Fall2019 Cent OS 7 OSSEC local Installation and Operation

The presentation installs OSSEC HIDS 3.3.0 in local mode. The presentation installs open-vm-tools and finger command.

Preuss
12/5/2019

Cent OS 7 Settings on both systems

40 GB disk
8 GB RAM
2 Processors
NAT Network Settings

Software Install: Server with GUI (no additional software)
Automatic partitioning
No security policy chosen

Post-Installation
Install open-vm-tools
Install updates

Resource:
ossec.org

ossec01 - VMware Workstation 15 Player (Non-commercial use only)

Player

Applications Places Fri 12:15

Home

Trash

The presentation logs into Cent OS 7.

7
CENTOS

ossec01 - VMware Workstation 15 Player (Non-commercial use only)

Player

Applications Places Terminal Fri 12:15

preuss@ossec01:/home/preuss

File Edit View Search Terminal Help

```
[preuss@ossec01 ~]$ su
Password:
[root@ossec01 preuss]#
```

Home

Trash

The presentation becomes root as shown.

preuss@ossec01:/home/preuss

1 / 4

Home

Trash

preuss@ossec01:/home/preuss

File Edit View Search Terminal Help

```
[root@ossec01 preuss]# ping -c 3 sweden.minnesota.edu
PING sweden.minnesota.edu (134.29.228.100) 56(84) bytes of data.
64 bytes from 134.29.228.100 (134.29.228.100): icmp_seq=1 ttl=128 time=3.28 ms
64 bytes from 134.29.228.100 (134.29.228.100): icmp_seq=2 ttl=128 time=0.800 ms
64 bytes from 134.29.228.100 (134.29.228.100): icmp_seq=3 ttl=128 time=0.833 ms

--- sweden.minnesota.edu ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2006ms
rtt min/avg/max/mdev = 0.800/1.640/3.289/1.166 ms
[root@ossec01 preuss]#
```

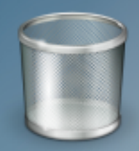
Your text will come here...

preuss@ossec01:/home/preuss

File Edit View Search Terminal Help

```
[root@ossec01 preuss]# yum install open-vm-tools
```

The presentation installs open-vm-tools as shown.

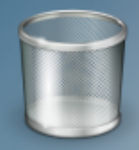


preuss@ossec01:/home/preuss

File Edit View Search Terminal Help

```
 open-vm-tools                  x86_64          10.3.0-2.el7              base          671 k
Updating for dependencies:
 open-vm-tools-desktop          x86_64          10.3.0-2.el7              base          169 k

Transaction Summary
================================================================================
Upgrade  1 Package (+1 Dependent package)

Total size: 840 k
Is this ok [y/d/N]: y
Downloading packages:
warning: /var/cache/yum/x86_64/7/base/packages/open-vm-tools-10.3.0-2.el7.x86_64.rpm: Header V3 RSA/SHA256 Signature, key ID f4a8
0eb5: NOKEY
Retrieving key from file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7
Importing GPG key 0xF4A80EB5:
 Userid     : "CentOS-7 Key (CentOS 7 Official Signing Key) <security@centos.org>"
 Fingerprint: 6341 ab27 53d7 8a78 a7c2 7bb1 24c6 a8a7 f4a8 0eb5
 Package    : centos-release-7-6.1810.2.el7.centos.x86_64 (@anaconda)
 From       : /etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7
Is this ok [y/N]: y
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Updating   : open-vm-tools-10.3.0-2.el7.x86_64                           1/4
  Updating   : open-vm-tools-desktop-10.3.0-2.el7.x86_64                   2/4
  Cleanup    : open-vm-tools-desktop-10.2.5-3.el7.x86_64                   3/4
  Cleanup    : open-vm-tools-10.2.5-3.el7.x86_64                           4/4
  Verifying  : open-vm-tools-10.3.0-2.el7.x86_64                           1/4
  Verifying  : open-vm-tools-desktop-10.3.0-2.el7.x86_64                   2/4
  Verifying  : open-vm-tools-10.2.5-3.el7.x86_64                           3/4
  Verifying  : open-vm-tools-desktop-10.2.5-3.el7.x86_64                   4/4

Updated:
  open-vm-tools.x86_64 0:10.3.0-2.el7

Dependency Updated:
  open-vm-tools-desktop.x86_64 0:10.3.0-2.el7

Complete!
[root@ossec01 preuss]# reboot
```

