**Introduction to zeek and log analysis**

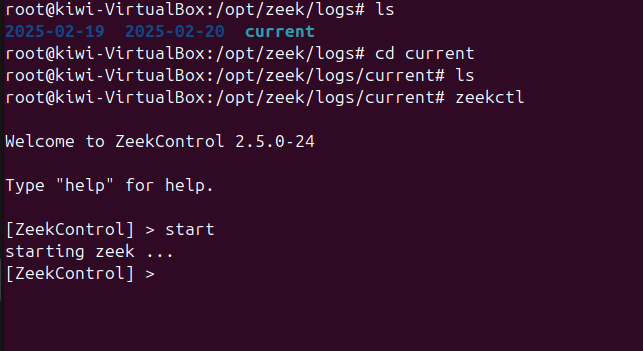
Zeek is a software used to monitor network traffic and create logs of what traffic it captures. Monitoring with Zeek starts with collecting data which is then followed by analysis of said data. Data collected from Zeek can be analyzed for malicious or suspicious traffic.

**How to analyze conn logs for active connections**

**Step 1. Find the log files at /opt/zeek/logs/current**

**Step 2. Run zeekctl**

**Step 3. At the zeekctl prompt use the start command**

****

**Step 4. Use the cat command to view any active conn logs in the directory**

****

**Step 5. Additionally you can use zeek-cut to display certain fields from the conn log**

**How to check dns.log for suspicious activity**

1. Read the log file
2. Search for any suspicious traffic like suspicious domains.

**How to find anomalies in http.log, ssl.log, and weird.log**

1. Read the file
2. Look for suspicious traffic such as unathorized connections, passwords, and possible payloads.