



Hacking Techniques

Black Hats vs. **White Hats**

IT-Security: Der Schutz unserer Systeme vor bösartigen Hacker-Angriffen!

Zu lange hatte man aus ethischen Gründen ignoriert, dass sich nur derjenige ausreichend schützen kann, der die Angriffstechniken seiner Feinde kennt. Die Feinde, das sind die **Black Hats**, die **kriminellen Hacker**, die Anonymität und Sicherheit auf unseren Computersystemen aushöhlen möchten - aus Habgier, Zerstörungswut oder dem reinen Wunsch nach Macht! Ihnen gegenüber agiert die Fraktion der **IT-Sicherheits-Spezialisten**, der **White Hats**, deren Ziel die möglichst umfassende technische Immunität der Computersysteme vor den Angriffen der Black Hats ist. Erst seit die unedlen Methoden der **bösen Hacker** Einzug in Literatur und Lehre finden durften, können ihnen die **guten Hacker** zunehmend wieder auf Augenhöhe begegnen. **IT-Security** wird durch das Wissen der Black Hats erst möglich.

Wie gehen Black Hats vor? Und wie wehren White Hats ihre Angriffe ab?

Das ist das Thema dieses Kurses für bereits PC-feste Teilnehmer ab ca. 12 Jahren.

Wir fahren reale Angriffe auf ein separiertes Rechnersystem, agieren wie Black Hats und lernen dabei, wie man sich als White Hat schützen kann. Dabei decken wir eine große Bandbreite von **Angriffszielen** und **Angriffs-Verteidigungs-Szenarien** ab.

Unsere Themen:

Exploits - IPv6 - Kali Linux - Metasploitable - Hacking Tools (u.a. Whireshark) - BIOS/EFI - Verschlüsselung - Passwort Hacking - Multi-Faktor-Authentifizierung - WLAN - Bluetooth - SDR (Software Defined Radio) - USB-Schnittstelle - Externe und interne Sicherheitsprüfungen - Penetration Testing - Netzwerke - Windows Server - Active Directory - Linux Absicherung - Samba Fileserver - Webanwendungen - Software Exploitation - Cloud Sicherheit - Office 365 - Mobile Security (Smartphone) - IoT (Internet of Things)

Kursleiter: *Dipl.-Ing. Thomas Krämer*