Outline of Module #9

- Presentation on Achilles
- Discussion of forensic topics in the news
- Windows host forensics and Windows forensic tools
- Network forensic tools and methods
New PayPal Scam

- Fraudsters now advertising anti-fraud measures!
- Outstanding social engineering
- The “virtual confidence game”
Avoiding Adverse Rulings in Forensic Discovery!

- Laura Zubulake case and many others
- Have an incident response plan in place!!
Zubulake Case

- Employment discrimination: Zubulake v. UBS
- Email discovery issues and rulings
  - Court ruled that defendant had to pay for discovery
  - Lost and deleted UBS emails
  - Court granted “adverse inference” jury instruction
- April 7, 2005: jury ruling against UBS
  - $20.1M punitive damages
  - $9.1M compensatory damages
Phen-Fen Diet Pill Case

- Settled in 2002 by American Home Products
- Surprise email from CEO: “Do I have to look forward to spending my waning years writing checks to fat people worried about a silly lung problem”
- Settlement: $4.75B
Eight Steps to Avoid Jail

- Written plan of attack
  - Potential data locations
  - People involved
  - Forensic tools
- Prioritize the data
  - People
  - Information collected
- Conduct thorough interviews with IT
- Don’t ignore any data locations or file types
Eight Steps, continued

- Don’t allow individual users to collect the data
  - Metadata
  - Commercial software vs. forensic tools
- Know when to image drive vs. copying
- Don’t limit names in searches
  - freds, fscholl, etc.
- Maintain chain of custody
New Federal Rules for Digital Evidence (In Preparation)

- What’s a “document”?
- Digital information
  - Active data
  - Replicant data
  - Archival data
  - Residual data (deleted)
  - Embedded data (metadata)
- Astronomical Costs!
  - Restoration: $850K-$4M
  - Privilege review: $16-$70M
Federal Rules of Evidence for Log Files

- Admissibility vs. “weight of evidence”
- Hearsay (business record exception)
- Authentication
  - Altered, manipulated
  - Program reliability
Investigating Windows Systems

- Basic
  - Application log files
  - Temp files
  - Recently used documents
  - Recycle bin
  - History + temporary Internet files
- Registry
- Hidden Files
  - ADS
  - .chk files (fragments from Windows crashes)
  - Swap space
Windows Log Files

- Stored in `%systemroot%\system32\config`
  - sysevent.evt
  - secevent.evt
  - appevent.evt
- No centralized log file hosting built in
  - Kiwi syslog for windows
  - EventReporter
- Logs are binary!
## Logging: Setting Audit Policy

### Local Security Settings

<table>
<thead>
<tr>
<th>Policy / Security Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit account logon events</td>
</tr>
<tr>
<td>Audit account management</td>
</tr>
<tr>
<td>Audit directory service access</td>
</tr>
<tr>
<td>Audit logon events</td>
</tr>
<tr>
<td>Audit object access</td>
</tr>
<tr>
<td>Audit policy change</td>
</tr>
<tr>
<td>Audit privilege use</td>
</tr>
<tr>
<td>Audit process tracking</td>
</tr>
<tr>
<td>Audit system events</td>
</tr>
</tbody>
</table>

### Audit Account Logon Events Properties

Audit account logon events

Audit these attempts:
- Success
- Failure
## Microsoft Recommended Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Success on domain controllers</th>
<th>Success</th>
<th>If required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit account logons</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audit account management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audit logons</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audit object access</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Recommended Settings, cont.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit policy changes</td>
<td>Success on domain controllers</td>
</tr>
<tr>
<td>Audit privilege use</td>
<td>If required</td>
</tr>
<tr>
<td>Audit system events</td>
<td>Success or failure</td>
</tr>
<tr>
<td>Enable process tracking</td>
<td>If required</td>
</tr>
<tr>
<td>Audit Directory Service access</td>
<td>If required</td>
</tr>
</tbody>
</table>
Analyzing Windows Logs
Registry Settings: Event Logging
Windows Investigation (Before Looking for Deleted Files!)

- Check application logs
  - C:\winnt\system32\config\appevent.evt

- Recently used documents
  - C:\Documents and Settings\User\Recent
  - Contains shortcuts to recently used files

- Programs from start > run menu
  - HKEY_CURRENT_USER\software\microsoft\windows\current version\explorer\RunMRU
More Windows Investigation

- Windows Temp Files
  - C:\WINNT\Temp
  - C:\Documents and Settings\User\Local Settings\Temp

- Find {Files, Computers, Text} Dialog Box
  - HKEY_CURRENT_USER\software\microsoft\Internet explorer\explorer bars\ID\Files Names MRU
  - ComputerNamedMRU
  - ContainingTextMRU
Windows Search Functions: Type

Select an item to view its description.

