

IT Security Training: Network Forensics Analysis (NFORE, 4 jours)

Description

The course Network Forensics Analysis (IT Security Training) explores the complexities of gathering digital evidence over a network. The training starts with a general discussion of evidence types and related evidence gathering techniques. This is followed by a detailed exploration of the fundamental tools of the digital forensics trade including the Squid proxy server, common packet analysis tools including tcpdump, Wireshark and NetFlow. The course includes a detailed study of application level protocols and services, firewalls, intrusion detection systems (IDS) and network security managers. The training concludes with an exploration of centralized logging, the Elastic Stack, wireless network considerations, encryption and SSL inspection.

Tarifs

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

Plan de cours

Network Fundamentals (Only if necessary)

The OSI Reference Model and Packet Structure

Essential IP Concepts: IP Addresses and Subnets

Obtaining an IP Address: Static and Dynamic Addressing

Essential IP Concepts: Transport Protocols (TCP and UDP)

IP Behavior: Understanding Sockets, Ports and Application Protocols

Understanding Routers and Layer 3 Switches

Working with and Understanding VLANs

Exploring VOIP Technologies

Introduction to Forensic Network Analysis

What is Forensic Analysis

What is valid Evidence?

Overview of Digital Forensic Analysis

More about Network Evidence Acquisition

Core Types of Network Evidence: Full Packet, Logs and NetFlow

The Importance of Data Integrity: Why SPAN ports are not sufficient

Exploring Capture Devices: NetFlow, Switches, TAPs and Layer 7 Devices

The Fundamental Tools of the Trade: The Squid

Understanding the Requirements of Forensic Analysis

Designing our Network for Forensic Analysis

The role of the Caching Proxy Server

Configuring the Squid Proxy Server

Configuring Logging in Squid

Configuring Squid Log Analysis Software

Configuring and Working with Cache Extraction

The Fundamental Tools of the Trade: Packet Analysis

Understanding Network Packet Structure

Setting up tcpdump

Exploring tcpdump options

Limiting Data Captured with tcpdump

Searching Trace results with grep

Installing the latest Version of Wireshark

Setting up Filters in Wireshark

Using Wireshark to Inspect Packets

Packet Capture Tips and Tricks

Key Application Level Protocols: HTTP

Exploring HTTP based Communications

Reviewing the HTTP Specification

Understanding HTTP Behavior in a Routed Scenario

Understanding HTTP Header Structure and Key Fields

Analyzing HTTP Request and HTTP Response

Extracting Artifacts

Implementing Logging

Applying Forensic Methodology to HTTP

Exploring and Analyzing FTP Traffic

Key Application Level Protocols: DNS

How DNS Servers Operate

Reviewing Common DNS Operations: Name Resolution, Zone Transfers and More

How Tunneling Works

Exploring Fast Flux and DGAs

Implementing Logging

Common uses of DNS in Attack Strategies

Exploring Amplification Attacks

Firewalls, Intrusion Detection Systems and Network Security Monitoring

The Role of Firewalls and Intrusion Detection Systems

The Role of Network Security Monitoring

Implementing Firewall Rules: Windows, Linux and Cisco

Exploring NAT and Masquerade

Implementing Firewall Logging

Implementing Intrusion Detection Systems

Implementing Network Security Monitoring

Exploring Bro NSM Features and Functionality

Implementing Bro NSM

Implementing Centralized Logging

Exploring the syslog Specification

Exploring Event Format

Implementing a syslog Central Server

Making use of rsyslog and other Tools

Exploring Microsoft Eventing

Exploring Log Aggregation: Benefits and Vulnerabilities

Implementing a Log Aggregation Solution

Working with Elastic Stack

What is the Elastic Stack?

The Specific Roles of Elastisearch, Logstash and Kibana

About the Elastic Stack and Log Aggregation

Installing an Elastisearch Server

Installing and Configuring Logstash

Using Kibana for Powerful Visualizations

NetFlow and Traffic Analysis

Exploring NetFlow Architecture, Components and Protocols

Configuring NetFlow on Cisco Routers

Examining Traffic using NetFlow

Using NetFlow for Encrypted Traffic

Using NetFlow for Linux Traffic: NFS, SSH and Apache

Using NetFlow with Microsoft Protocols: Exchange, Outlook, SMB and IIS

Modern Communications: Wireless Networks

Understanding Wireless Communication and Authentication

Exploring Authentication: WEP vs WPA

Hardware and Software Based Packet Capture

Exploring Useful Protocol Fields

Using Hardware: PineApple WIFI Device

Using Software: aircrack-ng and Aircrack-ng

Working with Moloch

Working with NetworkMiner

The Magic of SSL

Exploring Encryption Algorithms: Symmetric vs Asymmetric

More on Asymmetric Encryption: AES and RSA

Exploring a Typical HTTPS Session

Profiling SSL Sessions

Exploring Perfect Forward Secrecy and its Requirements

The Mechanics of a Man In The Middle (MITM) Attack

Performing Network Protocol Reverse Engineering Attacks

Putting it All Together
