?

Kezd? hackerek kézikönyve - avagy informatikai támadások és kivédésük (Fehér Krisztián)





224 oldal, B/5, ISBN 978-615-5477-44-7

Értékelés: Még nincs értékelve
Ár
Fogyasztói ár2700,00 Ft

Kedvezmény-290,00 Ft

Tegye fel kérdését a termékr?l

Leírás

Ha kíváncsi az olyan témákra, mint például hogy miként lehet feltörni egy jelszót, vagy egy webhelyet, esetleg hogyan lehet lehallgatni bárki kommunikációját egy nyílt wifi hálózaton, akkor ez a könyv önnek szól. Sokan azt hiszik, hogy ezek ördöng?s dolgok, pedig egyáltalán nem azok. Éppen ezért fontos, hogy védekezni is kell ellenük, ami szintén nem bonyolult, csak egy kis odafigyelésre van szükség. Könyvünk mindkét oldalt megmutatja, elrettentésképpen a lehet?ségeket, okulásként a védekezési módokat.

Ha ön azt hiszi, hogy biztonságban van, hiszen nem csinál semmi illegálisat és még vírusirtó is van a gépén, akkor nagyon téved! Teljeskör? védelem ugyanis nem létezik! Ha elolvassa ezt a könyvet, meg fog döbbenni, hogy milyen sok támadási lehet?ség van adataink ellen. A könyv, azon túl, hogy ismerteti, mit jelentenek az információbiztonsági szakkifejezések olyan témákkal foglalkozik, mint hogy milyen eszközök támadhatók és hogyan, hogyan dolgozik egy hacker, mekkora kockázatot jelent az emberi tényez? (social engineering), stb. Kitér a jelszavak biztonságára, a különféle hackeléshez használható programok és azok kezelésére, a billenty?zetnaplózási lehet?ségekre, a hálózatok és weboldalak támadására és feltörésére, az online bankolási kockázatokra, a titkosítási módszerekre, illetve hogy mit érdemes tenni a

biztonságos adattárolás érdekében.

Természetesen senkit sem akarunk illegális tevékenységre buzdítani, célunk sokkal inkább azt megmutatni, hogy mekkora veszélynek vagyunk kitéve, ezáltal a támadási és védekezési lehet?ségek bemutatásával ösztönözzük az embereket a biztonságosabb számítógéphasználatra.

Könyv megvásárlása a Libri-nél

Tartalomjegyzék:

EL?SZÓ 10

1. HACKER TÖRTÉNELEM 15

1.1. A „hacker” szó eredetér?l és értelmezésér?l 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 módszerekr?l 20

1.7. A hackercsoportok jöv?je 20

1.8. Elit hackercsoportok és a politika 21

2. INFORMATIKAI TÁMADÁSOK MADÁRTÁVLATBÓL 23

2.1. Gondolatok az adatvédelemr?l 23

2.2. A biztonság mítosza 25

2.3. Visszaélések típusai 26

2.4. Adatbiztonság és adatvédelem 27

2.4.1. Adatbiztonsági fenyegetettségek 27

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

Szkriptkölyök („script kiddies”) 31

Hacktivista („hacktivist”) 31

Telefon hacker („phreaker”) 31

2.6. Támadások, támadóeszközök, szakkifejezések 32

Adathalászat („Spoofing attack, phishing”) 32

Aranymosás 32

Befecskendezés ("injection") 32

Betör? készlet („rootkit”) 32

Billenty?naplózás („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

Közbeékel?déses támadás („man-in-the-middle attack”) 36

Köztes oldalon keresztül történ? szkripthívás

(„Corss-site scripting, XSS”) 36

Kriptográfia („cryptography”) 36

Kriptovírus („crypto virus”) 36

Lábnyomkészítés ("footprinting") 36

MAC cím hamisítás („MAC spoofing”) 36

Meglesés („shoulder surfing”) 37

Mézesbödön ("honeypot") 37

Munkamenet ellopása, eltérítése ("session hijacking") 37

Nulladik napi sebezhet?ség („zero day vulnerability”) 37

Nyers er? 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 („reverese 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. Böngész? b?vítmények 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 „felh?” technológiáról 52

3.10. Virtuális valóság 52

3.11. Önvezet? autók 53

3.12. Víruskeres?k 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 felel?sségér?l 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. Bels? hálózat feltérképezése, er?források 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 FELS? FOKON 98

7.1. A Kali Linux telepítése 98

7.2. Windowsról történ? telepítés 99

7.3. Linux alól történ? telepítés 100

7.4. Egyéb telepítési módok 101

7.5. Gyors áttekintés 102

8. HÁLÓZATI HOZZÁFÉRÉSEK ELLENI TÁMADÁSOK 106

8.1. Információgy?jtés 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 véletlenszer?ség… 127

9.5. Miért kellenek jeszólisták? 128

9.5.1. Egy szóból alkotható variációk száma 128

9.5.2. Pontosabb becslések 129

9.6. A jelszavak feltörésér?l 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. BILLENTY?NAPLÓZÁS 143

10.1. Egy billenty?naplózó program 144

11. WEBES TÁMADÁSOK 146

11.1. Hogyan zajlik egy hálózati támadás? 146

11.2. Információ gy?jtése webszerverr?l 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 el?idézése 205

11.17. Weblapépít? 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. Információgy?jtés a számítógépr?l 217

13.5. Egy billenty?naplózó program forráskódja 220

13.6. Tíz hatványai 222

13.7. Informatikai mértékegységek 223