Zeek Network Security Monitor Installation and Verification Report

Project Type: Zeek Installation and Initial Validation

Prepared by: Niknaz Sadehvandi

Role: Founder & Cybersecurity Consultant

Organization: NS Cybersecurity

Date: December 2024

System: Ubuntu 24.04.3 LTS (Noble)
Environment: Oracle VirtualBox (Linux VM)

1. Objective

The objective of this lab was to install and verify **Zeek Network Security Monitor** on an Ubuntu 24.04 system.
Zeek is a widely used network analysis framework in SOC environments for traffic inspection, protocol analysis, and security monitoring.

This lab demonstrates:

- Proper repository and key configuration
- Successful Zeek installation
- Functional verification of Zeek analyzers

2. System Information

The system was verified prior to installation to ensure compatibility.

Command used:

lsb_release -a

Result:

- Distributor ID: Ubuntu
- Description: Ubuntu 24.04.3 LTS
- Codename: noble

📸 *Screenshot 1: OS verification (lsb_release -a)*

3. Zeek Repository and GPG Key Setup

Since Zeek is not included in the default Ubuntu repositories, the official **OpenSUSE Zeek repository** was added.

3.1 GPG Key Download and Installation

The repository signing key was downloaded and verified.

Commands used:

curl -fsSL https://download.opensuse.org/repositories/security:/zeek/xUbuntu_24.04/Release.key -o /tmp/zeek-release.key

head -n 5 /tmp/zeek-release.key

sudo gpg --dearmor -o /etc/apt/trusted.gpg.d/zeek.gpg /tmp/zeek-release.key

The presence of a valid **PGP public key block** confirmed authenticity.

📸 *Screenshot 2: Zeek GPG key verification and installation*

3.2 Repository Configuration

The Zeek repository was added to the APT sources list.

Command used:

echo "deb http://download.opensuse.org/repositories/security:/zeek/xUbuntu_24.04/ /" | sudo tee /etc/apt/sources.list.d/zeek.list

Repository configuration was validated by displaying the file.

📸 *Screenshot 3: Zeek repository configuration (zeek.list)*

4. Package Update and Installation

After repository setup, package lists were refreshed.

Command used:

sudo apt update

The Zeek repository was successfully contacted during the update process.

📸 *Screenshot 4: Successful apt update with Zeek repository*

Zeek was then installed using APT.

sudo apt install zeek -y

5. Zeek Installation Verification

5.1 Binary Location and Version

Zeek installs under /opt/zeek/bin.

Command used:

/opt/zeek/bin/zeek --version

Result:

zeek version 8.0.4

This confirms a successful installation of Zeek.

5.2 Analyzer and Plugin Verification

To validate runtime functionality, Zeek's built-in analyzers were listed.

Command used:

/opt/zeek/bin/zeek -N

The output displayed numerous built-in protocol analyzers including:

- TCP, UDP, SSL/TLS
- DNS, HTTP, SSH
- SMB, X509, VLAN, VXLAN
- SQLite storage and event streaming modules

