Decoding the Pulse of Network Traffic: Unveiling Threats and Anomalies Through Log Analysis

18 May 2025

Agenda

- Network Traffic
- Network Log Analysis
- Internetworking Fundamental
- OSI Model
- Network Protocol
- Introduction to Zeek
- Colab Exercise
- Cyber Threat Intelligence

Key Takeaway

- Gain hands-on experience in analyzing network traffic logs using Zeek.
- Learn to parse, filter, and interpret logs to detect anomalies and potential threats.
- Perform IoC lookups using multiple CTI platforms (e.g., VirusTotal, AbuseIPDB, MISP).

What is Network Traffic?

- Network traffic refers to the flow of data across a computer network. It includes all data communication between devices, such as computers, servers, and smartphones.

Simple Analogy:

- Network traffic is like cars on a highway. Each car represents a data packet, and the highway is the network. Just like traffic can be smooth or congested, network traffic can be normal or abnormal.

Examples of Network Traffic:

- Sending and receiving emails
- Browsing websites (HTTP/HTTPS)
- Downloading or uploading files
- Chatting on messaging apps (e.g., WhatsApp, Telegram)
- Streaming videos (e.g., YouTube, Netflix)

Types of Network Traffic Behavior:

- **Normal Traffic:**
  - A student accessing Google at 10 AM
  - Staff sending email during working hours
  - Watching a YouTube tutorial in the evening
- **Suspicious Traffic:**
  - A large file upload at 3 AM
  - Login attempt from a different country
  - Sudden traffic spike from unknown IP address

Purpose of Network Traffic Monitoring:

- Detect Cyber Threats Early
- Troubleshoot Network Issues
- Understand Network Usage
- Ensure Compliance and Auditing
- Improve Overall Security Posture

What is Network Log Analysis?

- A process of reviewing computer-generated event logs to **proactively identify bugs, security threats or other risks**.
- Can also be used more broadly to ensure compliance with regulations or review user behavior.
- A log is a comprehensive file that **captures** activity within the **operating system, software applications or devices**.
- Automatically documents any information designated by the system administrators, including **messages, error reports, file requests, file transfers and sign-in/out requests**.
- The activity is also **timestamped**, which helps IT professionals and developers establish an audit trail in the event of a system failure, breach or other outlying event.

What Are Logs?

- **Logs** are digital records that capture events or activities happening within a system, network, or application.
- They answer questions like:
  - What happened?
  - When did it happen?
  - Where did it happen?
  - Who did it?

What Are Logs?

Think of Logs Like a Diary

- Just like a diary records your daily activities, **logs record system activities** for example, login attempts, file access, system errors, and more

Why Are Logs Important?

- Investigate suspicious activity
- Track changes or failures
- Provide evidence during security incidents
- Help IT teams troubleshoot problems

