

```
?SheevaPlug Debian Squeeze???Asterisk/FreePBX?, ?????????????,????,???Asterisk????????????????????,???
OSSEC?????????????.
```

```
OSSEC????????????1.5?????Asterisk????,?????(2010-11-30),???2.5.1.
```

```
??OSSEC?????????????,?????????????.
```

```
A??OSSEC?????????????.
```

Code:

```
cd /root
```

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

```
tar -zxvf ossec-hids-*.tar.gz
```

```
rm ossec-hids-*.tar.gz
```

```
cd ossec-hids-*
```

```
./install.sh
```

```
??./install.sh?????????, ?? *????????????,????, ???????????:
```

```
** Para instalaA$A?o em portuguaAs, escolha [br].
```

```
** e|a??c"?a?-a-?e??el?aR?e?..., e-·e€?a?c [cn].
```

```
** Fur eine deutsche Installation wohlen Sie [de].
```

```
** I"11I± I?I3IoI±I?I?I?I±I?I- I?I?I± I·I?I?I·I?I1IoI?, I?I€11I?I-I?I?I? [el].
```

```
** For installation in English, choose [en].
```

```
** Para instalar en EspaA±ol , eliga [es].
```

```
** Pour une installation en franA$ais, choisissez [fr]
```

```
** Per l'installazione in Italiano, scegli [it].
```

```
** a-?a??ea?a$a??a?3a?1a??a??a??a-a?a?i??e?a??a-a|a??a·a?i??[jp].
```

```
** Voor installatie in het Nederlands, kies [nl].
```

```
** Aby instalowaA? w jA?zyku Polskim, wybierz [pl].
```

```
** D"D?N D?D?NN?N€N?DoN?D?D1 D?D? N?NN?D°D?D?D2DoD? D?D° N€N?NNDoD?D? ,D2D2D?D'D?N?D?
[ru].
```

```
** Za instalaciju na srpskom, izaberi [sr].
```

```
** TA?rkA$e kurulum iA$in seA$in [tr].
```

```
(en/br/cn/de/el/es/fr/it/jp/nl/pl/ru/sr/tr) [en]: ?Enter?
```

```
OSSEC HIDS v2.5.1 Installation Script - http://www.ossec.net
```

You are about to start the installation process of the OSSEC HIDS.

You must have a C compiler pre-installed in your system.
 If you have any questions or comments, please send an e-mail
 to dcid@ossec.net (or daniel.cid@gmail.com).

- System: Linux debian 2.6.32-5-kirkwood
- User: root
- Host: debian

-- Press ENTER to continue or Ctrl-C to abort. -- **?Enter?**

?????????:

a.server:????????????????????Windows, Linux????????,????????????????????,????????.

b.agent:???a.server??,????????????server?????,??????????.

c.local:?????????,???server?????,?????????,??Asterisk/FreePBX????????????,???

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

- Server installation chosen.

2- Setting up the installation environment.

- Choose where to install the OSSEC HIDS [/var/ossec]: **?Enter?**

- Installation will be made at /var/ossec .

3- Configuring the OSSEC HIDS.

3.1- Do you want e-mail notification? (y/n) [y]: **?Enter?**

- What's your e-mail address? jackooo@gmail.com

- We found your SMTP server as: gmail-smtp-in.l.google.com.

- Do you want to use it? (y/n) [y]: **n**

- What's your SMTP server ip/host? **localhost**

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

- Running syscheck (integrity check daemon).

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

- Running rootcheck (rootkit detection).

3.4- 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]: **?Enter?**

- 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]: **?Enter?**

- firewall-drop enabled (local) for levels >= 6

- Default white list for the active response:

- 192.168.1.1

????????????????Ossec server????,??????IP??????,??????,??????????:

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

- IPs (space separated): **192.168.1.0/24**

3.5- Do you want to enable remote syslog (port 514 udp)? (y/n) [y]: **?Enter?**

- Remote syslog enabled.

3.6- Setting the configuration to analyze the following logs:

-- /var/log/messages

-- /var/log/auth.log

-- /var/log/syslog

-- /var/log/mail.info

-- /var/log/dpkg.log

-- /var/log/apache2/error.log (apache log)

-- /var/log/apache2/access.log (apache log)

- 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 --- **?Enter?**

????Ossec??.???...

