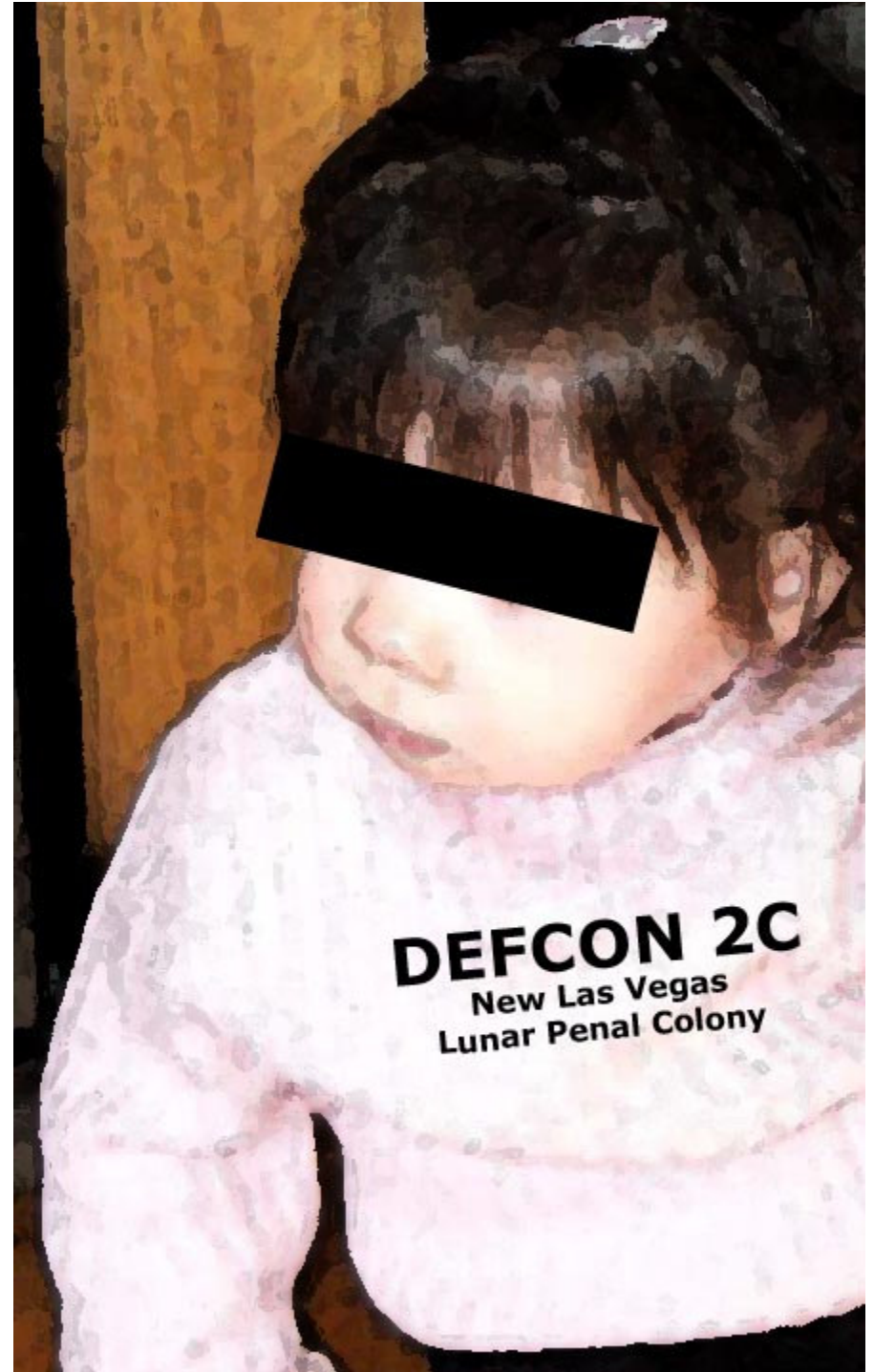


Network Attack Visualization

Greg Conti

www.cc.gatech.edu/~conti



Disclaimer



The views expressed in this presentation are those of the author and do not reflect the official policy or position of the United States Military Academy, the Department of the Army, the Department of Defense or the U.S. Government.

information visualization is the use of interactive, sensory representations, typically visual, of abstract data to reinforce cognition.

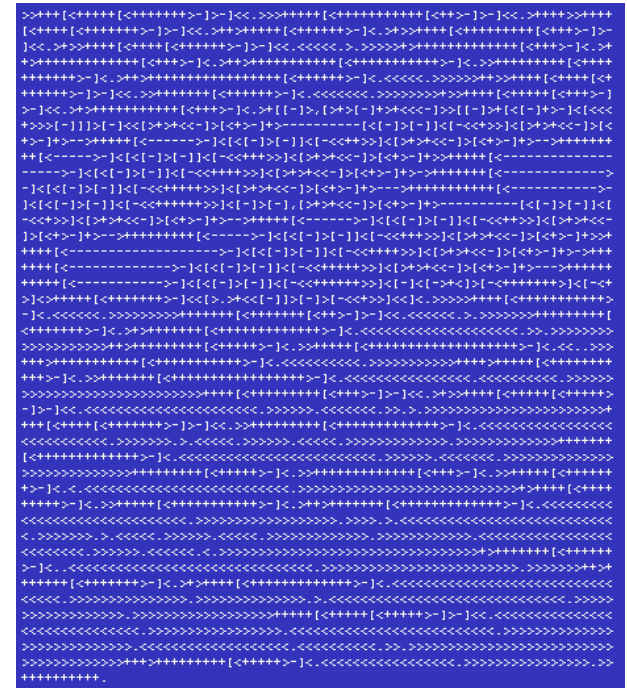
An Art Survey...



A



B




C

<http://www.clifford.at/cfun/progex/>
<http://www.muppetlabs.com/~breadbox/bf/>
<http://www.geocities.com/h2lee/ascii/monalisa.html>
http://www.artinvest2000.com/leonardo_gioconda.htm
































Why InfoVis?

- Helps find patterns
- Helps reduce search space
- Aids efficient monitoring
- Enables interaction (what if)
- Help prevent overwhelming the user

 new thread

Threads in Forum: Pre-Defcon 12

Forum Tools ▾ Search this Forum ▾

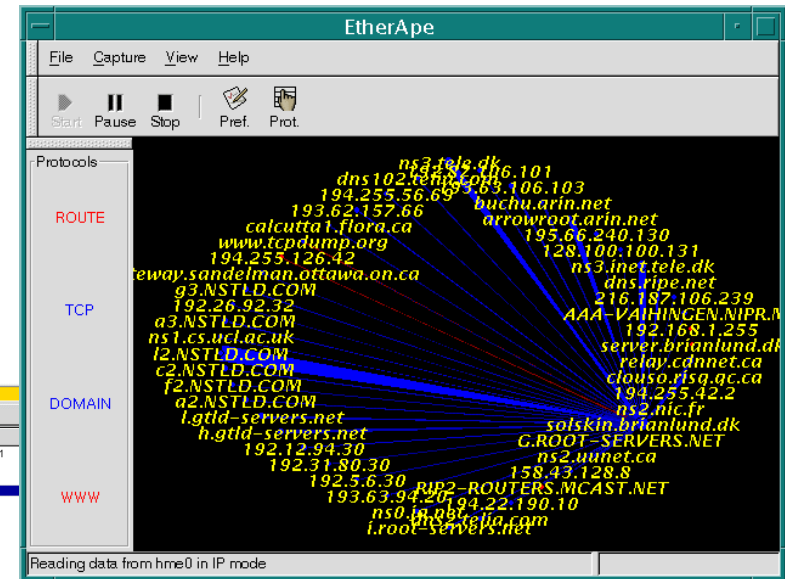
	Thread / Thread Starter	Rating	Last Post <input checked="" type="checkbox"/>	Replies	Views
	Sticky: DEF CON 12 [UNOFFICIAL] Toxic BBQ ( 1 2) converge		05-08-2004 12:28 AM by hackajar 	15	418
	Sticky: DEF CON 12 Homebrew IP Appliance Contest Announced Neural		04-23-2004 11:11 PM by Neural 	8	235
	Sticky: DEF CON 12 WarDriving Contest Announced Chris		04-17-2004 03:58 PM by Thorn 	5	214
	Sticky: DEF CON 12 Slogan Contest Chris		04-14-2004 03:35 PM by Chris 	3	340
	Sticky: All New Users: Read this BEFORE posting! Grifter		02-29-2004 08:09 PM by Grifter 	0	465
	 need advice on getting company to send me Guipo		Yesterday 05:43 AM by phobal 	9	126
	 AP sold out; chances of picking up cancellation? euro12		05-08-2004 04:37 PM by Contrarian 	11	126
	Don't Forget Howard Johnson hackajar		05-08-2004 04:22 PM by Zhym 	9	148
	Anyone know the area? Rebourne		05-08-2004 02:03 AM by HyperCityGirl 	12	130
	Who's bringing homebrews? skroo		05-07-2004 05:07 PM by h3adrush 	12	128
	Ironic timing for the "Official Star Trek Con" ( 1 2) Xodia		05-07-2004 04:43 AM by alkloyd 	26	453

So What?

- Go Beyond the Algorithm
- Help with detecting and understand some 0day attacks
- Make CTF and Root Wars a Spectator Sport
- Help find insider threats
- Stealth might not be so stealthy
- Help visually fingerprint attacks/tools

What tasks do you need help with?

Packet Capture Visualizations



EtherApe

The Ethernet Network Analyzer

No	Time	Source	Destination	Protocol	Info
1	0.000000	00:80:c8:11:b4:e1	ff:ff:ff:ff:ff:ff	ARP	Who has 192.168.1.2? Tell 192.168.1.1
2	0.000400	00:80:c8:33:1e:56	00:80:c8:11:b4:e1	ARP	192.168.1.2 is at 00:80:c8:33:1e:56
3	0.000446	uranus.beaupyrat.com	192.168.1.2	ICMP	Echo (ping) request
4	0.000690	192.168.1.2	uranus.beaupyrat.com	TCP	Echo (ping) reply
5	0.007376	uranus.beaupyrat.com	192.168.1.2	ICMP	Echo (ping) request
6	0.009473	192.168.1.2	uranus.beaupyrat.com	ICMP	Echo (ping) reply
7	96.726932	192.168.1.2	192.168.1.255	SMB	SMBtrans Response
8	246.703934	192.168.1.2	192.168.1.255	SMB	SMBtrans Response

Frame (98 on wire, 98 captured)
 -Arrival Time: Feb 24, 2000 00:16:57.4314
 -Time delta from previous packet: 0.000490 seconds
 -Frame Number: 4
 -Packet Length: 98 bytes
 -Capture Length: 98 bytes

```

0000 00 80 c8 11 b4 e1 00 80 c8 33 1e 56 00 45 00  ....V.V.E.
0010 00 54 6e 00 00 80 01 49 55 c0 a8 01 02 c0 a8  .Th....IU.....
0020 01 01 00 00 26 c5 44 03 00 00 69 6a b4 38 86 91  ...&.D...1j.8...
0030 06 00 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15  ....&.....fM88
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25  ....&.....fM88
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35  8(*)4.....7012345
0060 36 37
  
```

```

#4dos
16:27:55.327570 137.133.57.68.1040 > 137.133.24.8.1352: tcp 0 CDF
16:27:55.330774 209.1.224.18.www-http > 137.133.57.68.1255: tcp 5
16:27:55.336912 209.1.224.18.www-http > 137.133.57.68.1255: tcp 0
16:27:55.348174 137.133.57.68.1255 > 209.1.224.18.www-http: tcp 0
16:27:55.343677 209.1.224.18.www-http > 137.133.57.68.1255: tcp 5
16:27:55.437533 209.1.224.18.www-http > 137.133.57.68.1255: tcp 4
16:27:55.440488 137.133.57.68.1255 > 209.1.224.18.www-http: tcp 0
16:27:55.444033 209.1.224.18.www-http > 137.133.57.68.1255: tcp 1
16:27:55.447087 137.133.57.68.1255 > 209.1.224.18.www-http: tcp 0
16:27:55.450144 209.1.224.18.www-http > 137.133.57.68.1255: tcp 1
16:27:55.456636 137.133.57.68.1255 > 209.1.224.18.www-http: tcp 0 CDF
16:27:55.457583 209.1.224.18.www-http > 137.133.57.68.1255: tcp 1160
16:27:55.460751 137.133.57.68.1255 > 209.1.224.18.www-http: tcp 0 CDF
16:27:55.477792 137.133.16.54.32793 > 137.133.53.36.1798: tcp 147 CDF
16:27:55.481254 209.1.224.18.www-http > 137.133.57.68.1255: tcp 592
16:27:55.484685 209.1.224.18.www-http > 137.133.57.68.1255: tcp 616
16:27:55.487087 137.133.57.68.1255 > 209.1.224.18.www-http: tcp 0 CDF
16:27:55.490866 137.133.63.36.1730 > 137.133.16.54.32793: tcp 0 CDF
16:27:55.493980 209.1.224.18.www-http > 137.133.57.68.1255: tcp 1160
16:27:55.497088 209.1.224.18.www-http > 137.133.57.68.1255: tcp 1160
16:27:55.4991367 137.133.57.68.1255 > 209.1.224.18.www-http: tcp 0 CDF
16:27:55.499454 209.1.224.18.www-http > 137.133.57.68.1255: tcp 1112
16:27:55.527222 209.1.224.18.www-http > 137.133.57.68.1255: tcp 0 CDF
16:27:56.000966 137.133.63.36.33272 > 137.133.16.54.1798: tcp 147 CDF
16:27:56.004058 137.133.63.36.32789 > 137.133.16.53.1798: tcp 147 CDF
16:27:56.207253 nra-x.lac-srv > nra-x.lac-srv: udp 284
16:27:56.210769 nra-x.lac-srv > nra-x.lac-srv: udp 192
16:27:56.213192 209.1.224.18.www-http > 137.133.57.68.1255: tcp 664
16:27:56.216689 209.1.224.18.www-http > 137.133.57.68.1255: tcp 894
16:27:56.219818 137.133.57.68.1255 > 209.1.224.18.www-http: tcp 0 CDF
16:27:56.222877 209.1.224.18.www-http > 137.133.57.68.1255: tcp 326
16:27:56.218061 209.1.224.18.www-http > 137.133.57.68.1255: tcp 1160
16:27:56.321065 137.133.57.68.1255 > 209.1.224.18.www-http: tcp 0 CDF
16:27:56.324244 209.1.224.18.www-http > 137.133.57.68.1255: tcp 1106
16:27:56.327222 209.1.224.18.www-http > 137.133.57.68.1255: tcp 678
16:27:56.330206 137.133.57.68.1255 > 209.1.224.18.www-http: tcp 0 CDF
16:27:56.333267 209.1.224.18.www-http > 137.133.57.68.1255: tcp 708
16:27:56.420800 137.133.57.68.1255 > 209.1.224.18.www-http: tcp 0 CDF
16:27:56.530872 209.1.224.18.www-http > 137.133.57.68.1255: tcp 460
16:27:56.541090 209.1.224.18.www-http > 137.133.57.68.1255: tcp 1160
16:27:56.544893 209.1.224.18.www-http > 137.133.57.68.1255: tcp 0 CDF
16:27:56.648239 209.1.224.18.www-http > 137.133.57.68.1255: tcp 1160
16:27:56.651262 209.1.224.18.www-http > 137.133.57.68.1255: tcp 616
16:27:56.654247 137.133.57.68.1255 > 209.1.224.18.www-http: tcp 0 CDF
16:27:56.657292 209.1.224.18.www-http > 137.133.57.68.1255: tcp 1160
16:27:56.660425 209.1.224.18.www-http > 137.133.57.68.1255: tcp 911
16:27:56.663376 137.133.57.68.1255 > 209.1.224.18.www-http: tcp 0 CDF
tcpdump 3.5 Eth: 139 <139>
  
```

TCP Dump

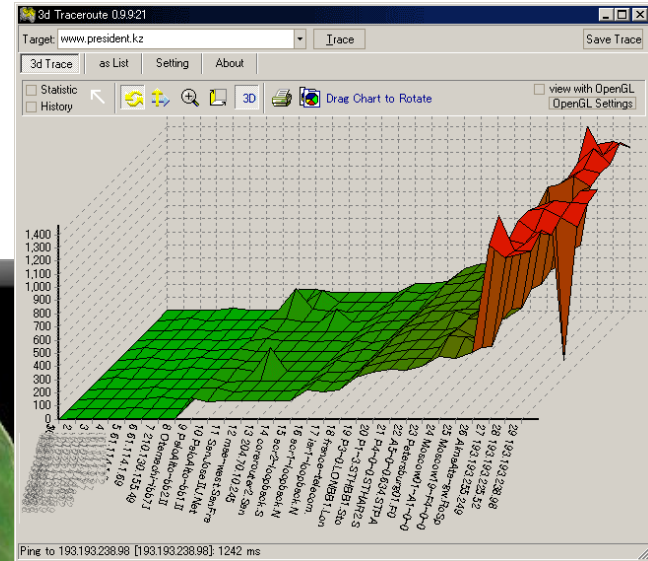
Ethereal

Tcpdump image: <http://www.bgnett.no/~giva/pcap/tcpdump.png>
 TCPDump can be found at <http://www.tcpdump.org/>

Ethereal image: <http://www.linux-france.org/prj/edu/archinet/AMSI/index/images/ethereal.gif>
 Ethereal by Gerald Combs can be found at <http://www.ethereal.com/>

EtherApe image: <http://www.solaris4you.dk/sniffersSS.html>
 Etherape by Juan Toledo can be found at <http://etherape.sourceforge.net/>

traceroute Visualizations



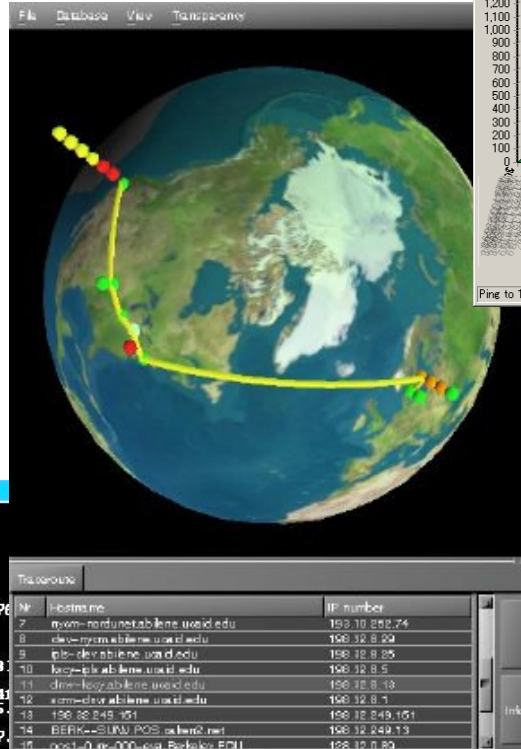
3D TraceRoute

```
C:\WINNT\System32\command.com
C:\>tracert jefferysanders.com

Tracing route to jefferysanders.com [66.218.65.125]
over a maximum of 30 hops:
  0  1 ms    1 ms    1 ms    192.168.0.1
  1  12 ms   13 ms   14 ms   cdn-66-105-1-pine.cox-internet.com [66.218.65.125]
  2  15 ms   15 ms   16 ms   172.16.110.1
  3  20 ms   18 ms   18 ms   12.119.71.133
  4  26 ms   25 ms   26 ms   gbr2-p59.hstx.ip.att.net [12.123.212.18]
  5  29 ms   33 ms   30 ms   gbr3-p40.dlstx.ip.att.net [12.122.2.97]
  6  30 ms   27 ms   31 ms   ggr1-p360.dlstx.ip.att.net [12.123.16.24]
  7  29 ms   30 ms   29 ms   pos1-3.core1.Dallas1.Level3.net [209.245.1.1]
  8  29 ms   31 ms   29 ms   so-4-0-0.mp2.Dallas1.Level3.net [209.247.1.1]
  9  69 ms   70 ms   69 ms   so-3-0-0.mp2.SanJose1.Level3.net [64.159.1.130]
 10  71 ms   71 ms   69 ms   gige10-0.ipcolo4.SanJose1.Level3.net [64.159.2.4]
 11  70 ms   71 ms   70 ms   cust-int.level3.net [64.152.69.18]
 12  69 ms   72 ms   73 ms   ge-1-3-0.ms1.pao.yahoo.com [216.115.100.150]
 13  72 ms   71 ms   73 ms   v110.hasi.scd.yahoo.com [66.218.64.134]
 14  71 ms   72 ms   71 ms   puebl.geo.vip.scd.yahoo.com [66.218.65.125]

Trace complete.
```

basic traceroute/tracert



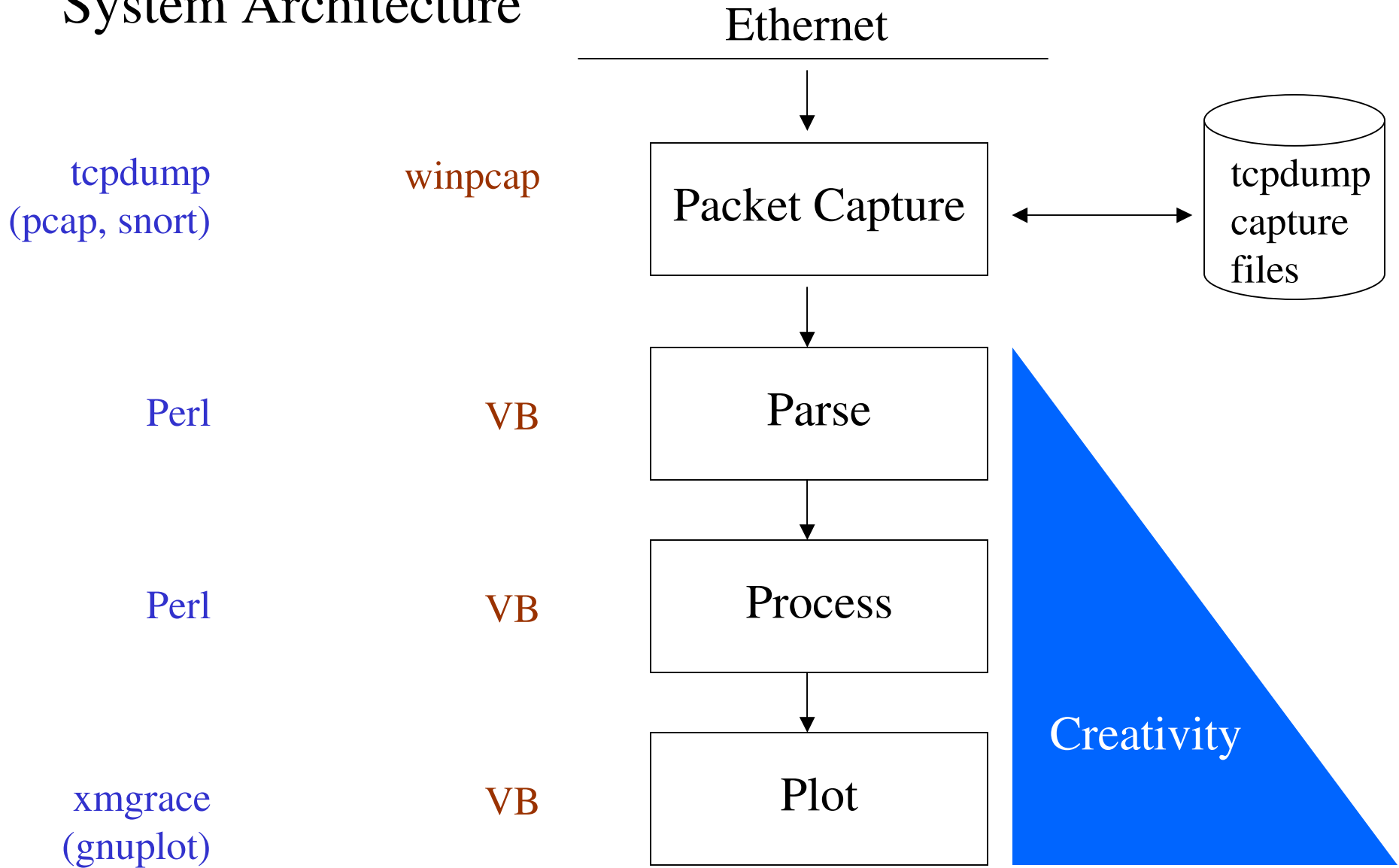
Xtraceroute

3D TraceRoute Developer: <http://www.hlembke.de/prod/3dtraceroute/>
 XTraceRoute Developer: <http://www.dtek.chalmers.se/~d3august/xt/>

Intrusion Detection System Types

- *Host-based intrusion-detection* is the art of detecting malicious activity within a single computer by using
 - host log information
 - system activity
 - virus scanners
- A *Network intrusion detection system* is a system that tries to detect malicious activity such as denial of service attacks, port-scans or other attempts to hack into computers by reading all the incoming packets and trying to find suspicious patterns.

