

ETIKUS HACKER KÉPZÉS TEMATIKA

A képzés alapvetően 5 témakörre bontható az alábbiak szerint:

- 1. külső internetes szegmens,**
- 2. on-line webes alkalmazások,**
- 3. belső LAN oldali,**
- 4. vezeték nélküli wifi,**
- 5. valamint mobil kommunikációs hálózatok sérülékenység vizsgálata.**

Hallgatóink a technológiai témakörök mellett megismerik az etikus hacker tevékenység jogi hátterét, illetve ízelítőt kapnak a humán hackelés, vagy másnéven social engineering információszerzési módszereiből.

A képzés kitér az etikus hackelés project és ügyfélmenedzsment aspektusaira is.

MODULOK:

JOGI ISMERETEK 1.

A hallgatók rövid áttekintést kapnak az IT biztonsági területére vonatkozó hazai és nemzetközi jogszabályokról, előírásokról.

KÜLSŐ HACK BEVEZETÉS

A külső sérülékenység vizsgálatok esetén a támadó teljesen kívülálló, azaz nincsen hozzáférése a célpont belső erőforrásaihoz, ezért csak a publikusan elérhető szolgáltatásokat látja. A hallgatókat ebben a modulban arra készítjük fel, hogy ezeket a publikusan elérhető felületeket megvizsgálva képesek legyenek minél több információt szerezni, szolgáltatásokat felderíteni, sérülékenységeket feltárni, majd jogosultságokat szerezni és hozzáférni a belső erőforrásokhoz.

KÜLSŐ HACK 1. FÁZIS (általános információgyűjtési technikák)

A publikusan (internet felől) elérhető információk felkutatási módszereinek, s a megszerzett információk felhasználási területeinek ismertetése.

KÜLSŐ HACK 2. FÁZIS (technikai információgyűjtési módszerek)

Technikai információk felkutatása és megszerzése a korábban összegyűjtött általános információk felhasználásával.

KÜLSŐ HACK 3. FÁZIS (rendszer-felderítési technikák)

Bemutatásra kerülnek azok a technikák, melyekkel az interneten keresztül elérhető hálózati felderítésre szolgáló információk szerezhetők meg. (pl. hol vannak az interneten a hálózat számítógépei, IP cím tartomány azonosítása)

KÜLSŐ HACK 4. FÁZIS (szolgáltatások felderítése és azonosítása)

Ebben a modulban hallgatóink megismerhetik a Portscan technikákat, melyek segítségével azonosításra kerül, hogy milyen típusú szerverek találhatóak a hálózaton, s az adott szervereken milyen szolgáltatások futnak.

KÜLSŐ HACK 5. FÁZIS (automatikus sérülékenység vizsgálat)

Az azonosított szolgáltatások után hallgatóink megismerhetik azokat a szoftveres módszereket, amelyek az elérhető a jól ismert sérülékenységek feltárására szolgálnak.

KÜLSŐ HACK 6. FÁZIS (manuális sérülékenység vizsgálat)

Ebben a fejezetben a kevésbé ismert sérülékenységek feltárási technikáiról lesz szó. Az ebben a fázisban feltárt hibák, hiányosságok révén megszerzett adatok értelmezéséhez és információvá alakításához már szükség van „manuális” kutatásra és elemzésre is.

KÜLSŐ HACK 7. FÁZIS *(penetrációs technikák)*

A modulban szó lesz arról, hogy hogyan kell a támadási profilokat összeállítani, s hogyan lehet kiaknázni az adott hiányosságokat, hibákat, melyek segítségével osztályozhatóvá válik a sérülékenység típusa, mértéke.

WEB HACK BEVEZETÉS

A webes sérülékenység vizsgálat egy szerteágazó terület. Ha csak abba gondolunk bele, hogy a cégek mennyi, sokszor felesleges információt tesznek közzé magukról hivatalos weboldalaikon, akár készakarva, akár véletlenül, elgondolkozhatunk, hogy a web igazából információs paradicsomként szolgál a rosszindulatú, és persze nem titkoltan az etikus hackerek számára is. A hallgatók megtanulják, hogy hogyan lehet ezeken az alkalmazásokon keresztül adatbázisokat, vagy akár egész belső hálózatokat kompromittálni.

WEB HACK 1. FÁZIS *(Információszivárgás/Hibák)*

Ebben a modulban hallgatóink megismerkedhetnek a webes rendszerekben tárolt, publikusan elérhető információk megszerzésének módszereivel.

WEB HACK 2. FÁZIS *(Cross site scripting)*

A téma a mai világban divatos Phising támadási technikák logikájának megismeréséről, tervezéséről, kivitelezéséről szól.

WEB HACK 3. FÁZIS *(Injection támadások, kártékony kód futtatása)*

A két terület a webes alkalmazások mögötti adatbázisok támadási technikáit mutatja be. (kártékony SQL kód injektálása)

WEB HACK 4. FÁZIS *(Session hijacking)*

Hallgatóink megtanulhatják, hogyan lehet egy regisztrált felhasználó profilját megszerezni anélkül, hogy ismernénk az azonosítóját és/vagy jelszavát. (ID theft)

WEB HACK 5. FÁZIS *(CSRF, kriptográfia)*

A hallgatók megismerkedhetnek a legelterjedtebb titkosítási módszerekkel, azok erősségeivel és gyengeségeivel egyaránt. Betekintést nyerhetnek az adatvédelem és a rejtjelezés gyakorlatába.

