

Certified Penetration Testing Specialist (ethischer Hacker)



Daten

Kursnummer: CPTS V4.0

Dauer: 5 Tage

Sprache:

- Deutsch
- Kursmaterial (Englisch)

Format:

Durch Trainer (Theorie u. Hands-on Labs)

Kursmaterial:

1. Arbeitsbuch
2. Handbuch
3. Software/Tools 2x DVDs

Prüfung:

1. **CPTS** - Certified Pen Testing Specialist (Thomson Prometric - Global)

Zertifierungsgang:

CPTS – Certified Pen Testing Specialist
 CPE - Certified Pen Testing Expert
 CFED - Computer Forensics & Electronic Discovery

Voraussetzungen:

- Mindestens 12 Monate Erfahrung als Netzwerk- bzw. Systemadmin
- Gute TCP/IP Kenntnisse
- Gute Hardware Kenntnisse
- Gute Microsoft Kenntnisse
- Network+, Microsoft Security+
- Linux Kenntnisse nicht erforderlich aber hilfreich



Kursbeschreibung

Das CPTS - Programm wurde basierend auf der praktischen und langjährig erprobten Penetration Testing Methodik (ethisches Hacking) entwickelt. Die Mile2-Trainer arbeiten hart und kontinuierlich an der Gestaltung unseres Programms und entwickeln es, unter anderem durch gegenseitige Konsultation, ständig weiter. Wir halten die gleichwertige Schwerpunktlegung auf theoretische wie auch auf eigene praktische Erfahrungen in diesem Gebiet für unbedingt erforderlich, um Ihnen, den Kursteilnehmern, die Kenntnisse effektiv und erfolgreich zu vermitteln.

Das CPTS- Programm präsentiert Informationen über aktuellste Netzwerk-Schwachstellen und Abwehrtechniken zur Absicherung des Netzwerkes. Zusätzlich bietet Ihnen unser Programm eine Verbesserung der Fähigkeit Schutzmöglichkeiten zu erkennen, Testaktivitäten zu rechtfertigen und Sicherheitskontrollen gemäß der Geschäftsbedürfnisse zu optimieren, um Geschäftsrisiken zu reduzieren.

Das CPTS- Programm geht weit über die Normen bisher gelehrter Kurse hinaus. Wir werden Sie daher nicht einfach nur das „Hacken“ lehren. Unser Kurs wurde zwar auf den selben Prinzipien basierend entwickelt und bedient sich der Methoden von Hackern, legt jedoch den Schwerpunkt auf der professionellen Durchführung von Pen Tests und der Sicherung von wertvollen Informationen.

Nach Abschluss des Kurses

Nach Abschluss des Kurses haben die CPTS-Kursteilnehmer die Möglichkeit entweder am Thomson Prometric CPTS-Examen oder am Certified Ethical Hacker-Examen teilzunehmen. Die Kursteilnehmer haben so die Chance an einem weiterführenden Programm teilzunehmen, in dem mit Hilfe kontinuierlicher Updates die Kenntnisse zur Aufrechterhaltung des sich ständig verändernden Sicherheitsumfelds und dessen Eingliederung in das Unternehmen vermittelt werden. Dieser Kurs stellt urheberrechtlich geschützte Labore zur Verfügung, die von führenden Sicherheitsexperten aus der ganzen Welt entwickelt und getestet wurden. Für Absolventen besteht die Möglichkeit am Certified Pen Testing Expert-Aufbaukurs (CPE) teilzunehmen.

Vorteile

Certified Penetration Testing Specialist-Absolventen haben authentische Sicherheitskenntnisse erhalten, die es ihnen ermöglichen Schwachstellen zu erkennen, Systemschwächen aufzuzeigen und dabei zu helfen Netzwerke gegen jegliche Bedrohung und Angriffe zu schützen. Die Absolventen haben die Kunst des „ethischen Hackens“ erlernt, allerdings mit einem rein professionellem Hintergrund (Pen Testing).

