PACKET ANALYSIS

This two part course first covers a high-level overview of networking concepts and covers packet tools like Wireshark, TCPdump, Stenographer, and Docket.

The second part of this course covers a high-level overview of network fundamentals to include numbering systems, network addressing, network devices and segmentation, and techniques around capturing traffic. These topics serve as a precursor to packet analysis concepts and cover foundational topics regarding traffic flow.

This course is part of the Elastic Network Security Learning Plan. Please review the pre-reqs section for additional information.

LESSONS

All lessons include a hands-on lab.

Transmission Control Protocol/Internet Protocol Model (TCP)
Use the Transmission Control Protocol/Internet Protocol Model (TCP/IP) to understand how a packet makes its way across the network.

Protocol Basis
Learn how protocols like Ethernet, IPv4, TCP and UDP interact to pass data across the wire.

Numbering Systems
The first lesson covers different numbering systems (decimal, hexadecimal, and binary) along with how each is represented at the packet level.

Network Addressing
Learn how computers and network devices assign values to assist packets moving throughout a network. Topics include MAC and IP addresses along with Network Address Translation (NAT).

Continued on the next page

COURSE INFORMATION

Audience
Security Analysts
System Administrators
Network Administrators

Duration
8 hours

Language
English

Prerequisites
- Linux Fundamentals
- Network Protocol Analysis
- Packet Analysis
- Intrusion Detection System (IDS) log analysis with Suricata
- Network Metadata log analysis with Zeek
- Kibana Security Analyst

Requirements
- Stable internet connection
- Mac, Linux, or Windows
- Latest version of Chrome or Firefox (other browsers not supported)
- Disable any ad blockers and restart your browser before class

elastic

PACKET ANALYSIS

LESSONS

All lessons include a hands-on lab.

Wireshark
This lesson introduces you to a popular network traffic analyzing tool called Wireshark. It covers basic navigation of the tool, filtering syntax and other features of the tool.

Transmissions Control Protocol Dump/Berkeley Packet Filter (TCPdump/BPF)
TCPdump is a major workhorse in capturing and filtering network traffic. This lesson uses the command line to investigate packets using Berkley Packet Filters.

Stenographer/Docket
This lesson covers Stenographer, which is a command line tool that captures and indexes large amounts of packets for quick retrieval and further analysis. Docket is a graphical alternative that allows users to quickly pull packets from Stenographer.

Network Devices and Segmentation
This lesson discusses the different roles devices play when moving packets across networks. You will also learn the different types of routing and how networks can be logically separated with VLANs.

Capturing Traffic
The final lesson compares the two most common ways for capturing network traffic. You will learn the pros and cons of using a network TAP versus implementing a mirrored port (or SPAN port).