Ossec Hybrid Installation

The presentation demonstrates installing Ossec hybrid （server and agent） on a single Linux machine. The Linux machine in this example is Slackware 14.2.

Preuss
4/26/2019

Desktop

ossec : bash - Konsole

File Edit View Bookmarks Settings Help

```
preuss@estonia:~$ cd apps/ossec/
preuss@estonia:~/apps/ossec$ ls
ossec-hids-3.2.0.tar.gz
preuss@estonia:~/apps/ossec$
```

The presentation downloads the current version of ossec tar zip file as shown.

ossec : bash

ossec : bash – Konsole

04:30 PM

Desktop

ossec : bash - Konsole

File Edit View Bookmarks Settings Help

```
preuss@estonia:~$ cd apps/ossec/
preuss@estonia:~/apps/ossec$ ls
ossec-hids-3.2.0.tar.gz
preuss@estonia:~/apps/ossec$ tar xzvf ossec-hids-3.2.0.tar.gz
```

The presentation unzips and untars the ossec tar zip as shown.

ossec : bash

ossec : bash – Konsole

04:30 PM

ossec : bash – Konsole

File Edit View Bookmarks Settings Help

```
ossec-hids-3.2.0/src/win32/doc.html
ossec-hids-3.2.0/src/win32/favicon.ico
ossec-hids-3.2.0/src/win32/help.txt
ossec-hids-3.2.0/src/win32/icofile.rc
ossec-hids-3.2.0/src/win32/nsProcess/
ossec-hids-3.2.0/src/win32/nsProcess/nsProcess.dll
ossec-hids-3.2.0/src/win32/nsProcess/nsProcess.nsh
ossec-hids-3.2.0/src/win32/os_win.h
ossec-hids-3.2.0/src/win32/ossec-installer.nsi
ossec-hids-3.2.0/src/win32/ossec-uninstall.ico
ossec-hids-3.2.0/src/win32/ossec.conf
ossec-hids-3.2.0/src/win32/read-registry.c
ossec-hids-3.2.0/src/win32/setup-iis.c
ossec-hids-3.2.0/src/win32/setup-shared.c
ossec-hids-3.2.0/src/win32/setup-shared.h
ossec-hids-3.2.0/src/win32/setup-syscheck.c
ossec-hids-3.2.0/src/win32/setup-win.c
ossec-hids-3.2.0/src/win32/ui/
ossec-hids-3.2.0/src/win32/ui/common.c
ossec-hids-3.2.0/src/win32/ui/favicon.ico
ossec-hids-3.2.0/src/win32/ui/os_win32ui.c
ossec-hids-3.2.0/src/win32/ui/os_win32ui.exe.manifest
ossec-hids-3.2.0/src/win32/ui/os_win32ui.h
ossec-hids-3.2.0/src/win32/ui/win32ui.rc
ossec-hids-3.2.0/src/win32/unix2dos.pl
ossec-hids-3.2.0/src/win32/vista_sec.txt
ossec-hids-3.2.0/src/win32/win_agent.c
ossec-hids-3.2.0/src/win32/win_service.c
preuss@estonia:~/apps/ossec$ cd ossec-hids-3.2.0
```

ossec : bash

The presentation changes directory as shown. Remember, your directory name could be different.

Desktop

ossec-hids-3.2.0 : bash - Konsole

File Edit View Bookmarks Settings Help

```
preuss@estonia:~/apps/ossec/ossec-hids-3.2.0$ ls
BUGS       CONFIG        INSTALL  README.md   active-response/  doc/  install.sh*
CHANGELOG  CONTRIBUTORS  LICENSE  SUPPORT.md  contrib/          etc/  src/
preuss@estonia:~/apps/ossec/ossec-hids-3.2.0$ su
Password:
root@estonia:/home/preuss/apps/ossec/ossec-hids-3.2.0#
```

The presentation lists fhe files as shown. The presentation becomes "root" as shown.

