S E M I N A R E

Microsoft

2235

Cyber Security - Ethical und SQL Server Sicherheit (MS IT Boot-Camp)

München
Berghamer Straße 14
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

o Zielgruppe

Dieser Intensiv-Workshop richtet sich an Entwickler von Datenbank- und Webanwendungen, Windows-Administratoren, IT-Sicherheitsbeauftragte, IT-Sicherheitsberater, Und alle die sich mit Hacking und Forensik beschäftigen bzw. daran interessiert sind.

o Voraussetzungen

Praktische Erfahrungen in der Administration von Windows und SQL Server Infrastrukturen und grundsätzliche Kenntnisse über TCP/IP-basierte Netzwerke, Datenbankserver und Webanwendungen mitbringen. Programmierkenntnisse sind hilfreich aber nicht erforderlich.

o Seminarziel

Verstehe deinen Feind um deine Applikationen zu schützen. Sie sind für die Sicherheit der SQL Server – Infrastruktur in Ihrem Unternehmen verantwortlich und stellen sich die Frage, ist diese sicher für Angriffe von außen oder von innen?

Sie suchen nach einer Möglichkeit, Hackerangriffe zu Verstehen und Schwachstellen in Ihrer SQL Server Infrastruktur zu finden? Mit unserem 5-tägigen Praxisworkshop können wir Ihnen dabei helfen, genau diese Anforderung zu erfüllen und einen fundierten Einstieg in die Materie von IT-Forensik/Hacking zu bekommen. Sie erhalten einen einzigartigen Einblick in die Motive sowie die Taktiken, Techniken und Prozeduren (TTP) der Angreifer.

Über 75 % des Seminars/Workshops ist LAB bzw. demobasiert. Wir leiten Sie in diesen Demos/Übungen an und versuchen ein Verständnis für die Möglichkeiten des **White-Hat Hacking** und **IT-Forensik** zu vermitteln.

Wir nehmen Sie mit auf die Reise in die Welt des Hackings von Datenbankserver und wie Sie Ihre Infrastruktur absichern können. Hauptthemen dabei sind Einstieg in das Ethical Hacking, Angriffe gegen SQL Server, Sicherheit von SQL Server und SQL Server Forensik. Neben der Vorgehensweise in aktuellen Angriffen lernen Sie, eine Laborumgebung mit wichtigen und verbreiteten Hacking-Tools einzurichten und mit vielen verschiedenen Techniken umzugehen, um die Sicherheit Ihrer Systeme zu testen und Schutzmaßnahmen verbessern zu können.

Fokus des Seminars lieg auf der Einrichtung einer sicheren SQL Server Infrastruktur. Mit der Definition einer Infrastruktur für IT-Forensik und White-Hat Hacking und den Schutz der SQL Server Infrastruktur.
Vortrag/Demonstrationen (geplant 40 ... 50 %) und Übungen am System.

o Seminarinhalt

Ethical Hacking

Einführung Ethical Hacking

- Rechtliches
- Einführung in das Hacking
- Vorgehensweise von Hackern
- Praktischer Teil
    - Auswertung von Schwachstellen
    - Suche nach Exploits für vorhandene Schwachstellen
    - Einrichten einer Laborumgebung einrichten (Kali Linux, Nmap, Wireshark ....)

Informationsbeschaffung

- Informationsbeschaffung mit öffentlich zugänglichen Mitteln
- Vertrauliche Daten in Suchmaschinen
- Google Hacking (Google Dorks)
- Port Scanning mit NMAP

CONSULTING & INFORMATIONSDIENSTE GMBH

Microsoft

2235

- Vulnerability Scanning (Suche nach Schwachstellen) mit Nessus
- Praktischer Teil:
    - Identifikation von Angriffszielen mittels DNS
    - Zuordnung der IP-Adressen anhand der RIPE-Datenbank
    - Sweep Scanning mit Nmap
    - TCP Portscanning mit Nmap
    - UDP Portscanning mit Nmap
    - Installation von Nessus
    - Konfiguration von Nessus Scan-Profilen für das Scannen
    - Vulnerability Scan mit Nessus
    - Auswertung der Ergebnisse

