



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

Alle in dieser Seminarunterlage enthaltenen Programme, Darstellungen und Informationen wurden nach bestem Wissen erstellt und mit Sorgfalt getestet. Dennoch sind Fehler nicht ganz auszuschließen. Aus diesem Grund ist das in der vorliegenden Seminarunterlage enthaltene Material mit keiner Verpflichtung oder Garantie irgendeiner Art verbunden. Der Autor und CertPro Limited übernehmen infolgedessen keine Verantwortung und werden keine daraus folgende Haftung übernehmen, die auf irgendeine Art aus der Benutzung dieses Materials, oder Teilen davon, oder durch Rechtsverletzungen Dritter entsteht.

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in dieser Seminarunterlage berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann verwendet werden dürften.

Die in diesem Dokument aufgeführten Namen tatsächlicher Firmen und Produkte sind möglicherweise Marken der jeweiligen Eigentümer und werden ohne Gewährleistung der freien Verwendbarkeit benutzt. CertPro ist eine eingetragene Marke von Carlo Westbrook.

Dieses Werk ist urheberrechtlich geschützt.

Kein Teil dieses Dokuments darf ohne ausdrückliche schriftliche Erlaubnis für irgendwelche Zwecke vervielfältigt oder in einem Datenempfangssystem gespeichert oder darin eingelesen werden (auch nicht zur Unterrichtsvorbereitung), unabhängig davon, auf welche Art und Weise oder mit welchen Mitteln (elektronisch, mechanisch, durch Fotokopieren, Aufzeichnen, usw.).

Copyright © 2004-2013 CertPro Limited.
Alle Rechte vorbehalten.

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

Inhaltsverzeichnis

Inhalt	Seite
Voraussetzungen	12
Kursziel	13
Kursbeschreibung	14 - 17
Wichtiger Hinweis	18
Kursrauminstallation	19
Kurze Einführung in VMware Player	20
Inhalte der Teilnehmer-DVD-ROM.....	21
Einrichtungen	22
<i>Modul 01:</i>	
Grundlagen.....	23 - 100
Einführung.....	25
Aktuelle Trends und Entwicklungen.....	26 - 31
Bedrohungspotential	32 - 34
Gefahren für Computersysteme und -netzwerke	35 - 43
Gründe für Netzwerkangriffe	44 - 46
Arten von Angreifern (Hackern).....	47 - 50
Klassifizierung der „Hacker“	51 - 52
Angriffsziele & häufige Arten von Sicherheitslücken	53
Potentielle Angriffsziele	54
Häufige Arten von Sicherheitslücken	55
Arten von Sicherheitsbedrohungen	56
Die „Top 25-Schwachstellen“	57 - 58
Häufige Methoden bei Netzwerkangriffen.....	59 - 61
Phasen eines (geplanten) Hackerangriffs	62
Windows-Sicherheitsfeatures aus der Sicht des Angreifers.....	63 - 86
Wichtige Sicherheitsprinzipien.....	87
Schutz durch mehrstufige Verteidigung	88
Rechtliche Grundlagen.....	89 - 98
Strafbare Handlungen	91
Straftatbestände nach StGB und UWG.....	93
Strafanzeige und Strafantrag.....	96
Beweismittel.....	98
Zusammenfassung.....	99
Lernzielkontrolle	100
<i>Modul 02:</i>	
Planung und Vorbereitung von Angriffen	101 - 226
Einführung.....	103
Footprinting - dem Opfer auf der Spur	104
Ziele des Footprinting	105
Durchstöbern von Informationsquellen	106
Suche nach Firmeninformationen im Internet	107
Gelbe Seiten, Telefonbücher & Co.....	108
Personensuche im Internet.....	109
DEMO: Personensuche im Internet.....	110
Personensuche im Internet - „Nicknames“	111
Online-Dienste zur Personensuche	112
Suche in „Social Networks“	113
Suche nach Webseiten.....	114