<table>
<thead>
<tr>
<th>Name</th>
<th>In Folder</th>
</tr>
</thead>
<tbody>
<tr>
<td>forensics_module4</td>
<td>C:\Documents and Settings\fscholl\My Documents</td>
</tr>
<tr>
<td>forensics_module5</td>
<td>C:\Documents and Settings\fscholl\My Documents</td>
</tr>
</tbody>
</table>
Investigative Searching

- Create *private information* by analysis multiple sources of public information
- Google hacks
  - [www.dtsearch.com](http://www.dtsearch.com)
  - [www.copernic.com](http://www.copernic.com)
Copernic Search Tools

- Desktop Search: free
- Agent
  - Web search
  - Aggregates 90 search engines
  - $0-$79.95
- Flexible options
### Copernic Options

#### General Options

**On the Fly Indexing**
- Index new and modified files on the fly (requires Windows XP/2000/NT)
- Index received and sent emails on the fly (requires Outlook)

**Scheduled Indexing**
- Scan file folders for changes every 4 days
- Scan Outlook emails for changes every 4 days
- Scan Outlook Express emails for changes every 1 day
- Scan Thunderbird emails for changes every 1 day
- Scan Eudora emails for changes every 1 day
- Scan contacts for changes every 1 day
- Scan favorites and history for changes every 1 day

Perform daily indexing tasks at 12:00 AM

#### Indexing Performance

- When the program runs in background, suspend indexing while I use my computer
- Resume indexing after the computer has been idle for at least 30 seconds
- Suspend indexing while computer resources are highly used
- Resume indexing after low resources usage for at least 2 seconds
- Index in low priority when running in background
Copernic Image Search

Search For: graph

2 Matching Pictures

Folder: C:\Documents and Settings\fscholl\My Documents\frpatents\foxnews\

0_14_bush_kerry_graphic_090704.jpg  9/9/2004 9:51:32 AM  90x70

3_14_ricks_rambles_graphic2_90_70.jpg  9/9/2004 9:51:32 AM  90x70

No results in other categories.
FORENSIC SOURCES OF INFORMATION

- HARD DRIVE
  - REGISTRY & CONTENT
- ROUTER SYSLOG FILES
- SERVER LOG FILES
- FIREWALL LOG FILES
- LIVE SNIFFER DATA COLLECTION
- ISP RECORDS
- IP INVESTIGATIONS
  - INTERNET ARCHIVES
Network Sniffers

- Wildpackets Etherpeek: network engineers
- Eeye IRIS: user friendly
- Ethereal: free!
- Kismet (Linux): wireless and free!
- CommView (www.tamosoft.com)
- CommView for WiFi
CommView Remote Agent
Operation of Remote Agent

- RA captures packets and sends to CommView
- Filter configuration sent from CommView to RA
- RA accessed using challenge response protocol using SHA-1 hash
- All subsequent traffic between RA and Commview is compressed and encrypted
  - Use CAST with 128 bit key
USE OF COMMVIEW REMOTE AGENT

COMMVIEW

DIAL-UP

RA

WIREFLESS

BB

RA

RA
Acquiring web sites

- **www.tenmax.com**

- Teleport Pro
  - 10 threads, 65,000 URL’s
  - $39.95

- Teleport VLX
  - 40 million URL’s
  - $1995

- Teleport Exec
  - Developer tool: CIA, USDOJ, etc.
  - $2495
SIM Tools: Why Event Logging?

- Security Information Management
- One critical part of security infrastructure
  - Prevention
  - Detection
  - Response
- Regulatory requirements
  - Medical: HIPAA
  - Financial: GLB
Event Logging

- **Syslogd in Unix**
  - Configure `/etc/syslog.conf`
  - Message format: `time stamp/hostname/application specific body`
  - No standard for fields

- **Focus on infrastructure systems**
  - Mailservers, web server, routers, etc.

- **Create centralized loghost**
HIPAA Logging Requirements

§ 164.308 Administrative Safeguards
- (a) (1) Security Management Process
  - Information system activity review (Required)
- (a) (5) Security Awareness and Training
  - Log-in monitoring (Addressable)
- (a) (6) Security Incident Procedures
  - Identify and respond to suspected or known security incidents; ...document security incidents and their outcomes (Required)

§ 164.312 Technical Safeguards
- (b) Audit controls to record and examine activity in systems that contain or use electronic PHI
HIPAA Security Update

- Health Insurance Portability and Accountability Act
- Security Rule Deadline: April 21, 2005
- Reference: NIST Special Publication 800-66
  - Administrative Safeguards
  - Physical Safeguards
  - Technical Safeguards
  - Organizational Safeguards
  - Policies/Procedures/Documentation
Gramm Leach Bliley (GLB)

- FFIEC Handbook (Federal Financial Institutions Examination Council)
- “Control access to applications by logging access and security events”
- “Secure access to the OS of all system components by logging and monitoring user or program access to sensitive resources and alerting on security events”
Syslog Protocol