ossec-hids-3.2.0 : bash

ossec-hids-3.2.0 : bash – Konsole

04:31 PM

Desktop

ossec-hids-3.2.0 : bash - Konsole

File Edit View Bookmarks Settings Help

```
preuss@estonia:~/apps/ossec/ossec-hids-3.2.0$ ls
BUGS        CONFIG        INSTALL  README.md   active-response/  doc/  install.sh*
CHANGELOG   CONTRIBUTORS  LICENSE  SUPPORT.md  contrib/          etc/  src/
preuss@estonia:~/apps/ossec/ossec-hids-3.2.0$ su
Password:
root@estonia:/home/preuss/apps/ossec/ossec-hids-3.2.0# ./install.sh
```

The presentation begins the installation as shown.

ossec-hids-3.2.0 : bash

ossec-hids-3.2.0 : bash – Konsole

04:31 PM

Desktop

ossec-hids-3.2.0 : install.sh - Konsole

File Edit View Bookmarks Settings Help

```
preuss@estonia:~/apps/ossec/ossec-hids-3.2.0$ ls
BUGS       CONFIG        INSTALL  README.md   active-response/  doc/  install.sh*
CHANGELOG  CONTRIBUTORS  LICENSE  SUPPORT.md  contrib/          etc/  src/
preuss@estonia:~/apps/ossec/ossec-hids-3.2.0$ su
Password:
root@estonia:/home/preuss/apps/ossec/ossec-hids-3.2.0# ./install.sh
which: no host in (/usr/local/sbin:/usr/local/bin:/sbin:/usr/sbin:/bin:/usr/bin)

  ** Para instalaÃ§Ã£o em portuguÃªs, escolha [br].
  ** è¦ä½¿ç¨ä¸æè¿åè®®, è¯·éæ© [cn].
  ** Fur eine deutsche Installation wohlen Sie [de].
  ** ÎÎ¹Î± ÎµÎ³ÎºÎ±ÏÎ¬ÏÏÎ· ÏÏÎ± ÎÎ»Î»Î·Î½Î¹ÎºÎ¬, ÎµÏÎ¹Î»ÎÎ¾Îµ [el].
  ** For installation in English, choose [en].
  ** Para instalar en EspaÃ±ol , eliga [es].
  ** Pour une installation en franÃ§ais, choisissez [fr]
  ** A Magyar nyelvÅ± telepÃtÃ©shez vÃ¡lassza [hu].
  ** Per l'installazione in Italiano, scegli [it].
  ** æ¥æ¬èªã§ã¤ã³ãã¼ã«ãã¾ãéæãä¸ãã¼[jp].
  ** Voor installatie in het Nederlands, kies [nl].
  ** Aby instalowaÄ w jÄzyku Polskim, wybierz [pl].
  ** ÐÐ»Ñ Ð¸Ð½ÑÑÑÐºÐ¸Ð¹ Ð¿Ð¾ ÑÑÑÐ°Ð½Ð¾Ð²ÐºÐµ Ð½Ð° ÑÑÑÐºÐ¾Ð¼ ,Ð²Ð²ÐµÐ´Ð¸ÑÐµ [ru].
  ** Za instalaciju na srpskom, izaberi [sr].
  ** TÃ¼rkÃ§e kurulum iÃ§in seÃ§in [tr].
  (en/br/cn/de/el/es/fr/hu/it/jp/nl/pl/ru/sr/tr) [en]:
```

ossec-hids-3.2.0 : install.sh

The presentation presses "enter" to select english for the installation language.

ossec-hids-3.2.0 : install.sh - Konsole

04:31 PM

Desktop

ossec-hids-3.2.0 : install.sh - Konsole

File Edit View Bookmarks Settings Help

```
OSSEC HIDS v3.2.0 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 estonia 4.4.172
 - User: root
 - Host: estonia


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

The presentation presses "enter" to continue.

ossec-hids-3.2.0 : install.sh

ossec-hids-3.2.0 : install.sh – Konsole

04:31 PM

Desktop

ossec-hids-3.2.0 : install.sh - Konsole

File Edit View Bookmarks Settings Help

