This pdf shows the installation of OSSEC program and location of the log files.

Welcome to the Home of OSSEC - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.ossec.net/

Google

Most Visited openSUSE Getting Started Latest Headlines Mozilla Firefox

Welcome to the Home of OSSEC

OSSEC TREND MICRO Securing Your Web World

Search

Home | About | Documentation | Downloads | Support | Our Team

Welcome to the Home of OSSEC

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

It runs on most operating systems, including Linux, MacOS, Solaris, HP-UX, AIX and Windows. A list with all supported platforms is available here.

About» | Learn More» | How it works»

PCI Learn how we can help with PCI!

RECENT ENTRIES

>Week of OSSEC - Update Oct 21

>Week of OSSEC (2W0O) - Oct 17-23 Oct 15

>OSSEC v2.5 released Sep 27

>SecureCloud beta - Invitation to the OSSEC community Aug 25

(Archives)

SHORTCUTS

>Getting Started

>First steps

>Manual | Wiki | Blog

>Commercial Support

NEWS/ANNOUNCEMENTS

>Join OSSEC Linked-in Group

>Join Mailing List

Done

OSSEC

TREND MICRO

Securing Your Web World

Search

Home | About | Documentation | Downloads | Support | Our Team

Downloads

Unix/Linux version 2.5.1

OSSEC for Linux, Solaris, *BSD, Mac, AIX and variants:

ossec-hids-2.5.1.tar.gz Sig - Checksum - License

Installation instructions here.

Windows agent version 2.5.1

OSSEC for Windows 2000,XP, 2003 and Vista:

ossec-agent-win32-2.5.1.exe Sig - Checksum - License

Version 2.5 Changelog - Release Notes

Web Interface

RECENT ENTRIES

>Week of OSSEC - Update Oct 21

>Week of OSSEC (2W0O) - Oct 17-23 Oct 15

>OSSEC v2.5 released Sep 27

>SecureCloud beta - Invitation to the OSSEC community Aug 25

(Archives)

SHORTCUTS

>Getting Started

>First steps

>Manual | Wiki | Blog

>Commercial Support

NEWS/ANNOUNCEMENTS

>Join OSSEC Linked-in Group

>Join Mailing List

linux-msctc - VMware Player File Virtual Machine Help

Downloads - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.ossec.net/main/downloads/

Google

Most Visited openSUSE Getting Started Latest Headlines Mozilla Firefox

Downloads

OSSEC

TREND

Home About Docu

Downloads

Unix/Linux version 2.5

OSSEC for Linux, Solaris, *E

ossec-hids-2.5.1.tar.gz Si

Installation instructions her

Windows agent versio

OSSEC for Windows 2000,XP, 2003 and Vista:

ossec-agent-win32-2.5.1.exe Sig - Checksum - License

Version 2.5 Changelog - Release Notes

Web Interface

>Manual | Wiki | Blog

>Commercial Support

NEWS/ANNOUNCEMENTS

>Join OSSEC Linked-in Group

>Join Mailing List

Opening ossec-hids-2.5.1.tar.gz

You have chosen to open

ossec-hids-2.5.1.tar.gz

which is a: Gzip archive

from: http://www.ossec.net

What should Firefox do with this file?

Open with Ark (default)

Save File

Do this automatically for files like this from now on.

OK Cancel

Done

Downloads - Mozilla Firefox

vmware

linux-msctc - VMware Player File Virtual Machine Help

Downloads - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.ossec.net/main/downloads/

Most Visited openSUSE Getting Started Latest Headlines

Downloads

OSSEC

TREND MICRO

Securing You

Home About Documentation Downloads Support Ou

Downloads

Unix/Linux version 2.5.1

OSSEC for Linux, Solaris, *BSD, Mac, AIX and variants:

ossec-hids-2.5.1.tar.gz Sig - Checksum - License

Installation instructions here.

