Traditional IDS Should Be Dead

Richard Bejtlich
richard@taosecurity.com
www.taosecurity.com / taosecurity.blogspot.com
Introduction

• Bejtlich ("bate-lik") biography
  – TaoSecurity (05-present)
    • ManTech (04-05)
    • Foundstone (02-04)
    • Ball Aerospace (01-02)
    • Captain at US Air Force CERT (98-01)
    • Lt at Air Intelligence Agency (97-98)
  – Author
    • Tao of Network Security Monitoring: Beyond Intrusion Detection (solo, Addison-Wesley, Jul 04)
    • Extrusion Detection: Security Monitoring for Internal Intrusions (solo, Addison-Wesley, Nov 05)
    • Real Digital Forensics (co-author, Addison-Wesley, Sep 05)
    • Contributed to Incident Response, 2nd Ed and Hacking Exposed, 4th Ed
Argument

- Security environment has changed during the past ten years
- Prevention always eventually fails somewhere, yet most people focus on it exclusively and ignore detection
- "Intrusion Detection" must be an investigative process; "Intrusion Prevention" does not require investigation
- "Intrusion Detection" as currently practiced is actually managing attack or suspicious behavior inferences
- True intrusion detection requires investigating facts, not managing alerts based on inferences
- Traffic-centric forensics provides trustworthy evidence although details may be obfuscated
### Changing Security Environment

<table>
<thead>
<tr>
<th>1997</th>
<th>2007</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intruders obtain remote host control by abusing, subverting, or breaking unnecessary services and/or exposed services</td>
<td>Intruders gain remote host control via 1) client-side breaches; 2) abusing or subverting exposed and necessary applications; 3) breaking exposed services</td>
</tr>
<tr>
<td>Majority of malicious traffic is caused by humans interacting with targets</td>
<td>Majority of malicious traffic is caused by automated code operating on behalf of humans</td>
</tr>
<tr>
<td>Goal of exploitation is often control of target</td>
<td>Goal of exploitation is often theft of sensitive data</td>
</tr>
<tr>
<td>Defense involves preventing intrusions by applying patches for necessary services and disabling unnecessary services</td>
<td>Defense involves properly designing, coding, and deploying complex individualistic applications for which no commodity &quot;patch&quot; is available</td>
</tr>
<tr>
<td>Buffer overflows, SYN floods, and misconfiguration were the big problems</td>
<td>Web application abuse/subversion, root kits, bot nets, exploiting consumer data, etc. are huge</td>
</tr>
</tbody>
</table>

- Too many managers still live in 1997, along with their defensive strategies
Prevention Eventually Fails

• Risk environment changes faster than prevention system

Threats are exceptionally creative, numerous, determined, and always changing

Defenses usually focus on attacks from the outside and cannot understand everything that happens

New devices with various services and applications are always being introduced, often out of the control of the enterprise

Assets are stored anywhere and everywhere
Prevention vs Detection

• When prevention succeeds, investigation is not required
  – Nothing about the target changed because traffic was denied

• All other scenarios require investigation
  – Prevention system doesn't recognize attack, permits traffic
  – Passive detection system recognizes attack, triggers alert
  – Passive detection system doesn't recognize attack, ignores it

• Investigation requires having data to analyze
What Do Alerts Really Mean?

• "Intrusion Detection" systems are at best "incident indication" systems providing inferences based on observed events.


IDS says "I think I saw traffic that I've been programmed to report as the result of running the Unix id command as root. I need to alert."

Replace this example with any of the thousands of alerts that have little to do with the intent of the detection system programmer.
Inferences vs Facts

• This alert is an inference

-----------------------------------------------------
Count:1 Event#1.200816 2007-03-16 19:20:07
ATTACK-RESPONSES id check returned root
82.165.50.118 -> 69.143.202.28
IPVer=4 hlen=5 tos=32 dlen=363 ID=14523 flags=2 offset=0 ttl=43 chksum=33003
Protocol: 6 sport=80 -> dport=1655

Seq=4140666419 Ack=3568664633 Off=5 Res=0 Flags=***AP*** Win=6432 urp=44738 chksum=0

• This transcript is a fact

Real intrusion detection implies identifying facts
Which is better: conclusions based on facts or guesses based on assumptions?
This Is Alert Management, Not Security Investigation

1. Dashboard shows alert
2. Analyst looks at alert
3. Alert does not reveal if attack succeeded
4. Analyst looks for related alerts
5. If any related alerts exist, none reveal if attack succeeded
6. Repeat for next alert starting with Step 1
This Is Security Investigation, Not Alert Management

- Investigations with data present many more options

  Analyst sees original alert
  Database returns single alert
  Queries database for alerts
  Analyst sees FTP to retrieve tools
  FTP data channel allows analysis of intruder back door
  Reconstructs FTP control and data channels
  Analyst sees connections to other IPs
  Queries database for sessions
  Analyst sees FTP control and data channels
  Queries database for sessions
  Database returns single alert
  Analyst sees original alert

FULL CONTENT

Copyright 2007 Richard Bejtlich
Security Investigation Examples

• The following represent cases taken from a network for which I can fully authorize disclosing all event details
• Therefore, it does not represent the latest and greatest, uber-elite hax0r activity I may or may not see elsewhere
• The idea is to demonstrate an investigative methodology where network data is available for investigation
Example 1: Alerts Are Enough

In this example, other alerts imply the nature of the original alert.

