Cyber Security & ANTI-HACKING Workshop (HACK)

ID HACK **Preis** 2.980,– € (exkl. MwSt.) **Dauer** 4 Tage

Als Bonus zum 4-tägigen Cyber Security & ANTI-HACKING Workshop haben Sie für den Tag nach dem Kursende noch vollen Zugriff auf das bereits im Kurs vorgestellten Hacking Labor. Dieser zusätzliche Tag gibt den Ihnen die Möglichkeit aus dem Büro oder von zu Hause aus drei tiefergehende Übungen zu lösen. Für die Lösung ist eine Kette von komplexeren Angriffstechniken notwendig. Sie bekommen verschiedene Lösungshinweise, so dass Sie die Übungen in jedem Fall vollständig selbstständig lösen können. Die Übungen erfordern Kreativität, technisches Wissen und Hartnäckigkeit. Folgende typischen Bereiche werden abgedeckt:

- Infrastruktur Hacking
- Umgehen von Sicherheitsmechanismen
- Web Hacking
- Remote Exploitation
- Privilege Escalation

Kursüberblick

Cybersicherheit, Angriffstechniken und Gegenmaßnahmen: Lernen Sie aktuelle Techniken von Hackern kennen und finden Sie heraus, wie Sie sich mit beschränktem Sicherheitsbudget und beschränkter Zeit gegen fortgeschrittene Angriffe wehren können. Der Kurs lehrt anhand realistischer Übungen die Grundlagen der Cybersicherheit. Die Auswahl des praktischen Kursinhaltes orientiert sich dabei an dem angesehenen Mitre Att&ck Projekt. Der theoretische Teil basiert auf Industriestandards wie: BSI Grundschutz, CIS Benchmarks, OWASP und PTES. Im Kurs wechseln wir bei jedem Thema konsequent die Perspektive zwischen Angriff und Verteidigung. Dies befähigt die Teilnehmer direkt Verteidigungsmaßnahmen und Quick Wins aus den Erfahrungen mit dem praktischen Laborübungen abzuleiten. Der Kurs wird durch fortgeschrittene Themen, wie die Umgehung von Antivirus, WAFs, Intrusion Protection Systeme, Firewalls, Spam Gateways, Proxy Whitelisting, Sandboxes, EDRs und XSS Filter abgerundet.

Zielgruppe

Dieser Einsteigerkurs richtet sich vor allem an IT Sicherheitsbeauftragte, IT Administratoren (Client, Server, Netzwerk), Programmierer, IT Ingenieure und Security Operation Center (SOC) Operatoren, sowie alle, die Security-Risiken auch durch die Brille des Angreifers betrachten und dadurch Lösungsszenarien aufbauen möchten.

Voraussetzungen

- Erfahrungen mit dem Betrieb und Administration von IT-Systemen
- Grundlegende IT-Security Kenntnisse

Kursziele

Das Ziel des Kurses ist die Vermittlung von technischem und organisatorischem Wissen im Bereich der IT Sicherheit, so dass die Teilnehmer in Ihrem täglichen Aufgabengebiet sinnvolle Entscheidungen zur effizienten und nachhaltigen Verbesserung der IT Sicherheit treffen können. Zahlreiche praktische Übungen versetzen Sie in die Lage, Angriffe zu erkennen, abzuwehren oder vorhandene Sicherheitslücken zu schließen bzw. zu verringern.

Kursinhalt

- Cybersicherheit Grundlagen
- Aktuelle Bedrohungslage
- Social Engineering
- Infrastruktur Sicherheit
- Linux Sicherheit
- Windows Sicherheit
- Post Exploitation
- Defense in Depth
- Angriffe erkennen
- Web Security
- Denial of Service
- Network Security

Detaillierter Kursinhalt

Cybersicherheit Grundlagen

- Was ist Hacking?
- Was ist IT Sicherheit?
- Angreifertypen, Motivation und Taktiken
- Allgemeine Begriffsdefinitionen und Metriken
- Mitre Att&ck

Social Engineering

- Arten von Social Engineering
- Beispiele aus Pentests und aktuellen Kampagnen
- Phishing erkennen und verhindern
- E-Mail basierte Angriffe
- Browser basierte Angriffe
- Angriffe mit Peripheriegeräten
- Exploit vs. Social Engineering
- Physische Angriffe

Infrastruktur Sicherheit

- Einführung der Angriffskette
- Footprinting, Discovery
- Enumeration, Port Scanning
- Speicherung von Passwörtern
- Hashingverfahren
- Online / Offline Bruteforcing
- Vor- und Nachteile von Passwortpolicies
- Shells
- Klassifizierung und Bewertung von Verwundbarkeiten
- Command Injections
- Einführung in Metasploit

Linux Sicherheit

- Linux Grundlagen
- Linux Exploitation
- Lateral Movement und Pivoting
- Privilege Escalation
- Post Exploitation
- Fallstudien

Windows Sicherheit

- Windows Grundlagen
- Active Directory Grundlagen
- Windows Credential System
- IPS Evasion
- Pivoting
- Memory Corruptions
- Exploit Mitigations
- Meterpreter Fortgeschritten
- 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 Angriffe
- Exfiltration und C+C
- Client Side Exploitation
- Mimikatz
- AD Persistenz (Golden Tickets, Silver Tickets)
- Impersonation
- Volatility
- Sysinternals Tools
- Library Hijacking

Post Exploitation

- Post Exploitation Übersicht
- Fortgeschrittene Post Exploitation
- Native und Meterpreter Befehle für Post Exploitation
- Living off the Land Angriffe
- Fileless Malware
- Lateral Movemenent (RDP, WMI, WinRM, DCOM RPC)
- Windows Härtung