Google als „Proxy Server“ missbrauchen	115
DEMO: Aufruf von Cache-Inhalten in Google	116
Google-Hacking - Opfersuche leicht gemacht	117
GHDB - Die „Google Hacking-Database“	119
DEMO: Suche nach Kennwörtern in der GHDB	120
Google-Hacking leicht gemacht.....	121
DEMO: Google-Hacking mit SiteDigger 3.0	122
Firmenwebsite und Stellenausschreibungen	123
Zurück in die Vergangenheit – „archive.org“	124
DEMO: Internet-Recherche mithilfe von „archive.org“	125
Copernic Agent	126
DEMO: Internet-Recherche mithilfe von Copernic Agent	127
Maltego - professionelle Recherche	128
HTTrach Web Site Copier	129
Webbasierte Zugänge zu Netzwerkdiensten	130 - 131
Google-Earth & Co.....	132
DEMO: „Vogelperspektive“ von Gebäuden in Bing-Maps	133
Read Notify - „Invisible Tracking“ und mehr.....	134
DEMO: „Invisible Tracking“ mittels Readnotify.com	135
DNS-Abfrage & WHOIS	136
DEMO: Domäneninhaber mittels DeNIC & Internic ermitteln	138
Ermittlung des Inhabers bestimmter IP-Adressen.....	139
DEMO: Ermitteln des Inhabers bestimmter IP-Adressen	140
WhatsMyIp.com - Wer bin ich überhaupt?.....	141
SamSpade - detaillierte Informationssuche	142
DEMO: Routenverfolgung mittels SamSpade	143
Abfragen an DNS-Server	144
Routenverfolgung mit Traceroute	145
NeoTracePro (jetzt „McAfee Visual Trace“) & Co.	147
Scanning – die Suche nach der offenen „Tür“	149
Rechner orten – am Anfang steht die Suche	151
Angy IP	152
Portscan-Tools.....	153
SuperScan.....	154
Network Mapper	155
IPSecScan.....	158
Net Tools-Suite.....	159
Portscan-„Light“ mit telnet	160
Praktische Übung	162
Portscans erkennen	163
Firewalk - ab durch die Feuerwand.....	164
Firewalk - Gegenmaßnahmen.....	165
Enumeration – Server und Betriebssysteme ausspähen	166
Ausspähen von Webservern	167
Banner-Grabbing.....	168
Ausspähen weiterer Netzwerkdienste	173
Ausspähen von FTP-Servern.....	173
Ausspähen von SMTP-Servern.....	174
Ausspähen des Administrator-Kontos.....	180
DEMO: Ermitteln des Administratorkontos	182
Ausspähen von NetBIOS-Sitzungen.....	183
WinFingerPrint.....	187
DumpSec.....	188
Praktische Übung	190
Schutz gegen den Missbrauch der IPC\$-Freigabe	191
„RestrictAnonymous=1“ – umgehen	193
Praktische Übung	197
Active Directory ausspähen.....	198
Ausspähen von Active Directory verhindern	201
Unix ausspähen	203

Verhindern der RPC-Ausspähung unter Unix/Linux	205
Benutzer unter UNIX/Linux abfragen	206
Abfragemöglichkeit über rwho nd rusers verhindern	206
Suche nach passenden Exploits.....	207
Exploit-Kategorien	208
DEMO: Ermitteln aktueller Exploits	210
MetaSploit-Framework – Exploits für alle	211
Immunity CANVAS	214
Schwachstellen vorbeugen: Patch-Management.....	215
Update-Management mit WSUS	216
DEMO: Manueller Download von Patches	217
Secunia CSI & PSI.....	218
Praktische Übung	219
Schwachstellen-Scanner	220
Praktische Übung	221
Angriffsplan erstellen.....	222
Botnets.....	223
Angriffe verschleiern mittels offener Proxyserver.....	224
Zusammenfassung.....	225
Lernzielkontrolle	226

Modul 03:

