

Reassembling the Onion: Event and Log Correlation



Gregory W Zill, MBA, CISSP
me@gregoryzill.name

Reassembling the Onion: Event and Log Correlation

- Introduction
 - Intrusion Detection
 - Network Forensics
- Logging Sources
- Log Integrity and Time Sensitivity
 - Acquisition
 - Transmission
 - Collection
 - Storage
- Log and Event Normalization
 - Classification
 - Thresholds
- Network logging via syslog-ng

Reassembling the Onion: Event and Log Correlation

- Introduction
 - Security Now!

Event Correlation – finding relationships
between two or more log entries



Reassembling the Onion: Event and Log Correlation

- Intrusion Detection
 - Provide an additional layer of security that notifies when potential attack signatures are happening on your network
- Network Forensics
 - Investigating digital evidence for use in criminal proceedings

Reassembling the Onion: Event and Log Correlation

- Network Forensics Tools
 - Ethereal / Wireshark \$\$
 - TCPDump \$
 - NetIntercept \$\$\$\$\$\$
 - NetDetector \$\$\$\$\$\$
 - TCPFlow \$
 - Snort \$
 - Impost Ø

Even with the best of maps and instruments, we can never
fully chart our journeys. ~Gail Pool

Reassembling the Onion: Event and Log Correlation

- Logging Sources
 - Anti-malware software
 - IDS / IPS
 - Remote Access
 - Web Proxy
 - Vulnerability Management
 - Authentication
 - Routers Firewalls

Reassembling the Onion: Event and Log Correlation

- Logging Sources
 - Anti-malware example

8/3/2007 4:58:52 PM SYSTEM 1748 VRDB
(Virus Recovery Database) generation was
successfully completed.

Reassembling the Onion: Event and Log Correlation

- Logging Sources

- IDS example:

[illegible]

```
[**] [119:2:1] http inspect: DOUBLE DECODING ATTACK [**]
```

[Classification: Unknown] [Priority: 3]

Event ID: 17 Event Reference: 17

08/30/06-02:37:00.540541 68.15.239.23:2642 -> 216.52.17.134:80

TCP TTL:127 TOS:0x0 ID:37993 IpLen:20 DgmLen:196 DF

AP Seq: 0x5EB5C918 Ack: 0x72BBC708 Win: 0xFFFF TcpLen: 20

75 65 3B 20 73 5F 73 71 3D 61 70 70 6C 65 73 75	ue; s_sq=applesu
70 65 72 67 6C 6F 62 61 6C 25 33 44 25 32 35 32	perglobal%3D%252
36 70 69 64 25 32 35 33 44 41 70 70 6C 65 25 32	6pid%253DApple%2
35 32 35 32 30 25 32 35 32 35 32 38 55 53 25 32	52520%252528US%2
35 32 35 32 39 25 32 35 32 36 70 69 64 74 25 32	52529%2526pidt%2
35 33 44 31 25 32 35 32 36 6F 69 64 25 32 35 33	53D1%2526oid%253
44 68 74 74 70 25 32 35 32 35 33 41 2F 2F 77 77	Dhttp%25253A//ww
77 2E 61 70 70 6C 65 2E 63 6F 6D 2F 69 70 6F 64	w.apple.com/ipod
2F 61 64 73 2F 64 79 6C 61 6E 2F 25 32 35 32 36	/ads/dylan/%2526
6F 74 25 32 35 33 44 41 0D 0A 0D 0A	ot%253DA....

Reassembling the Onion: Event and Log Correlation

- Logging Sources
 - Web Proxy example:

```
1186364358.358      2 192.168.0.21
TCP_NEGATIVE_HIT/404 345 GET
http://i.i.com.com/cnwk.1d/css/ssa/7_site/3_e
dition-2001_pageType.css - NONE/- text/css
```

Reassembling the Onion: Event and Log Correlation

- Logging Sources
 - Firewall example:

```
Aug  4 17:45:09 192.168.0.1 Aug 04 2007
17:50:46: %PIX-4-106023: Deny tcp src
outside:67.108.68.62/8080 dst
inside:firewall/23168 by access-group
"outside"
```

Reassembling the Onion: Event and Log Correlation

- Syslog-ng – embodies the next generation of logging systems, and is the first truly flexible and scalable system logging application
 - Availability
 - Wide range of operating systems
 - Flexible source configurations
 - Flexible destination options
 - Flexible filter capabilities

<http://www.balabit.com>

Reassembling the Onion: Event and Log Correlation

- Types of logged information
 - Client requests and server responses
 - Account information
 - Usage information
 - Significant operational actions

Reassembling the Onion: Event and Log Correlation

- Compliance logging
 - Federal Information Security Management Act
 - Gramm-Leach-Bliley Act (GLBA)
 - Health Insurance Portability Accountability Act
 - Sarbanes-Oxley (SOX)
 - Payment Card Industry Data Security Standard

Reassembling the Onion: Event and Log Correlation

- Log storage
 - Multiple log sources
 - Inconsistent log content
 - Inconsistent timestamps
 - Inconsistent log format
 - Volume

Reassembling the Onion: Event and Log Correlation

- Log security
 - Limit access to log files and sources
 - Avoid recording unneeded sensitive information
 - Secure archived logs
 - Secure the processes that generate logs
 - Configure robust logging processes
 - Secure log transport
 - Consistent reliable time sources

Reassembling the Onion: Event and Log Correlation

- Log Analysis
 - Meaningful information
 - Drawing conclusions

The superior man, when resting in safety, does not forget that danger may come. When in a state of security he does not forget the possibility of ruin. When all is orderly, he does not forget that disorder may come. Thus his person is not endangered, and his States and all their clans are preserved.