📸 *Screenshot 5: Zeek analyzer list (zeek -N)*

6. Results and Validation

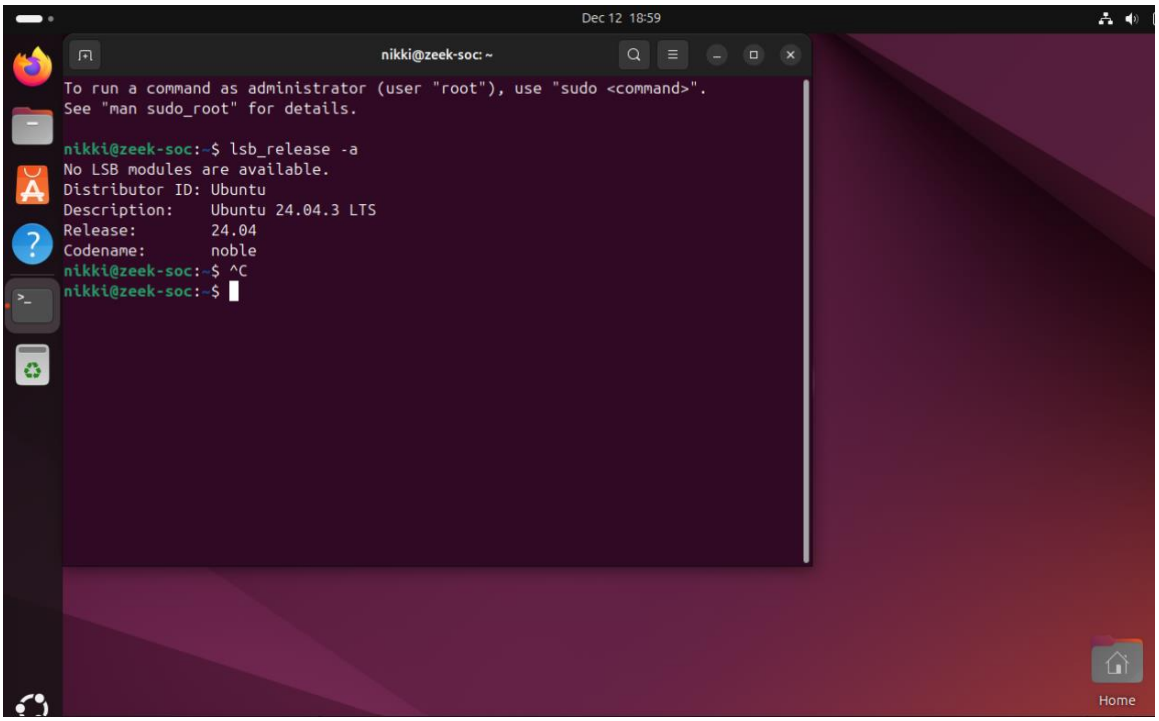
- Zeek version **8.0.4** installed successfully
- Repository and GPG trust configured correctly
- Zeek binary executes without errors
- Built-in analyzers load correctly
- System is ready for traffic analysis and SOC labs