System Architecture



Information Visualization Mantra

Overview First,

Zoom & Filter,

Details on Demand

- Ben Shneiderman

<http://www.cs.umd.edu/~ben/>

Overview First...

The screenshot shows the Wireshark interface with a packet capture of an FTP session. A large black oval highlights a sequence of packets from 11 to 21. Packet 11 is selected, showing details for a TCP Zero Window message.

No.	Time	Source	Destination	Protocol	Info
1	0.000000	10.1.3.1	10.1.100.3	FTP	Response: 530 Login
2	57.899660	10.1.3.1	10.1.100.3	FTP	Response: 530 Login
3	107.449220	10.1.3.1	10.1.100.3	FTP	Response: 530 Login
4	20.537217	10.1.3.1	10.1.100.3	FTP	Response: 530 Login
5	1416.995338	10.6.1.251	10.1.4.4	TCP	[TCP Zerowindow] ftp
6	1417.022253	10.6.1.251	10.1.4.4	TCP	[TCP Zerowindow] ftp
7	1417.032157	10.6.1.251	10.1.4.4	TCP	[TCP Zerowindow] ftp
8	1417.073243	10.6.1.251	10.1.4.4	TCP	[TCP Zerowindow] ftp
9	1417.144019	10.6.1.251	10.1.4.4	TCP	[TCP Zerowindow] ftp
10	1417.163352	10.6.1.251	10.1.4.4	TCP	[TCP Zerowindow] ftp
11	1417.177927	10.6.1.251	10.1.4.4	TCP	[TCP Zerowindow] ftp
12	1417.214781	10.6.1.251	10.1.4.4	TCP	[TCP Zerowindow] ftp
13	1417.308616	10.6.1.251	10.1.4.4	TCP	[TCP Zerowindow] ftp
14	1417.333711	10.6.1.251	10.1.4.4	TCP	[TCP Zerowindow] ftp
15	1417.425149	10.6.1.251	10.1.4.4	TCP	[TCP Zerowindow] ftp
16	1417.443194	10.6.1.251	10.1.4.4	TCP	[TCP Zerowindow] ftp
17	1417.485418	10.6.1.251	10.1.4.4	TCP	[TCP Zerowindow] ftp
18	1417.534217	10.6.1.251	10.1.4.4	TCP	[TCP Zerowindow] ftp
19	1417.608517	10.6.1.251	10.1.4.4	TCP	[TCP Zerowindow] ftp
20	1417.687446	10.6.1.251	10.1.4.4	TCP	[TCP Zerowindow] ftp
21	1417.745307	10.6.1.251	10.1.4.4	TCP	[TCP Zerowindow] ftp

Frame 11 (60 bytes on wire (96 bytes captured) on interface eth0):
Ethernet II, Src: 08:06:5b:04:20:14, Dst: 00:05:9a:50:70:09
Internet Protocol, Src Addr: 10.6.1.251 (10.6.1.251), Dst Addr: 10.1.4.4 (10.1.4.4)
Transmission Control Protocol, Src Port: ftp-data (20), Dst Port: echo (7), Seq: 0, Ack: 0,

```
0000  00 05 9a 50 70 09 00 06 5b 04 20 14 08 00 45 00  ...Pp... [. ...E.  
0010  00 28 13 4e 00 00 fd 06 90 7c 0a 06 01 fb 0a 01  .(.N.... .).....  
0020  04 04 00 14 00 07 00 07 13 4e 00 00 00 00 50 02  .....N....P.  
0030  00 00 82 6d 00 00 00 00 00 00 00 00 00 00 00 00  ...m.... ..
```

Zoom and Filter...

The screenshot shows the Wireshark interface with a packet list table. A context menu is open over the second packet (No. 2, Time 57.899660). The menu items include 'Follow TCP Stream', 'Decode As...', 'Display Filters...', 'Mark Packet', 'Time Reference', 'Match', 'Prepare', 'Coloring Rules...', 'Print...', and 'Show Packet In New Window'. The 'Follow TCP Stream' option is circled in black.

No.	Time	Source	Destination	Protocol	Info
1	0.000000	10.1.3.1	10.1.100.3	FTP	Response: 530 Login
2	57.899660	10.1.3.1	10.1.100.3	FTP	Response: 530 Login
3	107.449126	10.1.3.1	10.1.100.3	FTP	Response: 530 Login
4	620.537217	10.1.3.1	10.1.100.3	FTP	Response: 530 Login
5	1416.995338	10.6.1.1	10.6.1.1	TCP	[TCP Zerowindow] ftp
6	1417.022253	10.6.1.1	10.6.1.1	TCP	[TCP Zerowindow] ftp
7	1417.032157	10.6.1.1	10.6.1.1	TCP	[TCP Zerowindow] ftp
8	1417.073243	10.6.1.1	10.6.1.1	TCP	[TCP Zerowindow] ftp
9	1417.144019	10.6.1.1	10.6.1.1	TCP	[TCP Zerowindow] ftp
10	1417.163352	10.6.1.1	10.6.1.1	Match	
11	1417.177927	10.6.1.1	10.6.1.1	Prepare	
12	1417.214781	10.6.1.1	10.6.1.1	Prepare	
13	1417.308616	10.6.1.1	10.6.1.1	Coloring Rules...	
14	1417.333711	10.6.1.1	10.6.1.1	Print...	
15	1417.425149	10.6.1.1	10.6.1.1	Print...	
16	1417.443194	10.6.1.1	10.6.1.1	Show Packet In New Window	
17	1417.485418	10.6.1.1	10.6.1.1		
18	1417.534217	10.6.1.251	10.1.4.4		
19	1417.608517	10.6.1.251	10.1.4.4		
20	1417.687446	10.6.1.251	10.1.4.4		
21	1417.745307	10.6.1.251	10.1.4.4		

The screenshot shows the Wireshark interface with a zoomed-in view of packet 2. The packet list table is visible, with packet 2 selected and circled in black. The packet details pane shows the structure of the packet: Ethernet II, Internet Protocol, Transmission Control Protocol, and File Transfer Protocol (FTP). The packet bytes pane shows the raw data in hexadecimal and ASCII. A filter is applied to the packet list: 'eq 10.1.100.3 and (tcp.port eq 21 and tcp.port eq 33337)'. The filter field is also circled in black.

Time	Source	Destination	Protocol	Info	
2	57.899660	10.1.3.1	10.1.100.3	FTP	Response: 530 Login in

Filter: eq 10.1.100.3 and (tcp.port eq 21 and tcp.port eq 33337) [Reset] [Apply] File: tcpdump.log

The screenshot shows the Wireshark interface with the following details:

No.	Time	Source	Destination	Protocol	Info
2	57.899660	10.1.3.1	10.1.100.3	FTP	Response: 530 Login incorrect...

The packet details pane shows the following structure:

- Frame 2 (88 bytes on wire, 88 bytes captured)
- Ethernet II, Src: 00:05:9a:50:70:05 (10.1.3.1), Dst: 00:0c:29:00:00:00 (10.1.100.3)
- Internet Protocol Version 4, Src: 10.1.3.1 (10.1.3.1), Dst: 10.1.100.3 (10.1.100.3)
- TCP, Src Port: ftp (21), Dst Port: 33337 (33337), Seq: 0, Ack: 0, Len: 0
- File Transfer Protocol (FTP)

The packet bytes pane shows the following hex and ASCII data:

```
0000 00 06 5b 00 00 14 00 05 9a 50 70 09 08 00 45 00 ..[. . . .Pp..
0010 00 4a 27 d9 00 00 3f 06 98 cf 0a 01 03 01 0a 01 .J'.@.?.....
0020 64 03 00 15 82 3f 06 83 dc fe 06 b9 8d 80 18 d.....
0030 16 a0 07 42 00 00 01 01 67 69 6e 20 03 0e 05 0f <.530 Login incor
0040 3c 91 35 33 30 20 4c 6f 67 69 6e 20 03 0e 05 0f <.530 Login incor
0050 72 72 65 63 74 2e 0d 0a
```

Details on Demand...

The screenshot shows the 'Contents of TCP stream' window with the following text:

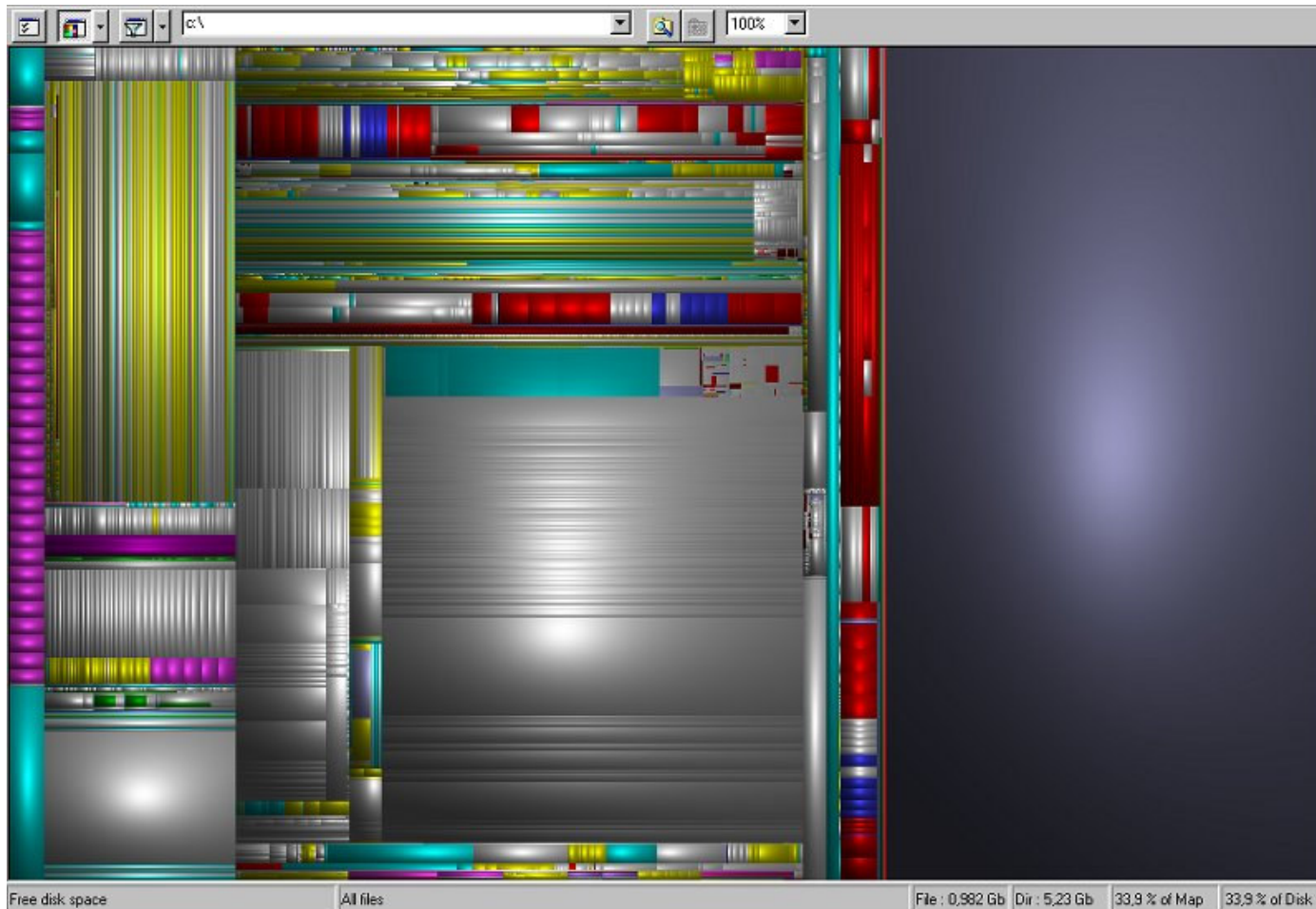
```
530 Login incorrect..
```

The window also shows the following details:

- Entire conversation (22 bytes)
- Filter out this stream
- Close

Representative Current Research

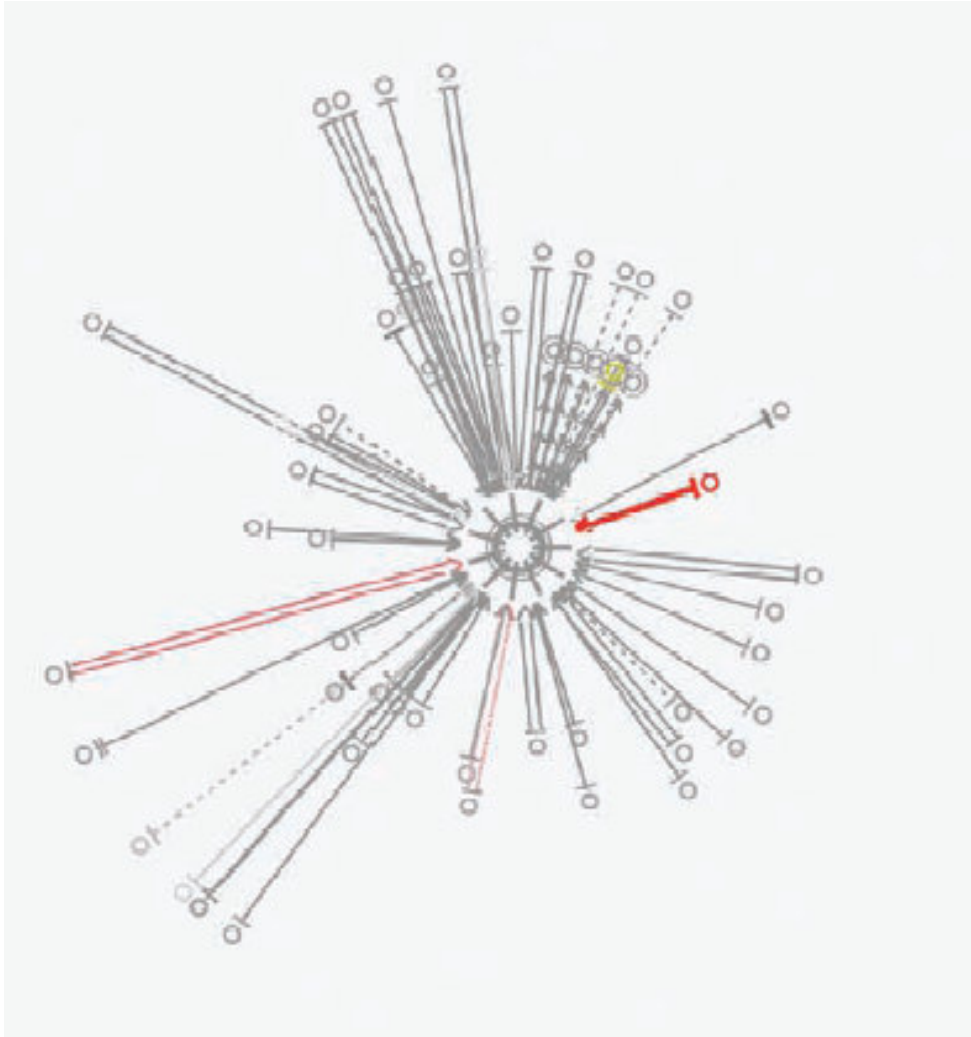
Sequoia View



Demo

<http://www.win.tue.nl/sequoiaview/>

Observing Intruder Behavior

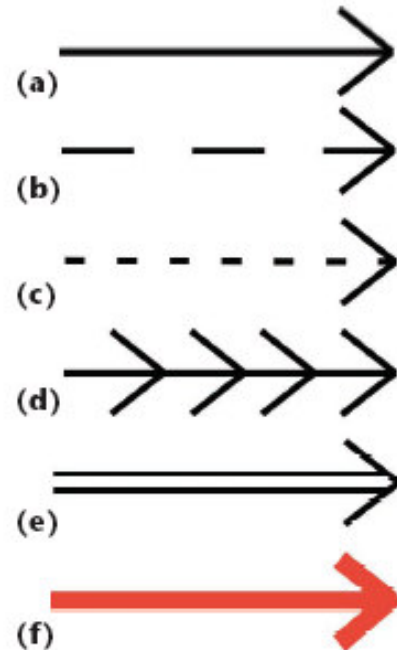


Dr. Rob Erbacher

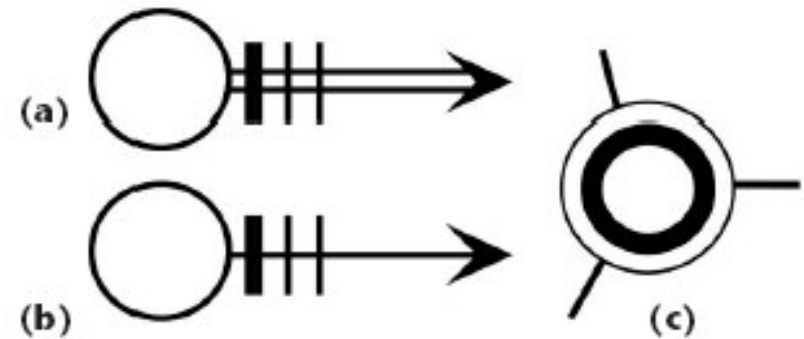
- Visual Summarizing and Analysis Techniques for Intrusion Data
- Multi-Dimensional Data Visualization
- A Component-Based Event-Driven Interactive Visualization Software Architecture

<http://otherland.cs.usu.edu/~erbacher/>

3 Line appearances and their relationships. (a) Telnet and rlogin connections as solid lines, (b) privileged FTPs as long dashed lines, (c) anonymous FTPs as short dashed lines, (d) Network file system (NFS) accesses as solid lines with many arrows, (e) initial inetd port connection, and (f) port scan.