Confucius (551 BC - 479 BC)

Reassembling the Onion: Event and Log Correlation

- Prioritizing log data
 - Log type

Aug 12 17:26:51 omega mysqld[1040]: Version:
'4.0.24_Debian-10sarge2-log' socket:
'/var/run/mysqld/mysqld.sock' port: 3306 Source
distribution

Event Type: Information

Event Source: SecurityCenter

Event Category: None

Event ID: 1800

Date: 7/21/2007

Time: 3:49:16 PM

User: N/A

Computer: ABCD

Description: The Windows Security Center Service has started.

Reassembling the Onion: Event and Log Correlation

- Prioritizing log data
 - Log type
 - Uniqueness

syslog:Aug 12 17:39:20 omega mysqld[1039]:
/usr/sbin/mysqld: ready for connections.

daemon.log:Aug 12 17:39:20 omega
mysqld[1039]: /usr/sbin/mysqld: ready for
connections.

Reassembling the Onion: Event and Log Correlation

- Prioritizing log data
 - Log type
 - Uniqueness
 - Log source

/usr/libexec/mysqld: ready for connections.

Aug 12 17:39:20 omega mysqld[1039]:
/usr/sbin/mysqld: ready for connections.

Reassembling the Onion: Event and Log Correlation

- Prioritizing log data
 - Log type
 - Uniqueness
 - Log source
 - Source or destination in log

Aug 12 21:55:30 192.168.0.1 Aug 12 2007
21:55:30: %PIX-4-106023: Deny icmp src
outside:75.126.203.75 dst inside:firewall (type
0, code 0) by access-group "outside"

Reassembling the Onion: Event and Log Correlation

- Prioritizing log data
 - Log type
 - Uniqueness
 - Log source
 - Source or destination in log
 - Time of day or day of week

ClamAV update process started at Mon Apr 2
12:05:01 2007

Reassembling the Onion: Event and Log Correlation

- Prioritizing log data
 - Log type
 - Uniqueness
 - Log source
 - Source or destination in log
 - Time of day or day of week
 - Frequency

Jun 16 23:45:36 pix last message repeated 37 times

Reassembling the Onion: Event and Log Correlation

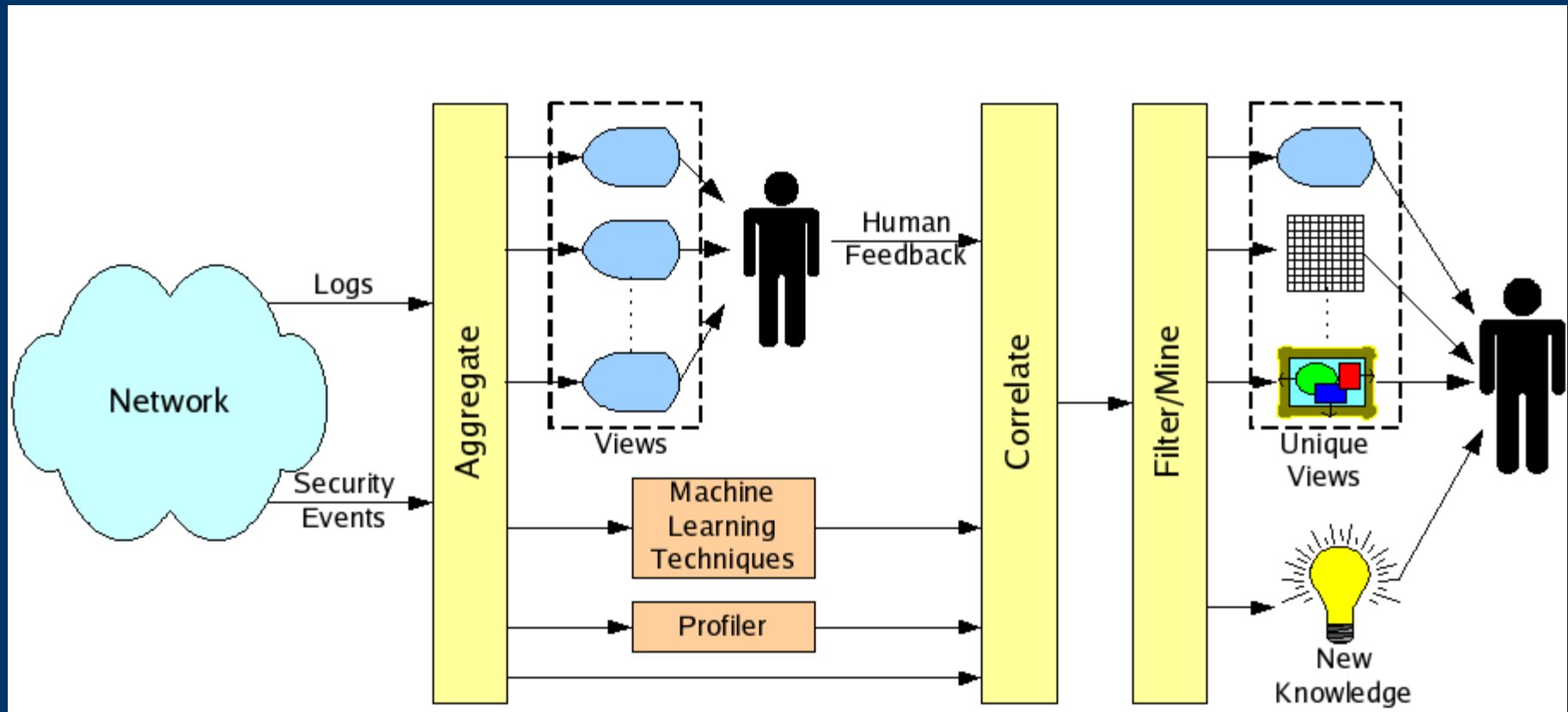
Common attacks and associated log recognition

