Cyber Security & ANTI-HACKING Workshop (HACK)

ID HACK **Price** 3,490.— €(excl. tax) **Duration** 4 days

Course Overview

Cyber security, attack techniques and countermeasures

Learn the latest techniques used by hackers and how to effectively defend against advanced attacks. In a time of limited security budgets, staff shortages and strict security standards, our workshop provides IT administrators, security officers and SOC analysts with the guidance they need.

Among other things, our workshop covers specific attack techniques for Linux and Windows, authentication processes, web and cloud security as well as methods for defending against ransomware and protecting infrastructures. The hands-on exercises are based on the prestigious Mitre ATT&CK project and actual attacks observed at customer sites. The theoretical part is based on industry standards such as the BSI baseline protection compendium and the CIS benchmarks and continuously integrates new content from security vendor reports, conference talks, news feeds, research papers and technical blogs.

In the course, we consistently switch between the perspective of the attacker and the defense. This enables participants to derive defense measures and quick wins directly from the practical lab exercises. Equip your organization with the knowledge to fend off 0-day and 1-day attacks and meet the requirements of the GDPR and NIS2 regulations.

The course is rounded off with advanced topics such as antivirus evasion, next-generation firewalls, XDRs, proxy whitelisting, sandboxes, EDRs and XSS filters. A special feature of our course compared to other basic cyber security courses and certification courses is that we do not dwell on outdated basics and attack techniques that are irrelevant today, but focus on the really important topics. We also provide space for questions that go beyond the course content.

At the end of the course, we take 30 minutes for an Ask Me Anything (AmA) to facilitate a discussion between the participants and the trainer. This provides an opportunity to talk about current projects and topics that are relevant to the participants but were not covered in the course.

Lab

The lab environment includes a powerful, fully dedicated lab per participant with more than 35 virtual cores and over 80 GB of RAM. The lab environment has a large bandwidth and low latency. It is accessed via a web browser and does not require any software to be installed.

Bonus

As a bonus, after completing the 4-day Cyber Security & ANTI-HACKING workshop, you will receive an additional day of full access to the hacking lab presented in the course. This additional day gives you the opportunity to deepen the attack techniques discussed and to independently get to know further attack scenarios in the lab. The exercises require creativity, technical knowledge and tenacity. You will also have time to repeat the exercises discussed in the course.

Who should attend

This beginner's course is aimed at IT security officers, IT administrators (client, server, network), programmers, IT engineers and Security Operation Center (SOC) operators as well as anyone who wants to view security risks from the perspective of the attacker and thus develop solution scenarios.

Prerequisites

- Experience with the operation and administration of IT systems
- Basic IT security knowledge

Course Objectives

The aim of the course is to impart technical and organizational knowledge in the field of IT security so that participants can make sensible decisions in their daily work to improve IT security

efficiently and sustainably. Numerous practical exercises will enable you to recognize and ward off attacks or to close or reduce existing security gaps.

Course Content

- Basics of cyber security
- Current trends
- Initial infection
- Infrastructure security
- Linux attacks
- Windows attacks
- Post-exploitation
- Active Directory
- Post Exploitation
- Defense in Depth
- Ransomware
- Ask me Anything
- Web Security
- Denial of Service
- Network Security

Detailed Course Outline

Cybersecurity basics

- What is hacking?
- What is IT security?
- Attackers, motivation and tactics
- General definitions and metrics
- Attack techniques and tactics according to Mitre Att&ck

Current trends

- Current metrics
- Proven attack techniques
- Cybersecurity trends and current threat situation

Initial infection

- Types of social engineering
- Password-based attacks
- Advantages and disadvantages of password policies
- Phishing and bypassing MFA / 2FA
- M365 attacks
- Adversary-in-the-browser attack
- Browser-in-the-browser attack
- Recognizing and preventing phishing
- Email-based attacks
- Browser-based attacks
- Attacks with peripheral devices
- Exploit vs. social engineering
- Physical attacks

Infrastructure security

- Introduction of the attack chain
- Enumeration and footprinting
- Discovery and port scanning
- Off-line cracking
- Reverse and bind shells
- Evaluation of vulnerabilities
- Command injections, webshells and SSRF
- Introduction to Metasploit

Linux Security

- Linux basics
- Linux Exploitation
- Lateral movement and pivoting
- Privilege Escalation
- Post-exploitation
- Case Studies

Windows Security

- Windows basics
- Windows Credential System
- NG Firewall Invasion
- Pivoting
- Memory Corruptions
- Exploit Mitigations
- Meterpreter advanced
- Keylogging
- Client-Side Exploitation
- Sysinternals Suite
- Library hijacking

Active Directory Security

- Active Directory basics
- Coercion attacks
- Passing on the hash (PTH)
- Passing on the ticket (PTT)
- Golden tickets, silver tickets
- Impersonation
- Kerberoasting
- Over-pass the Hash / Pass the Key
- Skeleton key
- Machine account quota
- AdminSDHolder
- Enterprise access model
- Privileged Access Workstations

Evasion

- Native Malware, Powershell Malware, .NET Malware
- A/V evasion
- Exfiltration and C+C

Post-exploitation

- Native and meterpreter commands for post-exploitation
- Living-off-the-land attacks
- Fileless malware
- Lateral Movemenent (RDP, WMI, WinRM, DCOM RPC)

Defense in Depth

- Windows hardening
- Active Directory Hardening
- The Kill Chain
- Network defense
- Basics of ISMS
- Advanced network defense
- Threat modeling and protecting crown jewels
- Setting up and operating security operation centers
- Incident response policies
- Threat intelligence

Ransomware defense

- Backup strategy
- RPO and RTO
- Recovery strategy
- Ransomware protection
- To pay or not to pay?
- Decryption considerations
- Tools

Web security

- Introduction to web applications, services and http
- OWASP TOP 10
- Dealing with browser developer tools
- Web vulnerabilities on the server side (SSRF, command injections, deserialization, SQLi, file inclusion)
- Browser-supported web vulnerabilities (XSS, XSRF, etc)
- Vulnerabilities in web services

Ask me Anything with trainer

- Open question and answer session
- Discussion of current projects
- Deepening

Network security

- Introduction to 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
- Different cryptosuites
- Public key infrastructures
- Crypto-Hardening
- Practical use of cryptography
- Introduction to TLS/SSL
- TLS/SSL attacks and defense
- Hard disk encryption

Denial of service

- Types of denial of service
- Motives of the attackers
- Memory corruption DoS
- Focus on volume-based DDoS
- Defense against denial of service
- Incident response for DoS

Case studies and exercises

Basics

- Setting up a phishing page
- DNS reconnaissance
- Port scanning
- Exchange-Exploitation

Linux

- Exploitation of a Linux server
- Post-exploitation of the Linux server
- Linux lateral movement
- Heartbleed

Windows

- Pivot to Windows
- Lateral movement in Active Directory - Coercion attack
- Kerberoasting
- Post-Exploitation

Web

- Web bruteforcing

- XSS vulnerability
- SQL Injection
- Exploitation Wordpress RCE

Networking

- Scapy basics
- Analysis of MiTM attacks
- Wireshark basics
- VoIP interception of WebRTC traffic
- TLS stripping with HSTS bypass

Demos

- Attack on Keepass
- Windows DLL hijacking
- Examples from Virustotal and Any.run
- Backdoor with MSFvenom
- Targeted breaking of an A/V signature

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