Enterprise Computing Solutions - Education Services

TRAINING OFFERING

Sie erreichen uns unter

Arrow ECS GmbH, Elsenheimerstraße 1, 80687 München

Email: training.ecs.de@arrow.com
Phone: +49 (0)89 930 99 168

SECURITY

Cybersecurity Workshop

CODE:	LÄNGE:	PREIS:
SEC_HACK_CYBERSEC	40 Hours (5 Tage)	€2,550.00

Description

Dieser Kurs bietet Ihnen eine umfassende Einführung in die Cybersicherheit, inklusive Angriffstechniken und Gegenmaßnahmen. Mit realistischen Übungen und einem Schwerpunkt auf dem angesehenen Mitre Att&ck-Projekt, werden Sie die Grundlagen der Cybersicherheit erlernen. Der theoretische Teil basiert auf Industriestandards wie BSI-Grundschutz Kompendium, CIS-Benchmarks und OWASP. Durch den Wechsel der Perspektive zwischen Angriff und Verteidigung, werden Sie in der Lage sein, direkt Verteidigungsmaßnahmen und Quick Wins aus den Erfahrungen der praktischen Laborübungen abzuleiten.
Der Kurs schließt mit einem Fokus auf fortgeschrittenen Themen, darunter die Umgehung von Antivirus-Systemen, WAFs, Intrusion-Protection-Systemen, Firewalls, Spam-Gateways, Proxy-Whitelisting, Sandboxes, EDRs und XSS-Filtern.

Zielgruppe

Unser Einsteigerkurs in die IT-Sicherheit ist speziell für IT-Sicherheitsbeauftragte, IT-Administratoren (Client, Server, Netzwerk), Programmierer, IT-Ingenieure und SOC-Operatoren sowie alle, die sich mit der Betrachtung von Sicherheitsrisiken aus der Perspektive des Angreifers auseinandersetzen möchten, um dadurch effektive Lösungen zu entwickeln, konzipiert.

Voraussetzungen

- Grundlegende Computerkenntnisse
- Kommandozeilenerfahrung und/oder Linuxerfahrung ist vorteilhaft

Inhalt

Unser Kurs verfolgt das Ziel, technisches und organisatorisches Know-how im Bereich der IT-Sicherheit zu vermitteln, damit die Teilnehmer in ihrem beruflichen Alltag entscheidungsstark und nachhaltig die IT-Sicherheit verbessern können. Durch zahlreiche praktische Übungen erlangen die Teilnehmer die Fähigkeit Angriffe zu erkennen, abzuwehren oder vorhandene Sicherheitslücken zu schließen oder zu minimieren.
Kursinhalt

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

Kursinhalt Details
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

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

Windows Sicherheit

- Windowsgrundlagen
- 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
- Tier-Modell und RaMP
- PAM/PAW-Angriffsvektoren

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

Gegen Ransomware verteidigen

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

Websicherheit

- 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 browserunterstützt (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
- Proxy-Logon

Linux

- Exploitation eines Linuxservers

- Post-Exploitation des Linuxservers
- 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
- Windows-Post-Exploitation
- PAM-/ WFH-Pivoting via Keystroke-Injection

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

Fallstudien

- Debian SSH-Verwundbarkeit
- XSS-Evasion
- Fuzzing eines Memory Corruption DoS
- Linux-Command-Injections
- Linux-Exploitation mit Metasploit
- Itch-Webanwendung (PHP-Verwundbarkeit)
- Root auf Linuxserver (Wordpress)
- IIS-Double-Decode
- Stack-Buffer-Overflow
- Extraktion von Meterpreter aus Prozessspeicher

Weitere Informationen

Virtuelle Umgebung für jeden Teilnehmer. Zugriff per RemoteLabsClient. VMs/Container simulieren ein Unternehmensnetzwerk (Linux, Windows, BSD) mit Servern, Clients, Firewalls, IPS, WAF, Endpoint Protection.
Systemvoraussetzungen für Teilnehmerrechner

- Internetzugang
- Installation von RemoteLabsClient auf Windows oder macOs für Zugriff auf Laborumgebung

Kurstermine

Auf Anfrage. Bitte kontaktieren Sie uns

Zusätzliche Information

Diese Schulung ist auch als Vor-Ort-Schulung verfügbar. Bitte kontaktieren Sie uns, um mehr zu erfahren.