Attack	Log								
	Syslog	Firewall	Netflow	TCP	DNS	Auth	Web	Mail	FTP
Dictionary	×	×	×	×		×	×	×	×
FTP-Write	×			×		×			×
Imap	×	×	×	×				×	
Named	×		×		×				
Phf	×			×			×		
Sendmail	×	×	×	×	×	×		×	
Xsnoop	×		×						
Apache2	×	×	×	×			×		
Back	×			×			×		
Mailbomb	×	×	×	×				×	
SYN Flood	×	×	×	×	×				
Ping of Death		×	×	×					
Process Table		×	×	×				×	
Smurf			×	×					
Udpstorm			×	×	×				

*Abad, Christina, Univ of Illinois, NCSA

Reassembling the Onion: Event and Log Correlation

Ideal Log Correlation Process



*Abad, Christina, Univ of Illinois, NCSA

Reassembling the Onion: Event and Log Correlation

Commercial Links:

- ♦ Security Center <http://tenablesecurity.com>
- ♦ LogCaster <http://rippletech.com>
- ♦ EventTracker <http://prismmicrosys.com>
- ♦ EventSentry <http://netikus.net>

Open Links:

- ♦ Toukon <http://sourceforge.net/projects/toukon>
 - ♦ Palantir <http://sourceforge.net/projects/palantir3>
 - ♦ DAD <http://sourceforge.net/projects/lassie>
 - ♦ SNARE <http://sourceforge.net/projects/snare>
 - ♦ OSSM <http://sourceforge.net/projects/os-sim>
-
-

Reassembling the Onion: Event and Log Correlation

TENABLE SECURITY CENTER 3

Bill Smith
Customer SN: 10
Role: manager

Vulnerabilities Events Scans Reporting Policies Users Assets Log Out

Analysis Tools

Select a tool:

Time Summary

apply

reset

Date Filter

Time Frame:

Last 5 Days

Start Time

(MM/DD/YYYY HH:MM:SS):

03/25/2006 15:48

End Time

(MM/DD/YYYY HH:MM:SS):

03/30/2006 15:48

Network Filter

Asset Lists:

-- none selected --

CIDR or IP address(es):

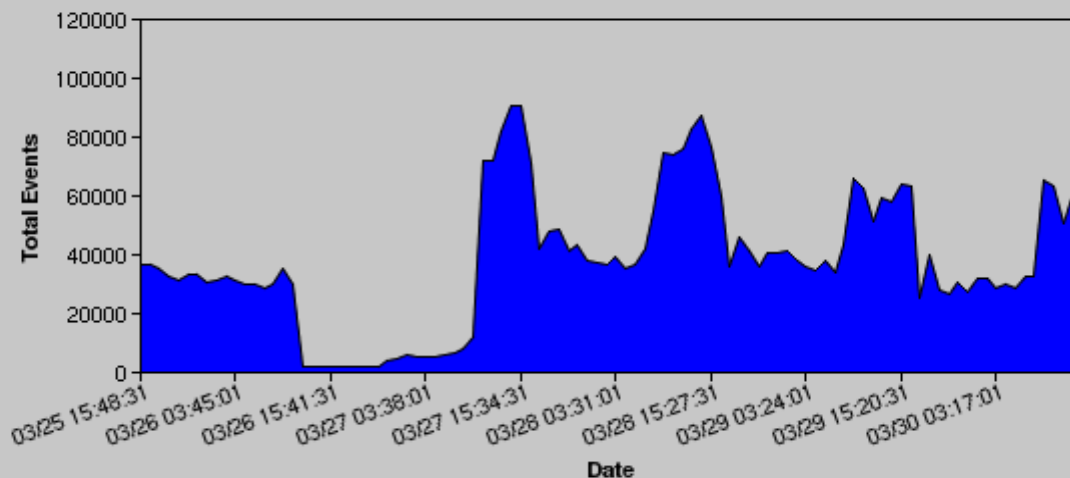
Port(s):

