AlienVault: OSSEC (IDS) Deployment

October 23, 2020 By Raj Chandel

In this article, we will discuss of Deployment of OSSEC (IDS) agents to the AlienVault server.

OSSEC is an open-source, host-based intrusion detection system (commonly called IDS) that market itself as the world's most widely used intrusion detection system that performs or helps us to Monitor: –

- Network Anomalies
- Log analysis
- Integrity Checking
- Windows registry monitoring
- Rootkit detection
- Process monitoring
- Real-time alerting
- Active response
- Policy monitoring

Intrusion detection systems are customizable like a firewall and also, they can be configured to send alarm messages upon a rule's instruction to automatically answer to the threat or warning as for your network or device.

OSSEC (IDS) can warn us against DDOS, brute force, exploits, data leak, and more external attacks. it monitors our network in real-time and interacts with us and with our system as we decide. It can be used to monitor one server or thousands of servers in a server/agent mode.

Table of content

For Linux

For Windows

- Run and verify OSSEC agent is connected or running

Prerequisites

- Ubuntu 20.04.1
- Windows 10
- Root or Admin privileges

For Ubuntu 20.04.1

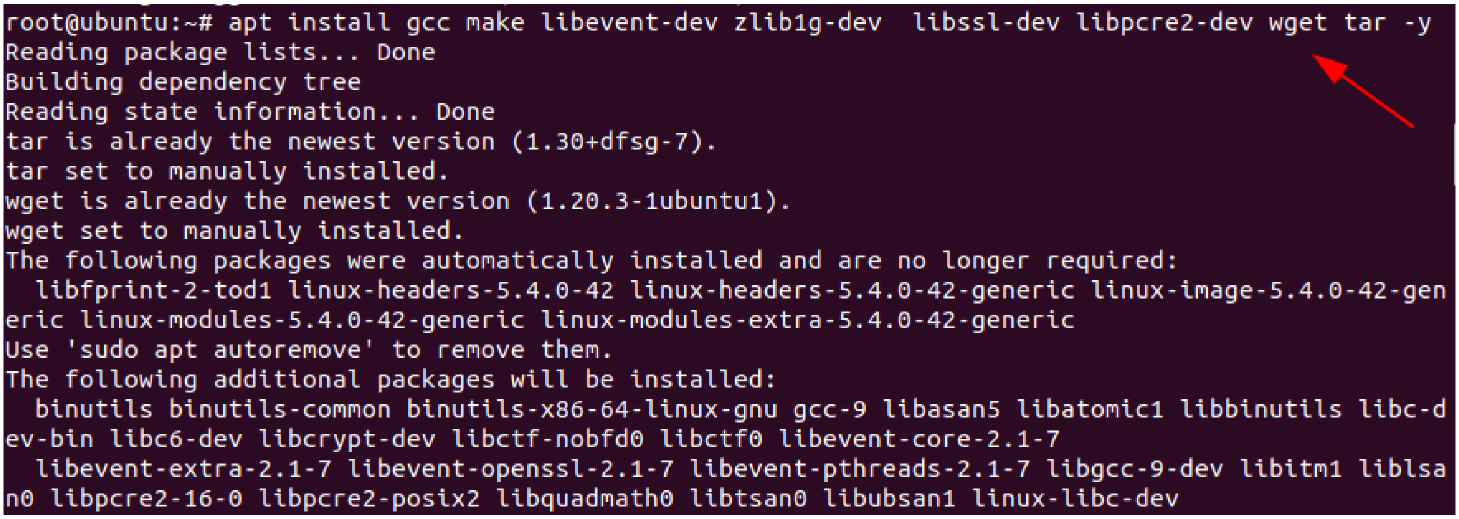
Required Dependencies

To install OSSEC agent on Ubuntu 20.04.1 there are some requirement need to be installed before agent installation as listed below: –

- GCC
- Make
- Libevent-dev
- Zlib-dev
- Libssl-dev
- Libpcre2-dev
- Wget
- Tar

You can download this all requirement by simply running this command: –

```
apt install gcc make libevent-dev zlib1g-dev  libssl-dev libpcre2-dev wget tar
```

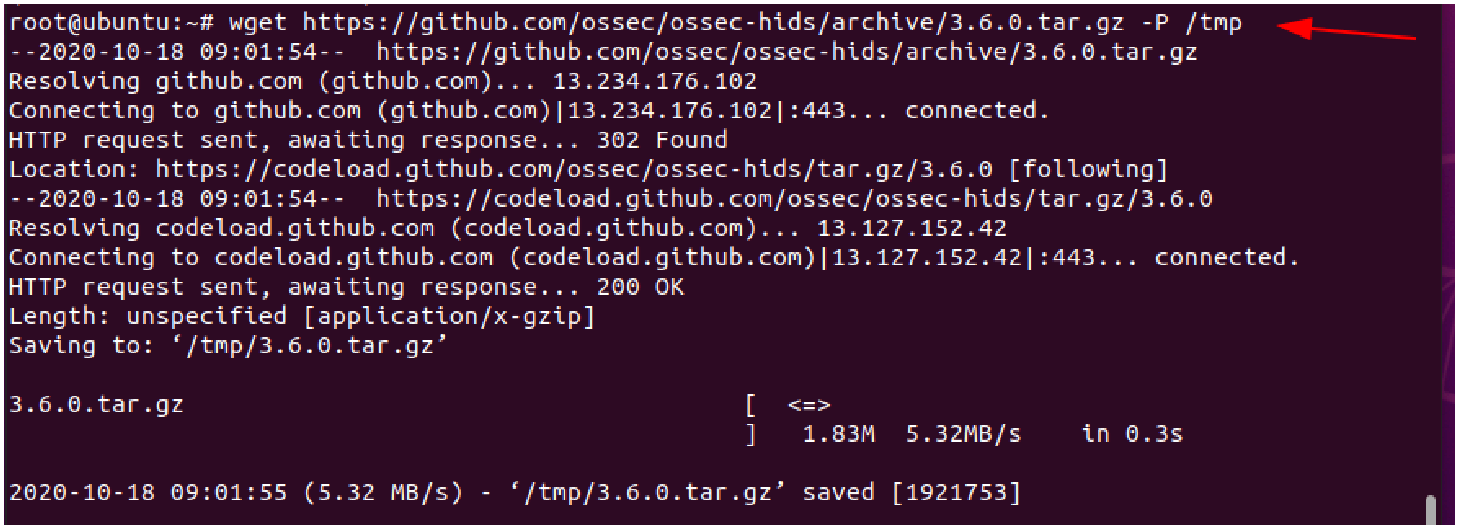


```
root@ubuntu:~# apt install gcc make libevent-dev zlib1g-dev  libssl-dev libpcre2-dev wget tar -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
tar is already the newest version (1.30+dfsg-7).
tar set to manually installed.
wget is already the newest version (1.20.3-1ubuntu1).
wget set to manually installed.
The following packages were automatically installed and are no longer required:
  libfprint-2-tod1 linux-headers-5.4.0-42 linux-headers-5.4.0-42-generic linux-image-5.4.0-42-gen
eric linux-modules-5.4.0-42-generic linux-modules-extra-5.4.0-42-generic
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  binutils binutils-common binutils-x86-64-linux-gnu gcc-9 libasan5 libatomic1 libbinutils libc-d
ev-bin libc6-dev libcrypt-dev libctf-nobfd0 libctf0 libevent-core-2.1-7
  libevent-extra-2.1-7 libevent-openssl-2.1-7 libevent-pthreads-2.1-7 libgcc-9-dev libitm1 liblsa
n0 libpcre2-16-0 libpcre2-posix2 libquadmath0 libtsan0 libubsan1 linux-libc-dev
```

Download OSSEC source code

You can download the latest OSSEC source code from the Official **release page** of GitHub or simply running this command: –

```
wget https://github.com/ossec/ossec-hids/archive/3.6.0.tar.gz -P /tmp
```



```
root@ubuntu:~# wget https://github.com/ossec/ossec-hids/archive/3.6.0.tar.gz -P /tmp
--2020-10-18 09:01:54--  https://github.com/ossec/ossec-hids/archive/3.6.0.tar.gz
Resolving github.com (github.com)... 13.234.176.102
Connecting to github.com (github.com)|13.234.176.102|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://codeload.github.com/ossec/ossec-hids/tar.gz/3.6.0 [following]
--2020-10-18 09:01:54--  https://codeload.github.com/ossec/ossec-hids/tar.gz/3.6.0
Resolving codeload.github.com (codeload.github.com)... 13.127.152.42
Connecting to codeload.github.com (codeload.github.com)|13.127.152.42|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [application/x-gzip]
Saving to: ‘/tmp/3.6.0.tar.gz’

3.6.0.tar.gz                                      [  <=>
                                                  ]   1.83M  5.32MB/s    in 0.3s

2020-10-18 09:01:55 (5.32 MB/s) - ‘/tmp/3.6.0.tar.gz’ saved [1921753]
```

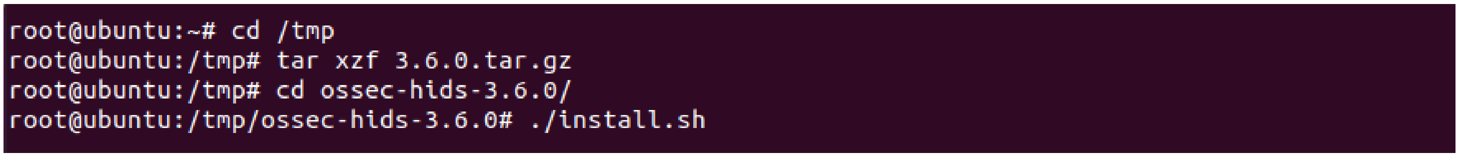
Extract & install OSSEC agent from source code