- RFC 3164

- Uses UDP port 514

- Message format
  - Priority field: 0-7
  - Header field: host name and time stamp
  - Message field: ASCII characters describing event
# Syslog Priority Levels

<table>
<thead>
<tr>
<th>SEVERITY</th>
<th>TYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Emergencies</td>
<td>System unusable</td>
</tr>
<tr>
<td>1</td>
<td>Alerts</td>
<td>Immediate action</td>
</tr>
<tr>
<td>2</td>
<td>Critical</td>
<td>Critical condition</td>
</tr>
<tr>
<td>3</td>
<td>Errors</td>
<td>Error messages</td>
</tr>
<tr>
<td>4</td>
<td>Warnings</td>
<td>Warning message</td>
</tr>
<tr>
<td>5</td>
<td>Notifications</td>
<td>Normal</td>
</tr>
<tr>
<td>6</td>
<td>Informational</td>
<td>Information</td>
</tr>
<tr>
<td>7</td>
<td>Debugging</td>
<td>Debug message</td>
</tr>
</tbody>
</table>
Configuring Syslog on Linux Host

```
UU PICO(tm) 4.8  File: syslog.conf

# /etc/syslog.conf - Configuration file for syslogd(8)
#
# For info about the format of this file, see "man syslog.conf".
#
#
# print most on tty10 and on the xconsole pipe
#
# kern.warning:*.*.err:authpriv.none /dev/tty10
# kern.warning:*.*.err:authpriv.none /dev/xconsole
#*.emerg
#
# enable this, if you want that root is informed
# immediately, e.g. of logins
#*.alert
#*.alert root
#
# all email-messages in one file
#
mail.*       ~/var/log/mail
mail.info     ~/var/log/mail.info
mail.warning  ~/var/log/mail.warn
mail.err      ~/var/log/mail.err
```

4/13/2005 Module 9
Syslog Message Structure

```
Dec 27 19:24:43 linux sdpd[9941]: terminating...
Dec 27 19:24:43 linux hci0[9937]: Exit.
Dec 27 19:25:00 linux kernel: ACPI: PCI interrupt 0000:01:02.0(1) -> GSI 3 (level, 1
\uw) -> IRQ 3
Dec 27 19:25:00 linux kernel: Model 1007 Rev 00000000 Serial 10071102
Dec 27 19:25:09 linux kernel: ALSA sound/pci/ac97/ac97_codec.c:1961: AC97 0 does no
t respond - RESET
Dec 27 19:25:09 linux kernel: ALSA sound/pci/ac97/ac97_codec.c:1972: AC97 0 access
is not valid [0x0], removing mixer.
Dec 27 19:25:18 linux init: Entering runlevel: 5
Dec 27 19:25:20 linux exiting on signal 15
Dec 27 19:25:20 dell13000 syslogd 1.4.1: restart.
Dec 27 19:25:22 dell13000 sshd[10543]: Server listening on :: port 22.
Dec 27 19:25:23 dell13000 rcpowersaved: CPU frequency scaling is not supported by you
r processor.
Dec 27 19:25:23 dell13000 rcpowersaved: enter 'POWERSAVE_CPUFREQD_MODULE=off' in /etc
/sysconfig/powersaved/cpufreq to avoid this warning.
Dec 27 19:25:25 dell13000 kernel: ACPI: Power Button [FF] [PURF]
Dec 27 19:25:25 dell13000 kernel: ACPI: Processor [CPU0] (supports C1)
Dec 27 19:25:25 dell13000 kernel: powersave: This module only works with AMD K7 CPUs
Dec 27 19:25:25 dell13000 /usr/sbin/cron[10047]: (CRON) STARTUP (V5.0)
Dec 27 19:25:28 dell13000 kdm: :0[10637]: pam_unix2: session started for user freds,
service xdm-mp
Dec 27 19:26:06 dell13000 kernel: ISU 9660 Extensions: Microsoft Joliet Level 3
Dec 27 19:26:06 dell13000 kernel: ISU 9660 Extensions: RRIP_1991A
Dec 27 19:27:00 dell13000 gconfd (freds-11261): starting (version 2.6.1), pid 11261 u
```