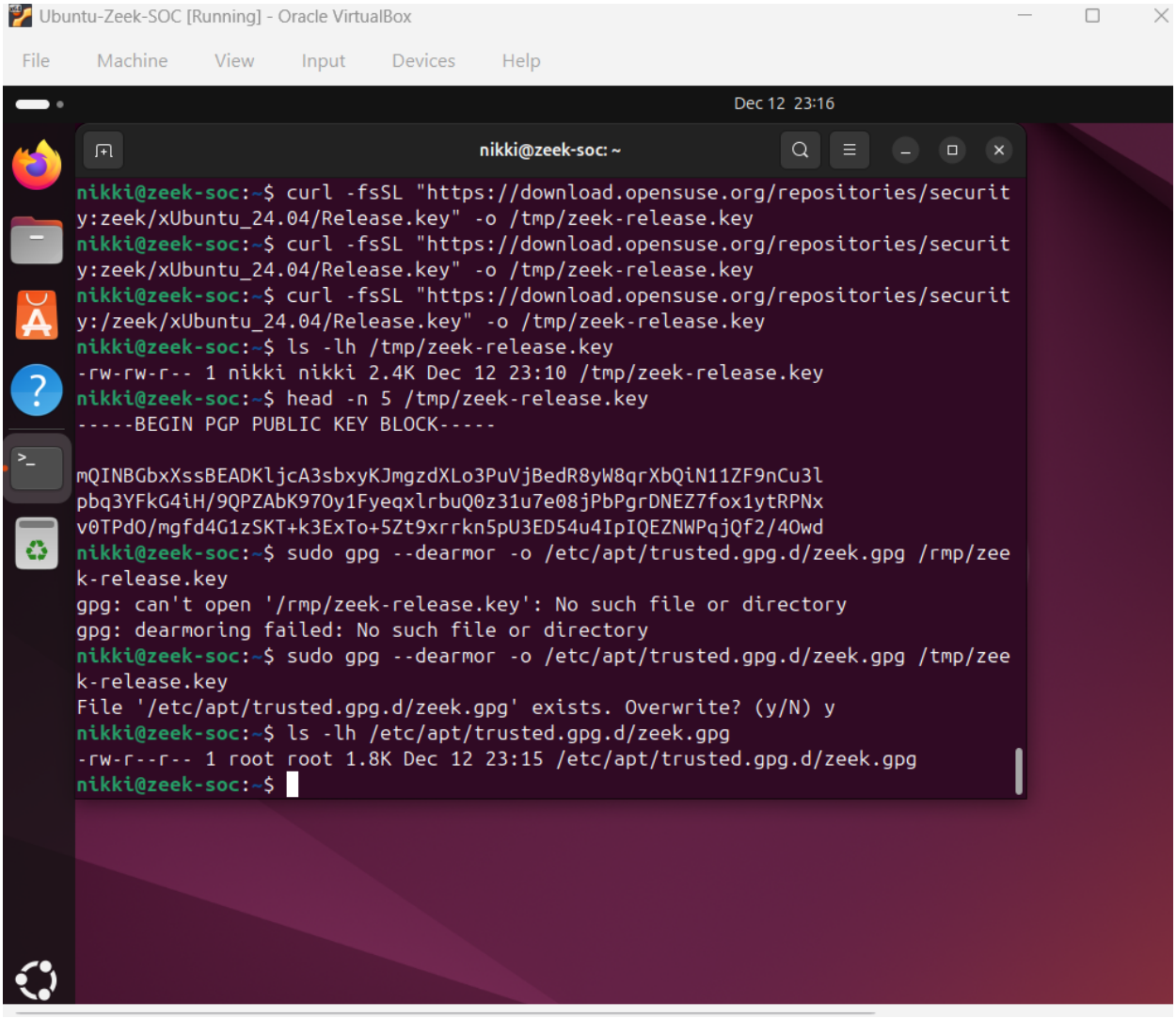
7. Conclusion

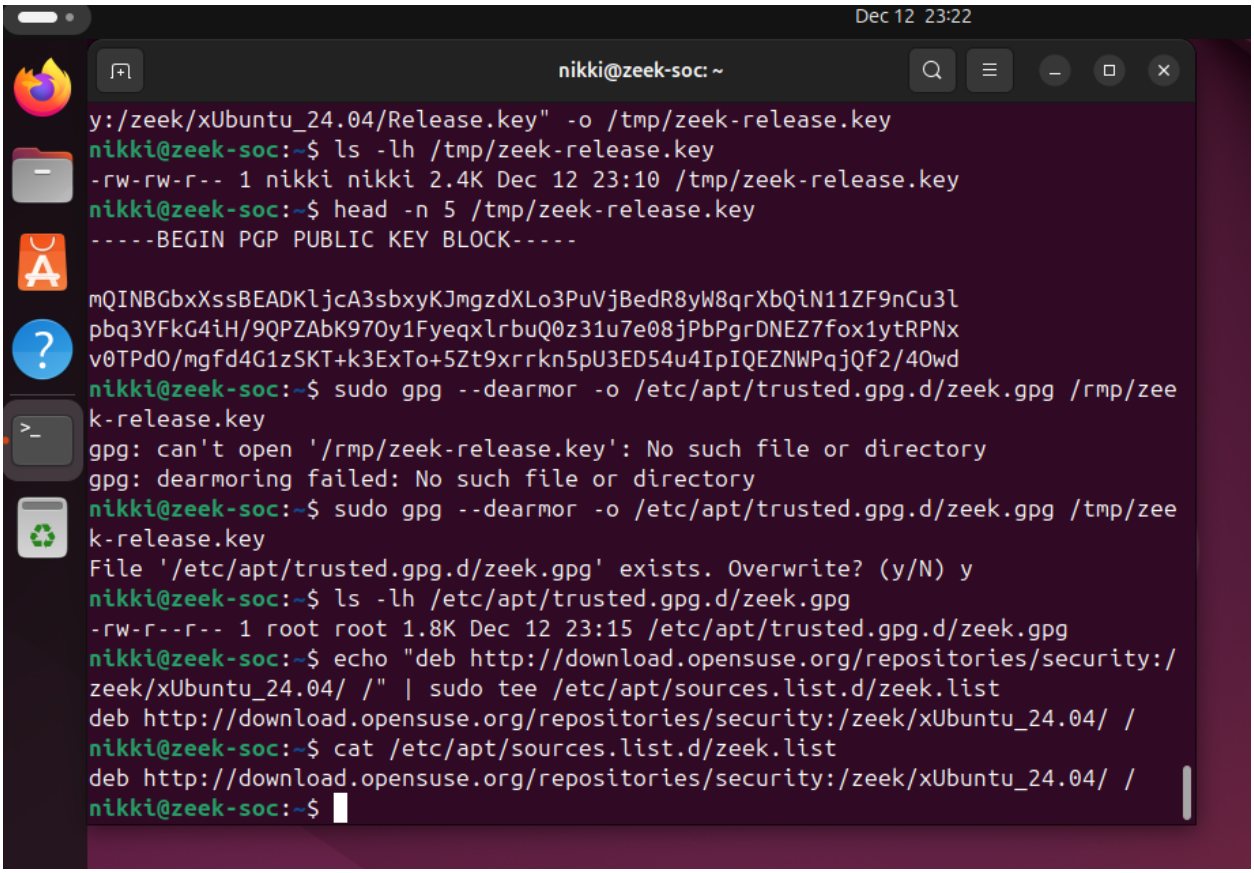
This lab successfully demonstrates the installation and validation of **Zeek Network Security Monitor** on Ubuntu 24.04.
The system is now prepared for further security monitoring tasks such as:

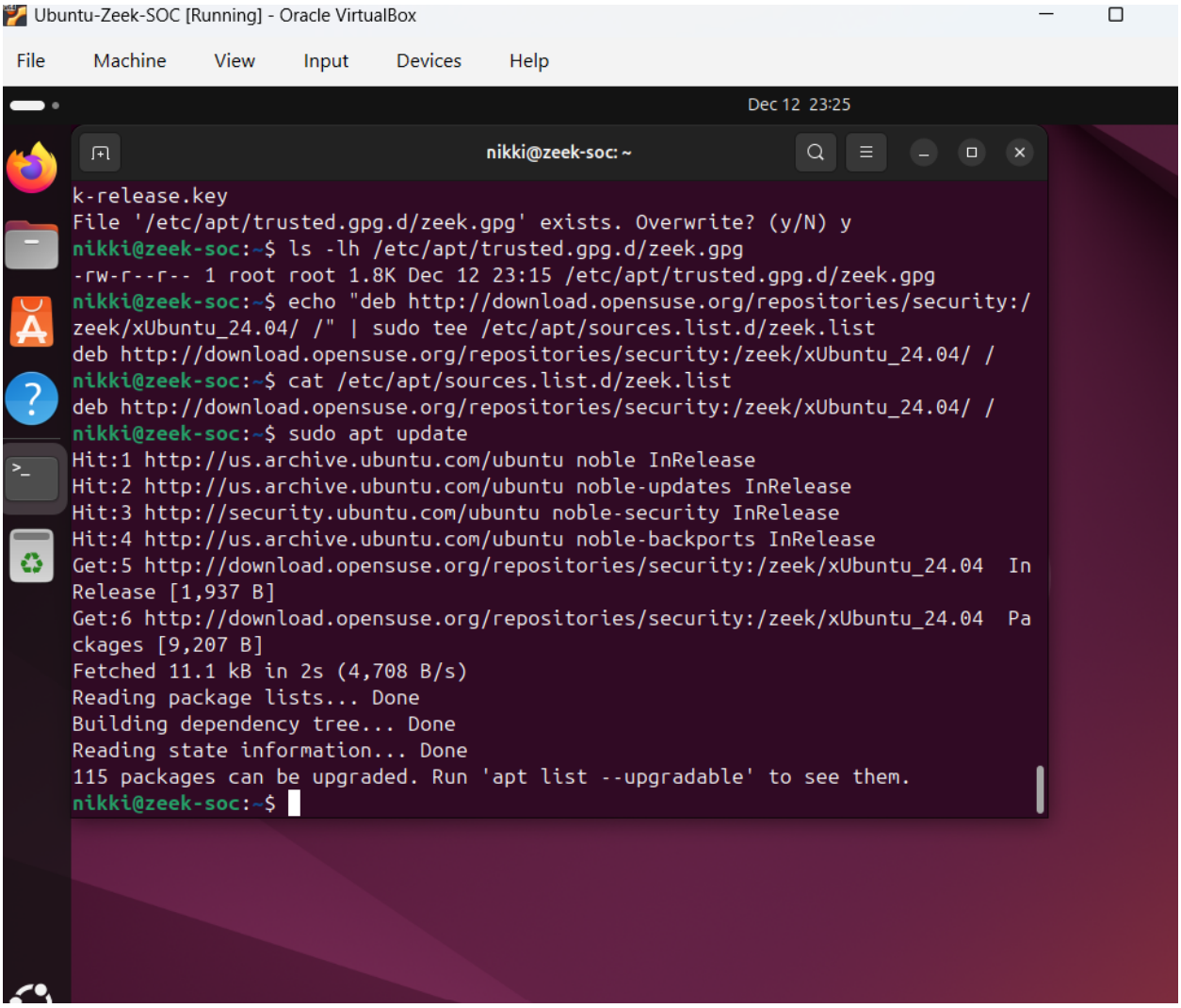
- Packet capture analysis
- Protocol inspection
- SOC alerting and detection development