Once the source download complete you can extract it by simply running this command

```
cd /tmp
tar xzf 3.6.0.tar.gz
```

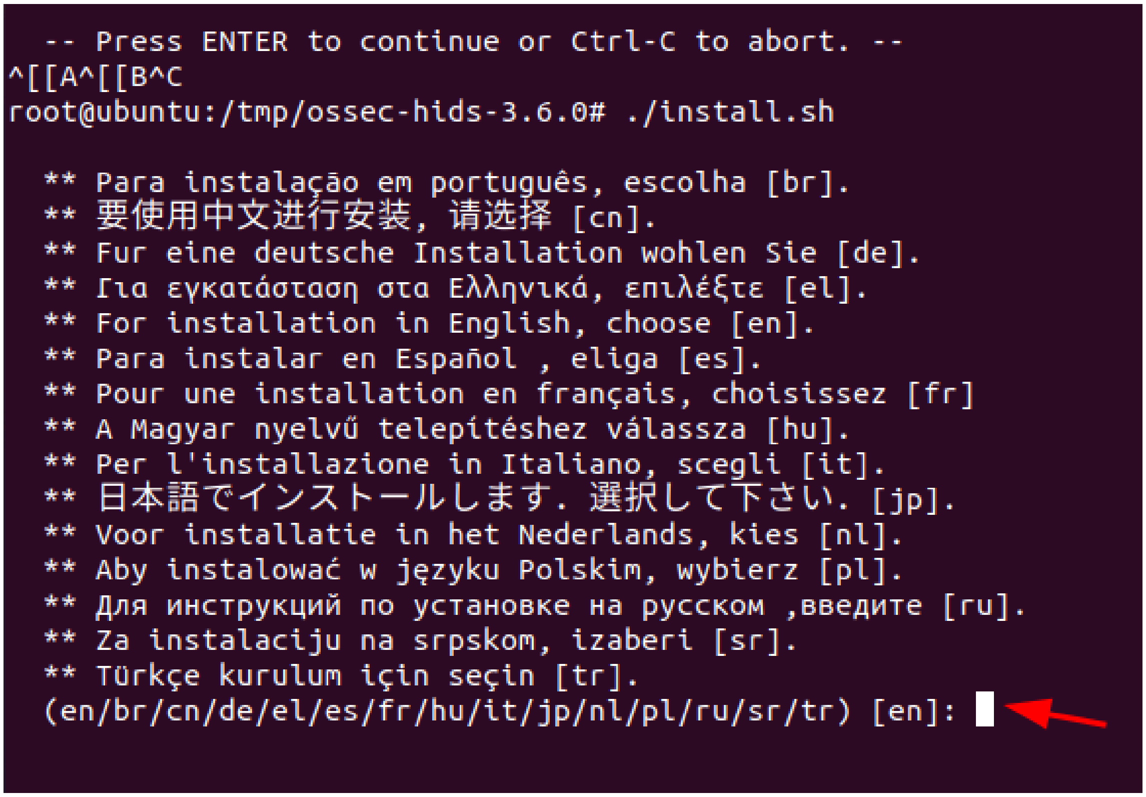
In manner to install OSSEC agent navigate to the source code directory and run the installation script as shown below

```
cd ossec-hids-3.6.0/
./install.sh
```



```
root@ubuntu:~# cd /tmp
root@ubuntu:/tmp# tar xzf 3.6.0.tar.gz
root@ubuntu:/tmp# cd ossec-hids-3.6.0/
root@ubuntu:/tmp/ossec-hids-3.6.0# ./install.sh
```

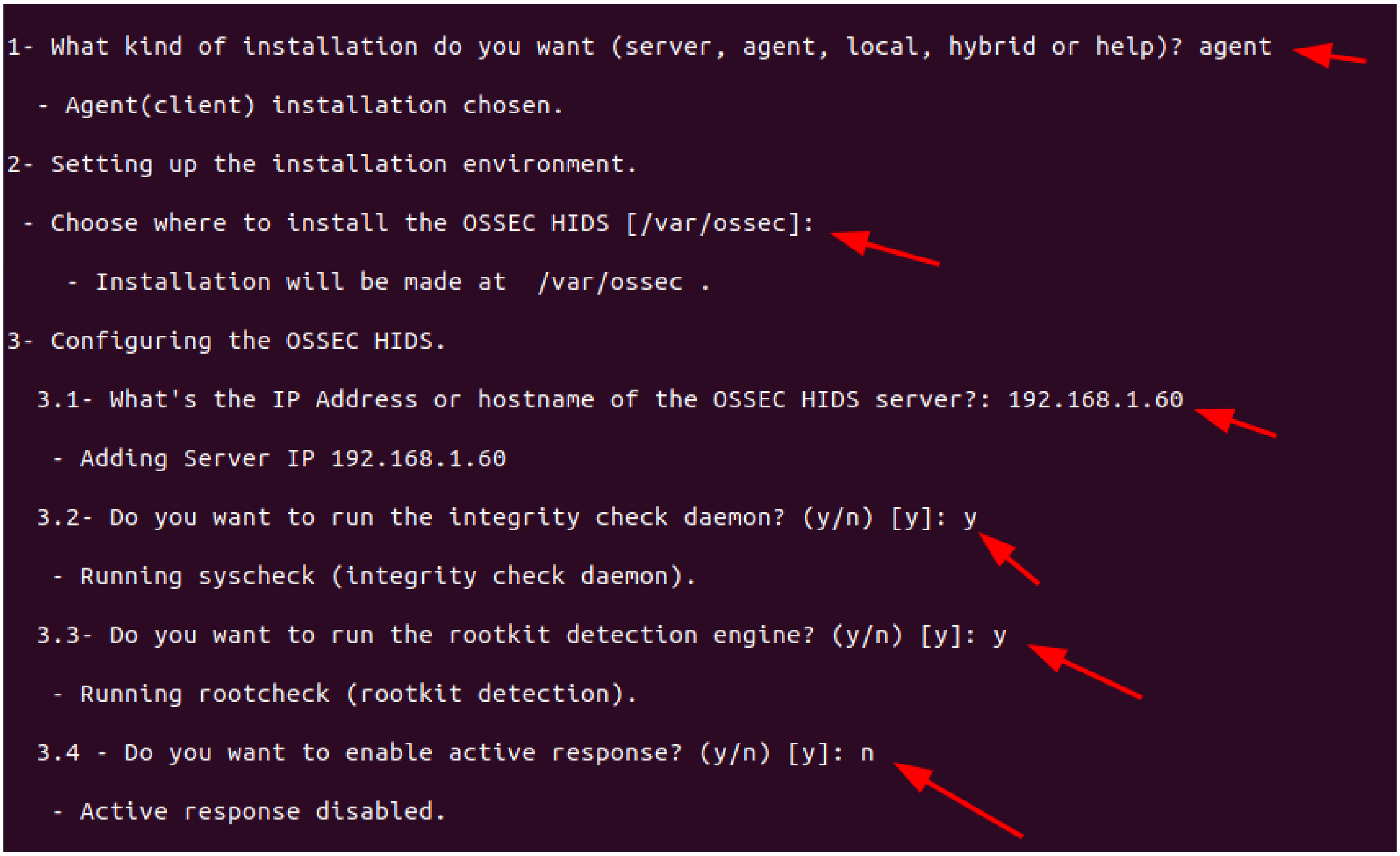
Further then select your installation language or press ENTER to choose default installation options and follow the steps as described below: –



```
  -- Press ENTER to continue or Ctrl-C to abort. --
^[[A^[[B^C
root@ubuntu:/tmp/ossec-hids-3.6.0# ./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]:
```

- Specify the type of installation. In our case we are installing an OSSEC-HIDS agent, so we go with the option of the agent.
- Choose the installation path. By default, it is /var/ossec or you can define the path as per your environment.
- Enter the OSSEC-HIDS server IP or AlienVault server IP.
- Enable the system integrity check.
- Enable rootkit detection.
- Enable or disable active directory response.
- Once you are done with defining the default options, proceed to install the OSSEC agent by **pressing ENTER**
- Then after **press ENTER** to close the installer as shown below



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

  - Agent(client) 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- What's the IP Address or hostname of the OSSEC HIDS server?: 192.168.1.60

