Fehér Krisztián

Hackertechnikák

Útmutató valódi hacker módszerek
biztonságos kipróbálásához

Fehér Krisztián

Hacker-technikák

Útmutató valódi hacker módszerek biztonságos kipróbálásához

BBS-INFO Kiadó, 2018.

A könyv nagyobb mennyiségben megrendelhető a kiadónál:
BBS-INFO Kiadó, Tel.: 407-17-07 info@bbs.hu

Papírkönyv: ISBN 978-615-5477-64-5
E-book: ISBN 978-615-5477-65-2

Kiadja a BBS-INFO Kft.
1630 Budapest, Pf. 21.
Felelős kiadó: a BBS-INFO Kft. ügyvezetője
Nyomdai munkák: Biró Family Nyomda
Felelős vezető: Biró Krisztián

Tartalomjegyzék

1. Bevezetés

1.1. Új könyv, régi elvek

A „Kezdő hackerek kézikönyve" kiadvány sikere után most a folytatást tartja a kezében az olvasó. A korábban megjelent könyv előszeretettel ajánlható az informatika biztonsági kérdései iránt érdeklődők számára, mivel egyszerű gyakorlati példákkal és sok magyarázattal ellátva vezeti végig az olvasót a tárgyalt témakörökön.

Jelen könyvünk azok számára készült, akik a gyakorlatban szeretnék továbbfejleszteni ezirányú képességeiket és a hackerek által használt további módszereket is meg szeretnének ismerni.

Rögtön az elején tisztázzuk: a könyvet az etikus hackelés szellemében írtuk, ezért az ismertetett módszerek felhasználása saját hálózati tesztinfrastruktúrákon kívül illegálisnak minősül és büntetőjogi következményeket vonhat maga után! Ennek értelmében minden illegális előjelű felhasználástól elhatárolódunk. Úgyis mondhatnánk: az olvasó saját felelőssége, hogy hogyan használja fel a megszerzett ismereteket.

1.2. A szerzőről

A szerző hivatásos szoftvertesztelő, minőségbiztosítási tanácsadó, diplomás német irodalmár, a Magyar Térinformatikai Társaság (HUNAGI) egyéni szakértői tagja.

Kibertámadások kivitelezését és ezek lehetséges kivédését évek óta tudatosan tanulmányozza, ebből született ez a könyv is. Több kiberbiztonsággal kapcsolatos előadást is tartott már Magyarországon, sőt vendégoktatóként még oktatási intézményben is. Szakmai munkáját évről évre növekvő érdeklődés és elismerés kíséri.

Gyerekkorában autodidakta módon tanult meg programozni, az évek során számos programozási nyelvvel megismerkedett. Megszerzett tudását előszeretettel használja alternatív, kísérleti alkalmazások készítésére, melyek egy része ingyenesen elérhető, sőt vannak köztük nyílt forráskódúak is. A szerző fejleszt Windows desktop, Android és webes környezetekre is.

Elsődleges szakterülete a digitális grafika programozása, valamint digitális térképalkalmazások készítése. Sok időt fordít saját térinformatikai keretrendszerének fejlesztésére, a ZEUSZra, melyet a NASA-nál is ismernek.

Tudását igyekszik minél szélesebb körben megosztani másokkal is. Ennek folyományaként több könyve is megjelent már a hazai könyvesboltokban az elmúlt években, nem egy közülük sikerlisták élére is került. Munkáiról bővebben a

http://feherkrisztian.atw.hu/

weboldalon is lehet olvasni.

1.3. A könyv szerkezete

Könyvünk témakörei, fejezetei csupán laza kapcsolatban állnak egymással, mégis az elején a hackelési feladatokra történő felkészülés segédleteivel kezdünk, ezután pedig mindenki a saját érdeklődésének megfelelően haladhat. Ennek ellenére a fejezetek egymás utáni elolvasása és kipróbálása is javasolható.

Igyekeztünk minél több helyen hivatkozni a támadások elhárítási lehetőségeire, a kockázatokra irányítva a figyelmet.

Felhívjuk a figyelmet arra, hogy a könyv számos illusztrációt tartalmaz. Ezek elsődleges célja a szemléltetés és eltérhetnek attól, amit az olvasó láthat a saját számítógépén.

