

Fehér Krisztián

Kezdő hackerek kézikönyve

**avagy
informatikai támadások
és kivédésük**

Fehér Krisztián

Kezdő hackerek kézikönyve

**avagy
informatikai támadások
és kivédésük**

BBS-INFO Kiadó, 2016.

Minden jog fenntartva! A könyv vagy annak oldalainak másolása, sokszorosítása csak a kiadó írásbeli hozzájárulásával történhet.

A könyv nagyobb mennyiségben megrendelhető a kiadónál:
BBS-INFO Kiadó, 1630 Bp. Pf. 21. Tel.: 407-17-07

Figyelem! A könyvben leírt tevékenységek egy része illegális, illetve sértheti mások jogait, vagy az adott ország törvényeit. Az esetleges végrehajtásukból eredő következményekért sem a kiadó sem a szerző nem vállal felelősséget!

A könyv megírásakor a szerző és a kiadó a lehető legnagyobb gondossággal járt el. Ennek ellenére, mint minden könyvben, ebben is előfordulhatnak hibák. Az ezen hibákból eredő esetleges károkért sem a szerző, sem a kiadó semmiféle felelősséggel nem tartozik, de a kiadó szívesen fogadja, ha ezen hibákra felhívják figyelmét.

ISBN 978-615-5477-44-7

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

ELŐSZÓ	10
1. HACKER TÖRTÉNELEM.....	15
1.1. A „hacker” szó eredetéről és értelmezéséről.....	15
1.2. Miért léteznek hackerek?	17
1.3. Miért lehet hackelni?.....	18
1.4. A hackerek titkai?.....	18
1.5. A szoftverkalózkodásról	19
1.6. A „tuti” hacker módszerekről	20
1.7. A hacker csoportok jövője.....	20
1.8. Elit hacker csoportok és a politika	21
2. INFORMATIKAI TÁMADÁSOK MADÁRTÁVLATBÓL	23
2.1. Gondolatok az adatvédelemről.....	23
2.2. A biztonság mítosza.....	25
2.3. Visszaélések típusai	26
2.4. Adatbiztonság és adatvédelem	27
2.4.1. Adatbiztonsági fenyegetettségek.....	27
Rendelkezésre állás ellen irányuló fenyegetettség	27
Sértetlenség ellen irányuló fenyegetettség	28
Hitelesség ellen irányuló fenyegetettség	29
Bizalmasság ellen irányuló fenyegetettség.....	30
2.5. Hackerek típusai	30
Fehér kalapos hacker („white hat hacker”)	30
Fekete kalapos hacker („black hat hacker”)	31
Szürke kalapos hacker („grey hat hacker”)	31
Elit hacker („elite hacker”).....	31
Szkriptkölgyök („script kiddies”)	31
Hacktivist („hacktivist”).....	31
Telefon hacker („phreaker”).....	31

2.6. Támadások, támadóeszközök, szakkifejezések	32
Adathalászat („Spoofing attack, phishing”).....	32
Aranymosás	32
Befecskendezés (“injection”)	32
Betörő készlet („rootkit”)	32
Billentyűnaplózás („keystroke logging, keylogging”).....	32
Csomagelemzés („packet analyzis”)	33
Emberek félrevezetése („social engineering”)	33
Feltörés („cracking”).....	33
Féreg („worm”)	33
Hagyma útvonalválasztás („onion routing”).....	34
Harci kocsikázás („war driving”)	34
Hash ütközés (“hash colosion”).....	34
Hátsó kapu („backdoor”).....	34
Jelszavak feltörése („password cracking”)	34
Kémprogramok (“spyware”).....	35
Kéretlen levelek („SPAM”)	35
Kéretlen reklámprogramok („adware”)	35
Kódvisszafejtés (“reverse engineering”).....	35
Könyvtárbejárás (“directory traversal”)	36
Közbeékelődéses támadás („man-in-the-middle attack”)....	36
Köztes oldalon keresztül történő szkriptthívás („Corss-site scripting, XSS”).....	36
Kriptográfia („cryptography”)	36
Kriptovírus („crypto virus”).....	36
Lábnymkésztítés (“footprinting”).....	36
MAC cím hamisítás („MAC spoofing”).....	36
Meglesés („shoulder surfing”)	37
Mézesbödön (“honeypot”).....	37
Munkamenet ellopása, eltérítése (“session hijacking”)	37
Nulladik napi sebezhetőség („zero day vulnerability”).....	37
Nyers erő alapú támadás („brute-force attack”).....	37
Rosszindulatú program (“malware”).....	38
Sérülékenységvizsgáló eszköz („vulnerability scanner”)	38
SQL befecskendezés („SQL injection”)	38
Sütimérgezés (“cookie poisoning”)	38
Szivárvány tábla („rainbow table”).....	38
Szolgáltatás megtagadásos támadás („Denial Of Service”, „DOS”).....	38
Trójai programok („trojan”)	39

