OSSEC

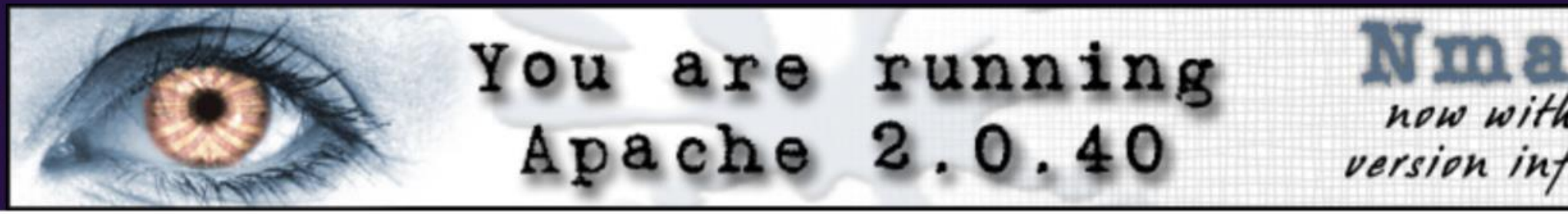
The Untold Story

Daniel Cid / dcid@noc.org

OSSEC Founder

Sucuri / CleanBrowsing Founder

VP Engineering at GoDaddy



OSSEC Host-Based IDS v0.1

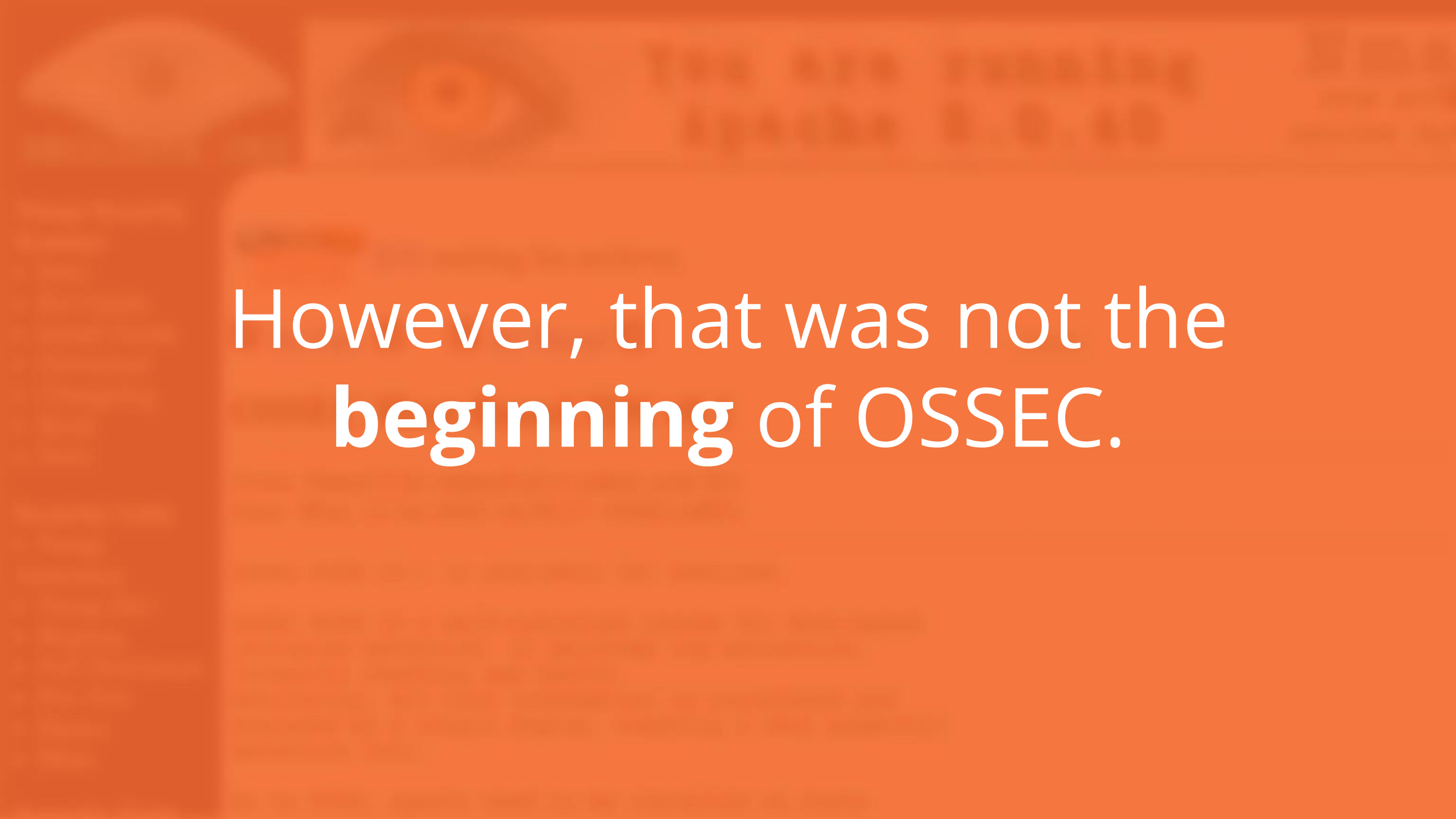
From: Daniel Cid <danielcid () yahoo com br>
Date: Wed, 13 Jul 2005 16:30:17 -0300 (ART)

```
Ossec HIDS v0.1 is available for download.

OSSEC HIDS is a self-contained system for Host-based
intrusion detection. It performs log extraction,
integrity checking and health
monitoring. All this information is correlated and
analyzed by a single engine, creating a very powerfull
detection tool.

As an HIDS, agents need to be installed on every
```