=

(comma separated):

Log Data Analysis

Events over Time



Reassembling the Onion: Event and Log Correlation

TENABLE SECURITY CENTER 3

Bill Smith
Customer SN: 10
Role: manager

Vulnerabilities Events Scans Reporting Policies Users Assets Log Out

Analysis Tools

Select a tool:

Events Summary

apply

reset

Log Date Filter

Date: 2006-03-31

Start Time (HH:MM:SS):

End Time (HH:MM:SS):

Network Filter

Asset Lists:

-- none selected --

CIDR or IP address(es):

Port(s): =

(comma separated):

Protocol(s): any

Direction:

any

Type Filter

Type:

Any

Correlation Filter

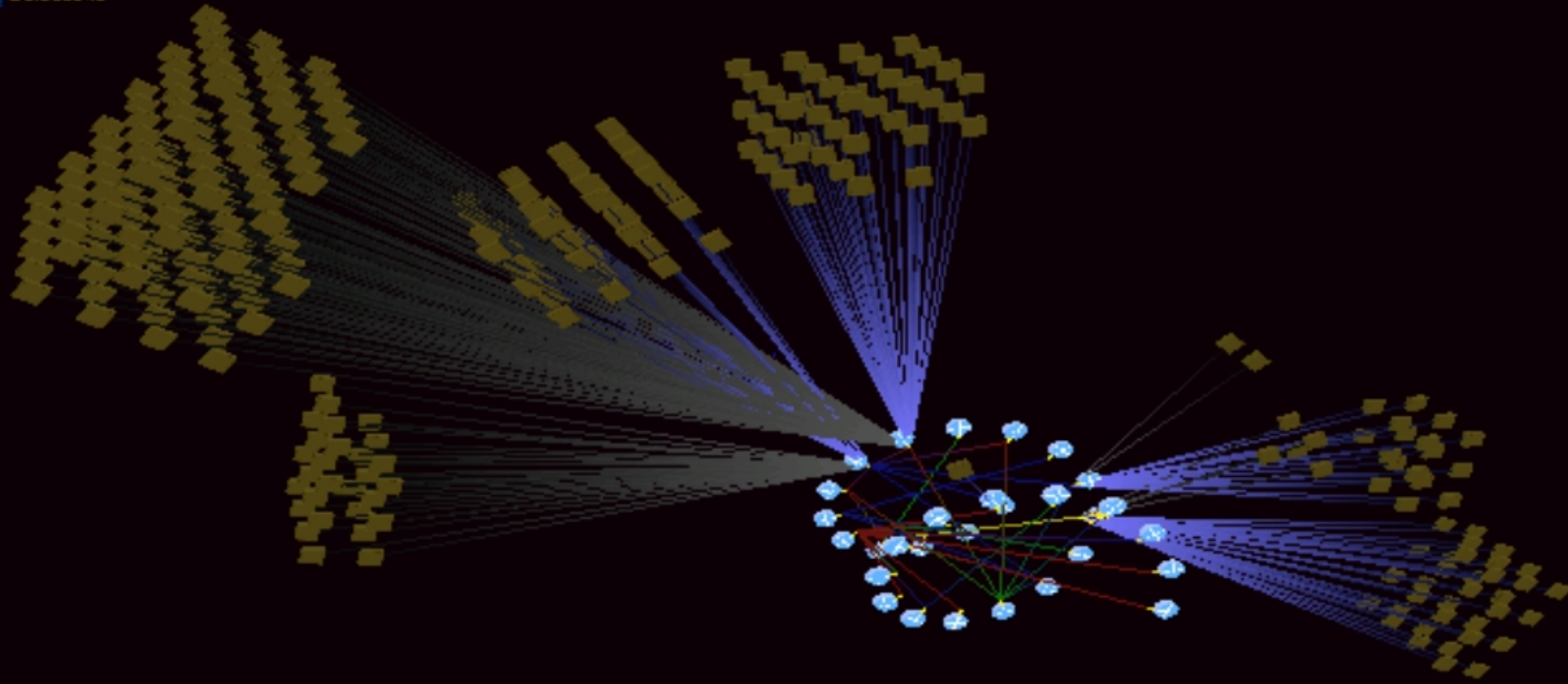
Correlated:

IDS Log Data Analysis

Event	Count	24-Hour Plot
MS-SQL Worm propagation attempt OUTBOUND	395	
MS-SQL version overflow attempt	394	
MS-SQL Worm propagation attempt	394	
ICMP Destination Unreachable Communicati	164	
BARE BYTE UNICODE ENCODING	127	
MISC UPnP malformed advertisement	85	
WEB-CGI redirect access	21	
OVERSIZE REQUEST-URI DIRECTORY	21	
DOUBLE DECODING ATTACK	17	
WEB-CGI campus access	15	
WEB-CGI calendar access	12	
ICMP Source Quench	11	
SCAN FIN	9	
ICMP PING CyberKit 2.2 Windows	9	
ICMP L3retriever Ping	8	
IMAP status overflow attempt	8	
ICMP PING NMAP	6	
WEB-FRONTPAGE /_vti_bin/ access	3	
SNMP request udp	2	
ICMP Destination Unreachable Communicati	2	
WEB-CGI finger access	2	
ICMP PATH MTU denial of service	1	
DNS SPOOF query response with TTL of 1 m	1	
WEB-CGI printenv access	1	

