(Certified)

# Penetration Testing Specialist (PTS)

Schwachstellen erkennen und beseitigen

**NEU!!!**
Workshop inklusive
***deutschsprachigen***
**Workshop-Unterlagen!**

Infobroschüre zum Praxis-Workshop

# (Certified) Penetration Testing Specialist (PTS)

## Hintergründe

Die Anzahl der Angriffe auf Unternehmensdaten aus dem Internet, sowie insbesondere auch aus dem internen Netzwerk nimmt aufgrund der weltweiten, wirtschaftlichen Entwicklungen der letzten Jahre stetig zu. Es ist deshalb umso wichtiger geworden, sich das Wissen anzueignen, um potentielle Schwachstellen im eigenen Umfeld noch vor dem möglichen Angreifer zu entdecken und zu beseitigen. Das hierfür notwendige Wissen vermittelt der in den nächsten Seiten vorgestellte Workshop auf völlig professionelle Weise - und völlig nach dem Motto: ***„Gib Hackern keine Chance!“***

## Dauer

Die Dauer des Workshops beläuft sich auf insgesamt 5 Tage Vollzeit.

## Zielgruppe

Dieser Praxis-Workshop wurde konzeptioniert und entwickelt für:

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

## Lernziele

Die Teilnehmer dieses Workshops erfahren das Wissen und die Fähigkeiten eines professionellen „Penetration Testing Specialist (PTS)“. Nach dem Workshop werden sie in der Lage sein, professionelle Penetrationstests gegen Computersystem und -netzwerke zu planen, vorzubereiten, durchzuführen, auszuwerten und zu dokumentieren. Die hierzu notwendigen Angriffstechniken, sowie die Verwendung entsprechender (Sicherheits-)Tools, Scripts und Methoden werden im Verlauf des Workshops gezielt vermittelt und gegen speziell dazu bereitgestellte Computersysteme angewendet.

## Voraussetzungen

Die Teilnehmer sollten für diesen Workshop die folgenden Voraussetzungen erfüllen:

- Mindestens 12 Monate Praxiserfahrung als Netzwerk- oder Systemadministrator
- Gute Kenntnisse im Umgang mit TCP/IP
- Gute Kenntnisse zu LANs (Local Area Networks) / WANs (Wide Area Networks)
- Umfangreiche Praxiserfahrung in der Installation und Verwaltung von Microsoft-Windows-Betriebssystemen
- Linux-Kenntnisse sind von Vorteil, jedoch nicht erforderlich

