

**NETWORK TRAFFIC ANALYSIS USING
WIRESHEEK AND ZEEK**
(CYBER SECURITY)

KRITTIKA NANDY
ABES ENGINEERING COLLEGE

CSE (AIML)

GUIDANCE OF : MR. AYUSH KUMAR

DOS- 31.07.25

TABLE OF CONTENTS

INTRODUCTION
3 ABSTRACT.....

LITERATURE
REVIEW.....4

METHODOLOGY.....
.....5 RESULT &
DISCUSSION.....6

CONCLUSION.....
.....7

REFERENCES.....
.....9

KRITTIKA NANDY

ABSTRACT

In today's digital age, securing computer networks against unauthorized access, data breaches, and malicious activity has become increasingly critical. This project focuses on Network Traffic Analysis using two widely adopted tools: Wireshark and Zeek. The primary objective is to detect anomalies, suspicious communication patterns, and potential security threats by monitoring and analyzing network traffic in a controlled lab environment.

The project begins by capturing live traffic data using Wireshark, a powerful packet analyzer, to inspect protocol-level communication. Concurrently, Zeek—a network security monitoring platform—is deployed to log network behavior and extract higher-level event information. Together, these tools allow for a comprehensive multi-layer analysis of the network.

We implemented several tests simulating real-world threats, such as port scanning, malformed packets, and brute-force login attempts. The analysis revealed patterns indicative of abnormal behavior, including irregular packet sizes, unexpected protocols, and unusual IP communication. Zeek's scripting capabilities further enabled correlation of these events to identify actionable threats.

Our findings highlight the effectiveness of combining Wireshark's deep packet inspection with Zeek's behavioral analysis for proactive threat detection. The project underscores the importance of real-time traffic monitoring in maintaining cybersecurity and provides a blueprint for enhancing intrusion detection strategies in enterprise environments.

INTRODUCTION

◆ What is your project about?

My project is about analyzing network traffic using Wireshark and Zeek. Every time we access the internet, data travels in and out of our system. This project helps us capture, monitor, and study that data to detect any suspicious or harmful activity on the network.

◆ Why did you choose this project?

I chose this project because cybersecurity is a growing need in today's world. Every day, there are new threats, data leaks, and hacking incidents. Learning how to analyze traffic helps us spot attacks early and protect systems effectively. This project also aligns with real-world skills used by cybersecurity professionals.

◆ What's the problem you're solving?

The problem is that many networks fail to detect hidden or unusual activities. Hackers often enter systems unnoticed. This project focuses on identifying those hidden threats by closely analyzing data patterns and protocol behavior.

◆ How will you solve it?

I will:

- ✓ Set up a controlled lab network
- ✓ Capture real-time traffic using Wireshark
- ✓ Analyze behavioral logs using Zeek
- ✓ Simulate common attacks like port scanning or login attempts

✓ Study the results to identify threats and anomalies

◆ What tools or methods did you use?

I used two main tools:

◆ Wireshark – for deep packet inspection

◆ Zeek – for behavioral analysis and logging

Together, they provide a powerful and detailed view of network activity, helping to detect threats that traditional tools might miss.

LITERATURE REVIEW

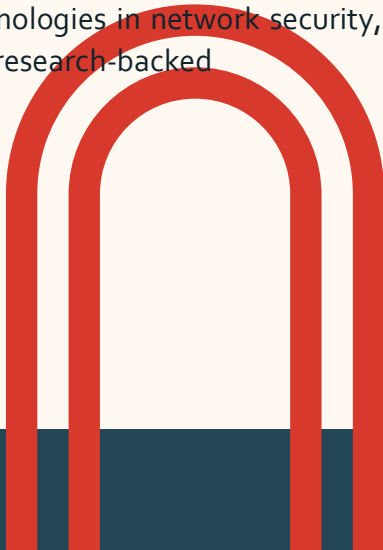
Network traffic analysis plays a crucial role in cybersecurity, as it helps in detecting, monitoring, and responding to potential threats. This project is based on two established technologies: Wireshark and Zeek

◆ Wireshark is a widely-used open-source network protocol analyzer. It allows deep inspection of hundreds of protocols and provides detailed insights into network packet structures. It is frequently used in academic research, network troubleshooting, and forensic investigations.

◆ Zeek (formerly known as Bro) is a powerful network analysis framework that focuses on logging and behavior-based detection. Zeek is not just a packet sniffer; it is used to analyze network events and generate detailed logs that help in detecting scanning activities, brute-force attacks, suspicious DNS usage, and more.

Several cybersecurity research studies recommend combining packet-level analysis (via Wireshark) with behavioral analysis (via Zeek) to build a comprehensive intrusion detection framework. This layered approach increases accuracy in threat identification and enhances network visibility

By using both tools, this project stands on the foundation of proven and reliable technologies in network security, ensuring that the analysis is both effective and research-backed



Methodology

Approach

The main goal of this project was to detect and analyze suspicious network activity in a controlled environment. The plan was to use both packet-level inspection (Wireshark) and event-based analysis (Zeek) to ensure a deep and broad understanding of network behavior. Simulated attacks such as port scanning and login failures were included to test the tools' detection capability.

