Unapredite svoje istraživačke veštine forenzičkom analizom mreže i memorije uz Kali Linux 2022.x

PREVOD TREĆEG IZDANJA

Kali Linux

digitalna forenzika

Šiva V N Parasram

kompjuter biblioteka

PREVOD TREĆEG IZDANJA

Kali Linux digitalna forenzika

Kali Linux je distribucija zasnovana na Linux operativnom sistemu koja se koristi za testiranje proboja i digitalnu forenziku. Ovo treće izdanje je dopunjeno realnim primerima i detaljnim laboratorijskim vežbama uz koje ćete, uz pomoć moćnih alata, unaprediti svoje veštine istrage.

Uz ovo izdanje ćete koristiti napredne alate, kao što su FTK Imager, Hex Editor i Axiom, da naučite savremene tehnike za analizu, izvlačenje podataka i izveštavanje. Obrađene su osnovne i napredne teme savremene digitalne forenzike tokom istraživanja domena operativnih sistema. Zatim su predstavljeni razni formati za skladištenje datoteka, uključujući mesta skrivena od krajnjeg korisnika, čak i od operativnog sistema. Takođe, naučićete da instalirate Windows Emulator Autopsy 4 na operativnom sistemu Kali Linux, da koristite alate Nmap i NetDiscover za pronalaženje vrste uređaja i računara na mreži, da kreirate forenzičke slike podataka i da održite integritet pomoću alata za heširanje. Na kraju su obrađene i napredne teme, kao što su obdukcija i prikupljanje podataka za istragu sa mreže, memorije i operativnog sistema.

Uz ovu knjigu o digitalnoj forenzici ćete steći praktično iskustvo implementacije temelja digitalne forenzike: prikupljanja, izvlačenja, analize i prezentacije podataka, pomoću najmodernijih alata operativnog sistema Kali Linux.

ŠTA ĆETE NAUČITI:

- Da instalirate operativni sistem Kali Linux na Raspberry Pi 4 uređaju i razne druge platforme
- Da pokrećete Windows aplikacije na operativnom sistemu Kali Linux pomoću emulatora Windows aplikacija poznatog kao Wine
- Da prepoznate važnost RAM memorije, sistema datoteka, podataka i keša za DFIR istragu
- Tehnike za oporavak datoteka, izdvajanje podataka i izvlačenje podataka pomoću alata Magic Rescue
- Upoznaćete najnoviji Volatility 3 radni okvir i analizu memorijskih ispisa
- Različite tipove ucenjivačkog softvera i otkrivanje artefakata za DFIR istragu
- Da sprovedete potpuno automatizovanu DFIR analizu pomoću pregledača Autopsy 4

Skenirajte QR kod, registrujte knjigu i osvojite nagradu

ISBN: 978-86-7310-600-7

Unapredite svoje istraživačke veštine forenzičkom analizom mreže i memorije uz Kali Linux 2022.x

Kali Linux

digitalna forenzika

Šiva V N Parasram

Prevod III izdanja

kompjuter biblioteka

Packt›

Izdavač:

kompjuter biblioteka

Obalskih radnika 4a
Beograd, Srbija

Tel: 011/2520272

e-pošta: kombib@gmail.com

veb-sajt: www.kombib.rs

Za izdavača:
Mihailo J. Šolajić, direktor

Autor:
Šiva V N Parasram

Prevod: Nemanja Lukić
Recezent: Miroslav Ristić
Slog: Zvonko Aleksić

Znak Kompjuter biblioteke:
Miloš Milosavljević

Štampa: „Pekograf“, Zemun
Tiraž: 500
Godina izdanja: 2024.

Broj knjige: 577
Izdanje: Prvo
ISBN: 978-86-7310-600-7

Naslov originala:

Digital Forensics with Kali Linux
3ND Edition
ISBN 978-1-83763-515-3

Packt Publishing Ltd.
Birmingham, UK, packt.com

Kali Linux
digitalna forenzika

Autorizovani prevod sa engleskog jezika.

CIP - Каталогизација у публикацији
Народна библиотека Србије, Београд

004.451.9LINUX
343.983:004
004.7.056.5

ПАРАСРАМ, Шива В. Н.

Kali linux : digitalna forenzika / Šiva V N Parasram; prevod 3. izd. [Nemanja Lukić]. - Izd. 1. - Beograd: Kompjuter biblioteka, 2024 (Zemun : Pekograf). - XVIII, 386 str.: ilustr.; 24 cm. - (Kompjuter biblioteka; br. knj. 577)

Prevod dela: Digital Forensics with Kali Linux. - Tiraž 500. - O autoru: str. III. - Registar.

