SARADNICI

O AUTORU

Šiva V. N. Parasram je konsultant za računarsku bezbednost i rizike sa više od 19 godina iskustva i izvršni direktor instituta **Computer Forensics and Security Institute (CFSI)**, specijalista za testiranje proboja, **digitalnu forenziku i odgovor na incidente (DFIR)** i naprednu obuku iz bezbednosti sa globalnim dosegom. Kao jedini sertifikovani **EC-Council instruktor (CEI)** na Karibima, obučio je hiljade ljudi i osnivač je programa CFSI CyberFence. Takođe, Šiva je autor još tri knjige koje je objavio izdavač Packt Publishing i držao je regionalne i globalne radionice za ISACA, ISC2, univerzitete i bezbednosne agencije. Takođe je konsultant za upravljanje bezbednosnim rizicima za PTRMS (Kanada) unutar globalne finansijske institucije, kao i mentor za računarsku bezbednost u Springbordu (SAD).

Želim da zahvalim timu izdavačke kuće Packt (Šrileki, Šonu, Adriji i Prači) na njihovoj podršci; tehničkim recenzentima, Aleksu Semu i Deodatu Gangi; mom guruu, Pt. Persadu; mojim roditeljima, Hariju i Indri; mojoj supruzi, Savi; voljenom Bindi; i dr. Mali, dr. Nilašu Ramnarineu i dr. Šaradu Mohipu. Takođe moram da zahvalim svim prijateljima koji su bili uz mene tokom mojih najtežih trenutaka, u poslednje vreme. Posebno hvala i porodici CFSI. Zaista sam blagosloven.

O RECENZENTIMA

Aleks Sem ima više od 10 godina iskustva u oblasti računarske bezbednosti, sa primarnim fokusom na testiranje proboja i crvene timove. Obavljao je testiranja proboja za organizacije finansijskog sektora, obrazovne i javne službe, naftne i gasne industrije, kao i za državne entitete. Takođe je sprovodio odgovor na incidente i digitalnu forenziku za finansijske institucije i druge državne entitete.

Trenutno radi u kompaniji BDO B.V. kao konsultant u timu za savetodavne usluge, gde pruža usluge koje obuhvataju testiranje proboja, procene ERP sistema, analitiku podataka, procene IT rizika i druge digitalne usluge.

Želim da zahvalim svojoj porodici na podršci koju mi pruža. Oni su podsticali moju opsesiju tehnologijom i motivisali me da više učim. Veliko hvala mojim prijateljima koji me podsećaju da nađem vreme za opuštanje.

Deodat Ganga je profesionalac u oblasti informacione bezbednosti i mrežnih tehnologija sa više od 20 godina radnog iskustva. On je viši savetnik za bezbednost i konsultant koji obavlja funkciju menadžera tehnološkog rizika u globalnom bankarskom sektoru. Takođe je iskusan tester proboja, istraživač digitalne forenzike i član ljubičastog tima. Takođe, on je iskusan predavač iz oblasti računarske bezbednosti, koji predaje etičko hakovanje, digitalnu forenzičku istragu i računarsku odbranu. Posvećen je bezbednosti na internetu i radi kao senior službenik za svest o računarskoj bezbednosti i edukuje ljude o opasnostima i načinima zaštite u kibernetičkom prostoru.

Miroslav Ristić je redovni profesor na Prirodno-matematičkom fakultetu Univerziteta u Nišu, sa preko 25 godina iskustva u razvoju statističkog softvera. Posebno se ističe njegov rad na razvoju grafičkog korisničkog interfejsa R Commander za programski jezik R. Dugi niz godina recenzirao je značajan broj knjiga za izdavačku kuću Springer i časopis Journal of Applied Statistics. Od 2023. godine aktivno recenzira najaktuelnija izdanja izdavačke kuće "Kompjuter biblioteka". Nakon prevođenja, svako izdanje prolazi kroz njegovo stručno vrednovanje i recenziju prevoda, sa ciljem da se osigura da prevodi budu ne samo jasni, precizni i prilagođeni čitaocima, već i da održe visok kvalitet i stručnu relevantnost knjiga.