   - Adding Server IP 192.168.1.60

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

   - Active response disabled.
```

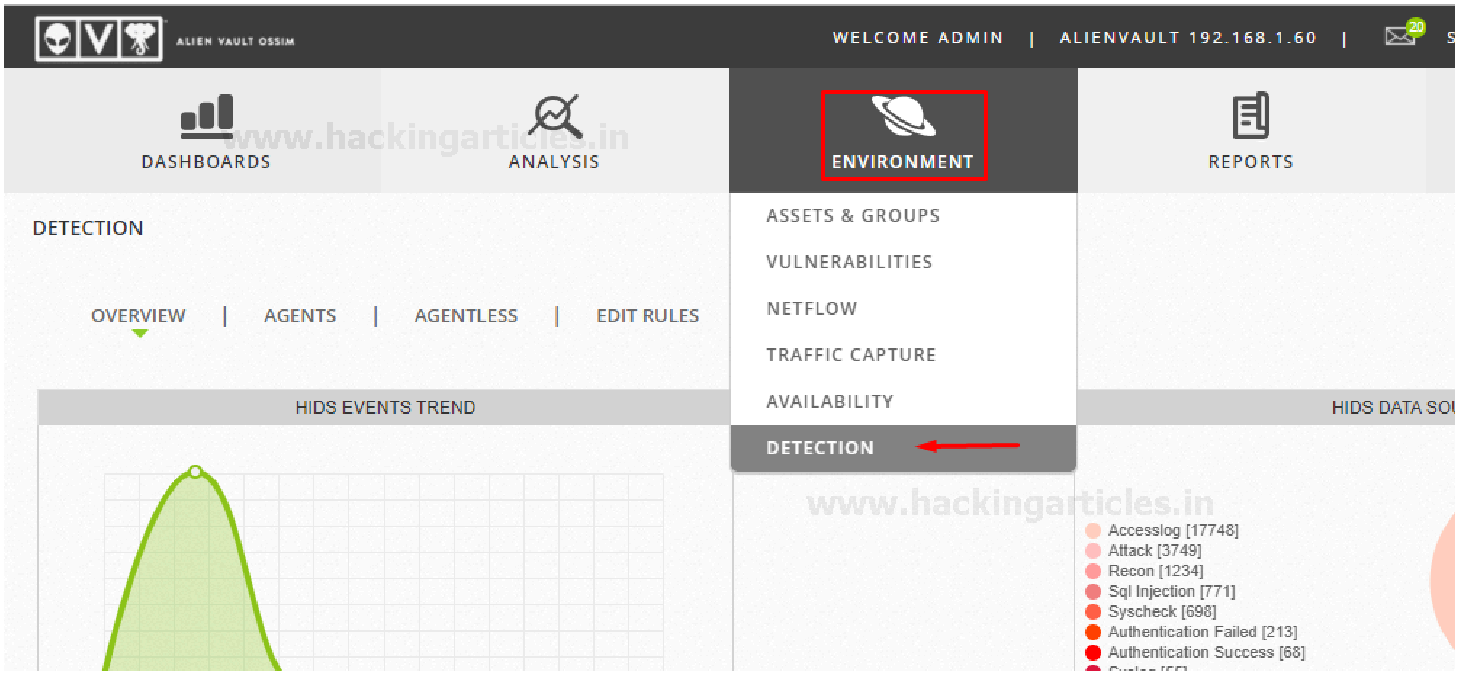
v

Deploying OSSEC agent to AlienVault server

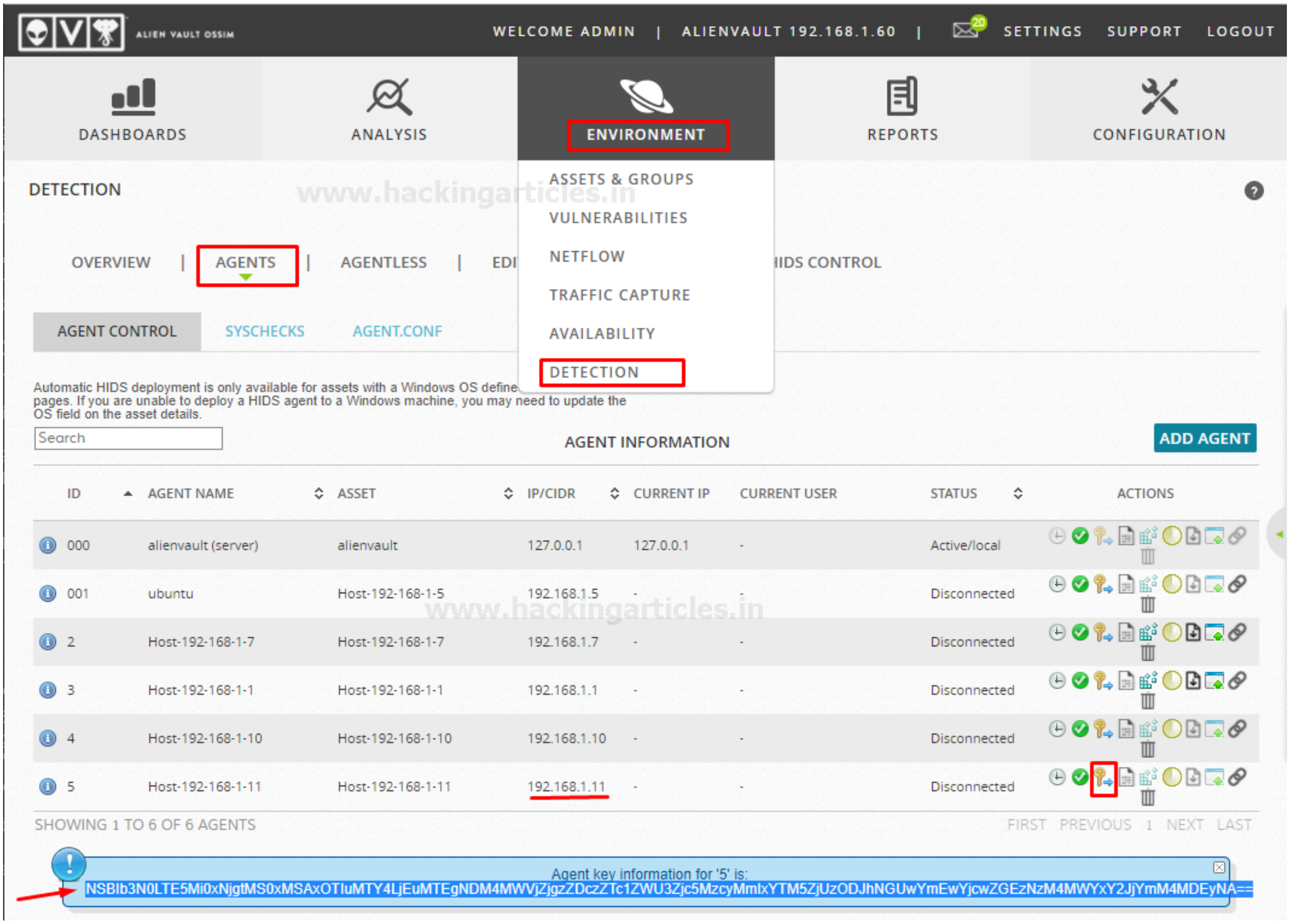
In a manner the agent to communicate with the server

- You need to first add it to the HIDS server or AlienVault server
- After that extract, the agent authentication key from the AlienVault server

To extract agent key from server, go to the AlienVault Web UI and then navigate to Environment > Detection as shown below: –



Then select or add Agent where you installed OSSEC agent and then extract or copy the key as shown below



Automatic HIDS deployment is only available for assets with a Windows OS define pages. If you are unable to deploy a HIDS agent to a Windows machine, you may need to update the OS field on the asset details.

AGENT INFORMATION

ID	AGENT NAME	ASSET	IP/CIDR	CURRENT IP	CURRENT USER	STATUS	ACTIONS
000	alienvault (server)	alienvault	127.0.0.1	127.0.0.1	-	Active/local	
001	ubuntu	Host-192-168-1-5	192.168.1.5	-	-	Disconnected	
2	Host-192-168-1-7	Host-192-168-1-7	192.168.1.7	-	-	Disconnected	
3	Host-192-168-1-1	Host-192-168-1-1	192.168.1.1	-	-	Disconnected	
4	Host-192-168-1-10	Host-192-168-1-10	192.168.1.10	-	-	Disconnected	
5	Host-192-168-1-11	Host-192-168-1-11	192.168.1.11	-	-	Disconnected	

SHOWING 1 TO 6 OF 6 AGENTS

FIRST PREVIOUS 1 NEXT LAST

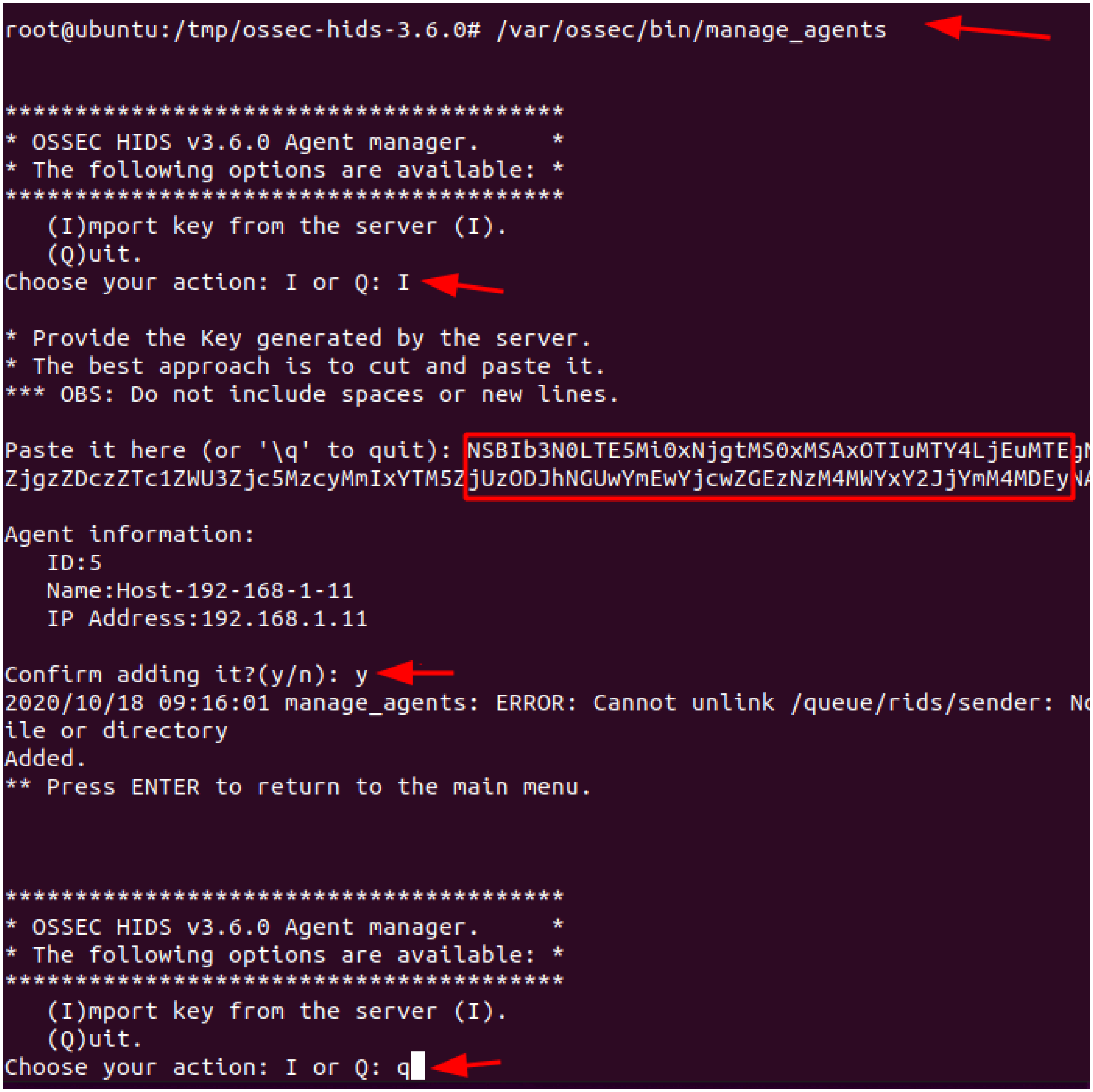
Agent key information for '5' is:

NSBlb3N0LTE5Mi0xNjgtMS0xMSAxOTIuMTY4LjEuMTEgNDM4MWVjZjgzZDczZTc1ZWU3Zjc5MzcyMmlxYTM5ZjUzODJhNGUwYmEwYjcwZGEzNzM4MWYxY2JjYmM4MDEyNA==

Once you have extracted the key, Import the key on the agent simply by running the following command: –

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

Enter I, paste the key that you copied from AlienVault Web UI and confirm adding the key then exit from the window by **pressing Q** as shown below