```
OSSEC HIDS v3.2.0 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 estonia 4.4.172
  - User: root
  - Host: estonia


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


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

The presentation enters "hybrid" and presses enter to continue.

ossec-hids-3.2.0 : install.sh

ossec-hids-3.2.0 : install.sh – Konsole

04:32 PM

ossec-hids-3.2.0 : install.sh – Konsole

File Edit View Bookmarks Settings Help

```
OSSEC HIDS v3.2.0 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 estonia 4.4.172
  - User: root
  - Host: estonia


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


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

  - Server installation chosen (hybrid).

2- Setting up the installation environment.

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

ossec-hids-3.2.0 : install.sh

The presentation presses "enter" to continue. The installation directory is good.

Desktop

ossec-hids-3.2.0 : install.sh - Konsole

File Edit View Bookmarks Settings Help

```
OSSEC HIDS v3.2.0 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 estonia 4.4.172
  - User: root
  - Host: estonia


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


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

  - Server installation chosen (hybrid).

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
```

ossec-hids-3.2.0 : install.sh

The presentation enters "n" and presses "enter" to continue. The presentation does not have an email server.

ossec-hids-3.2.0 : install.sh - Konsole

04:32 PM

Desktop

ossec-hids-3.2.0 : install.sh - Konsole

File Edit View Bookmarks Settings Help

```
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 estonia 4.4.172
  - User: root
  - Host: estonia


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


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

  - Server installation chosen (hybrid).

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]:
```

ossec-hids-3.2.0 : install.sh

The presentation presses "enter" to continue.

ossec-hids-3.2.0 : install.sh – Konsole

04:32 PM

Desktop

ossec-hids-3.2.0 : install.sh - Konsole

File Edit View Bookmarks Settings Help

```
  - System: Linux estonia 4.4.172
  - User: root
  - Host: estonia


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


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

  - Server installation chosen (hybrid).

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]:
```

ossec-hids-3.2.0 : install.sh

The presentation presses "enter" to continue.

ossec-hids-3.2.0 : install.sh – Konsole

04:32 PM

Desktop

ossec-hids-3.2.0 : install.sh - Konsole

File Edit View Bookmarks Settings Help

```
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]:

   - 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]:
```

ossec-hids-3.2.0 : install.sh

The presentation presses "enter" to continue.

ossec-hids-3.2.0 : install.sh - Konsole

04:32 PM

ossec-hids-3.2.0 : install.sh - Konsole

File Edit View Bookmarks Settings Help

```
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]:

   - 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]:
```

ossec-hids-3.2.0 : install.sh

The presentation presses "enter" to continue.

Desktop

ossec-hids-3.2.0 : install.sh - Konsole

File Edit View Bookmarks Settings Help

```
 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]:

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

  - Default white list for the active response:
     - 192.168.74.2

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

ossec-hids-3.2.0 : install.sh

The presentation presses "enter" to continue.

ossec-hids-3.2.0 : install.sh - Konsole

04:38 PM

ossec-hids-3.2.0 : install.sh - Konsole

File Edit View Bookmarks Settings Help

```
     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:
     - 192.168.74.2

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

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

ossec-hids-3.2.0 : install.sh

The presentation presses "enter" to continue. Do add this port address to your documentation. You will need to open the firewall port to allow access.

ossec-hids-3.2.0 : install.sh - Konsole

File Edit View Bookmarks Settings Help

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

  - Default white list for the active response:
    - 192.168.74.2

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

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

  - Remote syslog enabled.

 3.6- Setting the configuration to analyze the following logs:
   -- /var/log/messages
   -- /var/log/secure
   -- /var/log/syslog
   -- /var/adm/syslog
   -- /var/adm/messages
   -- /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 ---
```

ossec-hids-3.2.0 : install.sh

The presentation presses "enter" to continue.

ossec-hids-3.2.0 : install.sh - Konsole

File Edit View Bookmarks Settings Help

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


 - System is Slackware 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). ---
```

ossec-hids-3.2.0 : install.sh

The presentation presses "enter" to continue.

ossec-hids-3.2.0 : install.sh – Konsole

File Edit View Bookmarks Settings Help

```
OSSEC HIDS v3.2.0 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 estonia 4.4.172
  - User: root
  - Host: estonia


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

2- Setting up the installation environment.