Count: 1  Event#1.161790  2007-02-12  01:21:51
BLEEDING-EDGE MALWARE Socksv5 UDP Proxy Inbound Connect Request (Linux Source)
86.123.192.184 -> 69.143.202.28
IPVer=4 hlen=5 tos=32 dlen=78 ID=5907 flags=2 offset=0 ttl=37 chksum=6040
Protocol:  6 sport=50000   -> dport=45673
Seq=1162437692  Ack=2046273927  Off=11  Res=0  Flags=***AP***  Win=16022  urp=45361  chksum=0
Payload:
00 00 00 01 03 00 00 00 05 04 00 00 03 0B

<table>
<thead>
<tr>
<th>Date/Time</th>
<th>Src IP</th>
<th>SPort</th>
<th>Dst IP</th>
<th>D...</th>
<th>Pr</th>
<th>Event Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>2007-02-11 18:32:02</td>
<td>86.123.192.184</td>
<td>50000</td>
<td>69.143.202.28</td>
<td>41933</td>
<td>6</td>
<td>SHELLCODE x86 inc ebx NOOP</td>
</tr>
<tr>
<td>2007-02-12 01:21:51</td>
<td>86.123.192.184</td>
<td>50000</td>
<td>69.143.202.28</td>
<td>45673</td>
<td>6</td>
<td>BLEEDING-EDGE MALWARE Socksv5 UDP Proxy Inb...</td>
</tr>
<tr>
<td>2007-02-11 18:21:00</td>
<td>69.143.202.28</td>
<td>41933</td>
<td>86.123.192.184</td>
<td>50000</td>
<td>6</td>
<td>BLEEDING-EDGE P2P BitTorrent peer sync</td>
</tr>
<tr>
<td>2007-02-11 18:21:00</td>
<td>69.143.202.28</td>
<td>41933</td>
<td>86.123.192.184</td>
<td>50000</td>
<td>6</td>
<td>BLEEDING-EDGE P2P BitTorrent peer sync</td>
</tr>
</tbody>
</table>
Example 2: Alerts Are Not Enough

- Here the alert looks bad and no other alerts exist

```
```

Count:1 Event#1.166468 2007-02-14 02:42:45
69.143.202.28 -> 72.3.247.18
IPVer=4 hlen=5 tos=0 dlen=597 ID=45433 flags=2 offset=0 ttl=63 checksum=14696
Protocol: 6 sport=39684 -> dport=80
Seq=485697299 Ack=4282992985 Off=8 Res=0 Flags=***AP*** Win=5840 urp=31333 checksum=0
Payload:
47 45 54 20 2F 7A 2E 70 68 70 3F 69 3D 44 45 30  47 45 54 20 2F 7A 2E 70 68 70 3F 69 3D 44 45 30
35 35 44 35 33 43 35 46 42 26 7A 3D 31 20 48 54  35 35 44 35 33 43 35 46 42 26 7A 3D 31 20 48 54
54 50 2F 31 2E 30 0D 0A 55 73 65 72 2D 41 67 65  54 50 2F 31 2E 30 0D 0A 55 73 65 72 2D 41 67 65
6C 61 2F 35 2E 30 2E 37 0D 0A 55 73 65 72 2D 41 67 65
```
...continued...

Copyright 2007 Richard Bejtlich
Example 2: Alerts Are Not Enough

...continued...

• What are you supposed to do now?
Example 2: Alerts Are Not Enough

If you collect full content data you can reconstruct the application level view of the security event.

Note the page is gzip-encoded.
Example 2: Alerts Are Not Enough

- If you collect session data you can see other sessions beyond the one indicated by the IDS alert

<table>
<thead>
<tr>
<th>Start Time</th>
<th>End Time</th>
<th>Src IP</th>
<th>SPort</th>
<th>Dst IP</th>
<th>DPort</th>
<th>Pr</th>
<th>S Pc...</th>
<th>S Byt...</th>
<th>D Pc...</th>
<th>D Byt...</th>
</tr>
</thead>
<tbody>
<tr>
<td>2007-02-14 02:42:16</td>
<td>2007-02-14 02:42:16</td>
<td>69.143.202.28</td>
<td>39655</td>
<td>72.3.247.18</td>
<td>80</td>
<td>6</td>
<td>7</td>
<td>490</td>
<td>7</td>
<td>5162</td>
</tr>
<tr>
<td>2007-02-14 02:42:17</td>
<td>2007-02-14 02:42:17</td>
<td>69.143.202.28</td>
<td>39656</td>
<td>72.3.247.18</td>
<td>80</td>
<td>6</td>
<td>8</td>
<td>486</td>
<td>6</td>
<td>2491</td>
</tr>
<tr>
<td>2007-02-14 02:42:16</td>
<td>2007-02-14 02:42:16</td>
<td>69.143.202.28</td>
<td>39657</td>
<td>72.3.247.18</td>
<td>80</td>
<td>6</td>
<td>8</td>
<td>494</td>
<td>7</td>
<td>2961</td>
</tr>
<tr>
<td>2007-02-14 02:42:16</td>
<td>2007-02-14 02:42:17</td>
<td>69.143.202.28</td>
<td>39658</td>
<td>72.3.247.18</td>
<td>80</td>
<td>6</td>
<td>8</td>
<td>502</td>
<td>7</td>
<td>3219</td>
</tr>
<tr>
<td>2007-02-14 02:42:17</td>
<td>2007-02-14 02:42:17</td>
<td>69.143.202.28</td>
<td>39660</td>
<td>72.3.247.18</td>
<td>80</td>
<td>6</td>
<td>7</td>
<td>509</td>
<td>7</td>
<td>3104</td>
</tr>
<tr>
<td>2007-02-14 02:42:17</td>
<td>2007-02-14 02:42:17</td>
<td>69.143.202.28</td>
<td>39661</td>
<td>72.3.247.18</td>
<td>80</td>
<td>6</td>
<td>5</td>
<td>572</td>
<td>5</td>
<td>527</td>
</tr>
<tr>
<td>2007-02-14 02:42:17</td>
<td>2007-02-14 02:42:17</td>
<td>69.143.202.28</td>
<td>39662</td>
<td>72.3.247.18</td>
<td>80</td>
<td>6</td>
<td>7</td>
<td>505</td>
<td>6</td>
<td>2436</td>
</tr>
<tr>
<td>2007-02-14 02:42:17</td>
<td>2007-02-14 02:42:17</td>
<td>69.143.202.28</td>
<td>39663</td>
<td>72.3.247.18</td>
<td>80</td>
<td>6</td>
<td>8</td>
<td>502</td>
<td>7</td>
<td>2983</td>
</tr>
<tr>
<td>2007-02-14 02:42:17</td>
<td>2007-02-14 02:42:17</td>
<td>69.143.202.28</td>
<td>39665</td>
<td>72.3.247.18</td>
<td>80</td>
<td>6</td>
<td>6</td>
<td>486</td>
<td>6</td>
<td>1602</td>
</tr>
<tr>
<td>2007-02-14 02:42:17</td>
<td>2007-02-14 02:42:17</td>
<td>69.143.202.28</td>
<td>39667</td>
<td>72.3.247.18</td>
<td>80</td>
<td>6</td>
<td>8</td>
<td>507</td>
<td>7</td>
<td>3778</td>
</tr>
<tr>
<td>2007-02-14 02:42:17</td>
<td>2007-02-14 02:42:17</td>
<td>69.143.202.28</td>
<td>39669</td>
<td>72.3.247.18</td>
<td>80</td>
<td>6</td>
<td>5</td>
<td>500</td>
<td>5</td>
<td>630</td>
</tr>
<tr>
<td>2007-02-14 02:42:17</td>
<td>2007-02-14 02:42:17</td>
<td>69.143.202.28</td>
<td>39670</td>
<td>72.3.247.18</td>
<td>80</td>
<td>6</td>
<td>5</td>
<td>502</td>
<td>5</td>
<td>574</td>
</tr>
<tr>
<td>2007-02-14 02:42:40</td>
<td>2007-02-14 02:42:40</td>
<td>69.143.202.28</td>
<td>39683</td>
<td>72.3.247.18</td>
<td>80</td>
<td>6</td>
<td>7</td>
<td>521</td>
<td>6</td>
<td>2518</td>
</tr>
<tr>
<td>2007-02-14 02:42:45</td>
<td>2007-02-14 02:42:45</td>
<td>69.143.202.28</td>
<td>39684</td>
<td>72.3.247.18</td>
<td>80</td>
<td>6</td>
<td>7</td>
<td>545</td>
<td>6</td>
<td>2563</td>
</tr>
<tr>
<td>2007-02-14 02:42:45</td>
<td>2007-02-14 02:42:45</td>
<td>69.143.202.28</td>
<td>39685</td>
<td>72.3.247.18</td>
<td>80</td>
<td>6</td>
<td>8</td>
<td>510</td>
<td>8</td>
<td>7130</td>
</tr>
</tbody>
</table>

- Is this enough to decide if there is a security problem?
Example 2: Alerts Are Not Enough

- Visiting the URL in the original alert shows a Valentine Rose jigsaw puzzle
- Sometimes solving a case requires reproducing the suspicious activity in a controlled environment
Example 3: What Happened Next?


Count:1 Event#1.175382 2007-02-21 17:32:47
BLEEDING-EDGE TROJAN Orderjack Reporting User Activity
69.143.202.28 -> 81.95.147.107 IPVer=4 hlen=5 tos=0 dlen=187 ID=8939 flags=2 offset=0 ttl=62 chksum=9436
Protocol: 6 sport=58307 -> dport=80
Seq=2867320777 Ack=3541503528 Off=8 Res=0 Flags=***AP*** Win=33304 urp=48386 chksum=0
Payload:
47 45 54 20 2F 63 67 69 2D 62 69 6D 6E 2F 6F 70 74 74 75 73 74 2F 65 73 74 69 6C 65 5F 72 65 71 75 65 73 74 69 63 6B 73 6F 6C 65 6D 69 6E 6D 65 73 75 70 74 74 2F 69 6E 64 65 69 63 6B 73 6F 6C 65 6D 69 6E 6D 73 0A 0f39fc.

Copyright 2007 Richard Bejtlich
Example 3: What Happened Next?

- Full content data shows the response from the Web server that options.cgi is unavailable, so the victim *may not* have reported its status

