

Die Anmeldung bitte per Fax an 02353-70889170  
oder per E-Mail an [p.herzog@escha.de](mailto:p.herzog@escha.de) schicken.

Workshop Hacking Advanced  
Anmeldung für Termin: \_\_\_\_ 01.-03.12.2015 in 58553 Halver

Teilnehmer: \_\_\_\_\_

E-Mail-Adresse: \_\_\_\_\_

Firma: \_\_\_\_\_

Kosten 2.290,00 € incl. Mittagessen, zzgl. MwSt (Sonderpreise)  
Jeder Teilnehmer erhält einen Notebook mit allen wichtigen Tools  
Diesen Notebook darf man dann für die spätere Arbeit behalten

Für Mitglieder der Geschäftsführung besteht am Montag, den  
30.11.2015 ab 14.00 Uhr an einem „Gefahren-Erkennungs-  
Workshop“ teilzunehmen. Besteht an diesem Angebot Interesse?  
JA / NEIN

In dem Praxis Workshop HACKING [advanced] zeigen wir Ihnen die Techniken,  
Vorgehensweisen und Tools die Hacker verwenden um sich Zugriff auf Ihre Systeme zu  
verschaffen.

Nur wer die aktuellsten Angriffstechniken kennt – weiß um die richtigen Gegenmaßnahmen!  
Lernen Sie Sich gegen diese Angriffe zu schützen indem Sie die Techniken und Tools selbst in  
unserer Workshop Umgebung erlernen und in der Praxis anwenden. Wir zeigen Ihnen „Das  
Handwerkzeug um ihren aktuellen Security Standard selbstständig zu überprüfen“

[Tag 1]

**Footprinting:** Welche Informationen sind im Netz öffentlich verfügbar

Praxis: Wir durchsuchen das Internet nach Informationen zu Ihrer Firma – Wo sind Sie  
angreifbar?

Hacking Tools für den Praxiseinsatz Kali 2.0 und Co.

Praxis: Sie identifizieren interessante Angriffsziele in unserem Hacking Lab

LAW rechtliche Rahmenbedingungen – Hackerparagraph

**Port Scanning** Zielsysteme finden

Google Hacking

Praxis: Hacking mittels Google live im Internet

WLAN HACKING -WEP, WPA oder WPA2

Praxis : Sie hacken WEP und WPA2 gesicherte WLAN Netzwerke

**Exploits** Funktionsweise und Gefahren

Praxis: Sie legen einen administrativen User auf einem Windows System an. Sie hacken die  
Admin Oberfläche einer Website

[Tag 2]

**Mobile Security** – Hacking Blackberry, iPhone & Co

Angriff auf Virtuelle Server

**Man in the Middle Attacken**

Sniffen auch im geschwichteten Netzwerk

Praxis: Sie leiten den Traffic eines anderen PCs über Ihren PC um – Sie können Passwörter mitlesen!

**DNS-Hacking**

Praxis: Sie leiten die Website microso\*.com auf linux.org um

**VPN-Hacking** So (un)sicher ist VPN

Praxis: Wir prüfen Ihr VPN Gateway auf Angreifbarkeit und zeigen wie man VPN Client Verbindungen hackt und somit das Domain Passwort rausfindet!

**SSL Hacking** Verbindungen abhören und verändern

Praxis: Sie fangen das Passwort einer gesicherten Verbindung mit https://www.paypa\*.com oder Ihrer https:// gesicherten Website ab.

**Website Hacking** (SQL Injection, XSS,..)

Praxis: Wir suchen im WEB nach tagesaktuellen Cross Site Scripting anfälligen Websites // Wir prüfen auf SQL Injection Möglichkeiten //

**Tunneling Firewalls** und Proxies umgehen

Praxis: Wir brechen mittels DNS aus einem gesicherten Netzwerk aus – sog. Calling Home bzw. Backchannel

[Tag 3]

**VOIP – abhören** und absichern

Praxis: Sie hören Telefongespräche zwischen VOIP Apparaten und VOIP Telefonanlage ab.

**Passwort Hacking**

Praxis: Sie hacken Windows Passwörter mittels Rainbow Tables und entschlüsseln Website Passwörter

**Biometrie** – Fingerabdruck fälschen

Praxis: Mittels eines gefälschten Fingerabdrucks melden Sie sich an einem Windows System an.

**Penetration Testing** – Security Audits im eigenen Unternehmen

**Forensik** – Hacker aufspüren

Capture the flag Contest – mit dem gesammelten Wissen aus dem Kurs hacken Sie ein System