

?

## Hackertechnikák (Fehér Krisztián)



152 oldal, B/5, ISBN 978-615-5477-64-5

Értékelés: Még nincs értékelve

**Ár**

Fogyasztói ár 2290,00 Ft

Kedvezmény-200,00 Ft

[Tegye fel kérdését a termék?](#)

### Leírás

A Kezdő hackerok kézikönyve után jelen kiadvány segítségével értesen gyakorlatorientált módon, haladó szintű kiberbiztonsági témaköröket ismerhet meg és próbálhat ki az olvasó. A hackeléshez használható eszközök beszerzésétől kezdve, újabb jelszófeltörési módszereken át egészen saját trójai programok elállításáig és bevetéséig számos gyakorlati kérdésre találhat választ, mígnem a könyv végére eljuthat az igazságügyi informatika alapvető gyakorlati kérdéseire. Közben pedig olyan témákat érintünk, mint például a MAC cím megváltoztatása, a titkosított levelezés, a törölt állományok visszaállítása, az archív weblaptartalmak megtekintése, a DOS támadás kivitelezése, vagy a számítógépek megfigyelése, illetve az adatelemzések és a korábbi tevékenységek vizsgálata. Sőt, ha esetleg elege lenne abból, hogy a társaságában mindenki a mobilján lógva wifit használ, a könyvben leírtak segítségével például akár azt is megoldhatja, hogy mindenkit ledobjon a rendszer a hálózatról.

Vigyázat! A könyv példái a gyakorlatban is alkalmazhatóak, ezért hangsúlyozzuk az olvasó felelősségét az egyes módszerek kipróbálásánál.

[Könyv megvásárlása e-booként](#)

**Tartalomjegyzék:**

- 1. Bevezetés 8
  - 1.1. Új könyv, régi elvek 8
  - 1.2. A szerzőről 8
  - 1.3. A könyv szerkezete 9
- 2. Merre tart a világ? 10
  - 2.1. Linux, még biztonságosabban? 11
    - 2.1.1. Bastille Linux segédprogram 11
    - 2.1.2. Astra Linux operációs rendszer 12
- 3. Az etikusság kérdése 13
  - 3.1. Mitől etikus egy hacker? 13
- 4. Alapvető eszközök beszerzése hackeléshez 15
  - 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
- 5. Tesztkörnyezet kialakítása 29
  - 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
- 6. Információszerzés 36
  - 6.1. Régi weblaptartalmak megtekintése 36
- 7. Social engineering 40
  - 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
- 8. Titkosított levelezés 50
  - 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
- 9. Jelszavak feltörése 75
  - 9.1. Windows jelszavak 75
  - 9.2. Jelszóvédett ZIP fájlok 81
- 10. MAC cím megváltoztatása 84
  - 10.1. Mi az a MAC cím? 84
  - 10.2. A macchanger használata 84
- 11. WIFI térkép készítése 87
  - 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
- 12. WIFI adatcsomagok és a Wireshark 101
  - 12.1. Adatelemzés a Wireshark segítségével 101
  - 12.2. Mit tartalmaznak a WIFI adatok? 102
  - 12.3. Adatcsomag-szerkezet alkalmazása a Wiresharkban 104
- 13. DOS támadás 107
  - 13.1. Mi a DOS támadás? 107
  - 13.2. Wifi hálózat elérhetetlenné tétele 107
- 14. Trójai program készítése és alkalmazása 111
  - 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
15. Törölt adatok visszaállítása	137
15.1. Hogyan törölődnek 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
16. Igazságügyi adatelemzések	144
16.1. A Kali Linux és igazságügyi elemzések	144
16.2. RegRipper	145
Záró gondolatok	151