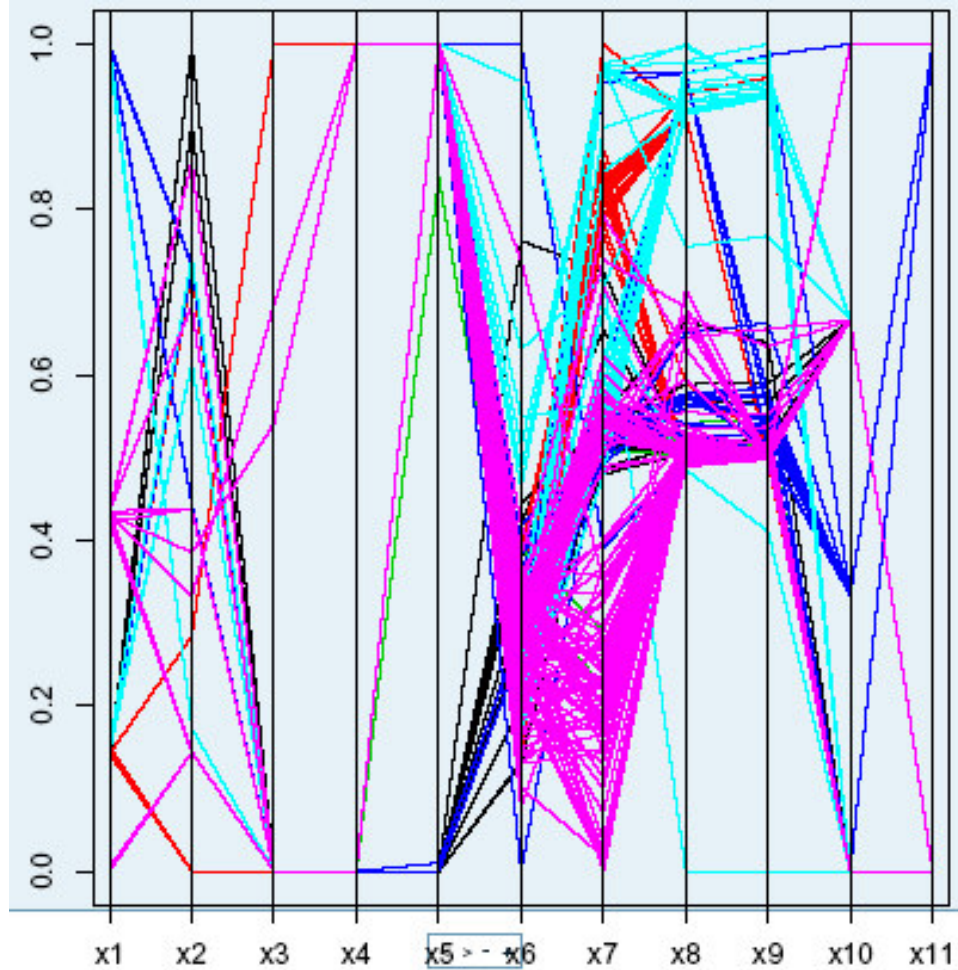


Demo



2 Basic glyph organization. (a) The initial inetd connection to the system. (b) The resulting connection after authentication. (a) and (b) also represent the number of users with connections from the given remote host and the number of connections by said users through the use of the cross hatches. The monitored system, (c) showing number of users and load.

Operating System Fingerprinting



Dr. David
Marchette

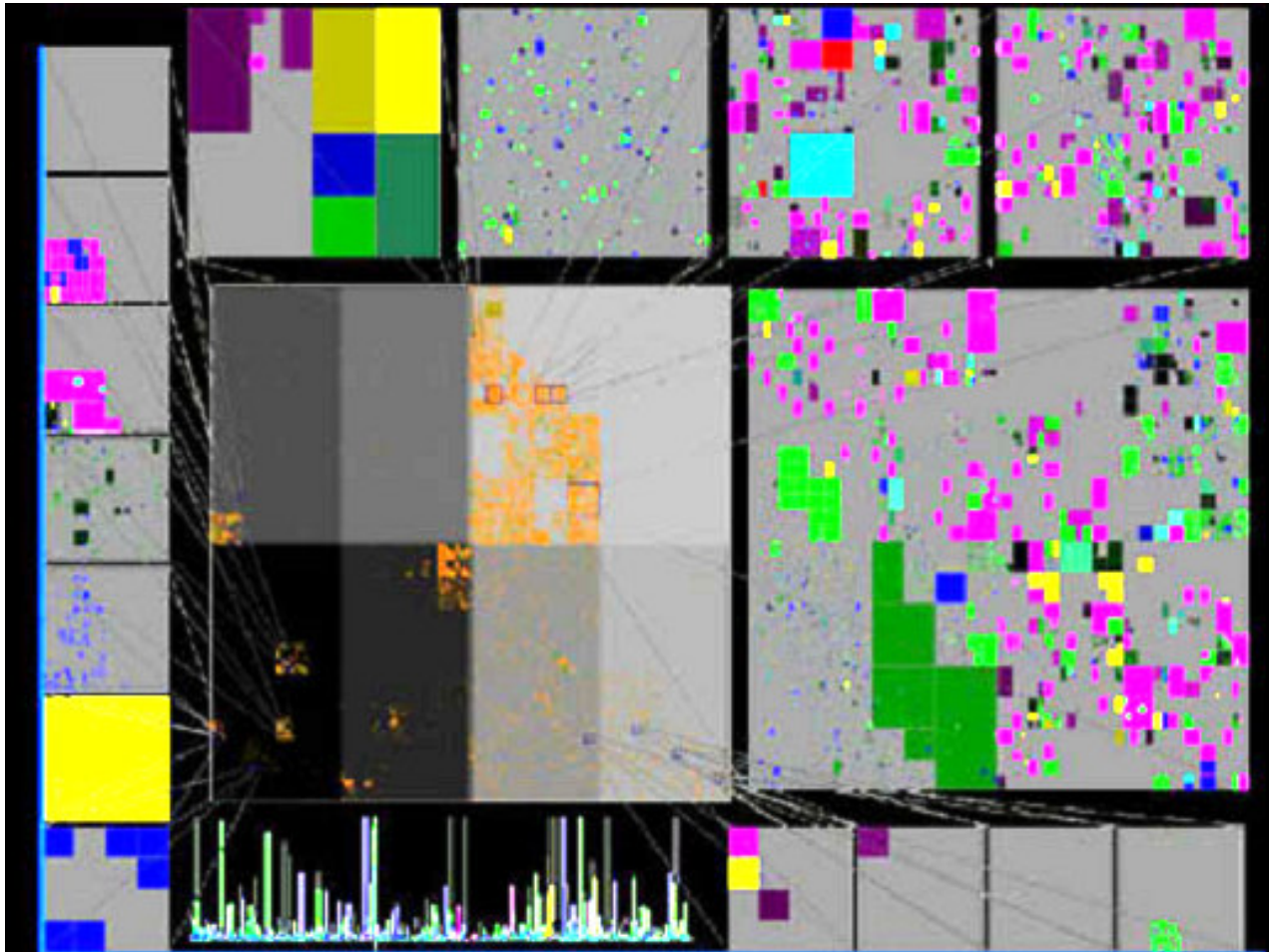
- Passive
Fingerprinting
- Statistics for
intrusion
detection

<http://www.mts.jhu.edu/~marchette/>

Visualizing Internet Routing Data

Soon Tee Teoh

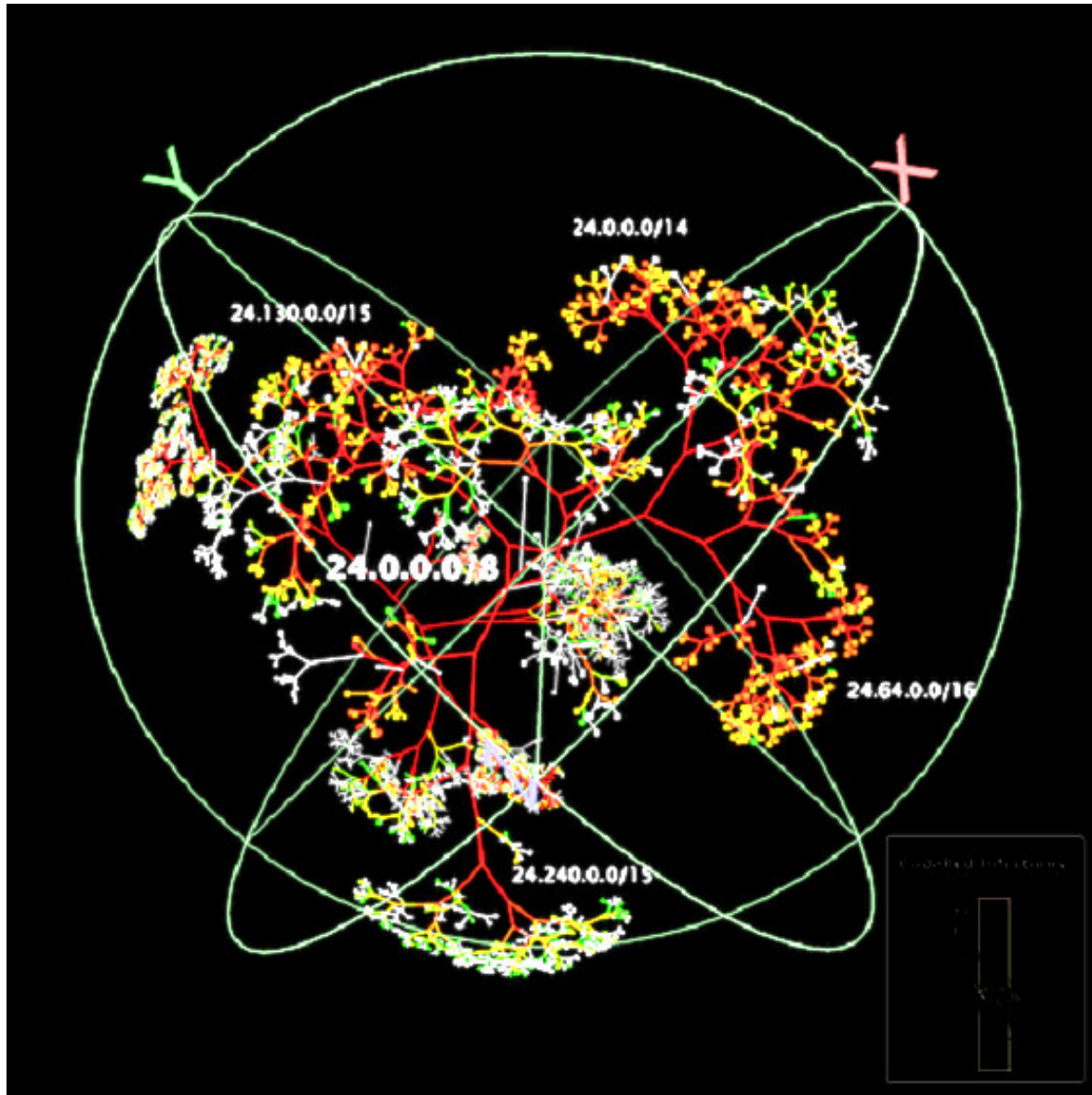
Demo



<http://graphics.cs.ucdavis.edu/~steoh/>

See also treemap basic research: <http://www.cs.umd.edu/hcil/treemap-history/index.shtml>

Worm Propagation

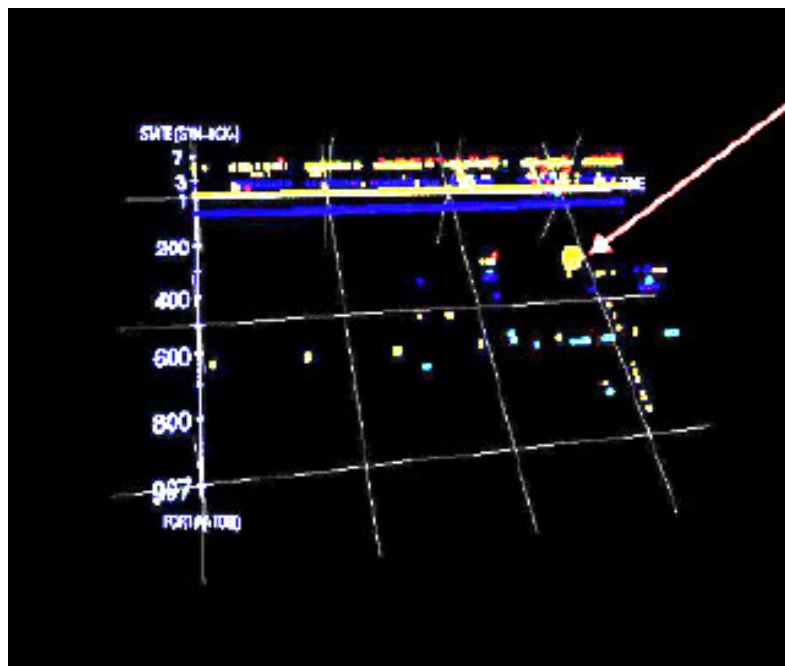
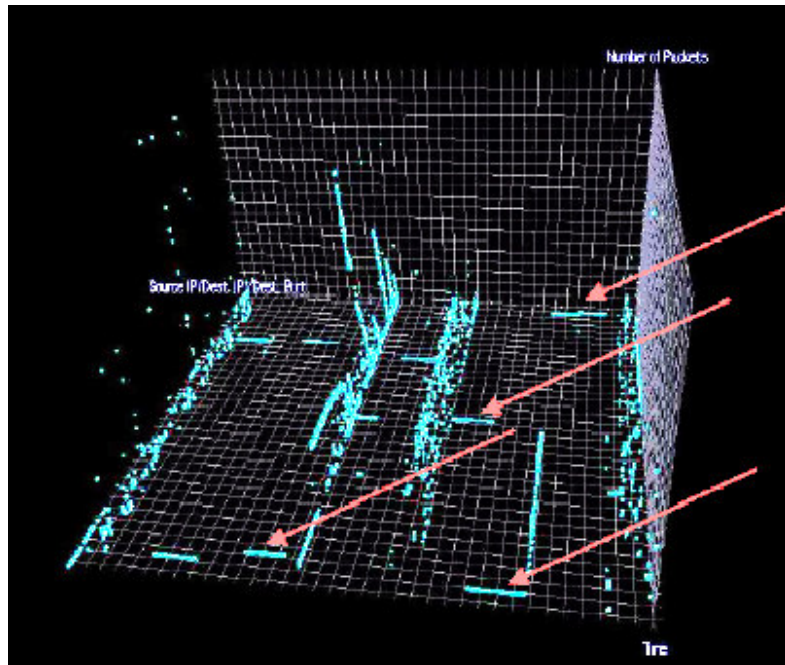


- CAIDA
- Young Hyun
- David Moore
- Colleen Shannon
- Bradley Huffaker

<http://www.caida.org/tools/visualization/walrus/examples/codered/>

Intrusion Detection and Visualization Using Perl

Jukka Juslin



3D plot of:

- Time
- SDP (Source-Destination-Port)
- Number of Packets

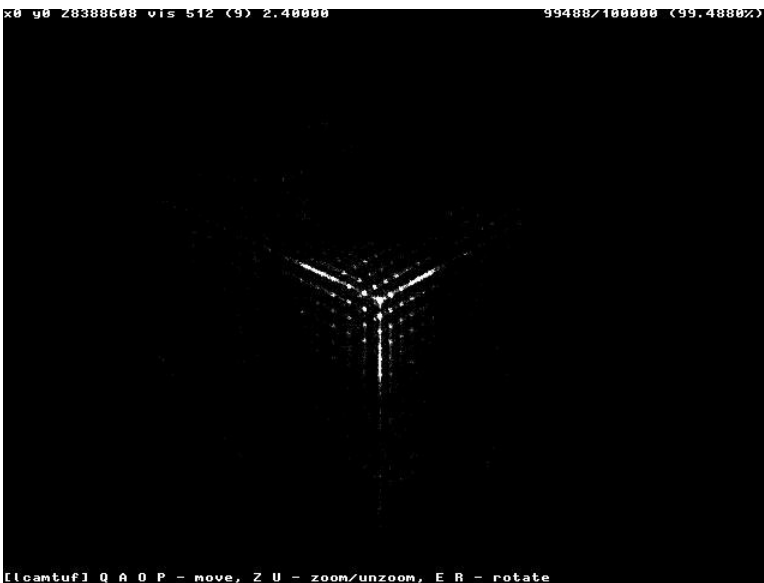
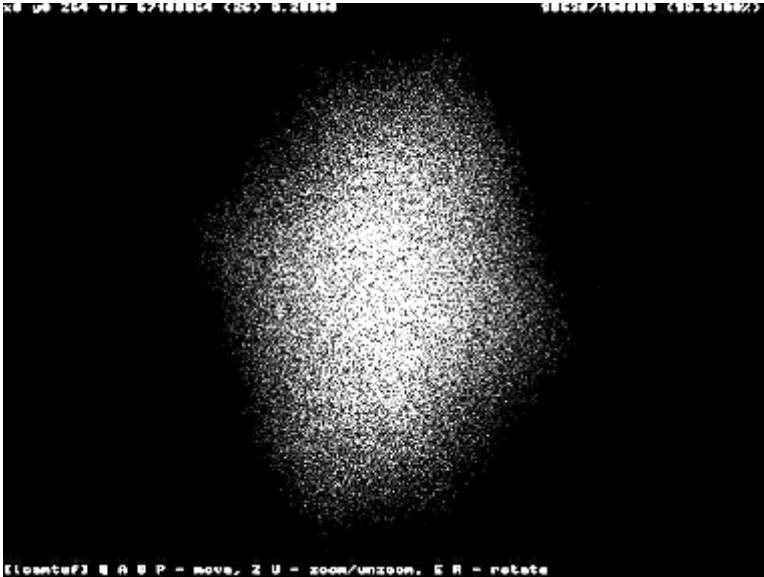
Data stored in Perl hashes

Output piped to GNUplot

<http://www.cs.hut.fi/~jtjuslin/>

TCP/IP Sequence Number Generation

Michal Zalewski



$$x[n] = s[n-2] - s[n-3]$$

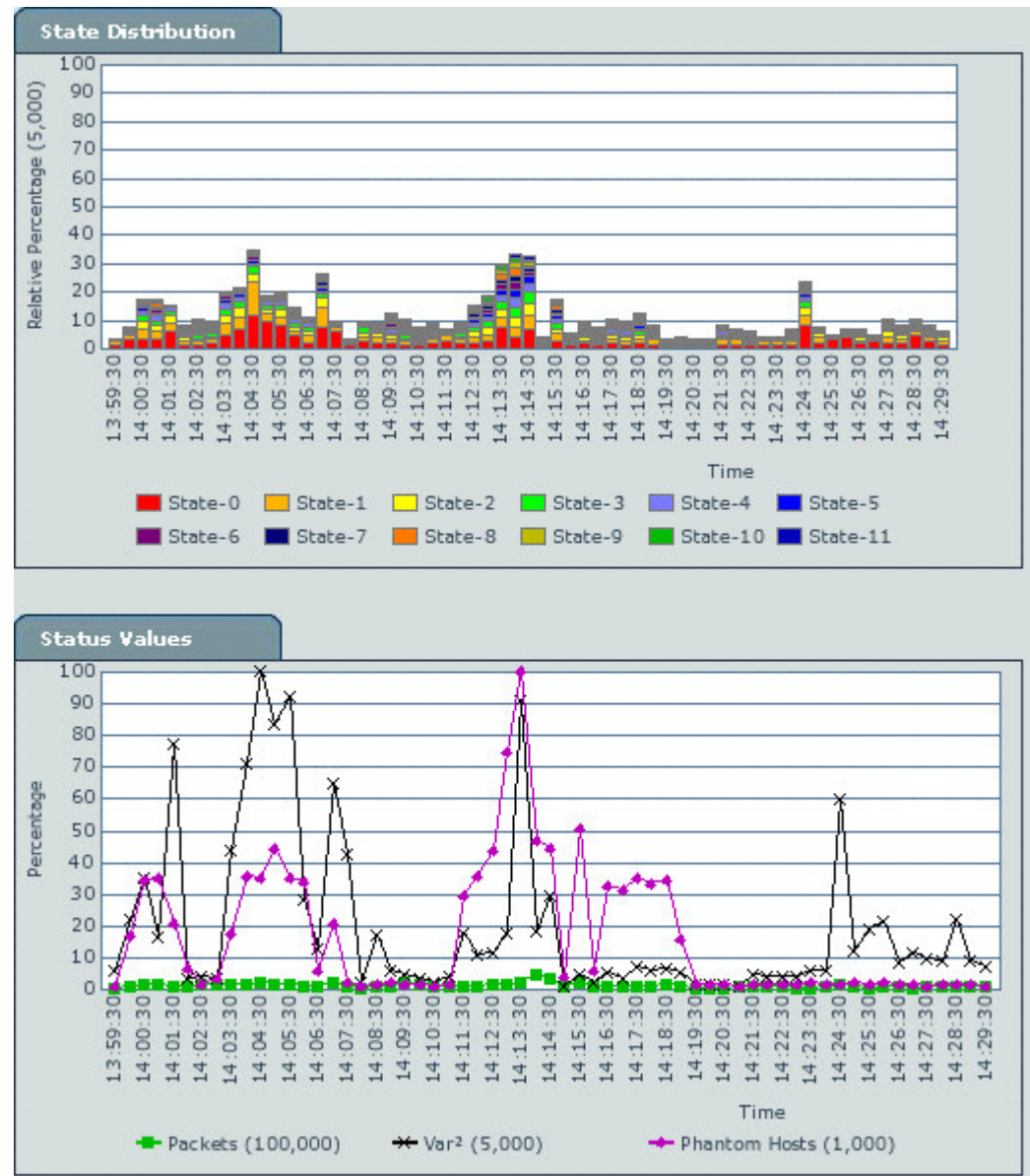
$$y[n] = s[n-1] - s[n-2]$$

$$z[n] = s[n] - s[n-1]$$

Follow-up paper - <http://lcamtuf.coredump.cx/newtcp/>

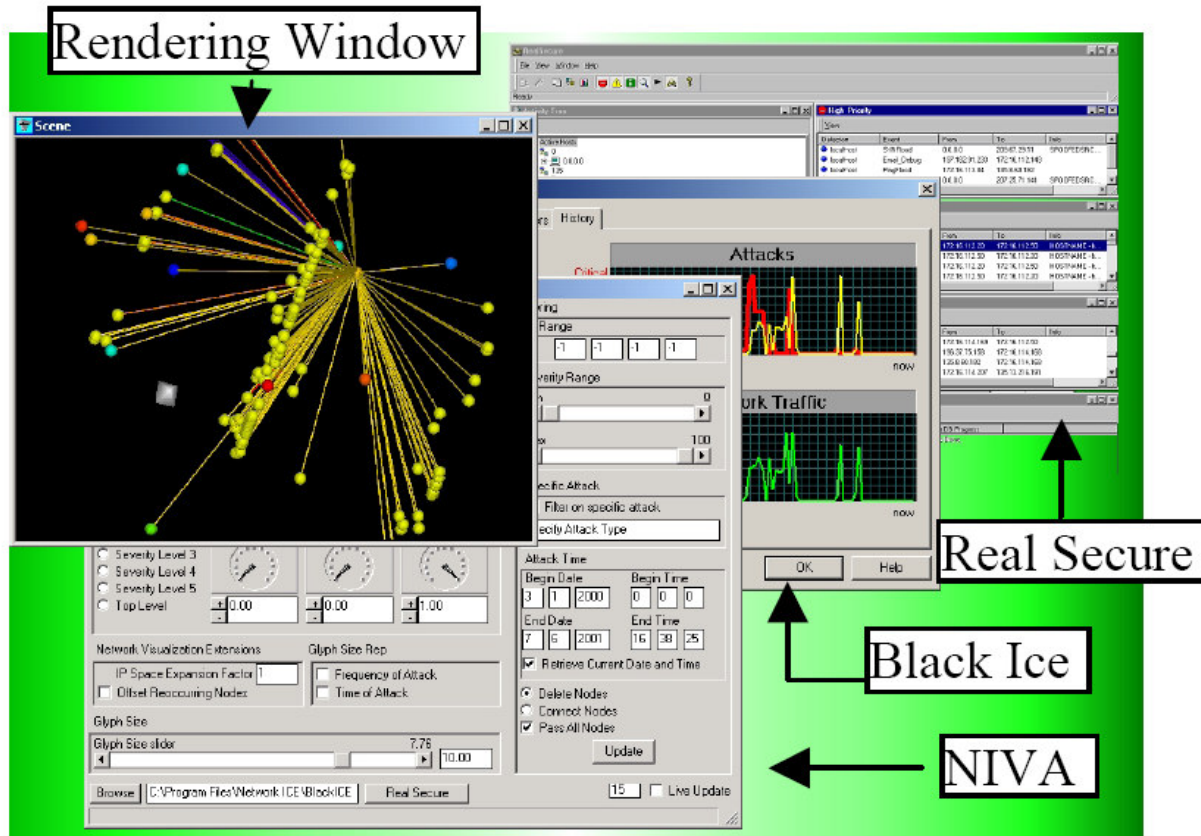
Initial paper - <http://razor.bindview.com/publish/papers/tcpseq/print.html>

High Speed Data Flow Visualization



Terminator technology watches the data stream and illustrates categories of data as colored bars that are proportional in height to the quantity of data at a given time. The process is repeated to form a stacked bar graph that moves across a computer screen to show current and past data traffic composition.