---More---(12)
Linux Log Files

```
-rw-r--r-- 1 root  root  21273 Apr 12 22:39 boot.msg
-rw-r--r-- 1 root  root  23535 Mar 29 14:31 boot.omsq
-rw-r--r-- 1 root  root   566 Dec 27 10:34 convert_for_getconf.log
drwxr-xr-x 2 lp  lp    136 Feb  5 12:50 cups
-rw-r--r-- 1 root  root   1800 Mar 10 23:01 faillog
-rw-r--r-- 1 root  root 105297 Apr 13 08:07 kdm.log
-rw-r--r-- 1 root  tty  292292 Apr 12 22:40 lastlog
-rw-r--r-- 1 root  root    0 Dec 27 10:45 localmessages
-rw-r--r-- 1 root  root  16236 Apr 12 22:39 mail
-rw-r--r-- 1 root  root   368 Dec 27 19:24 mail.err
-rw-r--r-- 1 root  root  16236 Apr 12 22:39 mail.info
-rw-r--r-- 1 root  root   2417 Dec 27 19:24 mail.warn
-rw-r--r-- 1 root  root   795309 Apr 13 07:59 messages
drwxr-x--- 2 news news    136 Dec 27 10:34 news
-rw-r--r-- 1 root  root    0 Dec 27 10:37 ntp
drwxr-xr-x 2 root  root   40 Oct  4 2004 samba
-rw-r--r-- 1 root  root   2800 Mar 28 22:30 scpm
drwxr-x--- 2 root  dialout  48 Oct  1 2004 smmmpd
-rw-r--r-- 1 root  root   136470 Apr 12 22:40 warn
-rw-r--r-- 1 root  tty   54912 Apr 13 08:08 utmp
-rw-r--r-- 1 root  root   13233 Feb 18 20:45 wtmp-20050218.gz
-rw-r--r-- 1 root  root   14334 Mar 28 19:15 wtmp-20050328.gz
```

```
dell3000:/var/log # more mail.err
Dec 27 19:12:24 linux postfix/postfix-script: fatal: the Postfix mail system is not running
Dec 27 19:12:28 linux postfix/postfix-script: fatal: the Postfix mail system is not running
Dec 27 19:21:30 linux postfix/postfix-script: fatal: the Postfix mail system is not running
Dec 27 19:24:04 linux postfix/postfix-script: fatal: the Postfix mail system is not running
```

```
dell3000:/var/log #
```

Limitations of Syslog

- UDP → not reliable
- No authentication or encryption
- RFC 3195: reliable syslog
- draft-ietf-syslog-sign-14.txt: signed syslog
- Relay function omits original IP address
# Security Information Vendors

<table>
<thead>
<tr>
<th>Function</th>
<th>Vendor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Visualize Information</td>
<td>Secure Decisions</td>
</tr>
<tr>
<td>Correlate Information</td>
<td>Intellitactics, NetForensics, ArcSight, GuardedNet, Open Services</td>
</tr>
<tr>
<td>Data Aggregation/Analysis</td>
<td>Network Intelligence, Forensics Explorers</td>
</tr>
<tr>
<td>Data Collection/Analysis</td>
<td>LogLogic, Addamark, Niksun Sandstorm</td>
</tr>
</tbody>
</table>
Network Traffic Recorders

- Record *all* traffic on network
- Niksun NetDetector
- Sandstorm NetIntercept
NetForensics Architecture

ORACLE DATABASE

NF ENGINE: EVENT AGGREGATION AND CORRELATION

REPORTING TOOL: REAL TIME ANALYSIS; FORENSIC REPORTS
Event Correlation

- Rules based: If...then...else
- Statistical: monitor changes in event statistics
- Behavioral: monitor trends in security events
Intellitactics Message Architecture

SYSLOG MESSAGE: DATE, TIME STAMP, SOURCE, DESTINATION, EVENT CODE (CISCO PIX 106001—DENY INBOUND TCP CONNECTION)

CREATE NORMALIZED TYPE FIELD BASED ON EVENT TYPE

ADD ZONE FIELDS BASED ON SOURCE LOCATION, TARGET LOCATION AND FIREWALL LOCATION

ADD PRIORITY FIELD: TYPE FIELD + ASSET CLASSIFICATION
Log Logic Log Appliance

- Archiving of log file data
  - Uses intelligent data compression technique
- Allows real time and historical threat analysis
  - Cisco message ID
  - Message volume
  - Regular expression filter
- LX-1000
  - Up to 1000 messages/second
  - 90 GB storage: 90 days storage
- Archive server: 2 TB and 2 years of data
Summarization of Log Files

20-50 TCP connections per web page

PC user

PIX firewall

Syslog messages

Takes 60-150 messages and summarizes to one database record

Loglogic logappliance

WWW server
Applications of Log File Forensics

- Help diagnose virus infections
  - Analysis of time zero events
  - Monitor inside traffic for infected machines
- Help analyze hacker events
- Set log alerts to catch breaches in real time
Log File Formats

- **CheckPoint**
  - Proprietary binary format, not human readable
  - Time | Action | Firewall | Interface | Product | Source | Source Port | Dest. | Service | Protocol | Translation (NAT)

- **Cisco PIX**
  - Syslog format
  - Date | Time | IP/Hostname | Message Code | Message

- **NetScreen**
  - Syslog format
  - Date | Time | Module | Severity | Type | Message Text
# Significance of Priority Levels

