



OSSEC HIDS - Ottsec

Daniel B. Cid
dcid@ossec.net



Agenda

- 1 - Concepts
- 2 – OSSEC in the “real world”



1 – Concepts

- 1.1 - Security terminology (HIDS, LIDS, etc)
- 1.2 - Defining LIDS
- 1.3 - LIDS benefits
- 1.4 - What is OSSEC
- 1.5 - Modes of operation
- 1.6 - Why OSSEC
- 1.7 - Why OSSEC(2)

1.1 – Security terminology

- **HIDS – Host-based intrusion detection**
 - Process or techniques to detect attacks, software misuse or policy violations from within the systems to protect.
 - Includes LIDS, Integrity checking, rootkit detection, etc.
- **LIDS – or security log analysis**
 - **Log-based Intrusion Detection System**
- **Integrity checking**
 - Process to detect changes to critical parts of a system(configuration files, binaries, kernel, etc).
- **Rootkit detection**
 - Process to detect the presence of kernel or application level rootkits or trojans on a system.

1.2 - Defining LIDS

- Log-Based Intrusion Detection
 - New terminology, widely used by OSSEC

Log Analysis for intrusion detection is the process or techniques used to detect attacks on a specific environment

using logs as the primary source of information.

LIDS is also used to detect computer misuse, policy violations

and other forms of inappropriate activities.



1.3 - LIDS benefits

- Cheap to implement
 - OSSEC is free, for example
 - Does not require expensive hardware
- Visibility of encrypted protocols
 - SSHD and SSL traffic are good examples
- Visibility of system activity (kernel, internal users, etc)
- Every application can be a part of it
 - They all have some kind of log!
 - Including firewalls, routers, web servers, applications, etc



1.4 - What is OSSEC?

- Open Source Host-based IDS (HIDS)
- <http://www.ossec.net>
- Main tasks:
 - *Log analysis (LIDS – Log-based Intrusion Detection)*
 - *File Integrity checking (Unix and Windows)*
 - *Registry Integrity checking (Windows)*
 - *Host-based anomaly detection (for Unix – rootkit detection)*
 - *Policy monitoring/enforcement*
 - *Active response*

OSSEC is an Open Source Host-based Intrusion Detection System. It performs log analysis, integrity checking, Windows registry monitoring, Unix-based rootkit detection, real-time alerting and active response.



1.5 – Modes of operation

- Centralized architecture
 - *Agent/server mode, where a small agent is installed on each system to be monitored.*
 - *All the analysis and correlation done at the server side.*
 - *OSSEC server = Centralized manager.*
 - *Recommended for most networks.*
 - *Agent/server communication is compressed/encrypted*
- Local mode
 - *When you just have one system to monitor (single desktops)*



1.6 - Why OSSEC?

- Solves real problems
- Free – GPLv3
- Easy to install
- Easy to customize (rules and config in xml format)
- Scalable (client/server architecture)
- Multi-platform (Windows, Solaris, Linux, *BSD, etc)
- Secure by default
- Comes with hundreds of decoders/rules out of the box:
 - *Unix Pam, sshd (OpenSSH), Solaris telnetd, Samba, Su, Sudo, Proftpd, Pure-ftpd, vsftpd, Microsoft FTP server, Solaris ftpd, Imapd, Postfix, Sendmail, vpopmail, Microsoft Exchange, Apache, IIS5, IIS6, Horde IMP, Iptables, IPF. PF, Netscreen, Cisco PIX/ASA/FWSM, Snort, Cisco IOS, Nmap, Symantec AV, Arpwatch, Named, Squid, Windows event logs, etc ,etc,*



1.7 - Why OSSEC (2)?

- External references:
 - OSSEC #1 open source security tool in the enterprise
<http://www.linuxworld.com/news/2007/031207-top-5-security.html>
 - OSSEC #2 IDS tool in the security tools survey
<http://sectools.org/ids.html>
- Additional references:
<http://www.ossec.net/wiki/index.php/InTheNews>



2 - OSSEC in the real world

- 2.1 – Authentication control
- 2.2 – MSN usage
- 2.3 – Squid logs
- 2.4 – Integrity checking
- 2.5 – Squid logs 2
- 2.6 – Authentication logs



2.1 – Authentication control

- Alerting on every authentication success outside business hours
 - Every authentication event is classified as “authentication success” (that's why we use `if_group`)
 - Added to **local_rules.xml**:

```
<rule id="100101" level="10">  
  <if_group>authentication_success</if_group>  
  <time>7 pm - 6:30 am</time>  
  <description>Login during non-business hours.</description>  
</rule>
```



