>> IT Security

Hacking & Defense für IT-Pro's

EGOS! the education company

Angriffe auf Netzwerke stellen eine ernstzunehmende Bedrohung für IT Netzwerke und damit das ganze Unternehmen dar. Systemadministratoren können ein Netzwerk nur mit fundierten Kenntnissen des "Hacking" sinnvoll schützen.

Ihr Nutzen

Dieses Training befähigt IT-Administratoren, die Sicherheit ihres eigenen Netzwerks strukturiert und reproduzierbar zu überprüfen – von der Angriffsfächenanalyse über Scans und Enumeration bis zum kontrollierten Nachweis von Schwachstellen und einem umsetzbaren Remediation-Plan. Der Fokus liegt auf praxistauglichen Workflows mit Kali Linux und Metasploit, kombiniert mit sauberen Evidence-Standards und „Fix & Verify"-Methoden.

Preis pro Teilnehmer

EUR 2150,- exklusive der gesetzlichen MwSt.

Seminardauer

3 Tag(e)/Day(s)

Seminarinhalte

Tag 1:
* Governance & Methodik
- Scope
- RoE
- Evidence
- Risikologik

* Recon/Footprinting
- Asset- und Exposure-Inventar

* Scanning & Enumeration
- Service-/OS-Discovery
- SMB/SNMP/DNS/LDAP-Basics

Tag 2:
* Vulnerability Analysis
- Scanner-Ergebnisse richtig lesen
- Priorisierung

* Controlled Exploitation (Einordnung)
- Metasploit-Workflow
- Preconditions
- Stabilität/Impact

* Network/Perimeter Concepts (adminrelevant)
- Sniffing-/Session als Design- und Kontrollfrage

Tag 3:
* Web-Basics für Admins
- Server vs App
- schnelle Web-Triage mit Proxy

* KI im Pentest (Responsible Use)
- KI als Analyse-/Reporting-Boost
- Grenzen/Compliance (Brücke zur AI-Spezialisierung)

* Praxis-Labs (Beispiele)
- Attack-Surface-Inventory + „Top 10 Risiken" fürs eigene Umfeld
- Scan-/Enum-Runbook erstellen und anwenden
- Vuln-Triage: aus 30 Findings ? 5 echte Prioritäten ableiten
- Kontrollierter Nachweis an Trainingszielen + Evidence-Standard
- Mini-Report + Remediation-Backlog + Re-Test-Checkliste

Voraussetzungen

TCP/IP-Basics, Windows-/Linux-Admin-Grundlagen

Hinweise

Version: N/A

* Tools
- Kali Linux, Metasploit Framework
- nmap, wireshark, burp suite community / OWASP ZAP, nuclei oder GVM, john/hashcat (kontrolliertes Audit), Standard-Linux-Tooling

* Teilnehmer-Output
- RoE-Template, Evidence-Checklist, Testplan, Report-Template, Remediation-Backlog (priorisiert), Re-Test-Runbook