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

3- Configuring the OSSEC HIDS.

  3.1- What's the IP Address or hostname of the OSSEC HIDS server?: 192.168.74.146
```

The presentation enters the host current IP address as shown. The presentation presses "enter" to continue.

ossec-hids-3.2.0 : install.sh

```
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:2f:92:63 brd ff:ff:ff:ff:ff:ff
    inet 192.168.74.146/24 brd 192.168.74.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe2f:9263/64 scope link
       valid_lft forever preferred_lft forever
preuss@estonia:~$
```

Desktop

ossec-hids-3.2.0 : bash - Konsole

File Edit View Bookmarks Settings Help

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

- The configuration can be viewed or modified at /var/ossec/ossec-agent/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). ---


- You first need to add this agent to the server so they
  can communicate with each other. When you have done so,
  you can run the 'manage_agents' tool to import the
  authentication key from the server.

   /var/ossec/ossec-agent/bin/manage_agents

   More information at:
   http://www.ossec.net/en/manual.html#ma

root@estonia:/home/preuss/apps/ossec/ossec-hids-3.2.0# /var/ossec/bin/ossec-control start
```

ossec-hids-3.2.0 : bash

```
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:2f:92:63 brd ff:ff:ff:ff:ff:ff
    inet 192.168.74.146/24 brd 192.168.74.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe2f:9263/64 scope link
       valid_lft forever preferred_lft forever
preuss@estonia:~$
```

The presentation starts the ossec server with the command shown.

ossec-hids-3.2.0 : bash - Konsole | preuss : bash - Konsole

Desktop

ossec-hids-3.2.0 : bash – Konsole

File Edit View Bookmarks Settings Help

```
    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). ---


 - You first need to add this agent to the server so they
   can communicate with each other. When you have done so,
   you can run the 'manage_agents' tool to import the
   authentication key from the server.

   /var/ossec/ossec-agent/bin/manage_agents

   More information at:
   http://www.ossec.net/en/manual.html#ma

root@estonia:/home/preuss/apps/ossec/ossec-hids-3.2.0# /var/ossec/bin/ossec-control start
Starting OSSEC HIDS v3.2.0...
Started ossec-execd...
Started ossec-analysisd...
Started ossec-logcollector...
Started ossec-remoted...
Started ossec-syscheckd...
Started ossec-monitord...
Completed.
root@estonia:/home/preuss/apps/ossec/ossec-hids-3.2.0# /var/ossec/ossec-agent/bin/ossec-control start
```

ossec-hids-3.2.0 : bash

```
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:2f:92:63 brd ff:ff:ff:ff:ff:ff
    inet 192.168.74.146/24 brd 192.168.74.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe2f:9263/64 scope link
       valid_lft forever preferred_lft forever
preuss@estonia:~$
```

The presentation starts the ossec agent with the command shown.

ossec-hids-3.2.0 : bash – Konsole | preuss : bash – Konsole

04:36 PM

Desktop

ossec-hids-3.2.0 : bash – Konsole

File Edit View Bookmarks Settings Help

```
   authentication key from the server.

   /var/ossec/ossec-agent/bin/manage_agents

   More information at:
   http://www.ossec.net/en/manual.html#ma

root@estonia:/home/preuss/apps/ossec/ossec-hids-3.2.0# /var/ossec/bin/ossec-control start
Starting OSSEC HIDS v3.2.0...
Started ossec-execd...
Started ossec-analysisd...
Started ossec-logcollector...
Started ossec-remoted...
Started ossec-syscheckd...
Started ossec-monitord...
Completed.
root@estonia:/home/preuss/apps/ossec/ossec-hids-3.2.0# /var/ossec/ossec-agent/bin/ossec-control start
Starting OSSEC HIDS v3.2.0...
Started ossec-execd...
2019/04/24 16:36:47 ossec-agentd: INFO: Using notify time: 600 and max time to reconnect: 1800
Started ossec-agentd...
Started ossec-logcollector...
2019/04/24 16:36:47 ossec-syscheckd(1702): INFO: No directory provided for syscheck to monitor.
2019/04/24 16:36:47 ossec-syscheckd: WARN: Syscheck disabled.
2019/04/24 16:36:47 rootcheck: Rootcheck disabled. Exiting.
2019/04/24 16:36:47 ossec-syscheckd: WARN: Rootcheck module disabled.
Started ossec-syscheckd...
Completed.
root@estonia:/home/preuss/apps/ossec/ossec-hids-3.2.0# /var/ossec/bin/manage_agents
```

