

OSSEC HIDS

Installation on FreeBSD 6.1

**August 2006
Secquard BV**

1. Overview

1. Overview.....	2
2. Introduction.....	3
3. Server installation.....	3
3.1. Choose language:.....	3
3.2. System information.....	4
3.3. Type of Installation.....	4
3.4. Setting up the installation environment	4
3.5. Configuring the OSSEC HIDS.....	5
3.6. Startup script	6
3.7. Add agents to server	7
4. Install FreeBSD agent.....	9
4.1. Choose language.....	9
4.2. System information.....	9
4.3. Type of Installation.....	10
4.4. Setting up the installation environment	10
4.5. Configuring the OSSEC agent.	10
4.6. Add key to agent.....	11
5. Install Windows agent	12
5.1. Download the .EXE.....	12
5.2. Install	12
5.3. Configuring the ossec agent	13
5.4. Ossec at startup.....	14
6. Finished.....	15
7. Resources	16

2. Introduction

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

If you have one system to monitor, you can install the OSSEC HIDS locally on that box and do everything from there. However, if you are administering a few systems, you can select one to be your OSSEC server and the others to be OSSEC agents, forwarding events to the server for analysis. One of the greatest benefits of the OSSEC HIDS is its scalability, allowing you to monitor multiple systems from a central point.

In this installation guide I am going to install the OSSEC HIDS Server on a FreeBSD 6.1 box and the agents on a Windows XP and FreeBSD box.

3. Server installation

First we have to download the latest version of OSSEC from their website:

```
# wget http://www.ossec.net/files/ossec-hids-0.9.tar.gz
```

Now unpack the archive:

```
# tar -zxvf ossec-hids-0.9.tar.gz
```

Enter the Ossec directory:

```
# cd ossec-hids-0.9
```

Run the “install.sh” script to install the server:

```
# ./install.sh
```

Follow the steps to install the server:

3.1. Choose language:

```
** Para instalaÃ§Ã£o em portuguÃªs, escolha [br].  
** Fur eine deutsche Installation wohlen Sie [de].  
** For installation in English, choose [en].  
** Pour une installation en franÃ§ais, choisissez [fr]  
** Per l'installazione in Italiano, scegli [it].  
** Aby instalowaÅ w jÃzyku Polskim, wybierz [pl]  
** TÃrkÃŸe kurulum iÃŸin seÃŸin [tr].  
(en/br/de/fr/it/jp/pl/ru/tr) [en]:
```

Just hit “enter” to choose “english”.

3.2. System information

The install script will print some system info on the screen like the following:

```
- System: FreeBSD ossec.howto.com 6.1-RELEASE  
- User: root  
- Host: ossec.howto.com (hostname.yourdomain.com)
```

If you want to continue installing hit “Enter”.

3.3. Type of Installation

Now we have to choose what type of installation we want.

```
- What kind of installation do you want (server, agent, local or  
help)?
```

We are going to install the server so type “server” and hit “Enter”.

3.4. Setting up the installation environment

```
- Choose where to install the OSSEC HIDS [/var/ossec]:
```

Hit “Enter” to install Ossec in “/var/ossec”, or choose your own environment.

3.5. Configuring the OSSEC HIDS

Now we have to configure the OSSEC server.

- Do you want e-mail notification? (y/n) [y]:
- What's your e-mail address? **Your email**
- What's your SMTP server ip/host? **Your smtp server**

- Do you want to run the integrity check daemon? (y/n) [y]:
 - Running syscheck (integrity check daemon).

- Do you want to run the rootkit detection engine? (y/n) [y]:
 - Running rootcheck (rootkit detection).

- Active response allows you to execute a specific command based on the events received. For example, you can block an IP address or disable access for a specific user.
More information at:
<http://www.ossec.net/en/manual.html#active-response>

- Do you want to enable active response? (y/n) [y]:
 - Active response enabled.

- By default, we can enable the host-deny and the firewall-drop responses. The first one will add a host to the /etc/hosts.deny and the second one will block the host on iptables (if linux) or on ipfilter (if Solaris, FreeBSD or NetBSD).
- They can be used to stop SSHD brute force scans, portscans and some other forms of attacks. You can also add them to block on snort events, for example.

- Do you want to enable the firewall-drop response? (y/n) [y]:
 - firewall-drop enabled (local) for levels >= 6

- Default white list for the active response:
 - 10.0.0.1

- Do you want to add more IPs to the white list? (y/n)? [n]: y
 - IPs (space separated): 10.0.0.0/24

- Do you want to enable remote syslog (port 514 udp)? (y/n) [y]:
 - Remote syslog enabled.