??????????????:

- System is Debian (Ubuntu or derivative).
- Init script modified to start OSSEC HIDS during boot.

- Configuration finished properly.

- To start OSSEC HIDS:
 /var/ossec/bin/ossec-control start

- To stop OSSEC HIDS:
 /var/ossec/bin/ossec-control stop

- The configuration can be viewed or modified at /var/ossec/etc/ossec.conf

Thanks for using the OSSEC HIDS.

If you have any question, suggestion or if you find any bug,
 contact us at contact@ossec.net or using our public maillist at
ossec-list@ossec.net
 (<http://www.ossec.net/main/support/>).

More information can be found at <http://www.ossec.net>

--- Press ENTER to finish (maybe more information below). --- **?Enter?**

- In order to connect agent and server, you need to add each agent to the server.
 Run the 'manage_agents' to add or remove them:

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

More information at:

<http://www.ossec.net/en/manual.html#ma>

B??ossec.conf?Ossec Server??????????????????????????????:

Code:

```
nano -w /var/ossec/etc/ossec.conf
```

```
<ossec_config>
<global>
  <email_notification>yes</email_notification>
  <email_to>jackooo@gmail.com</email_to>
  <smtp_server>localhost</smtp_server>
  <email_from>ossecm@dyndns.org</email_from>
</global>
```

C?FreePBX??Ossec Server Web??:

1.?FreePBX??Ossec Server Web????,??**asterisk**????/etc/group ?ossec????:

Code:

```
sed -i '/ossec:/s|s|asterisk|' /etc/group
```

2.????????,????:

Code:

```
reboot
```

3.????????OSSEC module - **ossec-1.0.2.tgz** for FreePBX:

?http://www.fonicaprojects.com/wiki/index.php/FreePBX_Module:_OSSEC ???ossec-1.0.2.tgz??Windows?
?

??FreePBX-> Tools-> Module Admin-> Upload Module-> ??-> ??-> ossec-1.0.2.tgz

??Upload ???Module Administration-> Maintenance-> OSSEC-> Install

????,???Tools-> ??OSSEC ???**Ossec Server Web**?????:

The screenshot shows the FreePBX web interface with the OSSEC configuration page. The page includes a navigation menu on the left, a search bar, and a main content area with the following sections:

- Available agents:**
 - +ossec-server (127.0.0.1)
 - +PlugSamba (192.168.1.0) - Inactive
 - +WindowsXP_Jack (192.168.1.0)
 - +WindowsXP_Ethan (192.168.1.0) - Inactive
- Latest modified files:**
 - +etc/iptables.up.rules
 - +etc/network/interfaces
 - +etc/ampportal.conf
 - +etc/webmin/webmin/oscache
 - +etc/shadow
 - +etc/webmin/webmin/update-cache
 - +etc/webmin/webmin/config
 - +etc/webmin/package-updates/current.cache..
- Latest events:**
 - 2010 Nov 06 23:19:10 Rule Id: 5501 level: 3
Location: debian->/var/log/auth.log
Login session opened.
Nov 6 23:19:09 debian sshd[4198]: pam_unix(sshd:session): session opened for user root by (uid=0)
 - 2010 Nov 06 23:19:10 Rule Id: 5715 level: 3
Location: debian->/var/log/auth.log

D??IPTables,?????Windows, Linux,???????Ossec Server??????:

Code:

```
nano -w /etc/iptables.up.rules
```

```
# Allow connections from Ossec Agents to our Ossec Server
```

```
-A INPUT -p udp -m udp -s 192.168.1.0/24 --dport 1514 -j ACCEPT
```

E??logger.conf??message, full?syslog.local0??????:

Code:

```
nano -w /etc/asterisk/logger.conf
```

```
messages => notice,warning,error
```

```
full => notice,warning,error,debug,verbose
```

```
syslog.local0 => notice,warning,error
```

??????? reload:

```
asterisk -rx "logger reload"
```

F????:

Code:

/var/ossec/bin/ossec-control stop

/var/ossec/bin/ossec-control start

/var/ossec/bin/ossec-control restart

/var/ossec/bin/manage_agents

ps -ef | grep ossec

G????Asterisk???IP-192.168.1.21???Ossec????:

1.????????????Asterisk ?????Ossec????????????????????email ??:

Received From: debian->/var/log/messages

Rule: 6251 fired (level 10) -> "Multiple failed logins."