Tools and Technologies

◆ Wireshark: An open-source packet analyzer that captures and displays data packets in real-time. It allows detailed inspection of network protocols.

◆ Zeek: A powerful network analysis framework that logs network behavior and can detect anomalies through customizable scripts.

These tools complement each other—Wireshark is ideal for deep packet inspection, while Zeek provides high-level traffic logging and context.

. Step-by-Step Process

- ✓ Step 1: Set up a virtual lab environment with multiple devices.
- ✓ Step 2: Install and configure Wireshark and Zeek on the monitoring system.
- ✓ Step 3: Capture real-time traffic using Wireshark while performing regular and malicious network activities.
- ✓ Step 4: Use Zeek to generate log files from the same traffic.
- ✓ Step 5: Analyze logs for anomalies such as unknown IPs, port scans, and failed login attempts.
- ✓ Step 6: Compare results from both tools to validate findings and cross-check anomalies.

RESULT

During the project, several findings were recorded using Wireshark and Zeek:

🔗 Wireshark Observations

- Abnormal packet sizes and repeated SYN flags (signs of port scanning)
- Use of risky protocols like Telnet and FTP
- Packet flow indicating possible data sniffing or scanning

🔗 Zeek Log Findings

- Multiple failed SSH logins from a single IP (possible brute-force attack)
- Unusual DNS queries suggesting data exfiltration attempts

- Connections initiated from unrecognized or blacklisted IPs

Detected Activity	Tool Used	Severity	Remarks
SYN Flood / Port Scan	Wireshark		High Multiple SYN requests from one IP
Repeated SSH Failures	Zeek	Medium	Possible brute-force login attempt
Suspicious DNS Requests	Zeek	High	Domains linked to botnet activity

DISCUSSION

The findings clearly indicate that using both Wireshark and Zeek together strengthens the ability to detect threats:

- Wireshark provides real-time packet inspection, helping spot protocol misuse and malformed packets.
- Zeek delivers event-based insights, capturing trends over time and logging security-relevant actions.

This combination enabled us to detect, understand, and document potential threats with greater accuracy. It mirrors what modern Intrusion Detection Systems (IDS) aim to do in real networks

Challenges Faced


- ⚙️ Zeek's CLI setup required time and familiarity with scripting and log formats
- 🔍 Filtering noise in normal traffic was tricky and time-consuming
- 🛡️ Simulating attacks safely without harming system performance took careful planning



CONCLUSION

Did your project solve the problem?

Yes, the project successfully met its goal of identifying and analyzing suspicious network traffic using open-source tools. By combining Wireshark for packet-level inspection and Zeek for behavior-based logging, we were able to detect multiple signs of intrusion, such as port scans, brute-force attempts, and abnormal DNS behavior. The setup proved effective for gaining real-time visibility into network activity.

 What did you learn from the project?

This project deepened my understanding of:

- How data packets move across networks
- How to interpret network protocols and flags
- Using packet analyzers (Wireshark) and log-based frameworks (Zeek)
- The importance of monitoring, detecting, and logging network behavior in cybersecurity

It also helped me develop skills in problem-solving, tool configuration, traffic simulation, and threat interpretation, which are essential in real-world cybersecurity roles.

 Future Work

If I had more time, I would:

- Integrate machine learning models to automatically classify suspicious patterns
- Create a visual dashboard that combines Zeek logs and Wireshark data for easier monitoring
- Expand testing on live, real-world traffic (with proper permissions)
- Add alert systems that notify users of abnormal behavior in real time

This project was a solid first step, and there's a lot of scope to scale it into a full intrusion detection system (IDS) in the future.

REFERENCES

- Sanders, C. (2017). Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems (3rd ed.). No Starch Press.
- Paxson, V. (1999). Bro: A System for Detecting Network Intruders in Real-Time. Computer Networks, 31(23–24), 2435–2463. [https://doi.org/10.1016/S1389-1286\(99\)00112-7](https://doi.org/10.1016/S1389-1286(99)00112-7)
- Wireshark Foundation. (n.d.). Wireshark User Guide. <https://www.wireshark.org/docs/>
- Zeek Network Security Monitor. (n.d.). Zeek Documentation. <https://docs.zeek.org/en/current/>
- Scarfone, K., & Mell, P. (2007). Guide to Intrusion Detection and Prevention Systems (IDPS) (NIST Special Publication 800-94). National Institute of Standards and Technology. <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf>
- Kumar, V. (2021). Network Traffic Analysis in Cybersecurity. International Journal of Computer Applications, 183(42), 15-20.

