SETC Training Corporate Logo

IT Security Training: Inspecting Networks with SNORT (SNORT, 4 jours)

Description

The course Inspecting Networks with SNORT (IT Security Training) is a complete exploration of SNORT from installation and configuration to the development of complex rules for malicious data extraction and network intrusion detection. The training starts with an overview of the theoretical foundations of network data analysis with SNORT. This is followed by a detailed investigation of working with SNORT pre-processors to analyze traffic and detect malicious attacks. The training course also discusses the use of filters and events and the writing of SNORT rules for payload detection, non-payload detection and post detection processing. The training ends with a discussion of best practices and challenges in writing rules and the use of the AppId pre-processor for user created application detectors. Wow! This is quite the jam packet IT security course.

Tarifs

- Tarification: $3,750/person
- Rabais de 10% lorsque vous inscrivez 3 personnes.

Plan de cours

Snort Concepts and Use

Understanding SNORT and its uses

Exploring Modes: Sniffer, Logger and Network Intrusion Detection System

About Packet Acquisition

Reading pcap Files: Practical How To

Reading Basic Output

Exploring Tunneling Protocol Support

About the Control Socket

About the Configure Signal Value

Configuring SNORT

Configuration Overview

Configuration Deep Dive

Using include for IP and Ports

Using Variable Modifiers and Limitations

Configuring Performance Profiling

Making use of Output Modules

Making use of Host Attribution Tables

Understanding the Role of Preprocessors

Working with Preprocessors Part I: Low Level Data

Introducing the Frag3 Preprocessor

Frag3 Format and Basic Configuration

Frag3 Advanced Configuration

Using the Stream and Session Preprocessors

Session Configuration

Stream Configuration

More on Stream: TCP. UDP, ICMP and IP

Working with Preprocessors Part II: Application Protocols

Application Level Capabilities Overview

Inspecting HTTP

Inspecting SMTP

Inspecting POP and IMAP
Inspecting FTP
Inspecting SSH
Inspecting DNS
Inspecting SSL
Inspecting SIP (VOIP)
Working with Preprocessors Part II: Intrusion Detection
Using sfPortscan to Detect an Attack
Configuring sfPortscan Alerts
Tuning sfPortscan
Making use of the Normalizer
Making use of the Reputation Preprocessor
Adding Rules to Reputation using Regular Expressions
Making use of the Sensitive Data Preprocessor
Working with Events and Filters
Overview of Events and Filters
Exploring Rate Filters
Exploring Event Filters
Working with Event Suppression
Working with Event Logging
About Event Tracing
Writing Rules: Concepts and Use
The Structure of a Rule
About Rule Actions
Specifying Protocols and IP Addresses
Specifying Port Numbers and Direction
Exploring PCRE Regular Expressions: Syntax and Use
Exploring Techniques: Byte Jump, Byte Test, and Byte Extract
About Dynamic Rules
Working with Rule Options
Payload Detection Rule Options
Writing Payload Detection Rules
Writing Rules for General Traffic
Writing Rules for HTTP Traffic
Writing Rules for HTTPs Traffic
Writing Rules for Malicious Intent
Writing Rules for SIP
Non-Payload Detection Rule Options
Writing Non-Payload Detection Rules
Writing Rules for TOS, TTL and IP Options
Writing Rules for Packet Fragmentation and Flow
Writing Rules for IP Protocol
Writing Rules for TCP Communication: SEQ, ACK and More
Writing Rules for ICMP
Writing Rules for RPC
Post-Detection Rule Options
Overview of Post-Detection Rule Options
Logging and Session Management
Combining Packets with tag
Implementing Conditional Rules that Respond to Events

- Dynamically Replacing Packet Content
- Implementing Conditional Events

Writing Good Rules

- Theoretical and Practical Rule Writing Challenges
- Content Matching
- Catch the Vulnerability, Not the Exploit
- Catch the Oddities of the Protocol in the Rule
- Optimizing Rules
- Testing Numerical Values

Using the AppId Pre-Processor

- Dependency Requirements
- Preprocessor Configuration
- Rule Options
- Application Rule Events
- Application Usage Statistics
- Open Detector Package (ODP) Installation
- User Created Application Detectors