IT-Sicherheit:
Hacking für Administratoren

Angriffe erkennen und Schutzmaßnahmen verstärken

Version 9.0

STUDENT-Pack

IT-Sicherheit: Hacking für Administratoren
Seminarunterlage – Artikelnr. HK-200513

Autor: Carlo Westbrook

Version: 9.0

Workshop-Übersicht

Modul 00 - Einführung

Modul 01 - Grundlagen

Modul 02 - Planung und Vorbereitung von Angriffen

Modul 03 - Moderne Angriffstechniken

Modul 04 - Angriffe auf Drahtlosnetzwerke (WLANs)

Modul 05 - Gefahren durch Viren, Würmer, Trojaner & Rootkits

Modul 06 - Firewalls, IDS & Honeypots

Modul 07 - Überblick zu Penetrationstests

Optionale Module (auf der Kursteilnehmer-DVD-ROM enthalten)

Modul 08 - Grundlagen der Kryptografie

Modul 09 - Einführung in das BSI-Grundschutzhandbuch

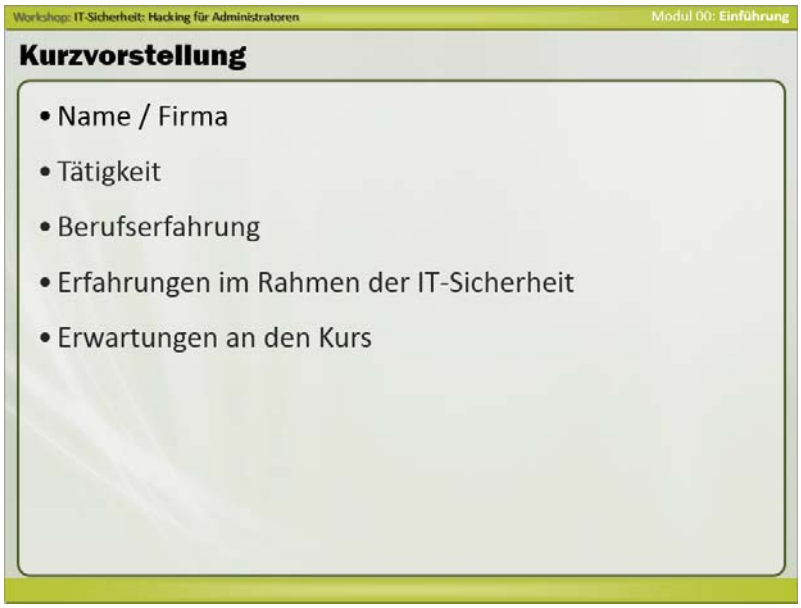
Konventionen & Symbole

Um bestimmten Textpassagen in der Workshop-Unterlage etwas hervorzuheben, wurden die folgenden typografischen Konventionen und Symbole verwendet:

Konvention	Bedeutung
`befehl`	Stellt die Befehlssyntax oder auch Befehlsausführung von Kommandozeilenbefehlen dar.
WEITER	Kennzeichnet die Ausführung einer bestimmten Programmfunktion, beispielweise den Mausklick auf eine Schaltfläche.
	Weist auf einen allgemeinen Hinweis zu bestimmten Themenbereichen hin.
	Gibt einen Hinweis auf wichtige Funktionen oder auch Situationen, die unbedingt beachtet werden sollten.
	Kennzeichnet Tipps für die praktische Anwendung bzw. Umsetzung.
	Kennzeichnet Informationen oder auch Situationen, die ein Risiko oder eine Bedrohung darstellen können.
	Weist auf weitere Informationsquellen zu bestimmten Themenbereichen im Internet hin.
	Verweist auf weitere Inhalte auf der beiliegenden CD-/DVD-ROM.
	Kennzeichnet Methoden oder Tools, mit denen man Gefahren durch Hacker mitunter abwenden kann.

