



Kursabstract für Kurs LAB-NP Networking & Penetration Testing

Subject	Beschrieb
Kursdauer	2 Tage
Zielgruppe	<ul style="list-style-type: none">✦ Security Officers✦ Netzwerk-Administratoren/Engineers✦ Unix-/Windows-Administratoren✦ Firewall-Administratoren/Engineers
Voraussetzung	<ul style="list-style-type: none">✦ Security Officers✦ Netzwerk-Administratoren/Engineers✦ Unix-/Windows-Administratoren✦ Firewall-Administratoren/Engineers
Inhalt	<ul style="list-style-type: none">✦ Information Gathering (Google, Website, WHOIS)✦ Port Scanning, Vulnerability Scanning, Exploitation✦ OSSTMM Prozess Beschreibung für Penetration Tests✦ Sniffing, ARP Spoofing✦ VLAN Hacking, Port Security✦ Tunneling Mechanisms (HTTP Tunnel, DNS Tunnel)✦ Voice over IP Attack✦ Hands-On mit Nessus, Metasploit, Nmap etc.
Lernziel	Die Teilnehmer kennen die Gefahren von Netzwerk-Attacken. Sie können ihr Unternehmen selbständig auf Schwachstellen überprüfen und die entsprechenden Gegenmassnahmen einleiten und anwenden.
Abgrenzung	Dieser Kurs behandelt vorwiegend Angriffe auf Netzwerk- und Systemebene. Die Angriffe auf Web Applikationen werden in den Kursen LAB-WAB und LAB-WAA geschult.