```html
SRC: GET /cgi-bin/options.cgi?user_id=40668581731297881844&version_id=0001&passphrase=fkjvhsdvl
ksdhvlsd&socks=7461&version=112&crc=a30f39fc
SRC:
DST: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 2.0//EN">
DST: <HTML>
DST: <HEAD>
DST: <TITLE>404 Not Found</TITLE>
DST: </HEAD>
DST: <BODY>
DST: <H1>Not Found</H1>
DST: The requested URL /cgi-bin/options.cgi was not found on this server.<P>
DST: </HR>
DST:
DST: </BODY>
DST: </HTML>
DST:
```

- Session data reveals the extent of the network-based evidence

<table>
<thead>
<tr>
<th>Start Time</th>
<th>End Time</th>
<th>Src IP</th>
<th>SPort</th>
<th>Dst IP</th>
<th>DPort</th>
<th>Pr</th>
<th>S Pc</th>
<th>S Byt</th>
<th>D Pc</th>
<th>D Byt</th>
</tr>
</thead>
</table>
Example 4: Protocol Analysis Preprocessors

Count: 1  Event#1.167160  2007-02-14 18:08:07

ftp_pp: FTP command channel encrypted
204.152.184.73 -> 69.143.202.28
IPVer=4  hlen=5  tos=32  dlen=82  ID=44797  flags=2  offset=0  ttl=38  chksum=4347
Protocol: 6  sport=21 -> dport=57229
Seq=3439200498  Ack=3554780672  Off=8  Res=0  Flags=***AP***  Win=65535  urp=57883  chksum=0
Payload:
76 73 66 5F  73 79 73  75 74 69  6C 5F 72 65 63 76 _sysutil_recv
5F 70 65 65 6E 6F 20 64 61 74 61 _peek: no data

- Full content data shows a normal FTP retrieval of a FreeBSD package

ftp.freebsd.org runs VSFTPD
vsf_sysutil_recv_peek: no data is some VSFTPD error that triggers Snort's ftp_pp
Example 5: So You Like TCP Options...

---

Count: 1  Event#1.161610  2007-02-12  00:46:29  

**snort_decoder: Truncated Tcp Options**

201.235.7.45  ->  69.143.202.28  

IPVer=4  hlen=5  tos=32  dlen=64  ID=55026  flags=2  offset=0  ttl=103  chksum=23521  

Protocol:  6  sport=21142  ->  dport=47820  

Seq=3375965127  Ack=557227574  Off=11  Res=0  Flags=***A****  Win=17520  urp=25587  chksum=0  

Payload: None.

- A check for other alerts involving the same source show P2P activity

<table>
<thead>
<tr>
<th>Date</th>
<th>Source</th>
<th>Destination</th>
<th>Source Port</th>
<th>Destination Port</th>
<th>Alert Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2007-02-11</td>
<td>69.143.202.28</td>
<td>201.235.7.45</td>
<td>45457</td>
<td>21142</td>
<td>BLEEDING-EDGE P2P BitTorrent Traffic</td>
</tr>
<tr>
<td>2007-02-11</td>
<td>69.143.202.28</td>
<td>201.235.7.45</td>
<td>45457</td>
<td>21142</td>
<td>BLEEDING-EDGE P2P BitTorrent Traffic</td>
</tr>
<tr>
<td>2007-02-12</td>
<td>69.143.202.28</td>
<td>201.235.7.45</td>
<td>21142</td>
<td>47820</td>
<td>snort_decoder: Truncated Tcp Options</td>
</tr>
<tr>
<td>2007-02-12</td>
<td>69.143.202.28</td>
<td>201.235.7.45</td>
<td>48318</td>
<td>21142</td>
<td>BLEEDING-EDGE P2P BitTorrent Traffic</td>
</tr>
<tr>
<td>2007-02-12</td>
<td>69.143.202.28</td>
<td>201.235.7.45</td>
<td>18563</td>
<td>6881</td>
<td>BLEEDING-EDGE SCAN NMAP -sS</td>
</tr>
<tr>
<td>2007-02-12</td>
<td>69.143.202.28</td>
<td>201.235.7.45</td>
<td>18563</td>
<td>6881</td>
<td>BLEEDING-EDGE SCAN NMAP -f -sS</td>
</tr>
<tr>
<td>2007-02-12</td>
<td>69.143.202.28</td>
<td>201.235.7.45</td>
<td>18573</td>
<td>6881</td>
<td>BLEEDING-EDGE SCAN NMAP -sS</td>
</tr>
<tr>
<td>2007-02-12</td>
<td>69.143.202.28</td>
<td>201.235.7.45</td>
<td>18573</td>
<td>6881</td>
<td>BLEEDING-EDGE SCAN NMAP -f -sS</td>
</tr>
</tbody>
</table>

- The so-called Nmap alerts are P2P-related too
Example 5: So You Like TCP Options...

- If you are really paranoid you can look for other sessions involving the source IP

<table>
<thead>
<tr>
<th>Start Time</th>
<th>End Time</th>
<th>Src IP</th>
<th>SPort</th>
<th>Dst IP</th>
<th>DPort</th>
<th>Pr</th>
<th>S Pc...</th>
<th>S Byt...</th>
<th>D Pc...</th>
<th>D Byt...</th>
</tr>
</thead>
<tbody>
<tr>
<td>2007-02-12 00:08:01</td>
<td>2007-02-12 00:08:05</td>
<td>201.1235.7.45</td>
<td>10232</td>
<td>69.143.202.28</td>
<td>6881</td>
<td>6</td>
<td>3</td>
<td>0</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>2007-02-12 00:11:26</td>
<td>2007-02-12 00:14:42</td>
<td>69.143.202.28</td>
<td>47017</td>
<td>201.1235.7.45</td>
<td>21142</td>
