

Anmeldung

Hiermit melde ich mich verbindlich an:

- 08.02.2012 (Tag 1)
 08.-10.02.2012 (Tag 1-3)

Firma:

Vor-/Nachname:

Funktion:

Straße/Nr:

PLZ/Ort:

Telefon:

E-Mail:

Unterschrift:

Ich habe zur Kenntnis genommen, dass für die Teilnahme an der Veranstaltung ein Betrag von **649,- € (Tag 1) bzw. 1225,-€ (Tag 1-3)** vorab zu entrichten ist. Außerdem ist mir bekannt, dass eine Abmeldung bis spätestens 7 Tage vor Veranstaltung möglich ist. Alternativ kann auch ein Vertreter geschickt werden. Bei Nichtteilnahme wird die Seminargebühr fällig.

Bitte Anmeldung faxen an: 02364 10538-29
Alternativ: Anmeldung unter www.puw-netzwerk.de

Veranstaltungsort

Hotel Seehof

Hullerner Straße 102
45721 Haltern am See, Südufer

Tel: 023 64/928-0
E-Mail info@hotel-seehof.de
www.wellness-hotel-seehof.de

Seien Sie heute auf die Gefahren von morgen vorbereitet.

Wir bieten Ihnen:

- Security-Checks
- Penetrationstests
- Sicherheitsberatung
- Firewall-Beratung und -Installation
- Netzwerk Access Control
- Festplattenverschlüsselung
- Moderne Anti-Virensoftware
- One-Time-Password-Schutz
- Netzwerk-Überwachung
- Monitoring
- WLAN-Check
- ... und vieles mehr.

Lassen Sie sich unverbindlich von unseren Experten beraten.

Kontakt

P&W Netzwerk GmbH & Co. KG

Bergenfahrerstraße 23
45721 Haltern am See
Tel.: 0 23 64 / 105 38 0
Fax: 0 23 64 / 105 38 29

info@puw-netzwerk.de

HACKING SEMINAR



Einführung



Liebe Kunden und Geschäftspartner,

Lernen Sie Ihren Feind kennen.

Mit diesem Seminar erhalten Sie einen Einblick in die Methoden und Tools der Hacker. Sie können Angriffe auf Ihre IT-Infrastruktur, Ihre Server und Applikationen

erkennen und zur Beweissicherung dokumentieren. Sie wissen, wie Sie Schutzmaßnahmen ergreifen, die Einbrüche verhindern und Angriffe erschweren. Angefangen mit der Informationsbeschaffung über Scannen der Systeme, Eindringen in Server einer DMZ bis zur Erlangung von Root-Rechten und Installation einer Hintertür werden alle Themen behandelt.

Preparing the attack - Hacking Networks

Unser Dozent führt selbst regelmäßig Sicherheitsprüfungen in Unternehmen durch und gibt Ihnen eigene Praxiserfahrungen sowie Insider-Wissen aus der aktuellen Hacker-Szene weiter.

Probieren Sie sich selbst als Hacker und führen Sie Live-Angriffe gegen Netzwerk-Komponenten durch.

Zielgruppe

System-/Netzwerk-Administratoren, IT-Sicherheitsbeauftragte und IT-Manager, die Security-Risiken aus der Sicht des Angreifers betrachten und dadurch effiziente Lösungsszenarien aufbauen möchten um ihr Unternehmen besser vor Angriffsszenarien schützen zu können.

Ulrich Puschmann,
Geschäftsführer P&W

Grundlagen/Schadprogramme 08. Februar 2012

- Wer sind die Angreifer?
- Strafrechtliche Bewertung von Angriffen (inkl. § 202c)
- Gängige Sicherheitslücken und Schwachstellen
- Buffer Overflows (Ursachen und Funktionsweise)
- Vorgehensweise von Angreifern (Hacking Cycle)
- Brute Force Methoden (Passwort Cracking)
- Viren & Trojaner
- Client-Side Exploits
- Rootkits zum Spuren verwischen

Windows-Hacking 09. Februar 2012

- Port-Scanning und Fingerprinting mit Nmap und SuperScan
- Vulnerability Scanning mit Nessus
- Auswertung von Scans und dienstspezifischer Informationen
- Enumeration von Benutzern und Diensten
- Exploitsnutzung zur Kompromittierung von Windows Systemen
- Exploit-Frameworks (Metasploit, ATK)
- NetBIOS-Schwachstellen (Exploits, IPC, Admin Shares)
- Ausnutzung fehlkonfigurierter Dienste und Anwendungen
- IIS-spezifische Schwachstellen und Schutz vor Angriffen

Netzwerk-Hacking 10. Februar 2012

- Sniffing und ARP-Spoofing
- Abhören von Passwörtern mit Cain&Abel
- Man-in-the-Middle-Angriffe
- Sicherheitsanalyse von Webanwendungen
- Vertrauliche Daten in Suchmaschinen (Google-Hacking)
- Informationsbeschaffung mit öffentlich zugänglichen Mitteln
- Angriffe gegen Netzwerkkomponenten
- WLAN-Hacking

Informationen

Gerne erstellen wir Ihnen ein individuelles Angebot für einen externen Penetrationstest, Web Applikation Sicherheitstest, Compliance Scan u.v.m. in Ihrem Unternehmen.

Dozentenprofil

Der Dozent ist zertifizierter CISSP (ISC²), und CEH (EC-Council) und beschäftigt sich seit über 15 Jahren mit Sicherheitsanalysen und der Aufdeckung von Schwachstellen verschiedenster Systeme.

Voraussetzungen

Gute Kenntnisse in der Administration von Windows- oder Linux-Systemen, sowie der Funktionsweisen der Internet-Kommunikationsprotokolle (TCP/IP) sind von Vorteil. Vor Ihrer Teilnahme an diesem Kurs müssen Sie sich schriftlich dazu verpflichten, die neu erworbenen Fähigkeiten nicht für rechtswidrige oder böswillige Angriffe zu verwenden, die Tools nicht zur Schädigung von Computersystemen einzusetzen und die CBT für den (beabsichtigten oder unbeabsichtigten) Missbrauch dieser Tools zu entschädigen.

Partner

2011 Preferred Partner

