Zeek (formerly Bro) - Network Security Monitoring Tool

- **Network Traffic Analysis –** Zeek monitors and logs network activity for security analysis.
- **Deep Packet Inspection –** Extracts detailed metadata from network packets.
- **Flexible Scripting –** Uses Zeek scripting language for custom security policies.
- **Protocol Detection –** Supports HTTP, DNS, SSL/TLS, and many more.
- **Security Event Detection** – Identifies anomalies, intrusions, and threats.
- **Log Generation –** Creates structured logs for further analysis in SIEMs.
- **Open Source & Scalable –** Used in large-scale network monitoring setups.

The apt-get update command updates the local package index by fetching the latest package lists from the repositories. This ensures the system is aware of available updates but does not install them.

```
root@agent:/home/lokesh# apt-get update
Get:1 http://security.ubuntu.com/ubuntu jammy-security InRelease [129 kB]
Hit:2 http://archive.ubuntu.com/ubuntu jammy InRelease
Get:3 http://archive.ubuntu.com/ubuntu jammy-updates InRelease [128 kB]
.
.
```

The apt-get upgrade command installs the latest versions of all installed packages without removing any existing ones. It updates only those packages that do not require dependency changes.

```
root@agent:/home/lokesh# apt-get upgrade
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
.
.
```

Downloading zeek-7.0.5.tar.gz zip file from zeek official website

```
root@agent:/home/lokesh# wget https://download.zeek.org/zeek-7.0.5.tar.gz
--2025-02-28 07:44:33--  https://download.zeek.org/zeek-7.0.5.tar.gz
Resolving download.zeek.org (download.zeek.org)... 52.84.45.124, 52.84.45.34, 52.84.45.68, ...
Connecting to download.zeek.org (download.zeek.org)|52.84.45.124|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 95847393 (91M) [application/x-gzip]
Saving to: ‘zeek-7.0.5.tar.gz’

zeek-7.0.5.tar.gz
100%[=============================================================================
=========================================>]  91.41M  3.79MB/s    in 25s


root@agent:/home/lokesh# ls
wazuh-agent_4.9.2-1_amd64.deb  zeek-7.0.5.tar.gz
```

use the following commands to add zeek repository into binary packages.

```
root@agent:/home/lokesh# apt-get install cmake make gcc g++ flex bison libpcap-dev libssl-dev
python3-dev swig zlib1g-dev -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
```

Extract zeek-7.0.5.tar.gz

```
root@agent:/home/lokesh# tar -xzf zeek-7.0.5.tar.gz
root@agent:/home/lokesh# ls
wazuh-agent_4.9.2-1_amd64.deb  zeek-7.0.5  zeek-7.0.5.tar.gz
```

Go to zeek-7.0.5

```
root@agent:/home/lokesh# cd zeek-7.0.5
root@agent:/home/lokesh/zeek-7.0.5# ls
CHANGES           Makefile   auxil           doc           src
CMakeLists.txt    NEWS       ci              docker        testing
COPYING           README     cmake           man           vcpkg.json
COPYING-3rdparty  README.md  cmake_templates  repo-info.json  zeek-path-dev.in
INSTALL           VERSION    configure       scripts
```

The ./configure command checks system dependencies and prepares the build environment for compiling Zeek 7.0.5.

```
root@agent:/home/lokesh/zeek-7.0.5# ./configure
.
.
-- Configuring done
-- Generating done
-- Build files have been written to: /home/lokesh/zeek-7.0.5/build
```

The command make install compiles and installs Zeek 7.0.5 from source in the /home/lokesh/zeek-7.0.5 directory on the agent system.

```
root@agent:/home/lokesh/zeek-7.0.5# make install
.
.
-- Installing: /usr/local/zeek/share/zeek/cmake/ZeekConfigVersion.cmake
-- Installing: /usr/local/zeek/share/zeek/cmake/ZeekTargets.cmake
make[1]: Leaving directory '/home/lokesh/zeek-7.0.5/build'
```

