Zeek Network Telemetry Deployment & Validation

Project Type: SOC Network Sensor Deployment

Prepared by: Niknaz Sadehvandi

Role: Founder & Cybersecurity Consultant

Organization: NS Cybersecurity

Date: December 2024

Objective

The objective of this project was to deploy, configure, and validate a Zeek Network Security Monitor sensor in a Linux-based SOC environment. The goal was to establish a reliable source of structured network telemetry capable of capturing real-time traffic and producing SIEM-ready logs for centralized security monitoring, detection engineering, and threat hunting.

Tools & Technologies

- Zeek Network Security Monitor v8.0.4
- Ubuntu 24.04 LTS (VirtualBox virtual machine)
- zeekctl (Zeek control framework)
- Linux networking utilities (ping, nslookup, curl)

Technical Steps Performed

1. Zeek Deployment & Service Initialization

- Installed Zeek under /opt/zeek and verified the correct binary and runtime environment.
- Configured Zeek to operate as a standalone SOC sensor.
- Deployed the service using zeekctl, which initialized policy files, logging directories, and runtime services.

2. Log Generation & Storage Validation

- Confirmed active log generation within the Zeek spool directory

/opt/zeek/spool/zeek

- Verified the presence of multiple Zeek log types, including:
  - conn.log
  - dns.log
  - http.log
  - notice.log
  - stats.log
- This confirmed that Zeek analyzers were actively capturing network activity.

3. Network Traffic Capture Validation

- Generated real network traffic from the monitored system using DNS queries, ICMP traffic, and HTTP requests.
- Verified that the generated traffic was captured and written to Zeek connection and DNS logs.

4. JSON Logging Configuration

- Enabled structured JSON logging by loading the official Zeek JSON policy.
- Redeployed Zeek to apply configuration changes.
- Confirmed logs were written in JSON format to support SIEM ingestion and parsing.

5. Log Content Verification

- Inspected Zeek connection logs to validate telemetry structure and data integrity.
- Verified the presence of key network fields including:
    - Timestamps
    - Source and destination IP addresses
    - Ports and protocols
    - Connection state and packet counts

Findings

- Zeek was successfully deployed and operated as a functional SOC network sensor.
- Live network traffic was captured and logged in real time.
- Multiple Zeek analyzers generated structured telemetry across connection, DNS, and HTTP activity.
- JSON logging was enabled and validated, producing SIEM-ready network logs.
- Log structure and field integrity were confirmed through direct inspection.

Outcome

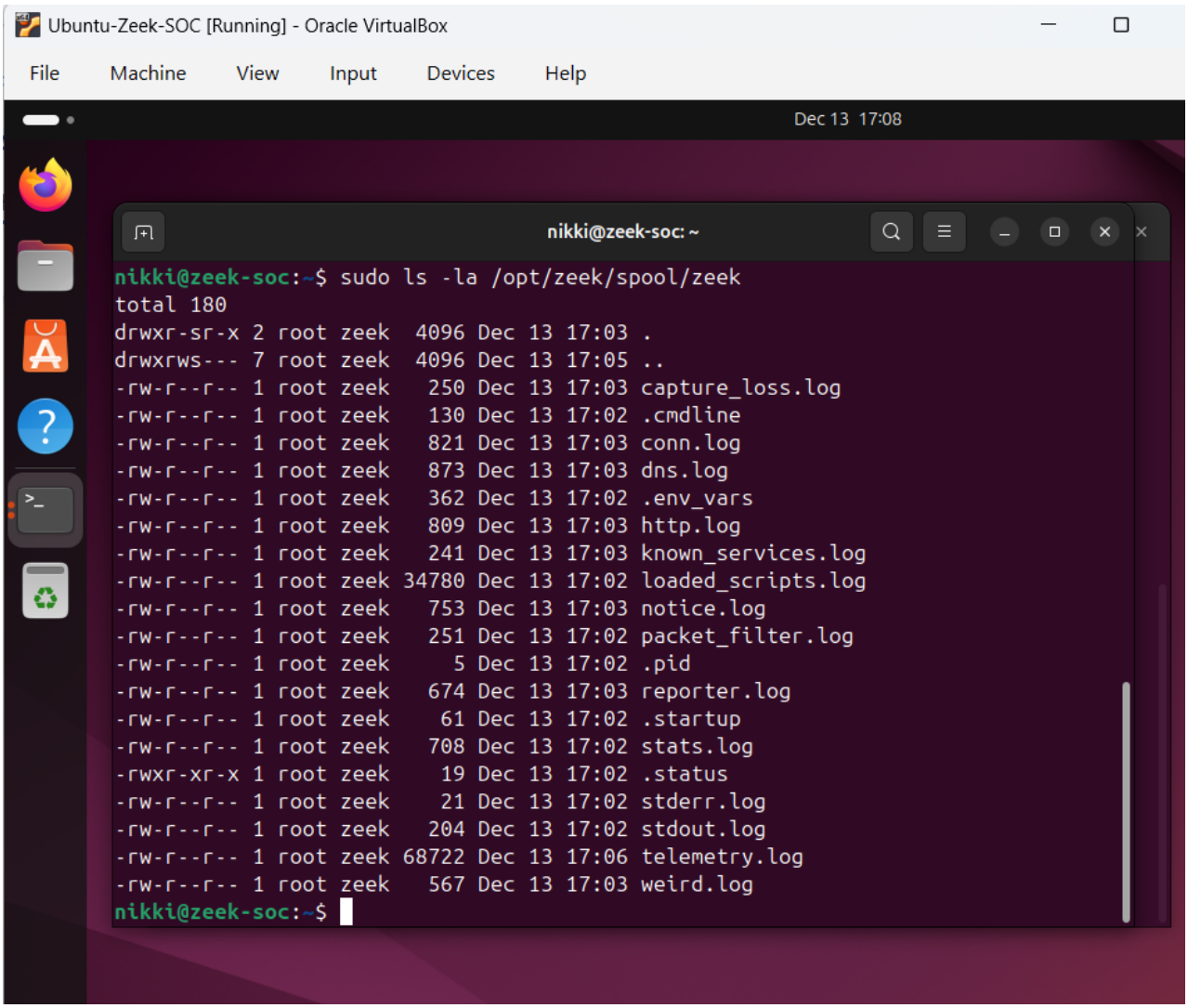
- Established a fully operational Zeek network telemetry sensor in a Linux SOC environment.
- Validated structured, JSON-formatted network logs suitable for centralized SIEM ingestion.
- Produced verifiable evidence demonstrating hands-on experience with SOC-grade network monitoring infrastructure.

