Security Onion

Network Security Monitoring in Minutes

Doug Burks
Feel the pain

Does your traditional IDS give you all the data you need?
The Beauty of Network Security Monitoring

- Multiple data types (not just IDS alerts)

- Sguil is the de facto reference implementation of NSM:
  - Alert data (NIDS alerts from Snort/Suricata and HIDS alerts from OSSEC)
  - Session data (SANCP)
  - Transaction data (HTTP logs from Bro)
  - Full content data (daemonlogger)
Lots of pieces in the jigsaw puzzle

Sguil 0.7.0
Data Flow

http://nsmwiki.org/images/e/ea/Sguil-0.7dfd.png
Setup wizard puts the jigsaw puzzle together for you!

Takes only 2 minutes!
Snorby

Web interface
- Web 2.0
- AJAX
- Ruby on Rails
- Buzzword compliant!
Squert web interface
The Ultimate Analyst Workstation

- Security Onion in a VM on your Desktop
- Sguil client connects to Sguil server
- Pull pcaps back to your VM for extended analysis
Sguil client designed by analysts for analysts
Right-click Src/Dst IP and Query SANCP table (Session Data)

```
SELECT sensor.hostname, sancp.sid, sancp.sanpcid, sancp.start_time as datetime, sancp.end_time, INET_NTOA(sanpc.src_ip), sanpc.src_port, INET_NTOA(sanpc.dst_ip), sanpc.dst_port, sanpc.proto, sanpc.src_pkts, sanpc.src_bytes, sanpc.dst_pkts, sanpc.dst_bytes FROM sanpc WHERE sanpc.start_time > '2011-11-05' AND sanpc.src_ip =
```

<table>
<thead>
<tr>
<th>Se...</th>
<th>Cnx ID</th>
<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 Pckts</th>
<th>S Bytes</th>
<th>D Pckts</th>
<th>D Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>De...</td>
<td>7.567189141...</td>
<td>2011-11-06 14:35:30</td>
<td>2011-11-06 14:35:30</td>
<td>192.168.1.102</td>
<td>3</td>
<td>207.35.251.172</td>
<td>1445</td>
<td>6</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>De...</td>
<td>7.567189141...</td>
<td>2011-11-06 14:35:30</td>
<td>2011-11-06 14:35:30</td>
<td>192.168.1.102</td>
<td>6</td>
<td>207.35.251.172</td>
<td>1281</td>
<td>6</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>De...</td>
<td>7.567189141...</td>
<td>2011-11-06 14:35:30</td>
<td>2011-11-06 14:35:30</td>
<td>192.168.1.102</td>
<td>21</td>
<td>207.35.251.172</td>
<td>2243</td>
<td>6</td>
<td>181</td>
<td>86197</td>
<td>186</td>
<td>14433</td>
</tr>
<tr>
<td>De...</td>
<td>7.567189141...</td>
<td>2011-11-06 14:35:30</td>
<td>2011-11-06 14:35:30</td>
<td>192.168.1.102</td>
<td>28</td>
<td>207.35.251.172</td>
<td>2882</td>
<td>6</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>De...</td>
<td>7.567189141...</td>
<td>2011-11-06 14:35:30</td>
<td>2011-11-06 14:35:30</td>
<td>192.168.1.102</td>
<td>38</td>
<td>207.35.251.172</td>
<td>2731</td>
<td>6</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>De...</td>
<td>7.567189141...</td>
<td>2011-11-06 14:35:30</td>
<td>2011-11-06 14:35:30</td>
<td>192.168.1.102</td>
<td>54</td>
<td>207.35.251.172</td>
<td>1256</td>
<td>6</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>De...</td>
<td>7.567189141...</td>
<td>2011-11-06 14:35:30</td>
<td>2011-11-06 14:35:30</td>
<td>192.168.1.102</td>
<td>78</td>
<td>207.35.251.172</td>
<td>1586</td>
<td>6</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>De...</td>
<td>7.567189141...</td>
<td>2011-11-06 14:35:30</td>
<td>2011-11-06 14:35:30</td>
<td>192.168.1.102</td>
<td>90</td>
<td>207.35.251.172</td>
<td>2733</td>
<td>6</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>De...</td>
<td>7.567189141...</td>
<td>2011-11-06 14:35:30</td>
<td>2011-11-06 14:35:30</td>
<td>192.168.1.102</td>
<td>97</td>
<td>207.35.251.172</td>
<td>2491</td>
<td>6</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>De...</td>
<td>7.567189141...</td>
<td>2011-11-06 14:35:30</td>
<td>2011-11-06 14:35:30</td>
<td>192.168.1.102</td>
<td>100</td>
<td>207.35.251.172</td>
<td>2730</td>
<td>6</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>De...</td>
<td>7.567189141...</td>
<td>2011-11-06 14:35:30</td>
<td>2011-11-06 14:35:30</td>
<td>192.168.1.102</td>
<td>104</td>
<td>207.35.251.172</td>
<td>1834</td>
<td>6</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>De...</td>
<td>7.567189141...</td>
<td>2011-11-06 14:35:30</td>
<td>2011-11-06 14:35:30</td>
<td>192.168.1.102</td>
<td>122</td>
<td>207.35.251.172</td>
<td>3028</td>
<td>6</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>De...</td>
<td>7.567189141...</td>
<td>2011-11-06 14:35:30</td>
<td>2011-11-06 14:35:30</td>
<td>192.168.1.102</td>
<td>139</td>
<td>207.35.251.172</td>
<td>2159</td>
<td>6</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>De...</td>
<td>7.567189141...</td>
<td>2011-11-06 14:35:30</td>
<td>2011-11-06 14:35:30</td>
<td>192.168.1.102</td>
<td>170</td>
<td>207.35.251.172</td>
<td>1807</td>
<td>6</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>De...</td>
<td>7.567189141...</td>
<td>2011-11-06 14:35:30</td>
<td>2011-11-06 14:35:30</td>
<td>192.168.1.102</td>
<td>172</td>
<td>207.35.251.172</td>
<td>2163</td>
<td>6</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Right-click Src/Dst IP and query Event table to access HTTP logs (Transaction Data)
Right-click Alert ID to pivot to Full Content (transcript in Sguil or pcap in Wireshark)
PCAP Tools