The presentation completes installing open-vm-tools as shown. The presentation reboots the system.



preuss@ossec01:/home/preuss

File Edit View Search Terminal Help

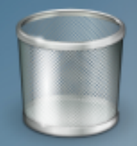
```
[preuss@ossec01 ~]$ su
Password:
[root@ossec01 preuss]# yum update
```

The presentation update CentOS 7 as shown.

```
  tigervnc-server-minimal.x86_64 0:1.8.0-17.el7
  tuned.noarch 0:2.11.0-5.el7_7.1
  tzdata.noarch 0:2019c-1.el7
  tzdata-java.noarch 0:2019c-1.el7
  udisks2.x86_64 0:2.7.3-9.el7
  unzip.x86_64 0:6.0-20.el7
  usermode.x86_64 0:1.111-6.el7
  util-linux.x86_64 0:2.23.2-61.el7
  vdo.x86_64 0:6.1.2.41-4.el7
  vim-common.x86_64 2:7.4.629-6.el7
  vim-enhanced.x86_64 2:7.4.629-6.el7
  vim-filesystem.x86_64 2:7.4.629-6.el7
  vim-minimal.x86_64 2:7.4.629-6.el7
  vinagre.x86_64 0:3.22.0-12.el7
  volume_key-libs.x86_64 0:0.3.9-9.el7
  webkitgtk4.x86_64 0:2.22.7-2.el7
  webkitgtk4-jsc.x86_64 0:2.22.7-2.el7
  webkitgtk4-plugin-process-gtk2.x86_64 0:2.22.7-2.el7
  wget.x86_64 0:1.14-18.el7_6.1
  xfsprogs.x86_64 0:4.5.0-20.el7
  xorg-x11-drv-ati.x86_64 0:19.0.1-2.el7
  xorg-x11-drv-qxl.x86_64 0:0.1.5-5.el7
  xorg-x11-drv-vesa.x86_64 0:2.4.0-3.el7
  xorg-x11-drv-wacom.x86_64 0:0.36.1-3.el7
  xorg-x11-server-Xorg.x86_64 0:1.20.4-7.el7
  xorg-x11-server-common.x86_64 0:1.20.4-7.el7
  yum.noarch 0:3.4.3-163.el7.centos
  yum-plugin-fastestmirror.noarch 0:1.1.31-52.el7
  yum-utils.noarch 0:1.1.31-52.el7

Replaced:
  urw-fonts.noarch 0:2.4-16.el7

Complete!
[root@ossec01 preuss]# reboot
```

The presentation finishes the update. The presentation reboots the system.

The kernel was updated.



preuss@ossec01:/home/preuss

File Edit View Search Terminal Help

```
[root@ossec01 preuss]# yum group install "Development Tools"
```

The presentation installs the required development tools to install OSSEC.