Ujjlenyomatkészítés ("fingerprinting").....	39
Vadon ("wild")	39
Vírus („virus”)	39
Visszafejtés („reverse engineering”).....	40
Zombihálózat („botnet”)	40
Zsaroló programok („ransomware”).....	40
3. TÁMADHATÓ CÉLPONTOK A MINDENNAPOKBAN	41
3.1. Okos tévék.....	42
3.2. Otthoni internetkapcsolatok típusai.....	43
3.3. Az internethozzáférés biztonsága.....	45
3.4. Böngésző bővítmények	46
3.5. Figyeljünk oda az URL-ekre!	47
3.6. Az operációs rendszerek	48
3.7. Mobileszközök.....	49
3.8. A dolgok internete	51
3.9. A „felhő” technológiáról	52
3.10. Virtuális valóság.....	52
3.11. Önvezető autók	53
3.12. Víruskeresők használata	53
3.13. Anonim internetezés.....	54
3.13.1. Privát böngészés	54
3.13.2. Virtuális magánhálózatok.....	56
3.13.3. Proxyk használata.....	57
3.13.4. Adatok küldése e-mail postafiók nélkül.....	58
3.14. A Tor hálózatról	59
3.15. Online fizetés és bankolás	60
3.16. Közösségi média és a megosztások	62
3.17. Hogyan ismerjük fel egy ellenünk végrehajtott támadást?..	63
4. SOCIAL ENGINEERING:	
AZ EMBER, MINT BIZTONSÁGI KOCKÁZAT	68
4.1. Munkahelyi példa	68
4.1.1. Azok a telefonhívások... ..	70
4.1.2. A biztonsági szolgálatok felelősségéről	72
4.2. Otthoni példa.....	72
4.3. Email alapú támadások.....	74
4.4. Közösségi hálózatok veszélyei	76
5. ADATTÁROLÓK BIZTONSÁGA.....	77
5.1. A biztonsági másolatok fontossága.....	77
5.2. Biztonsági mentések - SyncToy.....	79
5.3. Adatok biztonságos törlése.....	80

5.4.	Egy speciális terület: meghajtók klónozása	82
5.5.	DriveImage XML és MiniTool Partition Wizard Free.....	83
5.6.	Hálózati meghajtók, meghajtók megosztása.....	84
5.7.	Belső hálózat feltérképezése, erőforrások támadása.....	86
5.8.	Mobileszközök.....	86
6.	TITKOSÍTÁS	87
6.1.	Titkosítási módszerek.....	87
6.2.	Ujjlenyomatok, hash-ek.....	88
6.2.1.	MD5.....	89
6.3.	Rejtjelezés	90
6.4.	Szövegek rejtjelezése.....	92
6.5.	Fájlok rejtjelezése.....	95
6.6.	Meghajtók titkosítása kereskedelmi szoftverekkel	97
7.	KALI LINUX - BIZTONSÁGI TESZTELÉS FELSŐ FOKON	98
7.1.	A Kali Linux telepítése	98
7.2.	Windowsról történő telepítés.....	99
7.3.	Linux alól történő telepítés	100
7.4.	Egyéb telepítési módok	101
7.5.	Gyors áttekintés.....	102
8.	HÁLÓZATI HOZZÁFÉRÉSEK ELLENI TÁMADÁSOK	106
8.1.	Információgyűjtés	106
8.2.	WIFI jelszó feltörése - Reaver	109
8.3.	Offline WIFI jelszótörés - Cowpatty	115
8.4.	Androidos hotspot feltörése	118
8.5.	Védekezési javaslatok routerekhez.....	118
9.	JELSZAVAK ELLENI TÁMADÁSOK.....	122
9.1.	Milyen egy jó jelszó?.....	122
9.2.	Jelszógeneráló	126
9.3.	Jelszavak feltörése	126
9.4.	Apropó véletlenszerűség... ..	127
9.5.	Miért kellene jelszólisták?	128
9.5.1.	Egy szóból alkotható variációk száma.....	128
9.5.2.	Pontosabb becslések	129
9.6.	A jelszavak feltöréséről	130
9.6.1.	Brute force módszer.....	131
9.6.2.	Gyors jelszótörés	133
9.7.	Windows jelszó feltörése, visszaszerzése	136
9.7.1.	A Windows jelszavak tárolása.....	136
9.7.2.	Módszer lustáknak	137
9.7.3.	Látványos módszer.....	138