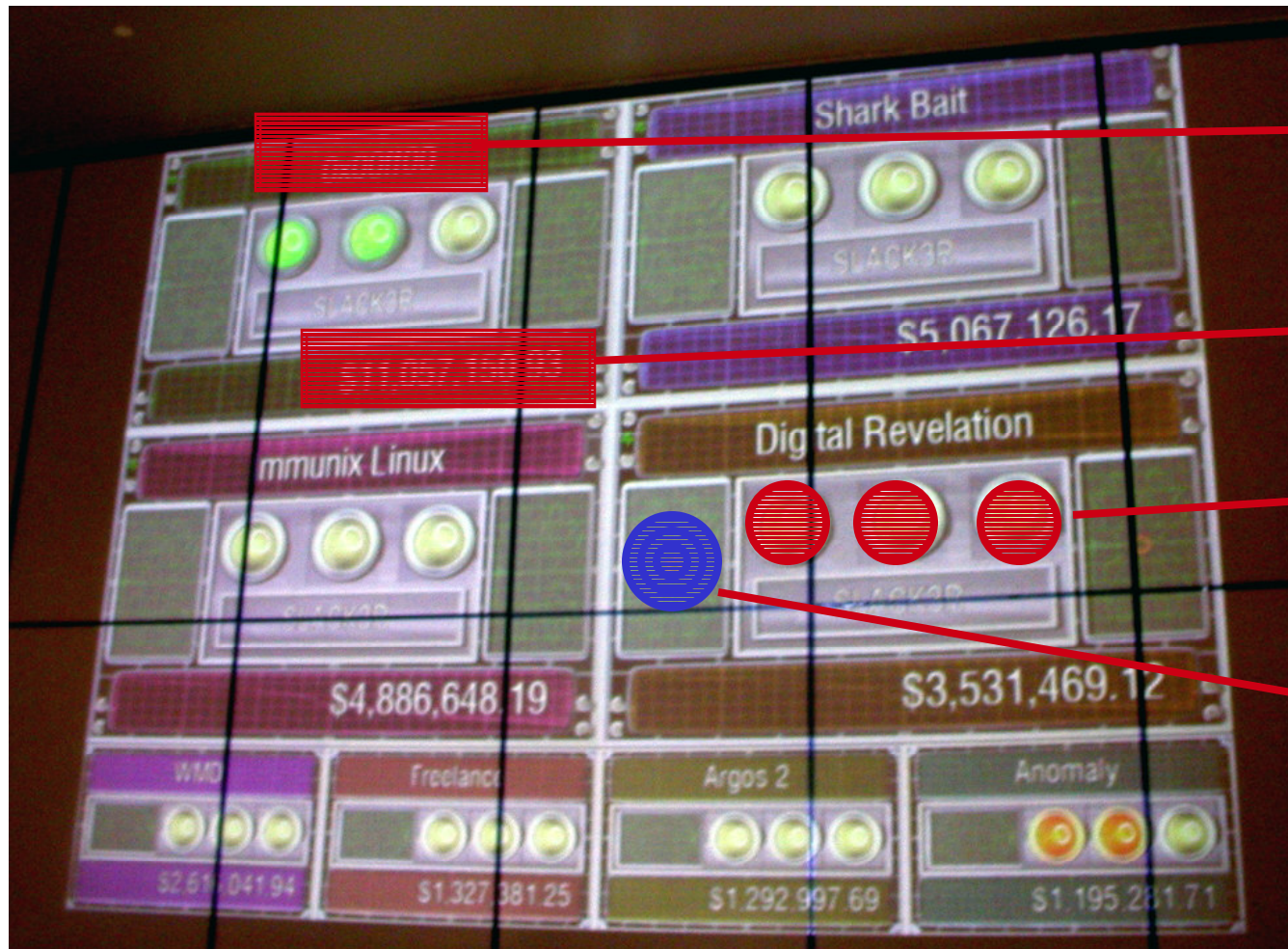
Haptic and Visual Intrusion Detection



NIVA System

- Craig Scott
- Kofi Nyarko
- Tanya Capers
- Jumoke Ladeji-Osias

SCOREBOARD DC 1 1



Team Name

Team Score

Hacking Rank

Count of services

Entire slide from: www.toorcon.org/slides/rootfu-toorcon.ppt

Atlas of Cyber Space

An Atlas Of Cyberspaces

Welcome to the Atlas of Cyberspaces

This is an atlas of maps and graphic representations of the geographies of the new electronic territories of the Internet, the World-Wide Web and other emerging Cyberspaces.

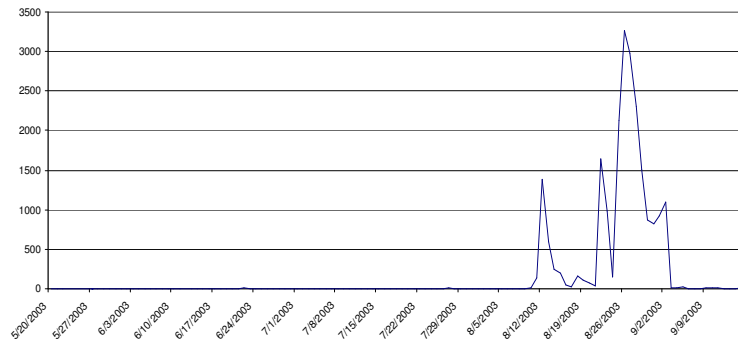
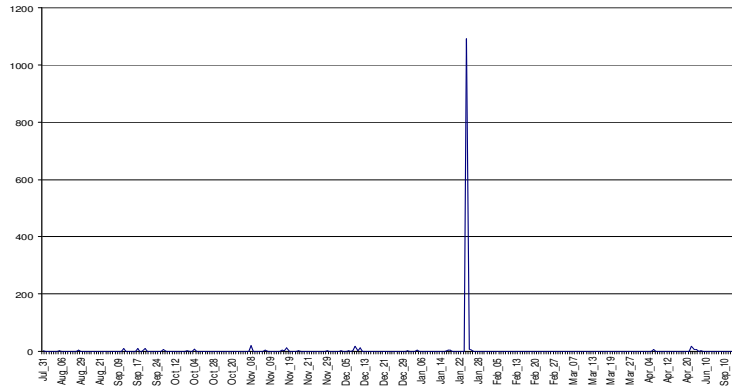
These maps of Cyberspaces - *cybermaps* - help us visualise and comprehend the new digital landscapes beyond our computer screen, in the wires of the global communications networks and vast online information resources. The cybermaps, like maps of the real-world, help us navigate the new information landscapes, as well being objects of aesthetic interest. They have been created by 'cyber-explorers' of many different disciplines, and from all corners of the world.

Some of the maps you will see in the Atlas of Cyberspaces will appear familiar, using the cartographic conventions of real-world maps, however, many of the maps are much more abstract representations of electronic spaces, using new metrics and grids. The atlas comprises separate pages, covering different types of cybermaps.

What's New
Conceptual
Artistic
Geographic
Cables & Satellites
Traceroutes
Census
Topology
Info Maps
Info Landscapes
Info Spaces
ISP Maps
Web Site Maps
Surf Maps
Muds & Virtual Worlds
Historical
Weather Maps
Wireless Maps

<http://www.cybergeography.org/atlas/atlas.html>

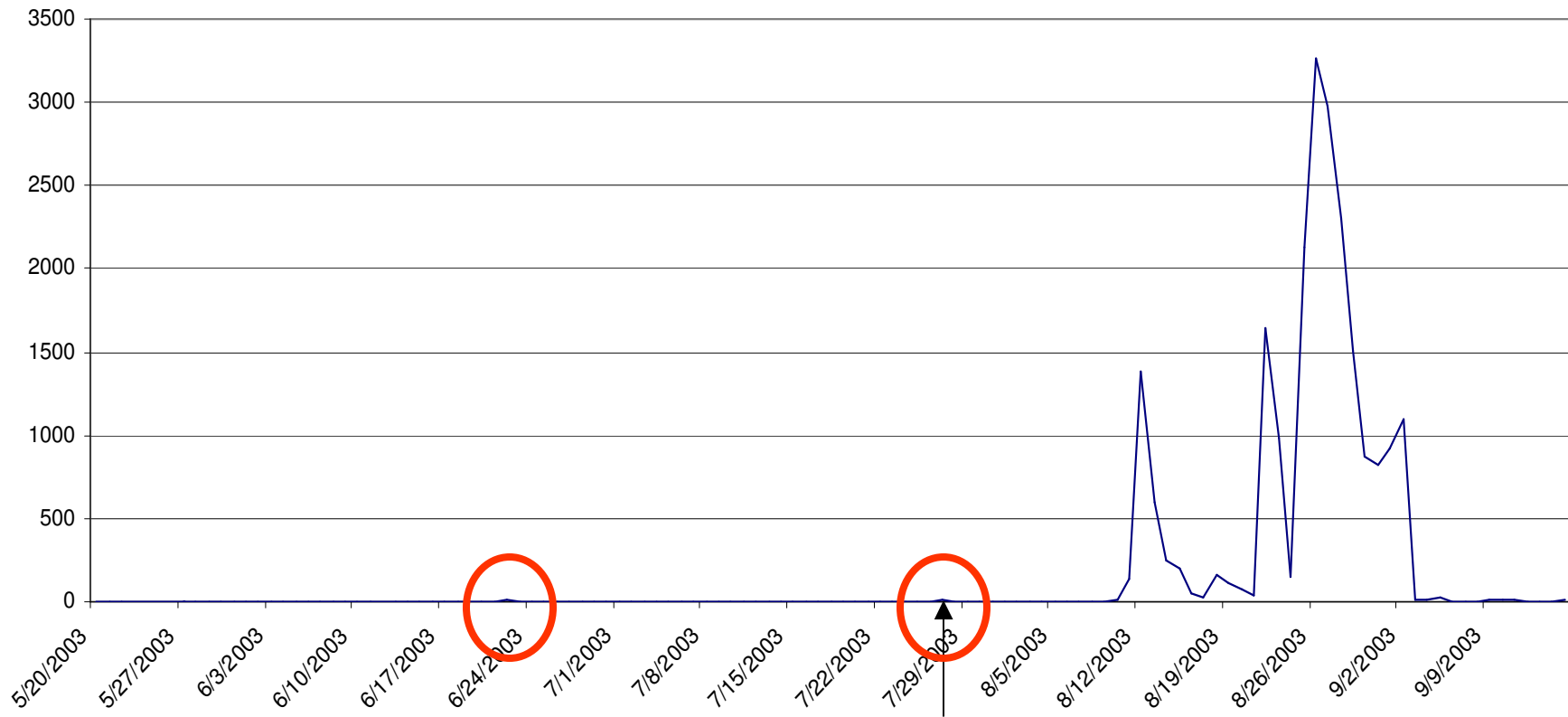
Honeynets



John Levine

- The Use of Honeynets to Detect Exploited Systems Across Large Enterprise Networks
- Interesting look at detecting zero-day attacks

Port 135 MS BLASTER scans



Date Public: 7/16/03 Date Attack: 8/11/03

Georgia Tech Honeynett

Source: John Levine, Georgia Tech

Hot Research Areas...

- visualizing vulnerabilities
- visualizing IDS alarms (NIDS/HIDS)
- visualizing worm/virus propagation
- visualizing routing anomalies
- visualizing large volume computer network logs
- visual correlations of security events
- visualizing network traffic for security
- visualizing attacks in near-real-time
- security visualization at line speeds
- dynamic attack tree creation (graphic)
- forensic visualization

More Hot Research Areas...

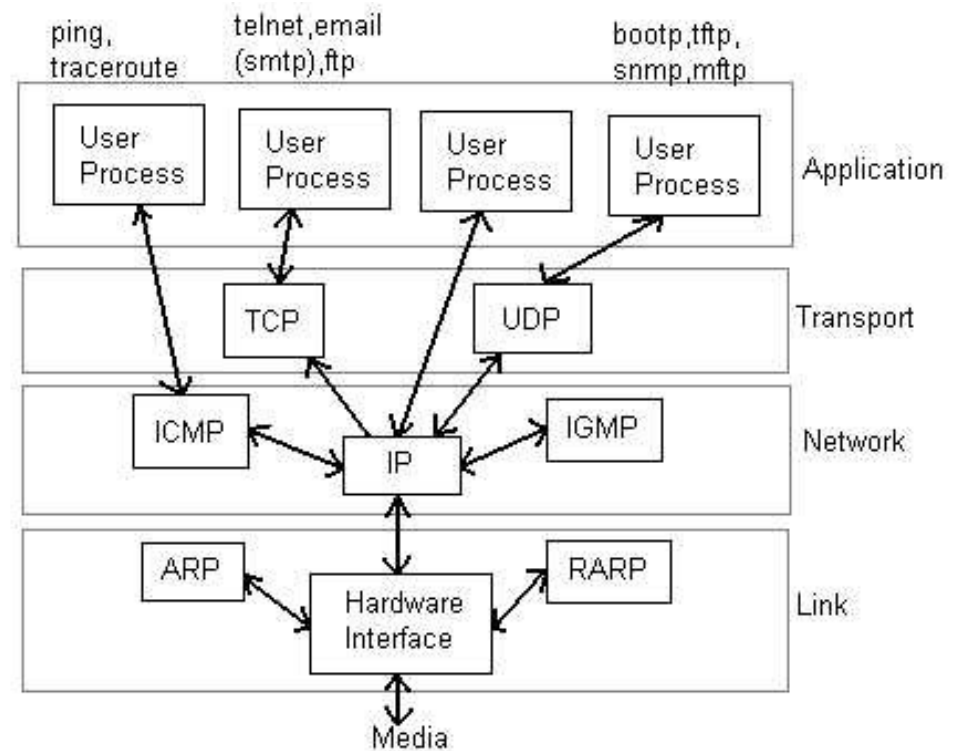
- feature selection and construction
- incremental/online learning
- noise in the data
- skewed data distribution
- distributed mining
- correlating multiple models
- efficient processing of large amounts of data
- correlating alerts
- signature and anomaly detection
- forensic analysis

One Approach...

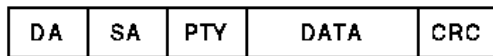
- Look at TCP/IP Protocol Stack Data (particularly header information)
- Find interesting visualizations
- Throw some interesting traffic at them
- See what they can detect
- Refine

Information Available On and Off the Wire

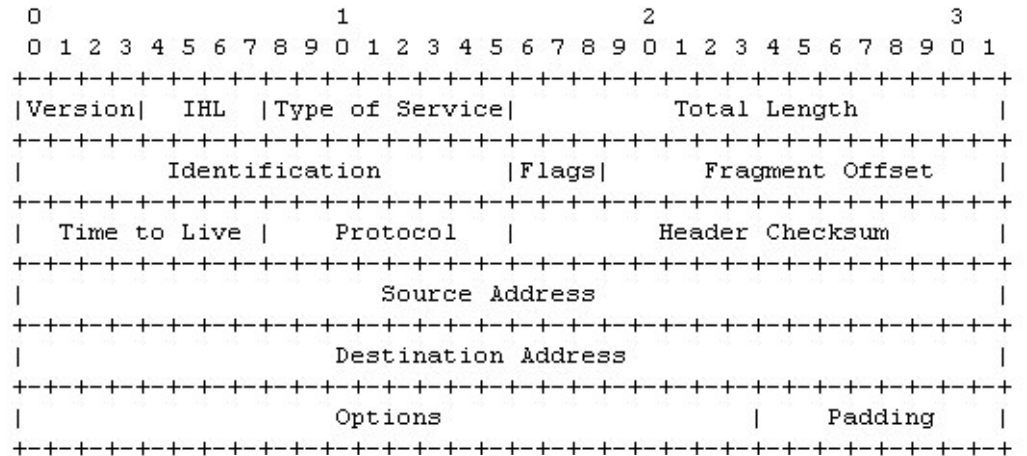
- Levels of analysis
- External data
 - Time
 - Size
 - Protocol compliance
 - Real vs. Actual Values
- Matrices of options
- Header slides



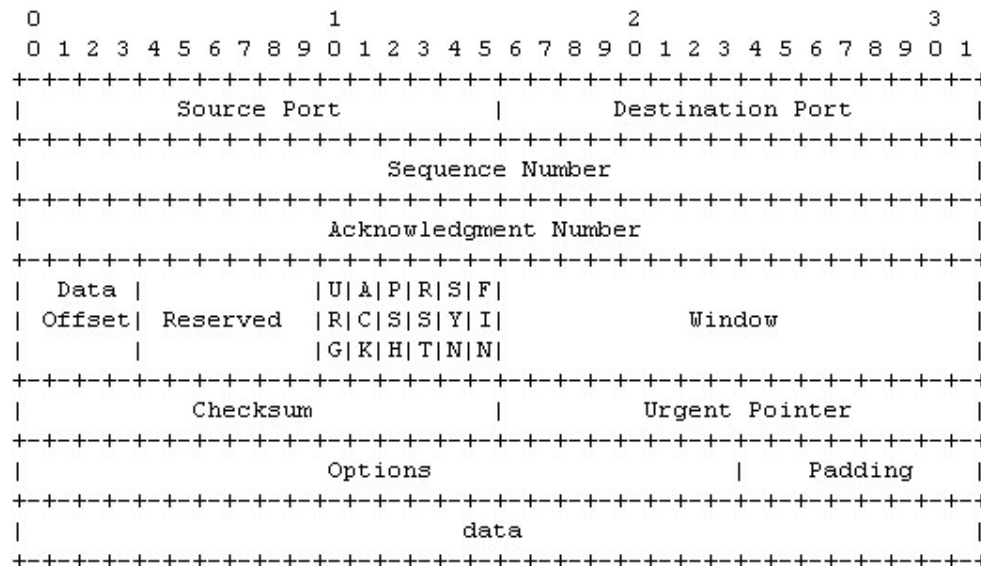
Examining Available Data...