The command `make` compiles the Zeek 7.0.5 source code in the `/home/lokesh/zeek-7.0.5` directory on the `agent` system.

```
root@agent:/home/lokesh/zeek-7.0.5# make
.
.

[100%] Built target rst
make[2]: Leaving directory '/home/lokesh/zeek-7.0.5/build'
make[1]: Leaving directory '/home/lokesh/zeek-7.0.5/build'
root@agent:/home/lokesh/zeek-7.0.5#
```

Go to /usr/local/zeek/

```
root@agent:/home/lokesh/zeek-7.0.5# cd /usr/local/zeek/
root@agent:/usr/local/zeek# ls
bin  etc  include  lib  logs  share  spool  var
root@agent:/usr/local/zeek# cd bin
root@agent:/usr/local/zeek/bin#
```

Edit the Bash configuration file for the current user.

```
root@agent:/usr/local/zeek/bin# nano ~/.bashrc
.
.
export PATH=/usr/local/zeek/bin:$PATH #Add this line at last
```

The command source ~/.bashrc reloads the .bashrc file without needing to restart the shell. This applies any changes made, such as new aliases, environment variables, or custom configurations, immediately.

```
root@agent:/usr/local/zeek/bin# source ~/.bashrc
```

Check whether zeek is deployed

```
root@agent:/usr/local/zeek/bin# zeek --version
zeek version 7.0.5
```

Check where zeek installed

```
root@agent:/usr/local/zeek/bin# which zeek
/usr/local/zeek/bin/zeek
root@agent:/usr/local/zeek/bin# cd ..
root@agent:/usr/local/zeek# cd etc
root@agent:/usr/local/zeek/etc#

root@agent:/usr/local/zeek/etc# ls
networks.cfg  node.cfg  zeekctl.cfg  zkg
```

Edit node.cfg make sure to use standalone , localhost , ethernet of local machine where zeek is hosting

root@agent:/usr/local/zeek/etc# nano node.cfg
[zeek]
type=standalone
host=localhost
interface=eth0

```
root@agent:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
17: eth0@if18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 00:16:3e:09:fc:b3 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.189.151.4/24 metric 100 brd 10.189.151.255 scope global dynamic eth0
       valid_lft 3147sec preferred_lft 3147sec
    inet6 fd42:71c6:d70c:1045:216:3eff:fe09:fcb3/64 scope global mngtmpaddr noprefixroute
       valid_lft forever preferred_lft forever
    inet6 fe80::216:3eff:fe09:fcb3/64 scope link
       valid_lft forever preferred_lft forever
```

zeekctl check verifies Zeek’s configuration for errors before deployment.

root@agent:/usr/local/zeek/etc# zeekctl check
Hint: Run the zeekctl "deploy" command to get started.
zeek scripts are ok.

root@agent:/usr/local/zeek/spool# apt-get install mailutils -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done

Deploy zeek

root@agent:/usr/local/zeek/etc# zeekctl deploy
checking configurations ...
installing ...
removing old policies in /usr/local/zeek/spool/installed-scripts-do-not-touch/site ...
removing old policies in /usr/local/zeek/spool/installed-scripts-do-not-touch/auto ...
creating policy directories ...
installing site policies ...
generating standalone-layout.zeek ...
generating local-networks.zeek ...
generating zeekctl-config.zeek ...
generating zeekctl-config.sh ...
stopping ...

stopping zeek ...
starting ...
starting zeek …

zeekctl status displays the current status of Zeek processes (running, stopped, or crashed).

```
root@agent:/usr/local/zeek/etc# zeekctl status
Name         Type       Host          Status    Pid    Started
zeek         standalone localhost     running   29477  28 Feb 11:17:04
```