We haz them
There’s gold in them thar PCAPs!

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0</td>
<td></td>
</tr>
<tr>
<td>62.146.92.202</td>
<td>[widehat.opensuse.org] (Linux)</td>
</tr>
<tr>
<td>66.87.68.166</td>
<td></td>
</tr>
<tr>
<td>69.195.137.28</td>
<td>[rules.emergingthreats.net] (FreeBSD)</td>
</tr>
<tr>
<td>91.189.90.132</td>
<td>[changelog.ubuntu.com]</td>
</tr>
<tr>
<td>91.189.92.166</td>
<td>[security.ubuntu.com]</td>
</tr>
<tr>
<td>91.189.92.167</td>
<td>[security.ubuntu.com]</td>
</tr>
<tr>
<td>91.189.92.169</td>
<td>[us.archive.ubuntu.com]</td>
</tr>
<tr>
<td>91.189.92.170</td>
<td>[us.archive.ubuntu.com]</td>
</tr>
<tr>
<td>91.189.92.176</td>
<td>[us.archive.ubuntu.com]</td>
</tr>
<tr>
<td>91.189.92.177</td>
<td>[us.archive.ubuntu.com]</td>
</tr>
<tr>
<td>91.189.92.179</td>
<td>[us.archive.ubuntu.com]</td>
</tr>
<tr>
<td>91.189.92.180</td>
<td>[us.archive.ubuntu.com]</td>
</tr>
<tr>
<td>91.189.92.181</td>
<td>[us.archive.ubuntu.com]</td>
</tr>
<tr>
<td>91.189.92.182</td>
<td>[us.archive.ubuntu.com]</td>
</tr>
<tr>
<td>91.189.92.183</td>
<td>[us.archive.ubuntu.com]</td>
</tr>
<tr>
<td>91.189.92.184</td>
<td>[us.archive.ubuntu.com]</td>
</tr>
<tr>
<td>91.189.92.188</td>
<td>[us.archive.ubuntu.com]</td>
</tr>
<tr>
<td>91.189.92.190</td>
<td>[us.archive.ubuntu.com]</td>
</tr>
<tr>
<td>91.189.94.4</td>
<td></td>
</tr>
<tr>
<td>97.74.215.184</td>
<td>[geekconnection.org] [<a href="http://www.geekconnection.org">www.geekconnection.org</a>]</td>
</tr>
</tbody>
</table>
Multiple Sguil sensors