Modul 1: Einführung in Penetration Testing

Modul 2 : Ansammlung von Information

Modul 3: Aufdeckung von Live Systemen

Modul 4: Bereicherung durch Enumeration

Modul 5: Cryptographie Entschlüsselt

Modul 6: Einstufung von Schwachstellen

Modul 7: Windows Hacking

Modul 8: Fortgeschrittene Schwachstellen und Ausbeute Techniken

Modul 9: Malware – Das Abtauchen der Software

Modul 10: Packet Sniffing - Session Hijacking

Modul 11: Netzwerke angreifen, Router, Firewall und IDS

Modul 12: Angriff von Linux

Modul 13: Angriff von Datenbanken

Modul 14: Pen Testing und das ROI

Modul 15: Einstufung von Schwachstellen und die Geschäftslogistik

Modul 16: Angriff von Netzwerk-Technologien

Modul 17: Angriff von drahtlosen Netzwerken



Zielsetzung der Labor Szenarios

Hierbei handelt es sich um einen praktischen Intensivkurs. Um nicht wertvolle Zeit mit der Installation von 300+ Tools zu verbringen, wird unser Schwerpunkt auf dem Pen Testing Model liegen, da so ein schnelles Erlernen von aktuellsten Pen Testing Tools und Methoden ermöglicht wird. Die Labore erneuern ihre Standards wöchentlich, da stets neue Methoden entwickelt werden. Wir werden zahlreiche Tools von GUI bis Command Line anwenden. Aufgrund unserer Anwendung von strukturierten Angriffen, werden wir uns mit Tools für Windows als auch Linux befassen.

Modul 1: Einführung in Pen Testing

- Definition eines Pen Tests
- Hacker: Die Bedrohung
- Hacker contra Pen Tester
- Das Definieren des Sicherheitsumfeldes
- Zusätzliche Sicherheitsbelange
Die Mitspieler in der Netzwerksicherheit
- Die Methodik der Netzwerkabsicherung
Arten von Pen Tests
- Die Pen Test Methodik
- Tools contra Technik
- Der Ehrenkodex des Pen Testers
- Vorkehrungen zu einem Pen Test
- Die Risiken des Pen Tests
- Die goldene Regel der Anwendung von Pen Tests

Modul 2: Ansammlung von Information

- Welche Informationen sammelt ein Hacker an?
- Methoden zur Beschaffung von Informationen
- Passive contra Aktive
Aufklärung/Erläuterung
- Die Definition von Footprinting
- Footprinting Tools
- Google und Rückfragevermittler
- Johnny.lhackstuff.com
- „Site Digger“
- Registrierung von Domain Namen
- Whois, ARIN
- Website Tools und Referenzen
- DNS Datenbanken
- Der Gebrauch von Nslookup und Dig
- Operation Zurückverfolgung
- Tools und Anwendungen
- Firewalking
- Footprinting Gegenmaßnahmen

Laborübungen



Modul 3: Aufdeckung von Live Systemen

- Port Scanning Einführung
- Ping
- Die TCP/IP Ansammlung
- Ports und Dienste
- Der TCP3 way – Händedruck
- TCP-Flags
- Der Vanilla Scan
- Der halboffene Scan
- Firewall-geschützte-Ports
- UDP Port-Scannen
- Umgekehrter TCP-Scan
- Tools zum Port-Scan
- Packet Crafting und fortgeschrittene Scan-Methoden
- OS-Fingerprinting
- Fragmentationserforschung
- Gegenmaßnahmen
- Laborübungen

Laborübungen

Modul 4: Bereicherung durch Enumeration

Überblick über die Enumeration

- Web Server-Banner
- SMTP-Banner
- DNS-Enumerationsmethoden
- Zonen-Transfers
- Enumerationstools
- SNMP Enumeration und Gegenmaßnahmen
- Aktive Directory Enumeration und Gegenmaßnahmen
- Null Session und Gegenmaßnahme

Laborübungen

Modul 5: Kryptographie entschlüsselt

- Definition von Kryptographie
- Verschlüsselung von Algorithmen und Schlüsseln
- Einschätzung des Verschlüsselungsgrades
- Durchführbarkeit von symmetrischen Verschlüsselungen
- Algorithmen für symmetrische Schlüssel
- HASH-Funktionen im Detail
- Öffentliche Key Verschlüsselung im Detail
- Digitale Signaturen
- RSA/IPSEC/AES/DES/Blowfish/MD5
- SHA/SSL/RC5/SSH/PGP
- RSA-Herausforderung
- Der Rainbow-Crack

Laborübungen

Modul 6: Einstufung von Schwachstellen

- Einführung: Die Einstufung von Schwachstellen
- Technische Cyber Alarmsignale
- Tools zur Einstufung von Open Source-Schwachstellen
- Kommerzielle Schwachstellen-Scanner
- Patch Management

Laborübungen

Modul 7: Windows Hacking

- Windows Network Security
- Windows Secure Communication
- Types of Password Attacks
- Keystroke Loggers
- Automated Password Guessing
- Windows NT and LAN Manager Passwords
- Windows LanManPassword
- Password extraction and password cracking
- Various Tools:
- Password Sniffing
- Windows Authentication Protocols
- GPO LAN Manager Authentication Level
- SAM Database Insecurities
- NTPASSWD Utility
- Strong Password Recommendations for Users
- Recommended Password Policies
- Additional Password Cracking Countermeasures
- Covering Tracks Overview:
- Disabling Auditing
- Clearing the Event Log
- Hiding Files with NTFS Alternate Data Streams
- NTFS Streams Countermeasures
- What is Steganography?
- Stenography Tools

