Network Traffic Analysis: Wireshark and Zeek

This presentation focuses on the critical domain of network traffic analysis, specifically utilizing powerful tools like Wireshark and Zeek. We will explore how these platforms enable in-depth inspection, monitoring, and security analysis of network data, outlining their capabilities, use cases, and best practices for implementation in enterprise environments.



**Name:** Arohi Singh

**Institution:** Dronacharya Group of Institution

**Course:** CSE(Cyber Security) **Date:** [Date of Presentation] **Supervisor:** Prof. Ayush Kumar

## Project Overview: Unmasking the Network

In a world of evolving threats and unseen vulnerabilities, your network is under siege. This project isn't just an analysis; it's a deep dive into the hidden currents of data, revealing the unseen, securing the vital.

**3**

**THE IMPACT**

Implementing Wireshark and Zeek ensures real-time threat detection and enables rapid, precise response capabilities. By pinpointing anomalies and suspicious patterns in network traffic, organizations gain actionable insights into potential security incidents. This proactive analysis allows for the timely identification and neutralization of threats, significantly reducing the attack surface and fortifying the digital frontier against evolving cyber threats, ultimately enhancing overall network

resilience and data integrity.

**1**

**THE PROBLEM**

Networks face sophisticated, constant attacks, leading to critical visibility gaps. Unseen threats, from advanced persistent threats (APTs) to zero-day exploits, jeopardize sensitive data and crucial operations, making traditional security measures insufficient. The sheer volume and complexity of network traffic often obscure malicious activities, leaving organizations vulnerable to breaches and data

loss.

**2**

**THE SOLUTION**

Our approach combines Wireshark for microscopic forensic detail and Zeek for macroscopic security intelligence. Wireshark provides granular packetlevel analysis, allowing for deep inspection of individual network conversations and anomalies. Zeek (formerly Bro) delivers high-level transaction logs and extracted content, offering a comprehensive overview of network activity, policy violations, and potential intrusions.

Together, these tools provide

unparalleled insight into network behavior, enabling both deep- dive forensics and broad- spectrum threat hunting.

# Table of Contents

**2**

**Key Findings: Unpacking the Data**

Presenting key findings from the analysis, discussing their implications, and interpreting the data gathered

using Wireshark and Zeek.

**4**

**Looking Forward: Impact and Evolution**

Summarizing the project's achievements, discussing challenges faced, outlining future research or implementation possibilities, providing a final summary of key takeaways, and proposing actionable next steps for continued development and

application.

**1**

**Project Introduction: Laying the Groundwork**

Setting the stage by outlining the project's purpose,

the significance of network analysis, and the objectives to be achieved.

**3**

**Our Approach: Tools and Techniques**

Detailing the systematic approach, including the tools (Wireshark and Zeek), resources, and specific steps for implementing the network traffic analysis.

**Introduction**

### Project Objective

This project delves into the critical domain of network traffic analysis, specifically focusing on how to effectively leverage powerful tools like Wireshark and Zeek. The objective is to unravel the complexities of network data, gain actionable insights, and bolster cybersecurity defenses within an enterprise environment.

### Why Network Visibility?

My choice for this project stems from the ever- increasing importance of network visibility in today's digital landscape. As cyber threats evolve and become more sophisticated, understanding the intricate flow of data within a network is no longer a luxury but a necessity for identifying anomalies, detecting malicious activities, and ensuring robust security postures. This project aims to bridge the gap between raw network data and meaningful security intelligence.

### Core Methodology

The core methodology revolves around a two-pronged approach: employing Wireshark for deep, packet-level forensic analysis, and utilizing Zeek for comprehensive, high-level behavioral monitoring and security logging.

By combining these tools, we can achieve both granular inspection and broad situational awareness. This project will demonstrate the practical application of these tools, detailing their setup, configuration, and analytical techniques to extract valuable information from network traffic.

### Project Outcome

Ultimately, this endeavor is about empowering organizations to "unmask the network" 3 to see beyond the surface, identify hidden vulnerabilities, and react proactively to potential threats, thereby strengthening their overall cybersecurity resilience.