ossec-hids-3.2.0 : bash

```
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:2f:92:63 brd ff:ff:ff:ff:ff:ff
    inet 192.168.74.146/24 brd 192.168.74.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe2f:9263/64 scope link
       valid_lft forever preferred_lft forever
preuss@estonia:~$
```

The presentation starts the server agent management program.

ossec-hids-3.2.0 : bash – Konsole | preuss : bash – Konsole

04:37 PM

Desktop

ossec-hids-3.2.0 : manage_agents - Konsole

File Edit View Bookmarks Settings Help

```
Starting OSSEC HIDS v3.2.0...
Started ossec-execd...
2019/04/24 16:36:47 ossec-agentd: INFO: Using notify time: 600 and max time to reconnect: 1800
Started ossec-agentd...
Started ossec-logcollector...
2019/04/24 16:36:47 ossec-syscheckd(1702): INFO: No directory provided for syscheck to monitor.
2019/04/24 16:36:47 ossec-syscheckd: WARN: Syscheck disabled.
2019/04/24 16:36:47 rootcheck: Rootcheck disabled. Exiting.
2019/04/24 16:36:47 ossec-syscheckd: WARN: Rootcheck module disabled.
Started ossec-syscheckd...
Completed.
root@estonia:/home/preuss/apps/ossec/ossec-hids-3.2.0# /var/ossec/bin/manage_agents


****************************************
* OSSEC HIDS v3.2.0 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: l

** No agent available. You need to add one first.

** Press ENTER to return to the main menu.
```

ossec-hids-3.2.0 : manage_agents

The presentation selects the letter "L" to list all current agents. No agents are found. The presentation presses "enter" to return to the menu.

Desktop

ossec-hids-3.2.0 : manage_agents - Konsole

File Edit View Bookmarks Settings Help

```
****************************************
* OSSEC HIDS v3.2.0 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: l

** No agent available. You need to add one first.

** Press ENTER to return to the main menu.



****************************************
* OSSEC HIDS v3.2.0 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
```

ossec-hids-3.2.0 : manage_agents

The presentation enters the letter "A" to add a new agent.

Kickoff Application Launcher
Favorites, applications, computer places, recently used items and desktop sessions

ossec-hids-3.2.0 : manage_agents - K

04:38 PM

ossec-hids-3.2.0 : manage_agents - Konsole

File Edit View Bookmarks Settings Help

```
* 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: l

** No agent available. You need to add one first.

** Press ENTER to return to the main menu.



****************************************
* OSSEC HIDS v3.2.0 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: estonia
```

ossec-hids-3.2.0 : manage_agents

The presentation provides a name for the new agent.

Desktop

ossec-hids-3.2.0 : manage_agents - Konsole

File Edit View Bookmarks Settings Help

```
****************************************
   (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: l

** No agent available. You need to add one first.

** Press ENTER to return to the main menu.



****************************************
* OSSEC HIDS v3.2.0 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: estonia
   * The IP Address of the new agent: 192.168.74.146
```

ossec-hids-3.2.0 : manage_agents

The presentation provides the IP address of the new agent.

