Open Source Network Security Monitoring With Sguil

David J. Bianco
President
Vorant Network Security, Inc.
david@vorant.com
Table of Contents

• Intro to Network Security Monitoring (NSM)
• NSM with Sguil
• Sguil architecture
• Working with Sguil
• Sguil in action
• Try it yourself!
• Summary
• More Information
• Questions
Network Monitoring

- Most mid/large-sized organizations perform network monitoring
  - Intrusion Detection Systems (IDS)
  - Syslogs/Event Logs
  - NetFlow/SFlow
  - Other sources(?)

- Lots of information but no coherence
  - Hard to correlate into usable intelligence
  - Difficult to reassemble the puzzle
  - Research & analysis takes lots of analyst time
Network Security Monitoring

The collection, analysis and escalation of indications and warnings to detect and respond to intrusions.
NSM in a Nutshell

- NSM is a methodology, not a product
- An extension/evolution of traditional network monitoring
- Integrates different sources into a single view
  - Easier to understand
  - Speeds the research process
How to do NSM

- Collect as much information as practical
- Present it to the analyst in ways that make sense
- Don’t waste analyst time!
Types of NSM Data

- You need lots of data to do NSM
- Common types
  - IDS alerts
  - Network session data
  - Full packet content
  - DNS
  - WHOIS
  - Specialized/homebrew sources
    - Dial-up access logs
    - Application level audit logs
    - Anything else you might have handy
NSM With Sguil

- Open Source
- Developed by Bamm Vischer since 2002
- Name comes from “Snort GUI”

Client
- Tcl/Tk GUI for Unix/Linux/Windows
- Also reported to work under OS X

Server
- Unix/Linux only
- Tcl glue code around individual monitoring utilities
Sguil 3-Tiered Architecture

Sguil Server & MySQL DB

Sguil Sensors

Security Analysts
Sguil Sensor Components

- **IDS (Snort)**
  - Sourcefire VRT rules, Bleeding Snort and/or locally-developed rules
  - Recommend using Oinkmaster to manage rule updates

- **Session information collection (SANCP)**
  - Security Analyst Network Connection Profiler
  - Records who talks to whom, start & end times, number of bytes and packets transferred
  - Covers TCP, UDP, ICMP

- **Full network packet capture (Snort)**
  - Needs LOTS of disk space
  - Automatically manages available storage
  - Tunable to store as much or as little as you like
  - Data retention varies by traffic observed & size of storage area
Sguil Server Components

- Sguil daemon (sguild)
  - Accepts connections from clients
  - Coordinates client requests with sensor data and MySQL DB

- MySQL DB
  - IDS alerts
  - Session information
  - Misc. related data

- SQL queries against network security data is a HUGE benefit
  - Greatly speeds up routine investigations
  - Easier to confirm/deny reports from external sources
  - Great for statistical anomaly detection and trend analysis
  - Allows us to capture metrics and generate reports
Data Flow

- IDS and session (SANCP) data
  - Collected on each sensor
  - Forwarded to the central server
    - Inserted into the database
    - IDS alerts may be sent via email/pager if necessary
  - Deleted from sensor
- Packet logs always stored on sensors
  - Server requests these when needed
## Sguil Main Screen

### RealTime Events

<table>
<thead>
<tr>
<th>ST</th>
<th>CNT</th>
<th>Sensor</th>
<th>sid.id</th>
<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>RT</td>
<td>4</td>
<td>reset</td>
<td>1.36942</td>
<td>2005-03-07 16:06:40</td>
<td>200.0.213.227</td>
<td>4205</td>
<td>10.1.1.101</td>
<td>80</td>
<td>6</td>
<td>WEB HS cmd.exe access</td>
</tr>
<tr>
<td>RT</td>
<td>4</td>
<td>reset</td>
<td>1.36943</td>
<td>2005-03-07 16:06:40</td>
<td>200.0.213.227</td>
<td>4205</td>
<td>10.1.1.101</td>
<td>80</td>
<td>6</td>
<td>WEB-MISC http directory traversal</td>
</tr>
<tr>
<td>RT</td>
<td>4</td>
<td>reset</td>
<td>1.36944</td>
<td>2005-03-07 16:06:40</td>
<td>200.0.213.227</td>
<td>4205</td>
<td>10.1.1.101</td>
<td>80</td>
<td>6</td>
<td>http inspect: DOUBLE DECODING ATTACK</td>
</tr>
</tbody>
</table>