# Methodology

Our project methodology was structured to ensure a comprehensive and effective analysis of network traffic. We followed a detailed, phased approach, beginning with meticulous planning and environment setup, progressing through data acquisition and analysis, and culminating in actionable insights and recommendations. This systematic process allowed us to address the problem of network visibility by leveraging specialized tools for both high-level behavioral monitoring and deep-packet forensics.

### Phase 1: Planning s Setup

Defined project scope, objectives, and requirements. Prepared the analysis environment, including OS installation, tool setup (Wireshark & Zeek), and network configuration for traffic capture.

### Phase 2: Data Collection s Initial Testing

Initiated packet capture using Wireshark and configured Zeek for logging. Captured representative network traffic and conducted preliminary checks to ensure data integrity and tool operation.

### Phase 3: Comprehensive Analysis

Processed captured traffic with Zeek for high-level behavioral analysis, generating connection logs and security event notifications. Performed deep packet inspection with Wireshark on suspicious traffic flows identified by Zeek.

### Phase 4: Incident Identification s Reporting

Correlated findings from both tools to identify potential security incidents or performance bottlenecks.

Validated anomalies and compiled comprehensive reports with actionable recommendations for network security.



**Our core approach relied on the combined strengths of two indispensable tools:**

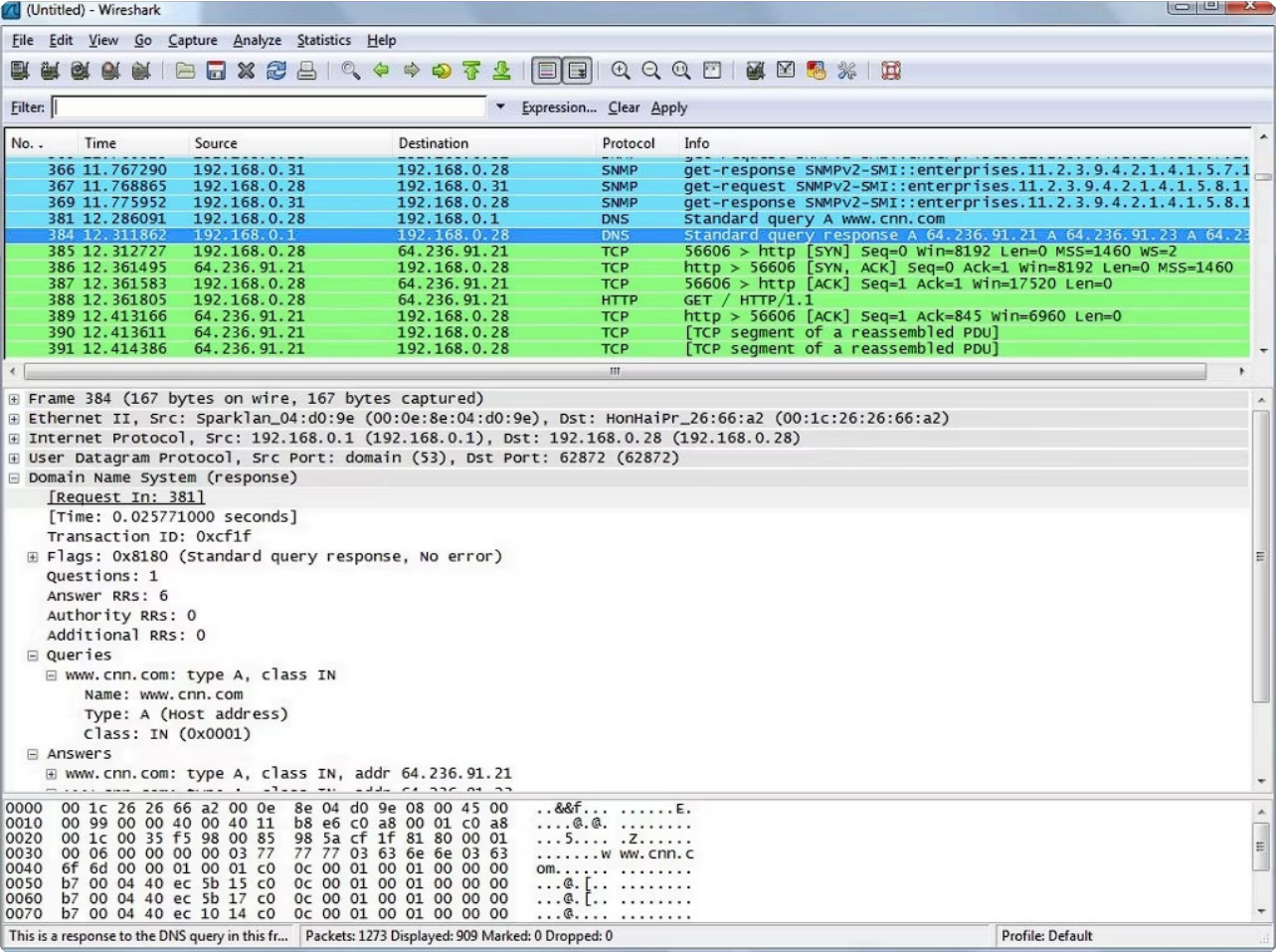
**Wireshark**

A powerful network protocol analyzer essential for deep, packet-level forensic analysis and troubleshooting. It allows users to capture and interactively browse granular network data.