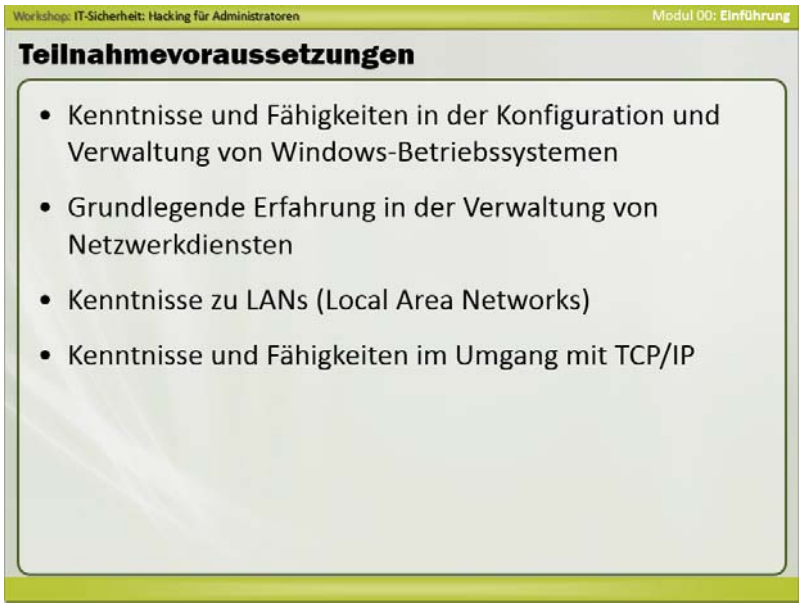
Inhaltsverzeichnis

Kurzvorstellung



Kursvorstellung des Trainers und der einzelnen Kursteilnehmer.

Voraussetzungen



Für diesen Kurs sollten die folgenden Voraussetzungen erfüllt werden:

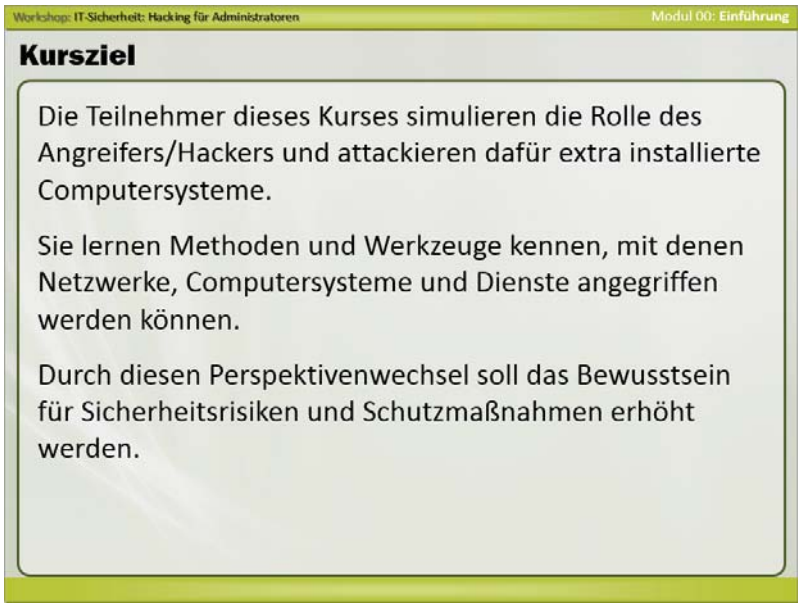
- Kenntnisse und Fähigkeiten in der Konfiguration und Verwaltung von Windows-Betriebssystemen
- Grundlegende Erfahrung in der Verwaltung von Netzwerkdiensten
- Kenntnisse zu LANs (Local Area Networks) – lokalen Netzwerken
- Kenntnisse und Fähigkeiten im Umgang mit TCP/IP