### Escalated Events

<table>
<thead>
<tr>
<th>ST</th>
<th>CNT</th>
<th>Sensor</th>
<th>sid.id</th>
<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>RT</td>
<td>1</td>
<td>reset</td>
<td>1.36730</td>
<td>2005-03-29 02:12:49</td>
<td>142.173.81.56</td>
<td>32010</td>
<td>10.1.1.12</td>
<td>7734</td>
<td>6</td>
<td>LOCAL_A MCed Incoming Connection</td>
</tr>
<tr>
<td>RT</td>
<td>1</td>
<td>reset</td>
<td>1.36731</td>
<td>2005-03-29 02:31:43</td>
<td>81.56.41.166</td>
<td>1150</td>
<td>10.1.1.12</td>
<td>7734</td>
<td>6</td>
<td>LOCAL_A MCed Incoming Connection</td>
</tr>
</tbody>
</table>

### System Messages

```
```
Working With Sguil

- Analysts typically start with IDS alerts displayed on the console, then use the NSM data to research and make decisions.
- Each alert must be dealt with. Analysts can:
  - Categorize the alert based on type of activity
  - Escalate the alert to a more senior analyst
- One of these two things must eventually happen!
  - Sguil is not an alert browser
Working With Sguil

- Once alerts are categorized, they disappear from the console
  - Still in the database until they expire
  - Available for reporting or further analysis at a later date
- Sguil provides full logging and audit trail of alert activity
  - Who took the action
  - When they took the action
  - Optional comments (why they took the action)
Working With Sguil

- Analysts don’t *have* to start with alerts

**Scenario:** Your upstream ISP has reported an IP address in your range that it suspects is “doing bad things”, but you’ve noticed nothing in your IDS alerts.

**Response:** Use the IP address to query your databases for matching events or network sessions.
  - From there, you may drill down even further to request session transcripts, copies of the packets or do further searches on other addresses that show up.
NSM Example: Have I Been Pwn3d?

<table>
<thead>
<tr>
<th>ST_CNT</th>
<th>Sensor</th>
<th>sid.eid</th>
<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>RT 4</td>
<td>reset</td>
<td>1.36942</td>
<td>2005-03-07 16:06:40</td>
<td>200.0.213.227</td>
<td>4205</td>
<td>10.1.1.101</td>
<td>80</td>
<td>6</td>
<td>WEB IS cmd.exe access</td>
</tr>
<tr>
<td>RT 4</td>
<td>reset</td>
<td>1.36943</td>
<td>2005-03-07 16:06:40</td>
<td>200.0.213.227</td>
<td>4205</td>
<td>10.1.1.101</td>
<td>80</td>
<td>6</td>
<td>WEB-MISC http directory traversal</td>
</tr>
<tr>
<td>RT 4</td>
<td>reset</td>
<td>1.36944</td>
<td>2005-03-07 16:06:40</td>
<td>200.0.213.227</td>
<td>4205</td>
<td>10.1.1.101</td>
<td>80</td>
<td>6</td>
<td>http_inspect: DOUBLE DECODING ATTACK</td>
</tr>
<tr>
<td>RT 2</td>
<td>reset</td>
<td>1.37628</td>
<td>2005-03-29 01:37:48</td>
<td>69.114.87.190</td>
<td>1141</td>
<td>10.1.1.2</td>
<td>7734</td>
<td>6</td>
<td>LOCAL Attempted Incoming Connection</td>
</tr>
<tr>
<td>RT 1</td>
<td>reset</td>
<td>1.36730</td>
<td>2005-03-29 02:12:49</td>
<td>142.173.81.56</td>
<td>32001</td>
<td>10.1.1.2</td>
<td>7734</td>
<td>6</td>
<td>LOCAL Attempted Incoming Connection</td>
</tr>
<tr>
<td>RT 1</td>
<td>reset</td>
<td>1.36731</td>
<td>2005-03-29 02:31:32</td>
<td>81.56.41.166</td>
<td>1150</td>
<td>10.1.1.2</td>
<td>7734</td>
<td>6</td>
<td>LOCAL Attempted Incoming Connection</td>
</tr>
</tbody>
</table>

| Src IP  | 200.0.213.227 |
| Dst IP  | 10.1.1.101   |

Reverse DNS Whois Query: None

Show Packet Data Show Rule

alert top $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB IS cmd.exe access")