ISBN 978-86-7310-600-7

a) Оперативни систем „Linux“
b) Вештачење -- Рачунарски системи
v) Рачунарске мреже -- Заштита

COBISS.SR-ID 148976905

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

Sadržaj

POGLAVLJE 10

POGLAVLJE 11

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

POGLAVLJE 12

Predgovor

U trećem izdanju ove knjige teorija i metodologije su, uglavnom, nepromenjene, sa ažuriranim opštim tehničkim informacijama, najboljim praksama i radnim okvirima, zbog standardizovanih postupaka i načina prikupljanja i kreiranja dokumenata. Međutim, tehnička poglavlja sadrže nove laboratorijske vežbe, sa novim primerima. Takođe, dodato je nekoliko potpuno novih poglavlja u kojima su podrobnije razmotrene teme analize artefakata, automatskog oporavka podataka, zlonamerni softver i analiza mreže, i predstavljeno nekoliko alata, uz praktične vežbe koje će čak i početnici lako pratiti. Koristimo i program Wine, što nam omogućava da unutar operativnog sistema Kali Linux instaliramo veoma popularne DFIR (**digitalne forenzike i odgovore na incidente**) alate napravljene za Windows operativni sistem (kao što je Autopsy 4). Ova knjiga je veoma korisna za članove crvenog tima i testere proboja koji žele da nauče, ili unaprede, DFIR veštine i poznavanje veština potrebnih za plavi tim, da bi postali članovi ljubičastog tima, koji kombinuju svoje veštine proboja sa veštinama digitalne forenzike i odgovora na incidente koje ćemo poučavati u ovoj knjizi.

Za koga je ova knjiga

Treće izdanje ove knjige pažljivo je strukturirano da bi bilo razumljivo korisnicima svih nivoa, početnicima u oblasti digitalne forenzike i profesionalcima za odgovor na incidente. Prvih šest poglavlja služi kao uvod u tehnologiju i vodič za instaliranje operativnog sistema Kali Linux, pre nego što se upustimo u forenzičke analize, oporavak podataka, analiziranje zlonamernog softvera, automatizovane DFIR analize i istraživanja mrežne forenzike. Ova knjiga će biti veoma korisna pripadnicima crvenog tima i testerima proboja koji žele da ovladaju veštinama plavog tima i postanu članovi ljubičastog tima.

Šta obuhvata ova knjiga

Poglavlje 1: Osnove crvenog, plavog i ljubičastog udruživanja, predstavlja različite vrste timova za kibernetičku bezbednost kojima pripadaju testeri proboja i forenzički istražitelji, kao i veštine članova tih timova.

Poglavlje 2: Uvod u digitalnu forenziku, predstavlja uvod u svet digitalne forenzike i forenzičke metodologije, kao i u razne forenzičke operativne sisteme.

Poglavlje 3: Instalacija operativnog sistema Kali Linux, predstavlja različite metode instaliranja operativnog sistema Kali Linux kao virtuelne mašine ili kao samostalnog operativnog sistema, koji je takođe moguće pokrenuti sa fleš memorije ili SD kartice.

Poglavlje 4: Dodatne instalacije operativnog sistema Kali Linux i zadaci nakon instalacije, nadovezuje se na prethodno i uvodi dodatne instalacije i zadatke nakon instalacije, kao što su omogućavanje root korisnika i ažuriranje operativnog sistema Kali Linux.

Poglavlje 5: Instaliranje programa Wine na operativnom sistemu Kali Linux, predstavlja svestranost Linux sistema, gde ćete naučiti da pomoću programa Wine u Kali Linux operativnom sistemu instalirate i koristite forenzičke alate dizajnirane za Windows operativni sistem.

Poglavlje 6: Koncept sistema datoteka i skladištenja, ulazi u oblast operativnih sistema i raznih formata za skladištenje datoteka, uključujući tajne skrivene lokacije nevidljive krajnjem korisniku, pa čak i operativnom sistemu. Takođe, ispituje podatke o podacima, metapodatke, kao i redosled njihovog nestajanja.

Poglavlje 7: Odgovor na incidente, prikupljanje podataka i DFIR radni okviri, postavlja pitanje šta se dešava kada je incident prijavljen ili otkriven. Koje osoblje prvo reaguje i koje su procedure za očuvanje integriteta dokaza? U ovom poglavlju bavimo se najboljim praksama, procedurama i radnim okvirima za prikupljanje podataka i sakupljanje dokaza.

Poglavlje 8: Alati za prikupljanje dokaza, predstavlja najbolje prakse prikupljanja podataka i najkorisnije alate u industriji, kao što su DC3DD, DD, Guymager, FTK Imager i RAM Capturer za prikupljanje podataka i slika uz očuvanje integriteta dokaza.

Poglavlje 9: Alati za oporavak datoteka i izvlačenje podataka, je uvod u istraživačku stranu digitalne forenzike i upotrebu raznih alata, kao što su Magic Rescue, Scalpel, Bulk_Extractor, scrounge_ntfs i recoverjpeg za izvlačenje i oporavak podataka i artefakata iz forenzički prikupljenih slika i medija.

Poglavlje 10: Forenzika memorije i analiza pomoću alata Volatility 3, je uvod u analizu memorijskih artefakata, gde se ističe važnost očuvanja nepostojanih dokaza, kao što su sadržaji RAM memorije i straničnih datoteka.

Poglavlje 11: Analiza artefakata, zlonamernog i ucenjivačkog softvera, predstavlja podrobniju analizu artefakata pomoću alata p0f, swap_digger i mimipenguin, uz demonstraciju analize zlonamernog i ucenjivačkog softvera alatima pdf-parser, hybrid-analysis.com i Volatility.

Poglavlje 12: Forenzički pregledač Autopsy, predstavlja automatski oporavak i analizu datoteka unutar operativnog sistema Kali Linux pomoću jednog alata.

Poglavlje 13: Izvođenje kompletne DFIR analize sa Autopsy 4 grafičkim korisničkim interfejsom, podrobnije razmatra automatsko izvlačenje datoteka, oporavak podataka i analizu pomoću jednog od najmoćnijih besplatnih forenzičkih alata, koji podiže mogućnosti forenzičke istrage na profesionalan nivo, kompletiranjem svih aspekata digitalnih forenzičkih istraga, od heširanja do izveštavanja.