OSSEC HIDS is a self-contained system for Host-based intrusion detection. It performs log extraction, integrity checking and health monitoring. All this information is correlated and analyzed by a single engine, creating a very powerful detection tool.



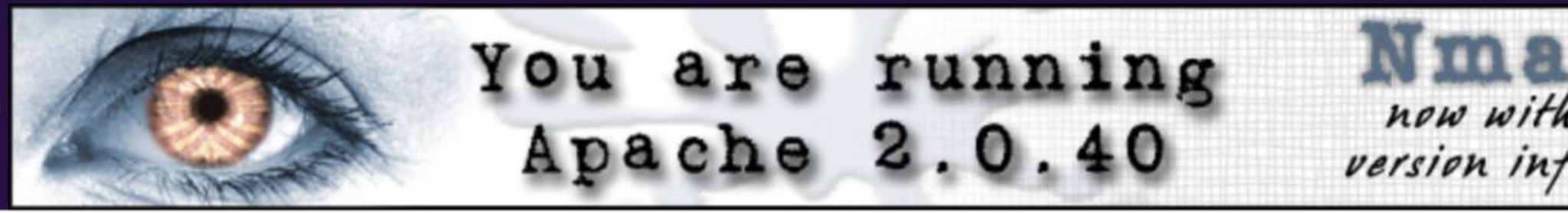
However, that was not the **beginning** of OSSEC.

Rootcheck project
OsHids project
SysCheck project
Owl (Web monitor) Project

SysCheck = Integrity Checking

RootCheck = Rootkit Detection

OSHIDs was actually a local version of the OSSEC log analysis engine. It was written in Perl and released back in 2003.



OsAudit v0.1 (log gathering, monitoring and analysis) available.

From: Daniel Cid <danielcid () yahoo com br>
Date: Thu, 17 Feb 2005 15:09:36 -0300 (ART)

```
OsAudit version 0.1 is available for download.

OsAudit is a complete system for log gathering,
monitoring and analysis. It has two different running
modes: server and client.

In client mode, OsAudit will read the logs and forward
them (encrypted) to the server station.
In server mode, OsAudit will receive external logs
from the clients or from any other device that can
```