- Shredding Files Left Behind
- RootKit's
- Windows Rootkit Countermeasures
- RootKitShark Detector

Laborübungen

Modul 8: Fortgeschrittene Schwachstellen und Ausbeute Techniken

- Wie funktioniert „Ausbeuten“?
- Memory-Organisation
- Puffer-Überfluß
- Heap-Überfluß
- Stufen der Ausbeutungsentwicklung
- Prävention
- TCP/IP OSI- Exploits
- Das Metasploit-Projekt

Laborübungen

Module 9: Malware – Das Abtauchen der Software

Definition von Malware: Trojaner und Hintertüren

- Definition von Malware: Viren und Würmer
- Definition von Malware: „Spyware“
- Wie Trojaner und Hintertüren operieren
- Malware-Verbreitungsmethoden
- Wie Hacker Malware nutzen
- Der Malware Privilegien-Level
- Autostart-Methoden
- Die Überwachung von Autostart-Methoden
- Netcat
- Netcat-Schalter
- Netcat-Kurspraxis
- Fernzugang zu Trojaner-Komponenten
- Ausführbare „Wrapper“
- Benign EXE: Die geschichtliche Bindung von „Wrappern“ und Trojanern
- Die infizierte CD-Rom-Technik
- Backdoor-Zombam.B
- JPEG GDI+ : Kombinierte Fern-Ausbeute
- Erweiterte Trojaner: Prozess-Injektion
- Erweiterte Trojaner: „Beast“
- Erweiterte Trojaner: Wie man Entdeckung vermeidet
- Malware-Überblick: Antivirus/Personal IDS &

- Gegenmaßnahmen zu Firewall-Software
- Anti-Spyware-Software
- Anti-Trojan-Scanner
- www.Glocksoft.com
- Port-Monitor-Software
- Software zum Schutz von Dateien
- Windows: Software
- Einschränkungsprogramm
- Hardware-basierende Malware-Detectoren
- Gegenmaßnahmen: Anwender-Weiterbildung
- Malware Gegenmaßnahmen

Laborübungen

Modul 10: Packet Sniffing – Session Hijacking

Teil 1: Packet Sniffers

Packet Sniffer: Ein Beispiel

- Überwachung des Netzwerks
- Erneute Zusammensetzung von TCP Session-Packets
- WinPcap
- Das Packing-Genre und die Erfassungstools
- Sniffer-Entdeckung
- Aktive und Passive Sniffing-Methoden
- Die Flutung des „Switch-Forwarding“-Verzeichnis
- ARP Cache-Poisoning und Gegenmaßnahmen
- Wie man ARP-Poisoning-Tools verwendet
- Dsniff-Tools
- Was ist DNS-Spoofing?
- DNS-Spoofing-Tools
- SSL: Sniffing und Abfangen
- Gefälschte Zertifikats-Injektion
- MAC: Adressenänderungsmöglichkeiten
- Weitere Manipulationsmethoden für Routing und zum erleichterten
- Sniffing
- Sniffing-Gegenmaßnahmen

Teil 2: Session-Hijacking

- Session-Hijacking-Szenarios
- Initial Sequence Number (ISN)
- TCP-Sessions
- Stufen des Session-Hijacking
- Die Desynchronisation einer Session
- Injektion des manipulierten Pakets
- Voraussage von Sequenznummern und Tools
- Tools zur Unterstützung von Session-Hijacking
- Gegenmaßnahmen zum Session-Hijacking

Laborübungen

Modul 11: Netzwerk Angriffe – Routers, Firewalls und IDS

Firewalls und IPS-Systeme: eine Einleitung

- Firewalls: Ein Überblick
- Die IDS-Verteidigungslinie
- IDS-Architektur
- Überblick über die IDS-Architektur
- CIDF-Netzwerkmodel eines IDS-Designs
- Ausweichtechniken
- Paketto Keiretsu
- Observierte Resultate
- Packet-Integrität

Laborübungen

Modul 12 –Angriff von Linux

Linux: eine Einleitung

- Linux-Konzepte
- Details zum Linux-Dateiensystem
- Linux: Der Kernel
- Linux Shell
- Linux-Konfigurationsdateien
- Linux-Dateien: Genehmigung und Zugang
- Linux-Schwachstellen
- Zugangserlangung-Physischer Zugang
- Linux-Kernel Root Kits
- Rootkit-Gegenmaßnahmen
- Zusammenstellungsprogramme in Linux
- IPT-Tabellen
- Verschlüsselung
- Log und Traffic-Monitoren

Laborübungen

Modul 13 – Angriff von Datenbanken

Überblick über Datenbank-Server

- Arten von Datenbanken
- Tabellen, Tuples (records), Attribute, Domains
- Datennormalisierung, SQL (Structured Query Language), objekt-orientiertes Management von Datenbanken
- Schwachstellen und verbreitete Angriffe
- SQL-Injektion
- SQL: Verbindungseigenschaften
- Erweiterte Speicherprozeduren
- Login-Erraten und ergänzung