Common Types of Logs

- System Logs
- Network Logs
- Application Logs
- Security Logs
- SIEM Logs

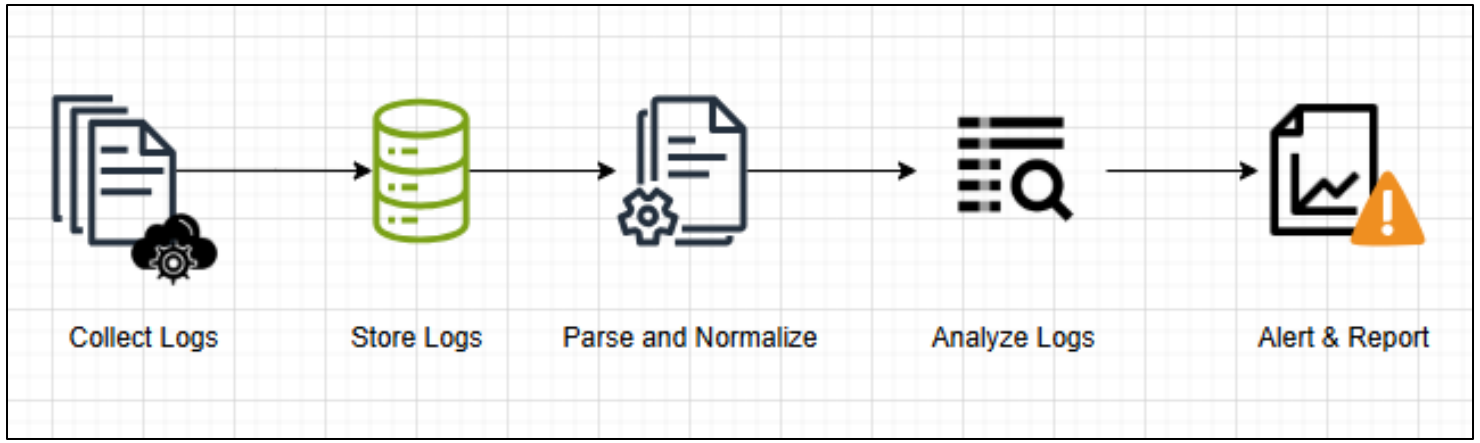
Anomalies in Network Traffic

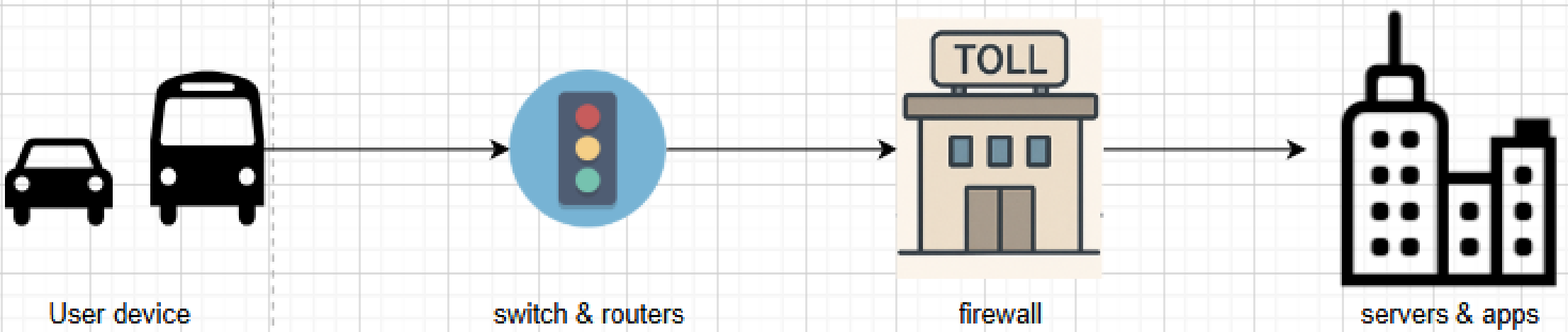
Anomalies are unusual or unexpected patterns in network traffic that may indicate errors, misuse, or cyberattacks.

Think of It Like This:

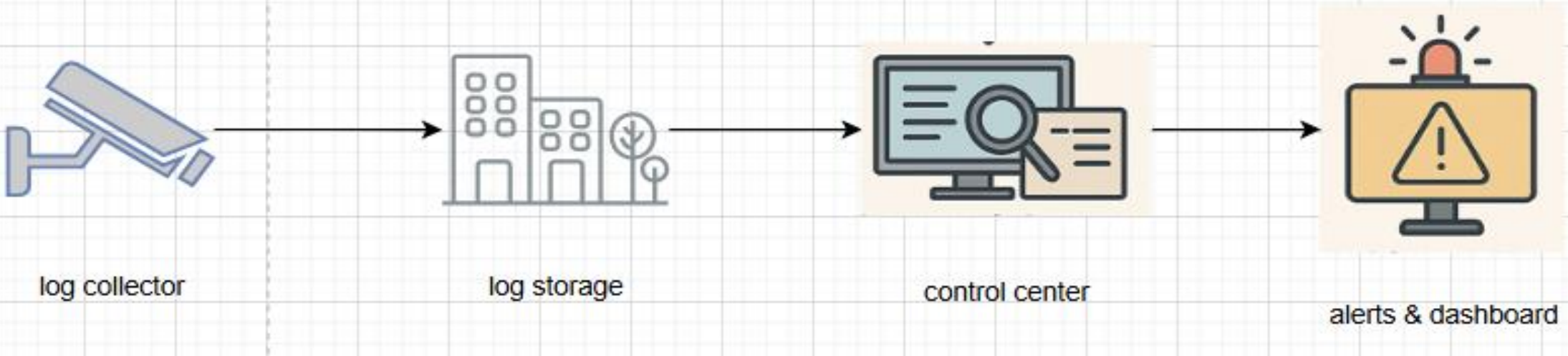
- Just like a sudden traffic jam on a highway might signal accident or unexpected spike or change in network activity could mean something is wrong.
- Types of Network Anomalies:
  - Volume Anomalies
  - Time-Based Anomalies
  - Behavior Anomalies
  - Location/IP Anomalies