Zielgruppe

Der Kurs ist entworfen worden für

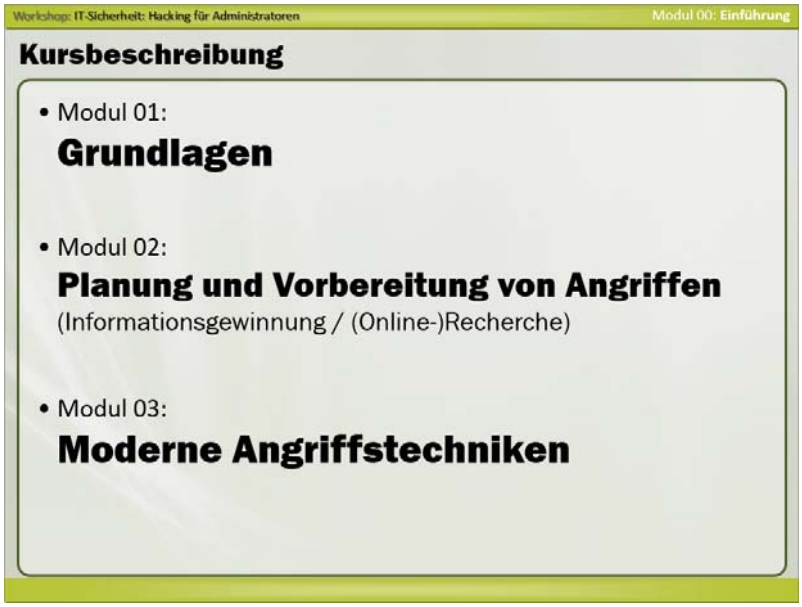
- Administratoren
- System- und Netzwerkverwalter
- IT- und Systemverantwortliche
- IT-Sicherheitsbeauftragte

Kursziel



Die Teilnehmer dieses Kurses simulieren die Rolle des Angreifers/Hackers und attackieren dafür extra installierte Computersysteme. Sie lernen Methoden und Werkzeuge kennen, mit denen Netzwerke, Computersysteme und Dienste angegriffen werden können. Durch diesen Perspektivwechsel soll das Bewusstsein für Sicherheitsrisiken und Schutzmaßnahmen erhöht werden.

Kursbeschreibung



Während des Kurses wird das Wissen rund um die folgenden Themenbereiche vermittelt:

Modul 01:

Grundlagen

In diesem Kapitel erfahren Sie Informationen über die Gründe für Netzwerkangriffe, sowie die Arten von Angreifern (Hackern), mit denen man als Administratoren konfirontiert wird. Auch werden Ihnen häufige Arten von Sicherheitslücken und die zumeist genutzten Methoden bei Netzwerkangriffen erläutert. Darüber hinaus erfahren Sie wichtige Informationen zu rechtlichen Grundlagen.

Modul 02:

Planung und Vorbereitung von Angriffen
(Informationsgewinnung / Recherche)

In diesem Abschnitt erfahren Sie, mit welchen Möglichkeiten Hacker an die notwendigen Informationen gelangen, um Unternehmen im Internet ausfindig zu machen. Die Informationsgewinnung wird Ihnen anhand einer Auswahl an Tools vorgestellt. Nachdem ein Hacker sein „Opfer“ ausfindig gemacht hat, recherchiert er auf verschiedene Weise nach weitern Informationen über das betroffene Unternehmen. Hierbei bedient er sich neben den gängigen Suchmaschinen auch den Informationen in Newsgroups und verwendet weitere, speziell zur Recherche entwickelte Tools, die Ihnen in diesem Abschnitt ausgiebig erläutert werden.

Modul 03:

Moderne Angriffstechniken

Nachdem Sie erfahren haben, wie Angreifer ihre Opfer ausfindig machen und nach möglichen Schwachstellen geforscht haben, wird ein Angriff mit entsprechenden Tools vorbereitet und vollzogen. In diesem Modul erhalten Sie einen umfangreichen Überblick über moderne Tools und Methoden, die von Hackern zum Einbruch in Firmen- und Behördennetzwerke genutzt werden. Hierbei sollen Sie die verschiedenen Merkmale der Tools und Vorgehensweisen erkennen, um die Sicherheitsrichtlinie in Ihrem Netzwerk darauf ausrichten zu können.

Kursbeschreibung (Fortsetzung)

Modul 04:

Angriffe auf Drahtlosnetzwerke (WLANs)

Die Mobilität der Mitarbeiter steht in Unternehmen und Behörden immer mehr im Vordergrund. Hierbei werden häufig mobile Geräte, wie bspw. PDAs und Notebooks eingesetzt, mit denen man sich über Wireless LAN oder Bluetooth auf die Unternehmensnetzwerke und –server verbindet, um Daten abzurufen oder zu speichern. In diesem Kapitel werden Ihnen Tools aufgezeigt, mit denen Hacker Ihre drahtlosen Netzwerke ausspähen oder gar hacken können. Die Veranschaulichung soll Ihnen für die Absicherung der drahtlosen Netzwerkkomponenten dienlich sein.