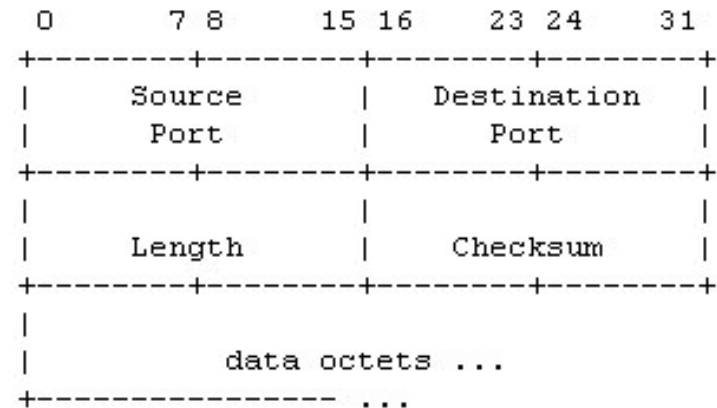
Link Layer (Ethernet)



Network Layer (IP)



Transport Layer (TCP)



Transport Layer (UDP)

IP: <http://www.ietf.org/rfc/rfc0791.txt>

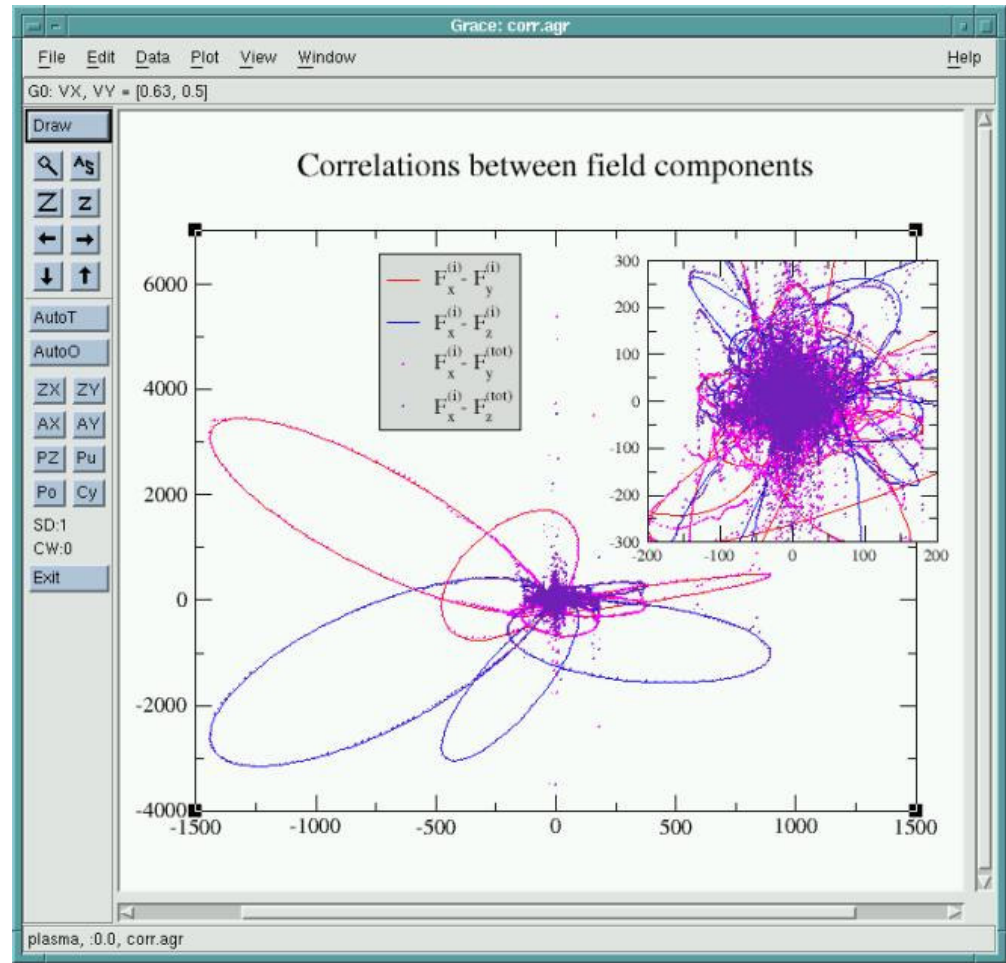
UDP: <http://www.ietf.org/rfc/rfc0768.txt>

TCP: <http://www.ietf.org/rfc/rfc793.txt>

Ethernet: <http://www.itec.suny.edu/scsys/vms/OVMSDOC073/V73/6136/ZK-3743A.gif>

Grace

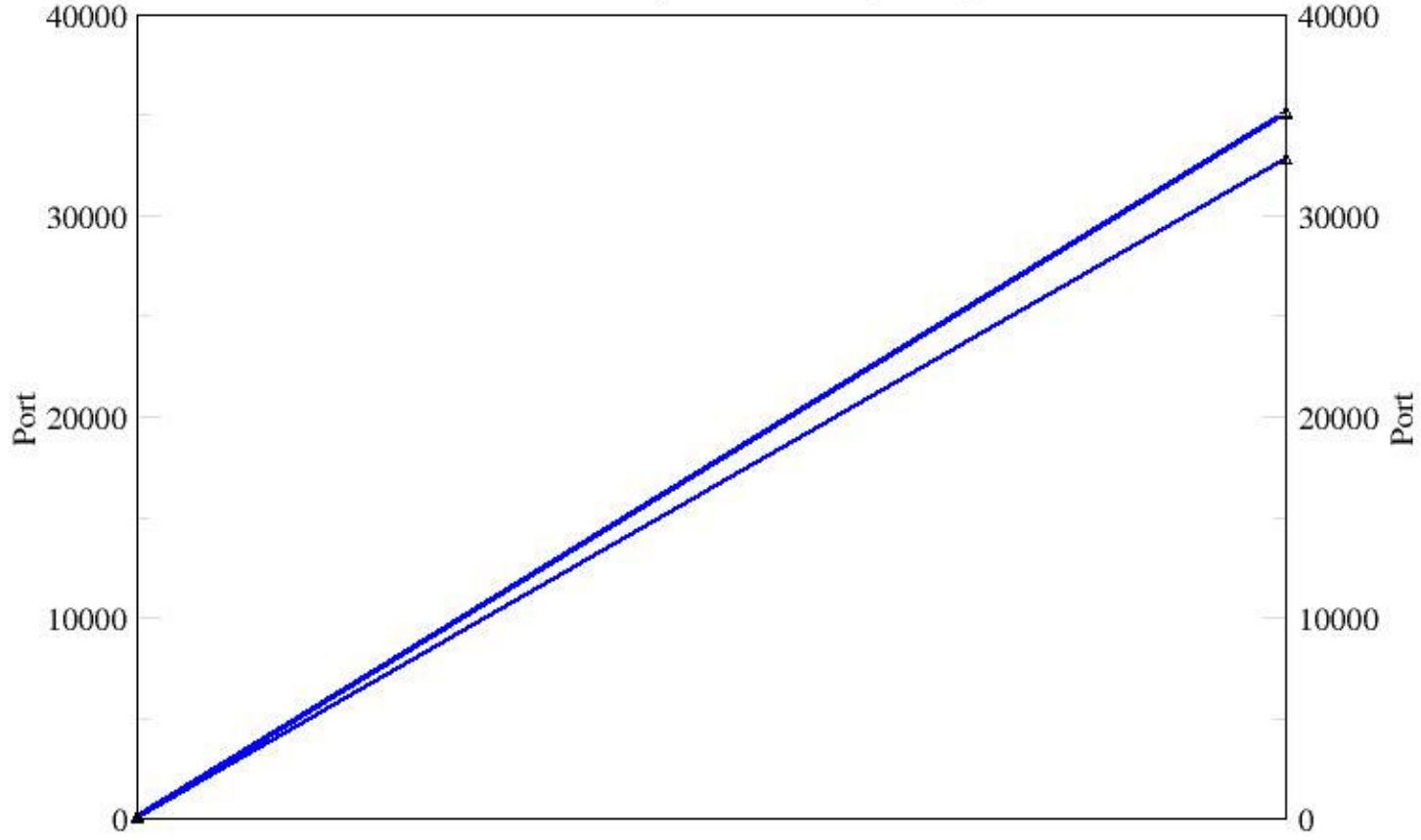
“Grace is a WYSIWYG 2D plotting tool for the X Window System and M*tif. Grace runs on practically any version of Unix-like OS. As well, it has been successfully ported to VMS, OS/2, and Win9*/NT/2000/XP”



<http://plasma-gate.weizmann.ac.il/Grace/>

Parallel Plot

Remote Machine's Ports



Target Machine's Ports

Results

Example 1 - Baseline with Normal Traffic

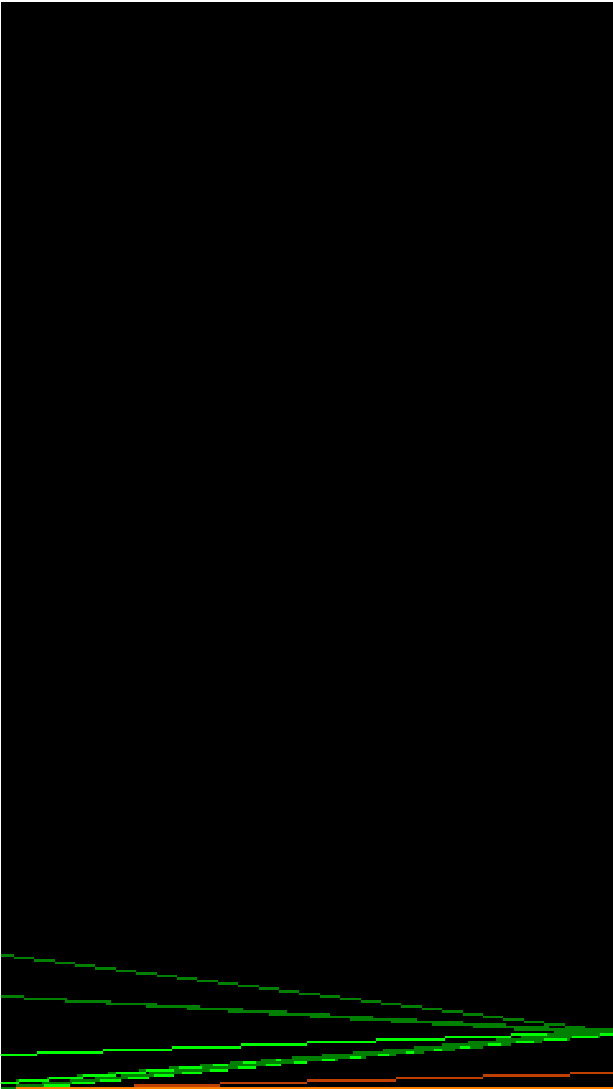
Example 2 - Port Scan

Example 3 - Port Scan “Fingerprinting”

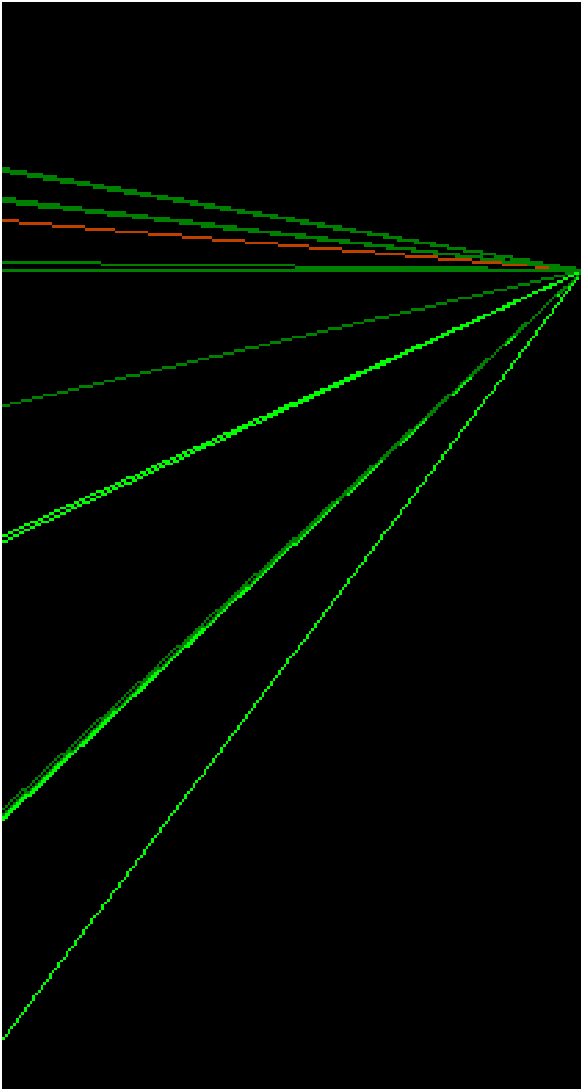
Example 4 - Vulnerability Scanner

Example 5 - Wargame

Example 1: Baseline



External Port Internal Port

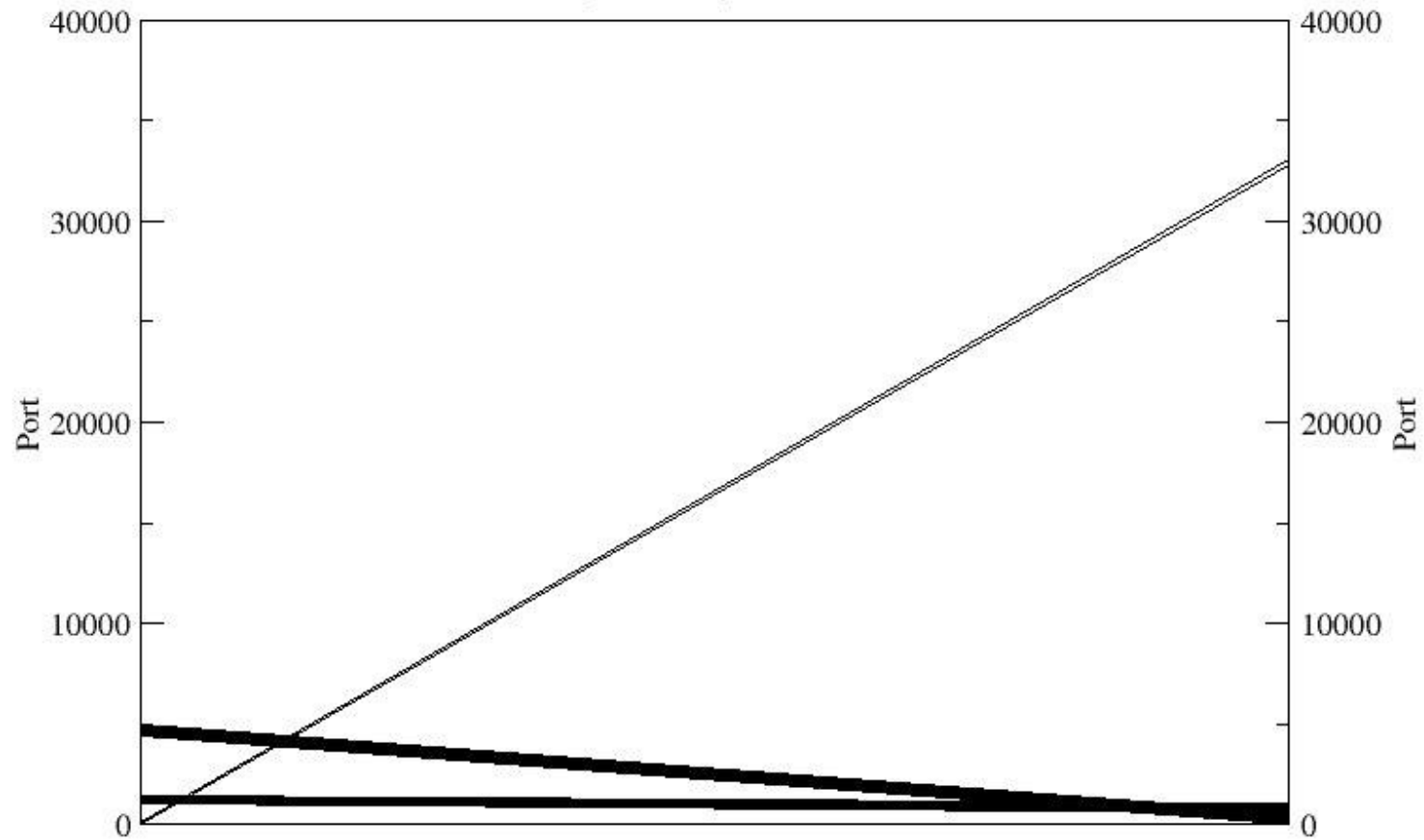


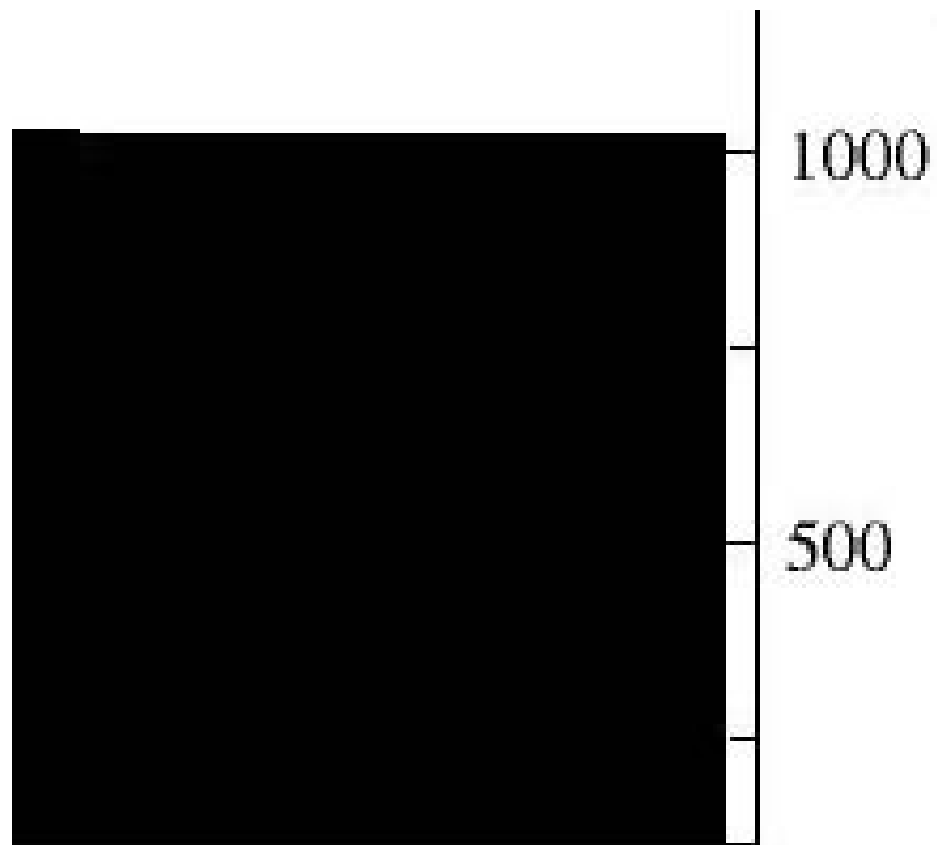
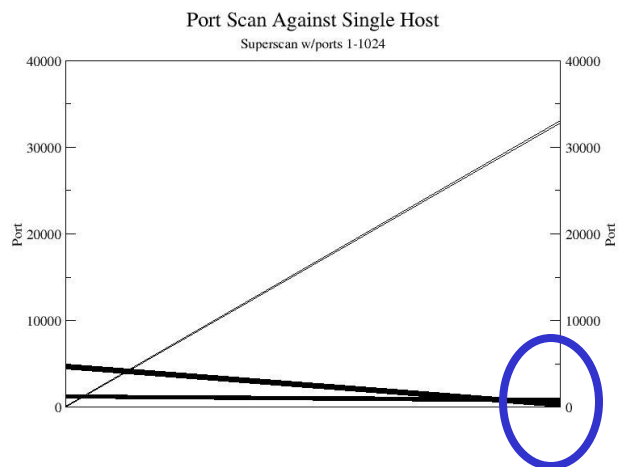
External IP Internal IP

Example 2 - PortScan

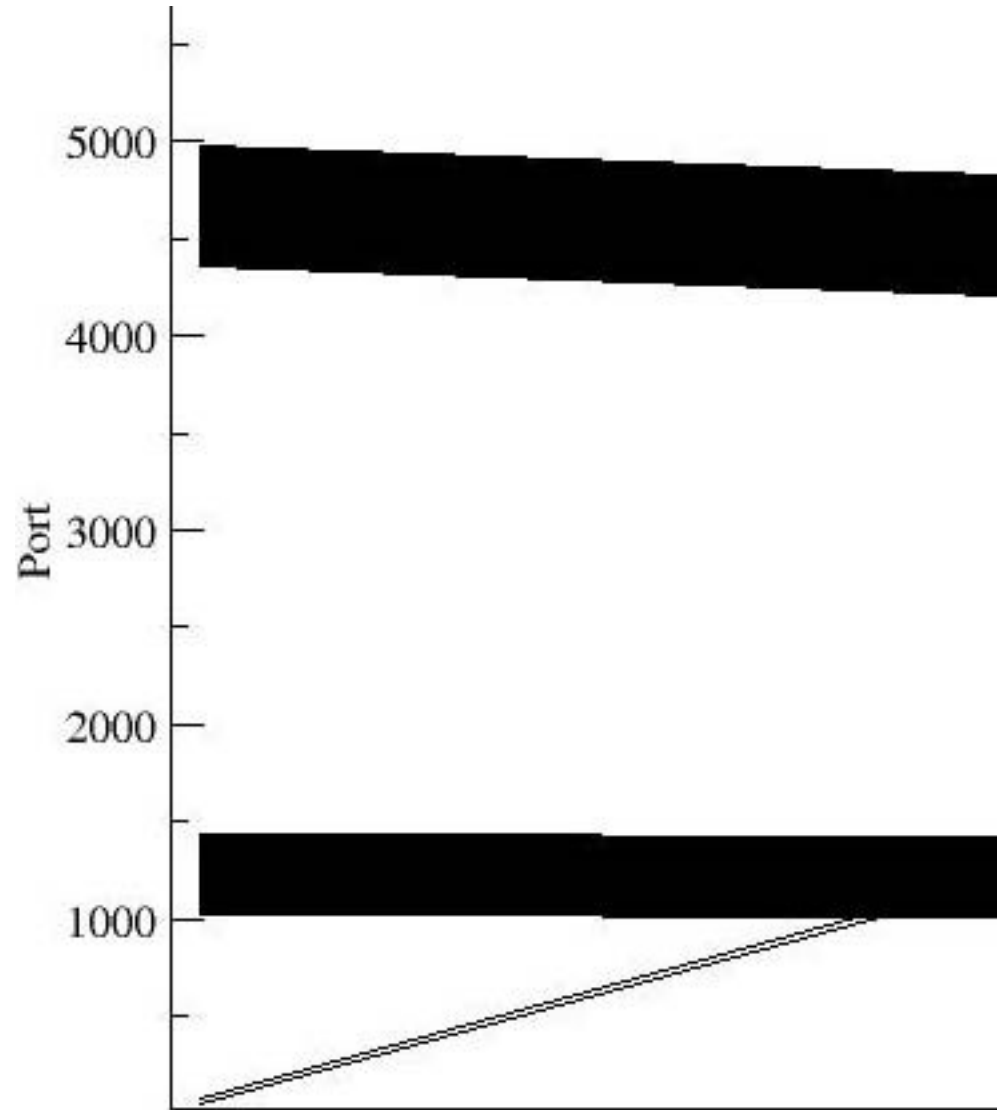
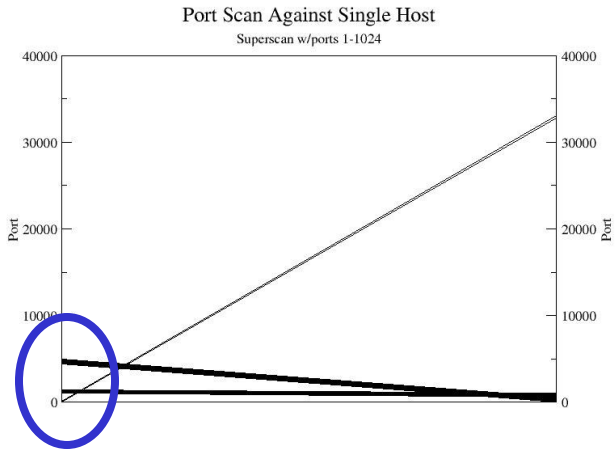
Port Scan Against Single Host