Poglavlje 14: Alati za otkrivanje mreže, predstavlja alate za skeniranje mreže i praćenje, kao što su netdiscover, nmap i Shodan, koji iako nisu po svojoj prirodi forenzički alati mogu biti korisni za prikupljanje dodatnih informacija pri odgovorima na incidente.

Poglavlje 15: Analiza hvatanja paketa alatom Xplico, je uvid u automatsku analizu paketa pomoću jednog alata za istraživanje mrežnog i internet saobraćaja.

Poglavlje 16: Alati za forenzičku analizu mreže, završava knjigu demonstracijom hvatanja i analiziranja paketa pomoću raznih alata i veb stranica, uključujući Wireshark, NetworkMiner, packettotal.com i apackets.com.

Da biste najbolje iskoristili ovu knjigu

Iako smo se potrudili da objasnimo sve pojmove i tehnologije u ovoj knjizi, koristiće vam predznanje o preuzimanju i instalaciji softvera i poznavanje bar osnovnih koncepata računarstva i umrežavanja, kao što su RAM memorija, CPU, virtuelizacija i mrežni portovi.

SOFTVER/HARDVER KORIŠĆEN U KNJIZI	ZAHTEVI OPERATIVNOG SISTEMA
Kali 2022.x i noviji	Minimalne specifikacije: PC ili laptop sa 8 GB RAM memorije, 250 GB slobodnog prostora na tvrdom disku i Ryzen 7 ili i5 CPU Preporučene specifikacije: 16 GB RAM memorije, 250 GB slobodnog prostora na tvrdom disku i Ryzen 7 ili i7 CPU

Ako koristite digitalnu verziju ove knjige, savetujem vam da sami kucate kod ili da pristupite kodu na GitHub spremištu knjige (adresa je dostupna u narednom odeljku). Tako ćete izbeći moguće greške pri kopiranju koda.

Preuzimanje datoteka primera koda

Možete preuzeti datoteke sa primerima kodova za ovu knjigu sa GitHub spremišta na adresi `https://github.com/PacktPublishing/Digital-Forensics-with-Kali-Linux-Third-Edition`. U slučaju ažuriranja koda, biće ažuriran i kod u GitHub spremištu.

Takođe, postoje i drugi paketi kodova iz našeg bogatog kataloga knjiga i video materijala dostupni na adresi `https://github.com/PacktPublishing/`. Pogledajte ih!

Preuzimanje slika u boji

Takođe, dostavljamo PDF datoteku koja sadrži slike u boji, snimke ekrana i dijagrame korišćene u ovoj knjizi. Možete je preuzeti na adresi: `https://packt.link/vLuYi`.

Konvencije

Postoji nekoliko tekstualnih konvencija za ovu knjigu.

`Kod u tekstu`: označava delove koda u tekstu, imena tabela u bazi podataka, imena direktorijuma, nazive datoteka, ekstenzije datoteka, putanje, lažne URL adrese, unos korisnika i Twitter naloge. Na primer: „Uključite svoj Pi i Kali će se pokrenuti. Ponavljam, podrazumevani korisnički nalog i lozinka su `kali` (malim slovima)."

Bilo koji unos ili izlaz sa komandne linije je napisan na sledeći način:

```
sudo apt update
```

Podebljano: označava novi termin, važnu reč ili reči koje vidite na ekranu. Na primer, reči u menijima ili dijalozima su podebljane. Na primer: „Možete pregledati neke od forenzičkih alata klikom na **Applications** | **11-Forensics** u glavnom meniju operativnog sistema Kali Linux."

> **Saveti**
> ili
> **Važne napomene**
> Prikazani su ovako.

Postanite član Kompjuter biblioteke

Kupovinom jedne naše knjige stekli ste pravo da postanete član Kompjuter biblioteke. Kao član možete da kupujete knjige u pretplati sa 40% popusta i učestvujete u akcijama kada ostvarujete popuste na sva naša izdanja. Potrebno je samo da se prijavite preko formulara na našem sajtu.
Link za prijavu: kombib.rs/kblista.php

Skenirajte QR kod
registrujte knjigu
i osvojite nagradu

DEO 1

Osnovni principi plavog i ljubičastog udruživanja

Na početku našeg putovanja u svet **digitalne forenzike i odgovora na incidente (DFIR)**, važno je da razjasnimo plavo i ljubičasto udruživanje, koja se upoređuju sa crvenim udruživanjem i da steknemo osnovno znanje potrebno za kreiranje laboratorijskog okruženja za plavo i ljubičasto udruživanje. U ovom delu objašnjavamo terminologiju i razmatramo veštine potrebne da se postane član plavog i ljubičastog tima, ali i prikazujemo različite metode postavljanja DFIR laboratorijskog okruženja.