# (Certified) Penetration Testing Specialist (PTS)

## Workshop - Themenübersicht

**Modul 00** - Einführung

**Modul 01** - Grundlagen

**Modul 02** - Planung, Organisation und Durchführung von Penetrationstests

**Modul 03** - Planen von Angriffen - Informationen sammeln

**Modul 04** - Scanning - Aufspüren von Servern, Diensten und Anwendungen

**Modul 05** - Enumeration - Erkennen und auswerten

**Modul 06** - Exploitation - Schwachstellen erkennen und ausnutzen

**Modul 07** - Physikalische Angriffe

**Modul 08** - Social Engineering - Feinde unter uns

**Modul 09** - Packet Sniffing - aktives und passives Mitlesen

**Modul 10** - Windows-Hacking

**Modul 11** - Angriffe auf UNIX/Linux

**Modul 12** - Angriffe auf Netzwerkdienste und Datenbankserver

**Modul 13** - Denial of Service - Destruktive Angriffe

**Modul 14** - Angriffe auf Voice-over-IP (VoIP), Fax-Server und Telefonanlagen

**Modul 15** - Viren, Trojaner, Malware und Rootkits

**Modul 16** - Spuren vernichten

**Modul 17** - Firewalls, IDS und Honeypots

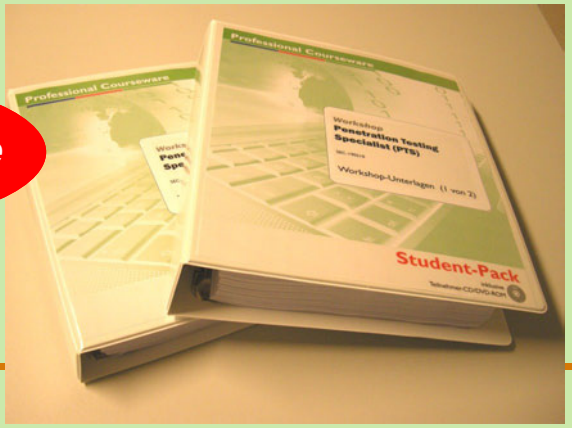
**Modul 18** - Angriffe auf Drahtlosnetzwerke (WLANs)

### Zusatzmodule:

Auf den Kursteilnehmer-DVD-ROMs im „Official STUDENT-Pack“ sind noch weitere Module mit vielfältigen Dokumentationen (zumeist englischsprachig) und (Sicherheits-)Tools zu verschiedenen Themenbereiche (u. a. RFID-, Bluetooth- und USB-Hacking, Spy und AntiSpy, Angriffe auf Mobiltelefone, MacOS-Hacking, Forensic, u.v.m.) enthalten.

Detailliertere Informationen zu den einzelnen Modulen dieses Workshops erhalten Sie in den nächsten Seiten.

NEU!!!
*deutschsprachige*
Workshop-Unterlagen!




# Workshop-Module

## Modul 1:
## Grundlagen

In diesem Modul erhalten die Teilnehmer einen Überblick über die aktuellen Gefahren und Bedrohungspotentiale, die potentiellen Angreifer und auch die möglichen Gründe für Angriffe auf Unternehmensdaten, Computersysteme und -netzwerke. Neben dem Vergleich eines „Hackers“ zum „Penetration Tester“ enthält dieses Modul auch eine Übersicht über die aktuellen „Top-25-Schwachstellen“, die in der Praxis anzutreffen sind. Darüber hinaus wird ihnen ein Überblick über rechtliche Grundlagen und Veränderungen verschafft.

## Modul 2:
## Planung, Organisation und Durchführung von Penetrationstests

Im zweiten Modul des Workshops werden der Zweck und die Arten von Penetrationstests erläutert. Auch vermittelt dieses die notwendigen Informationen zur Planung, sowie der möglichen Vorgehensweise während der Durchführung von Penetrationstests. Umfangreich werden die zu berücksichtigenden allgemeinen und strafrechtlichen Vorschriften und Gesetze aufgezeigt, die einerseits die Unternehmen prinzipiell zur Durchführung von Penetrationstests auffordern, andererseits jedoch auch die „Rahmenbedingungen“ für die Planung und Durchführung der Tests durch den Penetrationstester schaffen. Das Modul enthält viele Anregungen für die notwendige Vertragsgestaltung sowie auch wichtige Informationen zu den organisatorischen, technischen und auch personellen Voraussetzungen für die Planung und Durchführung von Penetrationstests.

## Modul 3:
## Planen von Angriffen - Informationen sammeln

Nach der Einführung in die Planung, Organisation und Durchführung von Penetrationstests geht es nun direkt los mit der Planung von Angriffen. Zuerst werden die möglichen Methoden und Werkzeuge aufgezeigt, die auch von Angreifern zum Sammeln von Informationen über mögliche Opfer genutzt werden. Von der Suche im World Wide Web über „Google-Hacking“, E-Mail-Auswertung, Ermittlung geografischer Daten, WhoIs-Abfragen bis hin zur Routenverfolgung führt dieses Modul bis hin zum oft noch unbekannten „Firewalking“, bei dem ein Angreifer womöglich die vermeintlich sicheren Ressourcen hinter der Unternehmens-Firewall im Internet ermitteln kann. In diesem Zusammenhang werden auch Tipps für mögliche präventive und auch Gegenmaßnahmen vermittelt, die von einem Penetrationtester in der Praxis dann auch an den potentiellen Auftraggeber weitergegeben werden können.