Superscan w/ports 1-1024



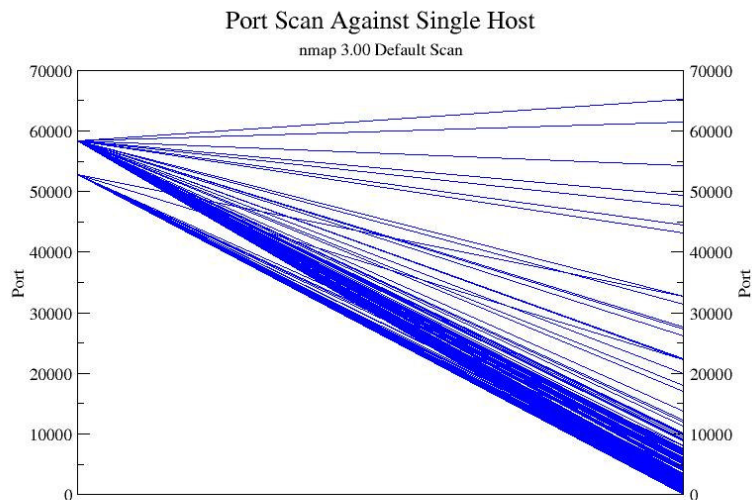


Defender

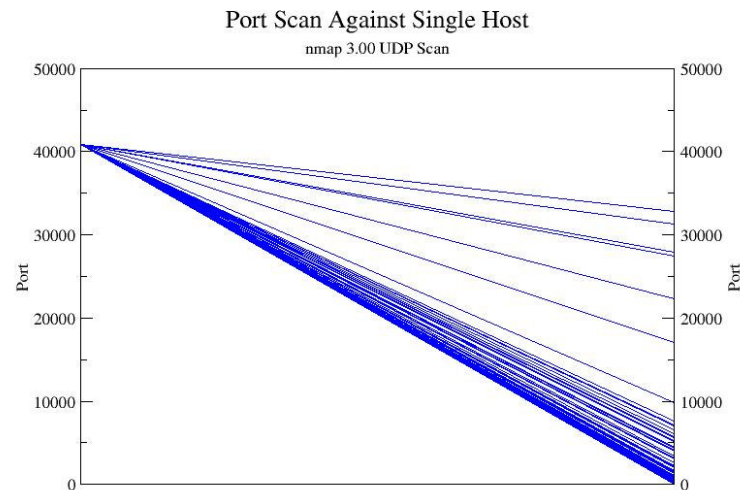


Attacker

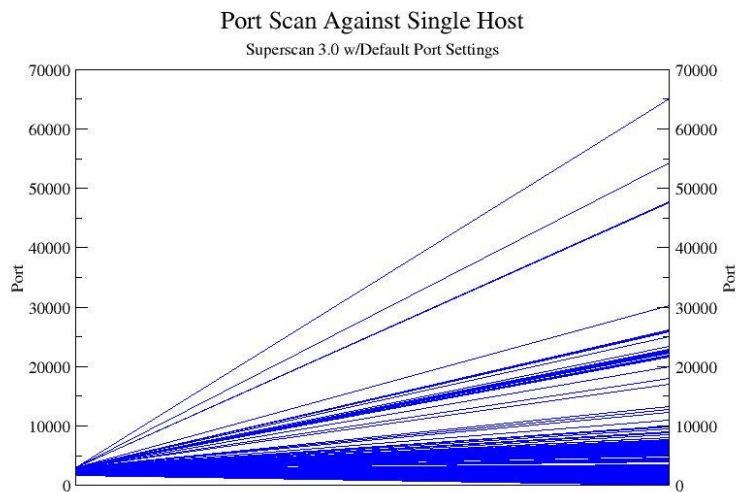
Example 3- PortScan “Fingerprinting”



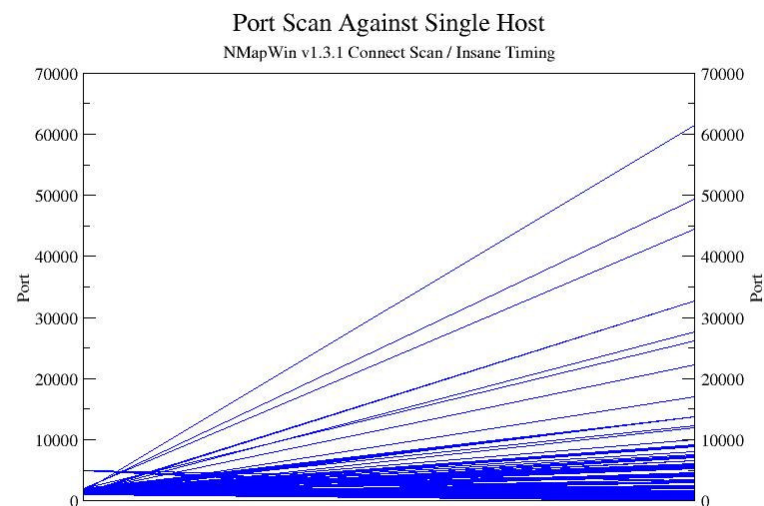
nmap 3.00 default (RH 8.0)



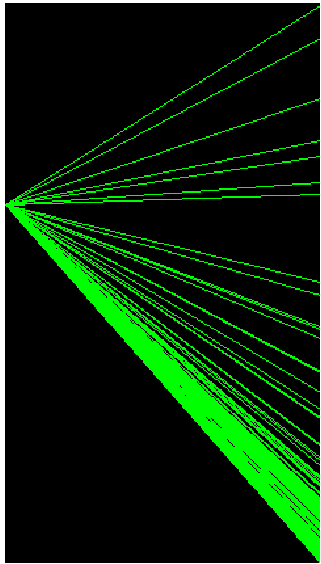
nmap 3.00 udp scan (RH 8.0)



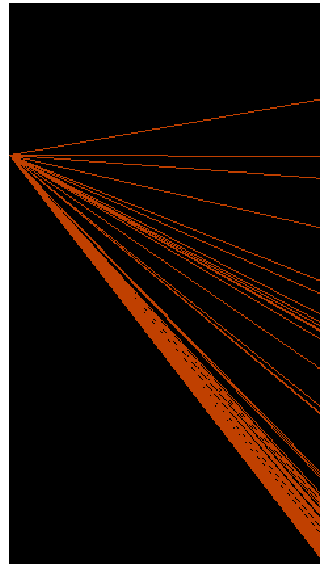
Superscan 3.0



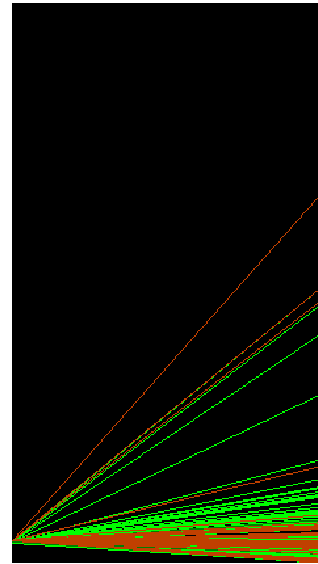
Nmap Win 1.3.1



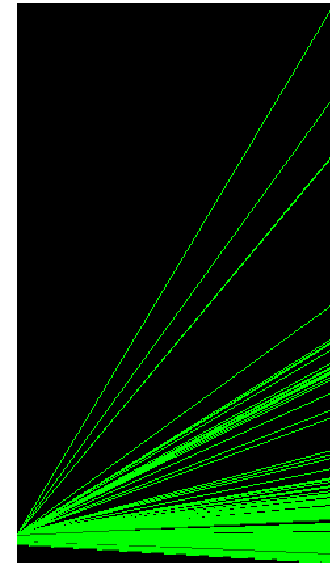
nmap 3 (RH8)



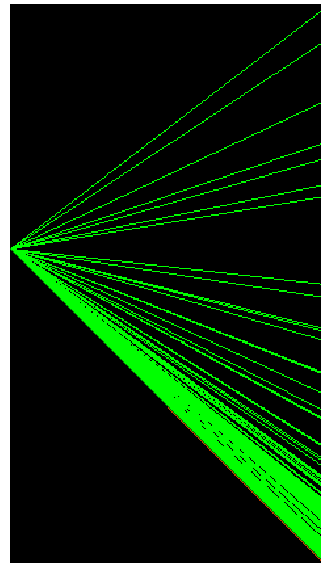
nmap 3 UDP (RH8)



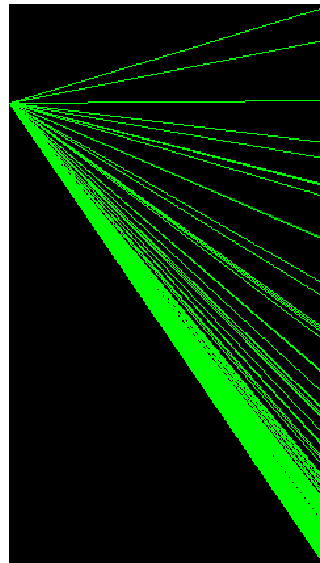
scanline 1.01 (XP)



SuperScan 3.0 (XP)



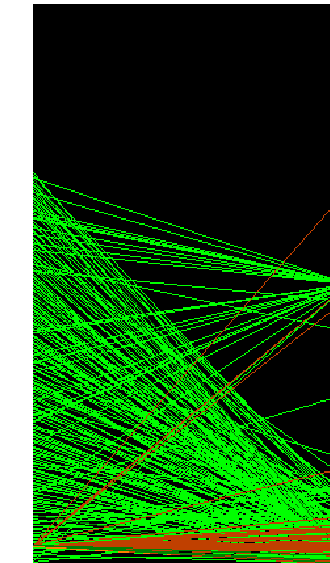
NMapWin 3 (XP)



nmap 3.5 (XP)



nikto 1.32 (XP)



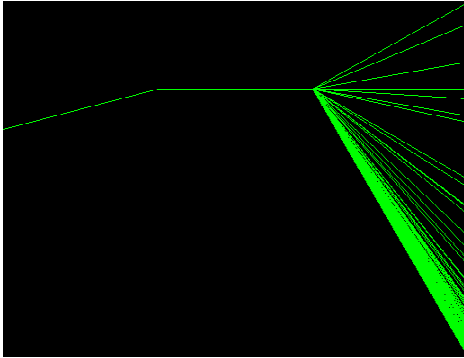
SuperScan 4.0 (XP)



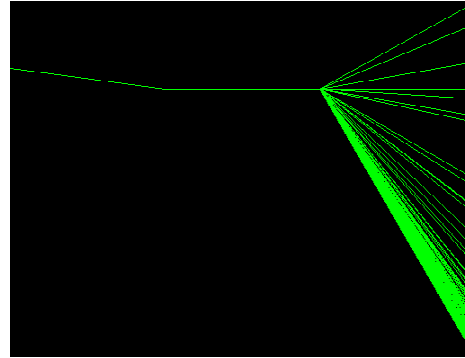
Demo

Exploring nmap 3.0 in depth

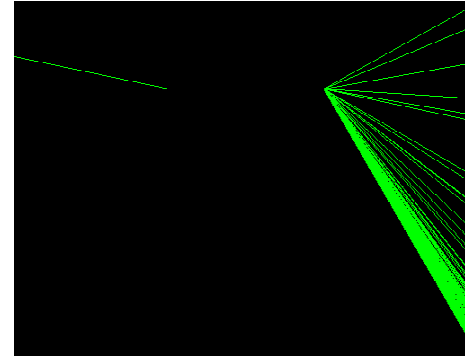
(port to IP to IP to port)



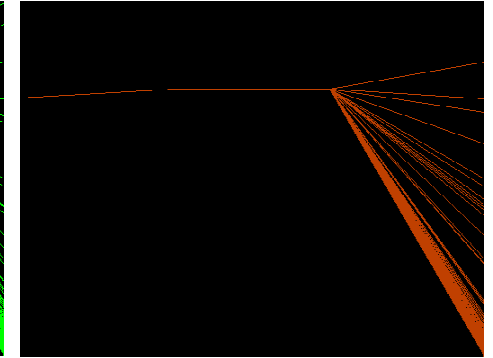
default (root)



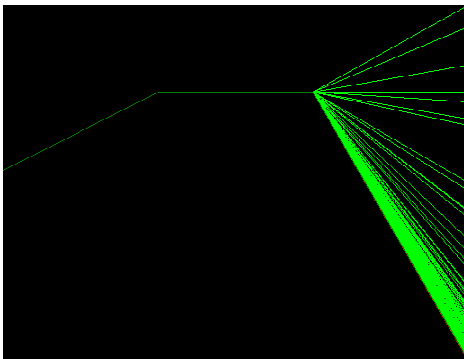
stealth FIN (-sF)



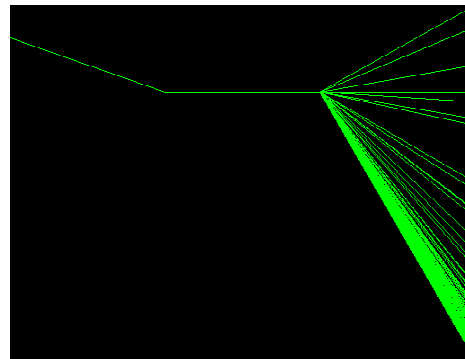
NULL (-sN)



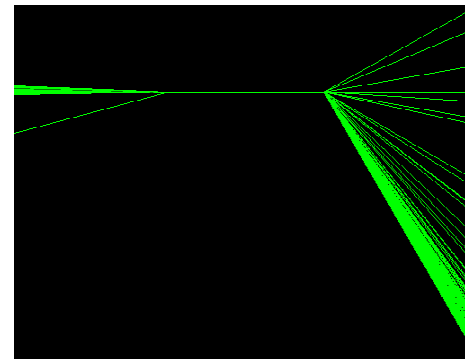
UDP (-sU)



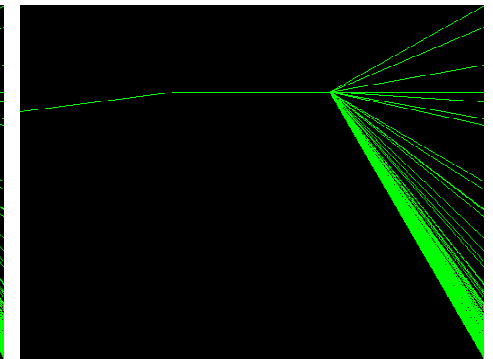
SYN (-sS -O)



stealth SYN (-sS)



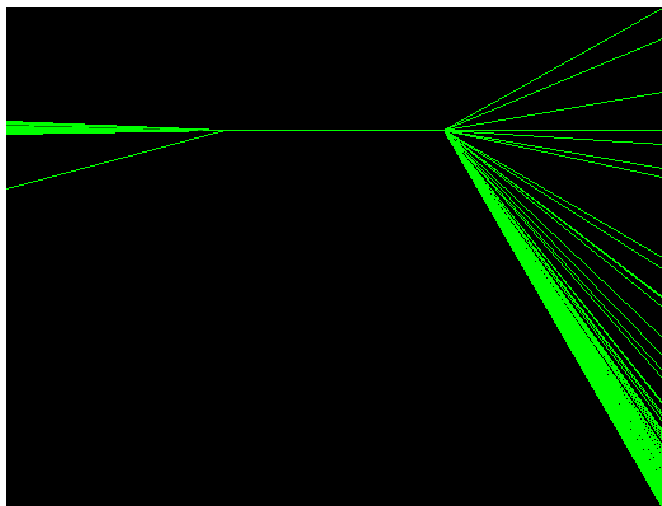
CONNECT (-sT)



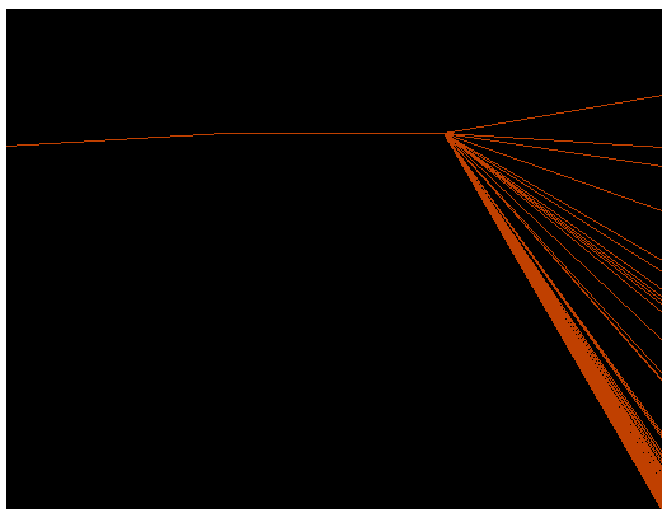
XMAS (-sX)

nmap within Nessus

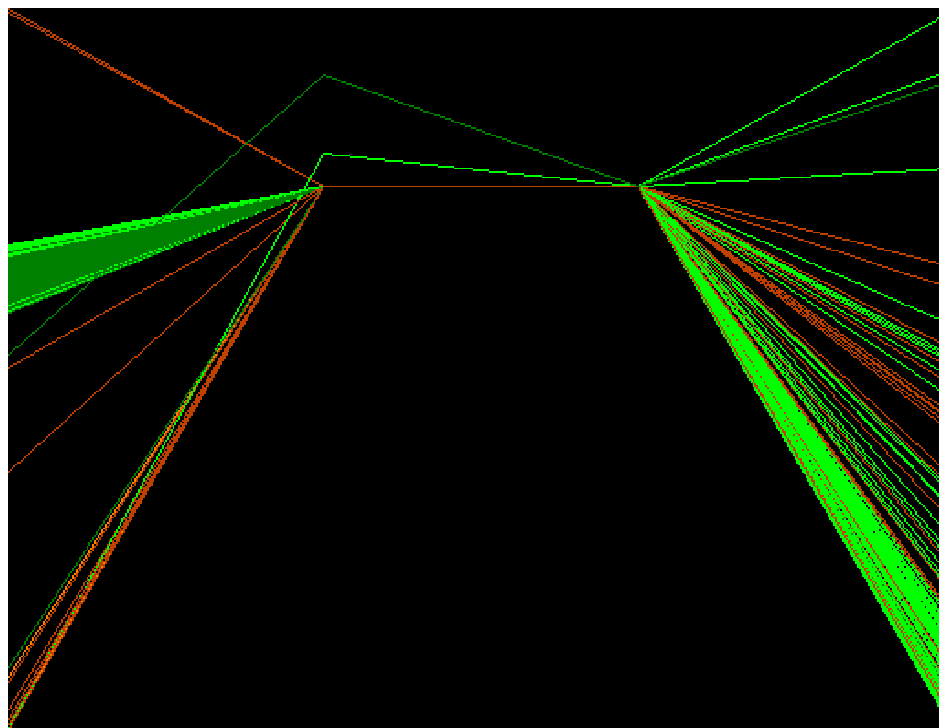
(port to IP to IP to port)



CONNECT (-sT)

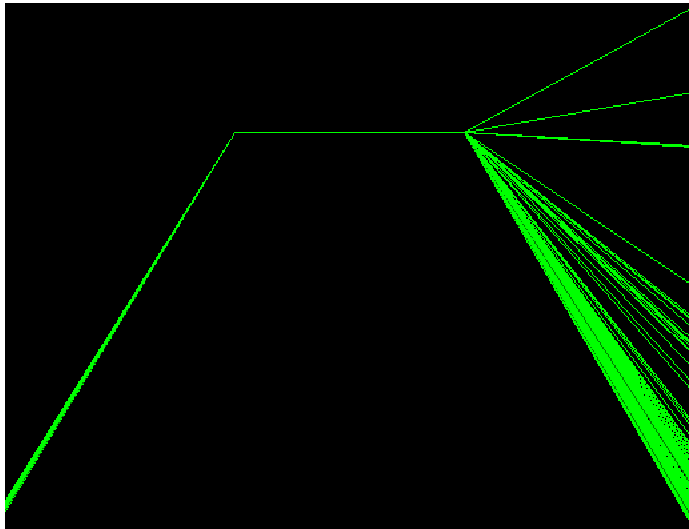


UDP (-sU)

