Cyber Security Tester/Analyst – Hands-On Exploiting («HAK4»)

In diesem Kurs lernen Sie wie Schwachstellen mittels Exploits gezielt ausgenutzt werden. Mit dem erlernten Wissen über Exploiting-Techniken können Sie im Anschluss Angriffe rascher aufdecken und dadurch geeignete Gegenmassnahmen vorschlagen.

Dauer: 2 Tage
Preis: 1'900.– zzgl. 8.1% MWST

Inhalt

Im Kurs wird mit KALI LINUX™ und diversen eigenen Codes gearbeitet. Für alle Teilnehmenden steht eine entsprechende LAB-Umgebung für die Hands-on-Übungen bereit. Sie werden in den geführten LAB-Übungen Schritt für Schritt an die spannende Exploit-Thematik herangeführt. Dabei werden neben professionellen Exploiting-Werkzeugen wie dem Metasploit™ Framework auch diverse eigene Skripts eingesetzt. Im LAB werden Angriffe auf Client- und Server-Systeme sowie auf Webapplikationen angeschaut. Dabei erlangen wir mittels Exploits Zugriff auf Systeme und erhöhen mittels Privilege Escalation unsere Systemrechte. Zum vertieften Verständnis aktueller Angriffe schauen wir uns den besonders interessanten Ansatz des «Living off the Land Hackings» an, gegen welchen grundlegende Schutzmassnahmen momentan nicht ausreichend sind.

Abgerundet wird der Kurs mit den essentiellen Angriffs-Techniken gegen Webapplikationen, da gerade diese ein exponiertes und beliebtes Ziel von kriminellen Hackern sind. Durch das gemeinsam erarbeitete Wissen können Sie im Anschluss an diesen Kurs in eigenen Testumgebungen bekannte und neuartige Exploit-Techniken analysieren und damit eigene Cyber Security Massnahmen und Erkennungsregeln verbessern. Alle Teilnehmenden verpflichten sich ausdrücklich, das erlernte Wissen nicht missbräuchlich zu verwenden. Vor Beginn des Kurses ist daher eine entsprechende schriftliche Vereinbarung zu unterzeichnen.

- Einrichten eines eigenen Exploiting-Labs
- Rechnerarchitekturen und Assemblercode im Kontext von Exploits einordnen
- Einstieg in Debugging-Programme wie gdb, OllyDbg und Immunity
- Aufdecken von Schwachstellen mittels Fuzzing
- Grundlegende Exploiting-Techniken wie Buffer- und Heap-Overflows, Format String Verwundbarkeiten usw. verstehen
- Eigene Exploit-Skripte gemeinsam erstellen
- Die Nutzung von Shellcodes innerhalb des Exploitings verstehen
- Shellcodes generieren und in den eigenen Exploit-Skript einbetten
- Lauffähigkeit des Exploits sicherstellen (Bad Chars)
- Diverse User Space Exploits durchführen
- Mittels Kernel Exploits Root-Rechte erlangen
- Verwundbare Programmbibliotheken (DLLs) ausnutzen
- Schutzwirkung und Grenzen von DEP und ASLR im Kontext der Systemhärtung einordnen
- Mit «Living off the Land Hacking» Schutzmassnahmen prüfen
- Grundlegende Angriffstechniken gegen Webapplikationen wie XSS, SQL-Injection usw. verstehen
- Aufgaben für eigene LABs zur selbstständigen Wissensvertiefung

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

Key Learnings

- Umsetzen von bekannten und neuartigen Exploiting-Techniken
- Prüfen von Sicherheitsmassnahmen gegenüber Exploits in Testumgebungen (Hacking-Labs)
- Schärfen der analytischen Fähigkeiten gegenüber gezielten Angriffen
- Verständnis und rasches Erkennen von Angriffsmustern

Zielpublikum

Dieser Kurs richtet sich an Security-Fachleute, Informatiker und Führungskräfte, die den Kurs «Cyber Security Tester – Hands-on Professional (HAK2)» besucht haben und ihr bisher erworbenes Wissen und die analytischen Fähigkeiten in einem Hands-on-Training mit diversen Exploiting-Techniken vertiefen möchten.

Anforderungen

Besuch einer der folgenden Kurse oder gleichwertige breite praktische Hacking-Erfahrungen mit KALI LINUX™:

- Cyber Security Tester – Hands-on Foundation («HAK»)
- Cyber Security Tester – Hands-on Professional («HAK2»)

Zertifizierung

Dieses Kompaktseminar kann zusammen mit eigenen Übungen zur Vorbereitung auf diverse IT-Security- und Hacking-Zertifikate verwendet werden und ist Bestandteil der Vorbereitung auf das renommierte Zertifikat: «OSSTMM Professional Security Analyst».

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/kurs-cyber-security-testeranalyst-hands-on-exploiting