10. BILLENTYŰNAPLÓZÁS.....	143
10.1. Egy billentyűnaplózó program	144
11. WEBES TÁMADÁSOK.....	146
11.1. Hogyan zajlik egy hálózati támadás?.....	146
11.2. Információ gyűjtése webserverről	147
11.3. Google.....	149
11.3.1. Keresés csak adott weboldalon.....	150
11.3.2. Keresés URL-ekben.....	150
11.3.3. Fájltípusok keresése.....	151
11.4. Tesztkörnyezet létrehozása: WAMP szerver	149
11.5. Könyvtárbejárás.....	159
11.6. Komplex elemzés végrehajtása	162
11.7. Forráskódelemzés és kód módosítása - Firefox Developer toolbar	163
11.8. Weboldal tükrözése - cURL	165
11.9. Teljes weboldalak tükrözése - HTTrack.....	166
11.10. Webes kommunikáció elemzése - Firefox Developer	170
11.11. Adatforgalom lehallgatása - Wireshark.....	170
11.11.1. Haladó információk.....	177
11.12. XSS támadások	178
11.13. SQL befecskendezés.....	184
11.14. Sütimérgezés.....	192
11.14.1. Hibrid technika	193
11.14.2. A Paros Proxy használata	197
11.14.3. Munkamenetek ellopása.....	202
11.15. DOS támadások.....	202
11.16. Tártúlcsordulás előidézése.....	205
11.17. Weblapépítő keretrendszerek	205
12. ZÁRSZÓ HELYETT	207
13. FÜGGELÉK.....	208
13.1. Hasznos weboldalak.....	208
13.2. Ajánlott irodalom	209
13.3. A Reaver kapcsolói	211
13.4. Windowsos parancssoros gyorstalpaló	212
13.4.1. Hálózati parancsok.....	213
13.4.2. Információgyűjtés a számítógépről.....	217
13.5. Egy billentyűnaplózó program forráskódja	220
13.6. Tíz hatványai	222
13.7. Informatikai mértékegységek.....	223

ELŐSZÓ

A mindennapjainkat átszövő informatikai megoldásokat sokszor tudatosan használjuk, ám legtöbbször talán nem is gondolunk ebbe bele. Használatuk során információkhoz jutunk és információkat osztunk meg magunkról. Ezt úgy is szokták mondani, hogy „**digitális lábnyomokat**” hagyunk magunk után. Napjainkban az információ sok esetben olyan értéket képvisel, amit közvetlen, vagy közvetett módon pénzzé lehet tenni, vagy más módon hasznot lehet belőle húzni. Ez pedig sajnos történhet rossz szándékkal is.

A korábban csak a televíziók képernyőjén látott „kiberbűnözők” manapság teljesen megszokott szereplőivé váltak a hétköznapiaknak, naponta olvasunk, hallunk híreket arról, hogy támadás ért egyik vagy másik weboldalt, számítógépes rendszert. A kiberbűnözők és a védekező oldal állandó versenyfutásban vannak, melyben a támadó oldal van előnyben, mert gyorsabban ki lehet használni egy biztonsági rést, mint kidolgozni és elkészíteni az ellenszerét, különösen úgy, hogy nem is tudunk róla.

A számítógépes bűnözők olyan emberek, akik jogtalanul szereznek és használnak fel információkat. Ők a **crackerek**, támadók, akik a **hackerektől** eltérően többnyire etikátlanul járnak el. A hacker szót tehát valójában tévesen használják gyűjtőfogalomként a „bűnözők”-re. Erre később még visszatérünk.

E könyvben különböző támadási módszereket szeretnénk megismertetni a nagyközönséggel, bemutatva olyan technikákat is, melyeket magas szinten a valóságban is használnak a rossz fiúk. Az ellenük történő védekezésnek ugyanis a megismerés a legbiztosabb alapja. Ez a könyv nem a (potenciális) bűnözőknek szól és nem hivatott senkit sem felkészíteni arra,

hogy törvénybe ütköző cselekedeteket hajtson végre. Éppen ellenkezőleg! Óva intünk ettől mindenkit.