Windows agent version 2.5.1

OSSEC for Windows 2000,XP, 2003 and Vista:

ossec-agent-win32-2.5.1.exe Sig - Checksum - License

Version 2.5 Changelog - Release Notes

Web Interface

>Week of OSSEC - Update Oct 21

>Week of OSSEC (2W00) - Oct 17-23 Oct 15

>OSSEC v2.5 released Sep 27

>SecureCloud beta - Invitation to the OSSEC community Aug 25

(Archives)

SHORTCUTS

>Getting Started

>First steps

>Manual | Wiki | Blog

>Commercial Support

NEWS/ANNOUNCEMENTS

>Join OSSEC Linked-in Group

>Join Mailing List

Downloads

ossec-hids-2.5.1(2).tar.gz 04:02 PM
723 KB — ossec.net

ebook-tools-0.2.1.tar.gz November 26
43.7 KB — sourceforge.net

cutecom-0.22.0.tar.gz November 26
22.7 KB — sourceforge.net

abiword-2.6.6-11.3.i586.rpm November 26
3.6 MB — pbone.net

iperf-2.0.5.tar.gz November 26
243 KB — sourceforge.net

Clear List Search...

Done

Downloads Downloads - Mozilla Firefox 04:02 pm

vmware

linux-msctc - VMware Player File Virtual Machine Help

preuss : bash

File Edit View Scrollback Bookmarks Settings Help

```
preuss@linux-msctc:~>
```

preuss : bash

preuss : bash

04:02 pm

vmware

linux-msctc - VMware Player File Virtual Machine Help

preuss : bash

File Edit View Scrollback Bookmarks Settings Help

```
preuss@linux-msctc:~> ls
archive.tgz   Documents     Music      preuss1.txt  tar_list.txt  test4.txt
bin           Downloads     new2.doc   preuss2.txt  Templates     testmd5.txt
cptr2224.txt  HOSTNAME.bak  new3.doc   Public       test1.txt     Videos
cptr2236.txt  md5test.txt   new.txt    public_html  test2.txt
Desktop       me.txt        Pictures   set.txt      test3.txt
preuss@linux-msctc:~>
```

preuss : bash

preuss : bash

04:02 pm

vmware

Downloads : bash

File Edit View Scrollback Bookmarks Settings Help

```
preuss@linux-msctc:~> ls
archive.tgz   Documents     Music      preuss1.txt  tar_list.txt  test4.txt
bin           Downloads     new2.doc   preuss2.txt  Templates     testmd5.txt
cptr2224.txt  HOSTNAME.bak  new3.doc   Public       test1.txt     Videos
cptr2236.txt  md5test.txt   new.txt    public_html  test2.txt
Desktop       me.txt        Pictures   set.txt      test3.txt
preuss@linux-msctc:~> cd Downloads/
preuss@linux-msctc:~/Downloads> ls
abiword-2.6.6-11.3.i586.rpm  ebook-tools-0.2.1.tar.gz  ossec-hids-2.5.1.tar.gz
cutecom-0.22.0.tar.gz        iperf-2.0.5.tar.gz        ossec-wui-0.3.tar.gz
preuss@linux-msctc:~/Downloads>
```

Downloads : bash

Downloads : bash

linux-msctc - VMware Player File Virtual Machine Help

Downloads : bash

File Edit View Scrollback Bookmarks Settings Help

```
preuss@linux-msctc:~> ls
archive.tgz   Documents     Music      preuss1.txt  tar_list.txt  test4.txt
bin           Downloads     new2.doc   preuss2.txt  Templates     testmd5.txt
cptr2224.txt  HOSTNAME.bak  new3.doc   Public       test1.txt     Videos
cptr2236.txt  md5test.txt   new.txt    public_html  test2.txt
Desktop       me.txt        Pictures   set.txt      test3.txt
preuss@linux-msctc:~> cd Downloads/
preuss@linux-msctc:~/Downloads> ls
abiword-2.6.6-11.3.i586.rpm  ebook-tools-0.2.1.tar.gz  ossec-hids-2.5.1.tar.gz
cutecom-0.22.0.tar.gz        iperf-2.0.5.tar.gz        ossec-wui-0.3.tar.gz
preuss@linux-msctc:~/Downloads> tar xzvf ossec-hids-2.5.1.tar.gz
```

Downloads : bash

Your version of OSSEC will be different than the one shown. You must use the name of the version you downloaded.