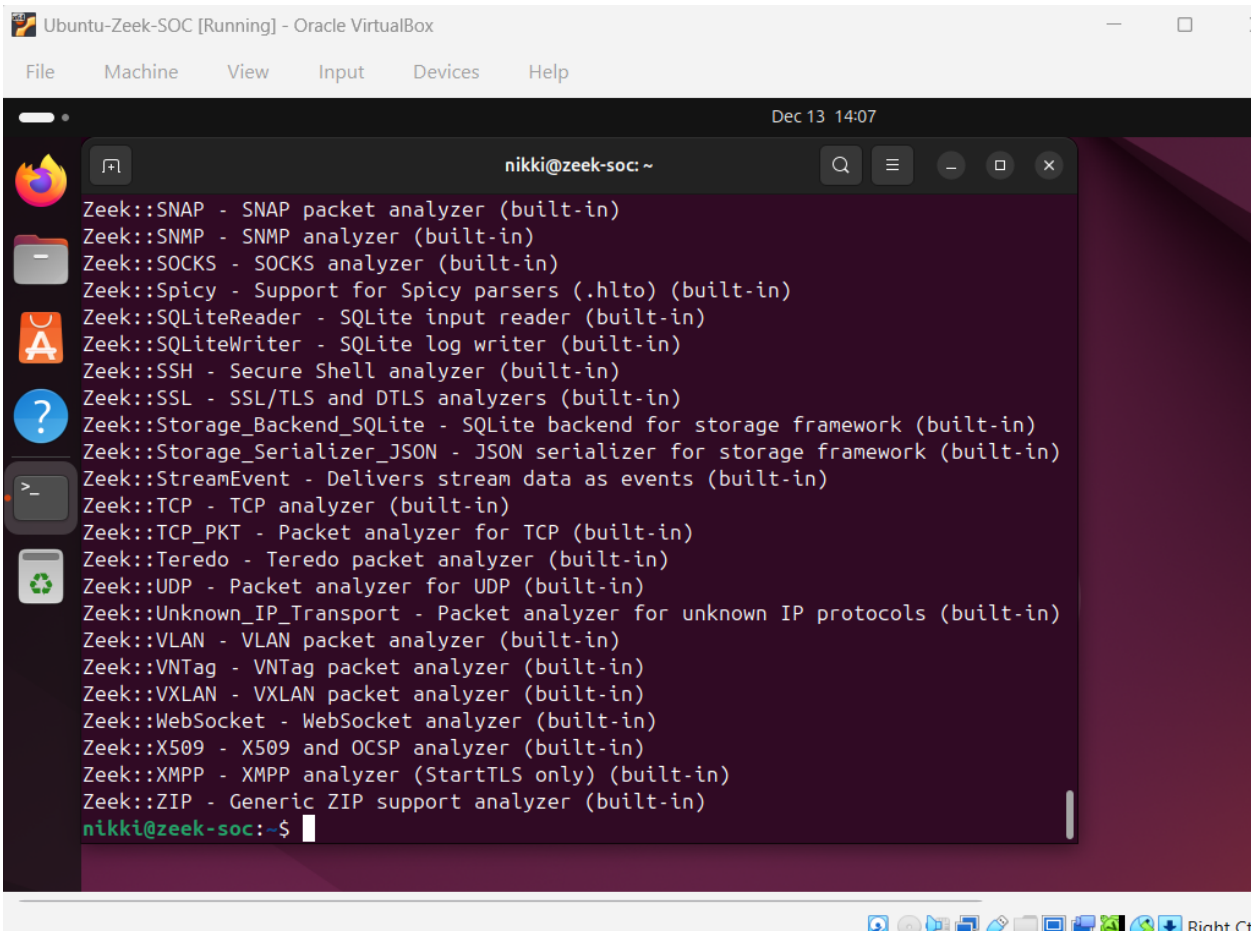
Zeek is fully operational and ready for advanced use in cybersecurity and SOC environments.


