S E M I N A R E

Microsoft

2270

Ethical Hacking – Microsoft SQL Server (Grundlagen)

Sicherheit verstehen · Angriffe erkennen · Systeme schützen

o Zielgruppe

Personen, die mit der Betreuung und Absicherung von Microsoft SQL Servern betraut sind oder diese Verantwortung künftig übernehmen.
Besonders geeignet für:
- SQL Server Administratoren (DBAs)
- IT-Sicherheitsverantwortliche und Auditoren
- Systemadministratoren mit Datenbankfokus
- DevOps- und Infrastrukturteams mit Sicherheitsaufgaben

o Voraussetzungen
- Kenntnisse von relationalen Datenbank-Managementsystemen
- Grundkenntnisse in Windows Server und Active Directory
- Basiswissen in Netzwerken (TCP/IP, DNS, Firewall)
- Empfehlenswert: Grundkenntnisse in T-SQL, PowerShell oder Skripting

o Seminarziel
- Durchführung von Recon-Scans und Interpretation der Ergebnisse
- Manuelle und automatisierte SQL Injection Tests durchführen
- Credential-Angriffe erkennen und gegensteuern
- Post-Exploitation Techniken sicher und nachvollziehbar anwenden
- Audit- und Monitoring-Mechanismen einrichten und auswerten
- Forensische Artefakte sichern und erste Analysen durchführen

Die Teilnehmer sind am Ende des Kurses in der Lage, Sicherheitslücken im SQL Server gezielt zu erkennen und zu bewerten, typische Angriffsvektoren nachzuvollziehen (z. B. SQL Injection, Credential Theft, Linked Server Chains), sinnvolle Gegenmaßnahmen zur Härtung und Überwachung umzusetzen und den SQL Server sicher zu administrieren.

Zentraler Lerneffekt: Think like an Attacker – Defend like a DBA

o Seminarinhalt

Fundament & Extern:
- Begrüßung, organisatorische Hinweise, Labor-Setup
- Rechtliche Rahmenbedingungen, Scope & Genehmigungen
- Hacker-Mindset, Bedrohungslandschaft
- Reconnaissance: OSINT, Shodan, Nmap
- SQL Injection (Theorie + erste Hands-on)
- Credential Attacks: Password Files, Brute Force, Config-Harvest

Intern & Post-Exploitation:
- Post-Exploitation Grundlagen (LotL, PowerShell)
- Deep Enumeration (sysadmin accounts, linked servers, service accounts)
- Lateral Movement & MITM (TDS Traffic Analysis)
- Privilege Escalation & CLR-Assembly Beispiele

Defense & Abschluss:
- Security Assessment & Auditing (PowerUpSQL, T-SQL Audits)
- Härtung: Network, Auth, Surface Reduction
- Monitoring & Detection (XE, Audit, Sysmon)
- Incident Response & Forensik Basics
- Review, Checklisten, Q&A

Software-Hinweis
Im Workshop kommen ausschließlich Test-, freie oder Trial-Versionen der Software zum Einsatz: Microsoft SQL Server Developer Edition, Windows Server (Evaluierungsversionen),

CONSULTING & INFORMATIONSDIENSTE GMBH

München
Berghamer Straße 10
85435 Erding
Tel.: 0 81 22 / 97 40 - 0
Fax: 0 81 22 / 97 40 - 10

Erfurt
Michaelisstraße 13a
99084 Erfurt
Tel.: 03 61 / 5 65 93 - 0
Fax: 03 61 / 5 65 93 - 10

Internet
www.md-consulting.de

E-Mail
info@md-consulting.de

Bankverbindung
HypoVereinsbank
Erfurt

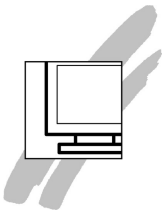
IBAN:
DE84 8202 0086
0003 9840 95

SWIFT/BIC:
HYVEDEMM 498

Geschäftsführer
Dr. Martin Diestelmann

HRB München 289362

USt.Id Nr.:
DE 150 108 446



Microsoft

2270

Kali Linux, freie Tools wie Nmap, SQLMap, PowerUpSQL, Wireshark, Sysinternals. Es werden keine produktiven Lizenzen verwendet.

KI als Angriffs- und Assistenz-Werkzeug
Im Workshop wird der Einsatz von KI-Tools (z. B. ChatGPT / sGPT) demonstriert – zur Payload-Generierung, Unterstützung bei Recon und zur Automatisierung. Ethische und rechtliche Aspekte werden besprochen; KI-Outputs werden stets validiert und in der isolierten Lab-Umgebung genutzt.

- **Seminardauer: 3 Tage**

Im Preis enthalten sind kursbegleitende Seminarunterlagen, Pausengetränke und Mittagessen.

- **Preis pro Person: 2.290 EUR netto**