Downloads : bash

04:04 pm

vmware

Downloads : bash

File Edit View Scrollback Bookmarks Settings Help

```
ossec-hids-2.5.1/contrib/specs/server/preloaded-vars.conf
ossec-hids-2.5.1/contrib/specs/server/ossec-hids-server.spec
ossec-hids-2.5.1/contrib/specs/local/
ossec-hids-2.5.1/contrib/specs/local/preloaded-vars.conf
ossec-hids-2.5.1/contrib/specs/local/ossec-hids-local.spec
ossec-hids-2.5.1/contrib/specs/getattr.pl
ossec-hids-2.5.1/contrib/specs/remove_ossec
ossec-hids-2.5.1/contrib/specs/agent/
ossec-hids-2.5.1/contrib/specs/agent/preloaded-vars.conf
ossec-hids-2.5.1/contrib/specs/agent/ossec-hids-agent.spec
ossec-hids-2.5.1/contrib/ossec2mysql.pl
ossec-hids-2.5.1/contrib/ossectop.pl
ossec-hids-2.5.1/contrib/compile_alerts.pl
ossec-hids-2.5.1/contrib/ossec-batch-manager.pl
ossec-hids-2.5.1/contrib/ossec_report.txt
ossec-hids-2.5.1/contrib/ossec2mysql.sql
ossec-hids-2.5.1/contrib/ossecmysql.pm
ossec-hids-2.5.1/contrib/compile_alerts.txt
ossec-hids-2.5.1/contrib/ossec-testing/
ossec-hids-2.5.1/contrib/ossec-testing/runtests.py
ossec-hids-2.5.1/contrib/ossec-testing/tests/
ossec-hids-2.5.1/contrib/ossec-testing/tests/named.ini
ossec-hids-2.5.1/contrib/config2xml
ossec-hids-2.5.1/contrib/add_localfile.sh
preuss@linux-msctc:~/Downloads>
```