<table>
<thead>
<tr>
<th>SEVERITY</th>
<th>TYPES</th>
<th>FUNCTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-4</td>
<td>Alert, Critical, Error, Warning</td>
<td>Packet anomalies, policy conflicts</td>
</tr>
<tr>
<td>5</td>
<td>Notifications</td>
<td>Work done on the firewall</td>
</tr>
<tr>
<td>6</td>
<td>Informational</td>
<td>Key to performing audit and policy verification</td>
</tr>
<tr>
<td>7</td>
<td>Debug</td>
<td>Resolve firewall operational issues</td>
</tr>
</tbody>
</table>
## Example PIX Syslog Messages

<table>
<thead>
<tr>
<th>Severity</th>
<th>Cisco #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>Not used</td>
</tr>
<tr>
<td>1</td>
<td>103001</td>
<td>No response from other firewall</td>
</tr>
<tr>
<td>2</td>
<td>106006</td>
<td>Deny inbound UDP from A.B.C.D/Port to L.M.N.O/Port</td>
</tr>
</tbody>
</table>
### Example Syslog Messages, cont.

<table>
<thead>
<tr>
<th>Severity</th>
<th>Cisco #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>106010</td>
<td>Deny inbound from outside: IP_addr to inside: IP_addr</td>
</tr>
<tr>
<td>4</td>
<td>209004</td>
<td>IP fragment malformed; total size exceeds 65,535 bytes</td>
</tr>
<tr>
<td>5</td>
<td>611103</td>
<td>User logged out</td>
</tr>
</tbody>
</table>
## Example Syslog Messages, cont.

<table>
<thead>
<tr>
<th>Level</th>
<th>Cisco #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>199005</td>
<td>Start PIX firewall</td>
</tr>
<tr>
<td>7</td>
<td>111009</td>
<td>User executed command string that does not alter configuration</td>
</tr>
</tbody>
</table>
Severity 5 + 6 Messages

- Contain critical information about traffic in/out of network
- %PIX-5-304001: user 192.168.69.71 Accessed URL 10.133.219.25: www.example.com

- %PIX-6-302013: Built TCP connection number for interface_name: real_address/real_port to interface_name:real_address/real_port
Real Time Reporting

<164>-Mar 20 2004 19:46:59: %PIX-4-106019: IP packet from 68.77.200.220 to 128.238.241.83, protocol tcp received from interface "outside" deny by access-group "mar19b"

<164>-Mar 20 2004 19:46:59: %PIX-4-106019: IP packet from 81.136.183.184 to 128.238.114.163, protocol tcp received from interface "outside" deny by access-group "mar19b"

<164>-Mar 20 2004 19:46:59: %PIX-4-106019: IP packet from 210.149.120.126 to 128.238.146.127, protocol tcp received from interface "outside" deny by access-group "mar19b"

<164>-Mar 20 2004 19:46:59: %PIX-4-106019: IP packet from 150.101.122.31 to 128.238.146.237, protocol udp received from interface "outside" deny by access-group "mar19b"

<164>-Mar 20 2004 19:46:59: %PIX-4-106019: IP packet from 68.251.144.173 to 128.238.134.85, protocol tcp received from interface "outside" deny by access-group "mar19b"

<164>-Mar 20 2004 19:46:59: %PIX-4-106019: IP packet from 138.89.179.236 to 128.238.8.190, protocol tcp received from interface "outside" deny by access-group "mar19b"

<164>-Mar 20 2004 19:46:59: %PIX-4-106019: IP packet from 68.77.2.83 to 128.238.230.145, protocol tcp received from interface "outside" deny by access-group "mar19b"

<164>-Mar 20 2004 19:46:59: %PIX-4-106019: IP packet from 68.93.21.85 to 128.238.70.56, protocol tcp received from interface "outside" deny by access-group "mar19b"
LogApp Configure Email Alerts

Configure Alert For Multiple Users


<table>
<thead>
<tr>
<th>Alert Criteria</th>
<th>Criticality</th>
<th>Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco PIX Message Code</td>
<td>1 (Alert)</td>
<td>1-01002</td>
</tr>
<tr>
<td>Message Volume Threshold</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Regular Expression</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