preuss@ossec01:/home/preuss

File Edit View Search Terminal Help

```
  Verifying  : autoconf-2.69-11.el7.noarch                                  41/51
  Verifying  : libstdc++-devel-4.8.5-39.el7.x86_64                          42/51
  Verifying  : perl-TermReadKey-2.30-20.el7.x86_64                          43/51
  Verifying  : libquadmath-4.8.5-39.el7.x86_64                              44/51
  Verifying  : dwz-0.11-3.el7.x86_64                                        45/51
  Verifying  : diffstat-1.57-4.el7.x86_64                                   46/51
  Verifying  : cpp-4.8.5-39.el7.x86_64                                      47/51
  Verifying  : redhat-rpm-config-9.1.0-88.el7.centos.noarch                 48/51
  Verifying  : perl-Test-Harness-3.28-3.el7.noarch                          49/51
  Verifying  : glibc-headers-2.17-292.el7.x86_64                            50/51
  Verifying  : rpm-sign-4.11.3-40.el7.x86_64                                51/51

Installed:
  autoconf.noarch 0:2.69-11.el7       automake.noarch 0:1.13.4-3.el7        bison.x86_64 0:3.0.4-2.el7
  byacc.x86_64 0:1.9.20130304-3.el7   cscope.x86_64 0:15.8-10.el7           ctags.x86_64 0:5.8-13.el7
  diffstat.x86_64 0:1.57-4.el7        doxygen.x86_64 1:1.8.5-3.el7          flex.x86_64 0:2.5.37-6.el7
  gcc.x86_64 0:4.8.5-39.el7           gcc-c++.x86_64 0:4.8.5-39.el7         gcc-gfortran.x86_64 0:4.8.5-39.el7
  git.x86_64 0:1.8.3.1-20.el7         indent.x86_64 0:2.2.11-13.el7         intltool.noarch 0:0.50.2-7.el7
  libtool.x86_64 0:2.4.2-22.el7_3     patch.x86_64 0:2.7.1-12.el7_7         patchutils.x86_64 0:0.3.3-4.el7
  rcs.x86_64 0:5.9.0-5.el7            redhat-rpm-config.noarch 0:9.1.0-88.el7.centos  rpm-build.x86_64 0:4.11.3-40.el7
  rpm-sign.x86_64 0:4.11.3-40.el7     subversion.x86_64 0:1.7.14-14.el7
  systemtap.x86_64 0:4.0-10.el7_7

Dependency Installed:
  apr.x86_64 0:1.4.8-5.el7                                  apr-u
  cpp.x86_64 0:4.8.5-39.el7                                 dwz.x
  gettext-common-devel.noarch 0:0.19.8.1-2.el7              gette
  glibc-devel.x86_64 0:2.17-292.el7                         glibc
  kernel-debug-devel.x86_64 0:3.10.0-1062.4.3.el7           kerne
  libgfortran.x86_64 0:4.8.5-39.el7                         libqu
  libquadmath-devel.x86_64 0:4.8.5-39.el7                   libst
  m4.x86_64 0:1.4.16-10.el7                                 perl-
  perl-Git.noarch 0:1.8.3.1-20.el7                          perl-
  perl-Test-Harness.noarch 0:3.28-3.el7                     perl-
  perl-XML-Parser.x86_64 0:2.41-10.el7                      perl-
  python-srpm-macros.noarch 0:3-32.el7                      subve
  systemtap-client.x86_64 0:4.0-10.el7_7                    systemtap-devel.x86_64 0:4.0-10.el7_7

Complete!
[root@ossec01 preuss]#
```

The presentation agrees to install all the requested options.

ossec01 - VMware Workstation 15 Player (Non-commercial use only)

Player

Applications Places Terminal Fri 12:35

preuss@ossec01:/home/preuss

File Edit View Search Terminal Help

```
[root@ossec01 preuss]# yum install zlib-devel
```

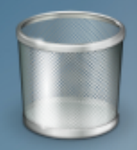
Home

Trash

The presentation installs the OSSEC required library zlib as shown.

preuss@ossec01:/home/preuss

1 / 4

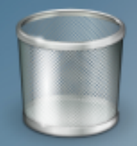


preuss@ossec01:/home/preuss

File Edit View Search Terminal Help

```
[root@ossec01 preuss]# yum install zlib-devel
Loaded plugins: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
 * base: repo1.dal.innoscale.net
 * extras: mirror.us-midwest-1.nexcess.net
 * updates: mirrors.usinternet.com
Resolving Dependencies
--> Running transaction check
---> Package zlib-devel.x86_64 0:1.2.7-18.el7 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================
 Package                 Arch                 Version                 Repository                 Size
================================================================================
Installing:
 zlib-devel              x86_64               1.2.7-18.el7            base                       50 k

Transaction Summary
================================================================================
Install  1 Package

Total download size: 50 k
Installed size: 132 k
Is this ok [y/d/N]: y
Downloading packages:
zlib-devel-1.2.7-18.el7.x86_64.rpm                                |  50 kB  00:00:00
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : zlib-devel-1.2.7-18.el7.x86_64                                  1/1
  Verifying  : zlib-devel-1.2.7-18.el7.x86_64                                  1/1

Installed:
  zlib-devel.x86_64 0:1.2.7-18.el7

Complete!
[root@ossec01 preuss]#
```

The presentation completes the zlib installation.

