Deploying Security Analytics
Tips & Tricks to Achieve Ludicrous Speed
Guy Bruneau, GSE
About Me

• Senior Security Consultant @IPSS Inc.
• Incident Handler @Incident Storm Center
  – gbruneau@isc.sans.edu
• Experience: NetWitness 8.x to SA 10.3x
• Deployment: Medium to large networks
• Twitter: @GuyBruneau
Overview

• Why use Security Analytics?
• Network Forensics Objectives And Tips
• First Things First – Pre-deployment Decisions
• Tuning SA
• Backing Up SA
• Automation With nwconsole And Malware Analysis
• Remote Logging
Network Forensics Objectives in SA

• The Goal Is To Provide Information For Response
  – What, When, Where, How, And Possibly Who/Why

• Forensics Is All About Meta
  – Creating, Querying, And Reporting

• Keep Only Forensically Sound Meta For Analysis
  – Query Response Slows Down A Lot
Network Forensics Tips In SA

• First, Appliances Time Must Be Accurate
• Identify What Meta Can Be Stitched Together To Answer
  
  Example:
  – alias.host = adobe.flash-player-v12.com && directory = /update && filename = 'exe.exe'
First Things First

• Retention - How Long Do You Want (Need) Data?
  – Packet And Meta Retention May Be Different

• Capture Speed And Length
  – Under 1 GB → Default Interface Is Good
  – > 1 GB+ → Must Use A 10 GB Card
  – Test The Decoder Interface Capture Length
    • `root@decoder:~# tcpdump -ni eth1 'len >=1514'`

• Retention + Speed Determine Number Of Decoders And Concentrators
Network Forensics Deployment Models

• Basic Setup
  – 1 Broker
  – 1 Concentrator
  – 1 Decoder
    ▪ 1+ DAC
  – Optional
    ▪ Malware Analysis
    ▪ Visualize

• Complex Setup
  – 1 Broker
  – 1 or More Concentrators
  – 2+ Decoders
    ▪ Multiple DAC
  – 1 Malware Analysis
  – Visualize (optional)
Tuning SA - Offloading

• TCP Offloading And Network Capture Effects Can Be Significant
  – Offload Processing Of The Entire TCP/IP Stack To The NIC
  – Used Primarily With High-speed Network Interfaces (Gigabit & 10 Gigabit Ethernet Controller)

• `ethtool -k eth(1-5)` To Check Card Status

  Recommended 1 GB Card Configuration

  `/etc/init.d/rc.local`
  `/usr/sbin/ethtool -K eth1 gso off`
  `/usr/sbin/ethtool -K eth1 gro off`
Tuning SA - Network Model

- Tuning The Network Model Is Worth The Effort
- Identify IP Ranges And Names
- Categorize & Prioritize Business Assets and Networks
  - Create Metadata Feeds
  - Identify Which Networks Should Never Exchange Data
- Track Anomalies
  - Generate Automated Reports Or Notifications

<key description="Network Name" format="Text" level="IndexKeys" name="netname"/>

© Copyright 2014 EMC Corporation. All rights reserved.
Tuning SA - Index Meta

- Not All Meta Is Indexed!
  - streams = 1 → Detect Portscan Activity
  - tcp.flags → Detect Inbound Backscatter Activity
    - select ip.src where tcp.flags = 18 && streams = 1
  - tcp.srcport and udp.srcport
    - select ip.src where tcp.srcport = 0 || tcp.srcport = 6000 && streams = 1
  - ASN = 872 → Portscan By ASN Top 10 Target Ports
    - select asn.src where streams = 1 then lookup_and_add ('tcp.dstport','asn.src',10)

<key description="TCP Source Port" level="IndexNone" name="tcp.srcport" />
Tuning SA - Improve Decoder Performance

- Filter Packets (Proto 47, 50, 51) At The Decoder
- Unless You Have The Private Key; Keep Metadata And Truncate SSL Payload
- Turn Off Meta And Delete Non-used Parsers
- Use Custom Snort Rules When Needed
- Increase Decoder Kernel Cache Memory to 1GB

```
/etc/sysctl.conf
vm.min_free_kbytes = 1048576
```
Tuning SA - Parsers Affecting Performance

• Some Parsers Are Known To Affect Capture
  – DNS, GeoIP, And Mail

• Evaluate These To Determine If You Have 100% Collection

<table>
<thead>
<tr>
<th>Time</th>
<th>Message Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mar 10 16:47:12</td>
<td>TDC-Decoder nw[2806]: [Parse] [warning] Parser ethernet_oui loaded without callbacks</td>
</tr>
<tr>
<td>Mar 10 16:47:12</td>
<td>TDC-Decoder nw[2806]: [Parse] [warning] Parser spectrum_lua loaded without callbacks</td>
</tr>
<tr>
<td>Mar 10 16:47:12</td>
<td>TDC-Decoder nw[2806]: [Parse] [warning] Parser TLD_lua loaded without callbacks</td>
</tr>
</tbody>
</table>
Backing Up SA

• Not Perfect But Worth Doing

• Copy These Configuration Folders/Files
  – /etc/netwitness
  – /etc/ntp.conf
  – /etc/hosts
  – /home/rsasoc -> Reports
  – /var/lib/netwitness/uax -> Server Configuration
Automation With NwConsole

• Copy Binary From Decoder To A Workstation And Script Advanced Use Cases
  – Automated File Carving
  – Inbound Attachment Extraction
  – Carve Session ID As pcap

sdk open nw://admin:netwitness@192.168.25.50:50005
sdk output /home/Executables
sdk content session=now-u where="filetype=windows_executable"
render=files includeFileTypes=.exe maxDirSize=1000000
Automation With Malware Analysis

• Adjust Decoder And Malware Analysis Settings
  – Tune In Decoder App Rules
  – Process Just The Data You Want Analyzed
    • Create A Feed With HP, Win Updates, etc To Remove Unwanted Files

• Move Files To This Directory
  – /var/lib/rsamalware/spectrum/infectedZipWatch/pendingUpload

• Create Hash Lists For Good & Bad In CSV Format
  – /var/lib/rsamalware/spectrum/hasWatch
Remote Logging

• Syslog RSA SA devices To A SIEM Of Your Choice
  – Log Queries Executed By Users
  – Monitor Device Status Including Collection

• Broker Reporting Engine - CEF Format To ArcSight

CEF:0|NetWitness|SA|10.3.2|${name}|${name}|5| rt={#time:MMM dd yyy HH:mm:ss} externalId={#sessionid} proto={#ip.proto} deviceDirection=0 src={#ip.src} spt={#udp.srcport} shost={#alias.host} dst={#ip.dst} dpt={#udp.dstport} dvchost={#did} cat=/Security
Summary

• Tune, Tune, Tune, Never Stop Tuning
• Forensics Is All About Meta
• Keep Only Forensically Sound Meta For Analysis
• Retention - How Long Do You Want (Need) Data?
• Categorize & Prioritize Business Assets and Networks
• Automate Tasks With NwConsole