```
root@ubuntu:/tmp/ossec-hids-3.6.0# /var/ossec/bin/manage_agents


****************************************
* OSSEC HIDS v3.6.0 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): NSBIb3N0LTE5Mi0xNjgtMS0xMSAxOTIuMTY4LjEuMTEg
ZjgzZDczZTc1ZWU3Zjc5MzcyMmIxYTM5ZjUzODJhNGUwYmEwYjcwZGEzNzM4MWYxY2JjYmM4MDEy

Agent information:
   ID:5
   Name:Host-192-168-1-11
   IP Address:192.168.1.11

Confirm adding it?(y/n): y
2020/10/18 09:16:01 manage_agents: ERROR: Cannot unlink /queue/rids/sender: N
ile or directory
Added.
** Press ENTER to return to the main menu.



****************************************
* OSSEC HIDS v3.6.0 Agent manager.     *
* The following options are available: *
****************************************
   (I)mport key from the server (I).
   (Q)uit.
Choose your action: I or Q: q
```

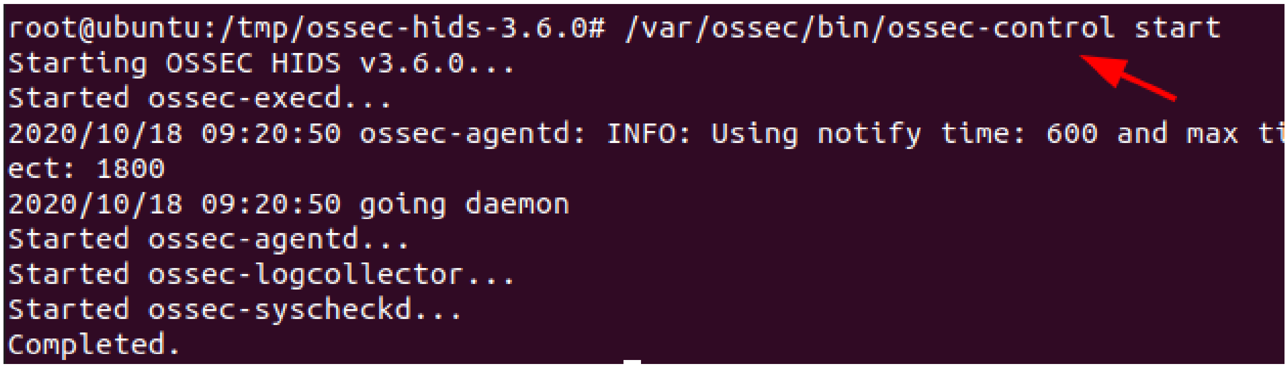
Running OSSEC agent

Once the installation completes starting the OSSEC agent simply by running the following command:

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

Or

```
systemctl start ossec
```



```
root@ubuntu:/tmp/ossec-hids-3.6.0# /var/ossec/bin/ossec-control start
Starting OSSEC HIDS v3.6.0...
Started ossec-execd...
2020/10/18 09:20:50 ossec-agentd: INFO: Using notify time: 600 and max ti
ect: 1800
2020/10/18 09:20:50 going daemon
Started ossec-agentd...
Started ossec-logcollector...
Started ossec-syscheckd...
Completed.
```

To stop the agent run the below command

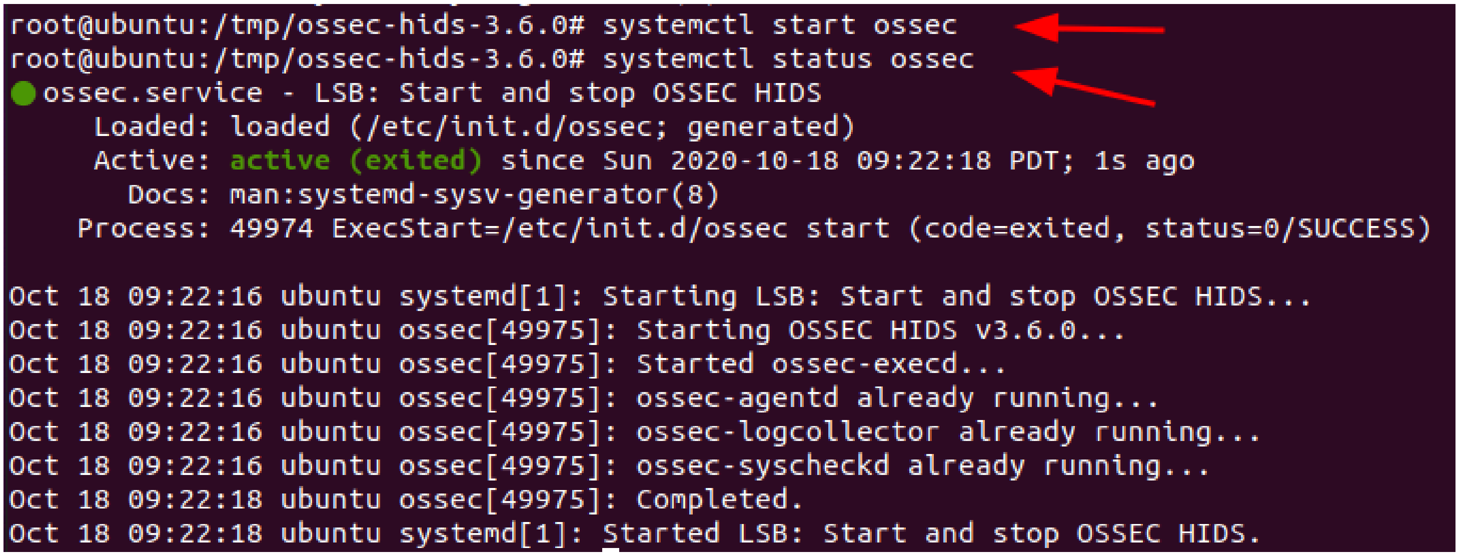
```
/var/ossec/bin/ossec-control stop
Or
systemctl stop ossec
```

Other service control commands are described below.

```
/var/ossec/bin/ossec-control {start|stop|reload|restart|status}
```

To check the status.

