Network Security Monitoring with Sguil

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

BSDCan 14 May 04
Overview

• Introduction to NSM
• The competition (ACID, etc.)
• Sguil
• Case 1: 403 forbidden
• Case 2: MS-SQL grinding
• Case 3: MS-SQL version overflow attempt
• Case 4: Portscan
• Case 5: Admin-PHP access
• Case 6: SMB grinding
• Case 7: Port 20 to port 20
• Future developments
Introduction: My Background

• Hired 1 March 2004 by ManTech Intl. Corp.
• Previously at Foundstone (02-04), Ball Aerospace & Technology Corp (01-02)
• Captain in US Air Force CERT (98-01), trained as intel officer (96-01)
• Author of The Tao of Network Security Monitoring (Addison-Wesley, 800+ pages, due late July 2004)
• Co-author of Real Digital Forensics (Addison-Wesley) with Keith Jones, Curtis Rose (early 2005)
Introduction: Network Security Monitoring

- NSM is the collection, analysis, and escalation of indications and warnings to detect and respond to intrusions
- NSM \(\neq\) IDS
- Intrusion detection vendors are alert-focused and consider their job done when they activate the “red blinking light”
- NSM assumes prevention eventually fails and some intruders are smarter than you
- Prepare for the worst by collecting everything you can, technically and legally
The Competition: ACID, etc.

- ACID (acidlabs.sf.net) and the like are Web-based alert browsers
- They only query, display, and store Snort alerts
- Do not give enough information for an analyst to make a decision
- Predominantly consider the number of alerts as a proxy for their severity
- No capability for workflow, alert categorization, analyst responsibility, or information sharing
ACID's high count implies 'bad'
ACID's clunky query screen
ACID's questionable results
A packet -- so what?
NSM Requirements

• Need to investigate different sorts of events
  • *Normal* activity triggers alerts but is not harmful
  • *Suspicious* activity is unusual but probably not harmful
  • *Malicious* activity is definitely designed to harm targets

• Need supporting data to make decisions
  • *Alert* data provides a potential indicator of security incidents
  • *Session* data is a content neutral summary of transactions
  • *Full content* data captures packet-level details, including application contents
  • *Statistical* data summarizes traffic
Sguil
(sguil.sf.net)

- Sguil is an open source interface for NSM
- Written by Bamm Visscher, mostly in Tcl/Tk (cross-platform, especially the client)
- Consists of components to collect NSM data:
  - Alert data: Snort and Barnyard
  - Session data: SANCP or Snort stream4 keepstats
  - Full content data: Second instance of Snort
  - Statistical data: Nothing formal (yet)
- Detailed install docs for FreeBSD available; Linux, other BSDs work
Sguil Architecture

Credit: Chris Reining
Case studies

• The following case studies show real data collected during the last few weeks
• Local sensor watches traffic to and from various network perimeters
• Data has been sanitized to remove identifying information
Case 1

Why did the target respond with 403 Forbidden? This isn't very useful -- it's the intruder's attempt which is more important (even though it failed)
Transcript shows an attempted HTTP MOVE was not accepted by the server. This is not an attack.
Case 2

MS-SQL version overflow attempt -- what caused this?
Because we capture everything technically and legally possible, we see the outbound DNS query prompted a response which triggered Snort.
### Case 3

MS-SQL `sa` login failed alerts indicate MS-SQL brute forcing.
Integration with Ethereal facilitates understanding binary protocols like TDS, SMB, RPC, etc.

Full content data retrieved from sensor is archived locally for forensic and investigative purposes.
Sguil portscan data is integrated and shows targets and ports scanned, plus TCP flags.
Query for traffic from intruder IP shows at least one lengthy interaction with a target. Since full content collection to port 443 is disabled, no transcripts available.
Still query for session data around the time of the attack to see if target system suddenly initiated an outbound connection, or if a new party connected to the victim on another port. Essentially, look for anything suspicious. Nothing happened here, so our estimate is all is well.
Case 5

Packet data gives details: op=AddAuthor, id kiegera

Alert indicates admin.php access from Brazilian IP
Transcript captures Web server reply showing 405 error