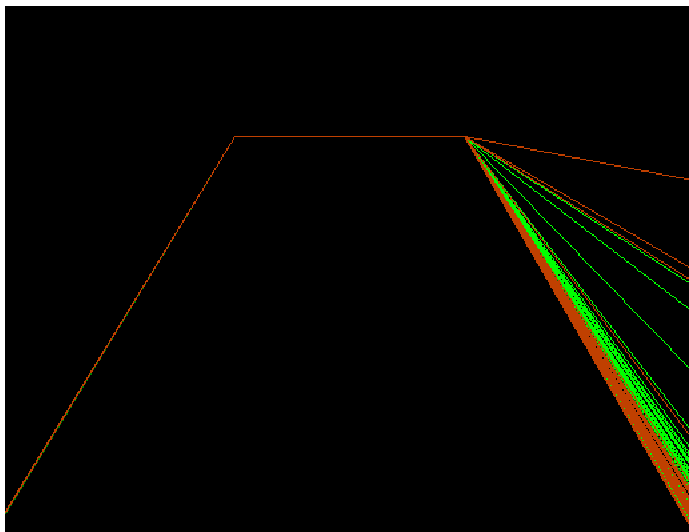


Nessus 2.0.10

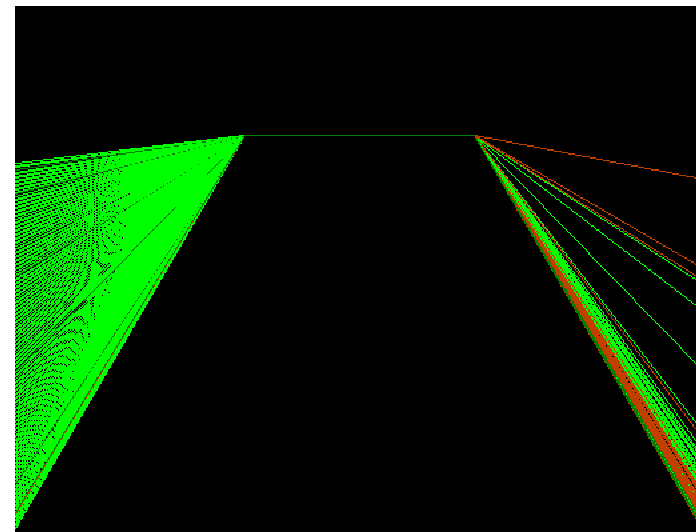
Codebase Evolution



SuperScan 3.0



scanline 1.01

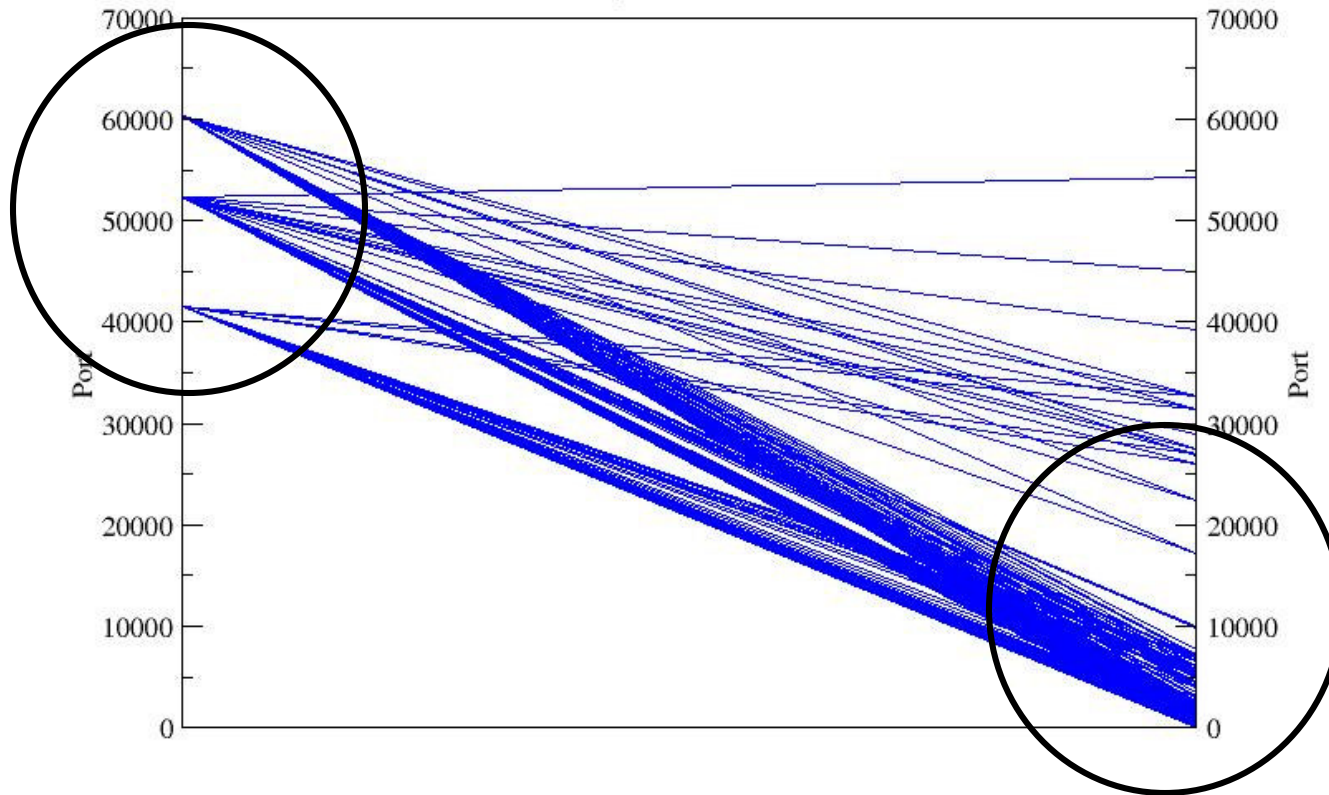


SuperScan 4.0

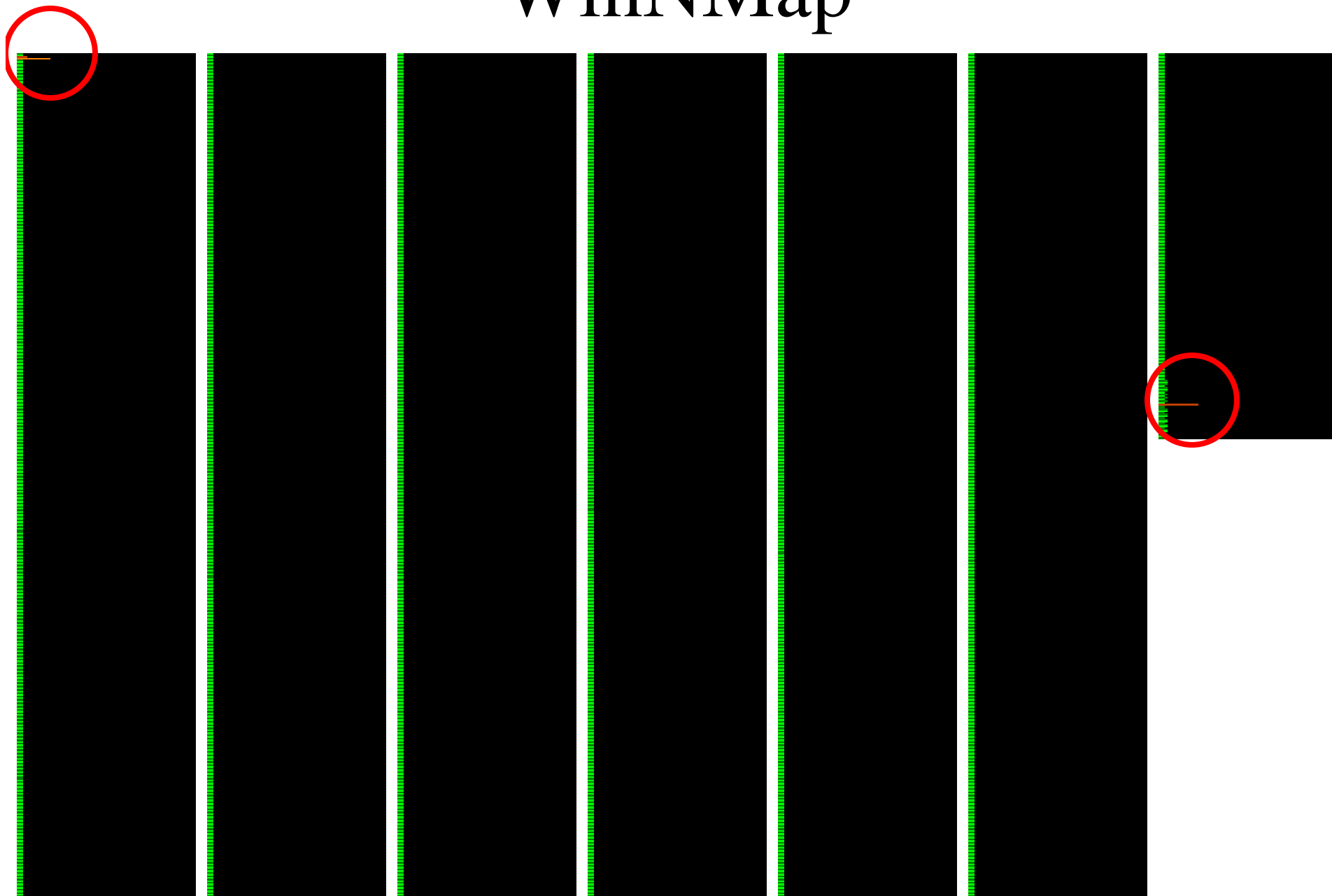
Three Parallel Scans

Port Scan Against Single Host

nmap 3.00 UDP Scan



WinNMap



SuperScan 4.0

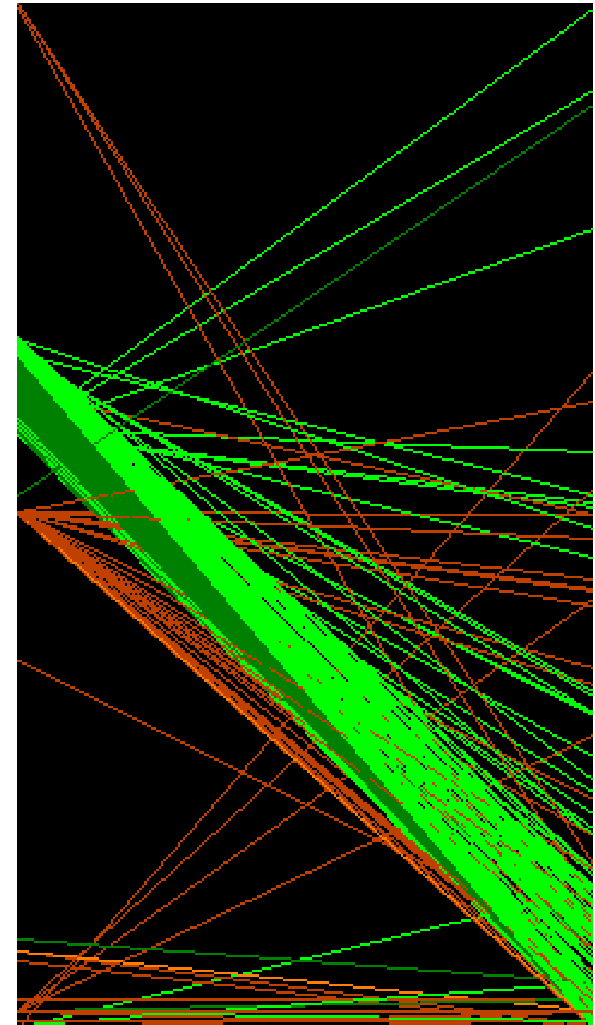
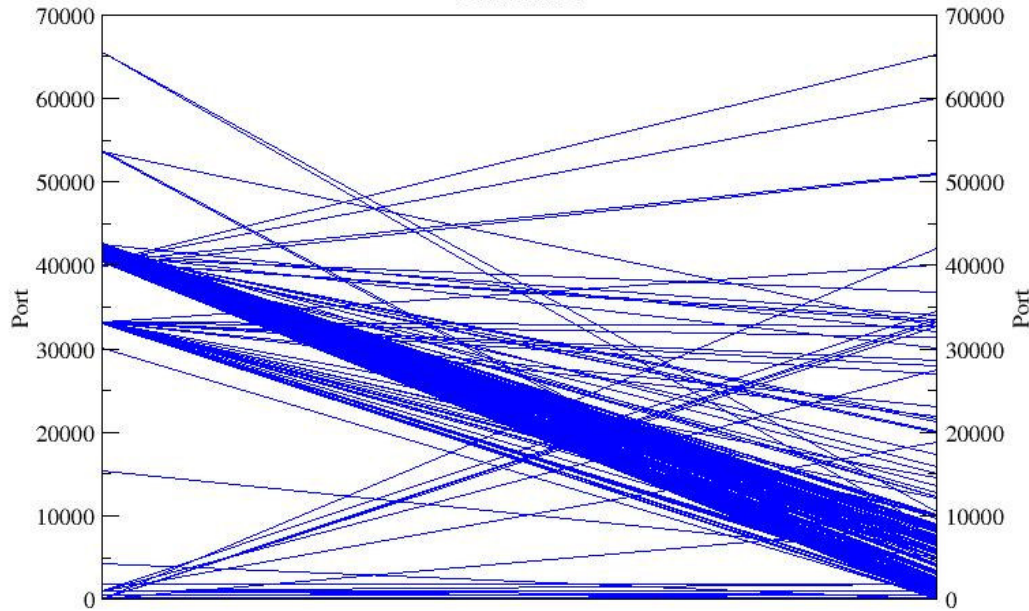