Downloads : bash

Downloads : bash

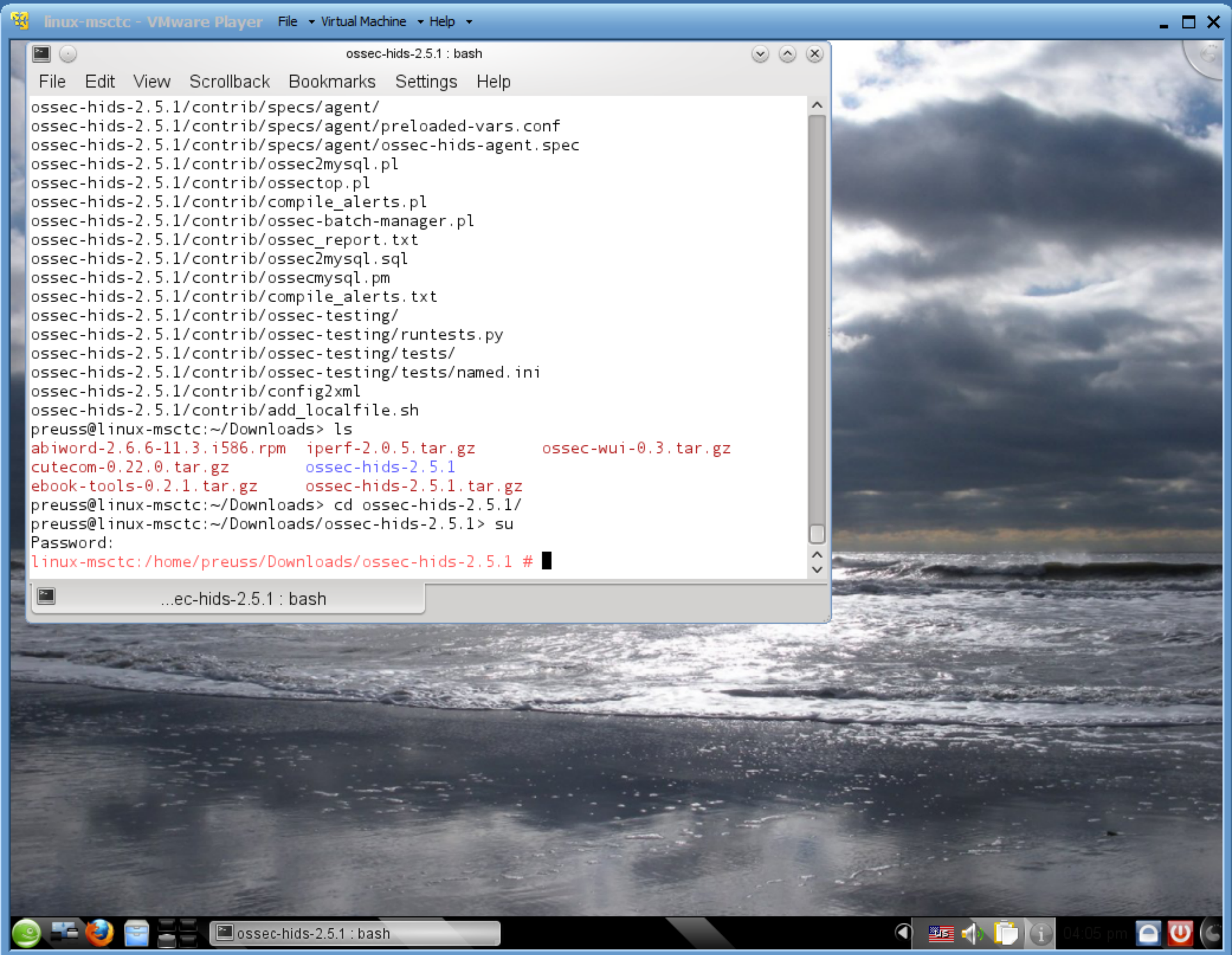
ossec-hids-2.5.1 : bash

File Edit View Scrollback Bookmarks Settings Help

```
ossec-hids-2.5.1/contrib/specs/getattr.pl
ossec-hids-2.5.1/contrib/specs/remove_ossec
ossec-hids-2.5.1/contrib/specs/agent/
ossec-hids-2.5.1/contrib/specs/agent/preloaded-vars.conf
ossec-hids-2.5.1/contrib/specs/agent/ossec-hids-agent.spec
ossec-hids-2.5.1/contrib/ossec2mysql.pl
ossec-hids-2.5.1/contrib/ossectop.pl
ossec-hids-2.5.1/contrib/compile_alerts.pl
ossec-hids-2.5.1/contrib/ossec-batch-manager.pl
ossec-hids-2.5.1/contrib/ossec_report.txt
ossec-hids-2.5.1/contrib/ossec2mysql.sql
ossec-hids-2.5.1/contrib/ossecmysql.pm
ossec-hids-2.5.1/contrib/compile_alerts.txt
ossec-hids-2.5.1/contrib/ossec-testing/
ossec-hids-2.5.1/contrib/ossec-testing/runtests.py
ossec-hids-2.5.1/contrib/ossec-testing/tests/
ossec-hids-2.5.1/contrib/ossec-testing/tests/named.ini
ossec-hids-2.5.1/contrib/config2xml
ossec-hids-2.5.1/contrib/add_localfile.sh
preuss@linux-msctc:~/Downloads> ls
abiword-2.6.6-11.3.i586.rpm  iperf-2.0.5.tar.gz       ossec-wui-0.3.tar.gz
cutecom-0.22.0.tar.gz        ossec-hids-2.5.1
ebook-tools-0.2.1.tar.gz     ossec-hids-2.5.1.tar.gz
preuss@linux-msctc:~/Downloads> cd ossec-hids-2.5.1/
preuss@linux-msctc:~/Downloads/ossec-hids-2.5.1>
```