## Modul 4:

# Scanning - Aufspüren von Servern, Diensten und Anwendungen

Nach den bislang zumeist passiven Methoden zur Angriffsvorbereitung werden in diesem Modul die Methoden und Tools aufgezeigt, anhand derer man Computersysteme, Dienste und bestimmte Anwendungen im Internet, sowie auch in lokalen Computernetzwerken auffindet und womöglich auch identifiziert. Das dabei u. a. auch verwendete „Banner-Grabbing“ stellt für bestimmte Dienste, wie Webdienste oder auch FTP-Dienste eine besondere Gefahr dar, weshalb auch die potentiellen Gegenmaßnahmen im Verlauf des Moduls erklärt werden. Um sich selbst gegenüber dem potentiellen Opfer zu verschleiern, verwenden die Angreifer häufig bestimmte Methoden, Tools und Dienste (u. a. auch „open Proxies“ im Internet), die in diesem Modul ebenso vorgestellt werden.

## Modul 5:

# Enumeration - Erkennen und auswerten

In diesem Modul werden die möglichen Methoden und Tools vorgestellt, die ein Angreifer zum Ausspähen von Arbeitsgruppen und Domänen, den Sicherheitsrichtlinien für Benutzerkennwörter, dem Administrator-Konto, Freigaben im Netzwerk sowie vielem mehr zur Verfügung stehen.

## Modul 6:

# Exploitation - Schwachstellen erkennen und ausnutzen

Die zumeist sehr effektive Methode eines Angreifers besteht im Ausnutzen vorhandener Schwachstellen in Betriebssystemen oder Computerprogrammen. In diesem Modul werden die Quellen für die dabei einzusetzenden Exploits, sowie auch kommerzielle und nicht-kommerzielle Exploitation-Frameworks aufgezeigt. Auch werden die aktuellen, kommerziellen und nicht-kommerziellen Schwachstellenscanner (Nessus, ISS Internet Security Scanner u.v.m.) vorgestellt, welche auch seitens eines Penetration Testers für die Schwachstellensuche eingesetzt werden. Letztlich erhalten die Teilnehmer eine Einführung in die Installation und Konfiguration in die Windows Server Update Services (WSUS) von Microsoft, womit sich das Patch-Management in Verbindung mit dem Corporate Software Inspector (CSI) der Firma Secunia unternehmensweit und über die Grenzen der Microsoft-Software hinaus auch für Drittanbieter-Software realisieren lässt.

## Modul 7:

# Physikalische Angriffe

Eine große Gefahr geht von den physikalischen Angriffen auf Computersysteme und Netzwerkkomponenten aus. In diesem Modul werden die Gefahren aufgezeigt, die sich aus dem Zurücksetzen von BIOS-Kennwörtern, dem Ausspähen von Anmeldedaten durch Keylogger und ähnlichen Methoden ableiten lassen.

## Modul 8:

# Social Engineering - Feinde unter uns

Das „Social Engineering“ wirklich überhaupt nichts mit dem allgemeinen, sozialen Verständnis zu tun hat, wird in diesem Modul anhand verschiedener Angriffstechniken mittels Shoulder Surfing, Dumpster Diving, Phishing, Pharming und auch Spamming klar verdeutlicht.

## Modul 9:

# Packet Sniffing - aktives und passives Mitlesen

Viele Administratoren wähnen sich teils bereits aufgrund von MAC-Filtern auf den im Netzwerk eingesetzten, aktiv verwalteten Switches gegenüber Man-in-the-Middle-Attacken als vermeintlich „sicher“. Eines „Besseren“ belehren die in diesem Modul eingesetzten, vielzähligen Tools, Programme und Methoden, die ein Angreifer oft problemlos - und trotz bestimmter Sicherheitsmechanismen - für aktive und auch passive Sniffing-Attacken einsetzen kann. Die Teilnehmer erfahren auch mögliche Methoden und Tools, um mit hoher Wahrscheinlichkeit selbst passive Angriffe im Netzwerk zu erkennen.