OSSEC V0.1

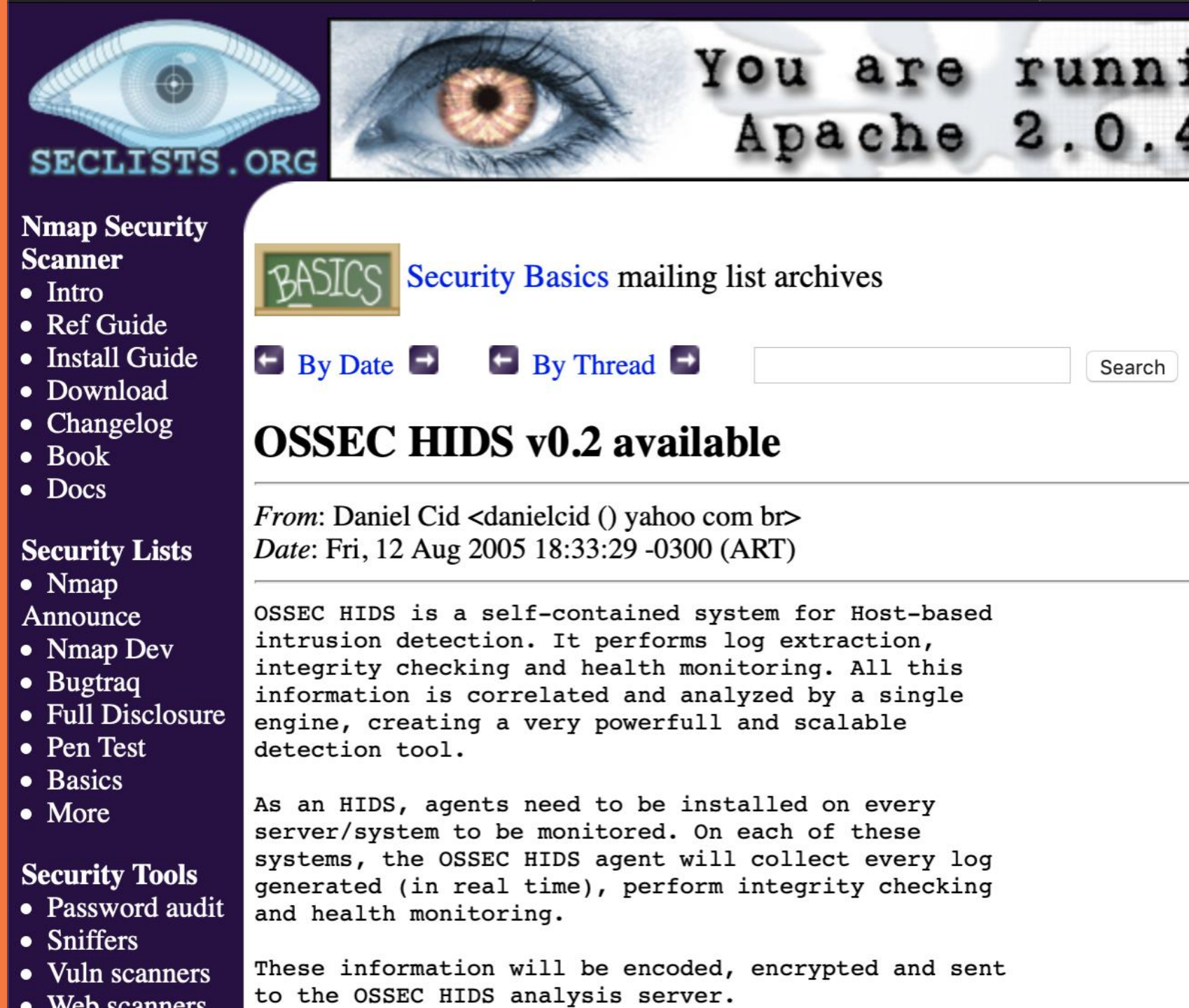
OSSEC HIDS Project

OSSEC HIDS is an Open source Host-based intrusion detection software. It performs log extraction, integrity checking, rootkit detection and health monitoring.
All this information is correlated and analyzed by a single engine, creating a very powerfull detection tool.

As an HIDS, agents need to be installed on every server/system to be monitored. On each of these systems, the OSSEC HIDS agent will collect every log generated (in real time), perform integrity checking, rootkit detection and health monitoring.
This information will be encoded, encrypted and sent to OSSEC HIDS analysis server.

On the OSSEC HIDS analysis server, these events will be compared against a set of "analysis rules", checked using the "FTS" detection and using a statistical analysis. The analysis server can also receive syslog messages remotely (UDP 514) and analyze Snort, Barnyard and Apache logs (for better correlation).