2.1 Authentication control 2

- Alerting on first time logins outside business hours
 - We have some FTS (first time seen) rules
 - Increased severity when a user logs in for the first time on a specific system outside business hours
 - Added to **local_rules.xml**:

```
<rule id="100101" level="13">  
  <if_sid>18119, 10100</if_sid>  
  <time>7 pm - 6:30 am</time>  
  <description>First time Login during non-business hours.</description>  
</rule>
```



2.2 – MSN usage

- Alerting on new MSN users
 - MSN logs to the event log (with the email address) every time it starts

```
<rule id="100213" level="7">  
  <if_sid>18101</if_sid>  
  <id>102</id>  
  <match>The database engine started a new instance</match>  
  <description>MSN login.</description>  
</rule>
```

```
2008 Apr 17 20:02:16 (xx) 192.168.2.190->WinEvtLog WinEvtLog: Application:  
INFORMATION(102): ESENT: (no user): no domain: OSSEC-HM: msnmsgr (1240)  
\\.\C:\Documents and Settings\xyz\Local Settings\Application  
Data\Microsoft\Messenger\xyz@hotmail.com\SharingMetadata\Working\database_F218_E  
79B_18E7_5CDB\dfsр.db: The database engine started a new instance (0)
```

2.3 – User agent (squid)

- Rule to detect internal hosts scanning the outside
 - We already have rules to detect multiple 400/500/600 errors codes
 - Added one to detect non-standard user agents (had to modify squid config to log it).
 - Also added FTS rule to alert on new user agents (best method so far)

```
<rule id="100245" level="5">  
  <if_sid>35000</if_sid>  
  <id>^2</id>  
  <match>libwww-perl</match>  
  <description>User agent libwww-perl.</description>  
</rule>
```



2.3 User agent (squid)

- Alert from the new user agent

OSSEC HIDS Notification.

Received From: (proxy) 10.1.2.3->/var/log/squid/usragent.log

Rule: 100467 fired (level 10) -> "New user agent detected."

Portion of the log(s):

```
10.4.45.102 [05/Nov/2007:03:11:43 -0700] "%%%%%%%%%%%6%6%6"
```

2.4 – Integrity checking

- Alerting with high severity on changes to /var/www
 - Every integrity checking event is on the group “syscheck”
 - Sometimes it may be useful to get a high severity alert for changes to critical files, like the htdocs directory on a web server.
 - Added to **local_rules.xml**:

```
<rule id="100345" level="12" >  
  <if_matched_group>syscheck</if_matched_group>  
  <description>Changes to /var/www/htdocs – Critical file!</description>  
  <match>/var/www/htdocs</match>  
</rule>
```



2.5 - Squid logs 2

- Indication of an internal compromised system:
OSSEC HIDS Notification.

Received From: (proxy) 10.1.2.3->/var/log/squid/access.log

Rule: 35058 fired (level 10) -> "Multiple 500/600 error codes (server error)."

Portion of the log(s):

```
179993 1.2.3.4 TCP_MISS/504 1430 GET http://xx.com/cgi/stats/awstats.pl -  
NONE/- text/html
```

```
179504 1.2.3.4 TCP_MISS/504 1410 GET http://xx.com/awstats.pl - NONE/-  
text/html
```

```
179493 1.2.3.4 TCP_MISS/504 1422 GET http://xx2.com/stats/awstats.pl -  
NONE/- text/html
```

```
179494 1.2.3.4 TCP_MISS/504 1438 GET http://xx2.com/cgi-  
bin/stats/awstats.pl - NONE/- text/html
```

```
179507 1.2.3.4 TCP_MISS/504 1426 GET http://xx3.com/awstats/awstats.pl -  
NONE/- text/html
```

2.6 - Auth logs

- Brute force attempts followed by a success

Rule: 5720 (level 10) -> 'Multiple SSHD authentication failures.'

Src IP: 125.192.xx.xx

Feb 11 09:31:58 wpor sshd[4565]: Failed password for root from 125.192.xx.xx port 42976 ssh2

Feb 11 09:31:58 wpor sshd[4565]: Failed password for admin from 125.192.xx.xx port 42976 ssh2

Feb 11 09:31:58 wpor sshd[4565]: Failed password for admin from 125.192.xx.xx port 42976 ssh2

Rule: 40112 (level 12) -> '**Multiple authentication failures followed by a success.**'

Src IP: 125.192.67.136

User: admin

Feb 11 09:31:58 wpor sshd[7235]: Accepted password for admin from 125.192.xx.xx port 42198 ssh2



Conclusion

- OSSEC is very extensible and provides out of the box functionality
- Lots of new features planned for the future
- Web interface also available!

- Look at our manual and FAQ for more information:
<http://www.ossec.net>

- For questions and support, subscribe to our mailing list or visit us at **#ossec** on freenode

QUESTIONS ?