ETIKUS **HACKER** TRÉNING

Az etikus hacker tréning hallgatói megismerhetik a komplex vállalati informatikai rendszereket, valamint az információbiztonságot fenyegető veszélyeket és támadási módokat. A hallgatók konkrét esettanulmányokon keresztül sajátíthatják el azokat a módszereket, taktikákat és stratégiákat, amelyekkel hatékonyan és eredményesen ismerhetik fel, előzhetik meg és védhetik ki a rosszindulatú támadásokat.

A képzés módszertanát a hosszabb, 2 szemeszteres képzés módszertanának alábbi, egyszerűsített részei alkotják:

TÁMADÁSI TECHNIKÁK

Ez a modul 5 témakört ölel fel az alábbiak szerint: külső internetes szegmens, on-line webes alkalmazások, belső LAN oldali, vezeték nélküli wifi, valamint mobil kommunikációs hálózatok sérülékenység vizsgálata. Érintjük az etikus hacker tevékenységgel kapcsolatos jogi kereteket, illetve hallgatóink rövid betekintést kapnak a humán oldali, úgynevezett social engineering információszerzési módszerekbe.

VÉDELMI TECHNIKÁK

A tréning fő célja, hogy a fenyegetettségek, támadási technikák megismerésével hallgatóink képesek legyenek a megszerzett információkat értelmezni, segítségükkel a fenyegetettségek hatásait csillapítani.

Webes alkalmazások védelme

A tanfolyam résztvevői megismerhetik a webes alkalmazásokat fenyegető támadási formákat, képessé válnak azok felismerésére és elhárítására. Átfogó képet kapnak arról, hogy milyen biztonsági szempontokat érdemes figyelembe venni egy webes alkalmazás kiválasztásakor, avagy egy fejlesztési projekt indításakor. Elsajátíthatják, hogy hogyan lehet támadás-detektáló, tartalomszűrő módszerekkel védeni a publikus alkalmazásokat, információkat.

Belső hálózat védelme

Hallgatóink megtanulhatják, hogy hol lehet a leghamarabb felfedezni a különféle támadásokat, hol és hogyan lehet a leghatékonyabban csillapítani a lehetséges károkozás mértékét. A modulban arról is szó lesz, hogy hogyan kell egy biztonságos hálózatot kiépíteni. Bemutatásra kerülnek a különféle buktatók, s azok kezelése.
A hallgatók többek között ilyen típusú kérdésekre kaphatnak választ:
Hogyan észlelhető egy belső hálózati visszaélés (pl. programozott fenyegetettség, vírustámadás)?
Hogyan alakítsunk ki jól működő patch menedzsmentet, vírusvédelmi rendszert?
Miért fontos a változáskezelés, hogyan lehet sikeresen kialakítani IDM-et?
Mekkora jelentőséggel bír a rendszereinkhez hozzáférő felhasználók biztonsági tudatossági szintjének ismerete és folyamatos fejlesztése?

WIFI hálózat védelme

A tanfolyam részvevői megismerkedhetnek a vezeték nélküli hálózatok veszélyeivel, az ilyen hálózatok használatából adódó problémákkal, valamint a támadási lehetőségekkel (pl. lehallgatási technikák, jelszó feltörési technikák.) A megszerzett tudás birtokában képessé válnak biztonságos vezeték nélküli hálózatokat kialakítani, vagy azokat biztonságos módon felhasználni, üzemeltetni.

INCIDENSEK KEZELÉSE

A tanfolyam anyagának jelentős részét az incidensek felismerése és kezelése adja, azaz, ha már megtörtént a baj, azt hogyan lehet a leghamarabb felismerni, s az esemény kivizsgálásával olyan intézkedéseket hozni, amellyel az adott típusú sérülékenység minimalizálható. A hallgatók tehát képessé válnak olyan testreszabott incidens kezelési munkafolyamat kialakítására, amelynek kereténben a lehető legtöbb visszaélés, incidens kezelhetővé válik.

Felnőttképzési intézmény nyilvántartási száma: 00594-2009
Intézmény-akkreditációs lajstromszám: AL-2134