- Setting the configuration to analyze the following logs:
 - /var/log/messages
 - /var/log/auth.log
 - /var/log/userlog
 - /var/log/security
 - /var/log/xferlog
 - If you want to monitor any other file, just change the ossec.conf and add a new localfile entry. Any questions about the configuration can be answered by visiting us online at <http://www.ossec.net> .
- Press ENTER to continue ---

Now it will compile everything. After it is completed hit "Enter" to finish.

3.6. Startup script

I grabbed this script from the **Howto "setup OSSEC-HIDS on your ubuntu box"** by **RShadow**

Make the startup script in /usr/local/etc/rc.d/

```
# ee /usr/local/etc/rc.d/ossec
```

And add the following lines:

```
#!/bin/sh

case "$1" in
start)
  /var/ossec/bin/ossec-control start
  ;;
stop)
  /var/ossec/bin/ossec-control stop
  ;;
restart)
  $0 stop && sleep 3
  $0 start
  ;;
reload)
  $0 stop
  $0 start
  ;;
*)
echo "Usage: $0 {start|stop|restart|reload}"
exit 1
esac
```

Make the script executable:

```
# chmod +x ossec
```

3.7. Add agents to server

To manage agent run the following command:

```
# /var/ossec/bin/manage_agents
```

Lets make an agent for a windowsXP box!

```
*****
* OSSEC HIDS v0.9 Agent manager.          *
* The following options are available:    *
*****
(A)dd an agent (A).
(E)xtract key for an agent (E).
(L)ist already added agents (L).
(R)emove an agent (R).
(Q)uit.
Choose your action: A,E,L,R or Q: a

- Adding a new agent (use '\q' to return to the main menu).
Please provide the following:
* A name for the new agent: windowsxp001
* The IP Address of the new agent: 10.0.0.100
* An ID for the new agent[001]: 001
Agent information:
ID:001
Name:windowsxp001
IP Address:10.0.0.100

Confirm adding it?(y/n): y
Agent added.
```


4. Install FreeBSD agent

To install the Ossec agent on a FreeBSD system you have to repeat some of the steps we did before to install the Ossec HIDS server.

First we have to download the latest version of OSSEC from their website:

```
# wget http://www.ossec.net/files/ossec-hids-0.9.tar.gz
```

Now unpack the archive:

```
# tar -zxvf ossec-hids-0.9.tar.gz
```

Enter the Ossec directory:

```
# cd ossec-hids-0.9
```

Run the “install.sh” script to install the server:

```
# ./install.sh
```

Follow the steps to install the server:

4.1. Choose language

```
** Para instalaÃ§Ã£o em portuguÃªs, escolha [br].  
** Fur eine deutsche Installation wohlen Sie [de].  
** For installation in English, choose [en].  
** Pour une installation en franÃ§ais, choisissez [fr]  
** Per l'installazione in Italiano, scegli [it].  
** Aby instalowaÅ w jÃzyku Polskim, wybierz [pl]  
** TÃ¼rkÃ¼se kurulum iÃ§in seÃ§in [tr].  
(en/br/de/fr/it/jp/pl/ru/tr) [en]:
```

Just hit “enter” to choose “english”.

4.2. System information

The install script will print some system info on the screen like the following:

```
- System: FreeBSD ossec.howto.com 6.1-RELEASE  
- User: root  
- Host: ossec.howto.com (hostname.yourdomain.com)
```

If you want to continue installing hit “Enter”.

4.3. Type of Installation

Now we have to choose what type of installation we want.

```
- What kind of installation do you want (server, agent, local or help)?
```

We are going to install the server so type “agentr” and hit “Enter”.

4.4. Setting up the installation environment

```
- Choose where to install the OSSEC HIDS [/var/ossec]:
```

Hit “Enter” to install Ossec in “/var/ossec”, or choose your own environment

4.5. Configuring the OSSEC agent.

```
- What's the IP Address of the OSSEC HIDS server?: 10.0.0.1  
- Adding Server IP 10.0.0.1
```

```
- Do you want to run the integrity check daemon? (y/n) [y]:
```

```
- Running syscheck (integrity check daemon).
```

```
- Do you want to run the rootkit detection engine? (y/n) [y]:
```

```
- Running rootcheck (rootkit detection).
```

```
- Do you want to enable active response? (y/n) [y]:
```

```
- Setting the configuration to analyze the following logs:
```

```
-- /var/log/messages  
-- /var/log/auth.log  
-- /var/log/userlog  
-- /var/log/security  
-- /var/log/xferlog
```

```
- If you want to monitor any other file, just change the ossec.conf and add a new localfile entry.  
Any questions about the configuration can be answered by visiting us online at http://www.ossec.net .
```

```
--- Press ENTER to continue ---
```

Now it will compile everything. After it is completed hit ”Enter” to finish.