OSSEC V0.2


SECLISTS.ORG
You are runni
Apache 2.0.4
Nmap Security Scanner
• Intro
• Ref Guide
• Install Guide
• Download
• Changelog
• Book
• Docs
Security Lists
• Nmap Announce
• Nmap Dev
• Bugtraq
• Full Disclosure
• Pen Test
• Basics
• More
Security Tools
• Password audit
• Sniffers
• Vuln scanners
• Web scanners
BASICS
Security Basics mailing list archives
By Date
By Thread
Search
OSSEC HIDS v0.2 available
From: Daniel Cid <danielcid () yahoo com br>
Date: Fri, 12 Aug 2005 18:33:29 -0300 (ART)
OSSEC HIDS is a self-contained system for Host-based
intrusion detection. It performs log extraction,
integrity checking and health monitoring. All this
information is correlated and analyzed by a single
engine, creating a very powerfull and scalable
detection tool.
As an HIDS, agents need to be installed on every
server/system to be monitored. On each of these
systems, the OSSEC HIDS agent will collect every log
generated (in real time), perform integrity checking
and health monitoring.
These information will be encoded, encrypted and sent
to the OSSEC HIDS analysis server.

OSSEC V0.3

```
Version 0.3 of the OSSEC HIDS is now available!

This new version includes a lot of new features and bug fixes.
Some of them are listed bellow:

-logcollector running as only one process and with major performanc
 improvements.

-Added automatic ignore to the syscheck. Now files that change cons
 will go to a ignore list.

-Added new options to the rules, including "noalert", "ignore" (tim
ignore
 a rule after matched) and "if_matched_sid".

-Added a bunch of new rules and improved some of the ones already
existent. Hashed
 some of them to improve performance (see kernel rules).

-Added support for the maild to send multiple messages at the same
It will
 avoid excessive emails at a short period of time.

-Local installation option added. A lot of people have only one mac
to
 monitor and wanted a simple installation for that.

-Added the manage_agents to add, delete, extract and import informa
related
 to agents. Now it's much simpler than the old addagent. Look here
more
```

OSSEC V0.4

```
Version 0.4 of the OSSEC HIDS is now available!

This version includes a new rootkit detection system, an
improved integrity detection engine (much more complete and with
much more detailed alerts), a faster and powerfull analysis
system and complete support to Solaris and MacOS (in addition
to Linux, *BSD, etc). Our FAQ (http://www.ossec.net/hids/faq.php)
has more information and we have a new mailling list for the projec
( http://www.ossec.net/hids/index.php#Maillists ).


Detailed changelog:

-Addition of the rootkit detection engine. Based on the rootcheck
 project (http://www.ossec.net/rootcheck). Very fast and with suppo
 to dynamic rules (http://www.ossec.net/hids/rootkits).
 More information at: http://www.ossec.net/rootcheck/rootcheck.txt

-Addition of an "automatic signatures update". Whenever you update
 the rootkit rules on the analysis server, they will be forwarded
 to the agents automatically (decreasing the configuration burden).
 The files under /var/ossec/etc/shared/ will be shared from the
 server to all agents.

-Much improved integrity checking alerts. We provide detailed infor
 regarding to what changed on the files.
 (thanks to Dimitris Ntelakis for the idea).

-Improved correlation engine. Much faster and reliable now.

-Addition of new log analysis rules and tunning of the old ones.
```

OSSEC V0.4

OSSEC HIDS v0.4 available - log analysis, rootkit detection and integrity checking

BACK

26 Oct 2005 | Intrusion Detection | 10299 | Brittany Day | Daniel Cid

Version 0.4 of the OSSEC HIDS is now available. OSSEC HIDS is an Open source Host-based intrusion detection software. It performs log analysis, integrity checking, rootkit detection and health monitoring. All this information is correlated and analyzed by a single engine, creating a very powerfull detection tool. OSSEC HIDS is very scalable, allowing you to easily monitor multiple systems from a central server. This new version includes a new rootkit detection system, an improved integrity detection engine (much more complete and with much more detailed alerts), a faster and powerfull analysis system and complete support to Solaris and MacOS (in addition to Linux, *BSD, etc).