Modul 05:

Gefahren durch Viren, Würmer, Trojaner & Rootkits

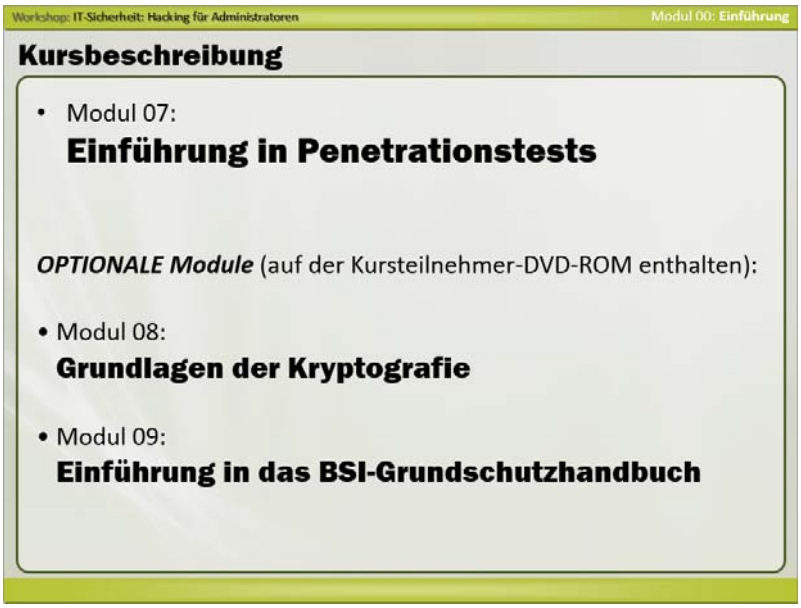
Die Gefahr durch Viren, Würmer, Trojaner, Malware und Rootkits bedroht nicht nur die vielen privat genutzten PCs, sondern auch die in Unternehmen betriebenen Computersysteme und Server - und natürlich insbesondere die darin verarbeiteten und gespeicherten Unternehmensdaten. In diesem Modul werden die aktuellen Gefahren, sowie die möglichen Abwehrmöglichkeiten umfangreich erläutert.

Modul 06:

Firewalls, IDS & Honeypots

In diesem Modul erhalten Sie einen Überblick über Firewall-Lösungen verschiedener Hersteller. Zudem werden Ihnen mögliche Lösungen zum Einrichten von IDS-Systemen und sogenannter Honeypots erläutert, um Angriffe von Hackern besser abwehren und auch rückverfolgen zu können.

Kursbeschreibung (Fortsetzung)



Modul 07:

Einführung in Penetrationstests

Um mögliche Sicherheitslücken aufdecken und beseitigen zu können, müssen das eigene Netzwerk, sowie die darin enthaltenen Server und Clients auf mögliche Schwachstellen untersucht werden. In diesem Kapitel erfahren Sie mehr über die Vorbereitung, Durchführung und Auswertung von sogenannten Penetrationstests.

OPTIONALE MODULE:

Auf der Teilnehmer-DVD-ROM finden sich noch die folgenden, zusätzlichen Module, die für die Vertiefung des Lernstoffes nach dem Kursbesuch gedacht sind:

Modul 08:

Grundlagen der Kryptografie

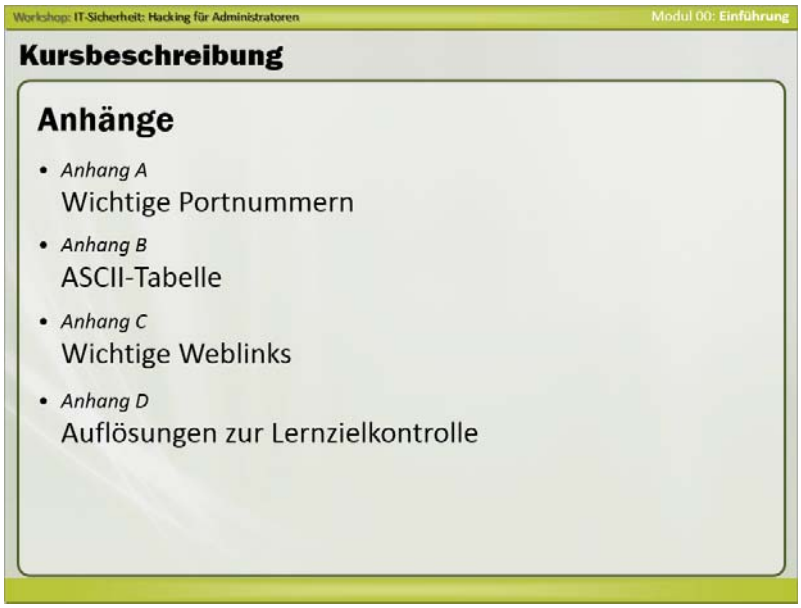
In diesem Modul werden Sie in die Grundlagen der Kryptografie eingeführt.