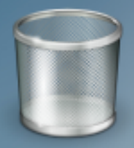


preuss@ossec01:/home/preuss/ossec/ossec-hids-3.3.0

File Edit View Search Terminal Help

```
[root@ossec01 ossec-hids-3.3.0]# yum install pcre2
```

The presentation installs the OSSEC required library pcre2.



preuss@ossec01:/home/preuss/ossec/ossec-hids-3.3.0

File Edit View Search Terminal Help

```
Dependencies Resolved

================================================================================
 Package                Arch              Version                 Repository  Size
================================================================================
Installing:
 pcre2-devel            x86_64            10.23-2.el7             base       545 k
Installing for dependencies:
 pcre2-utf32            x86_64            10.23-2.el7             base       181 k

Transaction Summary
================================================================================
Install  1 Package (+1 Dependent package)

Total download size: 726 k
Installed size: 2.2 M
Is this ok [y/d/N]: y
Downloading packages:
(1/2): pcre2-utf32-10.23-2.el7.x86_64.rpm                  | 181 kB  00:00:00
(2/2): pcre2-devel-10.23-2.el7.x86_64.rpm                  | 545 kB  00:00:00
--------------------------------------------------------------------------------
Total                                                       26 kB  00:00:00
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : pcre2-utf32-10.23-2.el7.x86_64                               1/2
  Installing : pcre2-devel-10.23-2.el7.x86_64                               2/2
  Verifying  : pcre2-devel-10.23-2.el7.x86_64                               1/2
  Verifying  : pcre2-utf32-10.23-2.el7.x86_64                               2/2

Installed:
  pcre2-devel.x86_64 0:10.23-2.el7

Dependency Installed:
  pcre2-utf32.x86_64 0:10.23-2.el7

Complete!
[root@ossec01 ossec-hids-3.3.0]#
```

The presentation completes the installation pcre2 libraries.

ossec01 - VMware Workstation 15 Player (Non-commercial use only)

Player

Applications Places Terminal Fri 12:36

Home

Trash

preuss@ossec01:~

File Edit View Search Terminal Help

```
[root@ossec01 preuss]# exit
exit
[preuss@ossec01 ~]$
```

The presentation logs out of root as shown.

preuss@ossec01:~

Source Downloads

Downloads

Source Downlo

RHEL, CentOS, others

Ubuntu, and D

Yum/DNF Au Installation Redhat, Ama Fedora

Manual Yum on Centos, R Linux or Fed

APT Automated Installation on Ubuntu and Debian

Manual APT Installation on Ubuntu and Debian

The presentation downloads the current version of the "Server/Agent Unix" file.

Latest development snapshots

/ossec/ossec-hids/releases

micorp.com/channels/ossec-3-testing

/ossec/ossec-wui/releases

/ossec/ossec-docs

Latest Stable Release (3.3.0)		Checksum	Signature
Server/Agent Unix	ossec-hids-3.3.0.tar.gz – Release Notes		GPG Unix
Agent Windows	ossec-agent-win32-3.1.0.exe		GPG

ossec01 - VMware Workstation 15 Player (Non-commercial use only)

Player | Applications Places Terminal Fri 12:38

Home

Trash

preuss@ossec01:~/ossec

File Edit View Search Terminal Help

```
[preuss@ossec01 ~]$ mkdir ossec
[preuss@ossec01 ~]$ cd ossec/
[preuss@ossec01 ossec]$ pwd
/home/preuss/ossec
[preuss@ossec01 ossec]$ cp ~/Downloads/ossec-hids-3.3.0.tar.gz .
```

The presentation creates a new directory and copies the download to the new directory as shown.

[preuss@ossec01:~] preuss@ossec01:~/ossec 1 / 4

ossec01 - VMware Workstation 15 Player (Non-commercial use only)

Player | Applications Places Terminal Fri 12:39

Home

Trash

preuss@ossec01:~/ossec

File Edit View Search Terminal Help

```
[preuss@ossec01 ossec]$ tar xzvf ossec-hids-3.3.0.tar.gz
```

The presentation extracts and ungzip the file as shown.

[preuss@ossec01:~] preuss@ossec01:~/ossec 1 / 4

ossec01 - VMware Workstation 15 Player (Non-commercial use only)

Player

Applications Places Terminal Fri 12:39

Home

Trash

preuss@ossec01:~/ossec

File Edit View Search Terminal Help

```
[preuss@ossec01 ossec]$ cd ossec-hids-3.3.0/
```

The presentation changes directories as shown.