...ec-hids-2.5.1 : bash

ossec-hids-2.5.1 : bash


linux-msctc - VMware Player
File
Virtual Machine
Help
ossec-hids-2.5.1 : bash
File Edit View Scrollback Bookmarks Settings Help
ossec-hids-2.5.1/contrib/specs/agent/
ossec-hids-2.5.1/contrib/specs/agent/preloaded-vars.conf
ossec-hids-2.5.1/contrib/specs/agent/ossec-hids-agent.spec
ossec-hids-2.5.1/contrib/ossec2mysql.pl
ossec-hids-2.5.1/contrib/ossectop.pl
ossec-hids-2.5.1/contrib/compile_alerts.pl
ossec-hids-2.5.1/contrib/ossec-batch-manager.pl
ossec-hids-2.5.1/contrib/ossec_report.txt
ossec-hids-2.5.1/contrib/ossec2mysql.sql
ossec-hids-2.5.1/contrib/ossecmysql.pm
ossec-hids-2.5.1/contrib/compile_alerts.txt
ossec-hids-2.5.1/contrib/ossec-testing/
ossec-hids-2.5.1/contrib/ossec-testing/runtests.py
ossec-hids-2.5.1/contrib/ossec-testing/tests/
ossec-hids-2.5.1/contrib/ossec-testing/tests/named.ini
ossec-hids-2.5.1/contrib/config2xml
ossec-hids-2.5.1/contrib/add_localfile.sh
preuss@linux-msctc:~/Downloads> ls
abiword-2.6.6-11.3.i586.rpm iperf-2.0.5.tar.gz ossec-wui-0.3.tar.gz
cutecom-0.22.0.tar.gz ossec-hids-2.5.1
ebook-tools-0.2.1.tar.gz ossec-hids-2.5.1.tar.gz
preuss@linux-msctc:~/Downloads> cd ossec-hids-2.5.1/
preuss@linux-msctc:~/Downloads/ossec-hids-2.5.1> su
Password:
linux-msctc:/home/preuss/Downloads/ossec-hids-2.5.1 #
...ec-hids-2.5.1 : bash
ossec-hids-2.5.1 : bash
04:05 pm
vmware

ossec-hids-2.5.1 : bash

File Edit View Scrollback Bookmarks Settings Help

```
ossec-hids-2.5.1/contrib/ossectop.pl
ossec-hids-2.5.1/contrib/compile_alerts.pl
ossec-hids-2.5.1/contrib/ossec-batch-manager.pl
ossec-hids-2.5.1/contrib/ossec_report.txt
ossec-hids-2.5.1/contrib/ossec2mysql.sql
ossec-hids-2.5.1/contrib/ossecmysql.pm
ossec-hids-2.5.1/contrib/compile_alerts.txt
ossec-hids-2.5.1/contrib/ossec-testing/
ossec-hids-2.5.1/contrib/ossec-testing/runtests.py
ossec-hids-2.5.1/contrib/ossec-testing/tests/
ossec-hids-2.5.1/contrib/ossec-testing/tests/named.ini
ossec-hids-2.5.1/contrib/config2xml
ossec-hids-2.5.1/contrib/add_localfile.sh
preuss@linux-msctc:~/Downloads> ls
abiword-2.6.6-11.3.i586.rpm  iperf-2.0.5.tar.gz       ossec-wui-0.3.tar.gz
cutecom-0.22.0.tar.gz        ossec-hids-2.5.1
ebook-tools-0.2.1.tar.gz     ossec-hids-2.5.1.tar.gz
preuss@linux-msctc:~/Downloads> cd ossec-hids-2.5.1/
preuss@linux-msctc:~/Downloads/ossec-hids-2.5.1> su
Password:
linux-msctc:/home/preuss/Downloads/ossec-hids-2.5.1 # ls
active-response  contrib       etc                .hgtags     LICENSE
BUGS             CONTRIBUTORS  .hg_archival.txt   INSTALL     README
CONFIG           doc           .hgignore          install.sh  src
linux-msctc:/home/preuss/Downloads/ossec-hids-2.5.1 #
```