BELSŐ HACK BEVEZETÉS

A belső sérülékenység vizsgálatok esetén az etikus hacker azt tanulja meg, hogy milyen módon tudja feltárni és bemutatni a rendszer biztonságát a belső, regisztrált felhasználók szemszögéből. Képessé válik a belső hálózat gyengeségeit felkutatni, és kiaknázni.

BELSŐ HACK 1. FÁZIS *(Hálózati hozzáférés, MITM)*

Ebben a fejezetben a hallgatók megtanulják, hogyan lehet és érdemes egy belső hálózatot vizsgálni, ha már fizikailag hozzáférhetővé tettük. Megismerhetik továbbá a belső hálózatok kialakításának buktatóit, gyengeségeit, illetve képesek lesznek azok felderítésére és kiaknázására.

BELSŐ HACK 2. FÁZIS *(Információgyűjtés)*

Hallgatóink útmutatót kapnak arról, hogyan lehet minél több információt megszerezni egy belső hálózatról. Megismerhetik azokat a technikákat, amelyek a rosszindulatú belső felhasználók kezében „fegyverként” alkalmazhatóak gyakorlatilag minden vállalat belső hálózatán. Az így megszerzett gyakorlati tudással felvértezve képesek lesznek a belső hálózatok feltérképezésére, a meglévő gyengeségek azonosítására, és kiaknázására egyaránt.

BELSŐ HACK 3. FÁZIS *(Manuális szolgáltatás-ellenőrzés)*

A hálózatok kevésbé ismert sérülékenységeinek feltárási technikáiról lesz szó. Az ebben a fázisban feltárt hibák, hiányosságok révén megszerzett adatok értelmezéséhez és információvá alakításához már szükség van „manuális” kutatásra és elemzésre is.

BELSŐ HACK 4. FÁZIS *(Automatikus szolgáltatás-ellenőrzés I. és II.)*

A hálózatban található szervereken futó szolgáltatások sérülékenységének vizsgálatára alkalmas szoftveres módszerekkel ismerkedhetnek meg hallgatóink.

BELSŐ HACK 5. FÁZIS *(Szolgáltatások feltörése (overflows))*

Ebben a fejezetben a különféle szolgáltatások feltörésére szolgáló módszereket vesszük górcső alá (buffer overflow, DOS stb.).

BELSŐ HACK 6. FÁZIS *(Jogosultságok szerzése)*

Ebben a modulban arról esik szó, hogy hogyan szerezzünk egy hálózathoz jogosultságot, illetve sikeres hozzáférés esetén magasabb jogosultsági szintet (k)et.

BELSŐ HACK 7. FÁZIS *(Nyomok elfedése)*

Résztevőink arról hallhatnak, hogy a rosszfiúk, azaz a hackerek egy kompromittálás során hol hagynak nyomokat, s ezeket milyen módszerekkel igyekeznek eltüntetni.

BELSŐ HACK 8. FÁZIS *(Ellenőrzés jogosultságokkal)*

A modul célja, hogy ismertesse a hallgatókkal, hogy hogyan lehet adminisztrátori jogosultsággal gyakorlatilag a rendszer összes hibáját feltárni.

WIFI BIZTONSÁG BEVEZETÉS

A vezeték nélküli, wifi hálózatok terjedésével egyre komolyabb és erőteljesebb munkát fektetnek a gyártók és a fejlesztők abba, hogy még biztonságosabbá tegyék termékeiket, protokolljaikat. A modul célja, hogy megmutassa, milyen eszközökkel lehet hozzáférni ezekhez a vezeték nélküli pontokhoz, hogyan lehet rajtuk keresztül csatlakozni a hálózatokhoz.

WEP, WPA-TKIP, WPA-CCMP, EAP, LEAP BIZTONSÁG

Ezzel a blackbox technikával a résztvevők megtanulhatják, hogyan lehet hozzáférni jogosultság nélkül a különféle erősségű védelemmel ellátott WIFI hálózatokhoz.

BEVEZETÉS A SPECIÁLIS TERÜLETEKRE

Az alábbi két speciális témakör célja, hogy átadja azt a tudásanyagot, mely egyrészt a mobil kommunikációs hálózatok (GSM, GPRS, UMTS) sérülékenység vizsgálatára teszi alkalmassá hallgatóinkat, másrészt betekinthetnek az úgynevezett social engineering módszerek titkaiba is.

SPECIÁLIS TERÜLETEK 1. GSM, UMTS, GPRS HACK

Ebben a modulban ismertetésre kerül az összes olyan módszer, mellyel az etikus hacker képessé válik jogosultság nélkül hozzáférni a különféle erősségű védelemmel ellátott mobil kommunikációs hálózatokhoz.

SPECIÁLIS TERÜLETEK 2. SOCIAL ENGINEERING

Minden korábbi modullal ellentétben a social engineering-et sokszor nem is tekintik igazi informatikai területnek, hiszen az emberre, mint gyenge láncszemre épít. A hallgatók a modul elvégzésével megértik, miért működnek a phishing támadások, hogyan lehet telefonon vagy e-mailben bizalmas, szenzitív adatokat megszerezni, egyszóval képessé válnak a humán erőforrás gyengeségeinek kiaknázására.

JOGI ISMERETEK 2.

Ebben a modulban részletesen ismertetésre kerülnek azok a törvényi előírások, jogszabályok, ajánlások, melyek az etikus hacker munkavégzéséhez elengedhetetlenül szükségesek (internetjog, szerzői jog, adatkezelés, adatvédelem, számítógépes bűncselekmény stb.)