TCP Source IP Dest IP Ver HL TOS Len ID Flags Offset TTL
200.0.213.227 10.1.1.101 4 5 0 99 64290 2 0 1008

System Messages

# Search For Related Events

<table>
<thead>
<tr>
<th>ST</th>
<th>CNT</th>
<th>Sensor</th>
<th>sid.eid</th>
<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>RT</td>
<td>1</td>
<td>reset</td>
<td>1.36942</td>
<td>2005-03-07 16:06:32</td>
<td>200.0.213.227</td>
<td>4205</td>
<td>10.1.1.101</td>
<td>80</td>
<td>6</td>
<td>WEB-INS cmd.exe access</td>
</tr>
<tr>
<td>RT</td>
<td>1</td>
<td>reset</td>
<td>1.36943</td>
<td>2005-03-07 16:06:34</td>
<td>200.0.213.227</td>
<td>4205</td>
<td>10.1.1.101</td>
<td>80</td>
<td>6</td>
<td>WEB-MISC http directory traversal</td>
</tr>
<tr>
<td>RT</td>
<td>1</td>
<td>reset</td>
<td>1.36944</td>
<td>2005-03-07 16:06:36</td>
<td>200.0.213.227</td>
<td>4205</td>
<td>10.1.1.101</td>
<td>80</td>
<td>6</td>
<td>http_inspect: DOUBLE DECODING ATTACK</td>
</tr>
<tr>
<td>RT</td>
<td>1</td>
<td>reset</td>
<td>1.36945</td>
<td>2005-03-07 16:06:38</td>
<td>200.0.213.227</td>
<td>4205</td>
<td>10.1.1.101</td>
<td>80</td>
<td>6</td>
<td>WEB-INS cmd.exe access</td>
</tr>
<tr>
<td>RT</td>
<td>1</td>
<td>reset</td>
<td>1.36946</td>
<td>2005-03-07 16:06:40</td>
<td>200.0.213.227</td>
<td>4208</td>
<td>10.1.1.104</td>
<td>80</td>
<td>6</td>
<td>WEB-MISC http directory traversal</td>
</tr>
<tr>
<td>RT</td>
<td>1</td>
<td>reset</td>
<td>1.36947</td>
<td>2005-03-07 16:06:42</td>
<td>200.0.213.227</td>
<td>4208</td>
<td>10.1.1.104</td>
<td>80</td>
<td>6</td>
<td>http_inspect: DOUBLE DECODING ATTACK</td>
</tr>
<tr>
<td>RT</td>
<td>1</td>
<td>reset</td>
<td>1.36948</td>
<td>2005-03-07 16:06:44</td>
<td>200.0.213.227</td>
<td>4208</td>
<td>10.1.1.104</td>
<td>80</td>
<td>6</td>
<td>WEB-INS cmd.exe access</td>
</tr>
<tr>
<td>RT</td>
<td>1</td>
<td>reset</td>
<td>1.36949</td>
<td>2005-03-07 16:06:46</td>
<td>200.0.213.227</td>
<td>4208</td>
<td>10.1.1.104</td>
<td>80</td>
<td>6</td>
<td>WEB-MISC http directory traversal</td>
</tr>
<tr>
<td>RT</td>
<td>1</td>
<td>reset</td>
<td>1.36950</td>
<td>2005-03-07 16:06:48</td>
<td>200.0.213.227</td>
<td>4208</td>
<td>10.1.1.104</td>
<td>80</td>
<td>6</td>
<td>http_inspect: DOUBLE DECODING ATTACK</td>
</tr>
<tr>
<td>RT</td>
<td>1</td>
<td>reset</td>
<td>1.36951</td>
<td>2005-03-07 16:06:50</td>
<td>200.0.213.227</td>
<td>4208</td>
<td>10.1.1.104</td>
<td>80</td>
<td>6</td>
<td>WEB-INS cmd.exe access</td>
</tr>
<tr>
<td>RT</td>
<td>1</td>
<td>reset</td>
<td>1.36952</td>
<td>2005-03-07 16:06:52</td>
<td>200.0.213.227</td>
<td>4208</td>
<td>10.1.1.104</td>
<td>80</td>
<td>6</td>
<td>WEB-MISC http directory traversal</td>
</tr>
</tbody>
</table>

