95
11.11.79.110
11.11.79.105
11.11.79.100
11.11.79.90
11.11.79.80
92
65.107.69.197
65.115.46.225
65.83.33.98
65.93.221.40
202.185.32.221
213.249.130.235
211.108.72.50
61.150.43.113
65.199.215.3
193.62.51.220
203.197.81.72
208.57.191.112
194.203.40.52
63.250.143.9
218.75.144.177
69.245.134.153
209.66.19.242
66.3.230.131
192.195.225.6
128.87.251.168
219.133.240.116
218.17.79.12
68.74.17.150

Detecting A Compromised System with Outbound Connections

- Honeynet systems should not make outbound connections to external networks (except for administrative or reporting communication with known addresses)
- SSH and IRC connections are particularly suspicious

Outbound Connections



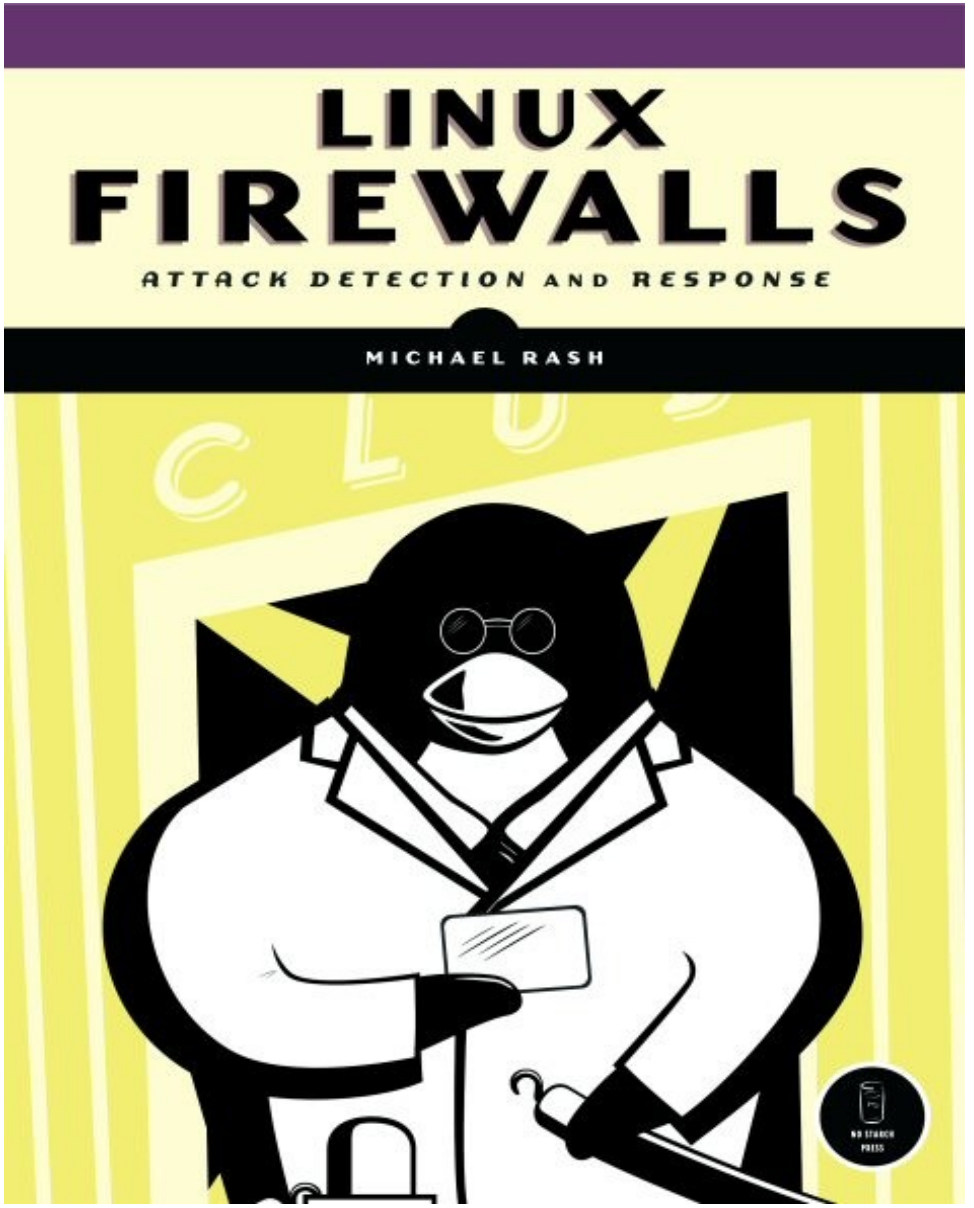

80
213.203.218.122
81.196.20.134
217.16.26.163
213.48.150.1
193.110.95.1
205.252.46.98
129.27.9.248
213.46.223.3
195.47.220.2
195.188.149.20
154.11.89.164
129.27.3.14
11.11.79.67
6667
199.170.91.114
195.54.102.4
217.106.2.92
140.99.102.4
213.208.119.11
132.207.4.33
64.21.117.248
62.250.14.6
207.96.122.250
151.25.187.213
21
195.115.0.4
195.115.0.8
195.115.0.11
195.115.0.13
195.115.0.12
195.115.0.6
195.115.0.1
66.198.160.2
195.115.0.5
195.115.0.7
22
8888
195.115.0.2
195.115.0.9
195.115.0.10
195.115.0.3
195.115.0.14

Iptables Logging Args

- When building iptables LOG rules:
  - Use --log-ip-options
  - Use --log-tcp-sequence
  - Use --log-tcp-options
  - More attacks can be detected, and operating systems can be passively fingerprinted

3D Graphing Demo...

No Starch Press, Sept 2007



Questions?

http://www.cipherdyne.org/

mbr@cipherdyne.org