...ec-hids-2.5.1 : bash

ossec-hids-2.5.1 : bash

ossec-hids-2.5.1 : bash

File Edit View Scrollback Bookmarks Settings Help

```
ossec-hids-2.5.1/contrib/ossectop.pl
ossec-hids-2.5.1/contrib/compile_alerts.pl
ossec-hids-2.5.1/contrib/ossec-batch-manager.pl
ossec-hids-2.5.1/contrib/ossec_report.txt
ossec-hids-2.5.1/contrib/ossec2mysql.sql
ossec-hids-2.5.1/contrib/ossecmysql.pm
ossec-hids-2.5.1/contrib/compile_alerts.txt
ossec-hids-2.5.1/contrib/ossec-testing/
ossec-hids-2.5.1/contrib/ossec-testing/runtests.py
ossec-hids-2.5.1/contrib/ossec-testing/tests/
ossec-hids-2.5.1/contrib/ossec-testing/tests/named.ini
ossec-hids-2.5.1/contrib/config2xml
ossec-hids-2.5.1/contrib/add_localfile.sh
preuss@linux-msctc:~/Downloads> ls
abiword-2.6.6-11.3.i586.rpm  iperf-2.0.5.tar.gz       ossec-wui-0.3.tar.gz
cutecom-0.22.0.tar.gz        ossec-hids-2.5.1
ebook-tools-0.2.1.tar.gz     ossec-hids-2.5.1.tar.gz
preuss@linux-msctc:~/Downloads> cd ossec-hids-2.5.1/
preuss@linux-msctc:~/Downloads/ossec-hids-2.5.1> su
Password:
linux-msctc:/home/preuss/Downloads/ossec-hids-2.5.1 # ls
active-response  contrib       etc                .hgtags     LICENSE
BUGS             CONTRIBUTORS  .hg_archival.txt   INSTALL     README
CONFIG           doc           .hgignore          install.sh  src
linux-msctc:/home/preuss/Downloads/ossec-hids-2.5.1 # ./install.sh
```

...ec-hids-2.5.1 : bash

ossec-hids-2.5.1 : bash

04:05 pm

vmware

ossec-hids-2.5.1 : install.sh

File Edit View Scrollback Bookmarks Settings Help

```
ebook-tools-0.2.1.tar.gz     ossec-hids-2.5.1.tar.gz
preuss@linux-msctc:~/Downloads> cd ossec-hids-2.5.1/
preuss@linux-msctc:~/Downloads/ossec-hids-2.5.1> su
Password:
linux-msctc:/home/preuss/Downloads/ossec-hids-2.5.1 # ls
active-response  contrib       etc               .hgtags     LICENSE
BUGS             CONTRIBUTORS  .hg_archival.txt  INSTALL     README
CONFIG           doc           .hgignore         install.sh  src
linux-msctc:/home/preuss/Downloads/ossec-hids-2.5.1 # ./install.sh

  ** Para instalação em português, escolha [br].
  ** 要使用中文进行安装，请选择 [cn].
  ** Fur eine deutsche Installation wohlen Sie [de].
  ** Για εγκατάσταση στα Ελληνικά, επιλέξτε [el].
  ** For installation in English, choose [en].
  ** Para instalar en Español , eliga [es].
  ** Pour une installation en français, choisissez [fr]
  ** Per l'installazione in Italiano, scegli [it].
  ** 日本語でインストールします．選択して下さい．[jp].
  ** Voor installatie in het Nederlands, kies [nl].
  ** Aby instalować w języku Polskim, wybierz [pl].
  ** Для инструкций по установке на русском ,введите [ru].
  ** Za instalaciju na srpskom, izaberi [sr].
  ** Türkçe kurulum için seçin [tr].
  (en/br/cn/de/el/es/fr/it/jp/nl/pl/ru/sr/tr) [en]:
```

