OSSEC

Protecting your network, one host at a time

What is OSSEC?

- Host-Based Intrusion Detection System
- Log Analyzer
- File Integrity Monitor
- Rootkit Detector

What is OSSEC?

- Host-Based Intrusion Detection System
- Log Analyzer
- File Integrity Monitor
- Rootkit Detector
- F R E E

Log Analysis

- Real Time
- Regular Expression Engine
- Level-Based Alerts
- Rules Inheritance

```
<!-- SSHD messages -->
<group name="syslog,sshd,">
  <rule id="5700" level="0" noalert="1">
    <decoded_as>sshd</decoded_as>
    <description>SSHD messages grouped.</description>
  </rule>

  <rule id="5701" level="8">
    <if_sid>5700</if_sid>
    <match>Bad protocol version identification</match>
    <description>Possible attack on the ssh server </description>
    <description>(or version gathering).</description>
</rule>

<rule id="5702" level="5">
  <if_sid>5700</if_sid>
  <match>^reverse mapping</match>
  <regex>failed - POSSIBLE BREAK</regex>
  <description>Reverse lookup error (bad ISP or attack).</description>
</rule>

<rule id="5703" level="10" frequency="4" timeframe="360">
  <if_matched_sid>5702</if_matched_sid>
  <description>Possible breakin attempt </description>
  <description>(high number of reverse lookup errors).</description>
</rule>
```

Active Response

- Programmable Response
- Timeout Escalation
- If you can script it, it can do it
- Whitelists

```
<command>
    <name>restart-ossec</name>
    <executable>restart-ossec.sh</executable>
    <expect>srcip</expect>
    <timeout_allowed>no</timeout_allowed>
</command>

<command>
    <name>firewall-drop</name>
    <executable>firewall-drop.sh</executable>
    <expect>srcip</expect>
    <timeout_allowed>yes</timeout_allowed>
</command>

<active-response>
    <command>firewall-drop</command>
    <location>local</location>
    <level>6</level>
    <timeout>21600</timeout>
    <repeated_offenders>720,1440,10080</repeated_offenders>
</active-response>

<active-response>
    <command>restart-ossec</command>
    <location>local</location>
    <rules_id>100005</rules_id>
</active-response>
```

File Integrity Monitor

- Multiple Checks
  - SHA1 / MD5 Hash
  - File Size
  - Permissions
  - Group / Owner
- Can be realtime (No Windows)

Rootkit Detection

- Periodic Scanning
- Database of common files and trojans
- /dev scanning
- Hidden port scanning
- Hidden Process Scanning
- Filesystem Scanning
  - "Unusual" Files
  - Permissions Problems
    - Root owns, others write

Did I mention it's FREE?

Questions?