Dec 12 18:59
nikki@zeek-soc: ~
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
nikki@zeek-soc:~$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description: Ubuntu 24.04.3 LTS
Release: 24.04
Codename: noble
nikki@zeek-soc:~$ ^C
nikki@zeek-soc:~$
Home


Ubuntu-Zeek-SOC [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Dec 12 23:16
nikki@zeek-soc: ~
nikki@zeek-soc:~$ curl -fsSL "https://download.opensuse.org/repositories/security:zeek/xUbuntu_24.04/Release.key" -o /tmp/zeek-release.key
nikki@zeek-soc:~$ curl -fsSL "https://download.opensuse.org/repositories/security:zeek/xUbuntu_24.04/Release.key" -o /tmp/zeek-release.key
nikki@zeek-soc:~$ curl -fsSL "https://download.opensuse.org/repositories/security:/zeek/xUbuntu_24.04/Release.key" -o /tmp/zeek-release.key
nikki@zeek-soc:~$ ls -lh /tmp/zeek-release.key
-rw-rw-r-- 1 nikki nikki 2.4K Dec 12 23:10 /tmp/zeek-release.key
nikki@zeek-soc:~$ head -n 5 /tmp/zeek-release.key
-----BEGIN PGP PUBLIC KEY BLOCK-----
mQINBGbxXssBEADKljcA3sbxyKJmgzdXLo3PuVjBedR8yW8qrXbQiN11ZF9nCu3l
pbq3YFkG4iH/9QPZAbK97Oy1FyeqxlrbuQ0z31u7e08jPbPgrDNEZ7fox1ytRPNx
v0TPdO/mgfd4G1zSKT+k3ExTo+5Zt9xrrkn5pU3ED54u4IpIQEZNWPqjQf2/4Owd
nikki@zeek-soc:~$ sudo gpg --dearmor -o /etc/apt/trusted.gpg.d/zeek.gpg /rmp/zeek-release.key
gpg: can't open '/rmp/zeek-release.key': No such file or directory
gpg: dearmoring failed: No such file or directory
nikki@zeek-soc:~$ sudo gpg --dearmor -o /etc/apt/trusted.gpg.d/zeek.gpg /tmp/zeek-release.key
File '/etc/apt/trusted.gpg.d/zeek.gpg' exists. Overwrite? (y/N) y
nikki@zeek-soc:~$ ls -lh /etc/apt/trusted.gpg.d/zeek.gpg
-rw-r--r-- 1 root root 1.8K Dec 12 23:15 /etc/apt/trusted.gpg.d/zeek.gpg
nikki@zeek-soc:~$


Dec 12 23:22
nikki@zeek-soc: ~
y:/zeek/xUbuntu_24.04/Release.key" -o /tmp/zeek-release.key
nikki@zeek-soc:~$ ls -lh /tmp/zeek-release.key
-rw-rw-r-- 1 nikki nikki 2.4K Dec 12 23:10 /tmp/zeek-release.key
nikki@zeek-soc:~$ head -n 5 /tmp/zeek-release.key
-----BEGIN PGP PUBLIC KEY BLOCK-----
mQINBGbxXssBEADKljcA3sbxyKJmgzdXLo3PuVjBedR8yW8qrXbQiN11ZF9nCu3l
pbq3YFkG4iH/9QPZAbK97Oy1FyeqxlrbuQ0z31u7e08jPbPgrDNEZ7fox1ytRPNx
v0TPdO/mgfd4G1zSKT+k3ExTo+5Zt9xrrkn5pU3ED54u4IpIQEZNWPqjQf2/4Owd
nikki@zeek-soc:~$ sudo gpg --dearmor -o /etc/apt/trusted.gpg.d/zeek.gpg /rmp/zee
k-release.key
gpg: can't open '/rmp/zeek-release.key': No such file or directory
gpg: dearmoring failed: No such file or directory
nikki@zeek-soc:~$ sudo gpg --dearmor -o /etc/apt/trusted.gpg.d/zeek.gpg /tmp/zee
k-release.key
File '/etc/apt/trusted.gpg.d/zeek.gpg' exists. Overwrite? (y/N) y
nikki@zeek-soc:~$ ls -lh /etc/apt/trusted.gpg.d/zeek.gpg
-rw-r--r-- 1 root root 1.8K Dec 12 23:15 /etc/apt/trusted.gpg.d/zeek.gpg
nikki@zeek-soc:~$ echo "deb http://download.opensuse.org/repositories/security:/
zeek/xUbuntu_24.04/ /" | sudo tee /etc/apt/sources.list.d/zeek.list
deb http://download.opensuse.org/repositories/security:/zeek/xUbuntu_24.04/ /
nikki@zeek-soc:~$ cat /etc/apt/sources.list.d/zeek.list
deb http://download.opensuse.org/repositories/security:/zeek/xUbuntu_24.04/ /
nikki@zeek-soc:~$


