Cyber Security & ANTI-HACKING Workshop (HACK)

ID HACK **Price** 2,980.— €(excl. tax) **Duration** 4 days

LIVE hacking, attack techniques, and countermeasures: Learn all about hacker's approaches and techniques!

Course Overview

Cybersecurity, attack techniques, and countermeasures: Learn about the latest hacker techniques and find out how to defend yourself against advanced attacks with limited security budget and time. The course uses realistic exercises to teach the basics of cybersecurity. The selection of the practical course content is based on the prestigious Mitre Att&ck project. The theoretical part is based on industry standards such as: NIST Standards, CIS Benchmarks, OWASP and PTES. In the course, we consistently change the perspective between attack and defense on every topic. This enables participants to derive direct defensive measures and quick wins from the experience of the practical laboratory exercises. The course is also discusses advanced topics such as antivirus bypass, WAFs, intrusion protection systems, firewalls, spam gateways, proxy whitelisting, sandboxes, EDRs, and XSS filters.

Who should attend

The entry-level course is aimed primarily at IT security officers, IT administrators (client, server, network), programmers, IT engineers, and security operation center (SOC) operators, as well as anyone who wants evaluate security risks from an attacker's perspective in order to defend.

Prerequisites

- Basic computer skills

Course Objectives

The aim of the course is to impart technical and organizational knowledge in the field of IT security, so that the participants can make meaningful decisions in their daily work with the goal of efficient and sustainable improvement of IT security. Numerous hands-on exercises enable you to detect, repel, or address existing vulnerabilities.

Course Content

- Course content
- Cybersecurity basics
- Current threat situation
- Social Engineering
- Infrastructure security
- Linux Security
- Windows Security
- Post Exploitation
- Defense in Depth
- Detect attacks
- Web Security
- Denial of Service
- Network Security

Detailed Course Outline

Detailed course content

Cybersecurity Basics

- What is hacking?
- What is IT security?
- Attacker types, motivation and tactics
- General definitions and metrics
- Mitre Att&ck

Social Engineering

- Types of social engineering
- Examples of pentests and current campaigns
- Detect and prevent phishing
- Email-based attacks
- Browser-based attacks
- Attacks with peripherals
- Exploit vs. Social Engineering
- Physical attacks

Infrastructure Security

- Introduction of the attack chain
- Footprinting, Discovery
- Enumeration, Port Scanning
- Storage of passwords
- Hashing procedure
- Online / Offline brute forcing
- Pros and cons of password policies
- Shells
- Classification and assessment of vulnerabilities
- Command Injections
- Introduction to Metasploit

Linux Security

- Linux Basics
- Linux Exploitation
- Lateral Movement and Pivoting
- Privilege Escalation
- Post Exploitation
- Case studies

Windows Security

- Windows Basics
- Active Directory Basics
- Windows Credential System
- IPS Evasion
- Pivoting
- Memory Corruptions
- Exploit Mitigations
- Meterpreter Advanced
- Proxy Whitelisting Evasion
- Keylogging
- Pass the Hash (PTH)
- Pass the Ticket (PTT)
- Kerberoasting
- Native Malware, Powershell Malware, .NET Malware
- Empire Post Exploitation
- A/V Evasion
- Spoofing attacks
- Exfiltration and C+C
- Client Side Exploitation
- Mimikatz
- AD Persistenz (Golden Tickets, Silver Tickets)
- Impersonation
- Volatility
- Sysinternals Tools
- Library Hijacking

Post Exploitation

- Post Exploitation Overview
- Advanced Post Exploitation
- Native and meterpreter commands for post exploitation
- Living off the Land Attacks
- Fileless Malware
- Lateral Movement (RDP, WMI, WinRM, DCOM RPC)
- Windows hardening

Defense in Depth

- Introduction to concept Defense in Depth
- The Kill Chain
- Basic network defense
- Basics of ISMS
- Advanced network defense
- Threat modelling and protection crown jewels
- Construction and operation of Security Operation Centers
- Incident Response Guidelines
- Threat Intelligence

