Software Setup

Contents

Installing Git Bash (To execute the code).

1. Download the Git Bash setup from the official setup- https://git-scm.com/
2. Download the Installer.
3. Run the .exe file you just downloaded and follow the instructions in the installer.
4. Git Bash will be installed in the system. By right clicking you can run as an administrator.

Installing the Visual Studio Code (Source Code Editor):

1. Download the VS code from the link: https://code.visualstudio.com/download
2. Run the installer i.e., .exe file.
3. Follow the installation instructions and complete the installation process.
4. By default, it will be installed under this path: "**C:\username\AppData\Local\Programs\Microsoft VS Code**"
5. Check the path in the system variables under environment variables for any issues in the installation.

Installing the Python (Source Code):

1. Download the installer from the link: https://www.python.org/downloads/
2. Run the executable installer i.e., .exe file.
3. Once it is installed, check the version using the "python -version" command either in the command prompt or in the Git Bash.
4. Check the path in the system variables under environment variables for any issues in the installation.

Installing Git (Version Control System):

1. Navigate to the latest https://gitforwindows.org/ and download the latest version.
2. Once the .exe file is downloaded, follow the installation instructions as provided in the Git Setup wizard until the installation is complete.
3. Open the command prompt or Git Bash.

Installing OSSEC

Then we must download the latest version of the OSSEC from GitHub repository with the following command:

```
wget https://github.com/ossec/ossec-hids/archive/2.9.0.tar.gz
```

Once the download is completed, then extract the downloaded file with the following command:

```
tar -xvzf 2.9.0.tar.gz
```

Next, change the directory to the extracted directory, then run `install.sh` to install OSSEC:

```
cd ossec-hids-2.9.0
```

```
sh install.sh
```

Then we'll be prompted to answer some questions,

Select your language, if your language is English then type en and press Enter:

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

Then we'll see the following output:

```
OSSEC HIDS v2.9.0 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 Node1 4.4.0-45-generic
- User: root
- Host: localhost

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

Now press enter, and we'll see the following output:

1- What kind of installation do you want (server, agent, local, hybrid or help)? Local
Choose local to monitor the server it has been installed on then press Enter:

```
- Server installation chosen.

2- Setting up the installation environment.

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

Choose OSSEC install location and press Enter:

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

3- Configuring the OSSEC HIDS.

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

Type y and press Enter if you want to get e-mail notification:

```
- What's your e-mail address? root@localhost

- We found your SMTP server as: 127.0.0.1
- Do you want to use it? (y/n) [y]: y
```

Type your local e-mail address and press Enter:

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

Press Enter for integrity check daemon:

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

Press Enter for rootkit detection engine:

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

Press Enter to enable active response:

```
- Do you want to enable the firewall-drop response? (y/n) [y]:
     - firewall-drop enabled (local) for levels >= 6
```

Press Enter to enable the firewall-drop response:

```
- Default white list for the active response:
     - 192.168.15.1

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

Type `n` and press Enter if you don't want to add white list:

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

Press Enter to enable remote Syslog:

```
- 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 ---
```

Finally, Press Enter to start installation. Once the installation succeeds, you should see the following output:

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

- Configuration finished properly.
- To start OSSEC HIDS:
 /var/ossec/bin/ossec-control start

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

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

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). ---
- In order to connect agent and server, you need to add each agent to t
Run the 'manage_agents' to add or remove them:

/var/ossec/bin/manage_agents
```

Once the installation is completed, start OSSEC with the following command:

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

You should see the following output:

```
Starting OSSEC HIDS v2.9 (by Trend Micro Inc.)...
Started ossec-maild...
Started ossec-execd...
Started ossec-analysisd...
Started ossec-logcollector...
Started ossec-syscheckd...
Started ossec-monitord...
Completed.
```

Installing Splunk

sudo wget -O splunk-9.0.2-17e00c557dc1-Linux-x86_64.tgz https://download.splunk.com/products/splunk/releases/9.0.2/linux/splunk-9.0.2-17e00c557dc1-Linux-x86_64.tgz

tar xvzf file.tgz -C /opt

/opt/splunk/bin/splunk start --accept-license

Opening port 8000 for splunk since splunk is running on port 8000

```
firewall-cmd --zone=public --add-port=8000/tcp --permanent
firewall-cmd --reload
```

installing the splunk forward

```
$wget -O splunkforwarder-9.0.2-17e00c557dc1-Linux-x86_64.tgz
"https://download.splunk.com/products/universalforwarder/releases/9.0.2/linux/splunkforwarder-9.0.2-17e00c557dc1-Linux-x86_64.tgz"
$tar -xvzf splunkforwarder-9.0.2-17e00c557dc1-Linux-x86_64.tgz -C /opt/
$sudo /opt/splunkforwarder/bin/splunk start --accept-license
```