Portion of the log(s):

Nov 29 18:13:10 debian asterisk[818]: NOTICE[1067]: chan_sip.c:16396 in handle_request_register: Registration from "xlite"<sip:1000@192.168.1.55>' failed for '192.168.1.21' - Wrong password

Nov 29 18:13:00 debian asterisk[818]: NOTICE[1067]: chan_sip.c:16396 in handle_request_register: Registration from "xlite"<sip:1000@192.168.1.55>' failed for '192.168.1.21' - Wrong password

Nov 29 18:12:51 debian asterisk[818]: NOTICE[1067]: chan_sip.c:16396 in handle_request_register: Registration from "xlite"<sip:1000@192.168.1.55>' failed for '192.168.1.21' - Wrong password

Nov 29 18:12:43 debian asterisk[818]: NOTICE[1067]: chan_sip.c:16396 in handle_request_register: Registration from "xlite"<sip:1000@192.168.1.55>' failed for '192.168.1.21' - Wrong password

Nov 29 18:12:34 debian asterisk[818]: NOTICE[1067]: chan_sip.c:16396 in handle_request_register: Registration from "xlite"<sip:1000@192.168.1.55>' failed for '192.168.1.21' - Wrong password

Nov 29 18:12:26 debian asterisk[818]: NOTICE[1067]: chan_sip.c:16396 in handle_request_register: Registration from "xlite"<sip:1000@192.168.1.55>' failed for '192.168.1.21' - Wrong password

Nov 29 18:12:19 debian asterisk[818]: NOTICE[1067]: chan_sip.c:16396 in handle_request_register: Registration from "xlite"<sip:1000@192.168.1.55>' failed for '192.168.1.21' - Wrong password

2.????????????????Asterisk ?????Ossec????????????????????email ??:

Received From: debian->/var/log/messages

Rule: 6252 fired (level 10) -> "Extension enumeration."

Portion of the log(s):

Nov 29 14:57:09 debian asterisk[818]: NOTICE[1067]: chan_sip.c:16396 in handle_request_register: Registration from "xlite"<sip:700@192.168.1.55>' failed for '192.168.1.21' - No matching peer found

Nov 29 14:57:02 debian asterisk[818]: NOTICE[1067]: chan_sip.c:16396 in handle_request_register: Registration from "xlite"<sip:700@192.168.1.55>' failed for '192.168.1.21' - No matching peer found

Nov 29 14:56:56 debian asterisk[818]: NOTICE[1067]: chan_sip.c:16396 in handle_request_register: Registration from "'xlite"< sip:700@192.168.1.55>' failed for '192.168.1.21' - No matching peer found

Nov 29 14:56:50 debian asterisk[818]: NOTICE[1067]: chan_sip.c:16396 in handle_request_register: Registration from "'xlite"< sip:700@192.168.1.55>' failed for '192.168.1.21' - No matching peer found

Nov 29 14:56:44 debian asterisk[818]: NOTICE[1067]: chan_sip.c:16396 in handle_request_register: Registration from "'xlite"< sip:700@192.168.1.55>' failed for '192.168.1.21' - No matching peer found

Nov 29 14:56:37 debian asterisk[818]: NOTICE[1067]: chan_sip.c:16396 in handle_request_register: Registration from "'xlite"< sip:700@192.168.1.55>' failed for '192.168.1.21' - No matching peer found

Nov 29 14:56:31 debian asterisk[818]: NOTICE[1067]: chan_sip.c:16396 in handle_request_register: Registration from "'xlite"< sip:700@192.168.1.55>' failed for '192.168.1.21' - No matching peer found

3.?FreePBX??OSSEC???:

??????:

<http://www.ossec.net/main/manual/man...ation/#install>
http://www.fonicprojects.com/wiki/i..._Module:_OSSEC

http://www.netadmin.com.tw/article_c...?sn=0810030005

<http://www.fonicaprojects.com/wiki/i...caPABX-Install>