<td>6</td>
<td>11</td>
<td>384</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>2007-02-12 00:16:17</td>
<td>2007-02-12 00:21:29</td>
<td>69.143.202.28</td>
<td>47080</td>
<td>201.1235.7.45</td>
<td>21142</td>
<td>6</td>
<td>36</td>
<td>27942</td>
<td>18</td>
<td>1399</td>
</tr>
<tr>
<td>2007-02-12 00:21:17</td>
<td>2007-02-12 00:21:18</td>
<td>69.143.202.28</td>
<td>47124</td>
<td>201.1235.7.45</td>
<td>21142</td>
<td>6</td>
<td>5</td>
<td>48</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>2007-02-12 00:26:18</td>
<td>2007-02-12 00:35:10</td>
<td>69.143.202.28</td>
<td>47385</td>
<td>201.1235.7.45</td>
<td>21142</td>
<td>6</td>
<td>310</td>
<td>435283</td>
<td>97</td>
<td>1988</td>
</tr>
<tr>
<td>2007-02-12 00:31:18</td>
<td>2007-02-12 00:34:40</td>
<td>69.143.202.28</td>
<td>47589</td>
<td>201.1235.7.45</td>
<td>21142</td>
<td>6</td>
<td>12</td>
<td>432</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>2007-02-12 00:31:29</td>
<td>2007-02-12 00:31:29</td>
<td>201.1235.7.45</td>
<td>21142</td>
<td>69.143.202.28</td>
<td>47080</td>
<td>6</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2007-02-12 00:36:19</td>
<td>2007-02-12 00:43:05</td>
<td>69.143.202.28</td>
<td>47635</td>
<td>201.1235.7.45</td>
<td>21142</td>
<td>6</td>
<td>42</td>
<td>38925</td>
<td>20</td>
<td>997</td>
</tr>
<tr>
<td>2007-02-12 00:41:38</td>
<td>2007-02-12 00:41:39</td>
<td>69.143.202.28</td>
<td>47765</td>
<td>201.1235.7.45</td>
<td>21142</td>
<td>6</td>
<td>6</td>
<td>48</td>
<td>4</td>
<td>68</td>
</tr>
<tr>
<td>2007-02-12 00:45:08</td>
<td>2007-02-12 00:45:08</td>
<td>201.1235.7.45</td>
<td>21142</td>
<td>69.143.202.28</td>
<td>47385</td>
<td>6</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2007-02-12 00:46:24</td>
<td>2007-02-12 01:03:09</td>
<td>69.143.202.28</td>
<td>47820</td>
<td>201.1235.7.45</td>
<td>21142</td>
<td>6</td>
<td>939</td>
<td>1318... 361</td>
<td>2912</td>
<td></td>
</tr>
<tr>
<td>2007-02-12 00:51:39</td>
<td>2007-02-12 00:51:41</td>
<td>69.143.202.28</td>
<td>47932</td>
<td>201.1235.7.45</td>
<td>21142</td>
<td>6</td>
<td>4</td>
<td>48</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>2007-02-12 00:56:39</td>
<td>2007-02-12 00:56:41</td>
<td>69.143.202.28</td>
<td>48007</td>
<td>201.1235.7.45</td>
<td>21142</td>
<td>6</td>
<td>4</td>
<td>48</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>2007-02-12 01:01:23</td>
<td>2007-02-12 01:04:26</td>
<td>69.143.202.28</td>
<td>48045</td>
<td>201.1235.7.45</td>
<td>21142</td>
<td>6</td>
<td>10</td>
<td>336</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>2007-02-12 01:06:24</td>
<td>2007-02-12 01:13:42</td>
<td>69.143.202.28</td>
<td>48125</td>
<td>201.1235.7.45</td>
<td>21142</td>
<td>6</td>
<td>115</td>
<td>140794</td>
<td>49</td>
<td>1360</td>
</tr>
<tr>
<td>2007-02-12 01:11:25</td>
<td>2007-02-12 01:11:27</td>
<td>69.143.202.28</td>
<td>48224</td>
<td>201.1235.7.45</td>
<td>21142</td>
<td>6</td>
<td>4</td>
<td>48</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>2007-02-12 01:13:04</td>
<td>2007-02-12 01:13:04</td>
<td>201.1235.7.45</td>
<td>21142</td>
<td>69.143.202.28</td>
<td>47820</td>
<td>6</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2007-02-12 01:16:44</td>
<td>2007-02-12 01:40:12</td>
<td>69.143.202.28</td>
<td>48318</td>
<td>201.1235.7.45</td>
<td>21142</td>
<td>6</td>
<td>1398</td>
<td>1963... 499</td>
<td>3540</td>
<td></td>
</tr>
</tbody>
</table>

- Port 21142 TCP and 6881 TCP indicate P2P activity
Example 5: So You Like TCP Options...

If you really really care about the TCP options the only answer is reviewing the full content data.
Example 6: Odd UDP Traffic


/nsms/rules/cel433/sql.rules: Line 66 --------------------------------------------------- ---------------------

Count:1 Event#1.164746 2007-02-12 16:44:49

MS-SQL probe response overflow attempt

68.101.70.85 -> 69.143.202.28 IPVer=4 hlen=5 tos=0 dlen=640 ID=30017 flags=0 offset=0 ttl=111 chksum=14790
Protocol: 17 sport=2361 -> dport=48549

len=620 chksum=55376

Payload:
05 2B 02 95 CD F8 EA 33 04 53 69 0A 5E 6F AD 2C .+.....3.Si.^o.,
1D 53 24 82 2E C5 1C 1A 16 BD B8 99 DA 65 A1 43 .S$............e.C
F0 9F 62 1D 0C 5C 32 CF 54 7F A8 9E EB 1B CC 51 ..b..\2.T.......Q
CF E7 58 B3 EF 4D 91 4E 99 63 84 BA 1C 15 65 D8 ..X..M.N.c....e.
3B 78 5A CA 30 53 DE 68 32 A7 71 12 3B 87 1C C7 ;xZ.0S.h2.q.;...
E8 7B 6A 4E 45 9E 63 84 BA 1C 15 65 D8 ..X..M.N.c....e.
E8 5E DD DD 2D 3C 81 8A 5B 5B AF D5 E9 31 4B 10 ..^..m<...[...1K.
E4 CA B4 40 1E 6C 65 CA 9F 7C B8 B5 4E 28 2D CF ...@.le..|..N(-.
D4 F0 62 30 72 04 C8 9A E3 32 81 9A A3 23 48 82 ..b0r.....2...H.
BE 21 49 51 BE 2A 3A 4C 91 EA 50 FE 44 D2 DB 3C .!IQ.*:L..P.D..<
0D B8 6A 1D B1 27 22 91 B6 54 2C E1 0E B0 AF 2E ..d..'"..T,.....
...continued...
Example 6: Odd UDP Traffic

...continued...

A9 15 4E 51 FC E6 63 59 8E BA 96 E2 34 AE BE AD ...
68 A1 8A F3 AB D7 A4 E5 FC EC 09 1E 7C FF 1C 92 h...

4B 70 D0 FB 18 30 61 DB 6F AE 89 4F AA 33 29 50 Kp...
0C 4A DC 42 4A BC FB 38 70 D5 75 2D B2 4F A6 5E J.BJ...

76 06 6F 03 17 86 C2 BA 83 9B 90 91 6F E4 23 BF v.o...
B3 51 A2 17 6F 59 1E A1 E7 0C 5C 9B BF 5D 1D 45 Q...

7A 45 30 EA 8E E6 9E FA 02 BD 9F 4F 44 9A 64 CC zE0...

2A C2 8C 4B A9 17 E0 04 33 13 FE B0 8F F2 3A CD ...

FC 45 98 F8 64 17 5D D2 1D 5F 76 9E 53 E9 CA AA ...

6D 84 2B 98 87 8A 9F 72 FD C4 84 C4 27 15 45 42 m+...
B1 27 54 5A 99 E7 C1 43 81 4C F1 64 70 20 BB 02 TZ...

4B 4D F6 CE DC 64 69 71 2A 79 5D F3 30 D4 DD DB KM...

68 D9 DD 8A 62 A1 EB 17 1B B1 82 A5 B8 8D EA F6 h...

4C 4C 99 AB 2E BC 33 CB 89 B0 4F 0F 30 E6 E1 6B LL...

1A 5B D1 CC 8A 0A D1 25 00 77 EB 11 EF 9F 0E AC ...

95 AC 7B 16 7E 86 92 F8 1A D6 22 09 B6 8F 1D 72 ...

01 D4 8F 43 CF 17 53 5E 70 64 7C 7E 27 5B B1 AD ...

A3 02 7D F6 58 7A AC CD E2 1B 11 00 CC 0E 08 AF ...

40 B7 36 E5 61 12 50 8C 36 D4 1E A8 58 81 58 54 @...

D9 8C F5 B6 44 95 D7 A2 34 CE 0C 89 DD 06 2B 6A ...

E2 F9 34 28 26 31 21 D5 D6 0B 60 CD 5B 28 A3 8B ...

7C AF 41 52 AB 11 C4 72 FB C8 26 A5 E0 0D 89 84 ...

18 99 93 5C CC 5E 52 51 1C 29 CC 68 A2 86 F1 41 ...

C6 F4 37 23 E0 0F 5F B9 89 E0 C1 AB F2 1E 04 1A D7 ...

FA 78 4D AC 39 A2 2F CE CB BF 99 B7 5A 2E E8 75 ...

E0 75 3E 04 F2 12 08 A4 43 EB 42 9A 44 DD 3A 37 ...

58 4D FA 19 E1 E8 E5 F7 26 F4 CD 6D BB CA F9 10...

1B 62 2B A4
### Example 6: Odd UDP Traffic

<table>
<thead>
<tr>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>2007-02-12 11:3</td>
<td>69.143.202.28</td>
<td>68.101.70.85</td>
<td>UDP</td>
<td>Source port: 48549</td>
</tr>
<tr>
<td>2007-02-12 11:3</td>
<td>68.101.70.85</td>
<td>69.143.202.28</td>
<td>UDP</td>
<td>Destination port: 2361</td>
</tr>
<tr>
<td>2007-02-12 11:3</td>
<td>69.143.202.28</td>
<td>68.101.70.85</td>
<td>UDP</td>
<td>Source port: 48549</td>
</tr>
<tr>
<td>2007-02-12 11:3</td>
<td>68.101.70.85</td>
<td>69.143.202.28</td>
<td>UDP</td>
<td>Destination port: 2361</td>
</tr>
<tr>
<td>2007-02-12 11:4</td>
<td>68.101.70.85</td>
<td>69.143.202.28</td>
<td>UDP</td>
<td>Source port: 48549</td>
</tr>
<tr>
<td>2007-02-12 11:4</td>
<td>69.143.202.28</td>
<td>68.101.70.85</td>
<td>UDP</td>
<td>Destination port: 2361</td>
</tr>
<tr>
<td>2007-02-12 11:5</td>
<td>68.101.70.85</td>
<td>69.143.202.28</td>
<td>UDP</td>
<td>Source port: 48549</td>
</tr>
<tr>
<td>2007-02-12 11:5</td>
<td>69.143.202.28</td>
<td>68.101.70.85</td>
<td>UDP</td>
<td>Destination port: 2361</td>
</tr>
</tbody>
</table>

**Frame 6 (654 bytes on wire, 654 bytes captured)**
- **Ethernet II, Src: 00:01:5c:22:aa:c2 (00:01:5c:22:aa:c2), Dst: 00:02:b3:0a:cd:5e (00:02:b3:0a:cd:5e)**
  - **Version:** 4
  - **Header length:** 20 bytes
  - **Differentiated Services Field:** 0x00 (DSCP 0x00: Default; ECN: 0x00)
  - **Total Length:** 640
  - **Identification:** 0x7541 (30017)
  - **Flags:** 0x00
  - **Fragment offset:** 0
  - **Time to live:** 111
  - **Protocol:** UDP (0x11)
  - **Header checksum:** 0x39c6 [correct]
    - **Source:** 68.101.70.85 (68.101.70.85)
    - **Destination:** 69.143.202.28 (69.143.202.28)
  - **User Datagram Protocol, Src Port:** 2361 (2361), Dst Port: 48549 (48549)
  - **Data (612 bytes):**

