(Certified) Penetration Testing Specialist (PTS)

Kursnummer: 6711

Ziele

Sie erfahren was Sie als professioneller Penetration Testing Specialist (PTS) wissen sollten und erlernen das Know How. Die Inhalte dieses Sicherheitstrainings vermitteln Informationen über aktuelle Schwachstellen und Abwehrtechniken zur Absicherung von Computersystemen und Netzwerken.

Nach dem Kurs werden Sie in der Lage sein, Schwachstellen zu erkennen und zu analysieren, um mögliche Geschäftsrisiken für Unternehmen zu reduzieren, und somit letztlich die Sicherung von wertvollen Informationen vor potentiellen Angreifern zu stärken.Um dieses Ziel zu erreichen, nehmen die Teilnehmer im Verlauf dieses Workshops die Rolle potentieller Angreifer ein, um deren Vorgehensweisen zu erkennen und nachzustellen.Das dabei gelernte Wissen kann anschließend zur Planung und zum Aufbau entsprechender Schutzmaßnahmen für Unternehmen vor potentiellen Angreifern verwendet werden.

Inhalt

Grundlagen der IT-Sicherheit

- eine Einführung und Überblick über die aktuellen Gefahren und Bedrohungspotentiale
- die potentiellen Angreifer und auch die möglichen Gründe für Angriffe auf Unternehmensdaten
- Computersysteme und -netzwerke
- einen Vergleich eines „Hackers“ zum „Penetration Tester“
- Übersicht über die aktuellen „Top-25-Schwachstellen“,
- rechtliche Grundlagen und Veränderungen

Planung, Organisation und Durchführung von Penetrationstests

- Zweck und die Arten von Penetrationstests
- Planung
- mögliche Vorgehensweise während der Durchführung von Penetrationstests
- Allgemeine und strafrechtliche Vorschriften und Gesetze
- Rahmenbedingungen für die Planung und Durchführung der Tests
- notwendige Vertragsgestaltung
- Informationen zu den organisatorischen, technischen und auch personellen Voraussetzungen für die Planung und Durchführung von Penetrationstests.

Planen von Angriffen - Informationen sammeln

- Planung von Angriffen
- Methoden und Werkzeuge
- Informationssammlung, von der Suche im World Wide Web über „Google-Hacking“, E-Mail-Auswertung, Ermittlung geografischer Daten, WhoIs-Abfragen bis hin zur Routenverfolgung
- „Firewalking“
- Tipps für mögliche präventive Maßnahmen
- Tipps für Gegenmaßnahmen

Scanning - Aufspüren von Servern, Diensten und Anwendungen

- Methoden und Tools zur Auffindung und Identifizierung
- Nmap im Einsatz

- „Banner-Grabbing“
- potentiellen Gegenmaßnahmen
- Verschleierungs-Methoden, -Tools und Dienste

Enumeration - Erkennen und auswerten

Methoden und Tools zum Ausspähen

- von Arbeitsgruppen und Domänen
- den Sicherheitsrichtlinien für Benutzerkennwörter
- dem Administrator-Konto
- Freigaben und auch verschiedenen Protokollen im Netzwerk sowie vielem mehr zur Verfügung stehen

Exploitation - Schwachstellen erkennen und ausnutzen

- Ausnutzen vorhandener Schwachstellen in Betriebssystemen oder Computerprogrammen.
- Quellen für die dabei einzusetzenden Exploits
- kommerzielle und nicht-kommerzielle Exploitation-Frameworks, wie beispielsweise MetaSploit oder auch Canvas
- aktuellen, kommerziellen und nicht-kommerziellen Schwachstellenscanner (Nessus, OpenVAS, Retina Network Security Scanner, u.v.m.)
- Einführung in das notwendige Patch-Management

Physikalische Angriffe

- Zurücksetzen von BIOS-Kennwörtern
- Ausspähen von Anmeldedaten durch Keylogger und ähnlichen Methoden

Social Engineering - Feinde unter uns

Verschiedener Angriffstechniken:

- Eavesdropping
- Impersonation Attack
- Shoulder Surfing
- Dumpster Diving
- Phishing
- Pharming
- Spamming
- notwendige Mitarbeiter-Awareness-Kampagnen