Ovaj deo se sastoji od sledećih poglavlja:

- *Poglavlje 1: Osnove crvenog, plavog i ljubičastog udruživanja*
- *Poglavlje 2: Uvod u digitalnu forenziku*
- *Poglavlje 3: Instalacija operativnog sistema Kali Linux*
- *Poglavlje 4: Dodatne instalacije operativnog sistema Kali Linux i zadaci nakon instalacije*
- *Poglavlje 5: Instaliranje programa Wine na operativnom sistemu Kali Linux*

1

Osnove crvenog, plavog i ljubičastog udruživanja

Dobrodošli u treće izdanje knjige *Kali Linux digitalna forenzika*, a za one koji su kupili prethodna izdanja, dobrodošli nazad. Takođe, želim iskreno da vam zahvalim što ste ponovo izabrali ovaj uzbudljiv naslov. Kao i drugo izdanje, i ovo treće izdanje je ažurirano sa novim alatima, jednostavnim laboratorijskim vežbama i sa nekoliko novih poglavlja. Pred nama je uzbudljivo putovanje, i drago mi je da najavim nekoliko značajnih dodataka, uključujući instalaciju programa Wine, koji će nam omogućiti pokretanje Windows alata unutar Kali Linux operativnog sistema i biće u potpunosti pokriven u *poglavlju 5, Instaliranje programa Wine na operativnom sistemu Kali Linux*. *Poglavlje 10, Forenzika memorije i analiza pomoću alata Volatility 3*, takođe je potpuno novo i pokazuje kako se vrši analiza RAM artefakata na novijim operativnim sistemima. Još jedno novo poglavlje o korišćenju Autopsy v4 **grafičkog korisničkog interfejsa** (**GUI**) za izvođenje potpune analize i istrage u okviru **digitalne forenzike i odgovora na incidente** (**DFIR**) je poglavlje *13, Izvođenje kompletne DFIR analize sa Autopsy 4 grafičkim korisničkim interfejsom*.

Pored ovih značajnih dodataka, razmotrene su i neke nove teme, kao što je kreiranje prenosive Kali Linux kutije pomoću Raspberry Pi 4 uređaja, kao i upoznavanje alata kao što su DD-rescue, scrounge-ntfs, Magic Rescue, PDF-Parser, Timeliner, netdiscover. Takođe, predstavljeni su alat **Shodan.io** i platforma **apackets.com** za otkrivanje **internet stvari** (**IoT**) uređaja i analizu paketa.

U ovoj knjizi pristupamo digitalnoj forenzici na veoma strukturiran način, kao što bismo to činili u forenzičkoj nauci. Prvo ćemo zakoračiti u svet digitalne forenzike, u njenu istoriju i neke od alata i operativnih sistema koji služe za forenziku, a odmah zatim ćemo vam predstaviti koncepte vezane za očuvanje dokaza.

Dakle, imamo mnogo toga da obradimo, a počećemo učenjem o operativnom sistemu Kali Linux i timovima za računarsku bezbednost, kao i razlikama između crvenog, plavog i

ljubičastog udruživanja. Povratnici i napredni čitaoci, koji imaju predznanje o Kali Linux operativnom sistemu i pomenutim timovima, mogu da preskoče prva dva poglavlja i pređu direktno na praktične aspekte *poglavlja 3, Instalacija operativnog sistema Kali Linux*, *poglavlja 4*, *Dodatne instalacije operativnog sistema Kali Linux i zadaci nakon instalacije* i *poglavlja 5*, *Instaliranje programa Wine na operativnom sistemu Kali Linux*, koja detaljno opisuju postupak instaliranja operativnog sistema Kali Linux i programa Wine.

Ključne teme u ovom poglavlju su:

- Šta je Kali Linux?
- Koncept crvenog tima
- Koncept plavog tima
- Koncept ljubičastog tima

Pre nego što pređemo na ove teme, sledi kratak opis mog ulaska u svet Kali Linux operativnog sistema, jer verujem da su neki od vas imali slično iskustvo!

Kako sam počeo da koristim operativni sistem Kali Linux

Digitalna forenzika me fascinira već više od 15 godina. Otkad sam dobio svoj prvi računar (hvala mama i tata), uvek sam se pitao šta se dešava kada izbrišem svoje datoteke sa svog ogromnog tvrdog diska od 2 GB (**gigabajta**), ili ih premestim na (i često sakrijem) više nego neupadljivu disketu od 3,5 inča, koja je imala maksimalni kapacitet od 1,44 MB (**megabajta**).

Brzo sam naučio da tvrdi diskovi i diskete ne poseduju digitalnu besmrtnost u koju sam tako samouvereno verovao. Nažalost, mnoge datoteke, dokumenti i neprocenjiva umetnička dela koja su od moje ruke nastala u programu Microsoft Paint zauvek su izgubljeni u digitalnom zagrobnom životu i nikada neće biti vraćena. Ah. Svet to nikada neće videti.

Tek godinama kasnije, dok sam pretraživao čarobnu **svetsku mrežu** (**WWW**) preko svoje munjevite 42 Kbps telefonske internet konekcije (omogućene mojim veoma skupim USRobotics telefonskim modemom), naišao sam na članak o oporavku datoteka i alatima koji za to služe. Svaki put kada bih pokušao da se povežem na internet, modem je ispuštao melodiju bogova tehnologije. Taj proces je zahtevao veštine nindže, na kojima bi mi pozavideli čak i članovi tima za tajne operacije, jer je uključivao prikriveno povezivanje bez roditeljskog znanja, što bi ih sprečilo da koriste telefonsku liniju za obavljanje ili primanje poziva (izvinjavam se dragoj majci, ocu i starijoj sestri tinejdžerki).