A legáltalánosabb hackelési technikák bemutatása mellett a hétköznapi emberek számára kívánunk tanácsokkal szolgálni. Olyan tanácsokkal, melyek segítségével hatékony válaszokat tud adni a napjainkra egyre inkább terjedőben levő informatikai bűnözés kihívásaira. A védekezés felé megtett első lépés a megértés. Mivel állunk szemben? Mit jelentenek a különböző szak kifejezések? Hogyan férhetnek hozzá adatainkhoz? A megértés teszi lehetővé a védekezési módok meglátását és keresését.

Célkeresztben az információ

Az informatika világában az értéket az információ képviseli. Az információ körül forog minden. Minél több van belőle, annál értékesebb lesz. Ha bizalmas információkról van szó, az tovább növeli az információ értékét. (Nagyon tágran értelmezve, kvázi a bankszámlán lévő pénz is csupán információ.)

Napjainkban két, egymással ellentétes folyamat figyelhető meg a hétköznapiakban: az emberek egyre több információt tesznek közzé magukról, miközben egyre nagyobb erőfeszítések szükségesek az információk védelme érdekében. Ebből egyenesen következik, hogy az információkhoz történő jogosulatlan hozzáférések száma is egyre nagyobb lesz.

Gondolatok a személyes adatokról

Könyvünk megírásának kezdetén egy dilemmával találtuk magunkat szembe: hogyan adhatunk tanácsot az embereknek bizalmas adataik védelmével kapcsolatban, hogy közben ne adjunk akaratlanul is ötleteket arra vonatkozóan, hogy hogyan lehet ilyen információkat megszerezni? Stratégiánk az, hogy a különböző módszerek inkább általános, példaszzerű leírását és az ellenük történő védekezés lehetőségeit adjuk közre. Az olvasó így ismereteket szerezhet a témában és tudását is gazdagíthatja, anélkül, hogy nagyon el kellene távolodnia a „gyakorlatától”. Az ismeretátadás ezen biztonságos megközelítése alatt értjük annak az ismertetését is, ahogyan egy valódi hacker gondolkodik és dolgozik.

A reklámoknak és a fogyasztás világának köszönhetően az emberek számítástechnikai eszközökkel végzett szinte minden tevékenysége hagy valamilyen nyomot. Ez az ún. digitális lábnyom. Ez lehet egy telefonhívás adatainak rögzítése, egy e-mail elküldése, egy naplófájl, egy elmentett dokumentum, szinte bármi.

A különféle telekommunikációs szolgáltatók, nagy szoftvercégek, hírszerző szervezetek és persze a „szabadúszó” bűnözők is rengeteg információt állítanak össze mindenkiről, aki informatikai eszközöket használ.

Ennek tudatában kell lennünk, mert már a személyes információk keletkezése is szinte észrevétlenül átszövi életünket. Alapvető fontosságú a személyes információk kezelésével kapcsolatos tudatosság kialakítása. Tudnunk kell, hogy személyes adataink csak hozzánk köthetőek, ránk vonatkoznak és senkinek sincsen joga akaraton kívül tárolni, vagy felhasználni azokat. Ennek megértése elsősorban a fiatalabb generációk számára fontos, mivel ők már „beleszületnek” egy olyan világba, ahol rengeteg információ keletkezik és kering körbe-körbe a Földön.

A világ mammutcégei számára hatalmas értéket képviselnek a potenciális vásárlóik szokásai. Talán bele sem gondolunk egy webáruház böngészése közben, hogy nagy valószínűséggel minden mozdulatunkat kiértékelik és rögzítik. Hová kattintunk, mennyi időt töltünk egy-egy oldalon, milyen kifejezésekre keresünk rá és még hosszasan sorolhatnánk. Noha ezen statisztikák mérése és kiértékelése elvileg anonimizált módon zajlik, erre kevés a garancia, és ha így is van, az az igazság, hogy az anonímmá tett adatok jelentős része mégiscsak felhasználható konkrét emberek azonosítására, mint azt több kutatás utólag bebizonyította. Ezért aztán könyvünk az információ védelméről is szól és bemutatja az információk jogosulatlan megszerzésére törekvő ellenoldal egyes módszereit is.

