

**Fehér Krisztián**

# **Hackertechnikák**

Útmutató valódi hacker módszerek  
biztonságos kipróbálásához



**Fehér Krisztián**

# **Hacker- technikák**

Útmutató valódi hacker módszerek biztonságos kipróbálásához

BBS-INFO Kiadó, 2018.

**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, Tel.: 407-17-07 [info@bbs.hu](mailto:info@bbs.hu)

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.

**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

<b>1. Bevezetés.....</b>	<b>8</b>
1.1. Új könyv, régi elvek.....	8
1.2. A szerzőről.....	8
1.3. A könyv szerkezete.....	9
<b>2. Merre tart a világ? .....</b>	<b>10</b>
2.1. Linux, még biztonságosabban?.....	11
2.1.1. Bastille Linux segédprogram.....	11
2.1.2. Astra Linux operációs rendszer.....	12
<b>3. Az etikusság kérdése .....</b>	<b>13</b>
3.1. Mitől etikus egy hacker?.....	13
<b>4. Alapvető eszközök beszerzése hackeléshez .....</b>	<b>15</b>
4.1. Számítógép.....	15
4.2. Alapszoftverek .....	15
4.3. Wifi adapterek .....	16
4.3.1. Chipkészlet mizéria.....	17
4.3.2. Ajánlott eszközök .....	19
4.3.3. Eszközök kipróbálása Linux alatt, tapasztalatok.....	27
<b>5. Tesztkörnyezet kialakítása.....</b>	<b>29</b>
5.1. Újdonságok a Kali Linux háza táján.....	29
5.2. Virtuális gépek használata.....	29
5.2.1. VMWare Player.....	30
5.2.2. Oracle Virtual Box .....	34
<b>6. Információszerzés .....</b>	<b>36</b>
6.1. Régi weblaptartalmak megtekintése.....	36
<b>7. Social engineering.....</b>	<b>40</b>
7.1. Passzív információgyűjtés emberekről.....	40
7.2. Bejutás épületekbe, irodahelyiségekbe .....	41
7.2.1. Liftes változat.....	42

7.3.	Weblapok átirányításának kikényszerítése.....	44
7.4.	QR kód hamisítás.....	46
7.5.	URL rövidítéseken alapuló támadások.....	48
<b>8.</b>	<b>Titkosított levelezés.....</b>	<b>50</b>
8.1.	A Thunderbird levelező telepítése.....	50
8.2.	Postafiók beállítása.....	51
8.3.	OpenPGP telepítése.....	54
8.3.1.	Asszimmetrikus titkosítás.....	55
8.4.	Az Enigmail telepítése.....	56
8.5.	Kulcspár létrehozása.....	59
8.6.	Kulcsok importálása.....	65
8.7.	Levelezés megkezdése, aláírások érvényesítése.....	68
8.8.	További beállítási lehetőségek.....	73
<b>9.</b>	<b>Jelszavak feltörése.....</b>	<b>75</b>
9.1.	Windows jelszavak.....	75
9.2.	Jelszóvédett ZIP fájlok.....	81
<b>10.</b>	<b>MAC cím megváltoztatása.....</b>	<b>84</b>
10.1.	Mi az a MAC cím?.....	84
10.2.	A macchanger használata.....	84
<b>11.</b>	<b>WIFI térkép készítése.....</b>	<b>87</b>
11.1.	A War driver használata.....	87
11.2.	Térképezés.....	90
11.2.1.	OpenStreetMap.....	91
11.2.2.	Geofabrik extraktumok.....	92
11.2.3.	A QGIS Desktop alkalmazása.....	93
11.3.	További megjelenítési lehetőségek.....	98
<b>12.</b>	<b>WIFI adatsomagok és a Wireshark.....</b>	<b>101</b>
12.1.	Adatelemzés a Wireshark segítségével.....	101
12.2.	Mit tartalmaznak a WIFI adatok?.....	102
12.3.	Adatsomag-szűrők alkalmazása a Wiresharkban.....	104
<b>13.</b>	<b>DOS támadás.....</b>	<b>107</b>
13.1.	Mi a DOS támadás?.....	107
13.2.	Wifi hálózat elérhetetlenné tétele.....	107
<b>14.</b>	<b>Trójai program készítése és alkalmazása.....</b>	<b>111</b>
14.1.	A Metasploit framework és az Armitage.....	112
14.2.	Trójai fertőzött PDF fájlban.....	114
14.2.1.	Social Engineering Toolkit.....	115

---

14.2.2. Metasploit framework .....	118
14.3. Trójai készítése és használata Metasploittal .....	122
14.3.1. A végrehajtható állomány létrehozása.....	122
14.3.2. A trójai elindítása tesztkörnyezetben .....	125
14.3.3. A trójai használata.....	126
14.4. Végrehajtható állományok anatómiája .....	131
14.5. Trójai Backdoor Factory használatával.....	132
14.5.1. Friss verzió használata.....	135
<b>15. Törölt adatok visszaállítása.....</b>	<b>137</b>
15.1. Hogyan törlődnek adataink?.....	137
15.2. A Recuva bemutatása .....	138
15.3. Az alapszituáció .....	139
15.4. Adatmentés a Recuva-val .....	139
15.5. Hasznos tanácsok adatmentéshez .....	143
<b>16. Igazságügyi adatelemzések.....</b>	<b>144</b>
16.1. A Kali Linux és igazságügyi elemzések.....	144
16.2. RegRipper.....	145
<b>Záró gondolatok .....</b>	<b>151</b>

# 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 hackerrek 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 elhatárolódkunk. 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 ZEUSZ-ra, 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.