```
/var/ossec/bin/ossec-control status
```

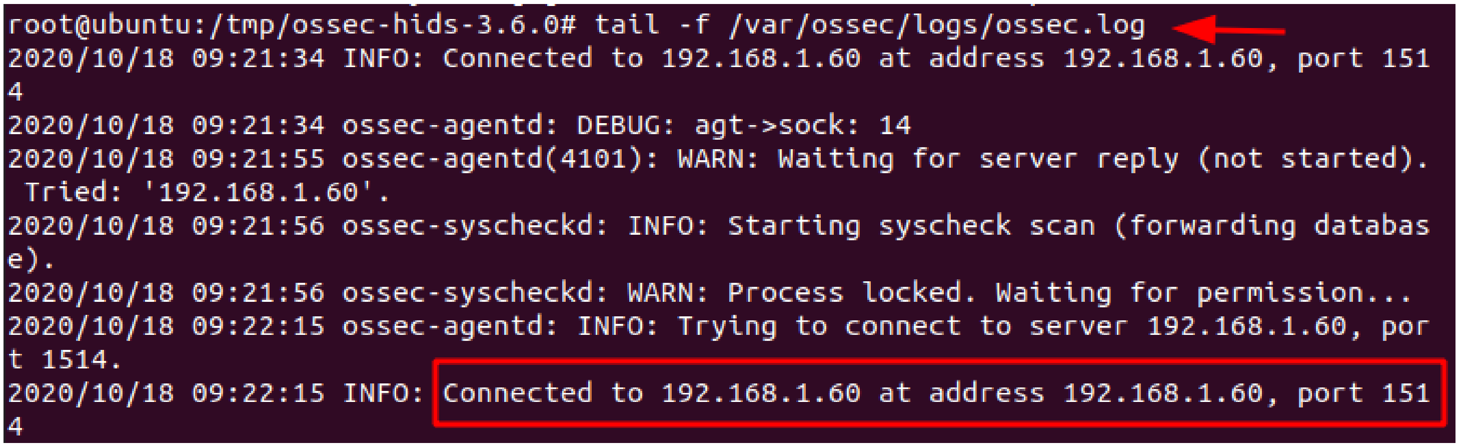


```
root@ubuntu:/tmp/ossec-hids-3.6.0# systemctl start ossec
root@ubuntu:/tmp/ossec-hids-3.6.0# systemctl status ossec
● ossec.service - LSB: Start and stop OSSEC HIDS
     Loaded: loaded (/etc/init.d/ossec; generated)
     Active: active (exited) since Sun 2020-10-18 09:22:18 PDT; 1s ago
       Docs: man:systemd-sysv-generator(8)
    Process: 49974 ExecStart=/etc/init.d/ossec start (code=exited, status=0/SUCCESS)

Oct 18 09:22:16 ubuntu systemd[1]: Starting LSB: Start and stop OSSEC HIDS...
Oct 18 09:22:16 ubuntu ossec[49975]: Starting OSSEC HIDS v3.6.0...
Oct 18 09:22:16 ubuntu ossec[49975]: Started ossec-execd...
Oct 18 09:22:16 ubuntu ossec[49975]: ossec-agentd already running...
Oct 18 09:22:16 ubuntu ossec[49975]: ossec-logcollector already running...
Oct 18 09:22:16 ubuntu ossec[49975]: ossec-syscheckd already running...
Oct 18 09:22:18 ubuntu ossec[49975]: Completed.
Oct 18 09:22:18 ubuntu systemd[1]: Started LSB: Start and stop OSSEC HIDS.
```

check the logs to see if the agent has connected to the server.