Modul 09:

BSI-Grundschutzhandbuch

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bietet mit dem Grundschutzhandbuch eine fast vollständige Quelle für Informationen rund um die Sicherheit in Unternehmensnetzwerken. In diesem Kapitel erhalten Sie einen Überblick über die darin bereitgestellten Informationen.

Kursbeschreibung (Fortsetzung)



Zur Vertiefung des Lernstoffes sind im Anhang dieser Seminarunterlage zusätzliche Informationen enthalten:

AnhangA - Übersicht über verwendete Portnummern (IANA)

Anhang B - ASCII-Tabelle

Anhang C - Wichtige Weblinks

Anhang D – Auflösungen zur Lernzielkontrolle

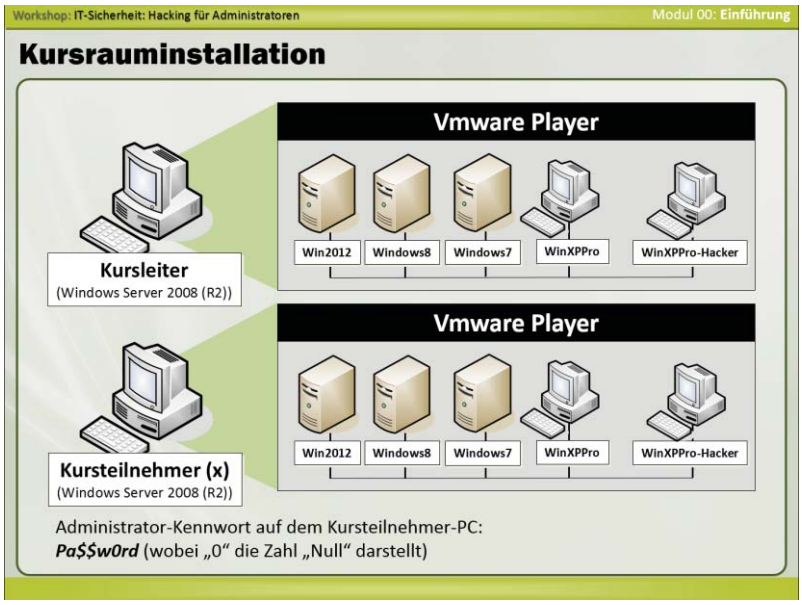
Wichtiger Hinweis

Wir empfehlen Ihnen, zum Ausprobieren der Methoden, Tools und Programme ein entsprechendes Testnetzwerk aufzubauen, welches - ***nicht*** - mit dem Produktivnetzwerk oder mit einzelnen Produktivsystemen des Unternehmens verbunden ist.

Wichtiger Hinweis: Die in diesem Kurs vorgestellten Methoden, Tools und Programme sollen Administratoren und Systemverantwortlichen dazu dienen, die eigene Netzwerk- und Systemsicherheit zu überprüfen und Sicherheitsmängel zu beseitigen. Wir raten, vor Verwendung zuerst Rücksprache mit den System-verantwortlichen oder auch Vorgesetzten in Ihrem Unternehmen zu halten, um Missverständnisse zu vermeiden. Der Missbrauch der in dieser Unterlage beschriebenen Methoden, Tools und Programme gegenüber Dritten ist untersagt und gemäß verschiedener Gesetze zumeist strafbar für den Durchführenden. Der Herausgeber der Schulungsunterlage, der Autor, die Ersteller der Tools und Programme sowie auch das Schulungsunternehmen übernehmen ausdrücklich keinerlei Haftung für die Verwendung der Methoden, Tools und Programme. Die Verwendung geschieht auf eigene Gefahr.

