S E M I N A R E

CONSULTING & INFORMATIONSDIENSTE GMBH

Microsoft

2230

Cyber Security - Ethical Hacking für das Development-Team (MS IT Boot-Camp)

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 Infrastrukturen und grundsätzliche Kenntnisse über TCP/IP-basierte Netzwerke, Datenbankserver und Webanwendungen. Programmierkenntnisse sind sehr hilfreich.
Der Kurs ist für "Einsteiger" in das Thema Hacking (Development) geeignet.

o Seminarziel

Verstehe deinen Feind um deine Applikationen zu schützen. Sie erstellen Web- oder Desktopapplikationen für Ihre Unternehmen 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 Ihrem System 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. In diesem intensiven Workshop erhalten Sie 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.

In diesem Workshop nehmen wir Sie mit auf die Reise in die Welt des Hackings von Windows basierten Systemen, Datenbanksystemen und Webapplikationen. 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 neben der Einrichtung einer Infrastruktur zur IT-Forensik und für das White-Hat Hacking in Windows-, SQL Server und Webapplikationen.

o Seminarinhalt

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
- 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
    - Nutzung eines Exploits zum Einbruch in Windows 10
    - Verwendung von Post Exploitation Modulen mit dem Meterpreter
    - Auslesen der SAM mit Mimikatz
    - Cracken der Passwörter mit John the Ripper und Cain&Abel

Malicious Code

- Viren und Trojaner
- Rootkits
- Praktischer Teil:
    - Test verdächtiger Programme mit Virustotal.com
    - Erzeugen eines Trojaners zum Tarnen der Schadsoftware basierend auf Netbus
    - Veränderung von Schadprogrammen zum Täuschen von Virenscannern
    - Trojanisierung von Programmen mit msfvenom
    - Einbetten von Schadsoftware in ein PDF
    - Einbetten des Meterpreters als Makro in ein Word-Dokument

Hacking Hardware Programmieren

- Rubber Ducky & Co.
- WLAN Jammer

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

Angriffe gegen Webanwendungen

- Sicherheitsanalyse von Webanwendungen
- Web Application Vulnerability Scanning
- Passwort Cracking Angriffe

Microsoft

2230

- Praktischer Teil:
    - Angriffe gegen Webanwendungen mit dem OWASP Zed Attack Proxy (ZAP)
    - Fuzzing von Formularfeldern mit dem OWASP Zed Attack Proxy (ZAP)
    - Demonstration von Angriffen anhand der DVWA
    - Erkennung und Ausnutzung von Cross Site Scripting (XSS) Angriffen
    - Passwort Brute Force mit Hydra

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

Verwendete Werkzeuge

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

o 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.

o Preis pro Person: 2.990 EUR netto