Cyber Security & ANTI-HACKING Workshop (HACK)

ID HACK **Preis** 3.490,– € (exkl. MwSt.) **Dauer** 4 Tage

Cybersicherheit, Angriffstechniken und Gegenmaßnahmen

Erlernen Sie die neuesten Techniken von Hackern und erfahren Sie, wie Sie sich effektiv gegen fortschrittliche Angriffe verteidigen können. In Zeiten begrenzter Sicherheitsbudgets, personeller Engpässe und strenger Sicherheitsstandards bietet unser Workshop IT-Administratoren, Sicherheitsbeauftragten und SOC-Analysten die notwendige Orientierung.

Unser Workshop behandelt unter anderem spezifische Angriffstechniken für Linux und Windows, Authentifizierungsprozesse, Web- und Cloud-Sicherheit sowie Methoden zur Abwehr von Ransomware und zum Schutz von Infrastrukturen. Die praxisorientierten Übungen basieren auf dem angesehenen Mitre ATT&CK Projekt und aktuellen Angriffen, die bei Kunden beobachtet wurden. Der theoretische Teil stützt sich auf Industriestandards wie das BSI-Grundschutz-Kompendium und die CIS-Benchmarks und integriert kontinuierlich neue Inhalte aus Berichten von Sicherheitsherstellern, Konferenzvorträgen, Newsfeeds, Forschungspapern und technischen Blogs.

Im Kurs wechseln wir konsequent zwischen der Perspektive des Angreifers und der Verteidigung. Dies befähigt die Teilnehmer, aus den praktischen Laborübungen direkt Verteidigungsmaßnahmen und Quick-Wins abzuleiten. Rüsten Sie Ihr Unternehmen mit dem Wissen aus, um 0-Day- und 1-Day-Angriffe abzuwehren und die Anforderungen der GDPR- und NIS2-Verordnungen zu erfüllen.

Der Kurs wird durch fortgeschrittene Themen abgerundet, wie die Umgehung von Antivirus-Programmen, Next-Generation Firewalls, XDRs, Proxy-Whitelisting, Sandboxes, EDRs und XSS-Filtern.

Ein besonderes Merkmal unseres Kurses im Vergleich zu anderen Cybersicherheits-Basiskursen und Zertifizierungskursen ist, dass wir uns nicht mit veralteten Grundlagen und heute irrelevanten Angriffstechniken aufhalten, sondern uns auf die wirklich wichtigen Themen konzentrieren. Zudem bieten wir Raum für Fragen, die über den Kursinhalt hinausgehen.

Am Ende des Kurses nehmen wir uns 30 Minuten Zeit für ein Ask Me Anything (AmA), um eine Diskussionsrunde zwischen den Teilnehmern und dem Trainer zu ermöglichen. Dies bietet die Gelegenheit, über aktuelle Projekte und Themen zu sprechen, die für die Teilnehmer relevant sind, aber nicht im Kurs behandelt wurden.

Schulungsumgebung

Die Laborumgebung umfasst ein leistungsfähiges, komplett dediziertes Labor pro Teilnehmer mit mehr als 35 virtuellen Kernen und über 80 GB RAM. Die Laborumgebung befindet sich in einem Rechenzentrum in Frankfurt und verfügt über eine große Bandbreite und geringe Latenzen. Der Zugriff erfolgt über den Web-Browser und erfordert keine Installation von Software.

Bonus

Als Bonus erhalten Sie nach Abschluss des 4-tägigen Cyber Security & ANTI-HACKING Workshops einen zusätzlichen Tag vollen Zugriff auf das im Kurs vorgestellte Hacking-Labor. Dieser zusätzliche Tag gibt Ihnen die Möglichkeit, die besprochenen Angriffstechniken zu vertiefen und eigenständig weitere Angriffszenarien im Labor kennenzulernen. Die Übungen erfordern Kreativität, technisches Wissen und Hartnäckigkeit. Zudem haben Sie in Ruhe Zeit, die im Kurs besprochenen Übungen zu wiederholen.

