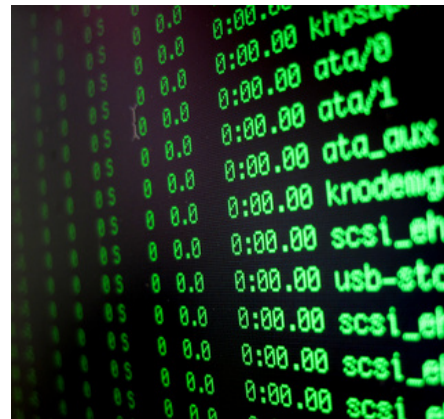


Security Awareness Workshop

{ Führen Sie selbst Angriffe durch und setzen Sie Gegenmaßnahmen um }



Kursbeschreibung

Dieser Kurs vermittelt technische Kenntnisse über aktuelle Angriffsszenarien, Hacking-Methoden und wie man sich von solchen schützen kann. Die Teilnehmer lernen die Vorgehensweisen von Hackern kennen und wenden im Zuge von Labor-Beispielen Werkzeuge an um Zugriff auf Systeme bzw. Daten zu bekommen. Unser Labor stellt eine Kopie eines klassischen Firmennetzwerks mit WLAN, Firewall Komponenten, Webserver, Mailserver, VoIP Equipment, etc. dar. Hier wird es möglich die Gefahren und

Risiken denen ein Unternehmen heute zu tage ausgesetzt ist, kennen zu lernen und gleichzeitig in der Dauer von 3 Tagen, das Ganze von dem Blickwinkel eines Hackers zu betrachten.

Um sich vor Hacker zu schützen, muss man denken wie einer! Sie werden erstaunt sein, mit welcher scheinbar trivialen Methoden Hacker in Ihr Netzwerk eindringen können!

KnowHow Gewinn

- Sie lernen Bedrohungen Ihrer Infrastruktur und Ihrer Daten zu erkennen und einzuschätzen.
- Sie lernen wie Sie diesen Gefahren effektiv und effizient entgegenwirken können.
- Sie lernen die Denkweise von potentiellen Angreifern zu verstehen.
- Sie lernen technische Details, die Ihnen bei der Auswahl von Hard- und Software für Ihre Infrastruktur hilfreich sein werden.

Zielgruppe

Es werden gute IT Kenntnisse vorausgesetzt. Das Seminar richtet sich an IT Leiter, Security Verantwortliche und IT Experten.

Dauer: **3 Tage**

Kosten: **2.290,- EUR exkl. Ust.**

die nächsten Termine finden Sie unter:

<http://www.securesolutions.at/academy>

Kursinhalt

Einführung in das Thema IT-Security

- ▶ Klassische Schutzziele
- ▶ Allgemeine Angriffsszenarien

Technische Grundlagen in Kurzwiederholung

- ▶ TCP/IP-Grundlagen
- ▶ Wichtige Protokolle

Vorgehen eines Angreifers

- ▶ Sammeln von Informationen
- ▶ Footprinting
- ▶ Ziele Ausschuchen
- ▶ Angriffe

✓ Praxisübungen:

Sie durchsuchen das Internet nach Informationen zu Ihrer Firma – wo sind Sie angreifbar?
Sie identifizieren interessante Angriffsziele in unserem Hacking-LAB
Sie lernen verschiedene Hacking Methoden mittels Google kennen

Sicherheit im LAN

- ▶ Sniffing in geschwichten Netzen
- ▶ Man in the Middle
- ▶ Denial of Service
- ▶ Sonstige Angriffe auf VLANs, STP, OSPF, ...
- ▶ Gegenmaßnahmen
- ▶ Layer 2 Sicherheitsfeatures
- ▶ IEEE 802.1X
- ▶ Verschlüsselung

✓ Praxisübungen:

Sie fangen Passwörter von gesicherten https:// Verbindungen ab

Sicherheit in WLANs

- ▶ Sicherheitsstandards
- ▶ Angriffsszenarien
- ▶ Rogue Access Points
- ▶ Gegenmaßnahmen
- ▶ IEEE 802.1X im WLAN
- ▶ RSN in WPA2

✓ Praxisübungen:

Sie hacken WEP und WPA2 gesicherte WLAN Netzwerke

Sicherheit in VPNs

- ▶ Definition und Arten von VPNs
- ▶ Sicherheit einzelner Standards

✓ Praxisübungen:

Sie prüfen Ihr VPN Gateway auf Angreifbarkeit und zeigen wie man VPN Client Verbindungen hackt und somit das Domain Passwort ausliest!

Sicherheit im Web

- ▶ Gefahren im Web
- ▶ Angriffsszenarien auf Webapplikationen
- ▶ SQL Injections
- ▶ XSS, CSRF
- ▶ Angriffsszenarien im Internet
- ▶ Angriffe auf DNS
- ▶ Man in the Middle Angriffe auf HTTPS
- ▶ Gegenmaßnahmen

Spezielle Anwendungsszenarien

- ▶ Sicherheit in IP Telefonie
- ▶ Sicherheit mobiler Geräte

✓ Praxisübungen:

Sie hören VoIP Telefongespräche mit
Sie schaffen sich Zugriff auf SmartPhones und
lesen dann Windows Domain Passwörter aus.

Kryptographische Grundlagen

- ▶ Verschlüsselung (AES, DES, RSA, DAS, ...)
- ▶ Hashes und MACs (SHA, MD5, RIPEMD, ...)
- ▶ Public Key Infrastructure
- ▶ TLS, Kerberos, SSH