Guide on Installing Snort on Kali

Why Snort?

“Snort is the foremost Open Source Intrusion Prevention System (IPS) in the world. Snort IPS uses a series of rules that help define malicious network activity and uses those rules to find packets that match against them and generates alerts for users.” https://www.snort.org/

1.Try first to install snort by typing *sudo apt install snort* command in your terminal:

```
┌──
└─$ sudo apt install snort
```

If you run an older Kali version this may work. On newer versions of Kali it won’t work, because snort is not included in the Kali repositories.

However, snort is included in Ubuntu repositories.

The solution to installing snort on Kali is to use the Ubuntu repositories.

Repositories are the servers that hold software for a particular Linux distro (eg Kali, Ubuntu). The repositories your system will search for software are stored in the *sources.list* configuration file.

To view the repositories on your Kali system:

```
└─$ nl /etc/apt/sources.list
```

Note: On line 2 is the Kali default repo and after that on line 3 (a comment) for additional repos

2.Try to add Debian repo to the list of Kali repositories by editing the sources.list file. (read more at https://wiki.debian.org/DebianRepository)

Steps:

Open sources.list with your editor (eg mousepad)

```
┌──
└─$ sudo mousepad /etc/apt/sources.list
```

Then append the following line (Debian repo) after the default Kali repo (say, on line 6):

deb http://ftp.debian.org/debian stable main contrib non-free

Save and close mousepad.

Then run update:

```
┌──
└─$ sudo apt update
```

Now try again to install snort by typing *sudo apt install snort* command in your terminal:

```
┌──
└─$ sudo apt install snort
```

Note: This may work on some newer Kali since both Kali and Ubuntu are Debian-based Linux distributions (but not for Kali 2023). If it worked, you can check what version of snort is installed by typing the command:

```
┌──
└─$ snort  --version
```

Note: If you installed snort, you may want to go back to the sources.list file and comment (add #) in front of the added line.

3. If 1 and 2 did not work, you will need to use Ubuntu repositories.

Step1: Make a backup copy of sources.list file:

```
└─$ sudo mv /etc/apt/sources.list   /etc/apt/sources.list.bak
```

Note that .bak extension allows to retrieve the original sources.list after completing snort installation

Step 2: Remove updates:

```
└─$ find /var/lib/apt/lists -type f -exec rm {} \;
```

Step 3: Open sources.list file with your editor (eg mousepad)

```
┌──
└─$ sudo mousepad /etc/apt/sources.list
```

Then paste following Ubuntu repos:

```
deb http://archive.ubuntu.com/ubuntu/ focal main restricted universe multiverse<br>
deb-src http://archive.ubuntu.com/ubuntu/ focal main restricted universe multiverse<br>

deb http://archive.ubuntu.com/ubuntu/ focal-updates main restricted universe multiverse<br>
deb-src http://archive.ubuntu.com/ubuntu/ focal-updates main restricted universe multiverse<br>
```

```
deb http://archive.ubuntu.com/ubuntu/ focal-security main restricted universe multiverse<br>
deb-src http://archive.ubuntu.com/ubuntu/ focal-security main restricted universe multiverse<br>

deb http://archive.ubuntu.com/ubuntu/ focal-backports main restricted universe multiverse<br>
deb-src http://archive.ubuntu.com/ubuntu/ focal-backports main restricted universe multiverse<br>

deb http://archive.canonical.com/ubuntu focal partner<br>
deb-src http://archive.canonical.com/ubuntu focal partner<br>
```

Save and close the mousepad.

Step 4. Add the specified public keys:

```
└─$ sudo apt-key adv --keyserver keyserver.ubuntu.com --recv-keys 3B4FE6ACC0B21F32
```

```
└─$ sudo apt-key adv --keyserver keyserver.ubuntu.com --recv-keys 871920D1991BC93C
Warning: apt-key is deprecated. Manage keyring files in trusted.gpg.d instead (see apt-key(8)).
```

Step 5:

```
└─$ sudo apt update
```

Step 6: Try now installing snort:

```
└─$ sudo apt install snort -y
```

Note: Now it will work – see:

```
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libdaq2 libestr0 libfastjson4 oinkmaster rsyslog snort-common
  snort-common-libraries snort-rules-default
```

Note: If you check the snort version it is (2.9.7.0) not the latest one, but there you have it:

```
└─$ snort  --version
```

Step 7: **You will need to restore default Kali repositories.** Follow the steps below:

Go to folder:

```
└─$ cd /var/lib/apt/lists

└─$ ls
```

You will see:

```
archive.canonical.com_ubuntu_dists_focal_InRelease
archive.ubuntu.com_ubuntu_dists_focal-backports_Contents-amd64.lz4
archive.ubuntu.com_ubuntu_dists_focal-backports_InRelease
archive.ubuntu.com_ubuntu_dists_focal-backports_main_binary-amd64_Packages
```

You will need to remove all Ubuntu files:

```
──(kaliadmin㉿kali)-[/var/lib/apt/lists]
└─$ rm archive*
```

The auxfiles and partial directory remains. Next we want now to bring the Kali sources.list back file:

```
└─$ sudo mv /etc/apt/sources.list.bak  /etc/apt/sources.list
```

Go home:

```
└─$ cd ~
```

Then apt update:

```
└─$ sudo apt update
```

Note: You can now try to open sources.list file to see that your default Kali repositories are back:

```
└─$ sudo mousepad /etc/apt/sources.list
```

4. Alternative Solution: Install Suricata

”Suricata is a high performance, open source network analysis and threat detection software used by most private and public organizations, and embedded by major vendors to protect their assets.” https://suricata.io/

```
└─$ sudo apt install suricata
```