ossec-hids-3.2.0 : manage_agents – K preuss : bash – Konsole

04:38 PM

ossec-hids-3.2.0 : manage_agents - Konsole

File Edit View Bookmarks Settings Help

```
   (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: l

** No agent available. You need to add one first.

** Press ENTER to return to the main menu.



****************************************
* OSSEC HIDS v3.2.0 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: estonia
   * The IP Address of the new agent: 192.168.74.146
   * An ID for the new agent[001]:
```

ossec-hids-3.2.0 : manage_agents

The presentation presses "enter" at the "ID" number.
The presentation does not need a custom ID number.

ossec-hids-3.2.0 : manage_agents - Konsole

File Edit View Bookmarks Settings Help

```
** No agent available. You need to add one first.

** Press ENTER to return to the main menu.



****************************************
* OSSEC HIDS v3.2.0 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: estonia
   * The IP Address of the new agent: 192.168.74.146
   * An ID for the new agent[001]:
Agent information:
   ID:001
   Name:estonia
   IP Address:192.168.74.146

Confirm adding it?(y/n):
```

ossec-hids-3.2.0 : mana

The presentation enters "Y" to confirm adding the new agent.

ossec-hids-3.2.0 : manage_agents - Konsole

File Edit View Bookmarks Settings Help

```
   (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: estonia
   * The IP Address of the new agent: 192.168.74.146
   * An ID for the new agent[001]:
Agent information:
   ID:001
   Name:estonia
   IP Address:192.168.74.146

Confirm adding it?(y/n): y
Agent added with ID 001.


****************************************
* OSSEC HIDS v3.2.0 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: e
```

ossec-hids-3.2.0 : manage_agents

The presentation selects "E" to extract the agent key.

ossec-hids-3.2.0 : manage_agents - Konsole

File Edit View Bookmarks Settings Help

```
- Adding a new agent (use '\q' to return to the main menu).
  Please provide the following:
   * A name for the new agent: estonia
   * The IP Address of the new agent: 192.168.74.146
   * An ID for the new agent[001]:
Agent information:
   ID:001
   Name:estonia
   IP Address:192.168.74.146

Confirm adding it?(y/n): y
Agent added with ID 001.


****************************************
* OSSEC HIDS v3.2.0 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: e

Available agents:
   ID: 001, Name: estonia, IP: 192.168.74.146
Provide the ID of the agent to extract the key (or '\q' to quit): 001
```

ossec-hids-3.2.0 : manage_agents

The presentation provides the ID number of the desired agent key.

Desktop

ossec-hids-3.2.0 : manage_agents - Konsole

File Edit View Bookmarks Settings Help

```
root@estonia:/home/preuss/apps/ossec/ossec-hids-3.2.0# /var/ossec/bin/manage_agents


****************************************
* OSSEC HIDS v3.2.0 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: e

Available agents:
   ID: 001, Name: estonia, IP: 192.168.74.146
Provide the ID of the agent to extract the key (or '\q' to quit): 001

Agent key information for '001' is:
MDAxIGVzdG9uaWEgMTkyLjE2OC43NC4xNDYgODlmNWFlMjI2NmQ3MDRjNWE0OWU3Mzg2MmRiZDUyYzFmYzg5OTU3YWNkMDE2ZTAyN2VmO
DM5YjFiNDgzNTYzNg==

** Press ENTER to return to the main mer
```

The presentation copies the "Agent key" to an editor. The presentation then presses "enter" to continue.

ous Document | Next Document | Save | Save As | Close | Undo | Redo

Docume...

Proje...

```
MDAxIGVzdG9uaWEgMTkyLjE2OC43NC4xNDYgODlmNWFlMjI2NmQ3MDRjNWE0OWU3Mzg2MmRiZDUyYzFmYzg5OTU3YWNkMDE2ZTAyN2VmODM5YjFiNDgzNTYzNg==
```

Line: 1 of 11 Col: 1 LINE INS Untitled ISO-8859-1

Search and Replace | Current Project

Untitled [modified] – Kate | ossec-hids-3.2.0 : manage_agents – K | preuss : bash – Konsole