Félreértés ne essék: nem paranoiás szemlélet kialakítása a célunk! Ez már a ló túloldalára történő átesés lenne. Ellenben igenis célunk egy egészséges, felvilágosult szemlélet kialakítása

arról, mi történik, és mi történhet adatainkkal ilyen vagy olyan esetekben és hogyan befolyásolhatjuk ezt.

A könyvünkben leírt ismeretanyag továbbá azt a biztonsági tudatosságot is terjeszteni kívánja, ami számos munkahelyen sajnos még manapság is hiányzik.

A könyv felépítése

Könyvünk felépítése messzemenően gyakorlatorientált. A fejezeteket igyekeztünk hétköznapi élethelyzetek köré felépíteni és sok példával illusztrálni. Több esetben szoftvereket is bemutatunk, melyeket a jó és a rossz oldalon álló szakemberek egyaránt felhasználnak védekezésre, ill. támadásra is.

A fejezetek tárgyalásakor a fokozatosság elvét alkalmazzuk. Az első két fejezetben alapfogalmakat tisztázunk és igyekszünk megvetni az alapjait a biztonságtudatos gondolkodásnak.

Miután megismertük azt, hogy miről fog szólni a könyv, a 3-6. fejezetekben biztonsági kockázatokról ejtünk szót, egyszerű, laikusok által is könnyen megérthető formában. Itt már néhány egyszerű gyakorlati példát is mutatunk.

A könyv második fele (7-11. fejezetek) különféle támadási és védekezési módszereket mutat be, melyek már némi számítás-technikai jártasságot igényelnek, de könnyen kipróbálhatóak, mivel lépésről lépésre leírunk mindent. Itt tehát már zömében gyakorlati példákkal találkozhatunk és a példák komplexebbek is lehetnek. Egyre több alkalmazást és módszert, valamint ezek kombinációját mutatjuk be, mely már valóban megközelíti a valódi támadók módszereit.

A könyv végén lévő függelék számos hivatkozást tartalmaz, melyek segítségével tovább bővíthetjük ismereteinket, illetve utat találhatunk egy-egy speciálisabb téma felé is. Szintén a függelékben kaptak helyet olyan információk is, melyek a könyv fejezeteinek sorába nem kerültek bele, de hasznosak, érdekesek lehetnek a könyv témaköreivel történő ismerkedés során.

Nem minden módszert, technikát mutatunk be, ez jóval meg is haladná egy könyv kereteit. Mégis igyekeztünk olyan témá-

kat válogatni, melyekkel hétköznapiakban gyakran találkozhatunk, illetve minél több területet lefednek.

A valódi hackerek folyamatosan naprakészen tartják tudásukat és fejlesztik magukat. Erre biztatjuk olvasóinkat is, és ehhez könyvünk is kiváló ugródeszka lehet. Egy könyv elolvasása után azonban még senkiből nem lesz profi hacker. Ehhez rengeteg gyakorlat, komoly tudás és kitartás szükséges.

A könyvben bemutatott módszerek kipróbálásáról

A könyv példáinak kidolgozásához elszigetelt tesztkörnyezetet, illetve saját hálózatot használtunk. Ezt javasoljuk olvasóinknak is. Óvva intünk mindenkit attól, hogy olyan tevékenységekbe kezdjen, ami külső szolgáltatások megzavarására, vagy egyéb károkozásra alkalmas. Ezekért nem vállalunk felelősséget!

Általánosságban elmondható, hogy saját hálózatunk vagy jelszavaink feltörése tökéletesen elégséges egy-egy módszer működésének a megismeréséhez. Szóval első felbuzdulásunkban ne kezdjük el vadul feltörni a szomszéd vegyesbolt WIFI jelszavát, mert annak rossz vége lehet...

A szerzőről

A szerző veterán szoftvertesztelő, minőségbiztosítási tanácsadó, Magyarországon dolgozik. 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. Néhány vonatkozó segédprogramjával ebben a könyvben is találkozni fogunk.

Sok időt fordít saját térinformatikai keretrendszerének fejlesztésére, a ZEUSZ-ra, mellyel a NASA-ig is eljutott.

Az Adobe Flash platform és az AIR keretrendszer, valamint az Android operációs rendszer lelkes híve.

Több könyve is megjelent már a hazai könyvesboltokban. Munkáiról bővebben a <http://feherkrisztian.magix.net/public> weboldalon is lehet olvasni.