Prethodni članak o oporavku podataka nije bio ni približno detaljan i sadržajan kao mnogi sjajni recenzirani radovi, časopisi i knjige o digitalnoj forenzici koji su danas svuda dostupni. Kao potpuni početnik (takođe poznat kao amater) u ovoj oblasti, naučio sam mnogo o osnovama sistema datoteka, podacima i metapodacima, merama skladišnog prostora i funkcionisanju različitih medija za skladištenje. Tek sam tada, iako sam i ranije čitao o Linux operativnom sistemu i njegovim različitim distribucijama (ili distrosima), počeo da shvatam zašto su Linux distribucije popularne za oporavak podataka i forenziku.

Uspeo sam hrabro da preuzmem Auditor i Slax Linux distribucije, takođe putem telefonske veze. Samo preuzimanje ovih operativnih sistema bilo je pravo dostignuće, koje me preplavilo osećajem velikog uspeha, iako nisam imao nikakvu predstavu o tome kako da ih

instaliram, a kamoli koristim. U to vreme, jednostavna instalacija i grafički korisnički interfejsi još uvek su bili u fazi intenzivnog razvoja, koliko god korisnički orijentisani, ili u mom slučaju, korisnički nepristupačni, bili (uglavnom zbog mog neiskustva, nedostatka preporučene hardverske opreme, kao i nedostatka resursa kao što su onlajn forumi, blogovi i YouTube, za koje tada još nisam znao).

Dok je vreme prolazilo, istraživao sam mnoge alate dostupne na raznim platformama za Windows, Macintosh i mnoge Linux distribucije. Otkrio sam da je mnoge alate koji se koriste za digitalnu forenziku moguće instalirati na razne Linux distribucije ili varijante, a da su mnogi od ovih alata dobro održavani, stalno razvijani i široko prihvaćeni od strane kolega u ovoj oblasti. Kali Linux je jedna od Linux distribucija ili varijante, a pre nego što nastavimo, dozvolite mi da objasnim koncept Linux distribucije, ili verzije. Na primer, vaše omiljeno piće, može biti različitih ukusa, bez zaslađivača ili šećera, u različitim bojama, pa čak i u različitim količinama. Bez obzira na varijacije, osnovni sastojci od kojih se piće sastoji su isti. Isto tako, imamo Linux i njegove različite tipove i varijante. Neke od popularnijih Linux distribucija i varijanti su RedHat, CentOS, Ubuntu, Mint, KNOPPIX i, naravno, Kali Linux. Više o Kali Linux operativnom sistemu govorimo u *poglavlju 3*, *Instalacija operativnog sistema Kali Linux*.

Dakle, hajde da pređemo na sledeći deo i započnemo istraživanje očaravajućeg sveta Kali Linux operativnog sistema!

Šta je Kali Linux?

Kali Linux je operativni sistem zasnovan na Debian operativnom sistemu koji širom sveta koriste stručnjaci za računarsku bezbednost, studenti i IT entuzijasti. Debian je potpuno besplatna, stabilna i redovno ažurirana verzija Linux operativnog sistema koja podržava mnoge vrste hardvera i služi kao osnova za popularne operativne sisteme, kao što su Ubuntu i Zorin. Kali Linux svakako nije novost u polju računarske bezbednosti i potiče iz sredine 2000-ih godina, ali je tada bio poznat kao BackTrack, koji je bio kombinacija dve platforme nazvane Auditor Security i Whax. Do spajanja je došlo 2006. godine, a naredne verzije operativnog sistema BackTrack su izlazile sve do 2011. godine, kada je izašao BackTrack 5, zasnovan na distribuciji Ubuntu 10.04.

Godine 2013, *Offensive Security* je izdao prvu verziju Kali Linux v1 (Moto), koja je bila zasnovana na distribuciji Debian 7, a zatim Kali v2 2015. godine, zasnovanu na distribuciji Debian 8. Nakon toga, 2016. godine, objavljen je Kali Linux Rolling, sa imenima distribucija koje odražavaju i godinu izdanja i glavna ažuriranja kvartalnog perioda. Na primer, u trenutku pisanja, koristim verzije Kali 2022.3 i 2022.4, zasnovane na najnovijim verzijama distribucije Debian. Više informacija o otvorenom kodu i besplatnom Debian projektu možete naći na adresi *https://www.debian.org/intro/about*.

Kao stručnjak za računarsku bezbednost, **glavni službenik za informatičku bezbednost** (**CISO**), **tester proboja** (**pentester**) i DFIR stručnjak, koristio sam BackTrack, a već više od decenije Kali Linux, otkako sam ga otkrio kada sam počeo da se pripremam za ispit za sertifikovanog etičkog hakera 2006. godine. Od tada sam koristio mnoštvo operativnih sistema za testiranje proboja i digitalnu forenziku, ali moj glavni alat, posebno za testiranje proboja, je Kali Linux. Iako je Kali Linux manje fokusiran na DFIR, a više na testiranje proboja, omogućava mi da imam i alate za testiranje proboja i DFIR na jednoj platformi, umesto da prelazim sa jedne na drugu.

Čitaocima koji su, eventualno, kupili prvo i/ili drugo izdanje ove knjige, mogu reći da ih čeka pravo uživanje, jer nisam samo ažurirao mnoge laboratorijske vežbe i uveo nove alate u ovom izdanju, nego sam dodao i poglavlje o instaliranju programa Wine na Kali Linux operativnom sistemu. **Windows Emulator** (**Wine**) vam omogućava da pokrećete Windows aplikacije na Kali Linux operativnom sistemu. Iako konfigurisanje nije zahtevno, sastavio sam detaljno uputstvo, korak po korak, kako instalirati Wine u *poglavlju 5*, *Instaliranje programa Wine na operativnom sistemu Kali Linux*.