04:42 PM

ossec-hids-3.2.0 : manage_agents - Konsole

File Edit View Bookmarks Settings Help

```
   (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: e

Available agents:
   ID: 001, Name: estonia, IP: 192.168.74.146
Provide the ID of the agent to extract the key (or '\q' to quit): 001

Agent key information for '001' is:
MDAxIGVzdG9uaWEgMTkyLjE2OC43NC4xNDYgODlmNWFlMjI2NmQ3MDRjNWE0OWU3Mzg2MmRiZDUyYzFmYzg5OTU3YWNkMDE2ZTAyN2Vm0
DM5YjFiNDgzNTYzNg==

** Press ENTER to return to the main menu.



****************************************
* OSSEC HIDS v3.2.0 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: q
```

ossec-hids-3.2.0 : manage_agents

The presentation selects "q" to quit the agent manager program.

Desktop

ossec-hids-3.2.0 : bash – Konsole

File Edit View Bookmarks Settings Help

```
root@estonia:/home/preuss/apps/ossec/ossec-hids-3.2.0# /var/ossec/ossec-agent/bin/manage_agents
```

The presentation starts the agent's key management program as shown.

ossec-hids-3.2.0 : bash

New Open Previous Document Next Document Save Save As Close Undo Redo

Docume...

Proje...

```
MDAxIGVzdG9uaWEgMTkyLjE2OC43NC4xNDYgODlmNWFlMjI2NmQ3MDRjNWE0OWU3Mzg2MmRiZDUyYzFmYzg5OTU3YWNkMDE2ZTAyN2VmODM5YjFiNDgzNTYzNg==
```

Line: 1 of 11 Col: 1 LINE INS Untitled ISO-8859-1

Search and Replace Current Project

Untitled [modified] – Kate | ossec-hids-3.2.0 : bash – Konsole | preuss : bash – Konsole

04:42 PM

Desktop

ossec-hids-3.2.0 : manage_agents - Konsole

File Edit View Bookmarks Settings Help

```
root@estonia:/home/preuss/apps/ossec/ossec-hids-3.2.0# /var/ossec/ossec-agent/bin/manage_agents


****************************************
* OSSEC HIDS v3.2.0 Agent manager.     *
* The following options are available: *
****************************************
   (I)mport key from the server (I).
   (Q)uit.
Choose your action: I or Q: i
```

The presentation enters "i" to import a key.

ossec-hids-3.2.0 : manage_agents

New Open Previous Document Next Document Save Save As Close Undo Redo

Docume...

Proje...

```
MDAxIGVzdG9uaWEgMTkyLjE2OC43NC4xNDYgODlmNWFlMjI2NmQ3MDRjNWE0OWU3Mzg2MmRiZDUyYzFmYzg5OTU3YWNkMDE2ZTAyN2VmODM5YjFiNDgzNTYzNg==
```

Line: 1 of 11 Col: 1 LINE INS Untitled ISO-8859-1

Search and Replace Current Project

Untitled [modified] – Kate | ossec-hids-3.2.0 : manage_agents – K | preuss : bash – Konsole

04:42 PM

Desktop

ossec-hids-3.2.0 : manage_agents - Konsole

File Edit View Bookmarks Settings Help

```
root@estonia:/home/preuss/apps/ossec/ossec-hids-3.2.0# /var/ossec/ossec-agent/bin/manage_agents


****************************************
* OSSEC HIDS v3.2.0 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): MDAxIGVzdG9uaWEgMTkyLjE2OC43NC4xNDYgODlmNWFlMjI2NmQ3MDRjNWE0OWU3Mzg2MmRi
ZDUyYzFmYzg5OTU3YWNkMDE2ZTAyN2VmODM5YjFiNDgzNTYzNg==
```

The presentation enters the key from the server as shown.

ossec-hids-3.2.0 : manage_agents

New Open Previous Document Next Document Save Save As Close Undo Redo

Docume...

Proje...