Sensor Name: -sensor-va
Connection ID: -sensor-va_30889
Dst IP: .13.196 ( 13.196)
Src Port: 3604
Dst Port: 80

-----------------------------

SRC: POST
/admin.php?op=AddAuthor&add_aid=kiegera&add_name=Goda&add_pwd=playboya&add_email=r00t System@hush.com&addadmins=super=1&admin=eCcGVU5JT04gU0VMRUNUIEvKjox
HTTP/1.0
SRC: Accept: */^
SRC: Accept-Language: en-us
SRC: Content-Encoding: gzip, deflate
SRC: Content-Type: application/x-www-form-urlencoded
SRC: Host: com
SRC: User-Agent: Mozilla 4.0 (Linux)
SRC: Content-Length:0
SRC: Connection: Close
SRC: 
SRC: 
DST: HTTP/1.1 405 Method not allowed
DST: Server: Microsoft-IIS/5.0
DST: Date: Tue, 27 Apr 2004 16:35:51 GMT
DST: Allow: OPTIONS, TRACE, GET, HEAD
DST: Content-Length: 3923
DST: Content-Type: text/html
DST: 

Debug Messages

Your request has been sent to the server.
Please be patient as this can take some time.
Using archived data:
Did intruder do anything else? Query session data.

```
WHERE sessions.start_time > '2004-04-21' AND
    (sessions.src_ip = INET_ATON('200.148.108.200') OR
    sessions.dst_ip = INET_ATON('200.148.108.200')) LIMIT 500
```

Exercise SQL-fu here or use query builder
Session data shows only one transaction, and it corresponds to packet which caused alert.

Can also launch transcripts from this window or execute a new query by modifying query bar at top.

<table>
<thead>
<tr>
<th>Sensor</th>
<th>Ssn ID</th>
<th>Start Time</th>
<th>End Time</th>
<th>Src IP</th>
<th>SPort</th>
<th>Dst IP</th>
<th>DP ort</th>
<th>S Pckts</th>
<th>D Pckts</th>
<th>S Bytes</th>
<th>D Bytes</th>
</tr>
</thead>
</table>
A user in Alaska is trying to establish SMB connections to port 445 TCP. Is this legitimate?
Ethereal follows the entire session and shows this is part of a brute forcing attempt. The target account is locked out.
Query for session data shows hundreds of similar sessions to multiple systems.
Adding a Snort rule to knock down connections with TCP RSTs foils a similar brute forcing attack.
Case 7

Repeated traffic from port 20 to port 20, with no application data. What is this?
Session data query shows traffic from the local IP outbound to the Total Velocity IP, using ports 80, 20, and 21 TCP.
Transcript shows local IP failing to retrieve AddybK.dll; probably infected with malware. Research ties DLL to centralmedia.ws, an adware developer. Note the private source IP in the “PORT” command.
Bonus Coverage!

As I was preparing this presentation, something changed at a client's site...
Never-before-seen (at this site) NetBIOS DCERPC ISystemActivator path overflow alerts appear!

<table>
<thead>
<tr>
<th>ST</th>
<th>CNT</th>
<th>Sensor</th>
<th>sid.cid</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>
</table>
A query for session data shows worm/intruder tried connecting to port 4444 TCP on two targets. Neither shows any bytes of data sent by the source or the destination, so the exploit probably did not succeed. Full content data reveals SYN - RST ACK sessions.
A more complicated session data query tries to discover why these alerts appeared out of nowhere.

By querying for one of the target IPs, with session bytes > 0, and ignoring ports 80 and 443, we see exactly when the outside world began interacting with newly available ports on this target.

Thanks again to session data, we can inform the client when a change was made to the access control at the client site.
Future Developments

- Snort rule and sensor management features
- Sguil 0.4.0 offers SANCP (www.metre.net) to replace Snort keepstats session logging
- Augment database output to include PostgreSQL and Oracle
- Test ability to scale
- Rewrite some components in compiled languages
- Live CD or install CDs to ease installation
- FreeBSD port
Questions?

• Thank you for your time.