Basic Penetration Tester («BASPEN»)

Der Basic Penetration Tester ist der ideale Einstieg in das vielschichtige Thema der offensiven Cyber-Security-Strategie. Nach Abschluss haben Sie eine von zwei Trainingsreihen bis hin zum Rollenzertifikat «Professional Penetration Tester» erreicht.

Dauer: 5 Tage
Preis: 4'525.– zzgl. 8.1% MWST
Kursdokumente: Digitale Kursunterlagen
Herstellercode: OPST

Inhalt

Unsere komplette Trainingssreihe «Penetration Testing» besteht aus 12 Tagen und ist in zwei Kompetenzstufen «Basic Penetration Tester und Advanced Penetration Tester» unterteilt. Mit dem Abschluss beider Stufen erhalten Sie das Digicomp-Rollenzertifikat «**Professional Penetration Tester**». Mit dem Rollenzertifikat sind Sie in der Lage, die Geschäfts- und IT-Leitung dabei zu unterstützen, Schwachstellen innerhalb der Unternehmensumgebung zu identifizieren sowie potenzielle Bedrohungen und Angriffe auf private und geschäftliche Netzwerke, Systeme und sensible Geschäftsinformationen frühzeitig zu erkennen. Die zusammengestellte zweistufige Kursabfolge ist der perfekte Start in die Welt des Penetration Testings und somit die perfekte Grundlage für effektive Abwehr- und Verteidigungsstrategien.

Kursinhalt Basic Penetration Tester:

Cyber Security Tester – Foundation (Hands-on) – 1 Tag

Anhand eines im LAB durchgeführten Hacking-Angriffs mit den entsprechenden Tools lernen Sie Schritt für Schritt, wie Sie Ihre eigenen Netzwerke absichern können.

- Einführung in die Sicherheitsproblematik und das Hacking-LAB
- Arbeitsweise, Techniken und Tools der Hacker
- Ablauf eines gezielten Hackerangriffs
- Open Source Intelligence & Social Engineering
- Netzwerk-Sniffing, -Scanning und Spoofing
- Passwörter abfangen und Passwörter knacken
- Getarnte Malware und gezielte Exploits einsetzen
- Zugriff mittels eines Backdoors sichern
- Allgemeine Abwehrmassnahmen der im Hacking-LAB gezeigten Szenarien

Cyber Security Tester – Professional (Hands-on) – 2 Tage

Im Kurs wird mit KALI LINUX™ und verschiedenen Erweiterungen gearbeitet. Für alle Teilnehmenden steht eine entsprechende Lab-Umgebung für die Hands-on-Übungen bereit.

- Grundlagen und Aufbau eines eigenen Hacking-Labs
- Nützliche Bash-Befehle in Linux
- Gezieltes Auskundschaften / Footprinting / Bannergrabbing
- Network-Sniffing-Techniken (inkl. passives WLAN Scanning)
- Network-Scanning-Techniken gezielt einsetzen (aktiv und passiv)
- Schwachstellen-Scanning durchführen
- Verschiedene Man-in-the-Middle-Angriffe durchführen (ARP-Poisoning, SSLStrip, usw.)
- Wireless-Angriffe durchführen (WEP, WPA2, WPS, DoS, usw.)
- Gefahren von Evil Twin WLAN-Angriffen verstehen
- Einführung ins MetasploitTM Framework (msfconsole, modules, payloads, auxiliary)
- Exploit-Auswahl für verschiedene Client-Side-Attacken

- Post-Exploitation durchführen (Zusatzmodule, Rechte-Eskalation, Pivoting, Festsetzen, usw.)
- Gefahren von Antivirus- und Firewall-Evasion-Techniken verstehen
- Advanced Threats Live-Demo (HID- und Bad-USB-Attacken)

* KALI LINUX™ is a trademark of Offensive Security.
* Metasploit™ is a tademark of Rapid7 LLC.

Web Application Security – Foundation – 2 Tage

Auf Basis der OWASP Top 10 lernen Sie die aktuellen Angriffsmethoden auf (Web)-Applikationen kennen und lernen, wie wirkungsvolle Schutzmassnahmen ergriffen werden:

- A01:2021-Broken Access Control
- A02:2021-Cryptographic Failures
- A03:2021-Injection
- A04:2021-Insecure Design
- A05:2021-Security Misconfiguration
- A06:2021-Vulnerable and Outdated Components
- A07:2021-Identification and Authentication Failures
- A08:2021-Software and Data Integrity Failures
- A09:2021-Security Logging and Monitoring Failures
- A10:2021-Server-Side Request Forgery

Prüfung zu Basic Penetration Tester – 1 Stunde

Sie schliessen die Basic Penetration Tester Kursreihe mit einer einstündigen Abschlussprüfung ab. Mehr Infos erhalten Sie unter der Sparte «Zertifizierung».