Moderne Angriffstechniken	227 - 322
Einführung.....	229
Gefahren für Gebäude, Serverräume und Netzwerkverbindungen	230
Schutz gegen Angriffe auf Gebäude, Serverräume, Netzwerkgeräte & -verbindungen	233
Gefahren für Computersysteme	234
BIOS-Kennwörter „knacken“.....	235
Benutzerkennwörter zurücksetzen	236
NTCrack & Co. - Passwort-Reset leichtgemacht	237
Kommerzielle Tools zum Passwort-Zurücksetzen.....	238
Ophcrack Live-CD - Passwort-Crack für „Jedermann“	239
Installations-DVD - Windows aushebeln leicht gemacht.....	240
DEMO: Windows mithilfe der Installations-DVD aushebeln	241
Physikalische Angriffe mit Keyloggern.....	242
Hardware-Keylogger - eine Auswahl	243
DEMO: Einsatz von Hardware-Keyloggern	244
Schutz gegen physikalische Angriffe auf Computersysteme	245
Software-Keylogger - die unsichtbare Gefahr	246
Software-Keylogger - eine Auswahl	247
USB-Spyware & Co. - die oft „verkannte“ Gefahr.....	248
Schutz gegen Software-Keylogger & Spyware.....	249
Social Engineering - „Feinde unter uns...“	250
Typische Social Engineering-Angriffe.....	251
„Shoulder Surfing“ - ohne großen Aufwand	252
DEMO: Einsatz von Spycams	254
„Dumpster Diving“ - die Mühe lohnt sich oft	255
USB-Sticks & Co. - die oft unerkannten Gefahren.....	256
Schutz gegen Social Engineering-Attacken	257
Electronic Social Engineering	258
Phishing - Typisches Beispiel für Phishing-E-Mails	260
Professionelles Phishing.....	261
Vorbereitende Schritte der Phisher	262
DEMO: Fake-Webseite im Internet Explorer	263
Pharming - die Unterstützung für den Phisher	264
DNS-Changer - weitere Unterstützung für den Phisher	265
DEMO: Pharming-Versuch unter Windows XP	266
Phishing /Pharming - ein Paradebeispiel aus der Praxis... ..	267
Phishing-Tricks - Basis 10-Adressen... ..	268

Phishing-Tricks- Kurz-URL-Dienste...	268
Schutz gegen Phishing- und Pharming	270
Imformationsammlung in Social Networks	271
Schutzmöglichkeiten gegen Angriffe in Social Networks	272
Einführung in Sniffer Tools	273
WireShark (ehemals Ethereal)	274
Nach Kennwort-Hashes "sniffen"	275
Sniffer-Attacken vorbereiten.....	276
Praktische Übung.....	278
Sniffer aufspüren mit PromiScan	279
Angriffe auf Kennwörter.....	280
Windows-Anmeldemaske - MSGina vs. Windows 7	281
Kennwörter und sichere Kennwörter.....	282
(Un-)Sichere Kennwörter	284
Das „Problem“ mit den GPUs.....	285
Angriffe auf Passwörter in Windows-Netzwerken	286
Windows und Passwörter.....	287
Verbesserung mit NTLMv2	289
Kerberos V5-Protokoll	290
Absichern der Authentifizierung	292
Methoden für den Angriff auf Kennwörter	297
Kennwörter erraten	298
Erraten von Kennwörtern automatisieren	299
Schutz gegen das Erraten von Kennwörtern	300
Kontosperrungsschwelle konfigurieren	301
Nach Kennwörtern „sniffen“	303
(Remote-)Kennwörter „knacken“	305
Weitere Passwort-Cracker	309
Praktische Übung.....	310
Schutz gegen Passwort-Cracker.....	311
Auslesen von Kennwortfeldern	312
DEMO: Auslesen von Kennwortfeldern	313
Kennwortschutz von Dateien cracken.....	314
DEMO: Kennwortschutz von Dateien cracken	315
Tricks der Hacker - Dateien verstecken.....	316
Alternative NTFS-Datenströme	317
In NTFS versteckte Dateien aufspüren.....	319
Praktische Übung.....	320
Zusammenfassung.....	321
Lernzielkontrolle	322