NOTE: 8089 already in use, so better use 8088

splunk has limit on disk space for root directory search not executed: The minimum free disk space (5000MB) reached for /opt/splunk/var/run/splunk/dispatch

If we get above error, then we need to change the limit as required in below path

```
$/opt/splunkforwarder/etc/system/default/server.conf
```

Enable the boot start

```
$/opt/splunkforwarder/bin/splunk enable boot-start
```

Add the Splunk IP where you want to forward the logs

```
$/opt/splunkforwarder/bin/splunk add forward-server 18.117.242.146:9997
```

Sending logs to splunk

```
$/opt/splunkforwarder/bin/splunk add monitor /etc/httpd/logs/access_log -index main
```

To check the above configuration

```
/opt/splunkforwarder/etc/apps/search/local/inputs.conf
```

Enable the forward ports

```
$firewall-cmd --zone=public --permanent --add-port=9997/tcp

$firewall-cmd --zone=public --permanent --add-port=9997/udp

$firewall-cmd --zone=public --permanent --add-port=8088/tcp

$firewall-cmd --zone=public --permanent --add-port=8088/udp
```

Add the IP on splunk

Follow the below

Settings -> Data -> Forwarding and Receiving -> Receive data

Click on "+ Add new" Button
Then add the 9997 port. Then restart the splunk and splunk global forwarder.

Delete the index data from the splunk UI

```
$index=main sourcetype=syslog | delete
```

After restart of the server.

1. Restart the spunk on splunk forwarder
2. Update the new IP

   ```
   $/opt/splunkforwarder/bin/splunk add forward-server 18.117.242.146:9997
   ```

3. Restart the splunk-on-splunk forwarder.

Get started with Amazon EC2 Linux/Ubuntu instances.

Step 1: Launch an instance

You can launch a Linux instance using the AWS Management Console as described in the following procedure.

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.

2. From the EC2 console dashboard, in the Launch instance box, choose Launch instance, and then choose Launch instance from the options that appear.

3. Under Name and tags, for Name, enter a descriptive name for your instance.

4. Under Application and OS Images (Amazon Machine Image), do the following:

- Choose Quick Start, and then choose Amazon Linux. This is the operating system (OS) for your instance.

- From Amazon Machine Image (AMI), select an HVM version of Amazon Linux 2. Notice that these AMIs are marked Free tier eligible. An Amazon Machine Image (AMI) is a basic configuration that serves as a template for your instance.

Under Instance type, from the Instance type list, you can select the hardware configuration for your instance. Choose the t2.micro instance type, which is selected by default. The t2.micro instance type is eligible for the free tier. In Regions where t2.micro is unavailable, you can use a t3.micro instance under the free tier. For more information, see AWS Free Tier.

5. Under Instance type, from the Instance type list, you can select the hardware configuration for your instance. Choose the t2.micro instance type, which is selected by default. The t2.micro instance type is eligible for the free tier. In Regions where t2.micro is unavailable, you can use a t3.micro instance under the free tier. For more information, see AWS Free Tier.

6. Under Key pair (login), for Key pair name, choose the key pair that you created when getting set up.

7. Next to Network settings, choose Edit. For Security group name, you'll see that the wizard created and selected a security group for you. You can use this security group, or alternatively you can select the security group that you created when getting set up using the following steps:

- Choose Select existing security group.
- From Common security groups, choose your security group from the list of existing security groups

8. Keep the default selections for the other configuration settings for your instance.

9. Review a summary of your instance configuration in the Summary panel, and when you're ready, choose Launch instance.

10. A confirmation page lets you know that your instance is launching. Choose View all instances to close the confirmation page and return to the console.

11. On the Instances screen, you can view the status of the launch. It takes a short time for an instance to launch. When you launch an instance, its initial state is pending. After the instance starts, its state changes to running and it receives a public DNS name. If the Public IPv4 DNS column is hidden, choose the settings icon ( ) in the top-right corner, toggle on Public IPv4 DNS, and choose Confirm.