Exploits

- Verständnis für Exploits
- Exploit Frameworks (Penetration)
- Nutzung von Exploits zur Kompromittierung von Windows Systemen
- Exploit Frameworks am Beispiel von Metasploit
- Praktischer Teil:
    - Nutzung der Ergebnisse von Nmap und Nessus für die Exploit-Vorbereitung
    - Verwendung von Post Exploitation Modulen mit dem Meterpreter
    - Auslesen der SAM mit Mimikatz
    - Cracken der Passwörter mit John the Ripper und Cain&Abel

Netzwerkangriffe

- Angriffe gegen Netzwerkkomponenten
- Sniffing und Passwörter abhören
- Password Cracking
- Man-in-the-Middle Angriffe
- Praktischer Teil:
    - ARP-Spoofing mit Cain&Abel
    - ARP-Spoofing mit Bettercap
    - Sniffing mit Cain&Abel und Wireshark

SQL Injection

- Was ist SQL
- Was ist SQL Injection
- Zunahme von SQL-Injection Angriffen
- Auswirkungen von SQL Injections
- Werkzeuge zum Finden von SQL Injections
- Wie funktionieren SQL Injections
- Fehler basierte SQL Injections
- Praktischer Teil:
    - SQL-Injection mit OWASP ZAP
    - Blind SQL-Injection mit OWASP ZAP
    - Erkennung und Ausnutzung von SQL-Injection Angriffen
    - Auslesen der SQL-Datenbank mit sqlmap

SQL Server Sicherheit

Sichern von Server und Netzwerk

- Einleitung
- Auswählen eines Kontos für das Ausführen von SQL Server
- Verwalten von Dienst-SIDs
- Verwenden eines verwalteten Dienstkontos
- Verwenden eines virtuellen Dienstkontos
- Verschlüsselung der Sitzung mit SSL
- Konfigurieren einer Firewall für den SQL Server-Zugriff
- Deaktivieren des SQL Server-Browsers
- Nicht benötigte Dienste beenden
- Verwenden von Kerberos für die Authentifizierung
- Verwenden des erweiterten Schutzes, um Angriffe auf Authentifizierungsrelais zu verhindern
- Verwenden transparenter Datenbankverschlüsselung
- Sichern des verbundenen Serverzugriffs
- Konfigurieren der Endpunktsicherheit
- Begrenzung der Funktionalitäten - xp_cmdshell und OPENROWSET

CONSULTING & INFORMATIONSDIENSTE GMBH

Microsoft

2235

Benutzerauthentifizierung, Autorisierung und Sicherheit

- Einleitung
- Auswahl zwischen Windows- und SQL-Authentifizierung
- Erstellen von Anmeldungen
- Schutz Ihres Servers vor Brute-Force-Angriffen
- Begrenzung der Administratorrechte des SA-Kontos
- Verwenden fester Serverrollen
- Berechtigungen für granularen Server
- Erstellen und Verwenden von benutzerdefinierten Serverrollen
- Erstellen von Datenbankbenutzern und Zuordnen zu Anmeldungen
- Verhindern von Logins und Benutzern, Metadaten zu sehen
- Erstellen einer enthaltenen Datenbank
- Korrigieren von Benutzer - Login - Mapping - Fehlern bei wiederhergestellten Datenbanken

Schützen der Daten

- Einleitung
- Berechtigungen verstehen
- Zuweisen von Berechtigungen auf Spaltenebene
- Erstellen und Verwenden von Datenbankrollen
- Anwendungsrollen erstellen und verwenden
- Verwenden von Schemata für die Sicherheit
- Verwalten von Objektbesitz
- Schutz von Daten durch Ansichten und gespeicherte Prozeduren
- Konfigurieren von datenbankübergreifender Sicherheit
- Verwalten der Sichtbarkeit des Ausführungsplans
- Verwenden von EXECUTE AS zum Ändern des Benutzerkontexts

Code und Datenverschlüsselung

- Einleitung
- Verwenden von Dienst- und Datenbank-Master-Schlüsseln
- Erstellen und Verwenden symmetrischer Verschlüsselungsschlüssel
- Erstellen und Verwenden von asymmetrischen Schlüsseln
- Erstellen und Verwenden von Zertifikaten
- Daten mit symmetrischen Schlüsseln verschlüsseln
- Daten verschlüsseln mit asymmetrischen Schlüsseln und Zertifikaten
- Erstellen und Speichern von Hash-Werten
- Daten unterzeichnen
- Authentifizierung der gespeicherten Prozedur durch Signatur
- Verwenden von Modulsignaturen zum Ersetzen der datenbankübergreifenden