4.6. Add key to agent

To add a key to an agent run the following command:

```
*****
* OSSEC HIDS v0.9 Agent manager.          *
* The following options are available:    *
*****
  (I)mport key from the server (I).
  (Q)uit.
Choose your action: I or Q: i

* Provide the Key generated by the server.
* The best approach is to cut and paste it.
*** OBS: Do not include spaces or new lines.

Paste it here (or '\q' to quit):
MDAxIHdpbmRvd3N4cDAwMSAxMC4wLjAuMTAwIGIwZWJlOWUwNjNkZDMxZmEyZ
jc1YjcxOWU1Zjk0NTNlMzRmMjFhYjZkOTM2ZTM5OWI4OTUxMTJhOTU1ZWl2Nz
U=

Agent information:
ID:002
Name:freebsd001
IP Address:10.0.0.101

Confirm adding it?(y/n): y

Now the agent is running!!
Restart the agent by running the following command:

# /var/ossec/bin/ossec-control stop
# /var/ossec/bin/ossec-control start
```

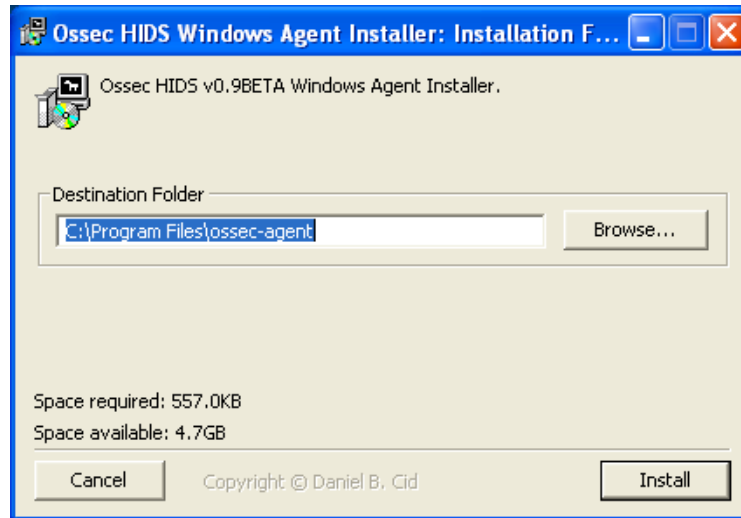
5. Install Windows agent

To install the ossec agent on a windows XP or 2000 box you must complete the next steps.

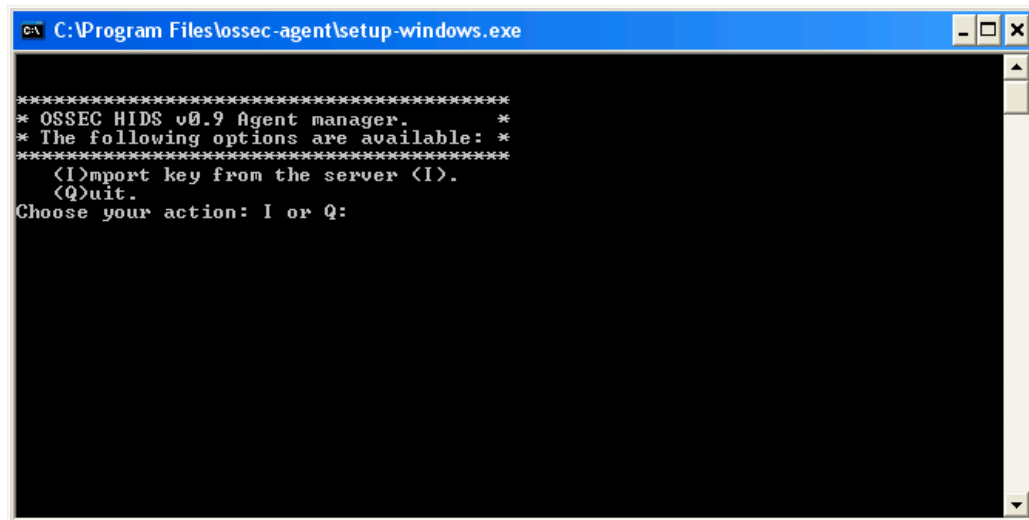
5.1. Download the .EXE

<http://www.ossec.net/files/ossec-agent-win32-0.9.exe>

5.2. Install



Click on the “Install” button to install the agent in C:\Program Files\ossec-agent. If you want to install the agent elsewhere fill in the path.