12. It can take a few minutes for the instance to be ready for you to connect to it. Check that your instance has passed its status checks; you can view this information in the Status check column.

Step 2- Connect to your instance.

Step 3- Clean up your instance

After you've finished with the instance that you created for this tutorial, you should clean up by terminating the instance.

To terminate your instance-

1. In the navigation pane, choose Instances. In the list of instances, select the instance.

2. Choose Instance state, Terminate instance.

3. Choose Terminate when prompted for confirmation.

Amazon EC2 shuts down and terminates your instance. After your instance is terminated, it remains visible on the console for a short while, and then the entry is automatically deleted. You cannot remove the terminated instance from the console display yourself.

Installing PHP:

The Apache web server is among the most popular web servers in the world. It’s well documented, has an active community of users, and has been in wide use for much of the history of the web, which makes it a great choice for hosting a website.

Start by updating the package manager cache. If this is the first time you're using sudo within this session, you'll be prompted to provide your user's password to confirm you have the right privileges to manage system packages with apt:

Install Apache

You'll be prompted to confirm Apache's installation. Confirm by pressing Y, then ENTER.

Once the installation is finished, you'll need to adjust your firewall settings to allow HTTP traffic. Ubuntu's default firewall configuration tool is called Uncomplicated Firewall (UFW). It has different application profiles that you can leverage. To list all currently available UFW application profiles, execute this command:

Apt Setup:

1) grab the package from the web

wget http://security.ubuntu.com/ubuntu/pool/main/a/apt/apt_1.0.1ubuntu2.17_amd64.deb -O apt.deb

2) install it with dpkg

sudo dpkg -i apt.deb

Yum Repo Setup

Step 1- Upgrading the system

We have executed the upgrade command for getting the latest package information and updating package repositories:

1. $ sudo apt upgrade

Step 2- Install YUM

1. $ sudo apt-get install yum

Installing MySQL

Now that you have a web server up and running, you need to install the database system to be able to store and manage data for your site. MySQL is a popular database management system used within PHP environments.

Again, use apt to acquire and install this software:

```
$ sudo apt install mysql-server
```

When prompted, confirm installation by typing Y, and then ENTER.

When the installation is finished, it's recommended that you run a security script that comes pre-installed with MySQL. This script will remove some insecure default settings and lock down access to your database system.

Start the interactive script by running:

```
$ sudo mysql_secure_installation
```

This will ask if you want to configure the VALIDATE PASSWORD PLUGIN.

Answer Y for yes, or anything else to continue without enabling.

```
VALIDATE PASSWORD PLUGIN can be used to test passwords
and improve security. It checks the strength of password
and allows the users to set only those passwords which are
secure enough. Would you like to setup VALIDATE PASSWORD plugin?

Press y|Y for Yes, any other key for No:
```

If you answer “yes”, you’ll be asked to select a level of password validation. Keep in mind that if you enter 2 for the strongest level, you will receive errors when attempting to set any password which does not contain numbers, upper and lowercase letters, and special characters:

```
There are three levels of password validation policy:

LOW    Length >= 8
MEDIUM Length >= 8, numeric, mixed case, and special characters
STRONG Length >= 8, numeric, mixed case, special characters and dictionary

Please enter 0 = LOW, 1 = MEDIUM and 2 = STRONG: 1
```

If you enabled password validation, you’ll be shown the password strength for the root password you just entered and your server will ask if you want to continue with that password. If you are happy with your current password, enter Y for “yes” at the prompt:

When you’re finished, test whether you’re able to log in to the MySQL console by typing:

```
$ sudo mysql
```

This will connect to the MySQL server as the administrative database user **root**, which is inferred by the use of sudo when running this command. Below is an example output:

```
Output
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 10
Server version: 8.0.28-0ubuntu4 (Ubuntu)

Copyright (c) 2000, 2022, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

To exit the MySQL console, type:

```
mysql> exit
```

Libraries setup:

Install the libraries using the below commands.

pip install numpy

pip install pandas

pip install sklearn

pip install joblib

pip install matplotlib.pyplot

pip install flask

Docker Setup (Optional: To host the current environment as a container):

1. We are using the Docker Playground to host the docker containers.
2. We are using the Docker Hub to maintain the docker images (Our Python web application).

Simulation Setup

Setup the required software as mentioned above to run the code.

1. Git Bash
2. VS Code
3. Python
4. Git
5. Docker