kibev

önkéntes kibervédelmi összefogás
voluntary cyber defence collaboration

# VESZÉLYES VIZEKEN

## AZ ETIKUS HACKELÉS IRÁNYELVEI

**Az elektronikus szolgáltatások használata és az internet mindennapjaink részévé vált. A digitális infrastruktúrától való függés és az egyre növekvő elektronikus adatvagyon az állami szervezeteket és az üzleti szereplőket egyaránt kihívások elé állítja. A kiberbiztonság állandó napirendi ponttá vált, és az egyre fejlettebb támadási technikákra offenzívabb elhárító módszerekkel kell válaszolni.**

**Az etikus hacker célja, hogy a támadó szemszögéből vizsgálja és tesztelje az adott szervezet védelmi rendszerét, ismert és ismeretlen sérülékenységeket keres, ezáltal segíti a hatékony felkészülést a valós támadásokra. Az ilyen munkakörben dolgozó biztonsági szakembereknek komoly feltételeknek kell megfelelniük nap mint nap.**

**Az elmúlt időszak sajtóhírei az etikus hacker fogalmát a szélesebb körű társadalom számára is ismertté tették, azonban nem feltétlenül a valóságot tükröző módon. Szeretnénk útmutatást adni a téma iránt érdeklődőknek, hogy milyen keretek között dolgozik egy valódi etikus hacker, továbbá segíteni kívánunk azoknak, akik biztonsági hibákkal, problémákkal találkoznak, vagy a jövőben ezt a kihívásokkal teli szakmát szeretnék hivatásuknak választani.**

## MIT MOND A JOG?

A hacker tevékenységet a magyar büntetőjog nem ismeri. A jog nyelvére lefordítva az végez ilyen tevékenységet, aki jogosulatlanul belép egy információs rendszerbe vagy meglévő jogosultságait túllépi, illetve bármilyen más módon jogosulatlanul akadályozza a rendszer működését. Már maga a jogosulatlan belépés is bűncselekménynek számít. Amennyiben ott más tevékenységet is végez (adatokat megváltoztat, töröl, hozzáférhetetlenné tesz, bevisz), akkor már más bűncselekmény is megvalósulhat, illetve súlyosabban büntetendő a tevékenység.

A belépés nemcsak a rendszerbe való klasszikus behatolást jelenti, hanem azt is, ha oda jogosultság nélkül vagy a tulajdonost, felhasználót megtévesztve adatot, futtatható kódot juttatunk be. Akkor van bárkinek jogosultsága egy rendszerbe belépni, ha a tulajdonosától erre kifejezetten engedélyt kap szerződés formájában vagy nyilvánosan közzétett felhívással (pl. bug bounty).

# MIT CSINÁL EGY ETIKUS HACKER?

1. Az etikus hacker mindig az adott szervezet felkérésére dolgozik, nem önkényes döntése alapján.

2. Munkáját szerződés alapján végzi, amely pontosan tartalmazza a sérülékenységvizsgálat fókuszát (pl. adott applikáció), célját (pl. adminisztrátori jog megszerzése), módszertanát (pl. white box testing), időtartamát, és nem lépheti túl a szerződés kereteit. Meghirdetett bug bounty program esetén ugyanígy jár el.

3. Az etikus hacker munkájának minden egyes lépését alaposan dokumentálja és bizalmasan kezeli. Ebbe beletartozik a teljes folyamat: a jogalap; a felderítés; a feltárt sérülékenységek kihasználása; a lehetséges védelmi intézkedések azonosítása; kinek, mikor, kinek lett jelezve a hiba; milyen válaszok voltak, és egy záró riport elkészítése.

4. A szerződésben rögzített feladat megoldásával az etikus hacker a teljes dokumentációt átadja a megbízónak, majd a birtokába jutott és a megbízóra vonatkozó adatokat, illetve dokumentumokat megsemmisíti (amennyiben a szerződés erről máshogy nem rendelkezik).

5. Az etikus hacker jellemzően rendelkezik nemzetközi minősítéssel (pl. CEH, OSCP, OSWP), mely igazolja szaktudását és etikus voltát (etikai kódexet kell elfogadnia). Ez nem feltétlen kötelező, de lehet szerződésben lefektetett követelmény.

## MITŐL ETIKUS EGY ETIKUS HACKER?

Az etikus hacker fő jellemzői: jogkövető, szakszerű, tisztességes, szándékosan nem okoz kárt, felelősségteljes, titoktartó, tudását és tapasztalatát a közösséggel megosztja.

## MIT KELL TENNI AHHOZ, HOGY VALAKI ETIKUS HACKER LEGYEN?

1. Legyen kíváncsi és kitartó. A jó hacker motivációja a kíváncsiságból és a szakmai érdeklődésből fakad. Ne hátráljon meg az ismeretlen programozási nyelv, környezet vagy technológia elől.

2. Ismerje a legnépszerűbb programozási nyelveket, és legyen legalább egy, amelyet magas szinten elsajátított.

3. Legyen tájékozott a Windows, a Linux, az alkalmazások, a webalkalmazások, illetve a hálózatok témakörökben. Tudja, hogy miként épül fel a kapcsolat két végpont között.