MDAxIGVzdG9uaWEgMTkyLjE2OC43NC4xNDYgODlmNWFlMjI2NmQ3MDRjNWE0OWU3Mzg2MmRiZDUyYzFmYzg5OTU3YWNkMDE2ZTAyN2VmODM5YjFiNDgzNTYzNg==

Line: 2 of 11 Col: 1 LINE INS Untitled ISO-8859-1

Search and Replace Current Project

Untitled [modified] – Kate | ossec-hids-3.2.0 : manage_agents – K | preuss : bash – Konsole

04:43 PM

Desktop

ossec-hids-3.2.0 : manage_agents - Konsole

File Edit View Bookmarks Settings Help

```
root@estonia:/home/preuss/apps/ossec/ossec-hids-3.2.0# /var/ossec/ossec-agent/bin/manage_agents


****************************************
* OSSEC HIDS v3.2.0 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): MDAxIGVzdG9uaWEgMTkyLjE2OC43NC4xNDYgODlmNWFlMjI2NmQ3MDRjNWE0OWU3Mzg2MmRi
ZDUyYzFmYzg5OTU3YWNkMDE2ZTAyN2VmODM5YjFiNDgzNTYzNg==

Agent information:
   ID:001
   Name:estonia
   IP Address:192.168.74.146

Confirm adding it?(y/n): y
```

The presentation enters "y" to continue.

ossec-hids-3.2.0 : manage_

New Op Save As Close Undo Redo

Docume... Proje...

MDAxIGVzd 2MmRiZDUyYzFmYzg5OTU3YWNkMDE2ZTAyN2VmODM5YjFiNDgzNTYzNg==

Line: 2 of 11 Col: 1 LINE INS Untitled ISO-8859-1

Search and Replace Current Project

Untitled [modified] – Kate | ossec-hids-3.2.0 : manage_agents – K | preuss : bash – Konsole | 04:48 PM

ossec-hids-3.2.0 : manage_agents - Konsole

File Edit View Bookmarks Settings Help

```
root@estonia:/home/preuss/apps/ossec/ossec-hids-3.2.0# /var/ossec/ossec-agent/bin/manage_agents


****************************************
* OSSEC HIDS v3.2.0 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): MDAxIGVzdG9uaWEgMTkyLjE2OC43NC4xNDYgODlmNWFlMjI2NmQ3MDRjNWE0OWU3Mzg2MmRi
ZDUyYzFmYzg5OTU3YWNkMDE2ZTAyN2VmODM5YjFiNDgzNTYzNg==

Agent information:
   ID:001
   Name:estonia
   IP Address:192.168.74.146

Confirm adding it?(y/n): y
Added.
** Press ENTER to return to the main menu.
```

The presentation presses "enter" to continue.

ossec-hids-3.2.0 : manage_agents

New Open Previous Documen Undo Redo

Docume... Proje...

Line: 2 of 11 Col: 1 LINE INS Untitled ISO-8859-1

Search and Replace Current Project

Untitled [modified] – Kate | ossec-hids-3.2.0 : manage_agents – K | preuss : bash – Konsole

04:48 PM

ossec-hids-3.2.0 : manage_agents - Konsole

File Edit View Bookmarks Settings Help

```
   (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): MDAxIGVzdG9uaWEgMTkyLjE2OC43NC4xNDYgODlmNWFlMjI2NmQ3MDRjNWE0OWU3Mzg2MmRi
ZDUyYzFmYzg5OTU3YWNkMDE2ZTAyN2VmODM5YjFiNDgzNTYzNg==

Agent information:
   ID:001
   Name:estonia
   IP Address:192.168.74.146

Confirm adding it?(y/n): y
Added.
** Press ENTER to return to the main menu.



****************************************
* OSSEC HIDS v3.2.0 Agent manager.     *
* The following options are available: *
****************************************
   (I)mport key from the server (I).
   (Q)uit.
Choose your action: I or Q: q
```

ossec-hids-3.2.0 : manage_agents

The presentation enters "q" to continue.

Desktop

Untitled [modified] – Kate

ossec-hids-3.2.0 : manage_agents – K

preuss : bash – Konsole

04:48 PM

Desktop

The installation is complete.

preuss : bash – Konsole

04:44 PM