```
tail -f /var/ossec/logs/ossec.log
```



```
root@ubuntu:/tmp/ossec-hids-3.6.0# tail -f /var/ossec/logs/ossec.log
2020/10/18 09:21:34 INFO: Connected to 192.168.1.60 at address 192.168.1.60, port 151
4
2020/10/18 09:21:34 ossec-agentd: DEBUG: agt->sock: 14
2020/10/18 09:21:55 ossec-agentd(4101): WARN: Waiting for server reply (not started).
 Tried: '192.168.1.60'.
2020/10/18 09:21:56 ossec-syscheckd: INFO: Starting syscheck scan (forwarding databas
e).
2020/10/18 09:21:56 ossec-syscheckd: WARN: Process locked. Waiting for permission...
2020/10/18 09:22:15 ossec-agentd: INFO: Trying to connect to server 192.168.1.60, por
t 1514.
2020/10/18 09:22:15 INFO: Connected to 192.168.1.60 at address 192.168.1.60, port 151
4
```

As you can see the agent is successfully connected to the AlienVault server

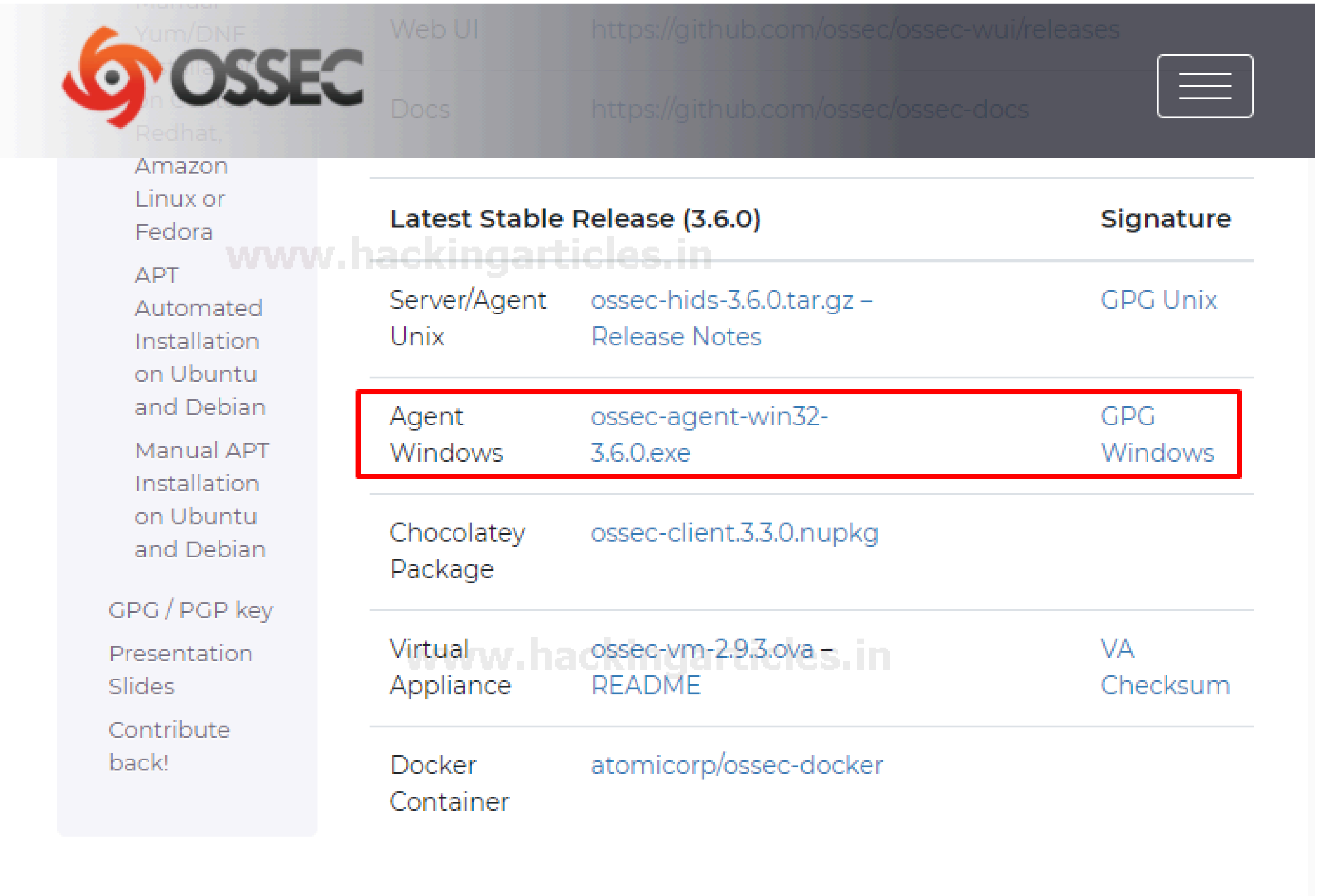
Congratulations !!! you have successfully deployed your Ubuntu machine to the AlienVault server

For Windows Machine

Download OSSEC agent for Windows

You can download the OSSEC agent for windows from the **OSSEC official page**

Locate and select package Agent Windows ossec-agent-win-32-3.6.exe or the latest one as shown below:



Web UI	https://github.com/ossec/ossec-wui/releases
Docs	https://github.com/ossec/ossec-docs

Yum/DNF
Redhat, Amazon Linux or Fedora

APT Automated Installation on Ubuntu and Debian

Manual APT Installation on Ubuntu and Debian

GPG / PGP key

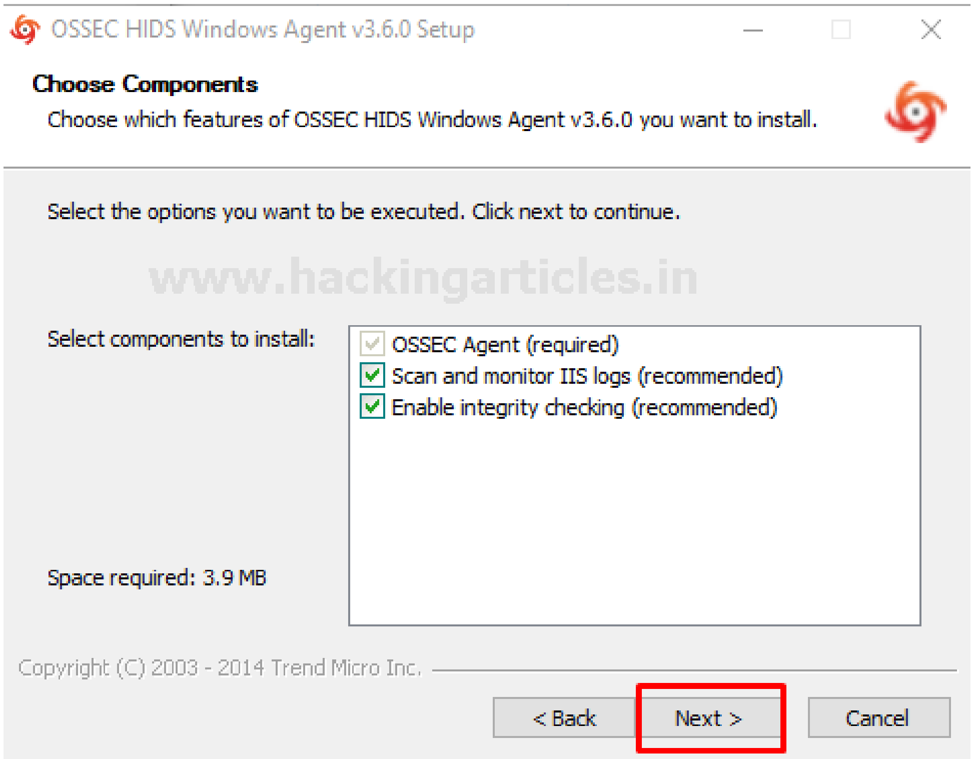
Presentation Slides

Contribute back!

Latest Stable Release (3.6.0)		Signature
Server/Agent Unix	ossec-hids-3.6.0.tar.gz – Release Notes	GPG Unix
Agent Windows	ossec-agent-win32-3.6.0.exe	GPG Windows
Chocolatey Package	ossec-client.3.3.0.nupkg	
Virtual Appliance	ossec-vm-2.9.3.ova – README	VA Checksum
Docker Container	atomicorp/ossec-docker	

Install OSSEC Agent

Go to the Downloads and run the OSSEC agent installer and hit next as shown below



OSSEC HIDS Windows Agent v3.6.0 Setup

Choose Components

Choose which features of OSSEC HIDS Windows Agent v3.6.0 you want to install.

Select the options you want to be executed. Click next to continue.

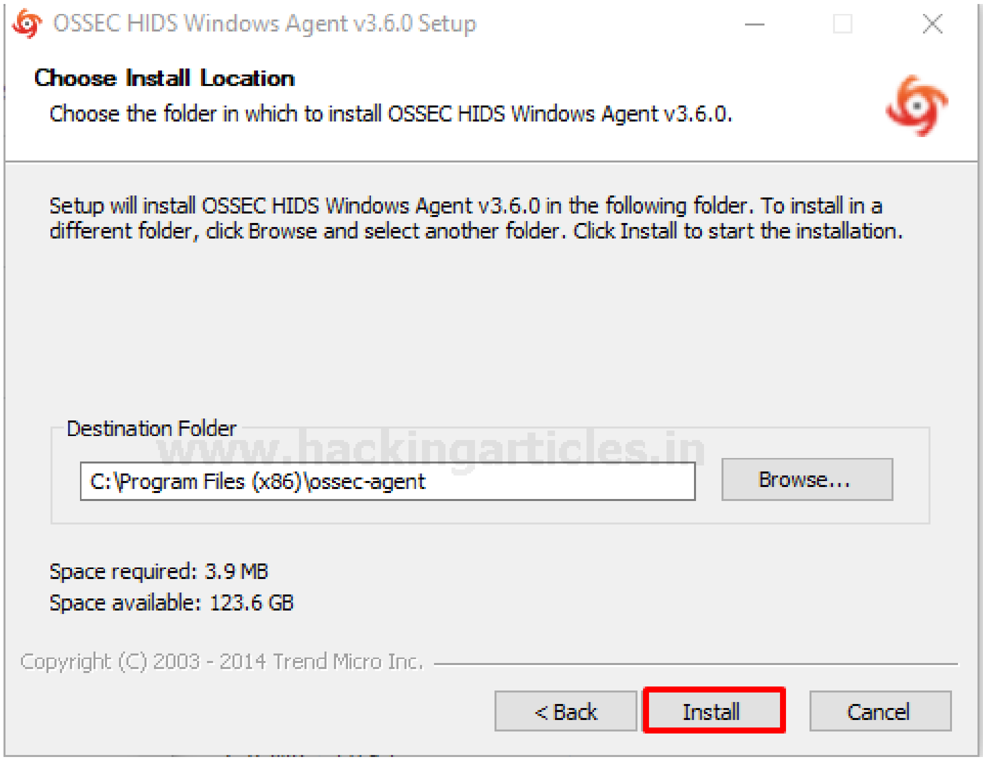
Select components to install:

☑ OSSEC Agent (required)
☑ Scan and monitor IIS logs (recommended)
☑ Enable integrity checking (recommended)

Space required: 3.9 MB

Copyright (C) 2003 - 2014 Trend Micro Inc.

Choose the path where you want to install the OSSEC agent and hit install


OSSEC HIDS Windows Agent v3.6.0 Setup

Choose Install Location

Choose the folder in which to install OSSEC HIDS Windows Agent v3.6.0.

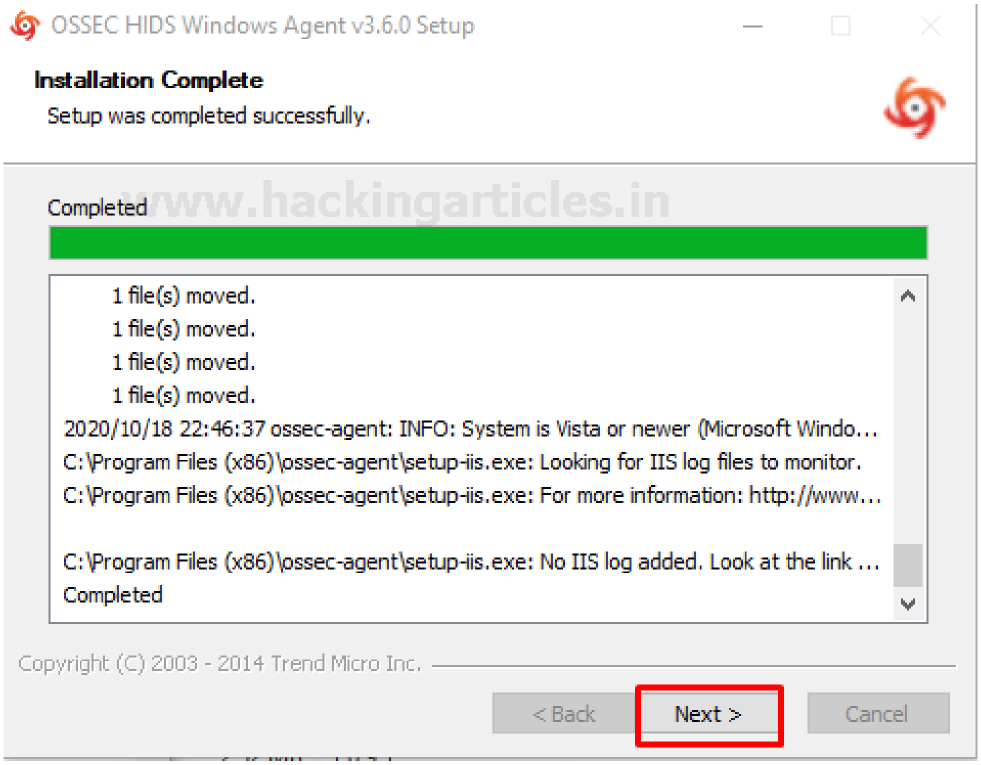
Setup will install OSSEC HIDS Windows Agent v3.6.0 in the following folder. To install in a different folder, click Browse and select another folder. Click Install to start the installation.

Destination Folder: C:\Program Files (x86)\ossec-agent

Space required: 3.9 MB
Space available: 123.6 GB

Copyright (C) 2003 - 2014 Trend Micro Inc.

Further, then wait for the setup completion and then hit next


OSSEC HIDS Windows Agent v3.6.0 Setup

Installation Complete

Setup was completed successfully.

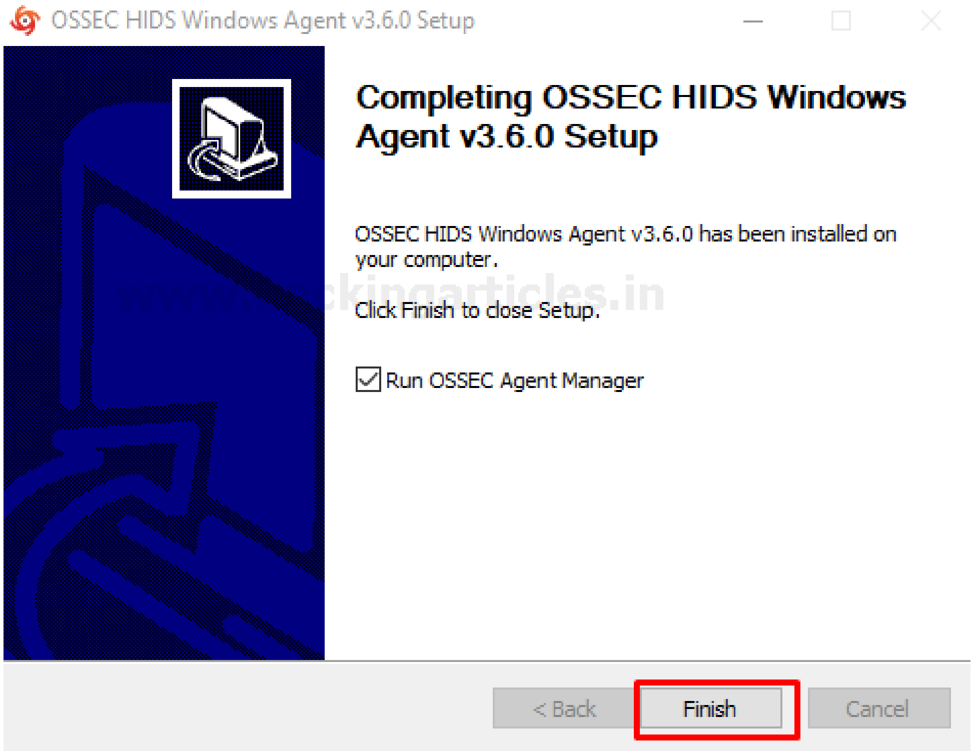
Completed

```
        1 file(s) moved.
        1 file(s) moved.
        1 file(s) moved.
        1 file(s) moved.
2020/10/18 22:46:37 ossec-agent: INFO: System is Vista or newer (Microsoft Windo...
C:\Program Files (x86)\ossec-agent\setup-iis.exe: Looking for IIS log files to monitor.
C:\Program Files (x86)\ossec-agent\setup-iis.exe: For more information: http://www...