Neki od vas se možda pitaju zašto da instaliramo Wine, umesto da jednostavno koristimo računar sa Windows operativnim sistemom. Postoji nekoliko valjanih razloga. Prvo, troškovi su ključni faktor. Windows licence nisu jeftine, posebno ako ste student, u periodu između poslova, menjate karijeru ili živite u regionu gde su kursna razlika i devizni propisi ograničavajući faktori pri kupovini licence. U trenutku pisanja, cena licence za operativni sistem Windows 10 Professional je 199 dolara, prema navodima na Microsoft sajtu https://www.microsoft.com/en-us/d/windows-10-pro/df77x4d43rkt?activetab=pivot:overviewtab.

Iako nećemo koristiti komercijalne alate u ovoj knjizi, postoje neki izvanredni besplatni DFIR alati dostupni za Windows, kao što su **Belkasoft RAM Capturer**, **Autopsy 4 GUI** i **NetworkMiner**, koje sada možemo instalirati unutar našeg Kali Linux okruženja otvorenog koda, umesto na računaru sa licenciranim Windows operativnim sistemom. Ovi alati će biti detaljno obrađeni u *poglavlju 8*, *Alati za prikupljanje dokaza*, *poglavlju 13*, *Izvođenje kompletne DFIR analize sa Autopsy 4 grafičkim korisničkim interfejsom* i *poglavlju 16*, *Alati za forenzičku analizu mreže*, redom.

Još jedan razlog za korišćenje programa Wine je to što nas oslobađa potrebe za upotrebom više fizičkih računara i može uštedeti resurse kao što su **radna memorija** (**RAM**), **centralna procesorska jedinica** (**CPU**), prostor na **tvrdom disku** (**HDD**) i druge resurse kada koristimo virtuelne mašine, o čemu ćemo detaljnije govoriti u sledećem poglavlju.

Na kraju, možemo instalirati mnoge druge Windows aplikacije u Kali Linux operativnom sistemu pomoću različitih alata, bilo da su to alati za produktivnost ili čak alati za testiranje proboja, čime naša instalacija operativnog sistema Kali Linux postaje savršeno okruženje za ljubičasti tim, o čemu govorimo kasnije u ovom poglavlju.

Zašto je Kali Linux toliko popularan?

Pored toga što je jedna od najstarijih distribucija za informacionu bezbednost, Kali Linux ima vrlo veliku bazu podrške, i postoji hiljade kurseva o instaliranju, upotrebi ugrađenih alata i instaliranju dodatnih alata na platformama YouTube, TikTok i širom interneta, što ga čini jednom od najpristupačnijih platformi za korisnike.

Kali Linux takođe sadrži više od 600 alata, lepo kategorizovanih u meniju **Applications**. Mnogi od tih alata mogu da služe za razne zadatke računarske bezbednosti, kao što su alati **za prikupljanje informacija iz otvorenih izvora** (**OSINT**), za skeniranje, za procenu ranjivosti, zloupotrebu i testiranje proboja, alati za kancelarijski rad i produktivnost, i, naravno, DFIR. Potpun spisak alata nalazi se na adresi https://www.kali.org/tools/all-tools/.

Sledeći snimak ekrana daje pregled kategorija menija operativnog sistema Kali Linux.

Slika 1.1 – Spisak kategorija u Kali Linux meniju

Korisnici operativnog sistema Kali Linux takođe imaju opciju da ručno preuzmu i instaliraju (meta)pakete, umesto preuzimanja veoma velike instalacione datoteke. Kali Linux (meta) paketi sadrže alate i zavisnosti specifične za datu procenu ili zadatak, kao što su prikupljanje informacija, procena ranjivosti, hakovanje bežičnih mreža i forenzika. Alternativno, možete preuzeti **kali-linux-everything (meta)paket**. Detaljnije ćemo se baviti instaliranjem (meta) paketa u *poglavlju 4, Dodatne instalacije operativnog sistema Kali Linux i zadaci nakon instalacije*, ali ako želite da saznate više o postojećim (meta)paketima, pronaći ćete potpun spisak na adresi https://www.kali.org/docs/general-use/metapackages/.

Kali Linux je vrlo popularan i zbog toga što postoji više verzija dostupnih za mnoštvo fizičkih, virtuelnih, mobilnih i prenosivih uređaja. Kali je dostupan kao samostalna operativna sistemska slika i možete ga instalirati virtuelno pomoću unapred izgrađene slike za virtuelne platforme, kao što su VMware i VirtualBox, što je detaljno obrađeno u *poglavlju 3, Instalacija operativnog sistema Kali Linux*, i *poglavlju 4, Dodatne instalacije operativnog sistema Kali Linux i zadaci nakon instalacije*. Takođe postoje verzije operativnog sistema Kali Linux za ARM uređaje, instance u oblaku, pa čak i mogućnost pokretanja na Windows 10, u okviru funkcije **Windows Subsystem for Linux** (**WSL**). Lično, koristim mobilnu verziju pod nazivom Kali NetHunter na starom OnePlus telefonu i, takođe, na Raspberry Pi 4 uređaju, koji, kada je povezan na prenosivi punjač, služi kao najbolji prenosivi alat za procenu bezbednosti. Što se tiče instaliranja na mobilnim telefonima, NetHunter (pa čak i Kali Linux u nekim slučajevima) moguće je instalirati na razne telefone, kao što su Samsung, Nokia, OnePlus, Sony, Xiaomi, Google ili ZTE. Razmotrićemo instalaciju operativnog sistema Kali Linux na VirtualBox i Raspberry Pi 4 u *poglavlju 4, Dodatne instalacije operativnog sistema Kali Linux i zadaci nakon instalacije*.

