CYBER SECURITY ACADEMY

HACK IT TO DEFEND IT (L1)

HACK IT TO DEFEND IT (L1)

Atakos prieš IT infrastruktūrą supratimas – esminis veiksnys efektyviai užtikrinant IT saugumą.

Hack IT to Defend IT (L1) etiškojo įsiveržimo principu pagrįstų mokymų tikslas – išaiškinti kaip priešininkai planuoja ir vykdo kibernetines atakas ir suteikti įgūdžių praktiškai jas atremti.

Ši mokymų programa sudaryta atsižvelgiant į šiuo metu aktualiausias įsiveržimo metodikas ir technologijas, koncentruojantis į tinklo pažeidžiamumų problemas ir nuodugnią kritiškiausių sričių analizę – visa tai iliustruojama pavyzdžiais ir aptariamos geriausios apsaugos praktikos (angl. best practices).

Mokymų metu įgyta praktika suteiks tiek reikiamus pagrindus saugumo lygio įvertinimui savo organizacijoje, tiek žinių operatyviai identifikuoti ir reaguoti į potencialiai pavojingus bandymus įsiveržti į organizacijos IT infrastruktūrą.

Hack IT to Defend IT (L1) mokymai skirti IT profesionalams, saugumo ekspertams, tinklo administratoriams ir entuziastams, kurie nori suprasti kas iš tikro vyksta kai vykdoma kibernetinė ataka bei kokie pažeidžiamumai yra išnaudojami.

Po mokymų visiems dalyviams išduodami dalyvavimą patvirtinantys pažymėjimai.

Rekomendacijos dalyviams:

Siekiant maksimalaus rezultato mokymuose dalyvaujantiems rekomenduojama turėti TCP/IP žinių ir Windows/Linux pagrindus.

Mokymų metu reikalingas nešiojamasis kompiuteris su šiomis specifikacijomis: kelių branduolių procesorius, 4GB RAM (min 2GB), WLAN, galimybe užkrauti OS iš USB, pageidautinas USBv3 palaikymas (min USBv2).*

* Jei kompiuterio su minėtomis specifikacijomis į mokymus atsinešti nėra galimybės, informuokite CSA ir mes jį parūpinsime (bus taikomas papildomas mokestis).

TRUKMĖ: 2 dienos

DĖSTYMO KALBA: lietuvių (galima vesti anglų kalba)

KAINA: 750 EUR

NUOLAIDOS:

Išankstinės registracijos nuolaida – 15 %

3 ir daugiau žmonių iš vienos įmonės – 20 %

(nuolaidos nesumuojamos)

Lektoriai

Teikia informacijos saugumo valdymo paslaugas, atlieka saugumo auditus, įsiveržimų testavimus, DDoS atsparumo bandymus, teikia konsultacijas ISO 27001 standarto klausimais.

Cyber Security Academy
Tel.: +370 6 888 1450
mokymai@cybersecurityacademy.lt
www.cybersecurityacademy.lt

HACK IT TO DEFEND IT (L1)

1-osios dienos darbotvarkė:

1. **Įsilaužimai. Pradžia.**
   - Įsilaužimų istorija;
   - Įsilaužėlių tipai ir jų motyvai;
   - Didelio mąsto įsilaužimų aptarimas;
   - Įsilaužimo etapai.
2. **Anonimiškumas**
   - *Proxy* serveriai;
   - TOR tinklas;
   - Virtualūs privatūs tinklai (VPN);
   - Naršyklių konfigūracija.
3. **Informacijos rinkimas**
   - Viešos interneto paieškos sistemos;
   - DNS, WHOIS ir kita techninė informacija;
   - Tinklalapio turinio analizė;
   - Meta duomenys;
   - El. pašto informacija.
4. **Prievadų skenavimas**
   - Pažeidžiamumų priežastys;
   - Pažeidžiamumų duomenų bazės;
   - Konfigūracijos spragos;
   - Slaptažodžių parinkimas;
   - *Fuzzing* technika.
5. **Pažeidžiamumų išnaudojimas**
   - *Exploit'ų* duomenų bazės;
   - Rankinis pažeidžiamumų išnaudojimas;
   - Automatinis pažeidžiamumų išnaudojimas;
   - Buferio perpildymas (ang. *buffer overflow*).

2-osios dienos darbotvarkė:

1. **Tinklo atakos**
   - ARP nuodijimas;
   - Tinklo srauto klausymasis;
   - DHCP *spoofing;*
   - DNS *spoofing;*
   - VLAN *hopping.*
2. **Web atakos**
   - *Cross-Site Scripting;*
   - *Path traversal;*
   - Kodo vykdymas;
   - SQL injekcija;
   - Loginės klaidos.
3. **Veiksmai po įsibrovimo**
   - Sisteminės informacijos rinkimas;
   - Slaptažodžių išgavimas;
   - Privilegijų pasikėlimas;
   - Galinės durys (ang. *backdoor*) ir Rootkit.
4. **Slaptažodžių parinkimas**
   - Slaptažodžių šifravimo algoritmai;
   - Parinkimas pagal žodyną;
   - Grubios jėgos (ang. *bruteforce*) metodas;
   - *Rainbow* lentelės.
5. **Klientinės programinės įrangos atakos**
   - Klientinės programinės įrangos pažeidžiamumai;
   - *Phishing* atakos;
   - *Drive-by download* atakos;
   - *Watering hole* atakos;
   - Kenkėjiška programinė įranga.
6. **Bevielio tinklo atakos**
   - Wi-Fi apsaugos mechanizmai;
   - WEP nulaužimas;
   - WPA/WPA2 nulaužimas;
   - WPS spragos.
7. **Atsisakymo aptarnauti (DDoS) atakos**
   - DDoS atakų anatomija;
   - *Botnet* tinklai;
   - Tinklo lygmens DoS atakos;
   - Taikomojo lygmens DoS atakos.

Cyber Security Academy
Tel.: +370 6 888 1450
mokymai@cybersecurityacademy.lt
www.cybersecurityacademy.lt