C:\Program Files (x86)\ossec-agent\setup-iis.exe: No IIS log added. Look at the link ...
Completed
```

Copyright (C) 2003 - 2014 Trend Micro Inc.

Select finish and then exit from the installer.



OSSEC HIDS Windows Agent v3.6.0 Setup

Completing OSSEC HIDS Windows Agent v3.6.0 Setup

OSSEC HIDS Windows Agent v3.6.0 has been installed on your computer.

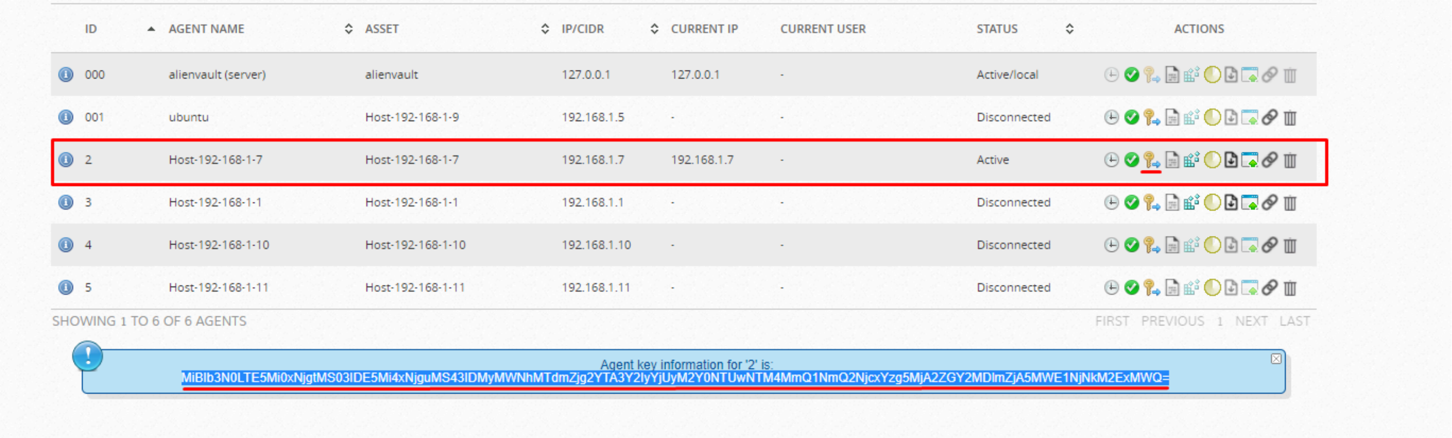
Click Finish to close Setup.

☑ Run OSSEC Agent Manager

Generate OSSEC key for the agent

Follow the steps as described below:

- At AlienVault Web UI go to “**Environment > Detection > HIDS”**
- Go to Agents (top right corner)
- Add a new agent
- Copy the key and use it at the agent as shown below



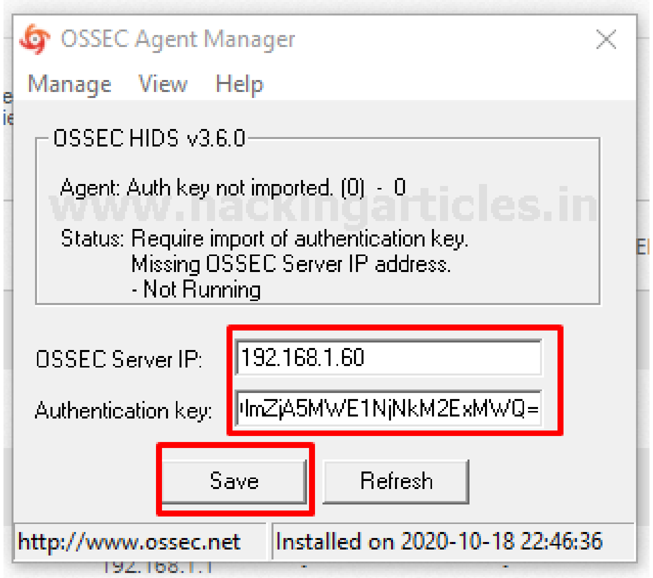
ID	AGENT NAME	ASSET	IP/CIDR	CURRENT IP	CURRENT USER	STATUS	ACTIONS
000	alienvault (server)	alienvault	127.0.0.1	127.0.0.1	-	Active/local	
001	ubuntu	Host-192-168-1-9	192.168.1.5	-	-	Disconnected	
2	Host-192-168-1-7	Host-192-168-1-7	192.168.1.7	192.168.1.7	-	Active	
3	Host-192-168-1-1	Host-192-168-1-1	192.168.1.1	-	-	Disconnected	
4	Host-192-168-1-10	Host-192-168-1-10	192.168.1.10	-	-	Disconnected	
5	Host-192-168-1-11	Host-192-168-1-11	192.168.1.11	-	-	Disconnected	

SHOWING 1 TO 6 OF 6 AGENTS

Agent key information for '2' is:
MiBIb3N0LTE5Mi0xNjgtMS03IDE5Mi4xNjguMS43IDMyMWNhMTdmZjg2YTA3Y2IyYjUyM2Y0NTUwNTM4MmQ1NmQ2NjcxYzg5MjA2ZGY2MDlmZjA5MWE1NjNkM2ExMWQ=

Come back to the windows machine

Enter the AlienVault server IP and paste the key as shown below



OSSEC HIDS v3.6.0

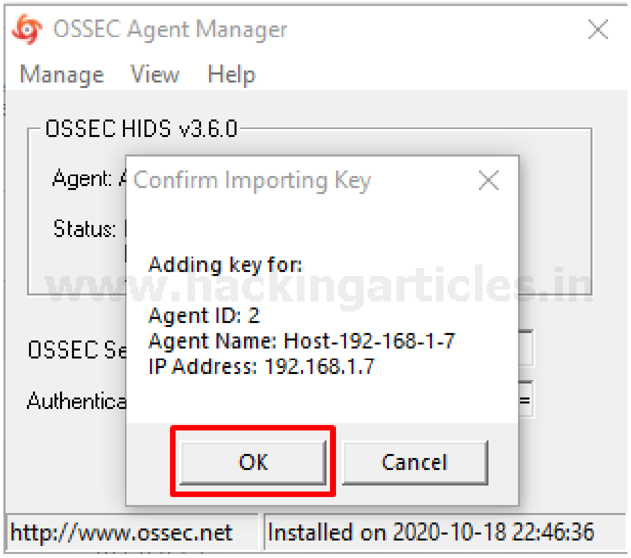
Agent: Auth key not imported. (0) - 0

Status: Require import of authentication key.
Missing OSSEC Server IP address.
- Not Running

OSSEC Server IP: 192.168.1.60

Authentication key: ImZjA5MWE1NjNkM2ExMWQ=

After that confirm agent deployment by pressing ok



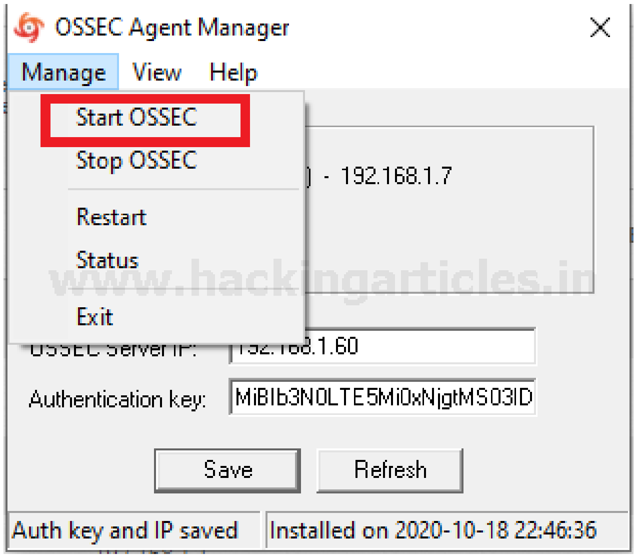
Confirm Importing Key

Adding key for:

Agent ID: 2
Agent Name: Host-192-168-1-7
IP Address: 192.168.1.7

Run and verify OSSEC agent is connected or running

After a successful deployment of OSSEC agent start service of OSSEC agent by navigating to "**Manage > Start OSSEC"** as shown below



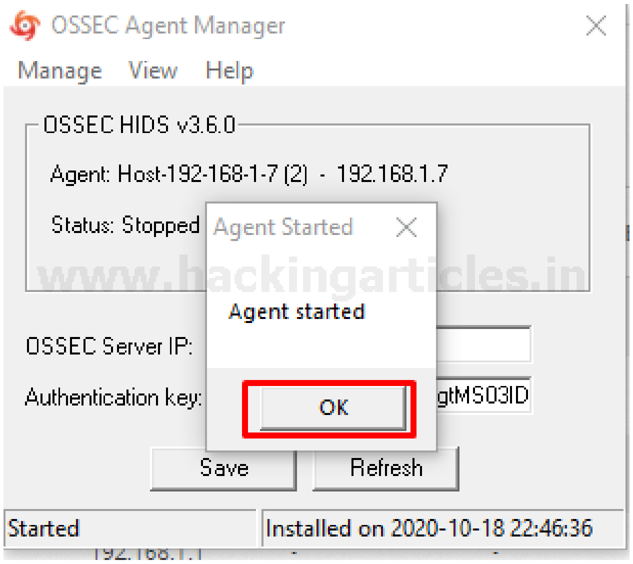
) - 192.168.1.7

OSSEC Server IP: 192.168.1.60

Authentication key: MiBIb3N0LTE5Mi0xNjgtMS03ID