## Modul 10:

# Windows-Hacking

Die Authentifizierung anhand von Benutzerkennwörtern stellt insgesamt ein hohes Risiko für die Unternehmensdaten dar. In diesem Modul werden die verschiedenen Authentifizierungsprotokolle, sowie die damit verbundenen Gefahren anhand verschiedener Beispiele, sowie auch bestimmter Tools, Programmen und Methoden verdeutlicht. Selbst der Angriff auf das Kerberos-Protokoll wird innerhalb dieses Moduls gezeigt. Auch wird erklärt, wie es ein Angreifer mitunter schafft, Daten innerhalb des Dateisystems von Festplatten unter den aktuellen Windows-Betriebssystemen so zu verstecken, dass ein Administrator diese ohne begründeten Verdacht nicht vermuten und somit auch nicht aufspüren kann.

## Modul 11:

# UNIX/Linux-Hacking

Dieses Modul zeigt die Gefahren auf, die seitens diverser Methoden, Tools und Programmen auch den UNIX- und Linux-basierten Computersystemen im Internet sowie auch in lokalen Computernetzwerken drohen. Auch werden einige Tipps aufgezeigt, wie man zum Beispiel das Ausspähen von Benutzern u. ä. unter UNIX/Linux verhindern kann.

GFILANguard

## Modul 12:
# Angriffe auf Netzwerkdienste und Datenbank-server

Angriffe auf Webserver, oft in Form sogenannter „Website-Defacements“, finden zumeist direkt aus dem Internet auf die vielen zig-millionen Websysteme weltweit statt. In diesem Modul werden die Gefahren, sowie auch die für Angriffe einzusetzenden Tools, Programme, Scripts und Methoden erklärt. Auch finden Angreifer immer häufiger die direkt aus dem Internet erreichbaren Terminalserver, oft auf der Basis von Windows oder Citrix, als potentiellen „Einstieg“ in die Computernetzwerke von Unternehmen vor. Oft setzen Unternehmen auch RAS-/VPN-Gateways für den Remote-Zugriff auf die Unternehmensnetzwerke durch Außendienstmitarbeiter und Home-Offices ein. Auch hier tun sich Angriffsflächen auf, die von potentiellen Angreifern durch den Einsatz bestimmter Tools mitunter ausgenutzt werden können. Letztlich befasst sich dieses Modul mit den möglichen Methoden und Tools für Angriffe auf Datenbankserver, wie die Microsoft SQL-Server. Neben möglichen Kennwort-Attacken wird u. a. auch aufgezeigt, wie Angreifer die Anfälligkeit für „SQL-Injection“-Angriffe auf Datenbankserver erkennen und ausnutzen können.

## Modul 13:
# Denial of Service - Destruktive Angriffe

Als Penetration Tester muss man sich auch mit den Tools und Methoden für die Durchführung von Denial of Services (DoS)-Attacken befassen. Auch muss man die Funktionsweise von Bot-Netzen (Botnets), sowie die damit verbundenen Gefahren kennen. Dies wird in diesem Modul veranschaulicht.

## Modul 14:
# Angriffe auf Voice-over-IP (VoIP), Fax-Server und Telefonanlagen

In modern ausgerichteten Unternehmen findet die Telekommunikation zwischenzeitlich häufig mittels Voice-over-IP statt. Oft findet man die dabei genutzten Geräte gleich innerhalb der Infrastruktur des eigentlich parallel vorhandenen Computernetzwerkes, so dass es einem Angreifer ermöglicht wird, die durchgeführten Telefonate digital aufzuzeichnen, ohne dass die Betroffenen davon Notiz nehmen können. Neben den Grundlagen zu Protokollen und möglichen Einsatzszenarien werden in diesem Modul auch mögliche Bedrohungen und auch Angriffe auf Voice-over-IP verdeutlicht. Das Modul enthält ebenso Tipps für die Implementierung einer sicheren VoIP-Infrastruktur.