Modul 04:

Angriffe auf Drahtlosnetzwerke (WLANs)	323 - 368
Einführung.....	325
Wireless LAN- (WLAN)- Grundlagen	326
WLAN-Standards und Frequenzen	328
Der IEEE 802.11-Standard und das ISO/OSI-Modell	330
WLAN-Sicherheit.....	332
Verschlüsselung	333
WEP (Wireless Equivalent Privacy)	334
WPA und WPA2	336
Zugriffskontrolle (Access Control)	337
Closed Network	338
IEEE 802.1x/EAP	339
Virtual Private Network (VPN).....	341
Open User Authentication (OUA).....	342
Traffic Lock.....	343
Gefahren für Drahtlosnetzwerke (WLANs)	344
Konfiguration "Open System"	346
"Gefährliche" Access Points	347
Man-In-Middle-Attacken	348

Passive Angriffe	349
Klartext- und Wörterbuch-Attacken.....	350
Denial of Service -Attacken gegen WLANs	352
Air-Jack-Suite.....	353
Footprinting - dem WLAN auf der Spur.....	354
WiFi-Finder	355
inSSIDer.....	256
Wireless LAN-Hacking	357
AirCrack NG.....	358
DEMO: WPA und WPA2-Crack mit AirCrack NG	359
Weitere WLAN-Cracker-Tools	360
WLAN-Hack ganz ohne Tools?	362
Tipps für das Betreiben von sicheren WLANs	363
DEMO: (optional) Konfiguration eines WLAN-AccessPoints	365
Zusammenfassung.....	366
Lernzielkontrolle	267

*Modul 05:***Gefahren durch Viren, Würmer, Trojaner & Rootkits.. 369 - 430**

Einführung.....	371
Computerviren & Würmer.....	372
Virusdefinition	373
Virus-Kategorien	374
DEMO: Analysieren von Virendateien	381
Virenbaukästen aus dem Internet.....	382
Verbreitungsmöglichkeiten von Computerviren und -würmern.....	383
Computerwurm - der Unterschied zu einem Virus.....	384
Schutz vor Viren und Würmern.....	385
Antivirus-Software - vielfältiges Angebot	386
Testviren & Co.	387
Praktische Übung	388
Online-Tests für Dateien	389
DEMO: Online-Überprüfung von Dateien	390
Spyware - die oft „verkannte“ Gefahr.....	391
Schutz vor Spyware	392
Trojaner.....	393
Trojaner-Arten.....	394
Bekannte Trojaner-Programme	397
Praktische Übung	401
Weitere Backdoor-Tools & Trojaner	402
DarkComet-RAT, BlackShades & Co. - aktuelle Gefahren	403
Infektionsmöglichkeiten mit Trojanern	404
Vortäuschen bestimmter Dateitypen.....	405
Verstecken von Trojanern mit Wrappern	406
EliteWrap.....	407
DEMO: Verstecken von Trojanern mit EliteWrap	408
Infektion mit Trojanern vermeiden	409
Trojaner und Backdoors aufspüren	411
sigverif.....	412
sfc.....	413
Taskmanager	414
Netstat.....	415
TCPView	416
Process Explorer.....	417
Autoruns.....	418
MSInfo32.....	419
Rootkits - die unsichtbare Gefahr.....	420
Arten von Rootkits.....	421
Weiter Rootkits.....	424
DEMO: Einsatz von Rootkits unter Windows.....	425

Rootkits aufspüren	426
Anti-Rootkit-Software - eine Auswahl.....	427
DEMO: Aufspüren von Rootkits unter Windows	428
Zusammenfassung.....	429

Modul 06:

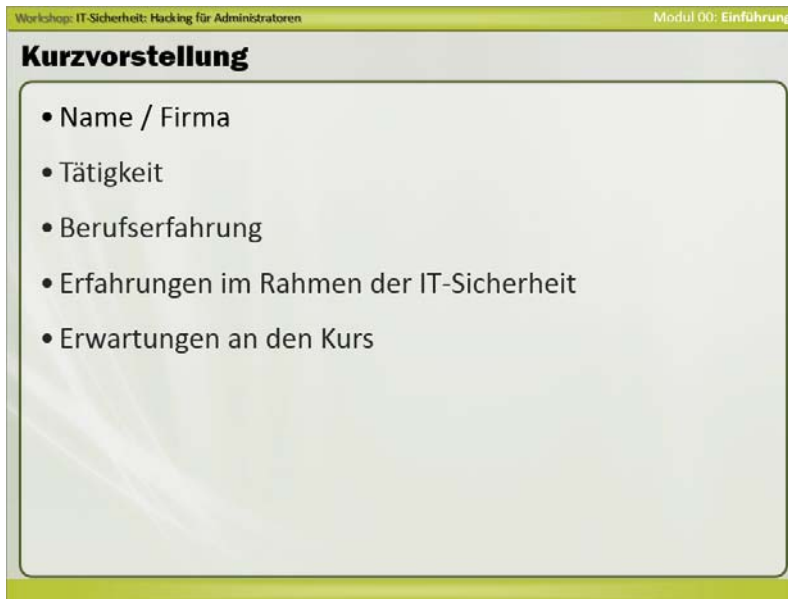
Firewalls, IDS & Honeypots	431 - 474
Einführung.....	433
Einführung in Firewalls	434
De-Militarisierte Zone (DMZ)	435
Filtertechnologien	436
Einsatzkonzepte für Firewalls	437
Unternehmens-Firewalls	441
DEMO: Einführung in Microsoft ForeFront TMG 2010	442
Personal Firewalls	443
DEMO: Windows-Firewall unter Windows 8	444
Beispiel für das Umgehen einer einfachen Firewall-Lösung	445
Portumleitung mit FPipe	448
DEMO: Verwendung von fpipe.exe für die Portumleitung	450
Firewalk - ab durch die Wand	451
HTTPTunnel	453
Intrusion Detection Systeme (IDS)	454
Arten von Intrusion Detection Systemen (IDS)	455
Platzierung von Intrusion Detection Systemen (IDS)	456
Eindringversuche erkennen	457
Snort	458
Funktionsweise von Snort	459
DEMO: Bereitstellung von Snort als IDS unter Windows	461
Weitere IDS-Systeme	462
Honeypots - die Honigtöpfe	463
Honeypots - Verwendungszwecke	464
Honeypots - Einsatzorte	465
Honeypots - Typen	466
KeyFocus KFSensor	467
Praktische Übung.....	469
SPECTER	470
Weitere Honeypot-Lösungen	472
Honeypots aufspüren	473
Zusammenfassung.....	474

Modul 07:

Einführung in Penetrationstests	475 - 486
Einführung.....	477
Zweck eines Penetrationstests.....	478
IT-Sicherheit und Penetrationstests	479
Arten von Penetrationstests	480
Phasen eines Penetrationstests.....	481
Erläuterung zu den einzelnen Phasen	482
Zusammenfassung.....	485

<i>Anhang A: Portnummern (Auszug).....</i>	<i>487</i>
<i>Anhang B: ASCII-Tabelle</i>	<i>495</i>
<i>Anhang C: Wichtige Weblinks</i>	<i>499</i>
<i>Anhang D: Antworten zur Lernzielkontrolle.....</i>	<i>503</i>

Kurzvorstellung



Workshop: IT-Sicherheit: Hacking für Administratoren Modul 00: Einführung

Kurzvorstellung

- Name / Firma
- Tätigkeit
- Berufserfahrung
- Erfahrungen im Rahmen der IT-Sicherheit
- Erwartungen an den Kurs

Kursvorstellung des Trainers und der einzelnen Kursteilnehmer.

