etikus hacker képzés

információk

A képzés helye: KÜRT Akadémia, 2040 Budaörs, Szabadság út 301.
Képzés időtartama: 2 szemeszter (240 óra)
Képzési alkalmak: szombatonként 9.00-16.00
A képzés ára: 950.000 Ft/szemeszter (A képzés akkreditált, így a képzési díj áfamentes.)
A képzés indulása: 2014. május 17.
Jelentkezési határidő: 2014. január 15.
A csoport maximális létszáma: 20 fő
Előfeltételek: Minimum alapfokú informatikai végzettség és érvényes erkölcsi bizonyítvány
Felvételi formája: Felvételi elbeszélgetés
Felvételi beszélgetés időpontja: 2014. január 24.
Program-akkreditációs lajstromszáma: PL-3784
A képzéssel megszerezhető végzettség: KÜRT Certified Etikus Hacker
Jelentkezés: www.kurt-akademia.hu/jelentkezes/

Ha bármilyen további kérdésed adódna a programmal kapcsolatosan, keresd Frankó Csuba Deát, a KÜRT Akadémia intézményvezetőjét az alábbi elérhetőségek bármelyikén!

E-mail: dea.csuba@kurt.hu
Telefon: 06-30-695-2229

a képzésről

A legfrissebb hacker technológiák első kézből a jövő informatikai, biztonsági és üzemeltetési szakértőinek. Terítéken a támadási és a védelmi technológiák teljes tárháza.

- Black, Grey, White Box hackelés
- Internet, WAN, LAN, WIFI, GPRS hálózatok támadása
- Hacker projektek jogi keretei
- Ügyfélkezelés és projektmenedzsment kényes biztonsági helyzetekben

Az Etikus hacker képzés házigazdája ***Frész Ferenc***, a KÜRT Biztonsági Intelligencia Központjának volt vezetője, aki számtalan, abszolút biztonságosnak hitt nagyvállalati rendszer súlyos hibáit és hiányosságait fedte már fel sérülékenységvizsgálatok során.

A program filozófiája szerint az etikus hacker csak úgy lehet sikeres, ha képes egy lépéssel a rosszfiúk előtt járni. Ez az egy esélye van, hogy teljesítse megbízatását. Nem elég ismernie az információk és a rendszerek biztonságát fenyegető technológiákat, képesnek kell lennie előre látni az újabb és újabb fenyegetettségeket.

A KÜRT Akadémia képzése erre a küldetésre készíti fel a hallgatókat, lehetőséget kínálva a jelentkezőknek az informatikai rendszerek megfelelő információbiztonsági szintjének tudatos megteremtésére.

Nézd meg a KÜRT Akadémia intézményvezetőjével, ***Frankó Csuba Deával*** készült interjút az Etikus hacker képzésről!

azoknak ajánljuk, **akik**

- hosszú távon piacképes szakmát szeretnének elsajátítani, és rászánnak egy évet arra, hogy tudásuk valódi értéket képviseljen az etikus hacker piacon,
- információbiztonsági szakterületen dolgoznak és szeretnék bővíteni tudásukat,
- már rendelkeznek az EC Council által kiadott CEH minősítéssel és szeretnének még jobban elmélyedni az etikus hackelés rejtelmeiben,
- szeretnének a képzés elvégzése után bekerülni egy inspiráló, aktív szakmai közegbe, ahol folyamatosan lehetőség nyílik a tudásfrissítésre.

miért mi?

Hallgatói statisztikáink szerint:

- A végzett hallgatóink 90%-a jobban keres a tanúsításunk megszerzése után, mint azelőtt.
- A nálunk végzett etikus hackerek több mint fele előre lépett a munkahelyén, vagy magasabban kvalifikált munkahelyre váltott a képzés befejeztével.
- A hallgatóink a képzés legnagyobb erősségének az ütőképes tudásanyagot és annak unikalitását tartják.

„Nem hiszem, hogy bármilyen újdonság mérhető lenne ahhoz a masszív alaphoz, amit a képzés nyújt. Erre épül minden, és ebből le is vezethető minden. Az újdonságok "csak" fejlődési irányok, de az alapok nélkül nincs értelme róluk beszélni."