Mit Urteil vom 12.05.1998 - Az. 312 O 85/98 - hat das Landgericht Hamburg entschieden, dass man durch die Anbringung eines Links die Inhalte der verlinkten Seite unter Umständen mit zu verantworten hat. Dies kann nur verhindertwerden, indem man sich ausdrücklich von diesen Inhalten distanziert.Um diesem Urteil Rechnung zu tragen distanzieren wir uns in diesem Sinne ausdrücklich von den Inhalten aller angegebenen Links zu Webseiten von Dritten.

Kursrauminstallation



Die Kursrauminstallation ist so konzipiert, dass jeder Teilnehmer über jeweils einen eigenen, physikalischen Computer unter Windows Server 2008 (R2) als Host-Computer mit installiertem Vmware-Player verfügt, auf dem weitere, virtuelle Computersysteme für die Durchführung von Übungen bereitgestellt sind.

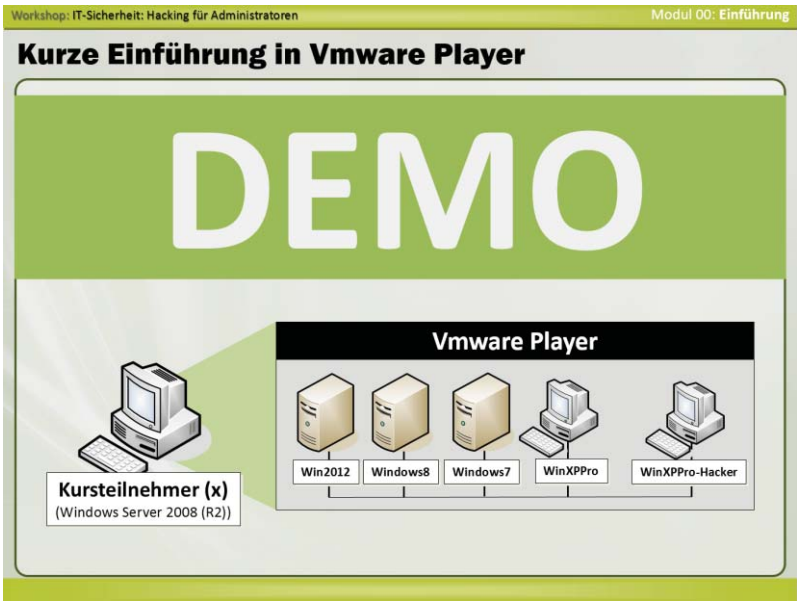
Die Übungen werden in der Regel innerhalb der virtuellen Umgebung im Vmware-Player unter Windows Server 2008 R2 als Host-System in Verbindung mit den darin enthaltenen, virtuellen PCs erarbeitet. Ein Netzwerkzugriff auf Systeme außerhalb der Schulungsumgebung ist während der Übungen nicht vorgesehen.

Jedem Teilnehmer stehen innerhalb des eigenen Host-Computers insgesamt 5 virtuelle Computersysteme im Vmware-Player zur Verfügung:

Hinweis

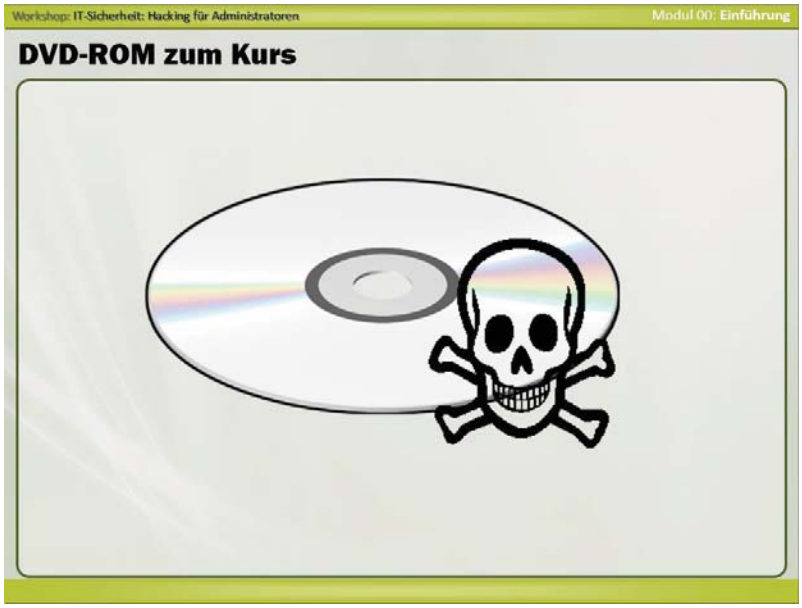
Die für den Kurs erforderlichen Programme und Tools sind auf der Kursteilnehmer-DVD-ROM bzw. teilweise in Freigaben hinterlegt und werden bei Bedarf innerhalb der Übungseinheiten installiert.