```
0000 00 02 b3 0a cd 5e 00 01 5c 22 aa c2 08 00 45 00 ...
0010 02 80 45 31 00 00 6f 11 39 c6 44 e5 24 65 55 45 8f ...
0020 ca 1c 09 39 bd a5 02 56 d8 50 05 2b 02 95 cd f8 ...
0030 ea 33 04 53 69 0a 5e 6f ad 2c 1d 53 24 82 2e c5 ...
0040 4c 1a 16 bd b8 90 da 65 a1 43 f0 0f 62 1d 0c 5c ...
0050 52 3f 54 7f a8 9e eb 1b cc 51 cf e7 58 b3 ef 4d ...
0060 91 4e 99 63 b4 ba 1c 15 d5 d8 3b 78 5a ca 30 53 ...
0070 de 68 32 a7 71 12 3b 87 1c ce 7e ef 78 33 93 42 61 ...
0080 b6 11 00 9c 04 45 b4 1d e1 20 e8 5e dd d2 6d 3c ...
0090 81 9a 5b 5b af d5 e9 31 4b 10 e4 ca b4 40 1e 6c ...
00a0 65 ca 9f 7c b8 b5 4e 28 2d cf d4 f0 02 30 72 04 e...
00b0 c8 9a e3 32 b1 9a a3 23 48 82 be 21 49 51 be 2a ...
00c0 3a 4c 91 ea 50 fe 44 d2 db 3c 0d e8 64 1d 21 27 ...
```
Example 6: Odd UDP Traffic

- Only one alert involved source IP

<table>
<thead>
<tr>
<th>Date/Time</th>
<th>Src IP</th>
<th>SPort</th>
<th>Dst IP</th>
<th>DPort</th>
<th>Pr</th>
<th>Event Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>2007-02-12 16:44:49</td>
<td>68.101.70.85</td>
<td>2361</td>
<td>69.143.202.28</td>
<td>48549</td>
<td>17</td>
<td>MS-SQL probe response overflow attempt</td>
</tr>
</tbody>
</table>

- Seven similar UDP sessions involving source IP

<table>
<thead>
<tr>
<th>Start Time</th>
<th>End Time</th>
<th>Src IP</th>
<th>SPort</th>
<th>Dst IP</th>
<th>DPort</th>
<th>Pr</th>
<th>S Pc...</th>
<th>S Byt...</th>
<th>D Pc...</th>
<th>D Byt...</th>
</tr>
</thead>
<tbody>
<tr>
<td>2007-02-12 16:32:49</td>
<td>2007-02-12 16:32:49</td>
<td>69.143.202.28</td>
<td>48549</td>
<td>68.101.70.85</td>
<td>2361</td>
<td>17</td>
<td>1</td>
<td>39</td>
<td>1</td>
<td>620</td>
</tr>
<tr>
<td>2007-02-12 16:38:48</td>
<td>2007-02-12 16:38:48</td>
<td>69.143.202.28</td>
<td>48549</td>
<td>68.101.70.85</td>
<td>2361</td>
<td>17</td>
<td>1</td>
<td>40</td>
<td>1</td>
<td>620</td>
</tr>
<tr>
<td>2007-02-12 16:44:49</td>
<td>2007-02-12 16:44:49</td>
<td>69.143.202.28</td>
<td>48549</td>
<td>68.101.70.85</td>
<td>2361</td>
<td>17</td>
<td>1</td>
<td>40</td>
<td>1</td>
<td>620</td>
</tr>
<tr>
<td>2007-02-12 16:50:50</td>
<td>2007-02-12 16:50:50</td>
<td>69.143.202.28</td>
<td>48549</td>
<td>68.101.70.85</td>
<td>2361</td>
<td>17</td>
<td>1</td>
<td>40</td>
<td>1</td>
<td>620</td>
</tr>
<tr>
<td>2007-02-12 16:56:52</td>
<td>2007-02-12 16:56:52</td>
<td>69.143.202.28</td>
<td>48549</td>
<td>68.101.70.85</td>
<td>2361</td>
<td>17</td>
<td>1</td>
<td>40</td>
<td>1</td>
<td>620</td>
</tr>
<tr>
<td>2007-02-12 17:03:35</td>
<td>2007-02-12 17:03:35</td>
<td>69.143.202.28</td>
<td>48549</td>
<td>68.101.70.85</td>
<td>2361</td>
<td>17</td>
<td>1</td>
<td>40</td>
<td>1</td>
<td>620</td>
</tr>
<tr>
<td>2007-02-12 17:09:54</td>
<td>2007-02-12 17:09:54</td>
<td>69.143.202.28</td>
<td>48549</td>
<td>68.101.70.85</td>
<td>2361</td>
<td>17</td>
<td>1</td>
<td>40</td>
<td>1</td>
<td>620</td>
</tr>
</tbody>
</table>
Example 6: Odd UDP Traffic

- Query for sessions involving our IP around the time of the original alert
- Investigating this Web session might be interesting

<table>
<thead>
<tr>
<th>Start Time</th>
<th>End Time</th>
<th>Src IP</th>
<th>SPort</th>
<th>Dst IP</th>
<th>DPort</th>
<th>Pr</th>
<th>S Pc...</th>
<th>S Byt...</th>
<th>D Pc...</th>
<th>D Byt...</th>
</tr>
</thead>
<tbody>
<tr>
<td>2007-02-12 16:32:47</td>
<td>2007-02-12 16:32:57</td>
<td>69.143.202.28</td>
<td>48549</td>
<td>207.216.68.94</td>
<td>44481</td>
<td>17</td>
<td>2</td>
<td>458</td>
<td>2</td>
<td>45</td>
</tr>
<tr>
<td>2007-02-12 16:32:47</td>
<td>2007-02-12 16:32:47</td>
<td>69.143.202.28</td>
<td>48549</td>
<td>164.67.198.69</td>
<td>12530</td>
<td>17</td>
<td>1</td>