Vargha Gergő, *etikus hacker*

„A KÜRT Akadémia 240 órás képzésén fokozatosan ismerkedtünk meg az etikus hackelés sérülékenységvizsgálati módszertanával. A webes vizsgálatok alkalmával betekintést nyertünk abba, hogy milyen a hazai és a külföldi weboldalak biztonsági állapota. Szinte minden esetben találhatók információszivárgást okozó hibák, ott felejtett fájlok, stb... Ezen túl nagyon sok esetben sikerült a célba vett oldalakról egy teljes adatbázist megszerezni a bennük lévő felhasználó nevekkel és jelszavakkal együtt. Több alkalommal teljesen át lehetett venni az irányítást egy-egy DMZ-ben található gép felett. A záróvizsga feladataként egy magyarországi telekommunikációs céget kaptunk. A képzésben talpon maradt hallgatók mind sikerrel vették a végső akadályt."

Dr. Erdődi László, *etikus hacker*

szakmai vezető

Frész Ferenc a KÜRT Zrt. Biztonsági Intelligencia Központjának volt vezetője. Szakértőként közel 20 éve kiemelten foglalkozik informatikai rendszerekhez kapcsolódó kockázatok, fenyegetettségek vizsgálatával és kezelésével. Információbiztonsági rendszerek etikus hackelésében, információbiztonsági projektek lebonyolításában jártas szakember. Szaktudása megközelítőleg ezer sikeres hazai és külföldi információbiztonsági projekt tapasztalatainak eredménye. 2011 óta a Közigazgatási és Igazságügyi Minisztérium Nemzeti Biztonsági Felügyelet E-biztonsági Intelligencia Központ (NBF CDMA) vezetőjeként részt vesz

- a kormányzat információs rendszereinek preventív jellegű védelmében, azok védelmi szintjének erősítésében,
- kormányzati kibervédelmi döntéshozatali folyamatokban,
- szakmai tanácsadóként a készülő információbiztonságról szóló törvény megalkotásában (munkacsoport vezetése 2012),
- a NATO és az EU információvédelemmel és kibervédelemmel foglalkozó munkacsoportjaiban és azok vezetésében,
- vezető oktatóként az információbiztonsági tudatosság emelését célzó képzések és szakmai továbbképzések fejlesztésében hazai és külföldi kormányzati és integrációs szervezetek számára, beleértve kibervédelmi és kríziskezelési hadgyakorlatokat is.

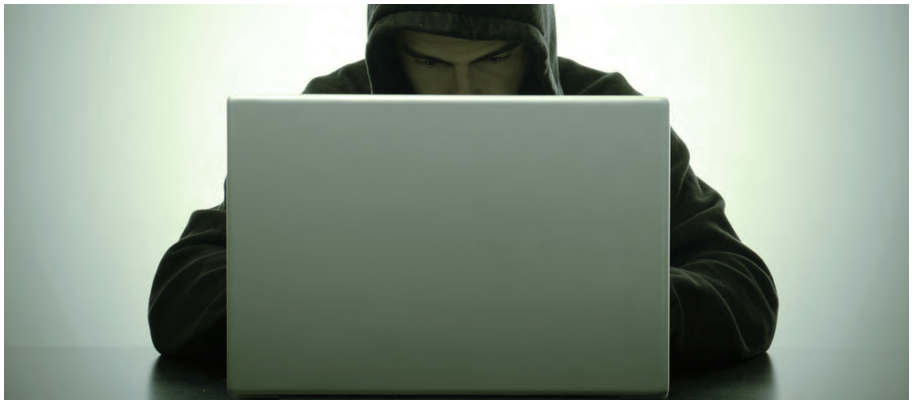
a képzés tematikája

I. Külső sérülékenységvizsgálat

A külső sérülékenységvizsgálatok 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.

II. Webes sérülékenységvizsgálat

A webes sérülékenységvizsgálat egy szerteágazó terület. Ha csak abba gondolunk bele, hogy a cégek mennyi, sokszor felesleges információt tesznek közzé magukról hivatalos weboldalaikon, akár készakarva, akár véletlenül, láthatjuk, 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.



III. Belső sérülékenységvizsgálat

A belső sérülékenységvizsgálatok esetén az etikus hacker azt tanulja meg, hogy milyen módon tudja feltárni és bemutatni a rendszer biztonsági réseit a belső, regisztrált felhasználók eszközeivel. Képessé válik a belső hálózat gyengeségeinek felkutatására, és kiaknáznására.