View list
## Denied IP Messages Report for All Data Sources


<table>
<thead>
<tr>
<th>Rank</th>
<th>Firewall</th>
<th>Attempts</th>
<th>Source IP</th>
<th>Source Port</th>
<th>Dest IP</th>
<th>Dest Port</th>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>128.238.1.254</td>
<td>5777</td>
<td>141.211.124.39</td>
<td>ANY</td>
<td>ANY</td>
<td>3675</td>
<td>tcp</td>
<td>Unknown</td>
</tr>
<tr>
<td>2</td>
<td>128.238.1.254</td>
<td>5775</td>
<td>141.211.124.39</td>
<td>ANY</td>
<td>ANY</td>
<td>1116</td>
<td>tcp</td>
<td>Unknown</td>
</tr>
<tr>
<td>3</td>
<td>128.238.1.254</td>
<td>5771</td>
<td>141.211.191.78</td>
<td>ANY</td>
<td>ANY</td>
<td>2472</td>
<td>tcp</td>
<td>Unknown</td>
</tr>
<tr>
<td>4</td>
<td>128.238.1.254</td>
<td>5765</td>
<td>141.211.191.77</td>
<td>ANY</td>
<td>ANY</td>
<td>2471</td>
<td>tcp</td>
<td>Unknown</td>
</tr>
<tr>
<td>5</td>
<td>128.238.1.254</td>
<td>5765</td>
<td>141.211.191.77</td>
<td>ANY</td>
<td>ANY</td>
<td>4771</td>
<td>tcp</td>
<td>Unknown</td>
</tr>
<tr>
<td>6</td>
<td>128.238.1.254</td>
<td>5764</td>
<td>217.113.99.66</td>
<td>ANY</td>
<td>ANY</td>
<td>3213</td>
<td>tcp</td>
<td>Unknown</td>
</tr>
<tr>
<td>7</td>
<td>128.238.1.254</td>
<td>5758</td>
<td>141.211.136.9</td>
<td>ANY</td>
<td>ANY</td>
<td>4176</td>
<td>tcp</td>
<td>Unknown</td>
</tr>
<tr>
<td>8</td>
<td>128.238.1.254</td>
<td>5757</td>
<td>141.211.136.10</td>
<td>ANY</td>
<td>ANY</td>
<td>3850</td>
<td>tcp</td>
<td>Unknown</td>
</tr>
<tr>
<td>9</td>
<td>128.238.1.254</td>
<td>5756</td>
<td>141.211.191.79</td>
<td>ANY</td>
<td>ANY</td>
<td>4773</td>
<td>tcp</td>
<td>Unknown</td>
</tr>
<tr>
<td>10</td>
<td>128.238.1.254</td>
<td>5754</td>
<td>141.211.191.78</td>
<td>ANY</td>
<td>ANY</td>
<td>4772</td>
<td>tcp</td>
<td>Unknown</td>
</tr>
<tr>
<td>11</td>
<td>128.238.1.254</td>
<td>5752</td>
<td>141.211.191.79</td>
<td>ANY</td>
<td>ANY</td>
<td>2473</td>
<td>tcp</td>
<td>Unknown</td>
</tr>
<tr>
<td>12</td>
<td>128.238.1.254</td>
<td>5751</td>
<td>141.211.136.9</td>
<td>ANY</td>
<td>ANY</td>
<td>3866</td>
<td>tcp</td>
<td>Unknown</td>
</tr>
<tr>
<td>13</td>
<td>128.238.1.254</td>
<td>5750</td>
<td>141.211.136.10</td>
<td>ANY</td>
<td>ANY</td>
<td>4177</td>
<td>tcp</td>
<td>Unknown</td>
</tr>
<tr>
<td>14</td>
<td>128.238.1.254</td>
<td>5749</td>
<td>141.211.191.76</td>
<td>ANY</td>
<td>ANY</td>
<td>4770</td>
<td>tcp</td>
<td>Unknown</td>
</tr>
<tr>
<td>15</td>
<td>128.238.1.254</td>
<td>5741</td>
<td>141.211.191.76</td>
<td>ANY</td>
<td>ANY</td>
<td>2470</td>
<td>tcp</td>
<td>Unknown</td>
</tr>
<tr>
<td>16</td>
<td>128.238.1.254</td>
<td>1526</td>
<td>128.238.241.235</td>
<td>ANY</td>
<td>ANY</td>
<td>445</td>
<td>tcp</td>
<td>Unknown</td>
</tr>
<tr>
<td>17</td>
<td>128.238.1.254</td>
<td>1501</td>
<td>128.238.241.235</td>
<td>ANY</td>
<td>ANY</td>
<td>135</td>
<td>tcp</td>
<td>Unknown</td>
</tr>
<tr>
<td>18</td>
<td>128.238.1.254</td>
<td>782</td>
<td>128.238.38.226</td>
<td>ANY</td>
<td>ANY</td>
<td>445</td>
<td>tcp</td>
<td>Unknown</td>
</tr>
<tr>
<td>19</td>
<td>128.238.1.254</td>
<td>770</td>
<td>128.238.38.226</td>
<td>ANY</td>
<td>ANY</td>
<td>135</td>
<td>tcp</td>
<td>Unknown</td>
</tr>
<tr>
<td>20</td>
<td>128.238.1.254</td>
<td>387</td>
<td>211.87.217.213</td>
<td>ANY</td>
<td>ANY</td>
<td>6881</td>
<td>tcp</td>
<td>Unknown</td>
</tr>
</tbody>
</table>
Cisco Router ACL Denied Messages Report
Sun Mar 21 12:36:06 2004