This project demonstrates practical experience deploying and validating network security sensors, configuring structured telemetry, and preparing network data for SIEM-based security operations.

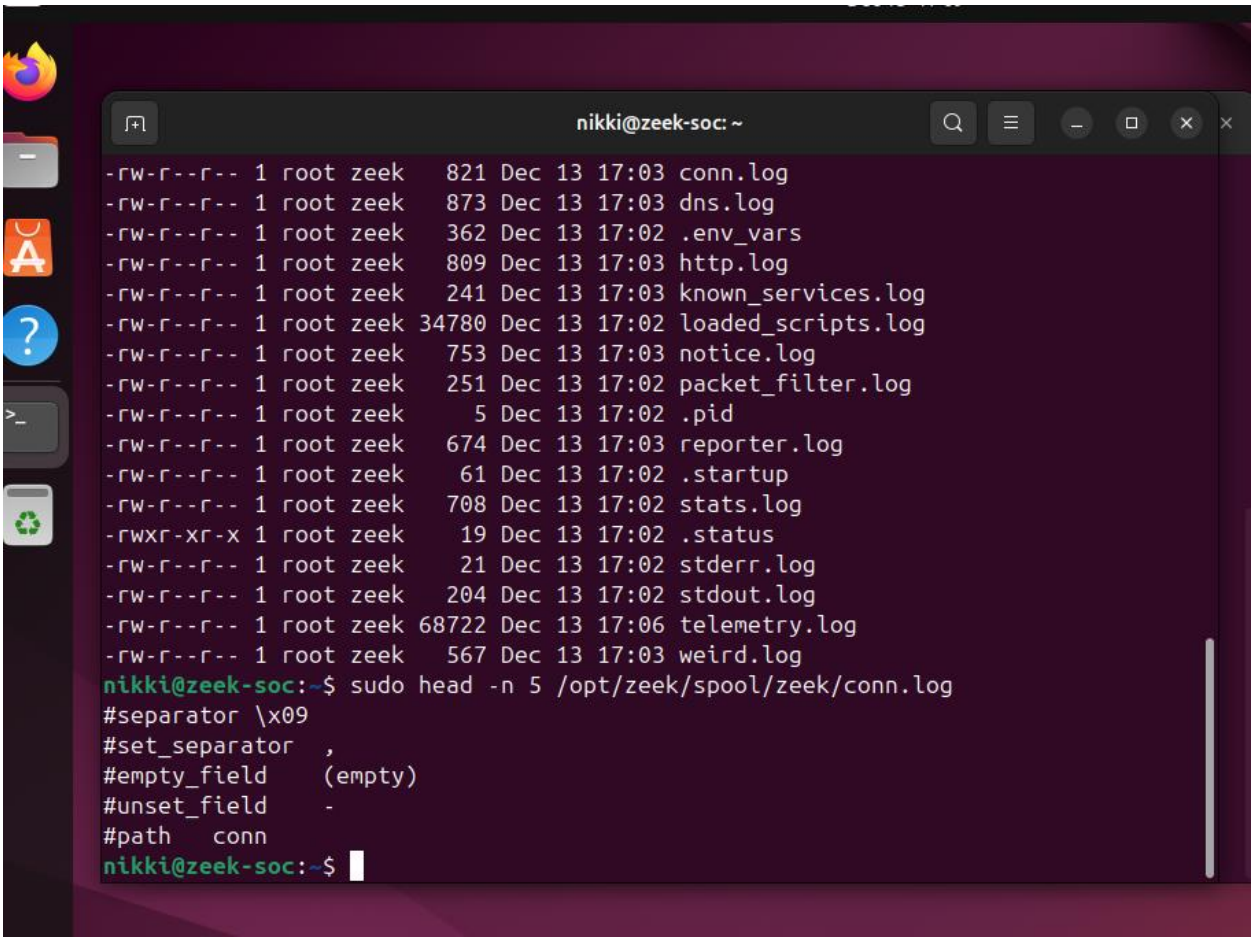