Voraussetzungen

Workshop: IT-Sicherheit: Hacking für Administratoren Modul 00: Einführung

Teilnahmevoraussetzungen

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

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

Workshop: IT-Sicherheit: Hacking für Administratoren Modul 00: Einführung

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 Perspektivenwechsel soll das Bewusstsein für Sicherheitsrisiken und Schutzmaßnahmen erhöht werden.

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

The image shows a slide titled 'Kursbeschreibung' (Course Description) from a workshop. The slide is framed with a green border and contains the following text:

Workshop: IT-Sicherheit: Hacking für Administratoren Modul 00: Einführung

Kursbeschreibung

- Modul 01:
Grundlagen
- Modul 02:
Planung und Vorbereitung von Angriffen
(Informationsgewinnung / (Online-)Recherche)
- Modul 03:
Moderne Angriffstechniken

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 konfrontiert 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 weiteren 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)

Workshop: IT-Sicherheit: Hacking für Administratoren Modul 00: Einführung

Kursbeschreibung

- Modul 04:
Angriffe auf Drahtlosnetzwerke (WLANs)
(Tools & Methoden)
- Modul 05:
Gefahren durch Viren, Würmer, Trojaner & Rootkits
- Modul 06:
Firewalls, IDS & Honeypots

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)

Workshop: IT-Sicherheit: Hacking für Administratoren Modul 00: Einführung

Kursbeschreibung

- Modul 07:
Einführung in Penetrationstests

OPTIONALE Module (auf der Kursteilnehmer-DVD-ROM enthalten):

- Modul 08:
Grundlagen der Kryptografie
- Modul 09:
Einführung in das BSI-Grundschutzhandbuch

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

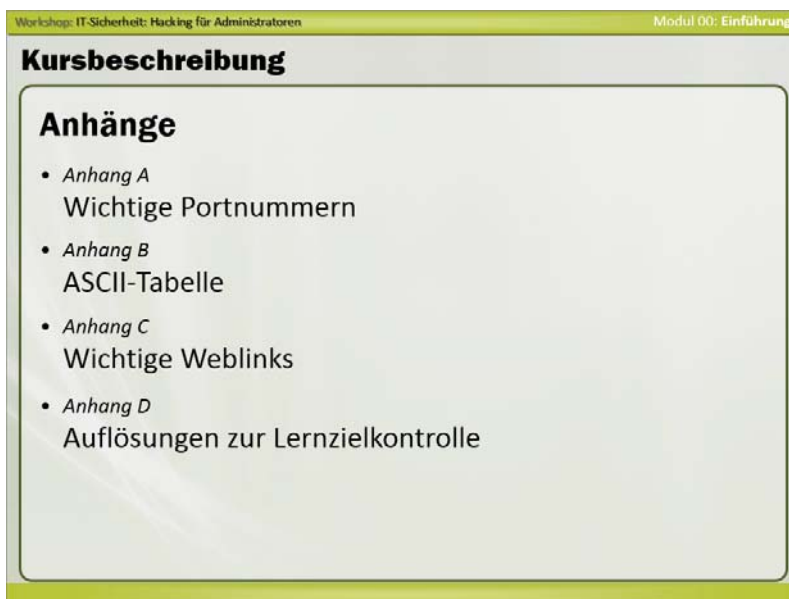
In diesem Modul werden Sie in die Grundlagen der Kryptografie eingeführt.

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)



The image shows a slide from a presentation. At the top left, it says 'Workshop: IT-Sicherheit: Hacking für Administratoren'. At the top right, it says 'Modul 00: Einführung'. The main title of the slide is 'Kursbeschreibung'. Below the title, there is a section titled 'Anhänge' (Attachments) with a bulleted list of four items:

- *Anhang A*
Wichtige Portnummern
- *Anhang B*
ASCII-Tabelle
- *Anhang C*
Wichtige Weblinks
- *Anhang D*
Auflösungen zur Lernzielkontrolle

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

Anhang A - Übersicht über verwendete Portnummern (IANA)

