Sadržaj

UVOD 1
O knjizi 1
Pretpostavke 2
Ikonice upotrebljene u knjizi 2
Uz knjigu 3
Kada završite sa čitanjem 3

DEO 1: POSTAVLJANJE TEMELJA ZA TESTIRANJE BEZBEDNOSTI 5

POGLAVLJE 1: **Uvod u testiranje ranjivosti i neprobojnosti** 7
Terminologija 7
Haker 8
Zlonamerni korisnik 9
Zlonamerni napadači i etički hakeri 9
Testiranje ranjivost i neprobojnosti i provera bezbednosti 10
Smernice za testiranje bezbednosti 11
Usklađenost i regulatorna pitanja 11
Zašto treba da hakujete svoje sisteme 12
Opasnosti sa kojima se suočavaju sistemi 13
Netehnički napadi 13
Napadi na mrežnu infrastrukturu 14
Napadi na operativne sisteme 14
Aplikacije i drugi specijalizovani napadi 15
Poštovanje principa procene bezbednosti 15
Poštovanje hakerske etike 15
Poštovanje privatnosti 16
Bez padova sistema 16
Pokretanje testa ranjivosti i neprobojnosti 17
Izrada plana 17
Izbor alatki 19
Sprovođenje plana 20
Procena rezultata 22
Primena preporuka 22

POGLAVLJE 2: **Kako razmišljaju hakeri** 23
Protiv čega se borite 23
Ko provaljuje u računarske sisteme 26
Tehnička znanja i veštine hakera 26
Motivacija hakera 27
Zašto to rade 28
Planiranje i izvođenje napada 31
Čuvanje anonimnosti 33

POGLAVLJE 3: **Priprema plana za testiranje bezbednosti** . . . 35
Definisanje ciljeva . . . 35
Biranje sistema za testiranje . . . 38
Definisanje standarda testiranja . . . 40
Pravi trenutak za testiranje . . . 40
Posebni testovi . . . 41
Procena sistema sa informacijama o njemu ili bez njih . . . 42
Izbor lokacije . . . 43
Odgovor na pronađene ranjivosti . . . 43
Pretpostavke . . . 44
Izbor alatki za procenu bezbednosti . . . 44

POGLAVLJE 4: **Metodologija hakovanja** . . . 47
Priprema za testiranje . . . 47
Posmatranje iz perspektive drugih . . . 49
Sistemi za skeniranje . . . 50
Hostovi . . . 50
Otvoreni priključci . . . 51
Šta se izvršava na otvorenim priključcima . . . 51
Procenjivanje ranjivosti . . . 54
Iskorišćavanje ranjivosti . . . 55

DEO 2: TESTIRANJE NA DELU . . . 57

POGLAVLJE 5: **Prikupljanje informacija** . . . 59
Prikupljanje javnih informacija . . . 59
Društveni mediji . . . 60
Pretraživanje veba . . . 60
Programi tragači . . . 61
Veb lokacije . . . 62
Mapiranje mreže . . . 62
WHOIS pretraživanje . . . 62
Pravilnik o privatnosti . . . 64

POGLAVLJE 6: **Socijalni inženjering** . . . 65
Šta je socijalni inženjering . . . 65
Testiranje pomoću socijalnog inženjeringa . . . 66
Zašto napadači koriste socijalni inženjering . . . 67
Posledice . . . 68
Sticanje poverenja . . . 69
Iskorišćavanje odnosa . . . 69
Napadi socijalnim inženjeringom . . . 72
Definisanje cilja . . . 72
Potraga za informacijama . . . 72
Mere protiv socijalnog inženjeringa . . . 77
Pravila . . . 77
Podizanje svesti i obuka korisnika . . . 77

POGLAVLJE 7: **Fizička bezbednost** 81
Najvažnije slabe tačke fizičke bezbednosti 82
Pronalaženje fizičkih ranjivosti u poslovnom prostoru 83
Infrastruktura objekta 83
Instalacije 84
Raspored u poslovnom prostoru i kako se koristi 86
Komponente mreže i računari 88

POGLAVLJE 8: **Lozinke** 93
Ranjivost lozinki 94
Organizacione ranjivosti lozinki 94
Tehničke ranjivosti lozinki 95
Provaljivanje lozinki 96
Provaljivanje lozinki na tradicionalan način 96
Provaljivanje lozinki pomoću alatki visoke tehnologije 99
Provaljivanje datoteka zaštićenih lozinkom 107
Ostali načini za provaljivanje lozinki 108
Opšte mere protiv provaljivanja lozinki 113
Čuvanje lozinki 114
Definisanje pravila o lozinkama 114
Ostale mere zaštite 115
Zaštita operativnih sistema 117
Windows 117
Linux i Unix 118