**Src IP:** 200.0.213.227  
**Src Name:** h227.juliabue.com.ar  
**Dst IP:** 10.1.1.104  
**Dst Name:** Unknown

---

System Messages


---

![Reverse DNS Whois Query](example.com)

- `status`: reassigned
- `owner`: DTC Argentina
- `ownerid`: AR-DAR-APNIC
- `address`: Av Cordoba 456 SE
- `address`: Buenos Aires, AR

---

TCP

<table>
<thead>
<tr>
<th>Source Port</th>
<th>Dest Port</th>
<th>Seq #</th>
<th>Ack #</th>
<th>Offset</th>
</tr>
</thead>
<tbody>
<tr>
<td>4208</td>
<td>80</td>
<td>2086320563</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

---

DATA

<table>
<thead>
<tr>
<th>Source IP</th>
<th>Dest IP</th>
<th>Ver</th>
<th>HL</th>
<th>TOS</th>
<th>len</th>
<th>ID</th>
<th>Flags</th>
<th>Offset</th>
<th>TTL</th>
<th>Payload</th>
</tr>
</thead>
</table>
| 200.0.213.227 | 10.1.1.104 | 4   | 5  | 0   | 99  | 64810 | 2     | 108  | GET /scripts/% to%get%255c.../system32/cmd.exe?/c=dir.
| 47          | 54        | 20  | 2   | 73  | 62  | 70   | 74    | 10   | 25      |
| 52          | 35        | 20  | 2   | 63  | 62  | 70   | 74    | 10   | 25      |
| 74          | 28        | 20  | 1   | 73  | 62  | 70   | 74    | 10   | 25      |
| 78          | 65        | 20  | 1   | 63  | 62  | 70   | 74    | 10   | 25      |

---

Search Packet Payload

- Show Packet Data
- Show Rule
- www.snort.org
- iaat.nist.gov
### Cross Check Against Session Data

<table>
<thead>
<tr>
<th>SENSOR</th>
<th>SANOP ID</th>
<th>START TIME</th>
<th>END TIME</th>
<th>SRC IP</th>
<th>S PORT</th>
<th>DST IP</th>
<th>D PORT</th>
<th>PR</th>
<th>S Pekts</th>
<th>S BYTES</th>
<th>D Pekts</th>
</tr>
</thead>
</table>

**Source Flags Summary**

<table>
<thead>
<tr>
<th>Source Flags</th>
<th>U</th>
<th>A</th>
<th>P</th>
<th>R</th>
<th>S</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Destination Flags Summary**

<table>
<thead>
<tr>
<th>Destination Flags</th>
<th>U</th>
<th>A</th>
<th>P</th>
<th>R</th>
<th>S</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**NOTE:** Sanop summarizes data across a session. If any packet within a session contains one of the above flags, then it will be logged as so. The above does NOT mean each flag was seen in ONE packet.
Try It Yourself!

• Download the Helix Incident Response LiveCD
  • Sguil client is preinstalled on the desktop
• Log into the server at demo.sguil.net with any username/password.
• Feel free to play around
  • Categorize alerts
  • Request transcripts
  • Search the DB
  • Don’t forget the IRC chat window!
Summary

- NSM is not a replacement for IDS, it’s an enhancement
- NSM concentrates on supporting the analyst
  - Increased ability to capture & analyze security data
  - Optimizes for analyst time
  - Despite analyzing more data, increased efficiency means less time and more accurate analysis
- Sguil is the *de facto* reference implementation
  - Open source
  - Multi-user, multi-platform

NSM with Sguil reduced daily IDS operations time from 5 hours to 45 minutes and resulted in improved detection ability.
More Information

- Sguil project page
  - http://www.sguil.org/

- Snort website
  - http://www.snort.org/

- Oinkmaster
  - http://oinkmaster.sourceforge.net/

- SANCP
  - http://www.metre.net/sancp.html

- Helix Incident Response LiveCD
  - http://www.e-fense.com/helix/
Questions?