4. Látogassa a szakmai konferenciákat (pl. ITBN, Hacktivity), kövesse a szakmai közösségek (pl. Hackersuli, Hackerspace) működését, és tájékozódjon online forrásokból (pl. Hack és Lángos podcast, OWASP).

5. Jelentkezzen egyetemi (pl. BME, NKE) és szakmai képzésekre (pl. SANS, Offensive Security).

## MIKOR ÉRDEMES ETIKUS HACKER SZOLGÁLTATÁST IGÉNYBE VENNI?

Ha függetlenségre van szükség:

- összehasonlító értékelés (benchmarking) esetén,
- egy külső harmadik fél szempontjából,
- auditok kiegészítésekor.

Ha speciális szaktudásra van szükség:

- cégen belül ritkán fellelhető tudás esetén,
- alkalmazás és rendszer fejlesztése, üzemeltetése és változtatása esetén,
- naprakész biztonsági információk és különleges eszközök ismerete esetén.

Ha speciális szemléletmódra van szükség:

- valós támadás szimulálása esetén,
- normál szerepköröktől eltérő (pl. üzemeltetők, fejlesztők) megközelítéshez,
- kifejezetten hibák kereséséhez.

# HIBÁT TALÁLTAK NÁLUNK! VAGY HA MÉG NEM, HOGYAN KÉSZÜLJÜNK FEL?

1. Soha ne ellenségnek tekintsük azt, aki felhívja a figyelmünket az általunk üzemeltetett vagy a tulajdonunkban álló rendszer hibájára.
2. Legyen egy előre meghatározott, dokumentált eljárásrendje annak, hogy miként kell kivizsgálni, ha bejelentenek egy hibát.
3. Tartsunk fenn egy dedikált bejelentő e-mail címet, ahol az ilyen jellegű bejelentéseket meg lehet tenni. Ennek hiányában a központi emailcímkezelők legyenek arra felkészítve, hogy az ilyen jellegű bejelentéseket kinek kell továbbítani.
4. Minden bejelentésnél jelezzünk vissza, hogy megkaptuk és elkezdtük a kivizsgálást.
5. Lehetőleg jelezzük azt is, hogy mikor kap információt a bejelentő a kivizsgálásról, és annak eredményről (pl. hibamegállapítás, javítás, nem valós hiba, további információ kérése, kommunikációs csatorna meghatározása).
6. Hívjuk fel a figyelmét, hogy a feltárt sérülékenységet többé ne használja ki, és a megszerzett adatokkal ne éljen vissza, ne terjessze azokat.
7. Tárgyalás esetén készítsünk emlékeztetőt, melyet mindkét fél elfogad.
8. Törekedjünk megállapodásra, amelynek része lehet az esetleges ellentételezés is.
9. Javasoljuk, hogy mindkét fél biztonsága érdekében a témában jártas (pl. informatikai) jogász segítségét vegyék igénybe a megbeszélésekhez és döntésekhez.
10. Tájékoztassuk a bejelentőt a lehetséges jogi következményekről, de a hatósági eljárásokat soha ne használjuk fenyegetésként, megfélemlítésként.
11. Ne felejtsük el, hogy a bejelentéssel kapcsolatban további feladataink vannak (pl. kríziskommunikáció, esetleges bejelentési kötelezettség).

# ÜZENET A SZÜRKE ZÓNÁBA

Ne feledd: az öncélú hibakeresés nem etikus hackelés! Minden olyan sérülékenységvizsgálat, amit nem megbízás alapján végzel, büntetőjogi következményekkel járhat. Ha sérülékenységet találsz, ne próbáld meg kihasználni, hanem dokumentáld le a megtett lépéseket, és értesítsd az illetékeseket: állami vagy közigazgatási szervezet esetén a GovCERT-et, versenyszektor esetében pedig az adott vállalat információbiztonsági csoportját vagy központi ügyfélszolgálatát. Bejelentésedet mindkét esetben akár anonim módon is megteheted.

Ne szabj egyoldalú feltételeket a hiba leírásának átadásához, se anyagi, se javítási idő, se állásajánlat, se egyéb tényezők tekintetében! Amennyiben valamilyen oknál fogva nem sikerül megoldást találni a bejelentésedre, megpróbálhatsz felettes szervhez, CERT-ekhez, tulajdonoshoz vagy az illetékes köztestülethez fordulni. Ha a nyilvánossághoz fordulsz (pl. a hibát nem javítják ki, vagy közérdeklődésre tart számot az ügy), akkor se add ki az összes technikai információt, hanem csak a jelenséget ismertesd, és lehetőleg olyan újságíróval oszd meg az részleteket, aki jártas a témában.

Ha például jogosulatlanul beléptél egy rendszerbe, akkor már ezzel a cselekedeteddel bűncselekményt követtél el. A rendszer tulajdonosának alapvető joga, hogy ellened büntetőeljárás megindítását kezdeményezze. Bár az eljárás végül kimondhatja, hogy cselekményed súlya olyan csekély mértékben veszélyes a társadalomra, hogy nem vagy büntethető, mégis azt tanácsoljuk, hogy mérlegeld, hogy az eljárás során elszenvedett károk ellentételezik-e a vélt vagy valós előnyöket.