2. **Merre tart a világ?**

A világ egyre jobb lesz és fejlődik. Vagy mégsem? A válasz korántsem egyértelmű, legalábbis információbiztonsági szempontból.

Elég, ha megnézünk néhány példát azon események, trendek közül, melyek csupán a Kezdő hackerek kézikönyvének megjelenése óta történtek.

Ezek a következők:

- Reneszánszukat élik az internetes átverések és csalások, melyek például egy-egy nagyobb, aktuális sportesemény iránti érdeklődést használnak ki.
- Van olyan európai uniós ország, mely 2017-ben lényegében eltörölte a levéltitok fogalmát. Az érintett állami szervek "indokolt esetben" legálisan beleolvashatnak például a hagyományos és az elektronikus levelezésbe, sőt rögzíthetik is az állampolgárok kommunikációját.
- Egyes országok bizonyítékok nélkül folyamatosan vádolnak más országokat hackertámadásokkal. A hackertámadások vádja így nemzetközi lejáratő- és zsarolóeszközzé vált és a politikai nyomásgyakorlás eszköztárába is bekerült.
- Botránnyá dagadt, hogy egy közösségi oldal „nem megfelelő módon” kezelte a felhasználók adatait. Újfent bebizonyosodott, hogy a közösségi oldalak mennyire gátlástalanul pénzzé teszik a felhasználóik személyes adatait.
- Az Európai Únió szigorú adatkezelési szabályokat vezetett be 2018 májusában (GDPR).

Bár a hírek mindig érdekfeszítően tálalják az újdonságokat, elmondhatjuk: nincs új a nap alatt. Az eddig megismert harc a digitális világban továbbra is folytatódik. Hol a háttérben,

csendben, hol reflektorfénybe állítva, nagy médiafelhajtás közepette. A GDPR-ről pedig csak annyit: az érintett vállalatok, cégek hozzáállásán ez jottányit sem fog változtatni.

Újdonság viszont, hogy egyre több ország tekinti – nagyon helyesen! – egyenesen nemzetbiztonsági kérdésnek a kibervédelmet mind polgári, mind katonai vonatkozásban. E tekintetben hazánkban is komoly előrelépések várhatóak.

2.1. Linux, **még biztonságosabban**?

A szerzőt többször is megkérdezték Linux felhasználók, hogy hogyan tehetnék még biztonságosabbá a rendszerüket, ezért feltételezhető, hogy más olvasóban is felmerül ugyanez a kérdés.

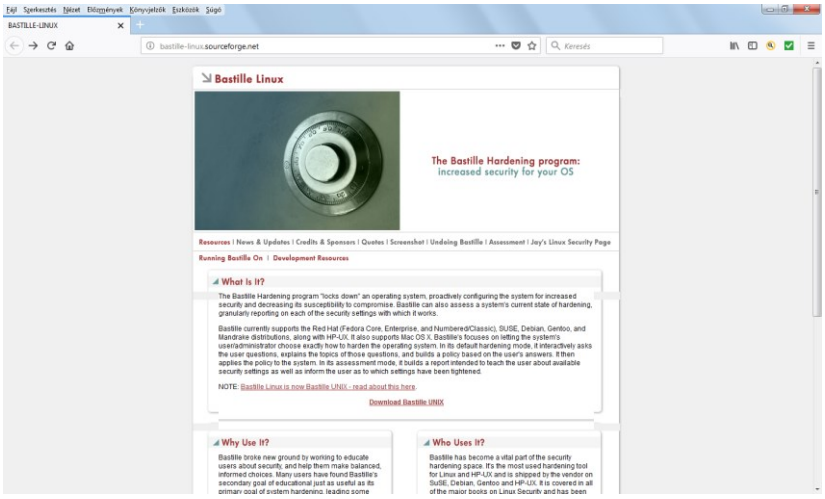
Két lehetséges megközelítést mutatunk be ebben az irányban.

2.1.1. **Bastille Linux segédprogram**

A Bastille Linux egy olyan segédprogram, mellyel meglévő Linux rendszerünket "keményíthetjük meg" biztonsági szempontból.