Bro records a tremendous amount of actionable intelligence about your network traffic. The logs can be found in: /nsm/bro/logs
Hunt for Evil User Agents

zcatalog /nsm/bro/logs//* | bro-cut -d user_agent | sort | uniq -c | sort -nr

Look for malicious user agents like:
Bob’s Evil Clown C&C Agent

or just outdated and vulnerable software like:
zcatalog /nsm/bro/logs//* | bro-cut -d name version.major | grep Firefox | grepv -v 12 | sort | uniq -c | sort -nr

110 Firefox 3
71 Firefox 11
53 Firefox 10

<table>
<thead>
<tr>
<th>Start Time</th>
<th>Flgs</th>
<th>Proto</th>
<th>SrcAddr</th>
<th>Sport</th>
<th>DstAddr</th>
<th>Sport</th>
<th>TotPkts</th>
<th>TotBytes</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>15:04:04.147668 e</td>
<td>0x0</td>
<td>TCP</td>
<td>192.0.5.1</td>
<td>123</td>
<td>192.0.1.1</td>
<td>123</td>
<td>2</td>
<td>120</td>
<td>CON</td>
</tr>
<tr>
<td>15:04:04.147668 e</td>
<td>0x0</td>
<td>TCP</td>
<td>192.0.5.2</td>
<td>123</td>
<td>192.0.1.1</td>
<td>123</td>
<td>4</td>
<td>846</td>
<td>CON</td>
</tr>
<tr>
<td>15:04:04.147668 e</td>
<td>0x0</td>
<td>TCP</td>
<td>192.0.5.3</td>
<td>123</td>
<td>192.0.1.1</td>
<td>123</td>
<td>4</td>
<td>846</td>
<td>CON</td>
</tr>
<tr>
<td>15:04:04.147668 e</td>
<td>0x0</td>
<td>TCP</td>
<td>192.0.5.4</td>
<td>123</td>
<td>192.0.1.1</td>
<td>123</td>
<td>2</td>
<td>180</td>
<td>CON</td>
</tr>
</tbody>
</table>

---

**Argus**

- Applications
- Places
- Argus
- IDS Config
- IDS Rules
- NSM
- Security Onion
- Ubuntu Software Center
- Settings
- Accessories
- Development
- Games
- Graphics
- Multimedia
- Network
- Office
- System
- Help
- About Xfce
- Log Out

**README.html**

- ranonymize
- rapath
- raplot
- rapolicy
- raptot
- raservices
- rarservations
- rsport
- rasper
- rastr
- rastrip
- ratermplate
- ratermmerage
- rattrap
- rataon
- rauseraon
- rauserdata
NIDS is great, but what about HIDS?

- OSSEC monitors local logs and can receive logs from OSSEC Agents and standard Syslog
- OSSEC alerts are stored in /var/ossec/logs/alerts/
- Sguil OSSEC Agent transmits those alerts to the Sguil server
One-man bands make crappy music

Interested in joining an open source project?

Security Onion needs:

- Documentation
- Artwork
- Web interface
- Performance benchmarks
- Package maintainers

http://code.google.com/p/security-onion/wiki/TeamMembers
Where do we go now?

http://securityonion.blogspot.com

Updates are announced here and it also has the following links:

- Download/Install
- FAQ
- Mailing List
- IRC #securityonion on irc.freenode.net