Kratak sadržaj

DEO 1
Osnovni principi plavog i ljubičastog udruživanja 1

POGLAVLJE 1
Osnove crvenog, plavog i ljubičastog udruživanja 3

POGLAVLJE 2
Uvod u digitalnu forenziku 15

POGLAVLJE 3
Instalacija operativnog sistema Kali Linux 45

POGLAVLJE 4
Dodatne instalacije operativnog sistema Kali Linux i zadaci nakon instalacije 81

POGLAVLJE 5
Instaliranje programa Wine na operativnom sistemu Kali Linux 99

DEO 2
Digitalna forenzika i odgovor na incidente Osnove i najbolje prakse 115

POGLAVLJE 6
Koncept sistema datoteka i skladištenja 117

POGLAVLJE 7
Odgovor na incidente, prikupljanje podataka i DFIR radni okviri 141

DEO 3
Alati za digitalnu forenziku i odgovor na incidente u operativnom sistemu Kali Linux 157

POGLAVLJE 8
Alati za prikupljanje dokaza 159

POGLAVLJE 9
Alati za oporavak datoteka i izvlačenje podataka 193

POGLAVLJE 10
Forenzika memorije i analiza pomoću alata Volatility 3 223

POGLAVLJE 11
Analiza artefakata, zlonamernog i ucenjivačkog softvera 245

DEO 4
Automatizovani paketi za digitalnu forenziku i odgovor na incidente 271

POGLAVLJE 12
Forenzički pregledač Autopsy 273

POGLAVLJE 13
Izvođenje kompletne DFIR analize sa Autopsy 4 grafičkim korisničkim interfejsom 291

DEO 5
Alati za forenzičku analizu mreže 311

POGLAVLJE 14
Alati za otkrivanje mreže 313

POGLAVLJE 15
Analiza hvatanja paketa alatom Xplico 329

POGLAVLJE 16
Alati za forenzičku analizu mreže 349

INDEKS 377



Sadržaj

PREDGOVOR XIX

DEO 1
Osnovni principi plavog i ljubičastog udruživanja 1

POGLAVLJE 1

Osnove crvenog, plavog i ljubičastog udruživanja 3

Kako sam počeo da koristim operativni sistem Kali Linux 4
Šta je Kali Linux? 5
Zašto je Kali Linux toliko popularan? 6
Koncept crvenog tima 8
Koncept plavog tima 9
Koncept ljubičastog tima 12
Rezime 14

POGLAVLJE 2

Uvod u digitalnu forenziku 15

Šta je digitalna forenzika? 15
Potreba za plavim i ljubičastim timovima 16
Metodologije i radni okviri digitalne forenzike 18
DFIR radni okviri 20
Poređenje operativnih sistema dizajniranih za digitalnu forenziku 21
Linux distribucija specijalizovana za digitalne dokaze i forenzičku analizu 23
Istražno okruženje sa računarskom podrškom (CAINE) 25
CSI Linux 30
Kali Linux 35
Potreba za raznovrsnim forenzičkim alatima u digitalnim istragama 39
Komercijalni forenzički alati 40
Belkasoft Evidence Centre X 40

Exterro Forensic Toolkit (FTK) 40
OpenText EnCase Forensic 41
Anti-forenzika – pretnje digitalnoj forenzici 41
Šifrovanje 42
Onlajn i oflajn anonimnost 43
Rezime 44

POGLAVLJE 3

Instalacija operativnog sistema Kali Linux 45

Tehnički zahtevi 45
Preuzimanje operativnog sistema Kali Linux 46
Preuzimanje potrebnih alata i slika 48
Preuzimanje Kali Linux Everything torenta 48
Instaliranje operativnog sistema Kali Linux za pokretanje DFIR alata sa prenosivog memorijskog uređaja 50
Instalacija operativnog sistema Kali Linux kao samostalnog operativnog sistema 56
Instalacija operativnog sistema Kali Linux u programu VirtualBox 57
Priprema Kali Linux virtuelne mašine 58
Instalacija operativnog sistema Kali Linux na virtuelnoj mašini 62
Instalacija i konfigurisanje operativnog sistema Kali Linux kao virtuelne mašine ili kao samostalnog operativnog sistema 67
Rezime 80

POGLAVLJE 4

Dodatne instalacije operativnog sistema Kali Linux i zadaci nakon instalacije 81

Instaliranje unapred konfigurisane verzije operativnog sistema Kali Linux u programu VirtualBox 81
Instaliranje operativnog sistema Kali Linux na Raspberry Pi4 uređaju 85
Ažuriranje operativnog sistema Kali Linux 89
Omogućavanje root korisničkog naloga na operativnom sistemu Kali Linux 92
Dodavanje forenzičkog metapaketa operativnog sistema Kali Linux 96
Rezime 97