Packet Sniffing - aktives und passives Mitlesen

- aktive und auch passive Sniffing-Attacken
- Methoden und Tools zur Identifizierung von Sniffing-Angriffen im Netzwerk
- Sniffing Angriffe verhindern

(Certified) Penetration Testing Specialist (PTS)
Kursnummer: 6711

System-Hacking - Angriffe auf Computersysteme

- Die Authentifizierung anhand von Benutzerkennwörtern
- Authentifizierungsprotokolle
- Pass-the-Hash- (PtH) und Pass-the-Ticket-Angriffe (PtT)
- Windows PowerShell
- Daten innerhalb des Dateisystems von Festplatten unter den aktuellen Windows-Betriebssystemen verstecken,

Attacken gegen Webserver und Webanwendungen •

- potentiellen Gefahren
- möglichen Schutzmaßnahmen,
- Einsatz entsprechender Web Application Firewalls (WAF) und deren Wirkungsweisen

SQL-Injection - Angriffe auf Datenbanken

- Methoden und Tools für Angriffe auf Datenbankserver, wie die Microsoft SQL- oder auch die im Internet oft eingesetzten MySQL-Servern.
- Kennwort-Attacken
- „SQL-Injection“-Angriffe auf Datenbankserver erkennen und ausnutzen

SQL- Denial of Service (DoS) - nichts geht mehr

- Tools und Methoden für die Durchführung von Denial of Services (DoS)-Attacken
- Funktionsweise von Bot-Netzen (Botnets)
- verbundene Gefahren

Malware-Angriffe - Viren, Würmer, Trojaner, Ransomware, Rootkits & Co

- Gefahren durch Viren, Würmer und Trojaner.
- präventiv verhalten
- Tools und Methoden um Trojaner und Backdoors aufzuspüren
- Ransomware-Angriffe und Abwehrmaßnahmen

Angriffe auf Drahtlosnetzwerke (WLANs) und BlueTooth

- Gefahren für Drahtlosnetzwerke (WLANs)
- Methoden und Tools der Angreifer
- Verschlüsselungsmethoden, wie WEP, WPA oder WPA2
- Infrastrukturnetzwerken und Angriffe
- physikalischen Access Points,ein lohnendes Ziel für potentielle Angreifer.
- Tipps zum Einrichten und Betreiben von „sicheren“ Drahtlosnetzwerken
- Gefahren rund um BlueTooth
- notwendigen Schutzmaßnahmen

Angriffe auf VoIP, Fax und Telefonanlagen

- durchgeführten Telefonate digital aufzuzeichnen, ohne dass die Betroffenen davon Notiz nehmen können

- Grundlagen zu Protokollen und möglichen Einsatzszenarien
- mögliche Bedrohungen
- Angriffe auf Voice-over-IP
- Tipps für die Implementierung einer sicheren VoIP-Infrastruktur

Covering Tracks - Spuren vernichten

- Spuren eines Hack-Angriffs zu verschleiern.
- Einträge in Ereignisprotokollen
- Tools und Methoden der Angreifer
- mögliche Abwehrmaßnahmen in Form von bestimmten Unternehmenslösungen (wie z. B. Tripwire)

Firewalls, IDS/IPS und Honeypots

- Einsatzkonzepte für Firewalls
- Intrusion Detection-Systeme (IDS)
- Einsatzort von Honeypots
- Methoden und Tools der Angreifer zum Aufspüren

Cloud Computing - Gefahren für die Virtualisierung

- Gefahrenpotential
- potentielle Gefahren
- mögliche Schutzmaßnahmen für die Dienste und Daten innerhalb des Cloud-Computing

Zielgruppe

• IT-Sicherheitsberater / -Consultants • IT-Sicherheitsbeauftragte • System- und Netzwerkadministratoren • Systemingenieure und Netzwerkplaner

Voraussetzungen

Informationen

Ihr Ansprechpartner

Andrea Nordhoff

Consultant Training & Development
Fon: 0221 | 29 21 16 - 13
E-Mail: training@ce.de