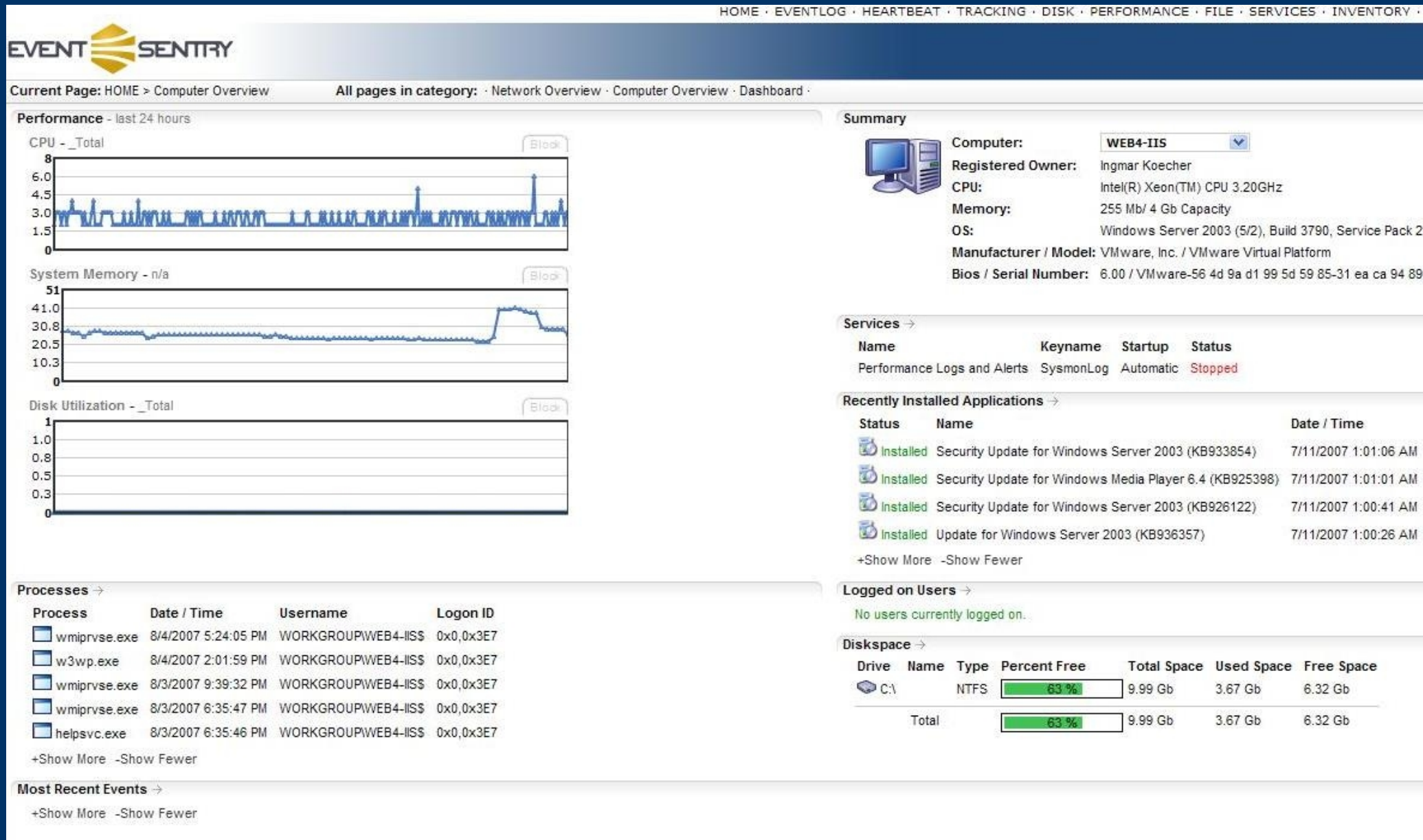
- Vulns/ Ps Graph
- Ports/ IPs Graph
- Dataset Mgmt

Selections



Router IP: 172.28.12.132
connections:
Endpoint count: 18
Router count: 2

Reassembling the Onion: Event and Log Correlation




Reassembling the Onion: Event and Log Correlation

Cannot find server - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites

Address <http://localhost:6161/network> Go Links



SNARE for Windows

Latest Events

Network Configuration

Remote Control Configuration

Objectives Configuration

View Audit Service Status

Apply the Latest Audit Configuration

Local Users

Domain Users

Local Group Members

Domain Group Members

Registry Dump

SNARE Network Configuration

The following network configuration parameters of the SNARE unit is set to the following values:

