Advanced Penetration Tester («ADVPEN»)

Der Advanced Penetration Tester ist eine vertiefende Kursreihe. Sie werden optimal auf die Prüfung «Certified OSSTMM Professional Security Tester» vorbereitet und sind dem Rollenzertifikat «Professional Penetration Tester» einen Schritt näher.

Dauer: 8 Tage
Preis: 9'300.– zzgl. 8.1% MWST
Kursdokumente: Digitale Kursunterlagen
Herstellercode: OPST

Inhalt

Unsere komplette Trainingsreihe «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 Advanced Penetration Tester:

Cyber Security Tester – Hands-on Advanced, 2 Tage

Im Kurs arbeiten wir mit KALI LINUX™ und verschiedenen Erweiterungen. Dabei ergänzen und vertiefen Sie die bereits gelernten Techniken aus den Vorgängerkursen. Für alle Teilnehmenden steht eine entsprechende Lab-Umgebung für die Hands-on-Übungen bereit.

- Erweitern der eigenen Hacking-Labs aus dem Kurs «Ethical-Hacking-Hands-on-Vertiefung (HAK2)»
- Vertiefung der im HAK2-Kurs erlernten Techniken mit weiteren Hands-on-Labs
- Eigene Kreativität beim Ethical-Hacking mit gezielter Kombination von Hacking-Techniken fördern
- Vertiefung von MitM-Techniken (z.B. HSTS-Umgehung, Code Injection, Keyloggers, DNS-Spoofing)
- Gezielte Advanced-Backdoor-Methoden mit Evasion-Techniken mittels Fake Updates, manipulierten Dateien, Einbetten in Programme, Makros)
- Gezielt Systemrechte erwirken (Bypass-UAC-Techniken)
- Gezielte Methoden zur Zugriffssicherung mittels Persistence-Skripts
- PowerShell-Hacking-Methoden und -Tools
- Browser Explotation (Hooking)
- Vertiefung mit dem Metasploit™ Framework (z.B. Post-Explotation, Pass-the-Hash, Pivoting, gezieltes Exploiting, kombinieren mit anderen Angriffsvektoren)
- Advanced-WLAN-Hacking-Techniken (z.B. Rogue AP, Evil Twin)
- Skills-Erweiterung mit Web-Hacking-Methoden (z.B. Website Spoofing, XSS, SQLInjection)
- Advanced Threats Live-Demo (IoT-Hacking)

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

Cyber Attack & Defense Hands-on, 2 Tage

Dieser hands-on Workshop bietet Ihnen folgende Inhalte:

- Anhand des MITRE ATT&CK® Frameworks (https://attack.mitre.org) lernen Sie die Taktiken und Techniken der Cyberkriminellen kennen.
- Sie haben die ultimative Möglichkeit in einer Laborumgebung (Windows Active Directory-Umgebung mit Client und Servern) die Tools der Angreifer kennenzulernen.
- Sie werden selbst Angriffssimulationen auf gängige IT-Infrastruktur von Unternehmen durchführen.
- Anhand von angeleiteten Übungen können Sie, die für Sie und Ihr Unternehmen relevanten Techniken ausprobieren.
- Zusammen mit den anderen Kursteilnehmern erarbeiten Sie mögliche Erkennungs- und Gegenmassnahmen zu den Angriffen.

OSSTMM Professional Security Tester, 3 Tage

Dieses «OSSTMM Professional Security Tester»-Bootcamp bereitet Teilnehmende mit bereits fundiertem Wissen im Hacking- und Penetration-Testing-Bereich auf die OPST-Zertifizierungsprüfung vor.