A projekt weboldala:

http://bastille-linux.sourceforge.net/



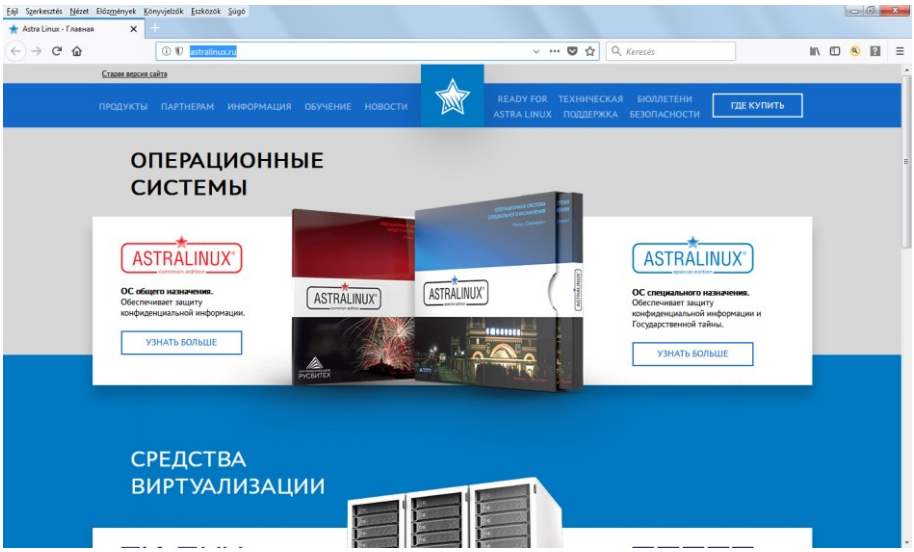
1. ábra

2.1.2. **Astra Linux operációs rendszer**

Azok számára, akik nem ragaszkodnak egy-egy, elsősorban a nyugati világban elterjedtebb Linux disztribúcióhoz és szeretnének megismerni új dolgokat, bátran ajánlható az Astra Linux, mely teljes mértékben orosz fejlesztés.

Az operációs rendszer hivatalos weboldala:

http://astralinux.ru/



2. ábra

Az Astra Linux megbízhatóságát mi sem jelzi jobban, minthogy az orosz Védelmi Minisztérium és az orosz hadsereg is ezt az operációs rendszert használja.

3. Az etikusság kérdése

Mielőtt elkezdenénk tárgyalni könyvünk fejezeteit, érdemes explicit módon is tisztázni, hogy mit értünk etikus hackelés alatt.

Ez már csak azért is fontos, mert gyakran találkozhatunk ezzel a fogalommal és sajnos nem mindig a megfelelő értelemben használják. Lássunk tisztán!

3.1. Mitől etikus egy hacker?

A hackelés információk megszerzéséről szól. Minden információnak van birtokosa, forrása, még akkor is, ha ezt sokszor kellemetlen elismerni.

A személyes adatokról szóló szigorított EU-s adatvédelmi előírás könyvünk írásakor lépett életbe, ezért ez egy igenis fontos kérdés.

Visszaélés a hackeléses tevékenységek esetén az információ megszerzésének és felhasználásának a tényében érhető tetten. Bármelyik tevékenység az információ birtokosának engedélye, hozzájárulása nélkül illegálisnak tekinthető, de legalábbis mindenképpen etikátlannak.

Ebben a tekintetben "közérdekű" információ nem létezik. Ezt azért fontos megértenünk, mert ha például a gyakorlatban egy súlyos biztonsági hibát talál valaki egy szoftverben, akkor az egy olyan bizalmas információnak számít, aminek már a nyilvánosságra hozatala sem etikus, ha az információ eredeti „tulajdonosa” nem engedélyezi azt. Ha ezt észben tartjuk, akkor sok fejfájástól és kellemetlen élethelyzettől kímélhetjük meg magunkat.

A hivatásos etikus hackerek mindig rendelkeznek a megbízójuk által kiállított írásos engedéllyel és szigorúan megszabott

keretek között és céllal tevékenykednek. Ez még akkor is igaz, ha a megbízó „szabad kezet" ad nekik.

A fentiektől eltérő magatartásformák nem tekinthetőek etikusnak, így hiába is vezérli bármennyire is jó szándék egy rendszer feltörőjét, egy hiba felfedezőjét, ha az nem a rendszer tulajdonosának megbízásából vagy felkérésére történt, nem nevezhető etikusnak a tevékenység.