Kurze Einführung in Vmware Player



Der Kursleiter führt Sie kurz in die Handhabung der virtuellen Maschinen mit dem **Vmware-Player** unter Windows Server 2008 R2 ein.

DVD-ROM zum Kurs

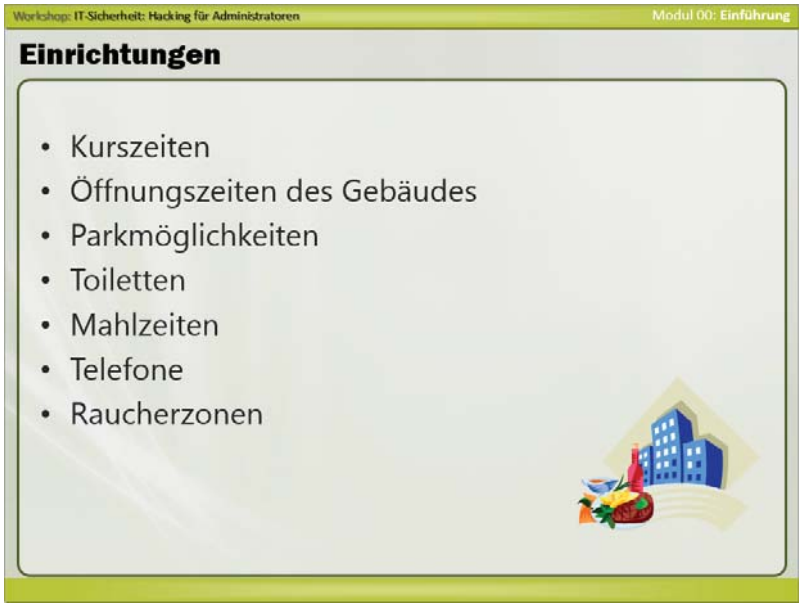


Damit Sie die einzelnen Kursübungen zur Vertiefung des Lernstoffs nachstellen können, liegt dieser Kursunterlage eine **Teilnehmer-DVD-ROM** bei, auf der die meisten, im Kursverlauf vorgestellten Tools und Programme, sowie Dokumentationen und mehr enthalten sind.

Setzen Sie die auf der DVD-ROM enthaltenen Tools und Programme nicht ungefragt und ungeprüft in einer produktiven Umgebung ein.

Beachten Sie vor dem Gebrauch der Tools und Programme unbedingt die Inhalte der Datei Wichtig.txt. Die darin genannten Inhalte erkennen Sie mitder Verwendung der Tools und Programme an.

Einrichtungen



Der Kursleiter gibt Ihnen noch weitere Informationen zu den Einrichtungen des Schulungscenters, den Kurszeiten und Öffnungszeiten, den Partmöglichkeiten und vielem mehr.

Wenden Sie sich bei Fragen gerne jederzeit an den Kursleiter.

Modul 01:
Grundlagen

Themeninhalt:

- Einführung
- Aktuelle Trends & Entwicklungen
- Bedrohungspotential
- Gründe für Netzwerkangriffe
- Arten von Angreifern
- Angriffsziele & Häufige Arten von Sicherheitslücken
- Häufige Methoden bei Netzwerkangriffen
- Windows-Sicherheitsfeatures aus Sicht des Angreifers
- Rechtliche Grundlagen

IT-Sicherheit: Hacking für Administratoren
Seminarunterlage – Artikelnr. HK-200513

Autor: Carlo Westbrook

Version: 9.0