Web Security

- Introducing web applications, services and http
- OWASP TOP 10
- Mapping a website
- Working with Intercepting Proxies
- Using Browser Developer Tools
- Web vulnerabilities server-side (SSRF, Command Injections, Deserialization, SQLi, File Inclusion)
- Web vulnerabilities browser supported (XSS, XSRF, etc)
- Vulnerabilities in Web Services

Network Security

- Introduction Wireshark and Scapy
- Different types of MiTM attacks
- Sniffing and injection
- Switching security
- Microsegementation
- Wifi security main threats
- Attacks on TCP/IP Stack
- TCP, UDP, IPv4/ IPv6 Threats
- Network Access Control

Secure communication

- Encryption basics
- Various cryptosuites
- Public Key Infrastructure
- Krypto Hardening
- Practical use of cryptography
- Introduction to TLS/SSL
- TLS/SSL attacks and defense
- Disk encryption

Denial of Service

- Types of Denial of Service
- Motives of the attackers
- Memory Corruption DoS
- Focus on volume-based DDoS
- Denial of Service defense
- Incident Response at DoS

Exercises

Basics

- Setting up a phishing page
- DNS Reconnaissance
- Port Scanning
- IIS Double Decode

Linux

- Exploitation of a Linux server
- Post Exploitation of the Linux Server
- Linux Lateral Movement
- Heartbleed
- Dev Ops compromise

Windows

- Pivot to Windows
- Lateral Movement in Active Directory
- Post Exploitation with Empire
- Kerberoasting
- Windows Client Side Exploitation
- Stack Buffer Overflow
- Windows Post Exploitation
- Extraction of meterpreter from process memory

Web

- Web Bruteforcing
- XSS Vulnerability
- SQL Injection
- Exploitation Wordpress RCE

Networking

- Scapy Basics
- Analysis of MiTM attacks
- Wireshark Basics
- VoIP eavesdropping on WebRTC traffic
- TLS stripping with HSTS bypass

Demos

- Attack on Keepass
- Windows DLL Hijacking
- Exploitable cronjob
- Examples of Virustotal and Any.run
- CSRF Demo
- Backdoor with MSFvenom
- Targeted breaking of an A/V signature

Case Studies

- Debian SSH Vulnerability
- XSS Evasion
- Fuzzing of a Memory Corruption DoS
- Linux Command Injections
- Linux Exploitation with Metasploit
- Itch Web App
- Root on Sisyphus

About Fast Lane

Fast Lane is a global, award-winning specialist in technology and business training as well as consulting services for digital transformation. As the only global partner of the three cloud hyperscalers- Microsoft, AWS and Google- and partner of 30 other leading IT vendors, Fast Lane offers qualification solutions and professional services that can be scaled as needed. More than 4,000 experienced Fast Lane professionals train and advise customers in organizations of all sizes in 90 countries worldwide in the areas of cloud, artificial intelligence, cyber security, software development, wireless and mobility, modern workplace, as well as management and leadership skills, IT and project management.

Fast Lane Services

✓ High End Technology Training
✓ Business & Soft Skill Training
✓ Consulting Services
✓ Managed Training Services
✓ Digital Learning Solutions
✓ Content Development
✓ Remote Labs
✓ Talent Programs
✓ Event Management Services

Training Methods

✓ Classroom Training
✓ Instructor-Led Online Training
✓ FLEX Classroom – Classroom & Online Hybrid
✓ Onsite & Customized Training
✓ E-Learning
✓ Blended & Hybrid Learning
✓ Mobile Learning

Technologies & Solutions

✓ Digital Transformation
✓ Artificial Intelligence
✓ Cloud
✓ Networking
✓ Cyber Security
✓ Wireless & Mobility
✓ Modern Workplace
✓ Data Center

Worldwide Presence
with high-end training centers around the globe

Multiple Awards
from vendors such as AWS, Microsoft, Cisco, Google, NetApp, VMware

Experienced SMEs
with over 19.000 combined certifications

Germany
Fast Lane Institute for Knowledge Transfer GmbH
Tel. +49 40 25334610

info@flane.de / www.flane.de

Austria
ITLS GmbH
(Partner of Fast Lane)
Tel. +43 1 6000 8800

info@itls.at / www.itls.at

Switzerland
Fast Lane Institute for Knowledge Transfer (Switzerland) AG
Tel. +41 44 8325080

info@flane.ch / www.flane.ch