POGLAVLJE 5

Instaliranje programa Wine na operativnom sistemu Kali Linux 99

Šta je Wine i koje su njegove prednosti na operativnom sistemu Kali Linux 99
Instaliranje programa Wine 100
Konfigurisanje instalacije programa Wine 105
Testiranje instalacije programa Wine 109
Rezime 114

DEO 2
Digitalna forenzika i odgovor na incidente Osnove i najbolje prakse 115

POGLAVLJE 6
Koncept sistema datoteka i skladištenja 117

Istorija i vrste medija za skladištenje ... 118
IBM i istorija medija za skladištenje ... 118
Prenosivi mediji za skladištenje ... 119
Magnetne trake ... 119
Flopi diskovi ... 119
Evolucija flopi diska ... 120
Optički mediji za skladištenje ... 120
Kompaktni diskovi ... 120
Digitalni višenamenski diskovi ... 121
Blu-rej disk ... 122
Fleš mediji za skladištenje ... 122
USB fleš memorije ... 123
Fleš memorijske kartice ... 125
Tvrdi diskovi ... 128
Tvrdi diskovi sa integrisanom elektronikom ... 129
Tvrdi diskovi sa serijskim naprednim tehnološkim priključkom ... 130
SSD diskovi ... 131
Sistemi datoteka i operativni sistemi ... 133
Microsoft Windows ... 133
Macintosh (macOS) ... 134
Linux ... 134
Tipovi podataka i stanja ... 135
Metapodaci ... 135
Rezervni prostor ... 136
Postojani i nepostojani podaci i redosled nestajanja ... 136
Važnost RAM memorije, stranične datoteke i keša u DFIR oblasti ... 138
Rezime ... 139

POGLAVLJE 7
Odgovor na incidente, prikupljanje podataka i DFIR radni okviri 141

Procedure za prikupljanje dokaza ... 142
Odgovor na incident i osoblje koje prvo reaguje ... 143
Prikupljanje dokaza i dokumentovanje ... 144
Fizički alati za prikupljanje dokaza ... 145
Prikupljanje podataka uživo naspram prikupljanja nakon što je sistem prestao sa radom ... 148
Redosled nestajanja ... 148
Prikupljanje podataka sa uključenih ili isključenih uređaja ... 148
Uključeni uređaji ... 149
Isključeni uređaji ... 149

Lanac čuvanja ... 150
Značaj uređaja za blokiranje upisa ... 150
Pretvaranje podataka u slike i održavanje integriteta dokaza ... 151
Heš sažetak poruke (MD5) ... 152
Sigurni algoritam heširanja (SHA) ... 153
Najbolje prakse za prikupljanje podataka i DFIR radni okviri ... 154
DFIR radni okviri ... 155
Rezime ... 156

DEO 3

Alati za digitalnu forenziku i odgovor na incidente u operativnom sistemu Kali Linux ... 157

POGLAVLJE 8

Alati za prikupljanje dokaza ... 159

Korišćenje komande fdisk za prepoznavanje particija ... 160
Identifikacija uređaja komandom fdisk ... 161
Kreiranje jakih heš vrednosti za integritet dokaza ... 163
Kopiranje sa diska pomoću DC3DD alata ... 165
Verifikacija heš izlaza datoteka slika ... 171
Brisanje diska pomoću DC3DD alata ... 171
Kopiranje sa diska pomoću DD alata ... 173
Kopiranje sa diska pomoću alata Guymager ... 175
Pokretanje alata Guymager ... 176
Prikupljanje dokaza alatom Guymager ... 177
Izračunavanje/verifikacija heš vrednosti ... 179
Istraživanje .info datoteke ... 181
Kopiranje sa diska i memorije pomoću alata FTK Imager u programu Wine ... 182
Instaliranje alata FTK Imager ... 182
Kopiranje RAM memorije alatom FTK Imager ... 190
Kopiranje RAM memorije i stranične datoteke pomoću alata Belkasoft RAM Capturer ... 191
Rezime ... 192

POGLAVLJE 9

Alati za oporavak datoteka i izvlačenje podataka ... 193

Osnovne informacije o datotekama ... 194
Preuzimanje uzoraka datoteka ... 194
Oporavak datoteka i izvlačenje podataka pomoću alata Foremost ... 195
Oporavak slika pomoću alata Magicrescue ... 201
Izvlačenje podataka pomoću alata Scalpel ... 205
Izvlačenje podataka pomoću alata bulk_extractor ... 209
Oporavak NTFS sistema pomoću alata scrounge-ntfs ... 214
Oporavak slika pomoću alata Recoverjpeg ... 218
Rezime ... 222