How Is Log Analysis Done




TOLL
User device
switch & routers
firewall
servers & apps

ANALOGIES


log collector
log storage
control center
alerts & dashboard

Internetworking Fundamental

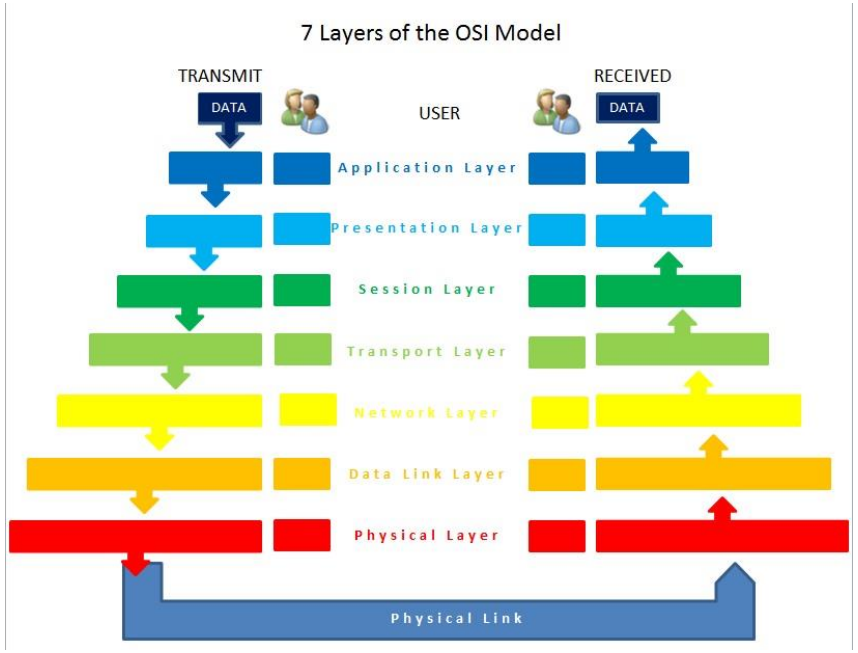
- **Local Area Network (LAN)**
  - A computer network that connects computers within a limited or ‘local’ geographic area
  - Typically, the medium these days is Ethernet or Wi-Fi
- **Wide Area Network (WAN)**
  - A computer network that connects computers within a large or ‘wide’ geographic area

    Often established via leased lines or VPN connections

    Can connect two or more LANs
- The Internet is the largest WAN in existence

OSI Model

- Open Systems Interconnection
- A conceptual model of communication that specify the functionalities
- Benefit in design, standardization, troubleshooting



Network Protocol

- An agreement on how computer networks will work.
- Entities exchanging messages are the software and hardware of the network.
- Protocols define the format and order of messages and action taken upon receipt of the messages.

Network Protocol - IP Address

- An IP Address (Internet Protocol Address) is a label assigned to a computer on a network that identifies it. It also defines its location on the network.
- There are two versions, IPv4 and IPv6
- IPv4 is easier to read but has a limited address space. We're running out of these!
- IPv6 is more recent and gaining traction. It can look intimidating, but the address space is large enough that trillions of IP addresses could be assigned to every human on the planet.