Anhang B - ASCII-Tabelle

Anhang C - Wichtige Weblinks

Anhang D – Auflösungen zur Lernzielkontrolle

Wichtiger Hinweis

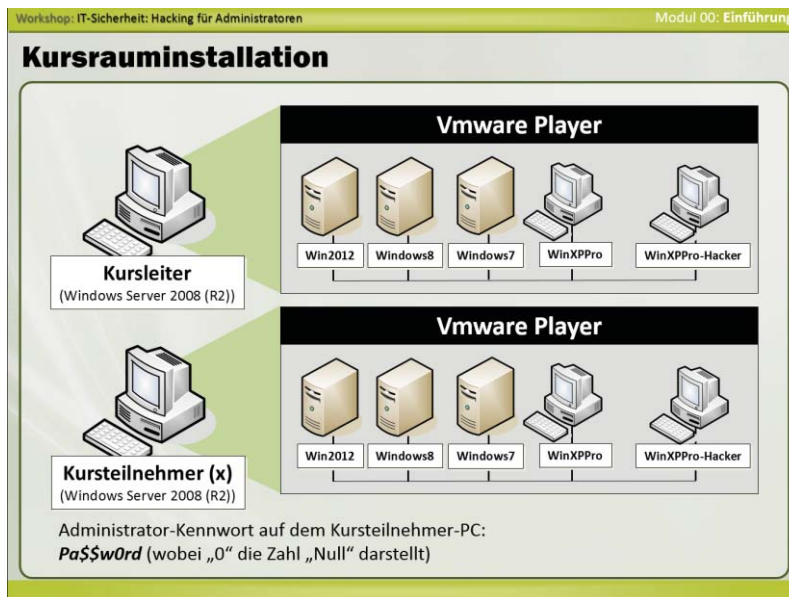


Wir empfehlen Ihnen, zum Ausprobieren der Methoden, Tools und Programme ein entsprechendes Testnetzwerk aufzubauen, welches - **nicht** - mit dem Produktivnetzwerk oder mit einzelnen Produkktivsystemen des Unternehmens verbunden ist.

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 Systemverantwortlichen 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 verhindert werden, 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.

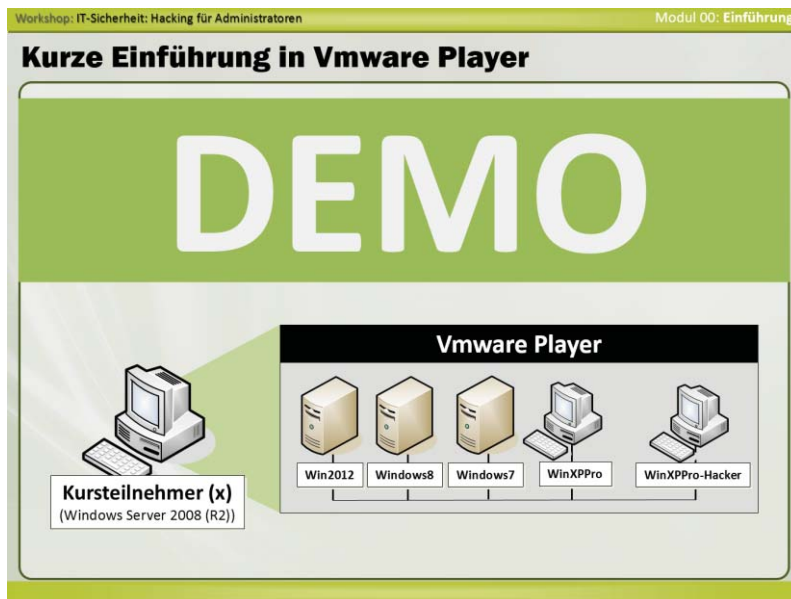
Die Übungen werden in der Regel innerhalb der virtuellen Umgebung im Vmware-Player unter Windows Server 2008 R2 als Host-System in Verbindung mit den darin enthaltenen, virtuellen PCs erarbeitet. Ein Netzwerkzugriff auf Systeme außerhalb der Schulungsumgebung ist während der Übungen nicht vorgesehen.