Auth key and IP saved | Installed on 2020-10-18 22:46:36

As you can see the server is started successfully



OSSEC HIDS v3.6.0

Agent: Host-192-168-1-7 (2) - 192.168.1.7

Status: Stopped

Agent started

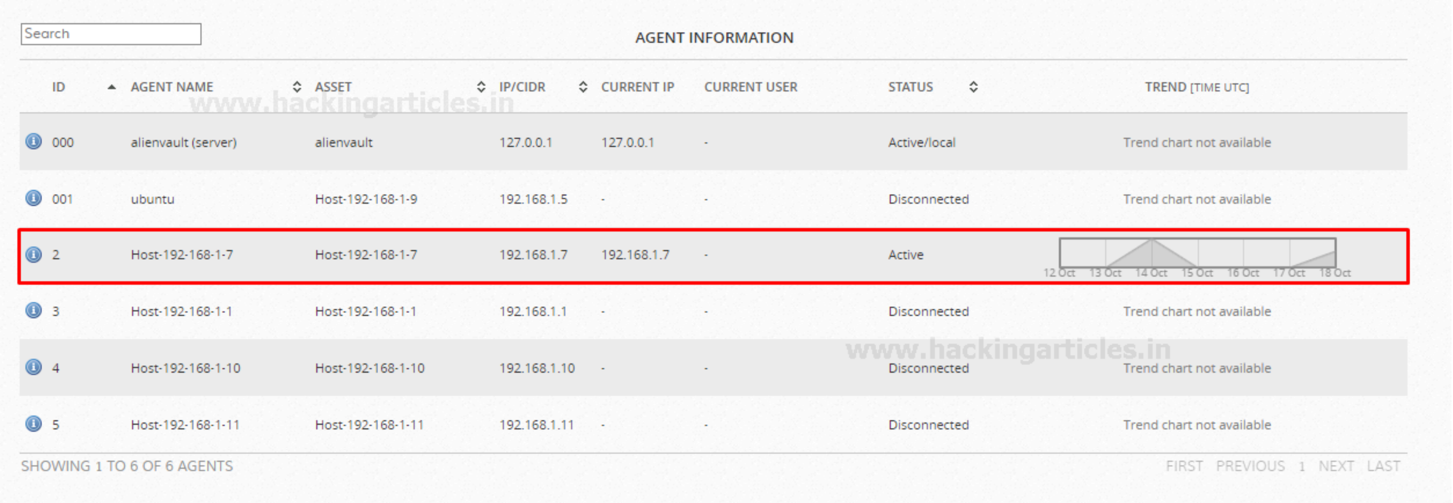
OSSEC Server IP:

Authentication key: gtMS03ID

Started | Installed on 2020-10-18 22:46:36

A new windows service can be found at OSSIM Web UI as shown below

Congratulation !!! you have successfully deployed your windows agent to the AlienVault server.



AGENT INFORMATION

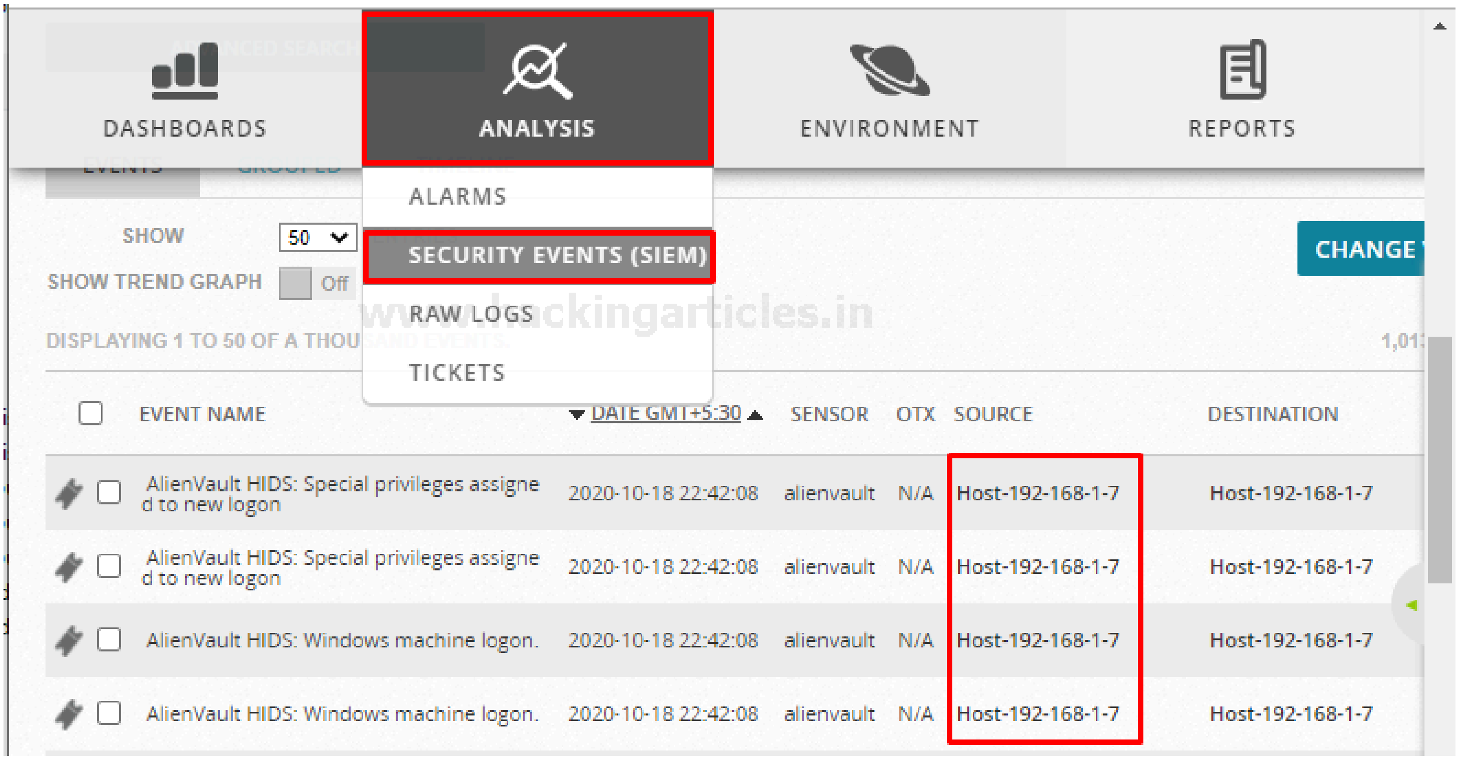
ID	AGENT NAME	ASSET	IP/CIDR	CURRENT IP	CURRENT USER	STATUS	TREND [TIME UTC]
000	alienvault (server)	alienvault	127.0.0.1	127.0.0.1	-	Active/local	Trend chart not available
001	ubuntu	Host-192-168-1-9	192.168.1.5	-	-	Disconnected	Trend chart not available
2	Host-192-168-1-7	Host-192-168-1-7	192.168.1.7	192.168.1.7	-	Active	
3	Host-192-168-1-1	Host-192-168-1-1	192.168.1.1	-	-	Disconnected	Trend chart not available
4	Host-192-168-1-10	Host-192-168-1-10	192.168.1.10	-	-	Disconnected	Trend chart not available
5	Host-192-168-1-11	Host-192-168-1-11	192.168.1.11	-	-	Disconnected	Trend chart not available

SHOWING 1 TO 6 OF 6 AGENTS

FIRST PREVIOUS 1 NEXT LAST

Hmm…

Let’s verify it checking the logs of windows machine it is processing or not by navigating to **“Analysis > Security Events (SIEM)”**



	EVENT NAME	DATE GMT+5:30	SENSOR	OTX	SOURCE	DESTINATION
□	AlienVault HIDS: Special privileges assigned to new logon	2020-10-18 22:42:08	alienvault	N/A	Host-192-168-1-7	Host-192-168-1-7
□	AlienVault HIDS: Special privileges assigned to new logon	2020-10-18 22:42:08	alienvault	N/A	Host-192-168-1-7	Host-192-168-1-7
□	AlienVault HIDS: Windows machine logon.	2020-10-18 22:42:08	alienvault	N/A	Host-192-168-1-7	Host-192-168-1-7
□	AlienVault HIDS: Windows machine logon.	2020-10-18 22:42:08	alienvault	N/A	Host-192-168-1-7	Host-192-168-1-7

Where 192.168.1.7 is my windows machine IP

As we can see the windows machine started sending the processing logs.

Hold tight! this is not enough…..

Have patience …

In this article, we explained the Deployment of the OSSEC agent to AlienVault OSSIM.

In the next article, our focus will be on the Threat Hunting, Malware analysis, network traffic monitoring, and much more…