[preuss@ossec01:~]

preuss@ossec01:~/ossec

1 / 4

Home

Trash

preuss@ossec01:/home/preuss/ossec/ossec-hids-3.3.0

File Edit View Search Terminal Help

```
[preuss@ossec01 ossec-hids-3.3.0]$ ls
active-response  BUGS  CHANGELOG  CONFIG  contrib  CONTRIBUTORS  doc  etc  INSTALL  install.sh  LICENSE  README.md  src  SUPPORT.md
[preuss@ossec01 ossec-hids-3.3.0]$ su
Password:
[root@ossec01 ossec-hids-3.3.0]#
```

The presentation becomes root to install OSSEC.

preuss@ossec01:/home/preuss/ossec/ossec-hids-3.3.0

File Edit View Search Terminal Help

```
[preuss@ossec01 ossec-hids-3.3.0]$ ls
active-response  BUGS  CHANGELOG  CONFIG  contrib  CONTRIBUTORS  doc  etc  INSTALL  install.sh  LICENSE  README.md  src  SUPPORT.md
[preuss@ossec01 ossec-hids-3.3.0]$ su
Password:
[root@ossec01 ossec-hids-3.3.0]# PCRE2_SYSTEM=yes ./install.sh
```

The presentation starts the installation as shown.

ossec01 - VMware Workstation 15 Player (Non-commercial use only)

Player | Applications Places Terminal Fri 12:40

Home

Trash

preuss@ossec01:/home/preuss/ossec/ossec-hids-3.3.0

File Edit View Search Terminal Help

```
[preuss@ossec01 ossec-hids-3.3.0]$ ls
active-response  BUGS  CHANGELOG  CONFIG  contrib  CONTRIBUTORS  doc  etc  INSTALL  install.sh  LICENSE  README.md  src  SUPPORT.md
[preuss@ossec01 ossec-hids-3.3.0]$ su
Password:
[root@ossec01 ossec-hids-3.3.0]# PCRE2_SYSTEM=yes ./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]
  ** A Magyar nyelvű telepítéshez válassza [hu].
  ** 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/hu/it/jp/nl/pl/ru/sr/tr) [en]:
```

The presentation selects English as the installation language.

[preuss@ossec01:~] preuss@ossec01:/home/preuss/oss... 1 / 4

ossec01 - VMware Workstation 15 Player (Non-commercial use only)

Player | Applications Places Terminal Fri 12:41

Home

Trash

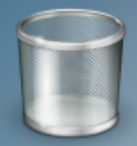
preuss@ossec01:/home/preuss/ossec/ossec-hids-3.3.0

File Edit View Search Terminal Help

```
OSSEC HIDS v3.3.0 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.

 - System: Linux ossec01.mait.minnesota.edu 3.10.0-1062.4.3.el7.x86_64
 - User: root
 - Host: ossec01.mait.minnesota.edu


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

The presentation presses "Enter" to continue.

[preuss@ossec01:~] preuss@ossec01:/home/preuss/oss... 1 / 4



preuss@ossec01:/home/preuss/ossec/ossec-hids-3.3.0

File Edit View Search Terminal Help

```
OSSEC HIDS v3.3.0 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.

 - System: Linux ossec01.mait.minnesota.edu 3.10.0-1062.4.3.el7.x86_64
 - User: root
 - Host: ossec01.mait.minnesota.edu


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


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

The presentation selects "local" installation.

Home

Trash

preuss@ossec01:/home/preuss/ossec/ossec-hids-3.3.0

File Edit View Search Terminal Help

```
OSSEC HIDS v3.3.0 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.

 - System: Linux ossec01.mait.minnesota.edu 3.10.0-1062.4.3.el7.x86_64
 - User: root
 - Host: ossec01.mait.minnesota.edu


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


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

 - Local installation chosen.

2- Setting up the installation environment.

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

The presentation presses "Enter" to install OSSEC into "/var/ossec".

preuss@ossec01:/home/preuss/ossec/ossec-hids-3.3.0

File Edit View Search Terminal Help

```
OSSEC HIDS v3.3.0 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.

 - System: Linux ossec01.mait.minnesota.edu 3.10.0-1062.4.3.el7.x86_64
 - User: root
 - Host: ossec01.mait.minnesota.edu


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


1- What kind of installation do you want (server, agent, local, hybrid 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
```

The presentation answers no to email notification.

ossec01 - VMware Workstation 15 Player (Non-commercial use only)

Player | Applications Places Terminal Fri 12:41

Home

Trash

preuss@ossec01:/home/preuss/ossec/ossec-hids-3.3.0

File Edit View Search Terminal Help

```
OSSEC HIDS v3.3.0 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.