DEO 3: HAKOVANJE MREŽNIH HOSTOVA 119

POGLAVLJE 9: **Sistemi mrežne infrastrukture** 121
Šta su ranjivosti mrežne infrastrukture 122
Biranje alatki 123
Programi za skeniranje i analizatori 123
Procenjivanje ranjivosti 124
Skeniranje i provociranje mreže 124
Priključci za skeniranje 125
Skeniranje SNMP protokola 130
Otimanje zaglavlja 132
Testiranje pravila mrežnih barijera 133
Analiziranje mrežnih podataka 135
MAC-daddy napad 141
Testiranje napada uskraćivanjem usluga 146
Otkrivanje najčešćih slabosti rutera, komutatora i mrežnih barijera . . . 149
Pronalaženje neobezbeđenih interfejsa 149
Otkrivanje problema sa protokolima SSL i TLS 150
Uspostavljanje opšte odbrane mreže 150

POGLAVLJE 10: **Bežične mreže** 153
Posledice ranjivosti bežičnih mreža 153
Biranje alatki 154
Otkrivanje bežičnih mreža 156
Provera globalnog prepoznavanja 156
Skeniranje lokalnih vazdušnih talasa 157
Otkrivanje napada na bežičnu mrežu i sprovođenje mera zaštite 158
Šifrovani saobraćaj 160
Mere protiv napada na šifrovani saobraćaj 164
Zaštićeno podešavanje Wi-Fi mreže 165
Mere protiv ranjivosti WPS PIN-a 167
Piratski bežični uređaji 168
Mere protiv piratskih bežičnih uređaja 171
Lažiranje MAC adresa 172
Mere protiv lažiranja MAC adresa 175
Problemi fizičke bezbednosti 175
Mere protiv problema fizičke bezbednosti 176
Ranjive bežične radne stanice 176
Mere protiv ranjivosti bežičnih radnih stanica 177
Unapred zadati parametri 177
Mere protiv iskorišćavanja unapred zadatih parametara 177

POGLAVLJE 11: **Mobilni uređaji** 179
Merenje ranjivosti mobilnih uređaja 179
Provaljivanje lozinki laptop računara 180
Biranje alatki 180
Primena mera zaštite 184
Provaljivanje lozinki telefona i tablet računara 185
Provaljivanje iOS lozinki 186
Primena mera protiv provaljivanja lozinki 189

DEO 4: HAKOVANJE OPERATIVNIH SISTEMA 191

POGLAVLJE 12: **Windows** 193
Uvod u ranjivosti Windows sistema 194
Biranje alatki 195
Besplatne Microsoft alatke 195
Univerzalne alatke za procenu 196
Alatke za posebne namene 196
Prikupljanje informacija o ranjivostima Windows sistema 197
Skeniranje sistema 197
NetBIOS 199
Otkrivanje anonimnih sesija 202
Mapiranje 202
Prikupljanje informacija 203
Mere protiv hakovanja anonimnih sesija 205

Provera dozvola za deljene resurse 206
Unapred zadate vrednosti za Windows. 207
Testiranje 208
Iskorišćavanje nezakrpljenih propusta 208
Korišćenje alatke Metasploit 211
Mere protiv iskorišćavanja ranjivosti nastalih zbog nezakrpljenih propusta 215
Pokretanje skeniranja sa proverom identiteta 216

POGLAVLJE 13: **Linux i macOS** 219
Razumevanje Linux ranjivosti 220
Izbor alatki 220
Prikupljanje informacija o ranjivosti sistema 221
Skeniranje sistema 221
Mere protiv skeniranja sistema 224
Nalaženje nepotrebnih i nesigurnih servisa 225
Skeniranje sistema 225
Mere protiv napada na nepotrebne usluge 227
Zaštita datoteka .rhosts i hosts.ekuiv 229
Hakovanje korišćenjem datoteka hosts.equiv i .rhosts. 229
Mere protiv napada na datoteke .rhosts i hosts.equiv 230
Procena bezbednosti NFS 232
NFS hacks. 232
Mere protiv napada NFS-a. 232
Provera ovlašćenja datoteka. 233
Hakovanje dozvola datoteka. 233
Mere protiv hakovanja dozvola datoteka 233
Pronalaženje ranjivosti prepunjavanjem bafera 234
Napadi 234
Mere protiv napada prepunjenog bafera 235
Provera fizičke sigurnost 235
Fizičko ugrožavanje sigurnosti 235
Mere protiv fizičkih napada na bezbednost 236
Izvršavanje opštih sigurnosnih testova 237
Krpljenje 238
Ažuriranje distribucija 239
Višeplatfomski menadžeri ažuriranja 239

DEO 5: HAKERSKE APLIKACIJE 241

POGLAVLJE 14: **Sistemi za komunikaciju i razmenu poruka** 243
Uvod u ranjivosti sistema za razmenu poruka. 243
Prepoznavanje i borba protiv napada na e-poštu 244
Bombardovanje e-poštom 244
Zaglavlja 248
Napadi na SMTP 249
Opšti najbolji postupci za smanjivanje rizika po sigurnost pošte . . . 258