Example 4: Vulnerability Scanner

Nessus 2.0.10

Vulnerability Scan Scan Against Single Host

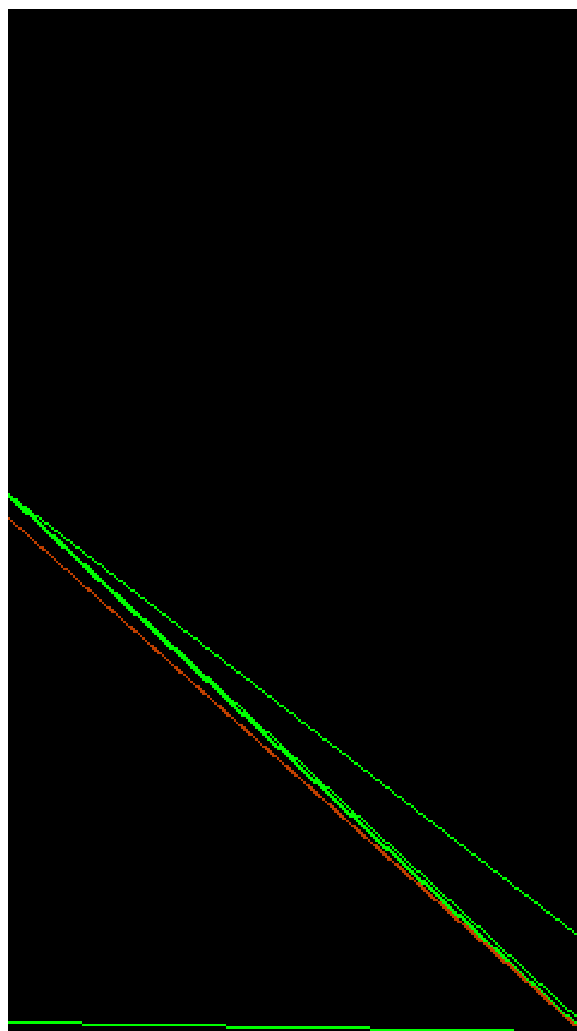
nessus 2.0.10



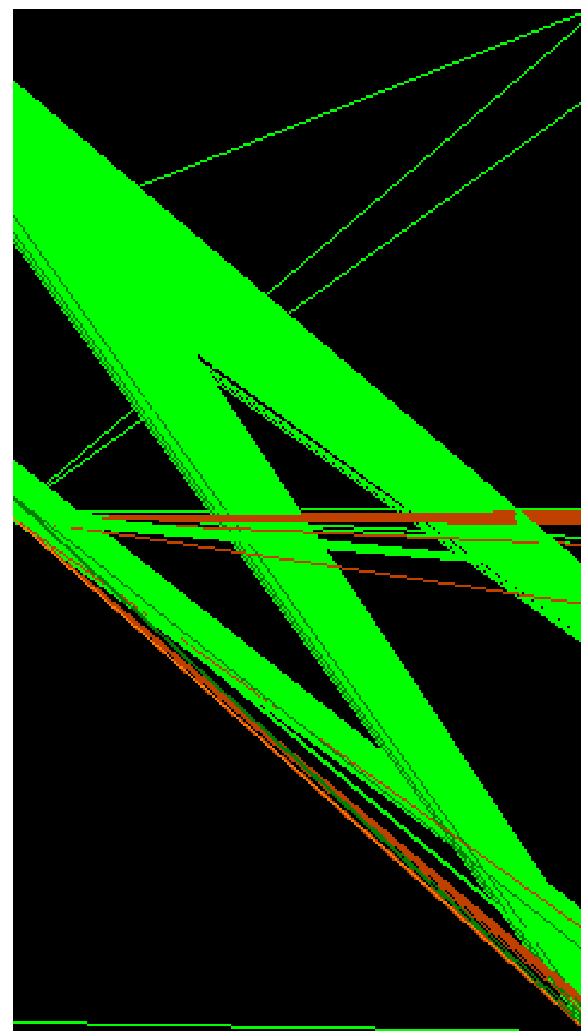
Sara 5.0.3



Light

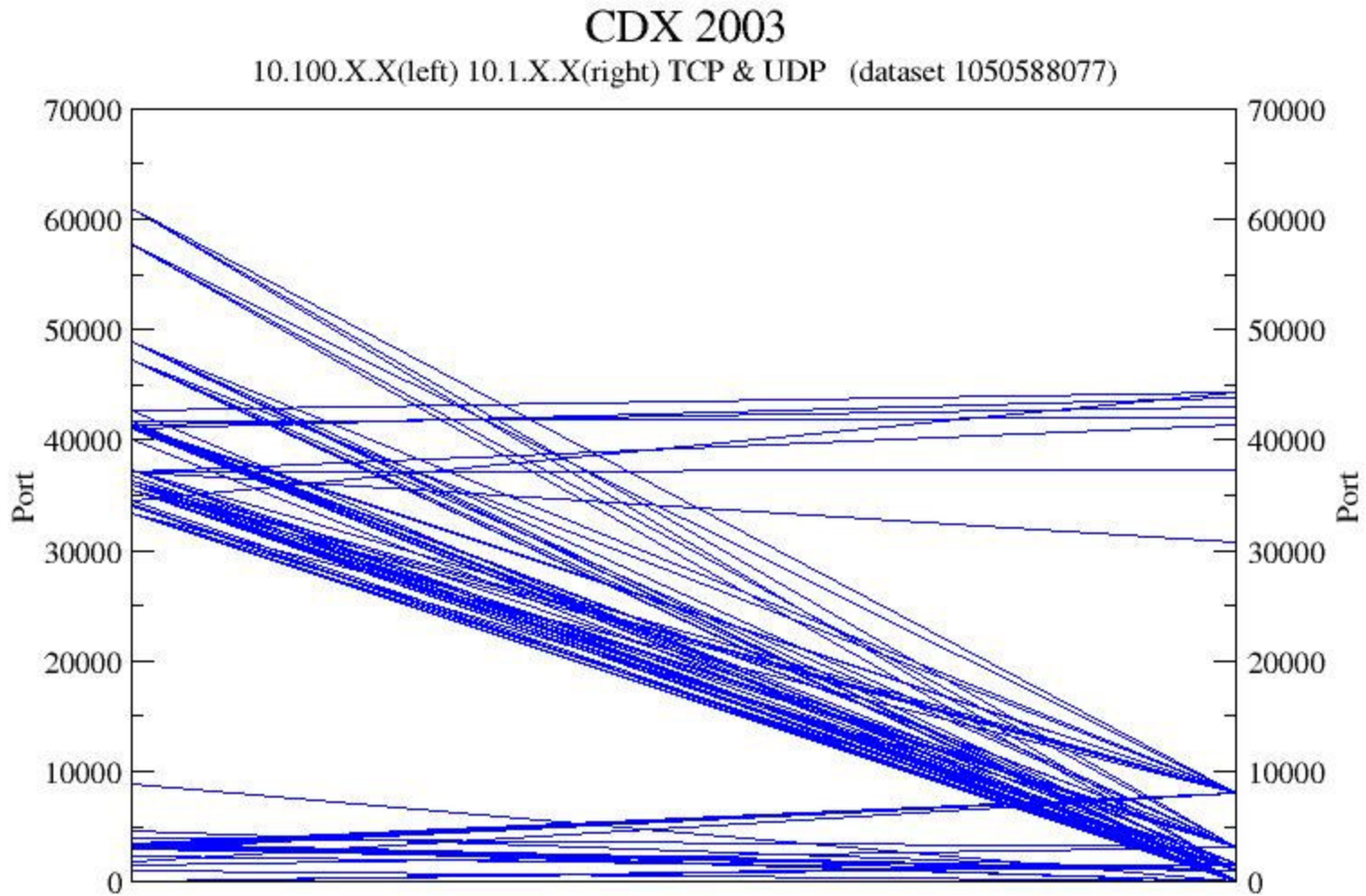


Medium



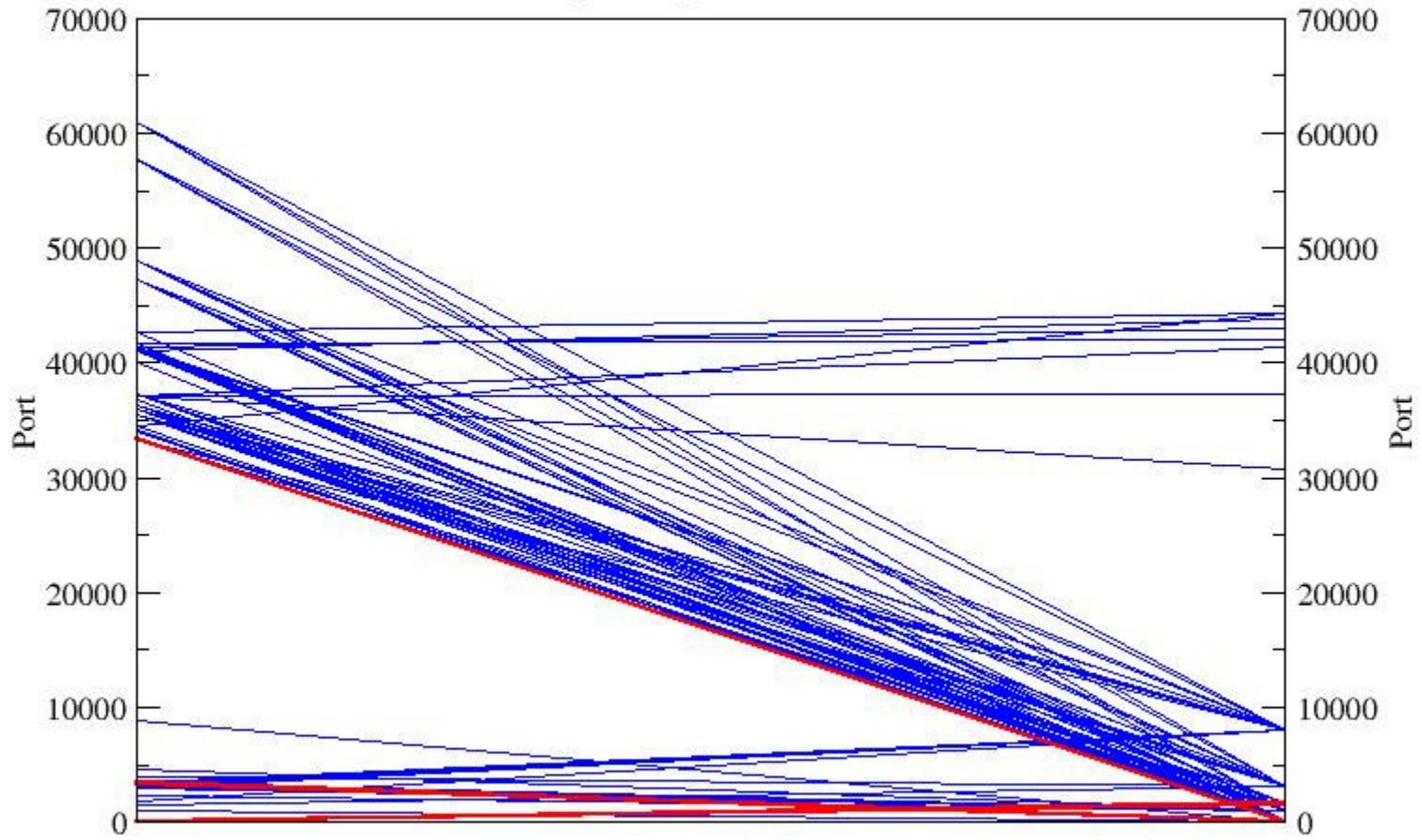
Heavy

Example 5: Wargame

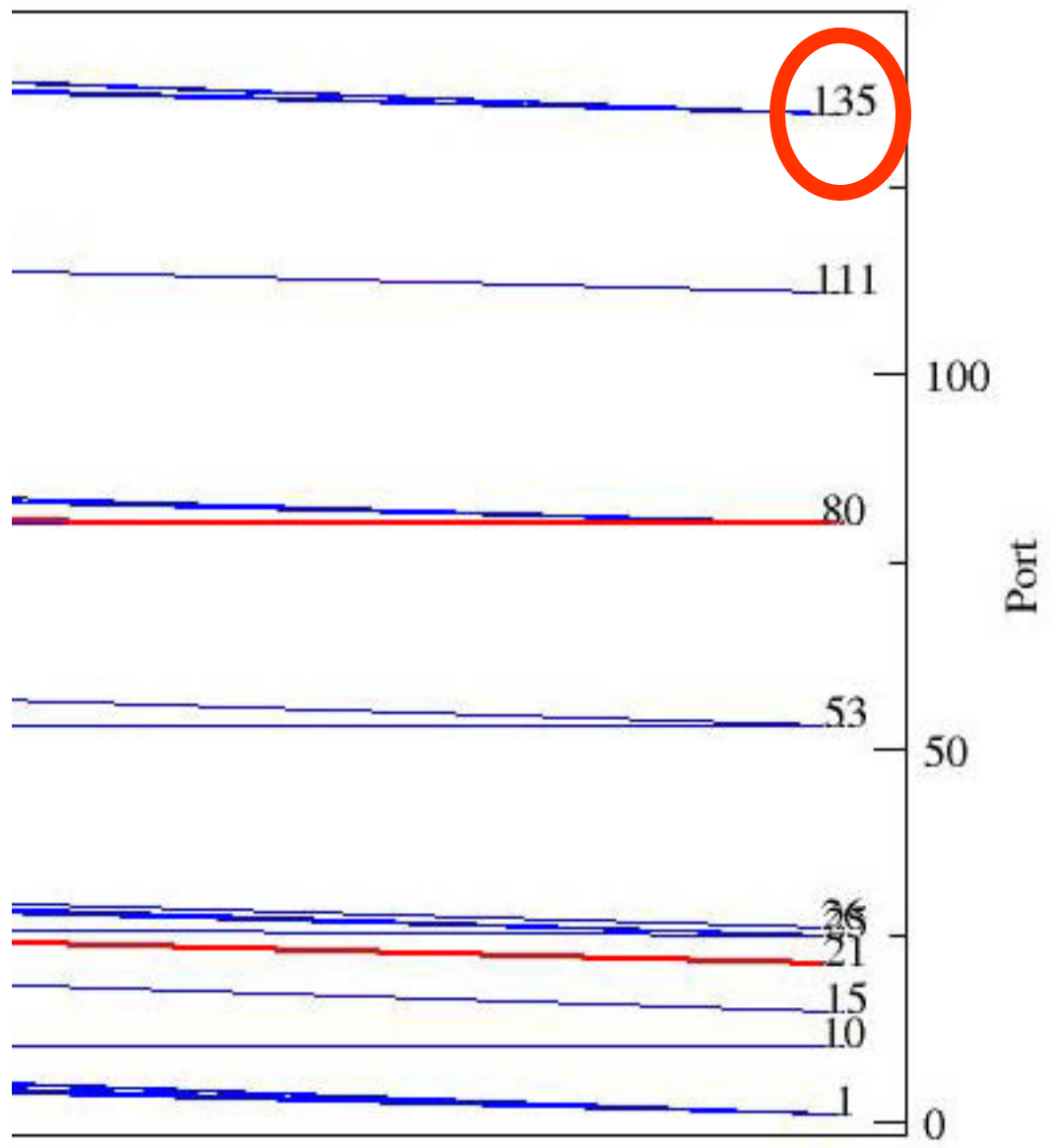


CDX 2003

10.100.X.X(left) 10.1.X.X(right) Target and Source Sets (dataset 1050588077)



Demo



Findings (Strengths)

- Tools can be fingerprinted
- Threading / multiple processes visible
- OS/Application features visible
- Sequence of ports scanned visible
- Useful against slow scans
- Useful against distributed scans

Findings (Weaknesses)

- Spoofing
- Interaction with personal firewalls
- Countermeasures
- Scale / Labeling are issues
- Occlusion is a problem
- Greater interactivity required for forensics and less aggressive attacks
- Some tools are very flexible
- Source code not available for some tools

Future

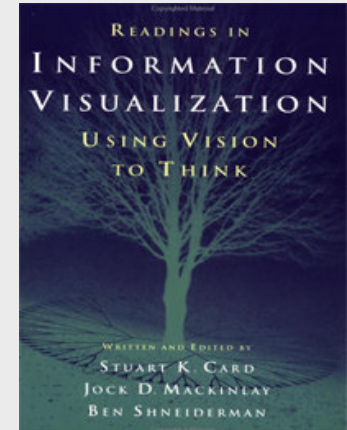
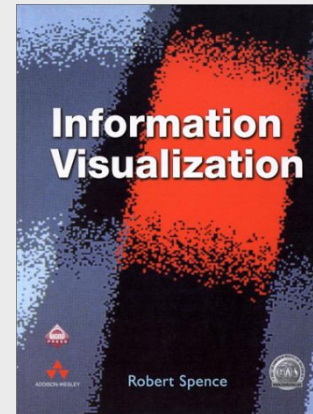
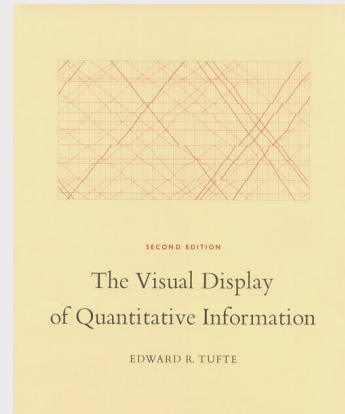
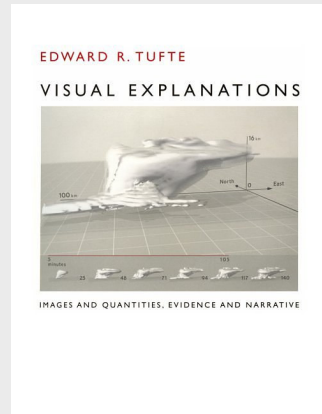
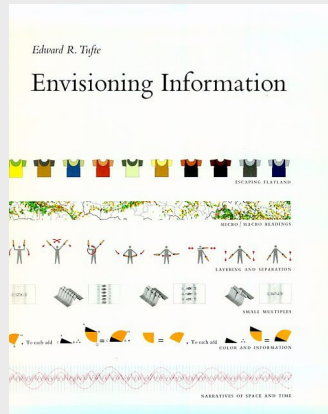
- Active scanning, visualization of Nmap results
- Real-time vs. Offline
- Interesting datasets
- Honeypot Fingerprinting
- Other visualization techniques
- Visualization of protocol attacks
- Visualization of application layer attacks
- Visualization of physical layer attacks (?)
- Code up some stand-alone tools

Where to go for more information...

- www.rumint.com - for latest version of tool
- Course websites
 - http://www.cc.gatech.edu/classes/AY2004/cs7450_spring/detailref.html
 - <http://people.cs.vt.edu/~north/infoviz/>
 - <http://graphics.stanford.edu/courses/cs448b-04-winter/>
 - <http://www.otal.umd.edu/Olive/>

More Information

Information Visualization



- Envisioning Information by Tufte
- The Visual Display of Quantitative Information by Tufte
- Visual Explanations by Tufte
- Information Visualization by Spence
- Information Visualization: Using Vision to Think by Card
- See also the Tufte road show, details at www.edwardtufte.com

What's on the CD

- rumint visualization tool
- tcpdump | perl | xmgrace
 - howto
 - sample scripts
- gallery of classic visualizations (w/links)
- webpage with security infovis links
- this talk

Acknowledgements

- 404.se2600
 - icer
 - StricK
 - Rockit
 - Hendrick
 - Clint
- Kulsoom Abdullah
 - <http://www.prism.gatech.edu/~gte369k/csc/>
- Dr. John Stasko
 - <http://www.cc.gatech.edu/~john.stasko/>
- Dr. Wenke Lee
 - <http://www.cc.gatech.edu/~wenke/>



Questions?

Backup Slides

Data Format

- tcpdump outputs somewhat verbose output

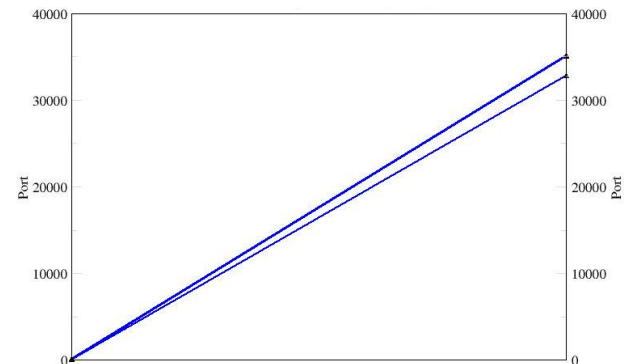
```
09:02:01.858240 0:6:5b:4:20:14 0:5:9a:50:70:9 62:  
10.100.1.120.4532 > 10.1.3.0.1080: tcp 0 (DF)
```

- parse.pl cleans up output

```
09 02 01 858240 0:6:5b:4:20:14 0:5:9a:50:70:9  
10.100.1.120.4532 10.100.1.120 4532 10.1.3.0.1080 10.1.3.0  
1080 tcp
```

- analyze.pl extracts/formats for Grace.

```
0 4532  
1 1080  
0 4537  
1 1080  
0 2370  
1 1080
```



Required Files

Perl, tcpdump and grace need to be installed.

- <http://www.tcpdump.org/>
- <http://www.perl.org/>
- <http://plasma-gate.weizmann.ac.il/Grace/>

to install grace...

Download RPMs (or source)

<ftp://plasma-gate.weizmann.ac.il/pub/grace/contrib/RPMS>

The files you want

grace-5.1.14-1.i386.rpm

pdflib-4.0.3-1.i386.rpm

Install

```
#rpm -i pdflib-4.0.3-1.i386.rpm
```

```
#rpm -i grace-5.1.14-1.i386.rpm
```

Hello World Example

```
# tcpdump -lnnq -c10 | perl parse.pl | perl analyze.pl  
  | outfile.dat  
# xmgrace outfile.dat &
```

Optionally you can run xmgrace with an external format language file...

```
# xmgrace outfile.dat -batch formatfile
```

See ppt file for more detailed howto information

Hello World Example (cont)

Optionally you can run xmgrace with an external format language file...

```
xmgrace outfile.dat -batch formatfile
```

formatfile is a text file that pre-configures Grace e.g.

```
title "Port Scan Against Single Host"  
subtitle "Superscan w/ports 1-1024"  
yaxis label "Port"  
yaxis label place both  
yaxis ticklabel place both  
xaxis ticklabel off  
xaxis tick major off  
xaxis tick minor off  
autoscale
```

To Run Demo

See readme.txt

Two demo scripts...

- runme.bat (uses sample dataset)
- runme_sniff.bat (performs live capture, must be root)

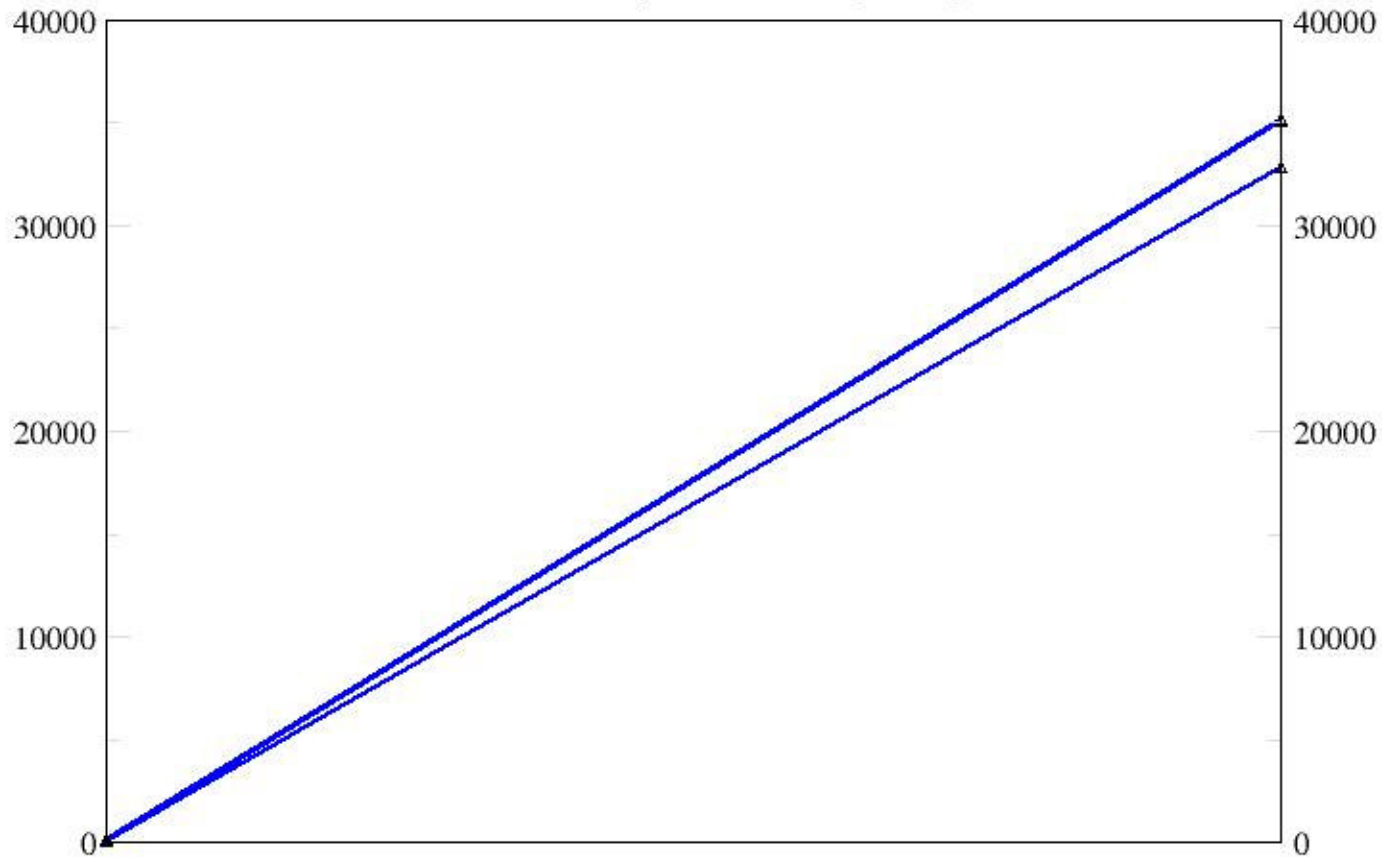
Note: you must modify the IP address variable in the Analyzer script. (See analyzer2.pl for example)

Example 1 - Baseline

- Normal network traffic
 - FTP, HTTP, SSH, ICMP...
- Command Line
 - Capture Raw Data
 - `tcpdump -l -nnqe -c 1000 tcp or udp | perl parse.pl > exp1_outfile.txt`
 - Run through Analysis Script
 - `cat exp1_outfile.txt | perl analyze_1a.pl > output1a.dat`
 - Open in Grace
 - `xmgrace output1a.dat &`

Example 1 - Baseline

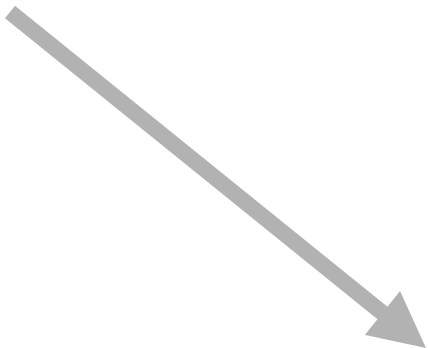
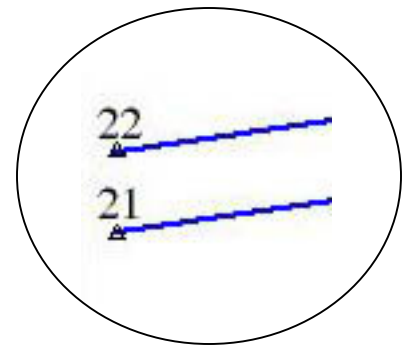
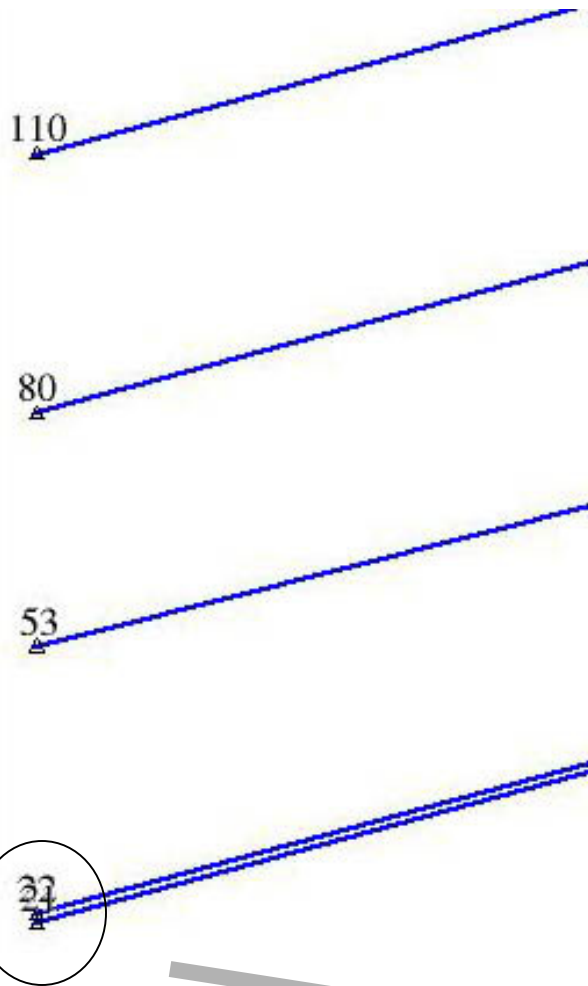
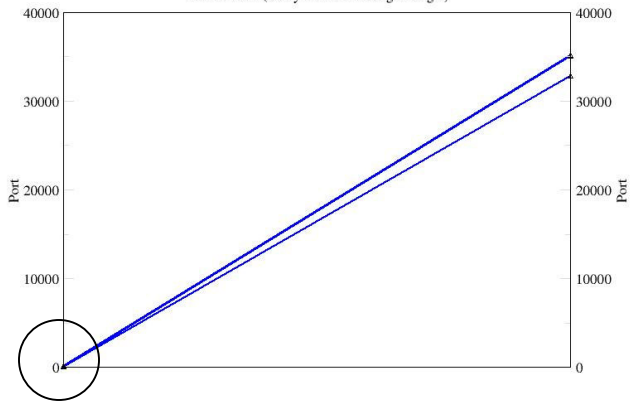
Normal Network Traffic (SMTP, HTTP, SSH, FTP, ICMP)
TCP & UDP (Many Sources to Single Target)



Remote Machine's Ports

Target Machine's Ports

Normal Network Traffic (SMTP, HTTP, SSH, FTP, ICMP)
TCP & UDP (Many Sources to Single Target)



Example 2 - PortScan

- Light “normal” network traffic (HTTP)
- Command Line
 - Run 2a.bat (chmod +x 2a.bat)

```
echo running experiment 2  
echo 1-1024 port scan
```

```
tcpdump -l -nnqe -c 1200 tcp or udp > raw_outfile_2.txt  
cat raw_outfile_2.txt | perl parse_2a.pl > exp2_outfile.txt  
cat exp2_outfile.txt | perl analyze_2a.pl > output_2a.dat  
xmgrace output_2a.dat &
```

```
echo experiment 2 completed
```

Example 3- PortScan “Fingerprinting”

Tools Examined:

- Nmap Win 1.3.1 (on top of Nmap 3.00)

XP Attacker

(<http://www.insecure.org/nmap/>)

- Nmap 3.00

RH 8.0 Attacker

(<http://www.insecure.org/nmap/>)

- Superscan 3.0

RH 8.0 Attacker

(<http://www.foundstone.com/index.htm?subnav=resources/navigation.htm&subcontent=/resources/proddesc/superscan.htm>)

Example 4: Vulnerability Scanner

- Attacker: RH 8.0 running Nessus 2.0.10
- Target: RH 9.0

Example 5: Wargame

- Attackers: NSA Red Team
- Defenders: US Service Academies

Defenders lock down network, but must provide certain services

Dataset - <http://www.itoc.usma.edu/cdx/2003/logs.zip>