NSF Award 1829698
CyberTraining CIP: Cyberinfrastructure Expertise on High-throughput Networks for Big Science Data Transfers

Hands-on Zeek (Bro) Labs

Christelle Nader

Zeek Hands-on Labs

Lab 1- Introduction to the Capabilities of Zeek

Lab 2 - An Overview of Zeek Logs

Lab 4 - Generating, Capturing and Analyzing Network Scanner Traffic

Lab 5 - Generating, Capturing and Analyzing DoS and DDoS-centric Network Traffic

Lab 9: Profiling and Performance Metrics of Zeek

Lab 1- Introduction to the Capabilities of Zeek

Lab 1- Introduction to the Capabilities of Zeek

Lab's Description

This lab introduces the capabilities of Zeek

Lab's Importance

This lab introduces Zeek's building blocks to facilitate the comprehension of the remaining set of the labs. In particular, it explains Zeek's layered architecture while demonstrating Zeek's capabilities towards performing network traffic analysis

Lab 1- Introduction to the Capabilities of Zeek

Learning Objectives

- Understand Zeek's layered architecture
- Manage a Zeek instance using the ZeekControl utility
- Generate and analyze live network traffic using Zeek

Lab 2 - An Overview of Zeek Logs

Lab 2 - An Overview of Zeek Logs

Lab's Description

This lab covers Zeek's logging files and basic analytical functions

Lab's Importance

Zeek's event-based engine generates log files based on signatures or events triggered during network traffic analysis. This lab thus explains each logging file and introduces some basic analytic functions and tools.

Lab 2 - An Overview of Zeek Logs

Learning Objectives

- Generate Zeek log files
- Use Linux terminal tools combined with Zeek's zeek-cut utility to customize the output of the logs for analysis
- Manipulate log files for ease of readably and to prepare it for further advanced use

Lab 4 - Generating, Capturing and Analyzing Network Scanner Traffic

Lab 4 - Generating, Capturing and Analyzing Network Scanner Traffic

Lab's Description

This lab provides an in-depth guide to scanning/probing network traffic

Lab's Importance

Given that network scanning is the most abundant type of unsolicited traffic on operational networks, this lab demonstrates the effectiveness of Zeek in analyzing and detecting such traffic.

Lab 4 - Generating, Capturing and Analyzing Network Scanner Traffic

Learning Objectives

- Perform Internet scanning through generating probing events
- Utilize the Nmap software
- Generate and collect scan traffic

Lab 5 - Generating, Capturing and Analyzing DoS and DDoS-centric Network Traffic

Lab 5 - Generating, Capturing and Analyzing DoS and DDoS-centric Network Traffic

Lab's Description

This lab covers Denial of Service (DoS)-based network traffic

Lab's Importance

DoS attacks continue to be one of the most debilitating threat on operational networks. To this end, this labs introduces the capability to generate DoS attack traffic in a controlled environment while showing how zeek can analyze and detect such traffic.

Lab 5 - Generating, Capturing and Analyzing DoS and DDoS-centric Network Traffic

Learning Objectives

- Generate real-time DoS and DDoS traffic
- Experiment with the Low Orbit Ion Canon (LOIC) software
- Analyze collected DDoS traffic

Lab 9: Profiling and Performance Metrics of Zeek

Lab 9: Profiling and Performance Metrics of Zeek

Lab's Description

This lab explains Zeek's profiling log stream and Zeek's resource consumption

Lab's Importance

Monitoring Zeek's online and offline processing performance is key to maintain proper functionality. Unfortunately, Zeek does not come with default performance monitoring capabilities. Thus, in this lab, we demonstrate how we can profile its performance offline as well as use various Linux-based tools to enable online monitoring.

Lab 9: Profiling and Performance Metrics of Zeek

Learning Objectives

- Enable Zeek's profiling log stream for session-based statistics
- Generate customized traffic to be captured by Zeek's profiling
- Implement tools necessary for testing Zeek's resource consumption