How to install Suricata IDS on Rocky Linux

Suricata is a free and open source intrusion detection (IDS), intrusion prevention (IPS) and network security monitoring (NSM) tool for Linux.

Suricata is a free and open source intrusion detection (IDS), intrusion prevention (IPS) and network security monitoring (NSM) tool for Linux. It uses a set of signatures and rules to inspect and process network traffic. When suspicious packets are detected for any number of services on the server, they are immediately blocked.

By default, Suricata operates as a passive intrusion detection system, scanning traffic on the server for suspicious packets. However, you can also use it as a proactive intrusion prevention system (IPS) to log, report, and completely block network traffic that follows certain rules.

This tutorial will show you how to install Suricata IDS on your Rocky Linux server.

Request

1. Server running or 9
2. The root password is configured on the server.

Install Suricata on Rocky Linux

Suricata is not included in the default Rocky Linux repositories. So you need to install it from EPEL repository.

First, install the EPEL repository with the following command:

```
dnf install epel-release -y
```

Once EPEL is installed, check the Suricata package information with the following command:

```
dnf info suricata
```

You will get the following output:

```
Available Packages Name : suricata Version : 5.0.8 Release : 1.el8 Architecture
```

Next, install Suricata with the following command:

```
dnf install suricata -y
```

After successful installation, you can proceed to the next step.

Suricata configuration

Suricata contains many rules called signatures to detect threats. All rules are located in the **/etc/suricata/rules/ directory.**

Run the following command to list all rules:

```
ls /etc/suricata/rules/
```

You will get the following output:

```
app-layer-events.rules dnp3-events.rules http-events.rules modbus-events.rules sm
```

Next, run the following command to update all the rules:

```
suricata-update
```

You will get the following output:

```
19/9/2023 -- 05:28:15 - -- Loading distribution rule file /usr/share/suricata/ru
```

Next, edit the Suricata configuration file and specify your server IP, rule path, and network interface:

```
nano /etc/suricata/suricata.yaml
```

Change the following lines:

```
 #HOME_NET: "[192.198.0.0/19,10.0.0.0/8,172.19.0.0/12]" HOME_NET: "[192.198.1.48]
```

Save and close the file when you're done and turn off the offload feature with the following command:

```
ethtool -K eth0 gro off lro off
```

Manage Suricata service

Next, start the Suricata service and enable it with the following command so that it opens when the system is restarted:

```
systemctl start suricata systemctl enable suricata
```

You can check the status of Suricata with the following command:

```
systemctl status suricata
```

You will get the following output:

```
? suricata.service - Suricata Intrusion Detection Service Loaded: loaded (/usr/li
```

To check the Suricata process log, run the following command:

```
tail /var/log/suricata/suricata.log
```

You will see the following output:

```
19/9/2023 -- 10:06:23 - - Running in live mode, activating unix socket 19/9/2023
```

You can check the Suricata warning log with the following command:

```
tail -f /var/log/suricata/fast.log
```

You will see the following output:

```
19/19/2022-10:06:23.059177 [**] [1:2402000:6215] ET DROP Dshield Block Listed Sou
```

To check the Suricata statistics log, use the following command:

```
tail -f /var/log/suricata/stats.log
```

You will see the following output:

```
------------------------------------------------------------------------------
```

Test Suricata IDS

After installing Suricata IDS, you also need to check whether Suricata IDS works or not. To do this, log in to another system and install the hping3 utility to perform a DDoS attack.

```
dnf install hping3
```

After installing hping3, run the following command to perform a DDoS attack:

```
hping3 -S -p 22 --flood --rand-source suricata-ip
```

Now go to the Suricata system and check the warning log with the following command:

```
tail -f /var/log/suricata/fast.log
```

You will see the following output:

```
09/19/2023-10:08:18.049526 [**] [1:2403393:73004] ET CINS Active Threat Intellig
```