 - System: Linux ossec01.mait.minnesota.edu 3.10.0-1062.4.3.el7.x86_64
 - User: root
 - Host: ossec01.mait.minnesota.edu


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


1- What kind of installation do you want (server, agent, local, hybrid 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]: y
```

The presentation answers yes to integrity check daemon.

[preuss@ossec01:~] preuss@ossec01:/home/preuss/oss... 1 / 4

Home

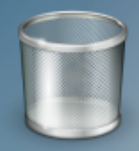
Trash

preuss@ossec01:/home/preuss/ossec/ossec-hids-3.3.0

File Edit View Search Terminal Help

```
OSSEC HIDS v3.3.0 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.

 - System: Linux ossec01.mait.minnesota.edu 3.10.0-1062.4.3.el7.x86_64
 - User: root
 - Host: ossec01.mait.minnesota.edu


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


1- What kind of installation do you want (server, agent, local, hybrid 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]: y

  - Running syscheck (integrity check daemon).

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

The presentation answers yes to rootkit detection engine.



preuss@ossec01:/home/preuss/ossec/ossec-hids-3.3.0

File Edit View Search Terminal Help

```
 - System: Linux ossec01.mait.minnesota.edu 3.10.0-1062.4.3.el7.x86_64
 - User: root
 - Host: ossec01.mait.minnesota.edu


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


1- What kind of installation do you want (server, agent, local, hybrid 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]: y

  - Running syscheck (integrity check daemon).

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

The presentation answers yes to enable active response.

Home

Trash

preuss@ossec01:/home/preuss/ossec/ossec-hids-3.3.0

File Edit View Search Terminal Help

```
 - 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]: y

   - Running syscheck (integrity check daemon).

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

The presentation answers yes to firewall-drop response.

Home

Trash

preuss@ossec01:/home/preuss/ossec/ossec-hids-3.3.0

File Edit View Search Terminal Help

```
 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]: y

  - Running syscheck (integrity check daemon).

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

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

-
    - 192.168.117.2

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

The presentation does not add any additional IP addresses to the white list.

Home

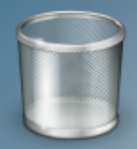
Trash

preuss@ossec01:/home/preuss/ossec/ossec-hids-3.3.0

File Edit View Search Terminal 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]: 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]: y

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

  -
     - 192.168.117.2

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

 3.6- Setting the configuration to analyze the following logs:
    -- /var/log/messages
    -- /var/log/secure
    -- /var/log/maillog

- 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 ---
```

The presentation presses "Enter" to continue.



preuss@ossec01:/home/preuss/ossec/ossec-hids-3.3.0

File Edit View Search Terminal Help

```
install -m 0550 -o root -g 0 syscheck_control /var/ossec/bin/
install -m 0550 -o root -g 0 rootcheck_control /var/ossec/bin/
install -m 0750 -o ossec -g ossec -d /var/ossec/stats
install -m 0550 -o root -g ossec -d /var/ossec/rules
install -m 0640 -o root -g ossec -b ../etc/rules/*.xml /var/ossec/rules
install -m 0750 -o ossec -g ossec -d /var/ossec/queue/fts
install -m 0750 -o ossec -g ossec -d /var/ossec/queue/rootcheck
install -m 0750 -o ossecr -g ossec -d /var/ossec/queue/agent-info
install -m 0750 -o ossec -g ossec -d /var/ossec/queue/agentless
install -m 0750 -o ossecr -g ossec -d /var/ossec/queue/rids
install -m 0640 -o root -g ossec ../etc/decoder.xml /var/ossec/etc/
rm -f /var/ossec/etc/shared/merged.mg


 - System is Redhat 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 https://github.com/ossec/ossec-hids or using
    our public maillist at
    https://groups.google.com/forum/#!forum/ossec-list

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

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


[root@ossec01 ossec-hids-3.3.0]# /var/ossec/bin/ossec-control start
```

The presentation starts OSSEC as shown on the last line.

