OSSEC & OSSIM
Unified Open Source Security
santiago@alienvault.com
Why OSSIM

Open Source SIEM – GNU GPL 3.0

• Provides **threat detection** capabilities

• **Monitors** network assets

• Centralizes **Information** and **Management**

• **Assesses** threats reliability and **risk**

• Collaboratively learns about **APT**

OSSIM Embedded Tools

**Assets**
- nmap
- prads

**Behavioral monitoring**
- fprobe
- nfdump
- ntop
- tcpdump
- nagios

**Threat detection**
- ossec
- snort
- suricata

**Vulnerability assessment**
- osvdb
- openvas
OSSIM Collectors
OSSIM Collector Anatomy

[apache log]
76.103.249.20 - - [15/Jun/2013:10:14:32 -0700] "GET /ossim/session/login.php HTTP/1.1" 200 2612 ""Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/27.0.1453.110 Safari/537.36"

[apache.cfg]
event_type=event
regexp="((?P<dst>\S+):(\?P<port>\d\{1,5\})?)\?(?P<src>\S+)\?(?P<id>\S+)\?(?P<user>\S+)\?\{(\?P<date>\d\{2\})/\w\{3\}/\d\{2\}:\d\{2\}:\d\{2\}:\d\{2\}\s+[+-\-\d\{4\}\}\"(?P<request>\.*)\"\?(?P<code>\d\{3\})\?(?P<size>\d\{1,5\})\?\"\?(?P<referer_uri>\.*)\"\?(?P<useragent>\.*)\")\?\$"
src_ip={resolv($src)}
dst_ip={resolv($dst)}
dst_port={$port}
date={normalize_date($date)}
plugin_sid={$code}
username={$user}
userdata1={$request}
userdata2={$size}
userdata3={$referer_uri}
userdata4={$useragent}
filename={$id}
OSSIM Threat assessment

- SSH Failed authentication event
  - SSH successful authentication event
  - 100 SSH Failed authentication events
    - 1000 SSH Failed authentication events
      - Persistent connections
      - SSH successful authentication event
      - 1000 SSH Failed authentication events
  - 10 SSH Failed authentication events
    - SSH successful authentication event
OSSIM Risk assessment

\[ \text{RISK} = \frac{(\text{ASSET VALUE} \times \text{EVENT PRIORITY} \times \text{EVENT RELIABILITY})}{25} \]

Source

- Asset Value = 2
- Event Priority = 2
- Event Reliability = 10

Destination

- Asset Value = 5
OSSIM Attack analysis

- Alert: Low reputation IP
  - OTX
- Vulnerability: IIS Remote Command Execution
  - OpenVAS
- Attack: WEB-IIS multiple decode attempt
  - SNORT
- Accepted HTTP packet from X.X.X.X to Y.Y.Y.Y
  - Web server
- Alert: IIS attack detected
  - OSSEC
- Target Y.Y.Y.Y
- Attack: X.X.X.X

Attacker

Target
Why OSSEC

Open Source Host-based IDS (HIDS)

• **Log analysis** based intrusion detection
• File **integrity checking**
• Registry keys integrity checking (Windows only)
• Signature based malware/\textit{rootkits detection}
• Real time **alerting** and active response
• Feeds SIEMs (OSSIM)
OSSEC Architecture

OSSEC Agent
• **Logcollectord**: Read logs (syslog, wmi, flat files)
• **Syscheckd**: File integrity checking
• **Rootcheckd**: Malware and rootkits detection
• **Agentd**: Forwards data to the server

OSSEC Server
• **Remoted**: Receives data from agents
• **Analysisd**: Processes data (main process)
• **Monitord**: Monitor agents
OSSEC Integration

Monitored Host

- Logcollector
- Syscheckd
- Rootcheckd

Agentd

OSSEC Server

- Monitored Host
- OSSIM Sensor

Remoted
- Analysisd
  - Decode
  - Analyze
- Monitorod

OSSIM Sensor

- Alerts.log
- Ossec collector
- Ossim-agent

OSSIM Server

- Alarm
- Ossim-server
- Correlation
- Risk assessment
- Logger

OSSEC Agent

OSSIM Agent

OSSIM Server
OSSEC Collector Anatomy

**[ossec.conf]**

```xml
<custom_alert_output>
</custom_alert_output>
```

**[alerts.log]**

AV - Alert - "1374721595" --> RID: "3333"; RL: "7"; RG: "syslog,postfix,service_availability,"; RC: "Postfix stopped."; USER: "None"; SRCIP: "None"; HOSTNAME: "10.0.0.80"; LOCATION: "/var/log/syslog";
EVENT: "[INIT]May 16 14:47:19 10.0.0.80 postfix/master[2925]: terminating on signal 15[END]"

**[ossec-single-line.cfg]**

```plaintext
[ossec.conf]
<custom_alert_output>
</custom_alert_output>
```
### OSSIM Correlation Rules