Type “I” to import a key from the server, Paste the key into the screen. Next type “Q” to quit.

Now the agent is installed!

5.3. Configuring the ossec agent

To configure the agent for connection with the server you have to edit the ossec.conf. If you exit the agent manager this file will automatically pop-up.

The file can be found in **C:\Program Files\ossec-agent** if you want to edit afterwards.

The script has to look like this:

```
<!-- Agent Example Configuration -->
<!-- First, change the server-ip to the IP of your OSSEC HIDS server -->
<!-- Second, add any file that you may want to monitor. -->
<ossec_config>
<client>
<!-- IP address of the Ossec HIDS server -->
    <server-ip>put your servers ip here</server-ip>
</client>
<!-- One entry for each file to monitor -->

<localfile>
    <location>Application</location>
    <log_format>eventlog</log_format>
</localfile>

<localfile>
    <location>Security</location>
    <log_format>eventlog</log_format>
</localfile>

<localfile>
    <location>System</location>
    <log_format>eventlog</log_format>
</localfile>
</ossec_config>

<!-- Default syscheck config -->
<ossec_config>
<syscheck>
    <frequency>7200</frequency>
    <directories check_all="yes">C:\WINDOWS,C:\Program Files</directories>

    <ignore>C:\WINDOWS/system32/LogFiles</ignore>
    <ignore>C:\WINDOWS/WindowsUpdate.log</ignore>
    <ignore>C:\WINDOWS/system32/wbem/Logs</ignore>
    <ignore>C:\WINDOWS/Prefetch</ignore>
    <ignore>C:\WINDOWS/PCHEALTH/HELPCTR/DataColl</ignore>
    <ignore>C:\WINDOWS/SoftwareDistribution/DataStore</ignore>
    <ignore>C:\WINDOWS/SoftwareDistribution/ReportingEvents.log</ignore>
    <ignore>C:\Program Files/ossec-agent</ignore>
    <ignore>C:\WINDOWS/Temp</ignore>
    <ignore>C:\WINDOWS/system32/config/systemprofile/Local Settings</ignore>
    <ignore>C:\WINDOWS/SchedLgU.Txt</ignore>
    <ignore>C:\WINDOWS/system32/config</ignore>
</syscheck>
</ossec_config>
```

To extend your ossec.conf with the log-files from IIS add the following lines to the ossec.conf, note that:

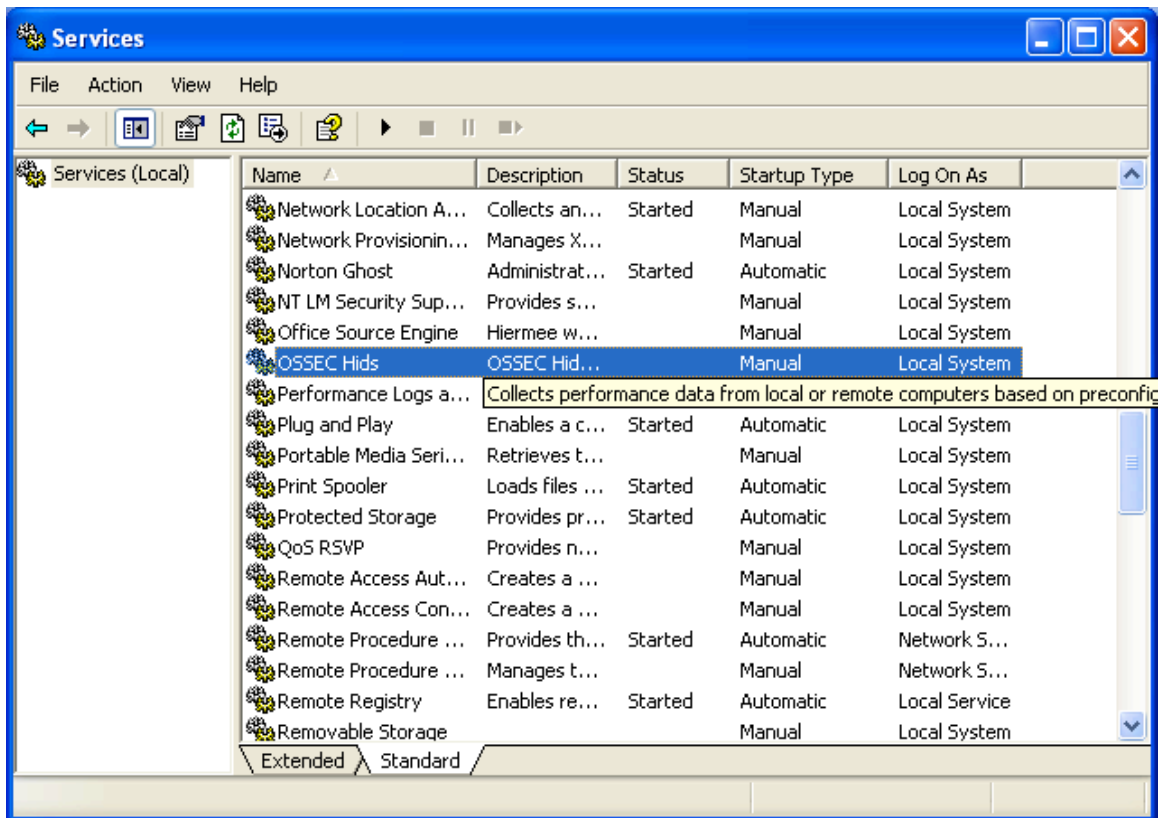
- %y - means currently year
- %m - means currently month
- %d - means currently day

```
<localfile>  
  <location>%WinDir%\System32\LogFiles\W3SVC2\ex%y%m%d.log</location>  
  <log_format>iis</log_format>  
</localfile>
```