Go to logs that captured by zeek

```
root@agent:/usr/local/zeek/etc# cd ..
root@agent:/usr/local/zeek# ls
bin  etc  include  lib  logs  share  spool  var
root@agent:/usr/local/zeek# cd logs/
root@agent:/usr/local/zeek/logs# ls
2025-02-28  current

root@agent:/usr/local/zeek/logs# cd current
```

These all are different logs that generated by zeek

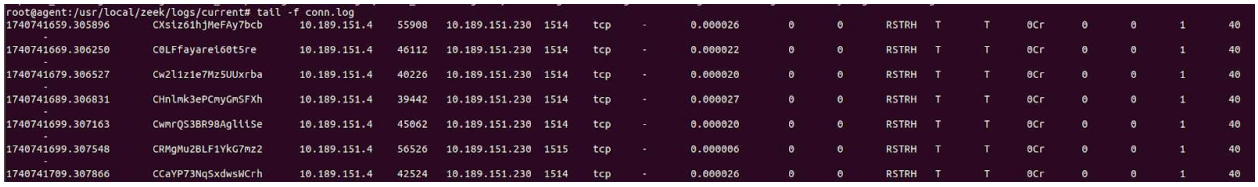
```
root@agent:/usr/local/zeek/logs/current# ls
capture_loss.log  conn.log  loaded_scripts.log  notice.log  packet_filter.log  reporter.log  stats.log
stderr.log  stdout.log  telemetry.log  weird.log
```

- **capture_loss.log –** Records packet loss statistics to detect missing network traffic.
- **conn.log –** Logs details of all network connections observed by Zeek.
- **loaded_scripts.log –** Lists all Zeek scripts loaded during execution.
- **notice.log –** Contains security-related alerts and notable network events.
- **packet_filter.log –** Logs information about packet filtering applied by Zeek.
- **reporter.log –** Stores warnings, errors, and debug messages from Zeek.
- **stats.log –** Captures Zeek's performance and resource usage statistics.
- **stderr.log –** Records errors and diagnostic messages from Zeek’s standard error output.
- **stdout.log –** Contains general runtime messages from Zeek’s standard output.
- **telemetry.log –** Logs detailed network telemetry data for analysis.
- **weird.log –** Tracks unusual or unexpected network behavior detected by Zeek.

Printing to the screen conn.log

In Zeek, conn.log is a foundational log file that tracks network connections, providing information about the source and destination hosts, ports, protocols, and connection state, allowing for analysis of network traffic and detection of unusual activity.

root@agent:/usr/local/zeek/logs/current# tail -f conn.log



root@agent:~# nano /usr/local/zeek/share/zeek/site/local.zeek
@load policy/tuning/json-logs.zeek
@load IP_Rep.zeek

root@agent:~# zeekctl deploy
checking configurations ...
installing ...
removing old policies in /usr/local/zeek/spool/installed-scripts-do-not-touch/site ...
removing old policies in /usr/local/zeek/spool/installed-scripts-do-not-touch/auto ...
creating policy directories ...
installing site policies ...
generating standalone-layout.zeek ...
generating local-networks.zeek ...
generating zeekctl-config.zeek ...
generating zeekctl-config.sh ...
stopping ...
stopping zeek ...
creating crash report for previously crashed nodes: zeek
starting ...
starting zeek ...

root@agent:~# zeekctl status
Name Type Host Status Pid Started
zeek standalone localhost running 1924 30 Mar 19:28:06