Defense in Depth

-
- Einführung in das Konzept Defense in Depth
- Die Kill Chain
- Basis Netzwerkverteidigung
- Grundlagen der ISMS
- Fortgeschrittene Netzwerkverteidigung
- Threat Modelling und Schützen von Kronjuwelen
- Aufbau und Betrieb von Security Operation Centern
- Incident Response Richtlinien
- Threat Intelligence

Web sicherheit

- Einführung Web Anwendungen, Dienste und http
- OWASP TOP 10
- Kartographieren einer Webseite
- Umgang mit Intercepting Proxies
- Umgang mit Browser Developer Tools
- Web Verwundbarkeiten serverseitig (SSRF, Command Injections, Deserialisation, SQLi, File Inclusion)
- Web Verwundbarkeiten browserunterstüzt (XSS, XSRF, etc)
- Verwundbarkeiten in Web Diensten

Netzwerksicherheit

- Einführung Wireshark und Scapy

- Verschiedene Arten von MiTM Angriffen
- Sniffing und Injektion
- Switching Sicherheit
- Microsegementation
- Wifi Sicherheit Hauptbedrohungen
- Angriffe auf TCP/IP Stack
- TCP, UDP, IPv4/ IPv6 Bedrohungen
- Network Access Control

Sichere Kommunikation

- Verschlüsselungsgrundlagen
- Verschiedene Kryptosuites
- Public Key Infrastrukturen
- Krypto Hardening
- Praktischer Einsatz von Kryptografie
- Einführung in TLS/SSL
- TLS/SSL Angriffe und Verteidigung
- Festplattenverschlüsselung
-

Denial of Service

- Arten von Denial of Service
- Motive der Angreifer
- Memory Corruption DoS
- Fokus auf volumenbasierte DDoS
- Verteidigung gegen Denial of Service
- Incident Response bei DoS

Übungen

Basics

- Aufsetzen einer Phishing Seite
- DNS Reconnaissance
- Port Scanning
- IIS Double Decode

Linux

- Exploitation eines Linux Servers
- Post Exploitation des Linux Servers
- Linux Lateral Movement
- Heartbleed
- Dev Ops Kompromittierung

Windows

- Pivot zu Windows
- Lateral Movement im Active Directory
- Post Exploitation mit Empire
- Kerberoasting
- Windows Client Side Exploitation
- Stack Buffer Overflow
- Windows Post Exploitation
- Extraktion von Meterpreter aus Prozessspeicher

Web

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

Networking

- Scapy Grundlagen
- Analyse von MiTM Angriffen
- Wireshark Basics
- VoIP Abhören von WebRTC Verkehr
- TLS Stripping mit HSTS Bypass

Demos

- Angriff auf Keepass
- Windows DLL Hijacking
- Exploitbarer Cronjob
- Beispiele von Virustotal und Any.run
- CSRF Demo
- Backdoor mit MSFvenom
- Gezieltes Brechen einer A/V Signatur

Case Studies

- Debian SSH Verwundbarkeit
- XSS Evasion
- Fuzzing eines Memory Corruption DoS
- Linux Command Injections
- Linux Exploitation mit Metasploit
- Itch Webanwendung
- Root auf Sisyphus

Über Fast Lane

Fast Lane ist weltweiter, mehrfach ausgezeichneter Spezialist für Technologie und Business-Trainings sowie Beratungsleistungen zur digitalen Transformation. Als einziger globaler Partner der drei Cloud-Hyperscaler Microsoft, AWS und Google und Partner von 30 weiteren führenden IT-Herstellern bietet Fast Lane beliebig skalierbare Qualifizierungslösungen und Professional Services an. Mehr als 4.000 erfahrene Fast Lane Experten trainieren und beraten Kunden jeder Größenordnung in 90 Ländern weltweit in den Bereichen Cloud, künstliche Intelligenz, Cybersecurity, Software Development, Wireless und Mobility, Modern Workplace sowie Management und Leadership Skills, IT- und Projektmanagement.

Fast Lane Services

- ✓ Highend-Technologietraining
- ✓ Business- & Softskill-Training
- ✓ Consulting Services
- ✓ Managed Training Services
- ✓ Digitale Lernlösungen
- ✓ Content-Entwicklung
- ✓ Remote Labs
- ✓ Talentprogramme
- ✓ Eventmanagement-Services

Trainingsmethoden

- ✓ Klassenraumtraining
- ✓ Instructor-Led Online Training
- ✓ FLEX Classroom – Klassenraum und ILO kombiniert
- ✓ Onsite & Customized Training
- ✓ E-Learning
- ✓ Blended & Hybrid Learning
- ✓ Mobiles Lernen

Technologien und Lösungen

- ✓ Digitale Transformation
- ✓ Artificial Intelligence (AI)
- ✓ Cloud
- ✓ Networking
- ✓ Cyber Security
- ✓ Wireless & Mobility
- ✓ Modern Workplace
- ✓ Data Center

Weltweit vertreten
mit High-End-Trainingszentren rund um den Globus

Mehrfach ausgezeichnet
von Herstellern wie AWS, Microsoft, Cisco, Google, NetApp, VMware

Praxiserfahrene Experten
mit insgesamt mehr als 19.000 Zertifizierungen

Deutschland
Fast Lane Institute for Knowledge Transfer GmbH
Tel. +49 40 25334610
info@flane.de / www.flane.de

Österreich
ITLS GmbH
(ITLS ist ein Partner von Fast Lane)
Tel. +43 1 6000 8800
info@itls.at / www.itls.at

Schweiz
Fast Lane Institute for Knowledge Transfer (Switzerland) AG
Tel. +41 44 8325080
info@flane.ch / www.flane.ch