Override detected DNS Name with:	<input type="text"/>
Destination Snare Server address(s) (Comma delimited)	<input type="text" value="10.0.0.3"/>
Destination Port (if SYSLOG Header NOT enabled)	<input type="text" value="6161"/>
Use UDP or TCP (Note that the Snare Micro Server only uses UDP at this stage)	<input checked="" type="radio"/> UDP <input type="radio"/> TCP
Perform a scan of ALL objectives, and display the maximum criticality?	<input type="checkbox"/>
Allow SNARE to automatically set audit configuration?	<input checked="" type="checkbox"/>
Allow SNARE to automatically set file audit configuration?	<input checked="" type="checkbox"/>
Export Snare Log data to a file?	<input type="checkbox"/>
Enable SYSLOG Header?	<input type="checkbox"/>
SYSLOG Facility	<input type="text" value="User"/>
SYSLOG Priority	<input type="text" value="Notice"/>

Reassembling the Onion: Event and Log Correlation

InterSect Alliance - Information Technology Security - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites

Address http://localhost:6161/setobjective?0=Modify Go Links

Latest Events

Network Configuration

Remote Control Configuration

Objectives Configuration

View Audit Service Status

Apply the Latest Audit Configuration

Local Users

Domain Users

Local Group Members

Domain Group Members

Registry Dump

SNARE Filtering Objective Configuration

The following parameters of the SNARE objective may be set:

Identify the high level event	<input checked="" type="radio"/> Logon or Logoff <input type="radio"/> Access a file or directory <input type="radio"/> Start or stop a process <input type="radio"/> Use of user rights	<input type="radio"/> Account Administration <input type="radio"/> Change the security policy <input type="radio"/> Restart, shutdown and system <input type="radio"/> Any event(s)
Event ID Search Term <i>Optional, Comma separated: only used by the 'Any Event' setting above</i>	<input type="text"/>	
General Search Term <i>Wildcards accepted</i>	<input type="text" value="*"/>	
Select the User Match Type	<input checked="" type="radio"/> Include <input type="radio"/> Exclude	
User Search Term <i>User Names, comma separated. Wildcards accepted</i>	<input type="text" value="*cora*"/>	
Identify the event types to be captured	<input checked="" type="checkbox"/> Success Audit <input checked="" type="checkbox"/> Information <input checked="" type="checkbox"/> Error	<input checked="" type="checkbox"/> Failure Audit <input checked="" type="checkbox"/> Warning
Identify the event logs (ignored if any objective other than 'Any event(s)' is selected):	<input checked="" type="checkbox"/> Security <input type="checkbox"/> Application <input type="checkbox"/> DNS Server	<input type="checkbox"/> System <input type="checkbox"/> Directory Service <input type="checkbox"/> File Replication
Select the Alert Level	<input type="radio"/> Critical <input type="radio"/> Priority <input type="radio"/> Warning <input checked="" type="radio"/> Information <input type="radio"/> Clear	

Change Configuration Reset Form

(c) InterSect Alliance Pty Ltd 1999-2005. This site is powered by [SNARE for Windows](#).

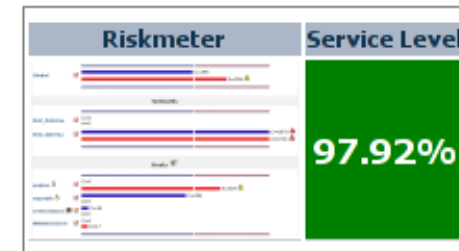
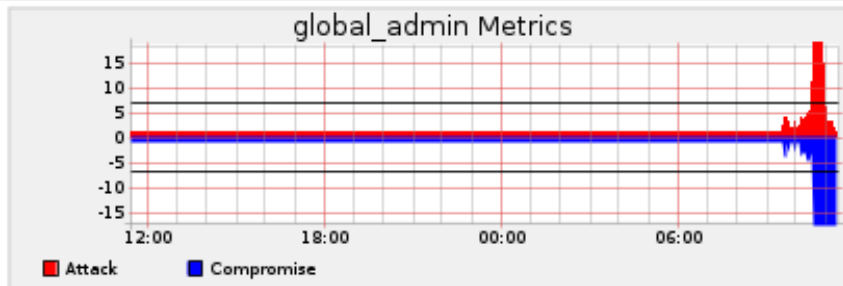
Reassembling the Onion: Event and Log Correlation



▼ CONTROL PANEL ► REPORTS ► MONITORS ► POLICY ► CORRELATION ► CONFIGURATION ► TOOLS ► LOGOUT

METRICS ALARMS ALERTS VULNERABILITIES

[Last Day] [Last Week] [Last Month] [Last Year]



Global

Global	Max C date	Max C	Current C
GLOBAL SCORE	2005-03-07 10:45:00	576	499

Global	Max A date	Max A	Current A
GLOBAL SCORE	2005-03-07 10:40:00	103	4

Networks

Network	Max C date	Max C	Current C
desarrollo	2005-03-07 11:20:00	0	0
dmz	2005-03-07 11:20:00	0	0
interna	2005-03-07 10:45:00	575	521
ossim	2005-03-07 10:45:00	570	495