Činjenica da Kali Linux sve ove funkcije nudi besplatno i da ga je lako unaprediti dodavanjem alata uz samo nekoliko klikova i komandi čini ga savršenim rešenjem za ljubičasto udruživanje. Hajde da razmotrimo crveno, plavo i ljubičasto udruživanje i veštine koje su potrebne za svaki tim.

Koncept crvenog tima

Verovatno najpoznatiji tim među korisnicima Kali Linux operativnog sistema, crveni tim je naziv za grupu pojedinaca odgovornih za ofanzivnu stranu bezbednosti, koja se odnosi na OSINT, skeniranje, procenu ranjivosti i testiranje proboja resursa, uključujući, ali ne ograničavajući se na pojedince, kompanije, krajnje korisnike (desktop računare, laptopove, mobilne uređaje), mrežnu i kritičnu infrastrukturu kao što su serveri, ruteri, mrežni prekidači, mrežni zaštitni zidovi, NAS, baze podataka, veb aplikacije i portali. Takođe, postoje sistemi kao što su IoT, uređaji **operativne tehnologije** (**OT**) i **industrijski kontrolni sistemi** (**ICS**), koji takođe zahtevaju procenu od strane visoko kvalifikovanih pripadnika crvenog tima.

Pripadnike crvenog tima generalno smatramo najveštijim etičkim hakerima i testerima proboja koji, pored veština za sprovođenje navedenih procena, verovatno poseduju i tehničke sertifikate koji im to omogućavaju. Iako sertifikati, možda, nisu direktan odraz sposobnosti pojedinca, jasno je da pomažu da se dobije posao.

Neki od sertifikata za crveni tim su (ali ne samo):

- **Sertifikovani stručnjak za ofanzivnu bezbednost (OSCP)**: Koji su razvilli kreatori Kali Linux operativnog sistema
- **Sertifikovani etički haker (CEH)**: Koji izdaje EC-Council
- **Praktični mrežni tester proboja (PNPT)**: Koji je razvio TCM Security
- **Pentest+**: CompTIA
- **SANS SEC**: Kursevi instituta SANS
- **e-Learn junior tester proboja (eJPT)**: Koji je razvio e-Learn Security za početnike zainteresovane da postanu članovi crvenog tima

Sve u svemu, sve ovo znanje omogućava članovima crvenog tima da (sa eksplicitnim dopuštenjem) sprovode ofanzivne napade na kompanije, da bi simulirali unutrašnje i spoljašnje pretnje i, u suštini, hakovali sisteme i bezbednosne mehanizme na isti način na koji zlonamerni akteri mogu da kompromituju i eksploatišu površinu napada pojedinca, kompanije ili vrednog resursa.

Uopšteno, Kali Linux sadrži alate potrebne za upražnjavanje gotovo svake vrste ofanzivne bezbednosti i za aktivnost crvenog tima. Kali Linux je moj omiljeni operativni sistem za testiranje proboja, jer je većina alata potrebnih za identifikaciju računara, izviđanje, OSINT, procenu ranjivosti, eksploataciju i izveštavanje odmah dostupna i unapred instalirana na platformi. Koristim Kali za izvođenje vežbi za crveni tim više od 12 godina i ne vidim da će se to uskoro promeniti, jer svih ovih godina imam održavan OS i podršku za alate.

Hajde da sada pređemo na plavi tim.

Koncept plavog tima

Plavi tim generalno smatramo odbrambenom stranom, za razliku od ofanzivne strane koju predstavlja crveni tim. Dok je crveni tim fokusiran na simulaciju pretnji i moguću eksploataciju, plavi tim je čuvar sistema.

Crveni i plavi tim su prilično slični, kada se uzme u obzir da je glavni cilj oba tima zaštita resursa i sagledanje potencijalnih uticaja i rizika povezanih sa narušavanjem bezbednosti i curenjem podataka. Crveni tim je fokusiran na tehnike napada, kao što su računarski lanac proboja i testiranje proboja, dok je fokus plavog tima da osigura funkcionalnost mehanizama za zaštitu od napada, kao i da implementira formalne politike, procedure, pa čak i okruženja da se osigura efikasan DFIR.

Posao plavog tima je mnogo obimniji, jer oni moraju da analiziraju pretnje, procene rizik i uticaj, implementiraju bezbednosne i zaštitne mere, poznaju forenziku i odgovaranje na incidente i da osiguraju efikasno sprovođenje mera nadzora i odgovora. Takođe, članu plavog tima veoma koristi eventualno iskustvo iz crvenog tima, jer mu pruža dodatnu dubinu u razumevanju površina napada i pretnji.

