

# Workshop Praktische IT-Security: Hackertechniken beherrschen I

(früher: Hackerfähigkeiten für System-Administratoren I)

Computermisbrauch und Cyber-Kriminalität bedrohen IT-Netze tagtäglich. Meist geschehen sie sehr unauffällig und werden erst bemerkt, wenn der Schadensfall schon eingetreten ist. Somit sind sie eine ernstzunehmende Bedrohung.

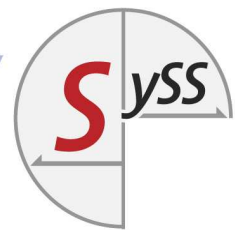
Damit Unternehmen ihre IT-Umgebung vor Gefahren dieser Art wappnen und schützen können, haben wir diesen Workshop entwickelt, in dem wir das Thema IT-Sicherheit aus der Perspektive eines Täters bzw. „Hackers“ betrachten.

Der Workshop ist in zwei Teile gegliedert, die zwar aufeinander aufbauen, jedoch auch gesondert besucht werden können.

## Inhalt von Teil I:

- **Informationsquellen:** Wie verraten sich angreifbare und verwundbare Systeme?
- **Standard-Sicherheitswerkzeuge und ihr Einsatz (Portscanner, Sniffer)**
- **Man-in-the-Middle-Angriffe:** Vor allem in lokalen Netzen können MitM-Angriffe verwendet werden, um verschlüsselten Verkehr oder auch Telefonate mitzulesen, bzw. zu hören. Durchführung von Angriffsszenarien, Besprechung von Schutzmechanismen.
- **Passwortsicherheit unter LINUX, WINDOWS und in WINDOWS-Netzen:** Anhand von verschiedenen Cracking-Techniken schätzen wir die Sicherheit ein, welche eine Passwort-Policy bietet.
- **Sicherheitslücken im Netz:** Ausnutzung, Eskalierung von Rechten – dies bietet Aufschluss über die Wirksamkeit von Schutzmechanismen.

Zielgruppe:	Administratoren, Sicherheitsspezialisten, IT-Sicherheitsbeauftragte, alle an tieferen Einblicken in IT-Sicherheit aus technischer Perspektive Interessierten
Erforderliche Vorkenntnisse	Grundkenntnisse über Betriebssysteme und Netzwerke, Grundkenntnisse in LINUX und WINDOWS, Grundkenntnisse TCP/IP
Dauer:	2 Tage



Teilnehmerzahl:	8-12
-----------------	------