Zeek Log Collector Installation Guide

Table of Contents

1. Introduction

Zeek (formerly known as Bro) is an open-source network monitoring tool that captures network traffic and generates detailed logs.
In this guide, we will walk through the steps to install a Zeek log collector on an Ubuntu system.

2. Prerequisites

Before proceeding with the installation, ensure the following prerequisites are met:
- A clean Ubuntu installation (preferably Ubuntu 20.04 LTS or higher).
- A user account with sudo privileges.
- Internet access to download dependencies and Zeek packages.

3. Step 1: System Update

Start by updating your system’s package index and upgrading all installed packages.

```
sudo apt update && sudo apt upgrade -y
```

4. Step 2: Installing Required Dependencies

Zeek requires several dependencies to be installed. Use the following command to install them:

```
sudo apt install cmake make gcc g++ flex bison libpcap-dev libssl-dev python3-dev swig zlib1g-dev -y
```

Optional: Installing GDB for Debugging

```
sudo apt install gdb -y
```

5. Step 3: Installing Zeek

### 5.1 Downloading Zeek

Navigate to the official Zeek download page and get the latest release, or use the following command to download and extract the tarball:

```
wget https://download.zeek.org/zeek-4.2.0.tar.gz
tar -xvzf zeek-4.2.0.tar.gz
cd zeek-4.2.0
```

### 5.2 Building and Installing Zeek

Use the following commands to build Zeek from the source:

```
./configure
make
sudo make install
```

6. Step 4: Configuring Zeek

6.1 Adding Zeek to PATH

To use the zeekctl command, add Zeek to your system's PATH:

```
echo "export PATH=/usr/local/zeek/bin:$PATH" >> ~/.bashrc
```

```
source ~/.bashrc
```

6.2 Initializing Zeek

Initialize Zeek using the following commands:

```
sudo /usr/local/zeek/bin/zeekctl deploy
```

7. Step 5: Running Zeek

Start the Zeek service to begin capturing network traffic and logging it:

```
sudo zeekctl start
```

To check the status of Zeek:

```
sudo zeekctl status
```

8. Step 6: Accessing Zeek Logs

Zeek generates logs that can be accessed at the following location:

```
/opt/zeek/logs/current/
```

9. Step 7: Automating Zeek Log Collection

9.1 Setting up a Cron Job

Open the crontab file for editing:

```
crontab -e
```

Add the following line to schedule log rotation and collection every day at midnight:

```
0 0 * * * /usr/local/zeek/bin/zeekctl cron
```

10. Conclusion

You have successfully installed and configured Zeek as a log collector on your Ubuntu system. By automating the log collection process, you can continuously monitor network traffic for security and performance insights.