Ubuntu-Zeek-SOC [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Dec 12 23:25
nikki@zeek-soc: ~
k-release.key
File '/etc/apt/trusted.gpg.d/zeek.gpg' exists. Overwrite? (y/N) y
nikki@zeek-soc:~$ ls -lh /etc/apt/trusted.gpg.d/zeek.gpg
-rw-r--r-- 1 root root 1.8K Dec 12 23:15 /etc/apt/trusted.gpg.d/zeek.gpg
nikki@zeek-soc:~$ echo "deb http://download.opensuse.org/repositories/security:/
zeek/xUbuntu_24.04/ /" | sudo tee /etc/apt/sources.list.d/zeek.list
deb http://download.opensuse.org/repositories/security:/zeek/xUbuntu_24.04/ /
nikki@zeek-soc:~$ cat /etc/apt/sources.list.d/zeek.list
deb http://download.opensuse.org/repositories/security:/zeek/xUbuntu_24.04/ /
nikki@zeek-soc:~$ sudo apt update
Hit:1 http://us.archive.ubuntu.com/ubuntu noble InRelease
Hit:2 http://us.archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:3 http://security.ubuntu.com/ubuntu noble-security InRelease
Hit:4 http://us.archive.ubuntu.com/ubuntu noble-backports InRelease
Get:5 http://download.opensuse.org/repositories/security:/zeek/xUbuntu_24.04 In
Release [1,937 B]
Get:6 http://download.opensuse.org/repositories/security:/zeek/xUbuntu_24.04 Pa
ckages [9,207 B]
Fetched 11.1 kB in 2s (4,708 B/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
115 packages can be upgraded. Run 'apt list --upgradable' to see them.
nikki@zeek-soc:~$


Ubuntu-Zeek-SOC [Running] - Oracle VirtualBox
File
Machine
View
Input
Devices
Help
Dec 13 14:07
nikki@zeek-soc: ~
Zeek::SNAP - SNAP packet analyzer (built-in)
Zeek::SNMP - SNMP analyzer (built-in)
Zeek::SOCKS - SOCKS analyzer (built-in)
Zeek::Spicy - Support for Spicy parsers (.hlto) (built-in)
Zeek::SQLiteReader - SQLite input reader (built-in)
Zeek::SQLiteWriter - SQLite log writer (built-in)
Zeek::SSH - Secure Shell analyzer (built-in)
Zeek::SSL - SSL/TLS and DTLS analyzers (built-in)
Zeek::Storage_Backend_SQLite - SQLite backend for storage framework (built-in)
Zeek::Storage_Serializer_JSON - JSON serializer for storage framework (built-in)
Zeek::StreamEvent - Delivers stream data as events (built-in)
Zeek::TCP - TCP analyzer (built-in)
Zeek::TCP_PKT - Packet analyzer for TCP (built-in)
Zeek::Teredo - Teredo packet analyzer (built-in)
Zeek::UDP - Packet analyzer for UDP (built-in)
Zeek::Unknown_IP_Transport - Packet analyzer for unknown IP protocols (built-in)
Zeek::VLAN - VLAN packet analyzer (built-in)
Zeek::VNTag - VNTag packet analyzer (built-in)
Zeek::VXLAN - VXLAN packet analyzer (built-in)
Zeek::WebSocket - WebSocket analyzer (built-in)
Zeek::X509 - X509 and OCSP analyzer (built-in)
Zeek::XMPP - XMPP analyzer (StartTLS only) (built-in)
Zeek::ZIP - Generic ZIP support analyzer (built-in)
nikki@zeek-soc:~$