IV. Wifi sérülékenységvizsgálat

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.

a képzés tematikája

V. Speciális sérülékenységvizsgálat

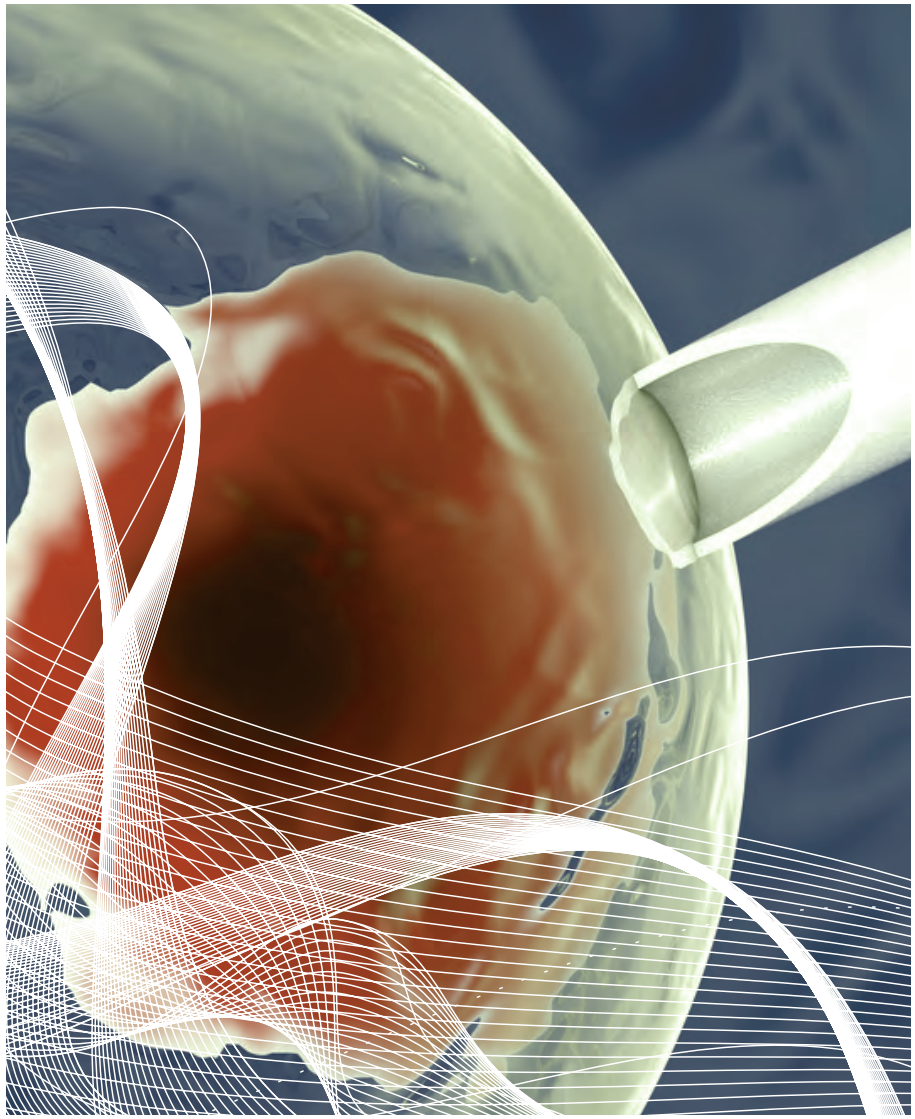
A témakör célja, hogy átadja azt a tudásanyagot, mely a mobilkommunikációs hálózatok (GSM, GPRS, UMTS) sérülékenység vizsgálatára teszi alkalmassá hallgatóinkat.

VI. Jogi kérdések

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...)