Firewall: All ▼  Report Type: Src IP/Any -» Any/Dest Port ▼
☐ Generate Comma Separated Value (CSV) Output
☐ Resolve DNS Names (can take a long time)

Select The Time Interval For The Report

Last Hour ▼  Today ▼  Yesterday ▼

Or Enter A Specific Time Interval

Date: 3/21/2004  Time: 12:00:00am  To Date: 3/21/2004  Time: 11:59:59pm

Run Report
## IP Address Search for 211.87.217.213 From All Data Sources

### PIX TCP Connections Containing IP 211.87.217.213

From Sat Mar 20 21:40:00 2004 to Sat Mar 20 22:40:00 2004 (top 50 entries)

<table>
<thead>
<tr>
<th>Rank</th>
<th>Firewall</th>
<th>Global Address</th>
<th>Local Address</th>
<th>Foreign Address</th>
<th>TCP Port</th>
<th>Messages</th>
<th>Inbound Con. TCP Bytes</th>
<th>Outbound Con. TCP Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>128.236.1.254</td>
<td>128.238.197.77</td>
<td>128.238.197.77</td>
<td>211.87.217.213</td>
<td>53329</td>
<td>4</td>
<td>0</td>
<td>136</td>
</tr>
</tbody>
</table>

### PIX UDP Connections Containing IP 211.87.217.213

From Sat Mar 20 21:40:00 2004 to Sat Mar 20 22:40:00 2004 (top 50 entries)

No UDP connections were established for this IP address.

### PIX Denied IP Messages Containing IP 211.87.217.213

From Sat Mar 20 21:40:00 2004 to Sat Mar 20 22:40:00 2004 (showing the 50 most recent entries)

<table>
<thead>
<tr>
<th>Rank</th>
<th>Firewall</th>
<th>Message Time</th>
<th>Protocol</th>
<th>Source IP</th>
<th>Source Port</th>
<th>Dest IP</th>
<th>Dest Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>128.236.1.254</td>
<td>Mar 20 22:39:50 2004</td>
<td>tcp</td>
<td>211.87.217.213</td>
<td>3014</td>
<td>128.236.197.77</td>
<td>6881</td>
<td>Unknown</td>
</tr>
<tr>
<td>6</td>
<td>128.236.1.254</td>
<td>Mar 20 22:39:17 2004</td>
<td>tcp</td>
<td>211.87.217.213</td>
<td>3069</td>
<td>128.236.197.77</td>
<td>6881</td>
<td>Unknown</td>
</tr>
<tr>
<td>7</td>
<td>128.236.1.254</td>
<td>Mar 20 22:39:03 2004</td>
<td>tcp</td>
<td>211.87.217.213</td>
<td>4782</td>
<td>128.236.197.77</td>
<td>6881</td>
<td>Unknown</td>
</tr>
<tr>
<td>8</td>
<td>128.236.1.254</td>
<td>Mar 20 22:39:03 2004</td>
<td>tcp</td>
<td>211.87.217.213</td>
<td>3650</td>
<td>128.236.197.77</td>
<td>6881</td>
<td>Unknown</td>
</tr>
<tr>
<td>9</td>
<td>128.236.1.254</td>
<td>Mar 20 22:38:50 2004</td>
<td>tcp</td>
<td>211.87.217.213</td>
<td>1200</td>
<td>128.236.197.77</td>
<td>6881</td>
<td>Unknown</td>
</tr>
<tr>
<td>10</td>
<td>128.236.1.254</td>
<td>Mar 20 22:38:50 2004</td>
<td>tcp</td>
<td>211.87.217.213</td>
<td>4288</td>
<td>128.236.197.77</td>
<td>6881</td>
<td>Unknown</td>
</tr>
<tr>
<td>11</td>
<td>128.236.1.254</td>
<td>Mar 20 22:38:50 2004</td>
<td>tcp</td>
<td>211.87.217.213</td>
<td>4878</td>
<td>128.236.197.77</td>
<td>6881</td>
<td>Unknown</td>
</tr>
<tr>
<td>12</td>
<td>128.236.1.254</td>
<td>Mar 20 22:38:30 2004</td>
<td>tcp</td>
<td>211.87.217.213</td>
<td>4099</td>
<td>128.236.197.77</td>
<td>6881</td>
<td>Unknown</td>
</tr>
<tr>
<td>13</td>
<td>128.236.1.254</td>
<td>Mar 20 22:38:13 2004</td>
<td>tcp</td>
<td>211.87.217.213</td>
<td>53329</td>
<td>128.236.197.77</td>
<td>2756</td>
<td>Unknown</td>
</tr>
<tr>
<td>14</td>
<td>128.236.1.254</td>
<td>Mar 20 22:38:12 2004</td>
<td>tcp</td>
<td>211.87.217.213</td>
<td>1616</td>
<td>128.236.197.77</td>
<td>6881</td>
<td>Unknown</td>
</tr>
</tbody>
</table>
# TCP Application Distribution Report for All Data Sources