Key Learnings

- Kennen der rudimentären Techniken und Vorgehensweisen der Hacker
- Erklären der Grundsätze des ethischen Hackings
- Kennen der Sicherheitsprobleme von Servern und Clientsystemen
- Erkennen und Verhindern der wichtigsten Bedrohungen aus dem Internet
- Anwenden der wichtigsten Hackingtools und Einschätzen der Gefahren, die davon ausgehen
- Prüfen der eigenen Sicherheit in Testumgebungen (Hacking-Labs) dank Ihrer Ethical-Hacking-Fähigkeiten
- Einbeziehen von offensiven Erkenntnissen in Cyber-Security-Strategien
- Kenntnisse über verschiedene Angriffe auf Webapplikationen (inkl. dahinterliegende Datenbanken und Backends), die Sie anschliessend selbst ausführen
- Verständnis über die Grundzüge der sicheren Softwareentwicklung
- Auseinandersetzung mit verschiedenen potenziellen Gefährdungsszenarien

Methodik & Didaktik

Diese Trainingseinheit beinhaltet aktive Lehrgespräche mit den Teilnehmenden, Reflexion und Austausch von Erfahrungen aus der eigenen Praxis im Kontext der Theorie und angeleitete Übungen in einer Hands-On Laborumgebung.

Zielpublikum

Zukünftige Penetration Tester, IT-Fachleute, Führungskräfte, IT Sicherheitsberater und -beauftragte, System- und Netzwerkadministratoren, Softwareentwickler und Webmaster sowie Sytemingenieure und Netzwerkplaner.

Zertifizierung

Obligatorische Abschlussprüfung

Sie schliessen die Basic-Penetration-Tester-Kursreihe mit einer einstündigen Abschlussprüfung ab, in der Sie belegen, dass Sie die erlernten Kursinhalte verstanden haben und umsetzen können. Die Prüfungskosten in der Höhe von CHF 200 sind nicht im Kurspreis inbegriffen. Sie können die Prüfung an einem beliebigen Datum und Uhrzeit (Mo bis Fr,Uhr) in einem unserer Testcenter in Zürich, Bern oder Basel ablegen. Sie haben die Prüfung bestanden, wenn Sie 60% der Fragen richtig beantworten. Sie erhalten das Prüfungsergebnis innerhalb einer Woche. Um sich für die Prüfung anzumelden, kontaktieren Sie bitte unsere Kundenberater unteroder info@digicomp.ch.

Wiederholung

Sie können die Prüfung maximal einmal wiederholen. Die Prüfungskosten fallen bei der Wiederholung weg. Kontaktieren Sie unsere Kundenberater über info@digicomp.ch.

Zertifikat

Nach bestandener Prüfung können Sie direkt in die abschliessende Kursreihe «Advanced Penetration Tester» einsteigen. Ab hier sind Sie dem Digicomp-Rollenzertifikat «Professional Penetration Tester» einen Schritt näher.

Zusatzinfo

Mögliche Prüfungsvorbereitungen

(Die Prüfungsgebühren sind nicht im Kurspreis inbegriffen)

Certified Ethical Hacker - EXIN

Diese erste Kursreihe bereitet Sie auf die internationale Zertifizierung Certified Ethical Hacker - EXIN vor. Sie bescheinigt Ihre Anti-Hacking-Fähigkeiten. Für die Prüfungsteilnahme empfehlen wir eine administrative Vorbereitungszeit von zwei Wochen und folgende Prüfungsfragen, für eine optimale Vorbereitung, durchzuspielen.

CompTIA Pentest+

Diese erste Kursreihe bereitet Sie auf die internationale Zertifizierung CompTIA Pentest+ vor. Das Zertifikat entspricht den IS 17024-Standards und ist einzigartig. Für die Prüfungsteilnahme empfehlen wir eine administrative Vorbereitungszeit von zwei Wochen und folgende Prüfungsfragen, für eine optimale Vorbereitung, durchzuspielen.

Empfohlen ist eine Comptia Security+ Zertifizierung.

Weiterführende Kurse

- Advanced Penetration Tester («ADVPEN»)

Haben Sie Fragen oder möchten Sie einen Firmenkurs buchen?

Wir beraten Sie gerne unter 044 447 21 21 oder info@digicomp.ch. Detaillierte Infos zu den Terminen finden Sie unter www.digicomp.ch/weiterbildung-security/cyber-security-offense/kurspaket-basic-penetration-tester