<td>40</td>
<td>1</td>
<td>26</td>
</tr>
<tr>
<td>2007-02-12 16:32:47</td>
<td>2007-02-12 16:32:47</td>
<td>69.143.202.28</td>
<td>48549</td>
<td>72.186.73.93</td>
<td>28432</td>
<td>17</td>
<td>1</td>
<td>40</td>
<td>1</td>
<td>26</td>
</tr>
<tr>
<td>2007-02-12 16:32:47</td>
<td>2007-02-12 16:32:50</td>
<td>69.143.202.28</td>
<td>48549</td>
<td>212.72.49.150</td>
<td>80</td>
<td>17</td>
<td>2</td>
<td>458</td>
<td>2</td>
<td>303</td>
</tr>
<tr>
<td>2007-02-12 16:32:49</td>
<td>2007-02-12 16:32:54</td>
<td>69.143.202.28</td>
<td>32769</td>
<td>68.87.73.242</td>
<td>53</td>
<td>17</td>
<td>2</td>
<td>458</td>
<td>2</td>
<td>128</td>
</tr>
<tr>
<td>2007-02-12 16:32:49</td>
<td>2007-02-12 16:32:49</td>
<td>69.143.202.28</td>
<td>48549</td>
<td>76.170.32.8</td>
<td>33364</td>
<td>17</td>
<td>1</td>
<td>458</td>
<td>2</td>
<td>37</td>
</tr>
<tr>
<td>2007-02-12 16:32:49</td>
<td>2007-02-12 16:32:49</td>
<td>69.143.202.28</td>
<td>48549</td>
<td>160.87.34.52</td>
<td>4775</td>
<td>17</td>
<td>1</td>
<td>458</td>
<td>2</td>
<td>447</td>
</tr>
</tbody>
</table>
Example 6: Odd UDP Traffic

- Port 80 TCP traffic shows Skype download

| Dst IP:       | 212.72.49.150 (Unknown)                              |
| Src Port:     | 1110                                                 |
| Dst Port:     | 80                                                   |
| OS Fingerprint: | -> 212.72.49.150:80 (distance 2, link: ethernet/modem) |

SRC: GET
/ui/0/3.0.0.216/en/getlatestversion?ver=3.0.0.216&uhash=1c5fd796911dd6a7462b172f5f2aa477
HTTP/1.1
SRC: User-Agent: Skype. 3.0
SRC: Host: ui.skype.com
SRC: Cache-Control: no-cache
SRC:

DST: HTTP/1.1 200 OK
DST: Date: Mon, 12 Feb 2007 16:32:55 GMT
DST: Server: Apache
DST: Last-Modified: Thu, 08 Feb 2007 14:10:40 GMT
DST: ETag: "cb32-9-9ba29800"
DST: Accept-Ranges: bytes
DST: Content-Length: 9
DST: X-Debug: Served from cache
DST: Connection: close
DST: Content-Type: text/plain; charset=utf-8
DST: Content-Language: en
DST:
DST: 2.0.0.105
Example 7: SANS ISC TCP Options

- Sometimes the best investigative method is to step away from Wireshark and talk to a human
- 2 March 2007: SANS ISC reports "generally" seeing SYN ACK traffic from sources "80, 6667, 6666, and 443" from 129.250.128.21 (compton.ameri.ca)
- I wrote about this in 1999 and taught it at SANS in 2000
Example 7: SANS ISC TCP Options

- SANS basically ignores me, so I contact the owner of compton.ameri.ca (Brad Dreisbach) who says:
  
  "i have been getting tcp syn attacked for about 3 weeks now. i have re-installed the OS on the host just to be safe, but im fairly sure my systems are secure. i have also taken measures with my upstream, whom i also work for, to mitigate the attack. some stuff is still getting through but at this point im just waiting for the attackers to give up..."

- Brad sends me a trace that also shows an ACK flood against his host from other parties

- SANS still ignores me, never posts additional details on isc.sans.org
Example 7: SANS ISC TCP Options

- ShadowServer project sends me bot net C&C traffic

Feb 26 16:59:16 xx.xx.xx.xx:6667 :ESP|846305!njhvef@xx.xx.xx.xx PRIVMSG ##r0x## :nzm tcp.plg) »» Done with ack flood to IP: 129.250.128.21. Sent: 19186 packet(s) @ 2KB/sec (1MB).

Feb 26 16:59:23 xx.xx.xx.xx:6667 :ESP|187844!guwcpbmq@xx.xx.xx.xx PRIVMSG ##r0x## :nzm tcp.plg) »» Done with ack flood to IP: 129.250.128.21. Sent: 49633 packet(s) @ 7KB/sec (2MB).

Example 7: SANS ISC TCP Options

TCP Bad Options Follow-up

Overview:

• All packets reported are SYN/ACKs which is what the analysis is based on below.
• All Packets have the same bad TCP option combination as shown below