From: Sat Mar 20 21:30:00 2004 to Sat Mar 20 22:30:00 2004

<table>
<thead>
<tr>
<th>Rank</th>
<th>Application</th>
<th>TCP Port</th>
<th>Description</th>
<th>Inbound Connections</th>
<th>TCP Bytes</th>
<th>(%)</th>
<th>Outbound Connections</th>
<th>TCP Bytes</th>
<th>(%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>80</td>
<td>12458</td>
<td>HTTP</td>
<td>159777890</td>
<td>3.41%</td>
<td>46111</td>
<td>648104617</td>
<td>13.48%</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>1561</td>
<td>0</td>
<td>Unknown</td>
<td>0</td>
<td>0.00%</td>
<td>3</td>
<td>251711325</td>
<td>5.23%</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>1543</td>
<td>0</td>
<td>Unknown</td>
<td>0</td>
<td>0.00%</td>
<td>26</td>
<td>24924080</td>
<td>5.16%</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>2039</td>
<td>0</td>
<td>Unknown</td>
<td>0</td>
<td>0.00%</td>
<td>1</td>
<td>183842484</td>
<td>3.82%</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>4662</td>
<td>12476</td>
<td>Unknown</td>
<td>97465564</td>
<td>2.08%</td>
<td>10178</td>
<td>108242165</td>
<td>2.25%</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>1402</td>
<td>1</td>
<td>Unknown</td>
<td>6509</td>
<td>0.00%</td>
<td>3</td>
<td>102030220</td>
<td>2.12%</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>2729</td>
<td>0</td>
<td>Unknown</td>
<td>0</td>
<td>0.00%</td>
<td>32</td>
<td>10062948</td>
<td>2.06%</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>1214</td>
<td>122</td>
<td>0</td>
<td>0</td>
<td>0.00%</td>
<td>2782</td>
<td>91672668</td>
<td>1.91%</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>6546</td>
<td>0</td>
<td>Unknown</td>
<td>0</td>
<td>0.00%</td>
<td>2140</td>
<td>99279400</td>
<td>1.96%</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>554</td>
<td>0</td>
<td>Unknown</td>
<td>0</td>
<td>0.00%</td>
<td>22</td>
<td>67484871</td>
<td>1.40%</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>1366</td>
<td>0</td>
<td>Unknown</td>
<td>0</td>
<td>0.00%</td>
<td>27</td>
<td>5951261</td>
<td>1.24%</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>3813</td>
<td>1</td>
<td>Unknown</td>
<td>414</td>
<td>0.00%</td>
<td>20</td>
<td>50275058</td>
<td>1.05%</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>4236</td>
<td>0</td>
<td>Unknown</td>
<td>0</td>
<td>0.00%</td>
<td>1</td>
<td>50011460</td>
<td>1.04%</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>4247</td>
<td>0</td>
<td>Unknown</td>
<td>0</td>
<td>0.00%</td>
<td>1</td>
<td>50009660</td>
<td>1.04%</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>4244</td>
<td>0</td>
<td>Unknown</td>
<td>0</td>
<td>0.00%</td>
<td>1</td>
<td>50005280</td>
<td>1.04%</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>1310</td>
<td>0</td>
<td>Unknown</td>
<td>0</td>
<td>0.00%</td>
<td>16</td>
<td>41493485</td>
<td>0.86%</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>1881</td>
<td>7</td>
<td>Unknown</td>
<td>0</td>
<td>0.00%</td>
<td>26</td>
<td>39795999</td>
<td>0.83%</td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>2342</td>
<td>0</td>
<td>Unknown</td>
<td>0</td>
<td>0.00%</td>
<td>8</td>
<td>34214829</td>
<td>0.71%</td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>3756</td>
<td>1</td>
<td>Unknown</td>
<td>0</td>
<td>0.00%</td>
<td>52</td>
<td>28864067</td>
<td>0.50%</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>2662</td>
<td>0</td>
<td>Unknown</td>
<td>0</td>
<td>0.00%</td>
<td>20</td>
<td>20388260</td>
<td>0.42%</td>
<td></td>
</tr>
</tbody>
</table>
## Security Syslog Messages for All Data Sources

From Sun Mar 21 18:01:28 2004 to Sun Mar 21 18:01:28 2004

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Data Source</th>
<th>Message Code</th>
<th>Raw Syslog Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Mar 21 19:01:20 128.238.1.254 209003</td>
<td></td>
<td>&lt;164&gt;Mar 21 2004 19:54:30: %PIX-4-209003: Fragment database limit of 200 exceeded: src = 64.82.244.105, dest = 128.238.70.112, proto = udp, id = 56</td>
<td></td>
</tr>
</tbody>
</table>
References

- www.loganalysis.org