CONSULTING & INFORMATIONSDIENSTE GMBH

Microsoft

2224

Cyber Security - Ethical Hacking und Forensic Einstieg (MS IT Boot-Camp)

o Zielgruppe

Dieser Kurs richtet sich an Systemadministratoren, Netzwerkadministratoren, Web-Administratoren, IT-Sicherheitsbeauftragte, IT-Sicherheitsberater und alle die sich mit Hacking und Forensik beschäftigen bzw. daran interessiert sind.

o Voraussetzungen

Bitte praktische Erfahrungen in der Administration von Windows Infrastrukturen und grundsätzliche Kenntnisse über TCP/IP-basierte Netzwerke und Webanwendungen mitbringen. Programmierkenntnisse sind hilfreich jedoch nicht erforderlich.

o Seminarziel

Verstehe deinen Feind um dich zu schützen. 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.

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 zu vermitteln.

In diesem Workshop nehmen wir Sie mit auf die Reise in die Welt des Hackings von Windows-basierten Systemen. Dabei werden wir Rechtliches betrachten, eine Laborumgebung mit einzelnen wichtigen Werkzeugen einrichten.

Vortrag/Demonstrationen und Übungen am System.

o Seminarinhalt

Einführung Ethical Hacking

- Rechtliches
- Einführung in das Hacking
- Vorgehensweise von Hackern
- Praktischer Teil
  - o Auswertung von Schwachstellen
  - o Suche nach Exploits für vorhandene Schwachstellen
  - o 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:
  - o Identifikation von Angriffszielen mittels DNS
  - o Zuordnung der IP-Adressen anhand der RIPE-Datenbank
  - o Scanning mit Nmap
  - o TCP Portscanning mit Nmap
  - o UDP Portscanning mit Nmap
  - o Installation von Nessus
  - o Konfiguration von Nessus Scan-Profilen für das Scannen
  - o Vulnerability Scan mit Nessus
  - o 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:

CONSULTING & INFORMATIONSDIENSTE GMBH

Microsoft

2224

- o Nutzung der Ergebnisse von Nmap und Nessus für die Exploit-Vorbereitung
- o Nutzung eines Exploits zum Einbruch in Windows 10
- o Verwendung von Post Exploitation Modulen mit dem Meterpreter
- o Auslesen der SAM mit Mimikatz
- o Cracken der Passwörter mit John the Ripper und Cain&Abel

Malicious Code

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

Hacking Hardware

- Rubber Ducky & Co.
- WLAN Jammer

Windows-Schwachstellen

- Windows-Architektur und -Design, Gruppenrichtlinien
- Enumeration von Benutzern und Diensten unter Windows
- NetBIOS-spezifische Schwachstellen (Exploits, IPC, Admin Shares)
- Auslesen von Zugangsdaten (LSA Cache, Mimikatz, Lateral Movement)
- Gezielte Ausnutzung von fehlkonfigurierten Diensten und Anwendungen
- AD-/RDP-/SQL-spezifische Schwachstellen/Fehler im Server-Handling
- Praktischer Teil:
  - o Windows Enumeration mit SuperScan
  - o Auslesen des LSA Cache mit Cain&Abel
  - o Auslesen der SAM und Logonpasswörter mit Mimikatz
  - o Cracken der Passwort-Hashes
  - o Offline Angriffe gegen AD mit DSInternals
  - o Pass-the-Hash Angriff mit Metasploi

Netzwerkangriffe

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

Denial-of-Service Angriffe

- DoS und DDoS
- Amplification Attacks

Wireless LAN Hacking

- WLAN-Sicherheit
- WEP Cracking
- WPA Cracking
- Praktischer Teil:
  - o WLAN-Analyse mit Kismet
  - o Abhören der Kommunikation mit airodump-ng
  - o Replay-Angriffe mit aireplay-ng
  - o WEP-Cracking mit aircrack-ng
  - o WPA-Cracking mit Hashdump

Verwendete Werkzeuge

- Kali Linux
- Python
- Cain & Abel
- Nmap
- Wireshark

Microsoft

2224

- 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

o Preis pro Person: 2.990 EUR netto