...s-2.5.1 : install.sh

ossec-hids-2.5.1 : install.sh

04:05 pm

ossec-hids-2.5.1 : install.sh

File Edit View Scrollback Bookmarks Settings Help

```
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 linux-msctc 2.6.34.7-0.7-desktop
 - User: root
 - Host: linux-msctc


 -- Press ENTER to continue or Ctrl-C to abort. --
```

...s-2.5.1 : install.sh

ossec-hids-2.5.1 : install.sh

04:05 pm

vmware

ossec-hids-2.5.1 : install.sh

File Edit View Scrollback Bookmarks Settings Help

```
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 linux-msctc 2.6.34.7-0.7-desktop
 - User: root
 - Host: linux-msctc


 -- Press ENTER to continue or Ctrl-C to abort. --


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

...s-2.5.1 : install.sh

ossec-hids-2.5.1 : install.sh

File Edit View Scrollback Bookmarks Settings Help

```
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 linux-msctc 2.6.34.7-0.7-desktop
 - User: root
 - Host: linux-msctc


 -- Press ENTER to continue or Ctrl-C to abort. --


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

 - Local installation chosen.

2- Setting up the installation environment.

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

...s-2.5.1 : install.sh

ossec-hids-2.5.1 : install.sh

File Edit View Scrollback Bookmarks Settings Help

```
 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 linux-msctc 2.6.34.7-0.7-desktop
  - User: root
  - Host: linux-msctc


  -- Press ENTER to continue or Ctrl-C to abort. --


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

  - Local installation chosen.

2- Setting up the installation environment.

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

    - Installation will be made at  /var/ossec .

3- Configuring the OSSEC HIDS.

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

...s-2.5.1 : install.sh

ossec-hids-2.5.1 : install.sh

ossec-hids-2.5.1 : install.sh

File Edit View Scrollback Bookmarks Settings Help

```
 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 linux-msctc 2.6.34.7-0.7-desktop
  - User: root
  - Host: linux-msctc


  -- Press ENTER to continue or Ctrl-C to abort. --


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

  - Local installation chosen.

2- Setting up the installation environment.

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

    - Installation will be made at  /var/ossec .

3- Configuring the OSSEC HIDS.

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

...s-2.5.1 : install.sh

ossec-hids-2.5.1 : install.sh

ossec-hids-2.5.1 : install.sh

File Edit View Scrollback Bookmarks Settings Help

```
  - System: Linux linux-msctc 2.6.34.7-0.7-desktop
  - User: root
  - Host: linux-msctc


  -- Press ENTER to continue or Ctrl-C to abort. --


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

  - Local installation chosen.

2- Setting up the installation environment.

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

    - Installation will be made at  /var/ossec .

3- Configuring the OSSEC HIDS.

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

   --- Email notification disabled.

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

...s-2.5.1 : install.sh

ossec-hids-2.5.1 : install.sh

ossec-hids-2.5.1 : install.sh

File Edit View Scrollback Bookmarks Settings Help

```
  -- Press ENTER to continue or Ctrl-C to abort. --

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

  - Local installation chosen.

2- Setting up the installation environment.

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

    - Installation will be made at  /var/ossec .

3- Configuring the OSSEC HIDS.

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

   --- Email notification disabled.

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

   - Running syscheck (integrity check daemon).

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

...s-2.5.1 : install.sh

ossec-hids-2.5.1 : install.sh

ossec-hids-2.5.1 : install.sh

File Edit View Scrollback Bookmarks Settings Help

```
   - Installation will be made at  /var/ossec .

3- Configuring the OSSEC HIDS.

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

   --- Email notification disabled.

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

   - Running syscheck (integrity check daemon).

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

   - 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]:
```

...s-2.5.1 : install.sh

ossec-hids-2.5.1 : install.sh

ossec-hids-2.5.1 : install.sh

File Edit View Scrollback Bookmarks Settings Help

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

  - 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]:

    - 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]:
```

...s-2.5.1 : install.sh

ossec-hids-2.5.1 : install.sh

ossec-hids-2.5.1 : install.sh

File Edit View Scrollback Bookmarks Settings Help

```
     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:
     - 192.168.5.1