Ettől függetlenül a szoftverfejlesztő cégek többféle módon állnak a rendszerükben hibát felfedező felhasználókhoz. Vannak olyan cégek, akik kifejezetten támogatják, adott esetben jutalmazzák is egy-egy kritikus hiba felfedezőjét, vannak, akik köszönettel fogadják, ha jelzik nekik a hibát, de a többség rossz néven veszi, ha valaki rájött arra, hogy a rendszerük nem tökéletes. Mindezek fényében, ha csak véletlenül is vettünk észre egy hibát – akkor is, ha az nem is hackeléssel jutott a tudomásunkra –, mindig a szoftver tulajdonosának jelentsük azt, és soha ne kürtöljük azt világgá, mivel ezzel jelentős károkozást valósíthatunk meg!

4. Alapvető eszközök beszerzése hackeléshez

A legfontosabb kérdés bizonyára ez:

"Mennyibe fog ez kerülni nekem?"

Jó hírünk van: már nulla forint beruházással is belevághatunk a tanulásba, önfejlesztésbe, amennyiben már rendelkezünk egy internetkapcsolattal bíró számítógéppel.

Ezt leszámítva persze a határ a csillagos ég, de nem kötelező erre elszórni minden pénzünket. Mire is gondolunk konkrétan? Lássuk tételesen, mit érdemes beszereznünk ahhoz, hogy a gyakorlatban is sikerrel mélyülhessünk el egy-egy témában!

4.1. Számítógép

Otthoni gyakorlásra, általános kutakodásra egy egyszerű asztali számítógép is megfelelő lesz. Legalább egy kétmagos processzor, 4-8 GB memória legyen a gépben, ez a legfontosabb.

Amennyiben „terepen" is ki szeretnénk próbálni magunkat, mindenképpen szükségünk lesz egy laptopra. Minél kisebb, annál jobb, a feltűnést ugyanis érdemes elkerülni.

4.2. Alapszoftverek

Szerezzünk be legalább egy Windows operációs rendszert és egy Linux rendszerünk is legyen. Érdemes utóbbit kineveznünk a fő rendszerünknek.

Windows tekintetében a Windows 7 és a Windows 10 ajánlott, mivel ezek a legelterjedtebb rendszerek napjainkban. Hazánkban ma már szinte kizárólag csak Windows 10 operációs rendszereket forgalmaznak, a Windows 7 támogatása megszűnt.

Ami a Linuxot illeti, messze a legajánlottabb a Kali linux használata, de egy Ubuntu Linux-szal sem járunk rosszul. Könyvünkben elsősorban Kali Linuxra (mi a 2018.1 és a 2018.2 verziókat használtuk) támaszkodunk és külön fejezetet is szentelünk a használatba vételének.

4.3. Wifi adapterek

Talán a legizgalmasabb részei a hackelésnek a Wifi vonatkozású tevékenységek, mivel itt el kell menni valahová, így valós időben történik minden.

Ahhoz viszont, hogy hatékonyak legyünk, megfelelő Wifi adóvevőre lesz szükségünk.

Egy jó minőségű wifi adapter természetesen nem csak hackelésnél remekel, hanem egészen egyszerű internethasználathoz is kiválóan alkalmazható. Tehát, ha amúgy is szükségünk lenne ilyen eszközre, két legyet üthetünk egy csapásra.

Megjegyezzük, hogy mi elsősorban a Wifi adapterek monitorozó módjának elérhetőségét vizsgáltuk, de ugyanígy fontos lehet az eszközök azon képessége is, hogy adatcsomagokat fecskendezzenek be meglévő hálózati kommunikációba. Az angolul **packet injection-**nek nevezett funkcionalitás nem magától értetődő adottsága az ilyen eszközöknek, bizonyos típusú támadásokhoz viszont elengedhetetlenek, éppen ezért az eszköz beszerzése esetén érdemes lehet ezt is megvizsgálni.

Kétféle megközelítés létezik alapvetően: ha a feltűnés elkerülése nagyon fontos, akkor vagy a gépünk beépített Wifi eszközére hagyatkozunk, vagy veszünk egy jobb minőségű, ún. "nano" méretű eszközt.

Más a helyzet, ha a hatékonyság és a távolságok áthidalása a legfontosabb. Így viszont az erre alkalmas eszközök nagyobb méretűek is lesznek, ezzel meg kell barátkozni.

A dolog ezzel azonban még messze nincs elintézve, ugyanis nem mindegy, milyen chipkészletet rejt az eszközök doboza.