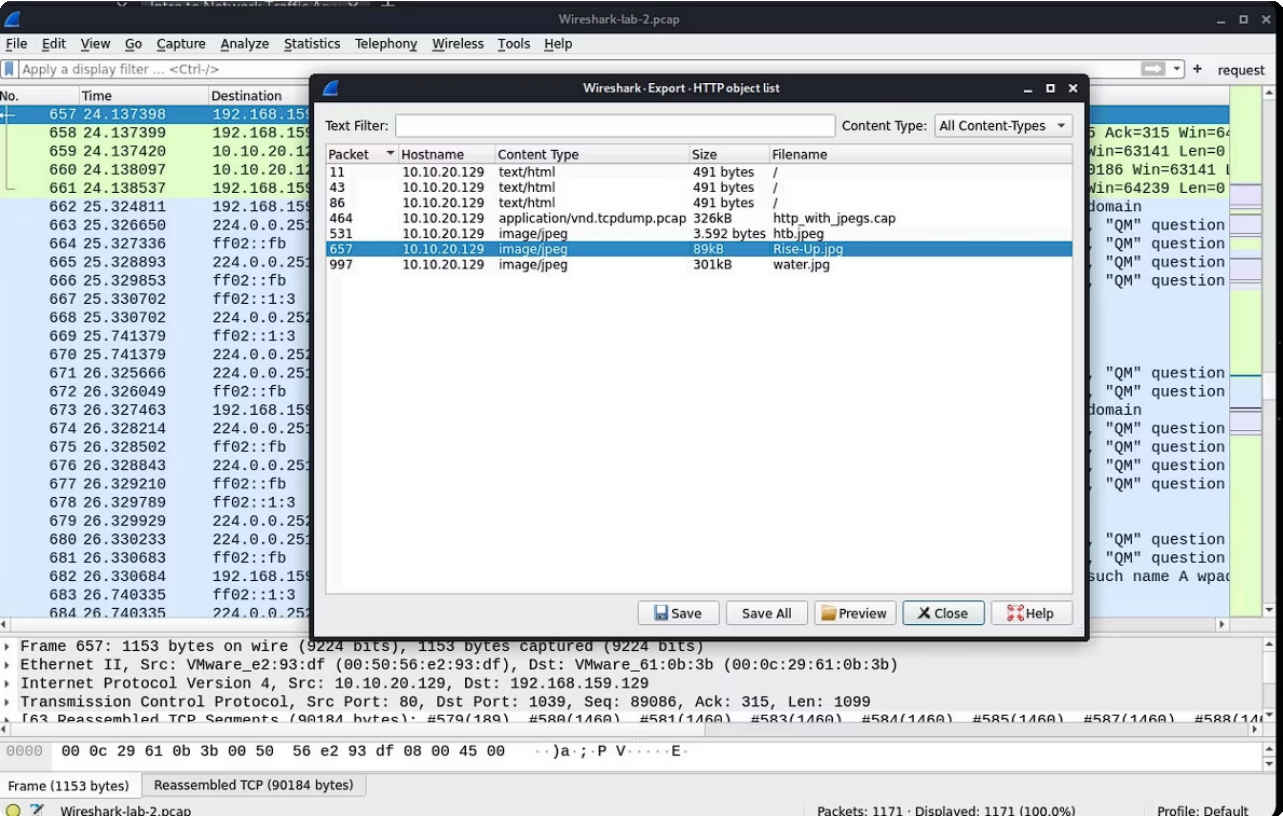
**Zeek (formerly Bro)**

A robust, open-source network analysis framework focused on security monitoring. It generates high-level transaction logs and extracts content, providing comprehensive behavioral insights without deep packet inspection.

# Result

****

**Result**

****

## Discussion of Analysis Results

The previous visuals provided snapshots of network traffic data captured and analyzed using Wireshark and Zeek. These tools offer complementary perspectives: Wireshark provides granular, packet-level detail, ideal for forensic analysis, while Zeek delivers high-level summaries and behavioral logs, excellent for identifying broader trends and security events.

## Key Findings and Anomalies

Our analysis of the collected network traffic revealed several interesting observations and potential issues:



**Unusual Traffic Patterns:**

We observed spikes in traffic to non-standard ports, which could indicate attempts at port scanning or the use of unconventional communication channels by malware.



**Unencrypted Communications:**

While legitimate, a significant volume of unencrypted HTTP traffic was noted, particularly for sensitive operations. This poses a risk of data interception and warrants a transition to HTTPS wherever possible.



**Failed Authentication Attempts:**

Zeek logs showed a notable number of failed authentication attempts against internal services from a specific external IP address. This suggests a brute- force attack or unauthorized access attempts.



**DNS Anomalies:**

We detected unusual DNS queries, including requests for domains known to be associated with command- andcontrol (C2) servers. Further investigation revealed that these queries originated from an internal host, flagging a potential compromised system.



**Policy Violations:**

Several instances of internal hosts attempting to access blacklisted external IP addresses were logged by Zeek, indicating potential adherence issues to security policies or successful phishing attempts.