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

Hinweis

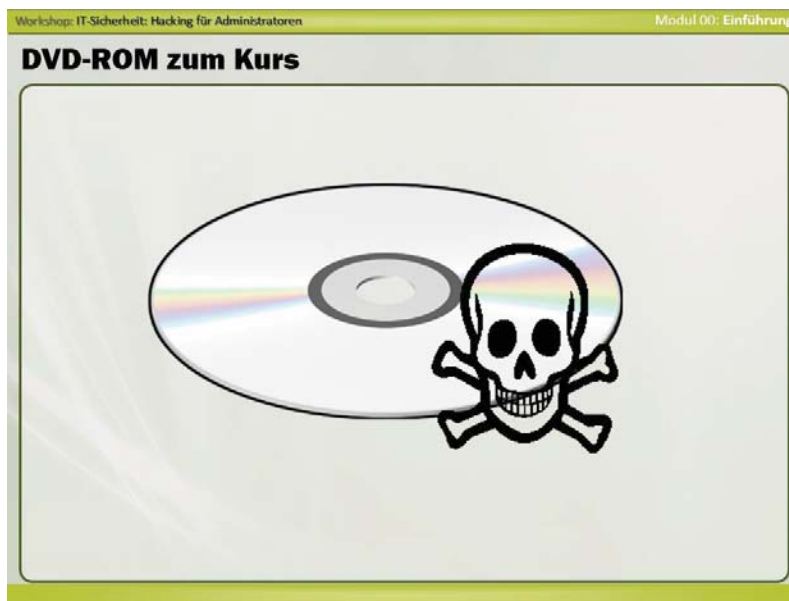
Die für den Kurs erforderlichen Programme und Tools sind auf der Kursteilnehmer-DVD-ROM bzw. teilweise in Freigaben hinterlegt und werden bei Bedarf innerhalb der Übungseinheiten installiert.

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 mit der Verwendung der Tools und Programme an.

Einrichtungen

Workshop: IT-Sicherheit: Hacking für Administratoren Modul 00: Einführung

Einrichtungen

- Kurszeiten
- Öffnungszeiten des Gebäudes
- Parkmöglichkeiten
- Toiletten
- Mahlzeiten
- Telefone
- Raucherzonen



Der Kursleiter gibt Ihnen noch weitere Informationen zu den Einrichtungen des Schulungscenters, den Kurszeiten und Öffnungszeiten, den Parkmöglichkeiten 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

Alle in dieser Seminarunterlage enthaltenen Programme, Darstellungen und Informationen wurden nach bestem Wissen erstellt und mit Sorgfalt getestet. Dennoch sind Fehler nicht ganz auszuschließen. Aus diesem Grund ist das in der vorliegenden Seminarunterlage enthaltene Material mit keiner Verpflichtung oder Garantie irgendeiner Art verbunden. Der Autor und CertPro Limited übernehmen infolgedessen keine Verantwortung und werden keine daraus folgende Haftung übernehmen, die auf irgendeine Art aus der Benutzung dieses Materials, oder Teilen davon, oder durch Rechtsverletzungen Dritter entsteht.

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in dieser Seminarunterlage berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann verwendet werden dürften.

Die in diesem Dokument aufgeführten Namen tatsächlicher Firmen und Produkte sind möglicherweise Marken der jeweiligen Eigentümer und werden ohne Gewährleistung der freien Verwendbarkeit benutzt.

Dieses Werk ist urheberrechtlich geschützt.
Kein Teil dieses Dokuments darf ohne ausdrückliche schriftliche Erlaubnis für irgendwelche Zwecke vervielfältigt oder in einem Datenempfangssystem gespeichert oder darin eingelesen werden (auch nicht zur Unterrichtsvorbereitung), unabhängig davon, auf welche Art und Weise oder mit welchen Mitteln (elektronisch, mechanisch, durch Fotokopieren, Aufzeichnen, usw.).

Copyright © 2004-2013 CertPro Limited. Alle Rechte vorbehalten.