- «Open Source Security Testing Methodology Manual (OSSTMM)»-Übersicht der Informationssicherheit
- Einführung in die OSSTMM-Methode
- Die sechs Sektionen des OSSTMM (mit Fallbeispielen)
- Internationale Best Practices und Standards
- OSSTMM Rules of Engagement (Ethischer Ansatz des OSSTMM)
- Security-Testtypen
- Aufbau des OSSTMM Compliance
- Vorgehen beim Testing
- RAV Risk Assessment Value als Benchmark
- Hands-on-Übungen zur Vorbereitung auf die Prüfung «Certified OSSTMM Professional Security Tester»

Key Learnings

- Nach Abschluss dieses Kurses sind Sie in der Lage, eigene kreative Ethical-Hacking-Ansätze in Ihre Überlegungen einzubeziehen
- Sie können mit Ethical-Hacking-Fähigkeiten die Wirksamkeit getroffener Massnahmen zur Abwehr vor Advanced Threats im eigenen Unternehmen prüfen (Hacking-Labs)
- Sie beziehen die offensiven Erkenntnisse in Cyber-Security-Strategien für gut gesicherte Umgebungen ein
- Aufzählen von mindestens drei Akteuren und deren Motivation bezüglich Cyberbedrohungen
- In Betrieb nehmen einer Lab-Umgebung (Windows Active Directory), um gängige Angriffe zu simulieren / üben
- Wissen, wo die Enterprise Matrix des MITRE ATT&CK® Frameworks zu finden ist
- Navigieren innerhalb der Matrix und herausfiltern der für Sie relevanten Techniken
- Benennen der 12 Taktiken der ATT&CK Matrix for Enterprise
- Beschreiben von mindestens drei Techniken pro Taktik und Ausprobieren von möglichen Angriffen im Lab
- Kenntnisse über mögliche Erkennungs- und Gegenmassnahmen zu den ausprobierten Angriffen
- Vorbereitung auf die offizielle OPST-Zertifizierungsprüfung, die vom Institute for Security and Open Methodologies (ISECOM) sowie von der La-Salle-Universität in Barcelona anerkannt wird
- Kennen der Grundlagen des OSSTMM
- Kennen der praktischen Anwendungen als Security Tester
- Kennen der Tools für das Security Testing und Umgang damit

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

Diese Advanced-Trainingseinheit richtet sich an alle, die den Basic Penetration Tester abgeschlossen beziehungsweise die Kurse HAK, HAK2 und SWO bereits besucht haben.

Anforderungen

Besuch der folgenden Trainingseinheit ist Voraussetzung für den Erhalt der Rollenzertifikat «Professional Penetration Tester»:

- Basic Penetration Tester («BASPEN»)
- Prüfung zum Basic Penetration Tester

Zertifizierung

Informationen zur OPST-Zertifizierungsprüfung

Die Prüfung ist im Kurspreis inbegriffen. Am letzten Kurstag absolvieren Sie die Prüfung zum «Certified OSSTMM Professional Security Tester». Die Prüfung dauert 3 Stunden und beinhaltet theoretische Fragen zu OSSTMM sowie praktische Aufgaben im Bereich Security Testing. Die Prüfung kann auf dem eigenen Laptop oder auf den Geräten der Digicomp durchgeführt werden.

Wiederholung der Prüfung

Eine Wiederholung kostet 249.50 € und wird vom Teilnehmer übernommen. Bei einer Wiederholung melden Sie sich direkt bei unseren Kundenberatern: info@digicomp.ch oder

Sie werden direkt auf die nächste Durchführung / Prüfung eingebucht.

OPST-Zertifizierung

Die OPST-Zertifizierung wurde für das Diplom «Master in Information Technology Security» der La-Salle-Universität in Barcelona anerkannt. Diese Einrichtung gehört zum internationalen La-Salle-Bildungsnetzwerk, dem auch das Manhattan College in New York und die La Salle University in Philadelphia angehören. Alle OPST-Zertifikate sind sowohl mit dem ISECOM- als auch mit dem La-Salle-Siegel versehen, als Zeichen des damit verbundenen Prestiges.

Rollenzertifikat «Professional Penetration Tester»

Sie haben die zweistufige Trainingsreihe Basic Penetration Tester und Advanced Penetration Tester inkl. OPST-Prüfung abgeschlossen und waren zu 80% in den Kursen anwesend.

Zusatzinfo

CAS Cyber Security Expert

Sie sind nur noch wenige Schritte vom CAS Cyber Security Expert entfernt. Besuchen Sie die folgenden Kurse, um den CAS-Abschluss bei Digicomp zu erreichen.

Kurs: ISO/IEC 27001 Foundation (FIS)

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-advanced-penetration-tester