Project Status: Completed

Deliverable: Zeek_Network_Telemetry_Deployment_and_Validation.pdf

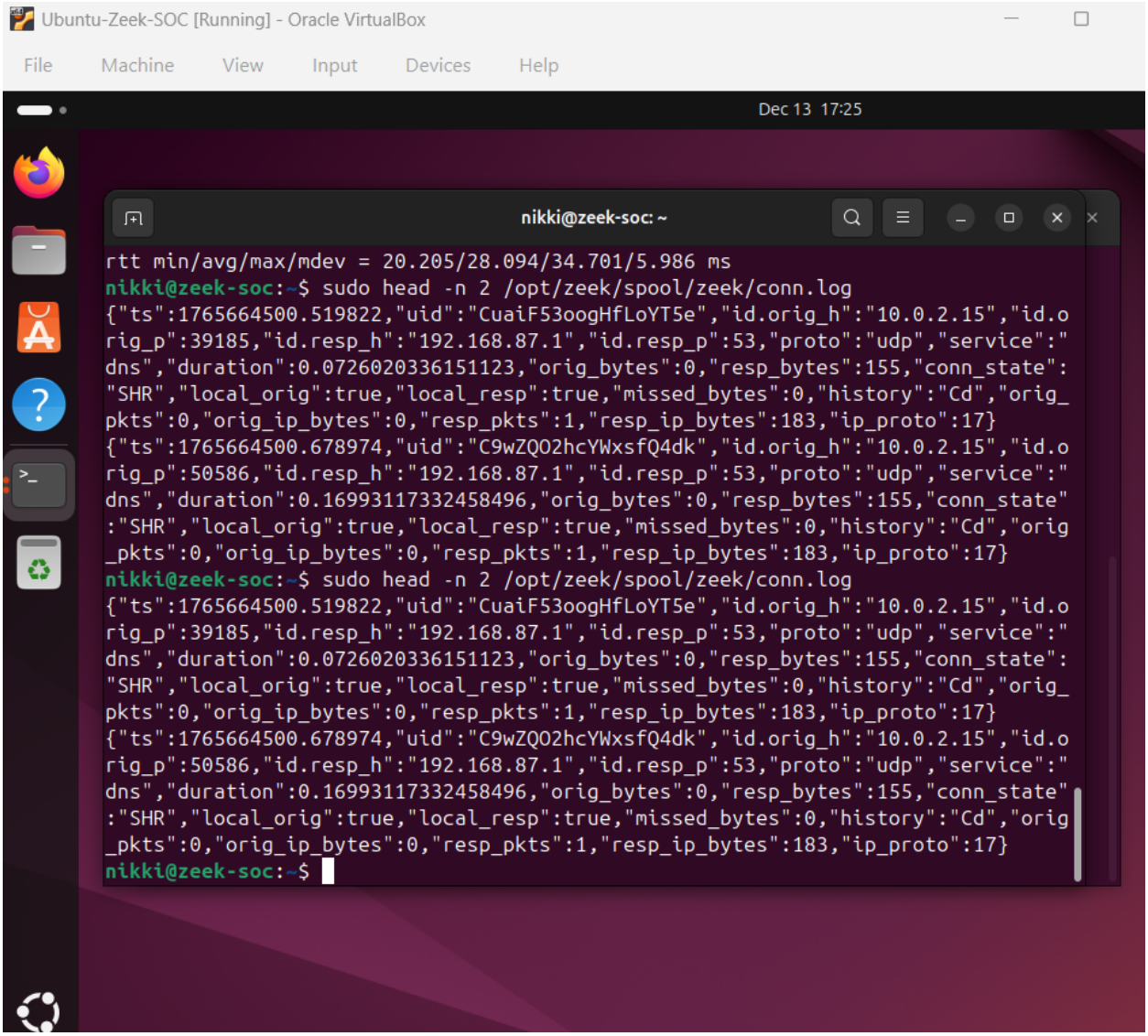
Evidence: Zeek log directory listing, structured log headers, JSON telemetry samples