POGLAVLJE 10

Forenzika memorije i analiza pomoću alata Volatility 3 223

Šta je novo u alatu Volatility 3 223
Preuzimanje uzoraka datoteka memorijskih ispisa 225
Instaliranje alata Volatility 3 na operativnom sistemu Kali Linux 225
Analiza memorijskih ispisa pomoću alata Volatility 3 232
Verifikacija slike i operativnog sistema 232
Identifikacija i analiza procesa 234
Dodatak pslist 234
Dodatak pstree 235
Dodatak psscan 236
Dodatak modscan 236
Dodatak getsids 237
Dodatak envars 238
Dodatak hivelist 240
Prikupljanje lozinki 240
Dodatak userassist 241
Dodatak malfind 241
Rezime 243

POGLAVLJE 11

Analiza artefakata, zlonamernog i ucenjivačkog softvera 245

Identifikacija uređaja i operativnih sistema pomoću alata p0f 245
Alat swap_digger za istraživanje Linux artefakata 250
Instaliranje i upotreba alata swap_digger 250
Izdvajanje lozinki pomoću alata MimiPenguin 252
Analiza PDF zlonamernih datoteka 253
Alat Hybrid Analysis za analizu zlonamernih datoteka 257
Analiza ucenjivačkog softvera pomoću alata Volatility 3 260
Dodatak pslist 262
Rezime 270

DEO 4
Automatizovani paketi za digitalnu forenziku i odgovor na incidente 271

POGLAVLJE 12

Forenzički pregledač Autopsy 273

Uvod u Autopsy – The Sleuth Kit 274
Preuzimanje uzoraka datoteka za upotrebu i kreiranje slučaja u pregledaču Autopsy 275
Pokretanje pregledača Autopsy 276
Kreiranje novog slučaja u forenzičkom pregledaču Autopsy 279
Analiza dokaza pomoću forenzičkog pregledača Autopsy 284
Rezime 289

POGLAVLJE 13

Izvođenje kompletne DFIR analize sa Autopsy 4 grafičkim korisničkim interfejsom 291

Karakteristike Autopsy 4 grafičkog korisničkog interfejsa 292
Instaliranje Autopsy 4 na operativnom sistemu Kali Linux pomoću Wine programa 292
Preuzimanje uzoraka datoteka za automatizovanu analizu 297
Kreiranje novih slučajeva i upoznavanje Autopsy 4 interfejsa 297
Analiza direktorijuma i oporavak obrisanih datoteka i artefakata pomoću Autopsy 4 GUI 305
Rezime 310

DEO 5

Alati za forenzičku analizu mreže 311

POGLAVLJE 14

Alati za otkrivanje mreže 313

Upotreba alata netdiscover na operativnom sistemu Kali Linux za identifikaciju uređaja na mreži . . 314
Upotreba alata Nmap za pronalaženje dodatnih računara i uređaja na mreži 316
Upotreba alata Nmap za identifikaciju detalja o računaru 319
Upotreba alata Shodan.io za pronalaženje IoT uređaja, uključujući mrežne zaštitne zidove, CCTV i servere 321
Upotreba Shodan filtera za pretrage IoT uređaja 322
Rezime 327

POGLAVLJE 15

Analiza hvatanja paketa alatom Xplico 329

Instalacija alata Xplico na operativnom sistemu Kali Linux 329
Instaliranje operativnog sistema DEFT Linux 8.1 u programu VirtualBox 331
Preuzimanje uzoraka datoteka za analizu 336
Pokretanje alata Xplico u DEFT Linux operativnom sistemu 337
Korišćenje alata Xplico za automatsku analizu veb, imejl i glasovnog saobraćaja 339
Automatska analiza veb saobraćaja 341
Automatska analiza SMTP saobraćaja 345
Automatska analiza VoIP saobraćaja 346
Rezime 348

POGLAVLJE 16

Alati za forenzičku analizu mreže 349

Hvatanje paketa pomoću alata Wireshark 350
Analiza paketa pomoću alata NetworkMiner 357
Analiza hvatanja paketa pomoću alata PcapXray 362
Analiza PCAP datoteka na platformi packettotal.com 368

Analiza PCAP datoteka na platformi apackets.com 371
Izveštavanje i prezentacija 375
Rezime 376

INDEKS 377