Razumevanje VoIP protokola 259
VoIP ranjivosti 260
Mere protiv VoIP ranjivost 264

POGLAVLJE 15: **Veb aplikacije i aplikacije za mobilne uređaje** 265
Izbor alata za testiranje sigurnosti na vebu 266
Traženje Web ranjivosti 267
Pregled direktorijuma 267
Mere protiv pregleda direktorijuma 270
Napadi filtriranja ulaza 271
Mere protiv napada preko polja za upis 278
Unapred zadati script napad 278
Mere protiv unapred zadatih skript napada 280
Nesigurni mehanizmi prijavljivanja 280
Mere za nezaštićene sisteme za prijavu 283
Izvršavanje opštih sigurnosnih skeniranja za proveru ranjivosti veb aplikacije 284
Smanjivanje veb sigurnosnih rizika 284
Sigurnost pomoću nevidljivosti 285
Postavljanje mrežne barijere 286
Analiziranje izvornog koda 286
Otkrivanje mana mobilne aplikacije 287

POGLAVLJE 16: **Baze podataka i sistemi skladištenja** 289
Zaronimo u baze podataka 289
Izbor alata 290
Pronalaženje baza podataka na mreži 290
Provaljivanje lozinki baze podataka 291
Skeniranje baza podataka na ranjivosti 292
Sledimo najbolje postupke za smanjivanje sigurnosnih rizika 293
O sistemima za skladištenje 294
Izbor alata 294
Pronalaženje sistema za skladištenje na mreži 295
Iskorenjivanje poverljivih sadržaja u datotekama na mreži 296
Držimo se najboljih postupka za smanjivanje rizika za skladištenje podataka 297

DEO 6: POSLE TESTIRANJA SIGURNOSTI 299

POGLAVLJE 17: **Izveštavanje o rezultatima** 301
Sakupljanje podataka 302
Određivanje prioriteta ranjivosti 303
Izrada izveštaja 304

POGLAVLJE 18: **Zatvaranje sigurnosnih rupa** 307
Pretvorite izveštaje u akciju 307
Krpljenjem do savršenstva 308

Upravljanje zakrpama 309
Automatizacija 309
Jačanje sistema 310
Procena sigurnosne infrastrukture 311

POGLAVLJE 19: **Upravljanje sigurnosnim procesima** 313
Automatizacija procene sigurnosti. 313
Nadgledanje zlonamerne upotrebe. 314
Angažovanje spoljnih saradnika za procenu sigurnosti 316
Podizanje svesti o sigurnosti. 317
Održati korak sa sigurnosnim naporima drugih 319

DEO 7: DEO SA DESET SAVETA 321

POGLAVLJE 20: **Deset saveta kako da budete prihvaćeni kao stručnjak za sigurnost** 323
Stvorite saveznika i podršku 323
Ne budite katastrofičar 324
Pokažite da organizacija ne može priuštiti sebi da bude hakovana 324
Istaknite opšte koristi testiranja sigurnosnosti 325
Pokažite kako testiranje sigurnosti na specifičan način može da pomogne vašoj organizaciji 325
Uključite se u posao 326
Uspostavite svoj kredibilitet 326
Razgovarajte jezikom uprave 326
Prikažite vrednost vašeg truda 327
Budite fleksibilni i prilagodljivi 327

POGLAVLJE 21: **Deset razloga zašto je hakovanje jedini uspešan način za testiranje** 329
Loši momci misle loše, koriste dobre alatke i razvijaju nove metode. . . 329
IT upravljanje i usaglašavanje 330
Ranjivost i detaljni testovi dopunjuju kontrolne i sigurnosne procene . . . 330
Klijenti i partneri će vas pitati koliko su sigurni vaši sistemi. 330
Zakon o proseku funkcioniše protiv kompanija. 331
Sigurnosne procene poboljšavaju razumevanje pretnji za poslovanje . . . 331
Ako se dogodi sigurnosni proboj, morate imati nešto na šta se možete osloniti. 331
Detaljno testiranje iznosi ono najgore u sistemima 332
Kombinovano testiranje ranjivosti i neprobojnosti 332
Odgovarajuće testiranje može da otkrije slabosti koje ste prevideli. . . . 332

POGLAVLJE 22: **Deset smrtnih grešaka** 333
Nedobijanje odobrenja 333
Pretpostavka da možete pronaći sve ranjivosti 334
Pretpostavka da možete ukloniti sve ranjivosti 334
Jednokratno testiranje 334
Mislite da sve znate 335
Testiranje bez gledanja na stvari iz perspektive hakera 335

Ne testirate prave sisteme 335
Ne koristite dobre alatke 335
Testiranje proizvodnih sistema u pogrešno vreme 336
Angažovanje spoljnih saradnika za testiranje 336

DODATAK: SPISAK ALATA I KORISNIH VEB STRANA 337

SPISAK TERMINA KORIŠĆENIH U KNJIZI 351

INDEKS 353