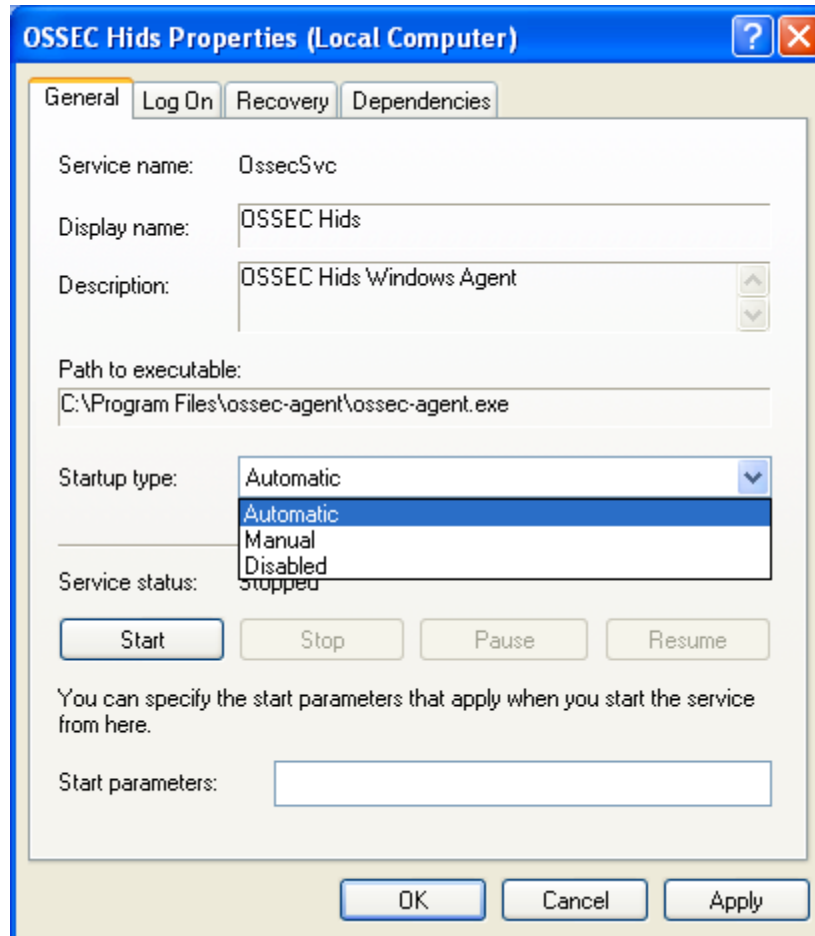
5.4. Ossec at startup

To run the ossec agent at startup you must go to:

- Control Panel → Administrative Tools → Services
- Now look for the 'OSSEC Hids' service



→ Right-click → Properties



Choose “Automatic” in the drop-down menu. Then push the Start button.
The agent is Running!!

6. Finished

Everything is installed and configured, now wait for your first alerts!

Have Fun!!

7. Resources

Ossec homepage – www.ossec.net

Ossec manual - www.ossec.net/en/manual.html

Log analysis for intrusion detection - www.ossec.net/en/loganalysis.html