Make sure that the logs are now in json format

```
root@agent:~# tail -f /usr/local/zeek/logs/current/conn.log
{"ts":1743363640.639459,"uid":"C1oVyf20pa4f7qAtv2","id.orig_h":"10.189.151.4","id.orig_p":43130,"
id.resp_h":"10.189.151.230","id.resp_p":1514,"proto":"tcp","conn_state":"OTH","local_orig":true,"
local_resp":true,"missed_bytes":0,"history":"Cc","orig_pkts":0,"orig_ip_bytes":0,"resp_pkts":0,"r
esp_ip_bytes":0,"ids_malicious":"zeek_conn"}
{"ts":1743363650.653423,"uid":"CHhvKe3dqV9wZ0h3sf","id.orig_h":"10.189.151.4","id.orig_p":43130,"
id.resp_h":"10.189.151.230","id.resp_p":1514,"proto":"tcp","conn_state":"OTH","local_orig":true,"
local_resp":true,"missed_bytes":0,"history":"Cc","orig_pkts":0,"orig_ip_bytes":0,"resp_pkts":0,"r
esp_ip_bytes":0,"ids_malicious":"zeek_conn"}
{"ts":1743363660.663586,"uid":"C6ZZwA2Uc8X6nZvRfg","id.orig_h":"10.189.151.4","id.orig_p":43130,"
id.resp_h":"10.189.151.230","id.resp_p":1514,"proto":"tcp","conn_state":"OTH","local_orig":true,"
local_resp":true,"missed_bytes":0,"history":"Cc","orig_pkts":0,"orig_ip_bytes":0,"resp_pkts":0,"r
esp_ip_bytes":0,"ids_malicious":"zeek_conn"}
```

In the endpoint where zeek deployed, changed the json default scope separator to _ . If we dont do this, opensearch will fail to save them to the indices.

root@agent:~# nano /usr/local/zeek/share/zeek/base/frameworks/logging/main.zeek

.

.

```
    #const default_scope_sep = "." &redef;
    const default_scope_sep = "_" &redef;
```

.

.

To see updated changes

root@agent:~# zeekctl deploy
checking configurations ...
installing ...
removing old policies in /usr/local/zeek/spool/installed-scripts-do-not-touch/site ...
removing old policies in /usr/local/zeek/spool/installed-scripts-do-not-touch/auto ...
creating policy directories ...
installing site policies ...
generating standalone-layout.zeek ...
generating local-networks.zeek ...
generating zeekctl-config.zeek ...
generating zeekctl-config.sh ...
stopping ...
stopping zeek ...
starting ...
starting zeek ...

Make sure that the field separator is _ instead of . (for eg. id_orig_h instead of id.orig_h)

root@agent:/usr/local/zeek/logs/current# tail -f conn.log
root@agent:~# tail -f /usr/local/zeek/logs/current/conn.log
{"ts":1743363860.520436,"uid":"CaH8Rc238dkFpRKTg","id_orig_h":"10.189.151.4","id_orig_p":43130,"id_resp_h":"10.189.151.230","id_resp_p":1514,"proto":"tcp","conn_state":"OTH","local_orig":true,"local_resp":true,"missed_bytes":0,"history":"Cc","orig_pkts":0,"orig_ip_bytes":0,"resp_pkts":0,"resp_ip_bytes":0,"ids_malicious":"zeek_conn"}
{"ts":1743363870.531438,"uid":"CWvyK31IMh9XQxEv3g","id_orig_h":"10.189.151.4","id_orig_p":43130,"id_resp_h":"10.189.151.230","id_resp_p":1514,"proto":"tcp","conn_state":"OTH","local_orig":true,"local_resp":true,"missed_bytes":0,"history":"Cc","orig_pkts":0,"orig_ip_bytes":0,"resp_pkts":0,"resp_ip_bytes":0,"ids_malicious":"zeek_conn"}
{"ts":1743363880.544493,"uid":"CUxkEM1OOVosqJNXig","id_orig_h":"10.189.151.4","id_orig_p":43130,"id_resp_h":"10.189.151.230","id_resp_p":1514,"proto":"tcp","conn_state":"OTH","local_orig":true,"local_resp":true,"missed_bytes":0,"history":"Cc","orig_pkts":0,"orig_ip_bytes":0,"resp_pkts":0,"resp_ip_bytes":0,"ids_malicious":"zeek_conn"}