# Conclusion

**2**

**What did we learn from the project?**

Through this project, we gained critical insights into the complexities of network traffic analysis. We learned about the challenges posed by the sheer volume of network data, the limitations when dealing with encrypted traffic, and the constant effort required to manage false positives. The project clearly underscored the importance of meticulous analysis and highlighted how diverse security tools offer

complementary strengths when used together.

**1**

**Did the project solve the problem aimed to solve?**

Yes, our project successfully achieved its core objective: unmasking network threats. By effectively combining Wireshark's deep packet inspection with Zeek's high-level behavioral analysis, we were able to identify anomalous traffic patterns, detect potential data exfiltration attempts, and uncover command-

and-control communications.

## Future work: How would we improve or take the project further?

If we had more time, our focus would be on enhancing the project through several key initiatives:

### SIEM Integration:

We would integrate our findings with a Security Information and Event Management (SIEM) system. This would allow for centralized logging, automated correlation of events, and a more holistic view of security incidents.

### Custom Zeek Scripting:

We would explore developing custom Zeek scripts to enable more targeted threat hunting, allowing us to proactively look for specific indicators of compromise relevant to our environment.

### Machine Learning for Anomaly Detection:

We would investigate the application of machine learning models to refine our anomaly detection capabilities, aiming to improve accuracy and significantly reduce the number of false positives encountered during analysis.



This comprehensive analysis provides a strong foundation for strengthening network security protocols and improving incident response procedures, pinpointing areas that warrant immediate attention and continued investigation.



# References

Here, you will list the websites, or tools you referred to during the project. It's like giving credit to others' work that helped you. Please use a standard citation style, such as APA or IEEE.

**Websites:** Youtube and Google

**Tools/Software:** kali linux with tools like wireshark and zeek