## Modul 15:
# Viren, Trojaner, Malware und Rootkits

Die weltweiten, aktuellen Statistiken zeigen stetig ansteigende Gefahren durch Viren, Würmer und Trojaner. Diese werden immer häufiger für Angriffe auf Computersysteme in Unternehmensnetzwerken verwendet. In diesem Modul wird erklärt, wie man sich präventiv verhalten sollte, um mögliche Infektionen zu vermeiden. U. a. werden auch Tools und Methoden vorgestellt, anhand derer man Trojaner und Backdoors womöglich aufspüren kann.

## Modul 16:

# Spuren vernichten

Angreifer versuchen häufig, die möglichen Spuren eines Hack-Angriffs zu verschleiern. Eine gängige Methode ist es, die möglichen Einträge in Ereignisprotokollen ins Visier zu nehmen und zu löschen. Die dabei eingesetzten Tools und Methoden der Angreifer, sowie auch mögliche Abwehrmaßnahmen in Form von bestimmten Unternehmenslösungen (wie z. B. Tripwire) werden in diesem Modul aufgezeigt.

## Modul 17:

# Firewalls, IDS und Honeypots

In diesem Modul werden die verschiedenen Einsatzkonzepte für Firewalls mitsamt ratsamer Erweiterungsmöglichkeiten erklärt, um die Unternehmensressourcen vor Angreifern aus dem Internet schützen zu können. Als erweiterte Sicherheitsvariante werden Intrusion Detection-Systeme (IDS), sowie auch der Verwendungszweck und möglicher Einsatzort von Honeypots, sowie auch die Methoden und Tools der Angreifer zum Aufspüren - insbesondere der letzteren - erklärt.

## Modul 18:

# Angriffe auf Drahtlosnetzwerke (WLANs)

Dieses Modul rundet den Workshop letztlich ab - und zeigt die aktuellen, potentiellen Gefahren für Drahtlosnetzwerke (WLANs) mitsamt der Methoden und Tools der Angreifer unverblümt auf. Nicht nur die Verschlüsselungsmethoden, wie WEP, WPA oder WPA2, sind den Angriffen durch Hacker ausgesetzt. Auch die in Infrastrukturnetzwerken eingesetzten Access Points sind mitunter ein lohnendes Ziel für potentielle Angreifer. In diesem Modul erhalten die Teilnehmer einen umfangreichen Überblick über die einsetzbaren Sicherheitsmechanismen in WLANs, sowie auch Tipps zum Einrichten und Betreiben von „sicheren“ Drahtlosnetzwerken.

Die Inhalte werden veranschaulicht dargestellt. Die Trainer setzen dabei neben einheitlich aufbereiteten, standardisierten PowerPoint-Folien noch weitere Medien wie Videos, Demos usw. ein. Für die praktische Durchführung von Laborübungen stehen entsprechend vorbereitete Computersysteme bereit.