Home

Trash

preuss@ossec01:/home/preuss/ossec/ossec-hids-3.3.0

File Edit View Search Terminal Help

```
install -m 0640 -o root -g ossec ../etc/decoder.xml /var/ossec/etc/
rm -f /var/ossec/etc/shared/merged.mg


 - System is Redhat 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 https://github.com/ossec/ossec-hids or using
    our public maillist at
    https://groups.google.com/forum/#!forum/ossec-list

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

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


[root@ossec01 ossec-hids-3.3.0]# /var/ossec/bin/ossec-control start
Starting OSSEC HIDS v3.3.0...
2019/11/22 12:48:03 ossec-maild: INFO: E-Mail notification disabled. Clean Exit.
Started ossec-maild...
Started ossec-execd...
Started ossec-analysisd...
Started ossec-logcollector...
Started ossec-syscheckd...
Started ossec-monitord...
Completed.
[root@ossec01 ossec-hids-3.3.0]#
```

OSSEC is now started on this system.

preuss@ossec01:/home/preuss/ossec/ossec-hids-3.3.0

File Edit View Search Terminal Help

```
[root@ossec01 ossec-hids-3.3.0]# ls -l /var/ossec/logs/
total 12
-rw-rw----. 1 ossec ossec     0 Nov 22 12:47 active-responses.log
drwxr-x---. 3 ossec ossec    36 Nov 22 12:48 alerts
drwxr-x---. 3 ossec ossec    38 Nov 22 12:48 archives
drwxr-x---. 3 ossec ossec    38 Nov 22 12:48 firewall
-rw-rw----. 1 ossec ossec 12232 Nov 22 12:48 ossec.log
[root@ossec01 ossec-hids-3.3.0]#
```

The presentation views the OSSEC log file location.

ossec01 - VMware Workstation 15 Player (Non-commercial use only)

Player | Applications Places Terminal Fri 12:50

Home

Trash

preuss@ossec01:/home/preuss/ossec/ossec-hids-3.3.0

File Edit View Search Terminal Help

```
[root@ossec01 ossec-hids-3.3.0]# whoami
root
[root@ossec01 ossec-hids-3.3.0]# finger preuss
bash: finger: command not found...
[root@ossec01 ossec-hids-3.3.0]# yum install finger
```

The presentation installs the "finger" program using "yum install finger".

[preuss@ossec01:~] preuss@ossec01:/home/preuss/oss... 1 / 4

ossec01 - VMware Workstation 15 Player (Non-commercial use only)

Player

Applications Places Terminal Fri 12:50

Home

Trash

preuss@ossec01:/home/preuss/ossec/ossec-hids-3.3.0

File Edit View Search Terminal Help

```
[root@ossec01 ossec-hids-3.3.0]# yum install finger
Loaded plugins: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
 * base: repo1.dal.innoscale.net
 * extras: mirror.us-midwest-1.nexcess.net
 * updates: mirrors.usinternet.com
Resolving Dependencies
--> Running transaction check
---> Package finger.x86_64 0:0.17-52.el7 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================
 Package                Arch                Version                Repository                Size
================================================================================
Installing:
 finger                 x86_64              0.17-52.el7            base                      25 k

Transaction Summary
================================================================================
Install  1 Package

Total download size: 25 k
Installed size: 32 k
Is this ok [y/d/N]: y
Downloading packages:
finger-0.17-52.el7.x86_64.rpm                                |  25 kB  00:00:00
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : finger-0.17-52.el7.x86_64                                    1/1
  Verifying  : finger-0.17-52.el7.x86_64                                    1/1

Installed:
  finger.x86_64 0:0.17-52.el7

Complete!
[root@ossec01 ossec-hids-3.3.0]#
```

The presentation finishes the finger installation.

[preuss@ossec01:~]

preuss@ossec01:/home/preuss/oss...

1 / 4

Home

Trash

preuss@ossec01:/home/preuss/ossec/ossec-hids-3.3.0

File Edit View Search Terminal Help

```
[root@ossec01 ossec-hids-3.3.0]# whoami
root
[root@ossec01 ossec-hids-3.3.0]# finger preuss
Login: preuss                           Name: preuss
Directory: /home/preuss                 Shell: /bin/bash
On since Fri Nov 22 12:32 (CST) on :0 from :0 (messages off)
On since Fri Nov 22 12:33 (CST) on pts/0 from :0
   14 minutes 51 seconds idle
On since Fri Nov 22 12:37 (CST) on pts/1 from :0
   3 seconds idle
No mail.
No Plan.
[root@ossec01 ossec-hids-3.3.0]#
```

The presentation "fingers" the preuss account.