Besitzverkettung

- Verschlüsseln von SQL-Code-Objekten
- Kampfangriffe und Injections
- Einleitung
- Definieren der Codezugriffssicherheit für .NET-Module
- Schützen von SQL Server gegen Denial of Service
- SQL Server gegen SQL-Injection schützen
- Sichern von dynamischem SQL aus Injektionen
- Verwenden einer SQL-Firewall oder einer Webanwendungsfirewall

Sicherungswerkzeuge und hohe Verfügbarkeit

- Einführung
- Auswahl des richtigen Kontos für SQL Agent
- Benutzer können ihre eigenen SQL-Agent-Aufträge erstellen und ausführen
- Erstellen von SQL-Agent-Proxys
- Einrichten der Transportsicherheit für Service Broker
- Einrichten der Dialogsicherheit für Service Broker
- Sicherung der Replikation
- Sichern von SQL Server-Datenbankspiegelung und AlwaysOn

Microsoft

2235

Auditierung

- Einleitung
- Verwenden des Profilers zum Überprüfen des SQL Server-Zugriffs
- Verwenden des DML-Triggers für die Prüfung der Datenänderung
- Verwenden von DDL-Triggern für die Prüfung der Strukturänderung
- Konfigurieren der SQL Server-Überwachung
- Auditing und Tracing von benutzerdefinierbaren Ereignissen
- Konfigurieren und Verwenden von Common Criteria Compliance
- Verwenden von System Center Advisor zur Analyse Ihrer Instanzen
- Verwenden des SQL Server Best Practice Analyzers
- Verwenden von Policy Based Management

SQL Server Forensik

Einführung in die SQL Server Forensik

- Überblick über SQL Server Forensik
- Grundlagen der forensischen Wissenschaft
- Bedeutung von Forensik für SQL Server
- Einführung in rechtliche Aspekte und Compliance

SQL Server Architektur und Protokollierung

- Verständnis der SQL Server Architektur
- Transaktionsprotokolle und ihre forensische Bedeutung
- SQL Server Audit-Funktionen
- Log Management und Überwachung

Erweiterte Datenanalyse

- Analyse von SQL Server Logs
- Datenextraktion aus Backups
- Umgang mit beschädigten oder manipulierten Daten
- Einsatz von Tools zur Datenanalyse und -wiederherstellung

Netzwerkforensik und SQL Server

- Netzwerkprotokolle und SQL Server
- Analyse von Netzwerkverkehr zu und von SQL Server
- Identifizieren von SQL-Injection und anderen Angriffsvektoren
- Verwendung von Netzwerk-Monitoring-Tools

Praktische Forensik-Workshops

- Hands-on Labs zur Anwendung von forensischen Techniken
- Untersuchung von realen Fallbeispielen
- Szenariobasierte Übungen zur Erkennung und Behebung von Sicherheitslücken

Forensik-Tools und Technologien

- Übersicht über forensische Software-Tools
- Bewertung und Auswahl von Tools für spezifische forensische Aufgaben

Verwendete Werkzeuge (ein Auszug)

- Kali Linux
- Python
- Cain & Abel
- Nmap
- SQLMap
- Wireshark
- Nessus usw.

CONSULTING & INFORMATIONSDIENSTE GMBH

Microsoft

2235

- **Seminardauer: 5 Tage**

Lernen im Schulungshotel Gröbern am See in Muldestausee/Gröbern, in der Dübener Heide.
Seminardauer: Erster Tag ab 10:00 Uhr, letzter Tag ca. 15:00 Uhr
Kleine Gruppen mit 2-4 Teilnehmer (max. 6) Im Preis enthalten sind:

- Übernachtungskosten im Hotel
- Vollverpflegung inkl. Getränke
- Schulungsunterlagen
- täglich open end
- intensive Übungs- und Nachbereitungsphasen nach Seminarende
- alle im Seminar durch uns installierten VMs können Sie nach dem Seminar mitnehmen.

- **Preis pro Person: 3.290 EUR netto**