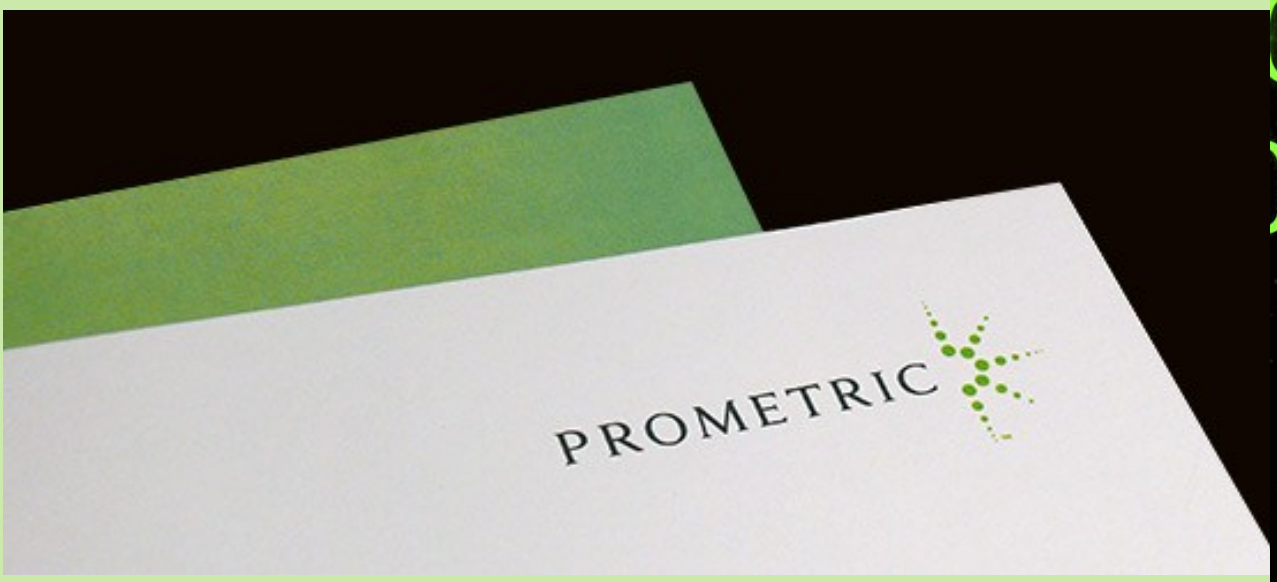
# (Certified) Penetration Testing Specialist (PTS)

## Workshop-Unterlagen / Material:

Das im Workshop eingesetzte *STUDENT-Pack* für die Workshop-Teilnehmer umfasst:

- **Workshop-Unterlage** (ca. 800 Seiten), DinA4 im Präsentationsordner (komplett deutschsprachig)
- **Zusatzdokumentation** (ca. 300 Seiten), DinA4 im Präsentationsordner (teilw. englischsprachig)
- **4 Kursteilnehmer-DVD-ROMs**
  (Sicherheitstools und -programme, Dokumentationen, Scripts, Videos, Demos, usw.)
- Offizielles **Prüfungsvorbereitungsbuch** für (*optionale*) CEH-Prüfung
- **802.11n-Wireless LAN USB-Adapter**

**NEU!!!**
***deutschsprachige***
**Workshop-Unterlagen!**




## Prüfungsmöglichkeit / Zertifizierung:

Der Inhalte des Workshops bereiten in weiten Teilen bereits auf die mögliche Teilnahme an den folgenden, weltweit anerkannten Zertifizierungsprüfungen vor:

*„Certified Penetration Testing Engineer (CPTE)“*
(Mile2 Security, USA)

*„Certified Ethical Hacker (CEH)“*
(EC-Council)

Die jeweilige Prüfung kann im Anschluss an den Workshop - ***optional*** - in einem der weltweit angesiedelten Testingcenter von Prometric (CEH-Prüfung - weitere Infos unter: **http://www.eccouncil.com**) bzw. direkt über das Webportal von Mile2 Security (CPTE-Prüfung - weitere Infos unter: **http://www.mile2.com**) abgelegt werden.

Die anfallenden Kosten für die Prüfung sind im Kurspreis ***nicht*** enthalten.

Nach dem Ablegen der Prüfung zum ***„Certified Ethical Hacker“ (CEH)*** bietet beispielsweise EC-Council noch weitere, vertiefende Zertifizierungsworkshops und Prüfungen an. Weitere Informationen hierzu finden Sie im Internet u. a. unter:

**http://www.eccouncil.com**

Weitere Informationen erhalten Sie von:

Copyright © 2004-2010 CertPro Limited. Alle Rechte vorbehalten. Irrtümer und Druckfehler ausgeschlossen. Kein Teil dieser Broschüre darf ohne ausdrückliche schriftliche Erlaubnis für irgendwelche Zwecke vervielfältigt oder in einem Datenverarbeitungssystem gespeichert oder darin eingelesen werden , unabhängig davon, auf welche Art und Weise oder mit welchem Mittel (elektronisch, mechanisch, durch Fotokopieren, Aufzeichnen usw.). 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. Die in dieser Broschüre enthaltenen Abbildungen sind lizenziert bei Fotolia.de.