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

...s-2.5.1 : install.sh

ossec-hids-2.5.1 : install.sh

ossec-hids-2.5.1 : install.sh

File Edit View Scrollback Bookmarks Settings Help

```
    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:
     - 192.168.5.1

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

 3.6- Setting the configuration to analyze the following logs:
    -- /var/log/messages
    -- /var/log/mail.info

- 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 ---
```

...s-2.5.1 : install.sh

ossec-hids-2.5.1 : install.sh

ossec-hids-2.5.1 : install.sh

File Edit View Scrollback Bookmarks Settings Help

```
make[1]: Entering directory `/home/preuss/Downloads/ossec-hids-2.5.1/src/external
/zlib-1.2.3'
gcc -c -g -Wall -I../../ -I../../headers  -DDEFAULTDIR=\"/var/ossec\" -DLOCAL -DU
SE_OPENSSL -DUSEINOTIFY    -DARGV0=\"zlib\" -DXML_VAR=\"var\" -DOSSECHIDS *.c
ar cru libz.a *.o
ranlib libz.a
make[1]: Leaving directory `/home/preuss/Downloads/ossec-hids-2.5.1/src/external/
zlib-1.2.3'
make[1]: Entering directory `/home/preuss/Downloads/ossec-hids-2.5.1/src/external
/zlib-1.2.3'
cp -pr zlib.h zconf.h ../../headers/
cp -pr libz.a ../
make[1]: Leaving directory `/home/preuss/Downloads/ossec-hids-2.5.1/src/external/
zlib-1.2.3'



 *** Making os_xml ***

make[1]: Entering directory `/home/preuss/Downloads/ossec-hids-2.5.1/src/os_xml'
gcc -DXML_VAR=\"var\" -g -Wall -I../ -I../headers  -DDEFAULTDIR=\"/var/ossec\" -D
LOCAL -DUSE_OPENSSL -DUSEINOTIFY    -DARGV0=\"os_xml\" -DXML_VAR=\"var\" -DOSSECH
IDS -c os_xml.c os_xml_access.c os_xml_node_access.c os_xml_variables.c os_xml_wr
iter.c
```

...s-2.5.1 : install.sh

ossec-hids-2.5.1 : install.sh

04:06 pm

vmware

ossec-hids-2.5.1 : install.sh

File Edit View Scrollback Bookmarks Settings Help

```
- System is Suse Linux.
- 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). ---
```

...s-2.5.1 : install.sh

ossec-hids-2.5.1 : install.sh

ossec-hids-2.5.1 : bash

File Edit View Scrollback Bookmarks Settings Help

```
- 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). ---


linux-msctc:/home/preuss/Downloads/ossec-hids-2.5.1 #
```

...ec-hids-2.5.1 : bash

ossec-hids-2.5.1 : bash

ossec-hids-2.5.1 : bash

File Edit View Scrollback Bookmarks Settings Help

```
- 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). ---


linux-msctc:/home/preuss/Downloads/ossec-hids-2.5.1 # cd /var/ossec/log
bash: cd: /var/ossec/log: No such file or directory
linux-msctc:/home/preuss/Downloads/ossec-hids-2.5.1 # cd /var/ossec/logs/
linux-msctc:/var/ossec/logs #
```

...ec-hids-2.5.1 : bash

ossec-hids-2.5.1 : bash

04:07 pm

vmware

ossec-hids-2.5.1 : bash

File Edit View Scrollback Bookmarks Settings Help

```
                /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). ---


linux-msctc:/home/preuss/Downloads/ossec-hids-2.5.1 # cd /var/ossec/log
bash: cd: /var/ossec/log: No such file or directory
linux-msctc:/home/preuss/Downloads/ossec-hids-2.5.1 # cd /var/ossec/logs/
linux-msctc:/var/ossec/logs # ls
alerts  archives  firewall  ossec.log
linux-msctc:/var/ossec/logs # less ossec.log
```

...ec-hids-2.5.1 : bash

As your system is running, more log files will appear at this location.

ossec-hids-2.5.1 : bash

04:08 pm

vmware