zeek_conn_log_header.png


nikki@zeek-soc: ~
-rw-r--r-- 1 root zeek   821 Dec 13 17:03 conn.log
-rw-r--r-- 1 root zeek   873 Dec 13 17:03 dns.log
-rw-r--r-- 1 root zeek   362 Dec 13 17:02 .env_vars
-rw-r--r-- 1 root zeek   809 Dec 13 17:03 http.log
-rw-r--r-- 1 root zeek   241 Dec 13 17:03 known_services.log
-rw-r--r-- 1 root zeek 34780 Dec 13 17:02 loaded_scripts.log
-rw-r--r-- 1 root zeek   753 Dec 13 17:03 notice.log
-rw-r--r-- 1 root zeek   251 Dec 13 17:02 packet_filter.log
-rw-r--r-- 1 root zeek   5 Dec 13 17:02 .pid
-rw-r--r-- 1 root zeek   674 Dec 13 17:03 reporter.log
-rw-r--r-- 1 root zeek   61 Dec 13 17:02 .startup
-rw-r--r-- 1 root zeek   708 Dec 13 17:02 stats.log
-rwxr-xr-x 1 root zeek   19 Dec 13 17:02 .status
-rw-r--r-- 1 root zeek   21 Dec 13 17:02 stderr.log
-rw-r--r-- 1 root zeek   204 Dec 13 17:02 stdout.log
-rw-r--r-- 1 root zeek 68722 Dec 13 17:06 telemetry.log
-rw-r--r-- 1 root zeek   567 Dec 13 17:03 weird.log
nikki@zeek-soc:~$ sudo head -n 5 /opt/zeek/spool/zeek/conn.log
#separator \x09
#set_separator ,
#empty_field   (empty)
#unset_field   -
#path   conn
nikki@zeek-soc:~$

ze


Ubuntu-Zeek-SOC [Running] - Oracle VirtualBox
File
Machine
View
Input
Devices
Help
Dec 13 17:25
nikki@zeek-soc: ~
rtt min/avg/max/mdev = 20.205/28.094/34.701/5.986 ms
nikki@zeek-soc:~$ sudo head -n 2 /opt/zeek/spool/zeek/conn.log
{"ts":1765664500.519822,"uid":"CuaiF53oogHfLoYT5e","id.orig_h":"10.0.2.15","id.orig_p":39185,"id.resp_h":"192.168.87.1","id.resp_p":53,"proto":"udp","service":"dns","duration":0.0726020336151123,"orig_bytes":0,"resp_bytes":155,"conn_state":"SHR","local_orig":true,"local_resp":true,"missed_bytes":0,"history":"Cd","orig_pkts":0,"orig_ip_bytes":0,"resp_pkts":1,"resp_ip_bytes":183,"ip_proto":17}
{"ts":1765664500.678974,"uid":"C9wZQO2hcYWxsfQ4dk","id.orig_h":"10.0.2.15","id.orig_p":50586,"id.resp_h":"192.168.87.1","id.resp_p":53,"proto":"udp","service":"dns","duration":0.16993117332458496,"orig_bytes":0,"resp_bytes":155,"conn_state":"SHR","local_orig":true,"local_resp":true,"missed_bytes":0,"history":"Cd","orig_pkts":0,"orig_ip_bytes":0,"resp_pkts":1,"resp_ip_bytes":183,"ip_proto":17}
nikki@zeek-soc:~$ sudo head -n 2 /opt/zeek/spool/zeek/conn.log
{"ts":1765664500.519822,"uid":"CuaiF53oogHfLoYT5e","id.orig_h":"10.0.2.15","id.orig_p":39185,"id.resp_h":"192.168.87.1","id.resp_p":53,"proto":"udp","service":"dns","duration":0.0726020336151123,"orig_bytes":0,"resp_bytes":155,"conn_state":"SHR","local_orig":true,"local_resp":true,"missed_bytes":0,"history":"Cd","orig_pkts":0,"orig_ip_bytes":0,"resp_pkts":1,"resp_ip_bytes":183,"ip_proto":17}
{"ts":1765664500.678974,"uid":"C9wZQO2hcYWxsfQ4dk","id.orig_h":"10.0.2.15","id.orig_p":50586,"id.resp_h":"192.168.87.1","id.resp_p":53,"proto":"udp","service":"dns","duration":0.16993117332458496,"orig_bytes":0,"resp_bytes":155,"conn_state":"SHR","local_orig":true,"local_resp":true,"missed_bytes":0,"history":"Cd","orig_pkts":0,"orig_ip_bytes":0,"resp_pkts":1,"resp_ip_bytes":183,"ip_proto":17}
nikki@zeek-soc:~$