Zielgruppe

Dieser Einsteigerkurs richtet sich an IT-Sicherheitsbeauftragte, IT-Administratoren (Client, Server, Netzwerk), Programmierer, IT-Ingenieure und Security Operation Center (SOC) Operatoren sowie an alle, die Security-Risiken aus der Perspektive des Angreifers betrachten und dadurch Lösungsszenarien entwickeln möchten.

Voraussetzungen

- Erfahrungen mit dem Betrieb und Administration von IT-Systemen

- Grundlegende IT-Security Kenntnisse

Kursziele

Das Ziel des Kurses ist es, technisches und organisatorisches Wissen im Bereich der IT-Sicherheit zu vermitteln, damit 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 beziehungsweise zu verringern.

Kursinhalt

- Grundlagen der Cybersicherheit
- Aktuelle Trends
- Initiale Infektion
- Infrastruktur-Sicherheit
- Linux-Angriffe
- Windows-Angriffe
- Post-Exploitation
- Active Directory
- Post Exploitation
- Defense in Depth
- Ransomware
- Ask me Anything
- Web Security
- Denial of Service
- Network Security

Detaillierter Kursinhalt

Cybersicherheit Grundlagen

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

Aktuelle Trends

- Aktuelle Metriken
- Bewährte Angriffstechniken
- Cybersecurity Trends und aktuelle Bedrohungslage

Initiale Infektion

- Arten von Social-Engineering
- Passwort-basierte Angriffe
- Vor- und Nachteile von Passwortrichtlinien
- Phishing und Umgehung von MFA / 2FA
- M365-Angriffe
- Adversary-in-the-Browser-Angriff
- Browser-in-the-Browser-Angriff
- 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
- Enumeration und Footprinting
- Discovery und Port-Scanning
- Offlline-Cracking
- Reverse- und Bind-Shells
- Bewertung von Verwundbarkeiten
- Command Injections, Webshells und SSRF
- Einführung in Metasploit

Linux Sicherheit

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

Windows Sicherheit

- Windowsgrundlagen
- Windows Credential System
- NG-Firewall-Evasion
- Pivoting
- Memory-Corruptions
- Exploit-Mitigations
- Meterpreter fortgeschritten
- Keylogging
- Client-Side-Exploitation
- Sysinternals Suite
- Library-Hijacking

Active Directory Sicherheit

- Active-Directory-Grundlagen
- Coercion-Angriffe
- Pass the Hash (PTH)
- Pass the Ticket (PTT)
- Golden-Tickets, Silver-Tickets

- Impersonation
- Kerberoasting
- Over-pass the hash / Pass the key
- Skeleton Key
- Machine Account Quota
- AdminSDHolder
- Enterprise Access Modell
- Privileged Acess Workstations

Evasion

- Native Malware, Powershell Malware, .NET Malware
- A/V Evasion
- Exfiltration und C+C

Post-Exploitation

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

Defense in Depth

- Windows-Härtung
- Active Directory Härtung
- Die Kill-Chain
- Netzwerkverteidigung
- Grundlagen der ISMS
- Fortgeschrittene Netzwerkverteidigung
- Threat-Modelling und Schützen von Kronjuwelen
- Aufbau und Betrieb von Security-Operation-Centern
- Incident-Response-Richtlinien
- Threat-Intelligence

Ransomware Verteidigung

- Backup-Strategie
- RPO und RTO
- Wiederherstellung
- Ransomware-Schutz
- Bezahlen oder nicht?
- Entschlüsselungs-Erwägungen
- Tools

Websicherheit

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

Ask me Anything mit Trainer

- Offene Fragerunde
- Diskussion von aktuellen Projekten
- Vertiefung

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

Fallstudien und Übungen

Basics

- Aufsetzen einer Phishing-Seite
- DNS-Reconnaissance
- Port-Scanning
- Exchange-Exploitation

Linux

- Exploitation eines Linuxservers
- Post-Exploitation des Linuxservers
- Linux-Lateral-Movement

- Heartbleed

Windows

- Pivot zu Windows
- Lateral-Movement im Active Directory • Coercion Angriff
- Kerberoasting
- Post-Exploitation

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
- Beispiele von Virustotal und Any.run
- Backdoor mit MSFvenom
- Gezieltes Brechen einer A/V Signatur

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