```plaintext
0000 00 01 c9 e0 58 00 00 90 69 77 44 bc 08 00 45 00 ....X...iwD...E.
0010 00 30 24 d9 40 00 66 06 e7 ab 89 d0 55 55 0a 00 .0$..@.f.....UU..
0020 1f 1e 1a 0b 04 d7 9f 0c 97 c5 99 a8 12 17 70 12 ...............p.
0030 40 00 39 56 00 00 02 04 05 b4 01 02 04 03 @.9V.......... 
```

• Michal Zalewski's Museum of Broken Packets shows traffic caused by junO-z DoS tool

```plaintext
0000 xx xx xx xx xx xx xx xx xx xx xx xx xx xx 08 00 45 00 ..................E.
0010 00 30 6f bb 40 00 7f 06 63 b6 40 be 19 30 xx xx .0o..@...c...@...
0020 xx xx 04 59 01 ea 10 10 02 39 00 00 00 00 70 02 ...Y......9....p.
0030 40 00 02 3b 00 00 02 04 05 b4 01 02 04 03 ...@.;.............. 
```
Example 7: SANS ISC TCP Options

• At the end of the day we have...
  – Backscatter traffic seen by various sites, reported to SANS ISC
  – Report from the victim of a DoS attack that he was flooded by multiple methods (including IPv6!) for three weeks
  – Traffic from DoS victim showing an ACK flood
  – Botnet C&C traffic showing bots attacking victim via ACK flood
  – Correlation with other traffic and identification of junoc-z DoS tool
Conclusion

- If you're not stopping absolutely everything that's malicious, you're either blindly permitting it or perhaps alerting on some of it.
- Investigating those suspicious events requires trusted data, and the network can provide one (not "the") independent source.
If You Thought I Was Going to Mention Gartner...

- 2003 Gartner Press Release
  - “IDSs have failed to provide value relative to its costs and will be obsolete by 2005.” *(didn't happen)*
  - “The Gartner Information Security Hype Cycle shows that IDS technology *does not add an additional layer of security* as promised by vendors. In many cases IDS implementation has proven to be *costly* and an *ineffective* investment.” *(probably true)*
  - Gartner recommends that enterprises redirect the money they would have spent on IDS toward defense applications such as those offered by thought-leading *firewall vendors* that offer both network-level and application-level firewall capabilities in an integrated product.” *(going to happen, eventually)*
• “According to the Gartner Information Security Hype Cycle research, some of the problems associated with IDSs are:
  1) False positives and negatives
  2) An increased burden on the IS organization by requiring full-time monitoring (24 hours a day, seven days a week, 365 days a year)
  3) A taxing incident-response process
  4) An inability to monitor traffic at transmission rates greater than 600 megabits per second”

• **Comment:** “Deep packet inspection firewalls” don't help
  1) False positives and negatives are unavoidable
  2) Constant vigilance is a requirement for any enterprise
  3) Incident response is always a PITA
  4) High rates is a technology issue common to any platform
Gratuitous Critique of Commercial Products

- This is Cisco MARS -- please see taosecurity.blogspot.com/2007/02/earth-to-mars.html

Notice the lack of IP ADDRESSES in this dashboard... how is this helpful?

Pretty graphs please managers but do not help analysts

Copyright 2007 Richard Bejtlich
Gratuitous Critique of Commercial Products

• This is ArcSight -- how do you avoid GIGO?

Don't trust consoles which use "Top X" as a way to identify security incidents
Questions?

KNOW YOUR NETWORK BEFORE AN INTRUDER DOES

Richard Bejtlich
richard@taosecurity.com
www.taosecurity.com
9532 Liberia Ave Suite 141
Manassas VA 20110
202.409.8045