Network	Max A date	Max A	Current A
desarrollo	2005-03-07 11:20:00	0	0
dmz	2005-03-07 11:20:00	0	0
interna	2005-03-07 10:45:00	40	0
ossim	2005-03-07 10:45:00	39	0

Hosts

Host	Max C date	Max C	Current C
golgotha	2005-03-07 10:45:00	579	495

Host	Max A date	Max A	Current A

Reassembling the Onion: Event and Log Correlation



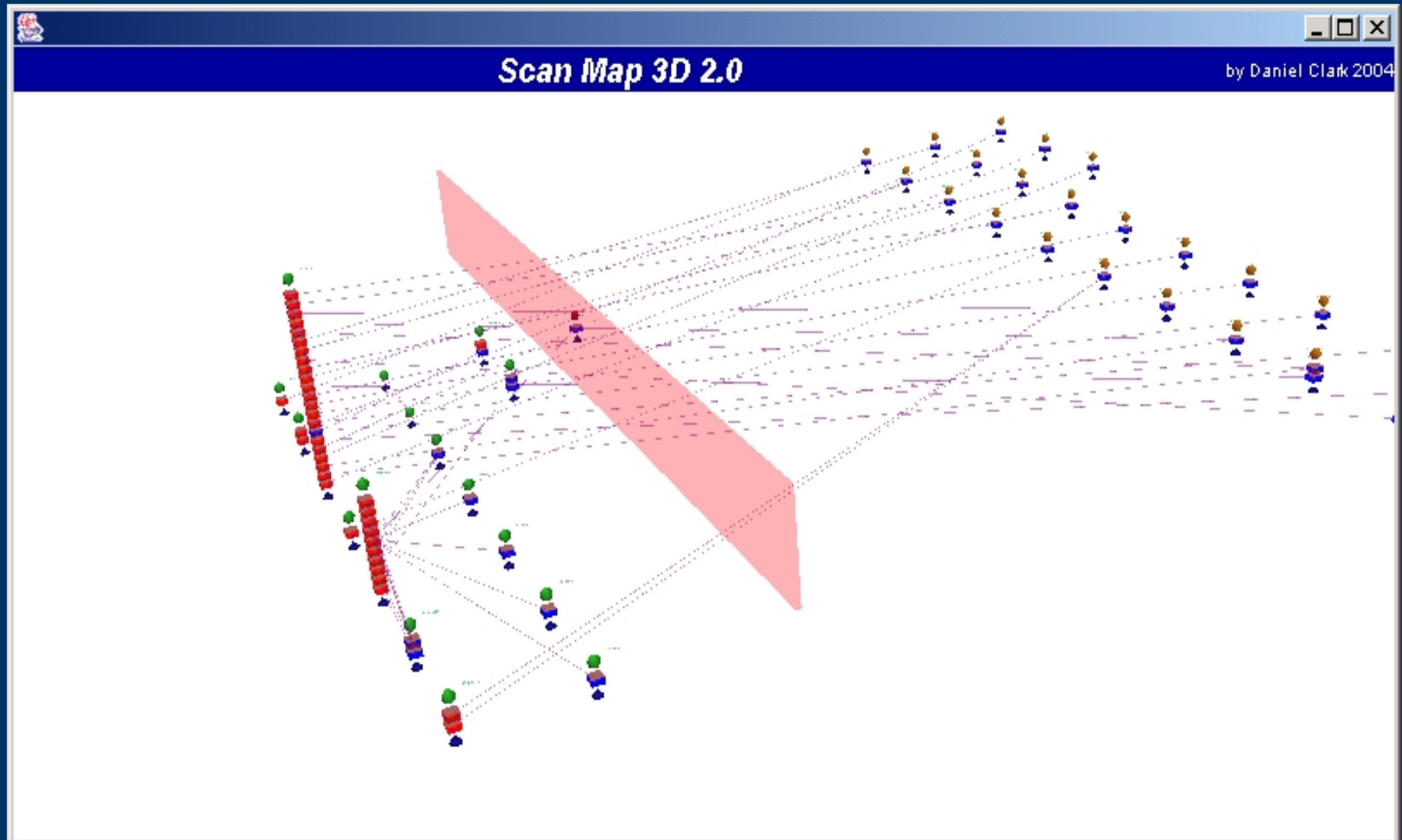
CONTROL PANEL ▶ REPORTS ▶ MONITORS ▶ POLICY ▶ CORRELATION ▶ CONFIGURATION ▶ TOOLS ▶ LOGOUT [admin]

METRICS ALARMS ALERTS VULNERABILITIES

[Page loaded in 4 seconds]