- Wie man den SQL-Server herunterfährt
- Schwachstellen und verbreitete Angriffe
- Schutzverstärkung der Datenbanken
- Zugangstools für SQL-Server

Laborübungen

Modul 14: Pen Testing und das ROI

- Wozu ein Pen Test?
- Generelle Punkte
- Definitionen
- Sicherheitszusicherung
- Kontrollvoraussetzungen
- Risiko Management
- Arten von Risiken
- Was sind Sicherheitsprotokolle?
- Einführung von Sicherheitsprotokollen und Sicherheitsprozeduren
- Sicherheitsprotokolle: Ausbildung der Nutzer
- Die Aufnahme von Sicherheitsprotokollen in das operative Management
- Die Lösung ethischer Dilemmas bei der Sicherung von wertvollen Daten

Laborübungen

Modul 15: Einstufung von Schwachstellen und die Geschäftslogistik

- Die Grundregeln
- Beschaffung und Verwendung persönlicher Daten
- Kopie, Lagerung, Erhaltung und Vernichtung von Information
- Informationsenthüllung
- Unerlaubte Beeinträchtigung von Informationssystemen
- Beschädigung und Modifizierung von Informationen oder Informationssystemen
- Aufzeichnung von Intentionen und Aktionen
- Aufzeichnung der Verantwortung
- Autorisierung
- Suspension des Sicherheitstests
- Informationen zu Vertrag, Laufzeit und Auflagen
- Haftung
- Inhalte

Laborübungen

Modul 16: Angriff von Netzwerk-Technologien

Abschnitt 1: Der Angriff von Netzwerktechnologien

- Web Server-Technologien für Unternehmen
- Verbreitete Sicherheitsbedrohungen
- Web-Einstufungstools
- Apache Web Server
- Angriffe gegen IIS
- ISS-Architektur
- ISAPI DLL Buffer Overflows
- Hacking-Tools und Methoden für das Web
- Schutz gegen Buffer Overflows
- Enthüllung der Quellen
- Traversal-Verzeichnis
- Unicodes
- IIS Logs
- ISS Gegenmaßnahmen

Abschnitt 2: Anmeldungsschwachstellen im Web

- Verbreitete Sicherheitsbedrohungen
- Anmeldungsschwachstellen im Web
- Web-Anmeldung: Pen Test Methodik
- Hacking-Tools zur Web-Anmeldung
- Input Manipulation
- Was ist Cross Side Scripting (XSS)?
- XSS-Gegenmaßnahmen

Abschnitt 3 Web basierte Password Cracking Methodik

- Authentifizierung
- NTLM Authentifizierung
- Certificate Based Authentifizierung
- Microsoft Passport Authentifizierung
- Forms-Based Authentifizierung
- Password Cracking Tools und Methoden
- Password Liste
- Query String
- Cookies
- Top Zehn Web Vulnerabilities
- Der Test

Laborübungen

Modul 17: Angriff von drahtlosen Netzwerken

Wireless LAN: Netzwerkkarten

- Eingesetzte Standards: A vs B vs G
- WEP
- WPA vs. WEP
- MAC-Spoofing
- EAP-Arten
- Wi-Fi-Netzwerksicherheitsmechanismen im Wireless LAN
- Schwachstellen
- Angriffe
- Angriffstools
- Verteidigungsstrategien

Laborübungen

Laborinformation:

- 1.) Der Großteil des Unterrichts findet in den Praxis - Laboren statt.
- 2.) Die Labore werden ihre Standards kontinuierlich erneuern, um sich ständigen Neuerungen in der Sicherheitsindustrie anzupassen.
- 3.) Mile2- Berater aus dem Sicherheitsbereich werden aktiv neueste Szenarios in die Tat umsetzen, die weit über die in den Basislaboren angewandten oder die in den Kursarbeitsbüchern erwähnten hinausgehen.
- 4.) Bitte beachten Sie, dass dies kein Kurs ist, der sich mit allen Feinheiten jedes einzelnen Tools befasst. Es handelt sich bei der angewandten Software um „Open Source“ und „Underground“-Software, was uns keine Garantie für Kompatibilität gibt.
- 5.) Die im Kurs angewandten Tools werden ständig von Mile2-Beratern getestet. Allerdings kann es sich mitunter ergeben, dass wir ein Tool verwenden, das noch nicht auf der IT- Umgebung unseres Partners getestet wurde.
- 6.) Wir werden eine Reihe von zahlreichen Betriebssystemen verwenden, welche konstruiert sind, sie auf unterschiedliche Art und Weise anzuwenden, zum Beispiel zum Angriff auf ein Netzwerk oder als „Hacker-Box“.