VII. Social engineering

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



órarend 2014/2015 I. félév

	szombat 9.00-12.30	szombat 13.30-16.00
május 17.	Bevezető gondolatok, jogi háttér	Modulok rövid ismertetése
május 24.	Külső hack bevezetés	Külső hack fázisok
május 31.	Külső hack 1. fázis (általános információgyűjtési technikák)	Külső hack 1. fázis (gyakorlat)
június 14.	Külső hack 2. fázis (technikai információgyűjtési technikák)	Külső hack 2. fázis (gyakorlat)
június 21.	Külső hack 3. fázis (rendszerfelderítési technikák)	Külső hack 3. fázis (gyakorlat)
június 28.	Külső hack 4. fázis (szolgáltatások felderítése és azonosítása)	Külső hack 4. fázis (gyakorlat)
július 5.	Külső hack 5. fázis (automatikus sérülékenységvizsgálat)	Külső hack 5. fázis (gyakorlat)
július 12.	Külső hack 6. fázis ("kézi" sérülékenységvizsgálat)	Külső hack 6. fázis (gyakorlat)
július 19.	Külső hack 7. fázis (penetrációs technikák)	Külső hack 7. fázis (kommunikációs gyakorlat)
július 26.	Külső hack feladat (gyakorlat)	Számonkérés (írásbeli, gyakorlati)
július 27. - augusztus 22.	**Nyári szünet**	
augusztus 23.	Web hack bevezetés	Webes támadások fajtái
augusztus 30.	Információ szivárgás/Hibák (elmélet)	Információ szivárgás/Hibák (gyakorlat)
szeptember 6.	Cross-site scripting (elmélet)	Cross-site scripting (gyakorlat)
szeptember 13.	Injection támadások (elmélet)	Injection támadások (gyakorlat)
szeptember 20.	Kártékony kód futtatása (elmélet)	Kártékony kód futtatása (gyakorlat)
szeptember 27.	Session hijacking (elmélet)	Session hijacking (gyakorlat)
október 4.	Kommunikációs modul (dokumentáció)	Összefoglalás
október 11.	Web hack feladat (gyakorlat)	Vizsga (írásbeli, gyakorlati)
november 8.	Belső hack bevezetés	Belső hack fázisok
november 15.	Hálózati hozzáférés, MITM (elmélet)	Hálózati hozzáférés, MITM (gyakorlat)

órarend 2014/2015 II. félév

	szombat 9.00-12.30	szombat 13.30-16.00
november 22.	Információ gyűjtés (elmélet)	Információ gyűjtés (gyakorlat)
november 29.	Szolgáltatás-felderítés (elmélet)	Szolgáltatás-felderítés (gyakorlat)
december 6.	Manuális szolgáltatásellenőrzés (elmélet)	Manuális szolgáltatásellenőrzés (gyakorlat)
december 20.	Automatikus szolgáltatásellenőrzés I. (elmélet)	Automatikus szolgáltatásellenőrzés I. (gyakorlat)
december 21. - január 9.	**Karácsonyi szünet**	
január 10.	Automatikus szolgáltatásellenőrzés II. (elmélet)	Automatikus szolgáltatásellenőrzés II. (gyakorlat)
január 17.	Szolgáltatások feltörése, overflows (elmélet)	Szolgáltatások feltörése, overflows (gyakorlat)
január 24.	Jogosultságok szerzése (elmélet)	Jogosultságok szerzése (gyakorlat)
január 31.	Nyomok elfedése – Forensics (elmélet)	Nyomok elfedése – Forensics (gyakorlat)
február 7.	Ellenőrzés jogosultságokkal (elmélet)	Ellenőrzés jogosultságokkal (gyakorlat)
február 14.	Belső hack feladat (gyakorlat)	Vizsga (írásbeli, gyakorlati)
február 21.	Wifi biztonság bevezetés	Wifi támadások fajtái
február 28.	WEP biztonság (elmélet)	WEP biztonság (gyakorlat)
március 7.	WPA-TKIP biztonság (elmélet)	WPA-TKIP biztonság (gyakorlat)
március 21.	WPA-CCMP, EAP, LEAP biztonság (elmélet)	WPA-CCMP, EAP, LEAP biztonság (gyakorlat)
március 28.	Wifi feladat (gyakorlat)	Számonkérés (írásbeli, gyakorlati)
március 29. - április 10.	**Húsvéti szünet**	
április 11.	Bevezetés a speciális területekre	Érintett területek támadhatósága
április 18.	GSM, UMTS, GPRS hack (elmélet)	GSM, UMTS, GPRS hack (gyakorlat)
április 25.	Social engineering (elmélet)	Social engineering (gyakorlat)
május 9.	Jogi kérdések	Jogi kérdések
május 16.	Vizsga (írásbeli, gyakorlati)	Záróvizsga (szóbeli, írásbeli)