Network Protocol - IP Address

- IPv4
  - Format: XXX.XXX.XXX.XXX
  - 8 bits separated by ‘dots’, 32 bits in total
  - E.g.: 192.168.0.1
- IPv6
  - Format: XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX
  - 16 bits separated by colons, 128 bits in total
  - E.g.: FE80:0000:0000:0000:903A:1C1A:E802:11E4

Network Protocol - Port

- A Port is a number which corresponds to a communications channel
- Only one application can listen on a specific port at a time
- Available ports range from 1 – 65535
- Given the differences between TCP protocols and UDP protocols, each computer actually has two sets of port ranges
- There are 1 – 65535 TCP ports
- Also 1 – 65535 UDP ports
- You can have one application listening on TCP Port 80 and also one application listening on UDP Port 80
- Despite having the same number, the two ports are separate

Network Protocol - Common Port

- Some common ports:
  - Port 21 – File Transfer Protocol (FTP)
  - Port 25 – Simple Mail Transfer Protocol (SMTP)
  - Port 80 – Hypertext Transfer Protocol (HTTP)
  - Port 443 – Hypertext Transfer Protocol Secure (HTTPS)

- $cat /etc/services
- Note : you can run any service on any port, just a matter of standard.

Introduction to Zeek

- Zeek (formerly known as Bro) is a powerful open-source network monitoring and security analysis tool.
- It operates as a network traffic analyzer, primarily designed to capture, inspect, and log data from network activity in real-time.
- Zeek is widely used in network security, threat hunting, and network performance monitoring.

Zeek Functionalities

- Protocol Analysis
  - Zeek decodes network traffic across various layers and supports a wide range of protocols.
  - Application Layer Protocols: HTTP, DNS, FTP, SMTP, SMB, SSL/TLS, etc.
  - Transport Layer Protocols: TCP, UDP.
  - Network Layer Protocols: ICMP, IPv4, IPv6.
- File Extraction and Analysis
  - Zeek can extract files transferred over the network for further analysis.
  - Metadata about files (e.g., hashes) is logged, and files can be sent to tools like antivirus software or sandboxes for examination.
- Threat Detection
  - Detecting Indicators of Compromise (IoCs), such as blacklisted IPs or domains.
  - Identifying behaviors associated with malware, lateral movement, or data exfiltration.

Types of Zeek Logs

- Here are some examples of common Zeek Logs that can provide us with a lot of information during our Network Log Analysis.
  - conn.log
    - Records every network connection Zeek observes, capturing details about the communication between devices.
  - dns.log
    - Captures DNS queries and responses, helping to track domain name lookups.
  - http.log
    - Records HTTP requests and responses, providing insights into web traffic.
  - files.log
    - Records information about files transferred over the network, including metadata and hash values.
  - smtp.log
    - Captures Simple Mail Transfer Protocol (SMTP) transactions, detailing email communications.
  - ssh.log
    - Records details about SSH (Secure Shell) connections, which are commonly used for secure remote access to servers.

Zeek Online

- To have a better idea on how what does each log contains, we can use the platform below to try some sample PCAP files, which will be convert to Zeek log format.
- Link: https://try-zeek.show.corelight.io/#/?example=hello

Colab Exercise

- Go to Colab Notebook Labsheet

Cyber Threat Intelligence

Threat intelligence is:

- Data that is collected, processed, and analyzed to understand a threat actor's motives, targets, and attack behaviors.
- Threat intelligence enables us to make faster, more informed, data-backed security decisions and change their behavior from reactive to proactive in the fight against threat actors.
- Threat intelligence is important for the following reasons:
- Sheds light on the unknown, enabling security teams to make better decisions.
- Empowers cyber security stakeholders by revealing adversarial motives and their tactics, techniques, and procedures (TTPs).
- Helps security professionals better understand the threat actor's decision-making process.

Cyber Threat Intelligence – Common Tools

- VirusTotal: https://www.virustotal.com/gui/home/search
- Abuse.ch: https://abuse.ch/
- IPInfo: https://ipinfo.io/
- IOC Radar: https://socradar.io/labs/app/ioc-radar

Feedback Form

Thank you for attending Decoding the Pulse of Network Traffic: Unveiling Threats and Anomalies Through Log Analysis. We value your feedback—please take a moment to fill out the short feedback form below to help us improve future workshops.