**[AV Bruteforce attack, SSH authentication attack]**

<table>
<thead>
<tr>
<th>Name</th>
<th>Reliability</th>
<th>Timeout</th>
<th>Occurrence</th>
<th>From</th>
<th>To</th>
<th>Data Source</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSH service authentication attempts failed detected</td>
<td>4</td>
<td>None</td>
<td>1</td>
<td>ANY</td>
<td>ANY</td>
<td>ossec-authentication_failures (7012)</td>
<td>SID: 5712</td>
</tr>
<tr>
<td>SSH service authentication attempts failed detected</td>
<td>6</td>
<td>1800</td>
<td>1</td>
<td>1:SRC_IP</td>
<td>1:DST_IP</td>
<td>ossec-authentication_failures (7012)</td>
<td>SID: 5712</td>
</tr>
<tr>
<td>SSH service authentication attempts failed detected</td>
<td>6</td>
<td>1800</td>
<td>10</td>
<td>1:SRC_IP</td>
<td>1:DST_IP</td>
<td>ossec-authentication_failures (7012)</td>
<td>SID: 5712</td>
</tr>
<tr>
<td>SSH service authentication attempts failed detected</td>
<td>6</td>
<td>1800</td>
<td>20</td>
<td>1:SRC_IP</td>
<td>1:DST_IP</td>
<td>ossec-authentication_failures (7012)</td>
<td>SID: 5712</td>
</tr>
<tr>
<td>SSH service authentication attempts failed detected</td>
<td>8</td>
<td>3600</td>
<td>50</td>
<td>1:SRC_IP</td>
<td>1:DST_IP</td>
<td>ossec-authentication_failures (7012)</td>
<td>SID: 5712</td>
</tr>
<tr>
<td>SSH service authentication attempts failed detected</td>
<td>8</td>
<td>30000</td>
<td>100</td>
<td>1:SRC_IP</td>
<td>1:DST_IP</td>
<td>ossec-authentication_failures (7012)</td>
<td>SID: 5712</td>
</tr>
<tr>
<td>SSH service authentication attempts failed detected</td>
<td>8</td>
<td>43200</td>
<td>500</td>
<td>1:SRC_IP</td>
<td>1:DST_IP</td>
<td>ossec-authentication_failures (7012)</td>
<td>SID: 5712</td>
</tr>
<tr>
<td>SSH service authentication successful detected</td>
<td>10</td>
<td>10</td>
<td>1</td>
<td>1:SRC_IP</td>
<td>1:DST_IP</td>
<td>ossec-authentication_success (7009)</td>
<td>SID: 5715</td>
</tr>
<tr>
<td>SSH service authentication successful detected</td>
<td>10</td>
<td>10</td>
<td>1</td>
<td>1:SRC_IP</td>
<td>1:DST_IP</td>
<td>ossec-authentication_success (7009)</td>
<td>SID: 5715</td>
</tr>
<tr>
<td>SSH service authentication successful detected</td>
<td>10</td>
<td>10</td>
<td>1</td>
<td>1:SRC_IP</td>
<td>1:DST_IP</td>
<td>ossec-authentication_success (7009)</td>
<td>SID: 5715</td>
</tr>
<tr>
<td>SSH service authentication successful detected</td>
<td>10</td>
<td>10</td>
<td>1</td>
<td>1:SRC_IP</td>
<td>1:DST_IP</td>
<td>ossec-authentication_success (7009)</td>
<td>SID: 5715</td>
</tr>
<tr>
<td>SSH service authentication successful detected</td>
<td>7</td>
<td>10</td>
<td>1</td>
<td>1:SRC_IP</td>
<td>1:DST_IP</td>
<td>ossec-authentication_success (7009)</td>
<td>SID: 5715</td>
</tr>
<tr>
<td>SSH service authentication successful detected</td>
<td>2</td>
<td>10</td>
<td>1</td>
<td>1:SRC_IP</td>
<td>1:DST_IP</td>
<td>ossec-authentication_success (7009)</td>
<td>SID: 5715</td>
</tr>
<tr>
<td>SSH service authentication successful detected</td>
<td>0</td>
<td>10</td>
<td>1</td>
<td>1:SRC_IP</td>
<td>1:DST_IP</td>
<td>ossec-authentication_success (7009)</td>
<td>SID: 5715</td>
</tr>
</tbody>
</table>

**Correlation Engine Alert**

**OSSEC Rule ID**

**Alert Reliability**

**OSSEC Event Type**
OSSIM Alarm

[AV Bruteforce attack, Windows authentication attack]

<table>
<thead>
<tr>
<th>#</th>
<th>Alarm</th>
<th>Risk</th>
<th>Date</th>
<th>Source</th>
<th>Destination</th>
<th>Correlation Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ossec: Windows Logon Failure.</td>
<td>0</td>
<td>2013-07-23 06:44:39</td>
<td>windows70</td>
<td>windows70</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>ossec: Windows Logon Failure.</td>
<td>0</td>
<td>2013-07-23 06:44:38</td>
<td>windows70</td>
<td>windows70</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>ossec: Windows Logon Failure.</td>
<td>0</td>
<td>2013-07-23 06:44:37</td>
<td>windows70</td>
<td>windows70</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>ossec: Windows Logon Failure.</td>
<td>0</td>
<td>2013-07-23 06:44:36</td>
<td>windows70</td>
<td>windows70</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>AV Bruteforce attack, Windows authentication attack against windows70</td>
<td>1</td>
<td>2013-07-23 06:44:35</td>
<td>windows70</td>
<td>windows70</td>
<td></td>
</tr>
</tbody>
</table>

Alarm Summary [Total events matched with high rule level: 4 - Total Events: 10 - Unique Dist IPAddr: 1 - Unique Types: 1 - Unique Dist Ports: 1]
OSSEC Embedded GUI

- Status monitor
- Events viewer
- Agents control manager
- Configuration manager
- Rules viewer/editor

- Logs viewer
- Server control manager
- Deployment manager
- Rules viewer/editor
- PDF/HTML Reports
Questions / Demo time
santiago@alienvault.com
@santiagobassett