(Anti-)Hacking für Administratoren

Kursnummer: 6710

Ziele

Sie gehen in diesen Training in die Rolle des Angreifers bzw. Hacker simulieren Vorgehensweisen und Ziele.

Nach einer umfangreichen Einführung in die Grundlagen der IT-Sicherheit, attackieren dafür extra installierte Computersysteme bis hin zu Windows 10 und auch Windows Server 2016. Sie erhalten einen Einblick in die Vielfalt der Methoden und Werkzeuge der Angreifer auf Netzwerke, Computersysteme und Dienste.

Durch diesen Perspektivwechsel wird das Bewusstsein für Sicherheitsrisiken und Schutzmaßnahmen geschärft - und somit die Sicherheit in Unternehmen erhöht.

Inhalt

Grundlagen der IT-Sicherheit

- Gründe für Cyberangriffe
- verschiedenen Arten von Angreifern (Hackern)
- Arten von Sicherheitslücken
- Methoden bei Hackerangriffen
- rechtlichen Grundlagen rund um die IT-Sicherheit

Planung und Vorbereitung von Angriffen

- Möglichkeiten Angreifer an Informationen zu gelangen, um Unternehmen oder auch Unternehmensmitarbeiter im Internet ausfindig zu machen.
- Tools und Methoden zur Informationsgewinnung
- Informationsgewinnung zu Unternehmen
- Informationsgewinnung über Suchmachinen, in Newsgroups, Boards usw.
- entwickelte Tools und Methoden zur Recherche

Moderne Angriffstechniken

- Angriffsszenarien
- moderne Tools und Methoden zum Einbruch in Computernetzwerke und Computersysteme
- Merkmale der Tools und Vorgehensweisen erkennen
- Netzwerk-Sicherheitsrichtlinien anpassen

Gefahren durch Viren, Würmer, Trojaner & Rootkits

- aktuellen Gefahren
- möglichen Abwehrmaßnahmen
- praktischer Beispiele

Angriffe auf Drahtlosnetzwerke (WLANs)

- Tools und Methoden zur Auspähung und hacken drahtloser Netzwerke
- Spezifikation IEEE 802.1x

Firewalls, IDS & Honeypots•

- Überblick über Firewall-Lösungen
- Einrichten von Netzwerk- oder Hostbasierten IDS-Systemen und sogenannter Honeypots
- Angriffe erkennen
- Möglichkeiten der Abwehr abwehren
- Rückverfolgung von Angriffen

Einführung in Penetrationstests

- Schwachstellen
- Planung
- Vorbereitun
- Durchführung
- Auswertung von sogenannten Penetrationstests

OPTIONALE MODULE

- Grundlagen der Kryptografie
- Einführung in das BSI-Grundschutzkompendium

Zielgruppe

System- und Netzwerkadministratoren, IT- und Systemverantwortliche, IT-Sicherheitsbeauftragte, IT-Architekten

Voraussetzungen

• Kenntnisse und Fähigkeiten in der Konfiguration und Verwaltung von Windows-Betriebssystemen • Grundlegende Erfahrung in der Verwaltung von Netzwerkdiensten • Kenntnisse zu LANs (Local Area Networks) - lokalen Netzwerken • Kenntnisse und Fähigkeiten im Umgang mit TCP/IP

Informationen

Ihr Ansprechpartner

Andrea Nordhoff

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