(0-50 of 794) Next 50 ->								
#	Alarm	Risk	Sensor	Since	Last	Source	Destination	Action
Tuesday 26-Apr-2005 [Delete]								
1	Possible Trojan against 207.171.41:26127	3	golgotha	2005-04-26 11:36:50	2005-04-26 11:42:05	dgil:33662	207.171.41:26127	[Ack] i
2	Possible Trojan against 207.171.41:1083	3	golgotha	2005-04-26 11:36:22	2005-04-26 11:41:44	dgil:34357	207.171.41:ansoft-lm-1	[Ack] i
3	Possible Trojan against 207.171.31:1863	3	golgotha	2005-04-26 10:54:09	2005-04-26 11:00:19	dgil:55405	207.171.31:1863	[Ack] i
4	Possible Trojan against 207.171.78:1863	3	golgotha	2005-04-26 10:48:35	2005-04-26 10:54:21	dgil:59256	207.171.78:1863	[Ack] i
5	Possible Trojan against 207.171.96:1863	2	golgotha	2005-04-26 10:35:33	2005-04-26 10:35:45	dgil:46173	207.171.96:1863	[Ack] i
6	Possible portscan originating at 192.168.6.254	6	golgotha	2005-04-26 10:28:55	2005-04-26 10:31:04	192.168.6.254:46322	192.168.250.50:671	[Ack] i
7	Possible Trojan against 207.171.136:1863	3	golgotha	2005-04-26 10:09:20	2005-04-26 10:14:37	dgil:44777	207.171.136:1863	[Ack] i
8	Possible Trojan against 207.171.77:1863	2	golgotha	2005-04-26 10:13:19	2005-04-26 10:13:35	dgil:39832	207.171.77:1863	[Ack] i
9	Possible Trojan against 207.171.8:1863	3	golgotha	2005-04-26 09:59:24	2005-04-26 10:04:42	dgil:48158	207.171.8:1863	[Ack] i
10	Possible Trojan against 207.171.69:1863	2	golgotha	2005-04-26 09:54:32	2005-04-26 09:54:44	dgil:49254	207.171.69:1863	[Ack] i
11	Possible Trojan against 207.171.118:1863	3	golgotha	2005-04-26 09:39:38	2005-04-26 09:44:56	dgil:52581	207.171.118:1863	[Ack] i
12	Possible Trojan against golgotha:21	3	golgotha	2005-04-26 09:32:07	2005-04-26 09:37:22	dgil:36519	golgotha:ftp	[Ack] i
13	Possible portscan originating at dgil	2	golgotha	2005-04-26 09:32:07	2005-04-26 09:32:11	dgil:36519	golgotha:ftp	[Ack] i
Monday 25-Apr-2005 [Delete]								
14	Possible Trojan against 207.171.113:1863	2	golgotha	2005-04-25 17:50:43	2005-04-25 17:50:57	dgil:41515	207.171.113:1863	[Ack] i
15	Possible Trojan against 207.171.135:1863	2	golgotha	2005-04-25 17:08:47	2005-04-25 17:09:02	dgil:41585	207.171.135:1863	[Ack] i
16	Possible Trojan against 207.171.114:1863	2	golgotha	2005-04-25 17:02:08	2005-04-25 17:02:19	dgil:54522	207.171.114:1863	[Ack] i
17	Possible Trojan against 207.171.1:1863	2	golgotha	2005-04-25 16:38:57	2005-04-25 16:39:10	dgil:41732	207.171.1:1863	[Ack] i
18	Possible Trojan against 207.171.23:1863	2	golgotha	2005-04-25 16:38:38	2005-04-25 16:38:51	dgil:45011	207.171.23:1863	[Ack] i
19	Possible Trojan against 207.171.154:1863	2	golgotha	2005-04-25 16:36:07	2005-04-25 16:36:22	dgil:55378	207.171.154:1863	[Ack] i
20	Possible Trojan against 192.168.6.88:22	3	golgotha	2005-04-25 16:15:45	2005-04-25 16:21:00	dgil:33757	192.168.6.88:ssh	[Ack] i
21	Possible Trojan against 207.171.82:6667	2	golgotha	2005-04-25 15:58:51	2005-04-25 15:59:03	dgil:34174	207.171.82:irc	[Ack] i
22	Possible Trojan against 192.168.8.120:139	5	golgotha	2005-04-25 15:52:39	2005-04-25 15:57:55	192.168.6.61:2910	192.168.8.120:netbios-ssn	[Ack] i
23	Possible Trojan against 192.168.8.120:139	5	golgotha	2005-04-25 15:52:39	2005-04-25 15:57:51	192.168.6.61:2908	192.168.8.120:netbios-ssn	[Ack] i
24	Possible Worm port 139/tcp	4	golgotha	2005-04-25 15:52:39	2005-04-25 15:53:38	192.168.6.61:2908	192.168.8.120:netbios-ssn	[Ack] i
25	Possible Trojan against 207.171.109:1863	3	golgotha	2005-04-25 15:44:29	2005-04-25 15:51:16	dgil:56519	207.171.109:1863	[Ack] i
26	Possible Trojan against fwtest:22	3	golgotha	2005-04-25 15:42:21	2005-04-25 15:47:41	punisher:33002	fwtest:ssh	[Ack] i
27	Possible Trojan against 207.171.47:83	5	golgotha	2005-04-25 15:40:35	2005-04-25 15:45:50	192.168.6.61:2797	207.171.47:mit-ml-dev	[Ack] i

Reassembling the Onion: Event and Log Correlation



Reassembling the Onion: Event and Log Correlation



Gregory W Zill, MBA, CISSP
me@gregoryzill.name