Our FAQ (http://www.ossec.net/hids/faq.php) has more information and we have a new mailling list for the project (

OSSEC V0.5

Version 0.5 of the OSSEC HIDS is now available!

This new version includes active response support, allowing responses to be executed on the server, on the agents, on an external device or everywhere. By default, it comes with two active response plugins. One to add a host to the hosts.deny file and the other one to add an IP address to the drop list of iptables (linux only). In addition to that, this version includes a a lot of bug fixes and small new features.

More information about active response:
http://www.ossec.net/hids/doc.php#active-response

To download the new version:
http://www.ossec.net/hids/files/ossec-hids-0.5.tar.gz

Use our mailling list if you have any question, suggestion or comment :
http://www.ossec.net/hids/index.php#Maillists

Detailed changelog:

-Addition of the active response. You can bind response to rules, specify where to execute the command and also set timeouts..
More information at http://www.ossec.net/hids/doc.php#active-response

-A lot of improvements to the communication channel between the agents and the server. It's much faster and reliable.

-A lot of fixes for the rootkit detection engine (much less false positives).

-Addition of new log analysis rules and tunning of the old ones.

-Created the manual for the project. It's far from complete, but it includes some good information already.
http://www.ossec.net/hids/doc.php

First OSSEC Feedback:

"Why are you wasting your time on this? Stop spamming the mailing lists. If you want to be helpful, just contribute to Tripwire which is a lot better. We don't need another hids."

OSSEC V0.7

Version 0.7 of the OSSEC HIDS is now available!

This is one of the most improved versions so far. It now includes
support for squid, pure-ftpd, postfix and AIX ipsec logs (in addition
to a lot of improvements to the previous rules).
The integrity checking engine now allows granular options, where
you can specify exactly what options you want to monitor (checksum,
size, ownership, etc).
The rootkit detection had a lot of improvements too, reducing false
positives on most of the systems and with a lot of new anomaly
checks to detect kernel level rootkits.
We also have a new website and the installation in 4 different
languages (portuguese, english, german and turkish).
In addition to that, this version includes a lot of bug fixes
and performance improvements.

To download the new version:
http://www.ossec.net/files/ossec-hids-0.7.tar.gz

Use our mailling list if you have any questions, suggestions or
comments :
http://www.ossec.net/en/mailing_lists.html

Detailed changelog (new features):

- Active response for AIX IPSEC (thanks Ahmet Ozturk).

- Rules for pure-ftpd (thanks Peter Ahlert for the logs).

- Rules for Squid (thanks Ahmet).

- Rules for Postfix (thanks Ahmet again :)).

- Improved integrity checking engine that allows granular
  options. You can choose what to monitor on each specific
  file or directory (checksum, size, ownership, etc).

Wednesday Webcast: Log analysis using OSSEC and Logging in Depth

Archived From:

Wednesday, August 02 at 1:00 PM EDT (1700 UTC/GMT)

SANS is happy to bring you the latest in our complimentary series of Webcasts. Join us on Wednesday, August 02 at 1:00 PM as SANS presents:

Log analysis using OSSEC and Logging in Depth

Featuring: Mike Poor & A.N. Ananth

Sponsored by:

PRISM MICROSYSTEMS

You need to register with the SANS portal to be able to sign in.

Webcast Overview:

Log analysis using OSSEC

Register For Webcast:

SANS portal account required. Create a portal account here. Once you have created and verified your portal account please return here to register for this webcast.

SANS Portal Email:

Password:

click here to register

By registering, you agree to share your information with SANS and the sponsor. This

WebCasts SANS

- Upcoming Webcasts
- Webcasts FAQ
- Webcast Archive

Check Them Out!

- **Network Security 2010**
- Security Awareness Training
- Top Cyber Security Risks

"OSSEC is a very powerful yet easy to interpret open source host based intrusion detection system. Over the years this tool has evolved into a powerful cross platform log aggregation and analysis system. In this brief talk we will discuss OSSEC's approach to detecting malicious events including live system root kit detection on Linux. "

Open Source lives and dies with the **community**

Do not take your be-loved open source projects for granted. Be a part of it. Get involved.