Pripadnici plavog tima moraju poznavati širok spektar tehnologija i analitika. Iako nije nemoguće da novajlije u svetu informacionih tehnologija uđu u plavi tim i DFIR, to zahteva prethodno znanje slično onom koje imaju mrežni i sistemski administratoti, kao i znanje analitičara bezbednosti i lovca na pretnje. Na primer, shvatanje da sistemi moraju biti ažurirani i zakrpljeni je deo najbolje prakse. Pripadnik plavog tima će razumeti zašto je potrebno zakrpiti sisteme i takođe će znati da učini mnogo toga da učvrsti uređaje da bi se smanjile površine napada, imajući u vidu mogućnosti eksploatacija nultog dana i ljudske slabosti, koje mogu da olakšaju proboj pretnji i da zaobiđu sve tehničke mere koje su implementirane.

Takođe, nisu retkost ni oglasi za posao kojima se traži član plavog tima koji poznaje veštinu upotrebe alata za **upravljanje bezbednosnim informacijama i događajima** (**SIEM**) koji daju analizu u realnom vremenu, nadzor i alarme koji značajno pomažu u DFIR okruženju i omogućavaju bolje razumevanje nivoa zaštite potrebnog za održavanje visokog nivoa bezbednosti podataka, sistema i resursa.

Takođe, članovi plavog tima snose odgovornost za interne i eksterne resurse, kao i za pretnje koje se odnose na imovinu koju je potrebno zaštititi. Pretnje obuhvataju uređaje, osobe, podatke i bilo koju informaciju koja može biti korisna napadaču prilikom planiranja napada. Tu dolazi do izražaja temeljno poznavanje OSINT alata. Iako je spomenuta u kontekstu crvenog tima, ova veština je podjednako važna i za plavi tim, jer omogućava pretraživanje interneta, društvenih mreža i mračnog interneta u potrazi za informacijama koje bi mogle predstavljati pretnju ili na neki način omogućiti napad.

Dobar primer je pretraživanje baze podataka sa kompromitovanim informacijama, gde plavi tim (nakon što preduzme sve potrebne mere zaštite) pretražuje mračni internet u potrazi za kompromitovanim imejl adresama ili akreditivima **virtuelne privatne mreže** (**VPN**) kompanije za koju radi. Plavi tim, takođe, može da pronađe dostupne uređaje iz spoljne perspektive, kao što je spoljnji pristup mrežnim zaštitnim zidovima, serverima i CCTV kamerama, pomoću pretraživača Shodan.io, koji ćemo detaljnije razmotiriti kasnije u ovoj knjizi. Sve prethodne situacije pomažu plavom timu da kreira takozvani profil pretnji, koji sakuplja potencijalne pretnje, pa i **pokazatelje kompromitacije** (**IoC**) pronađene spolja, iako mu interni i eksterni resursi nisu direktan fokus.

Odličan način da naučite da koristite OSINT alate je besplatan četvoročasovni kurs TCM Akademije na YouTube platformi, koji se nalazi na adresi https://www.youtube.com/watch?v=qwA6MmbeGNo.

Iako se mnoge od pomenutih veština stiču istraživanjem i nebrojenim satima rada, praćenjem YouTube kurseva i pohađanjem specijalizovanih kurseva, naveo sam nekoliko sertifikata koji vam mogu pomoći u razvoju karijere u plavom timu i DFIR okruženju.

Neki od sertifikata za plavi tim su (ali ne samo):

- **Forenzički istraživač računarskog hakovanja** izdaje ga EC-Council
- **Sertifikovani inženjer za bezbednost u oblaku (CCSE)** izdaje ga EC-Council
- **Sertifikovani forenzički ispitivač računara (CFCE)** izdaje ga IACIS
- **GIAC sertifikovani forenzički ispitivač (GCFE)** izdaje ga SANS

U ovoj knjizi ćemo do detalja razmotriti alate DFIR istražitelja i analitičara. Iako se nećemo detaljno baviti komercijalnim alatima, pomenuću neke koje bi trebalo istražiti ukoliko planirate karijeru DFIR istražitelja plavog tima. Ipak, alati otvorenog koda obuhvaćeni ovom knjigom su sasvim dovoljni za početak i sprovođenje kompletne DFIR istrage, pod uslovom da se pridržavate najboljih praksi i procedura.

Takođe je izuzetno važno da DFIR istražitelji i analitičari razumeju značaj pridržavanja najboljih praksi i procedura prilikom prikupljanja, sticanja, analize i dokumentovanja dokaza, jer je integritet dokaza i slučaja lako ugroziti. Analizu dokaza takođe mora biti moguće ponoviti i proveriti rezultate u izveštajima, što znači da bi drugi DFIR istražitelji i analitičari trebalo da budu u mogućnosti da ponove testove i dobiju iste rezultate kao i vi.

U tom smislu, plavi tim bi trebalo da ima detaljan i dobro dokumentovan plan akcije, zajedno sa poznavanjem specifičnih alata. Postoji mnogo besplatnih i dobro dokumentovanih praksi i radnih okvira za plavi tim, a neke ćemo razmotriti u narednom poglavlju.

Pogledajte listu alata koje ćete možda koristiti u DFIR istrazi, a koji su opisani u ovoj knjizi. Sledeća lista sadrži kratak opis određenog zadatka i alata za njegovo postizanje. Gledajte na to kao na puškice za plavi tim kada su u pitanju alati otvorenog koda. Svakako napravite kopiju ove stranice i koristite je kao referentni list u svom forenzičkom radu i odgovorima na incidente:

- Forenzički operativni sistemi za DFIR - naša prilagođena verzija operativnih sistema Kali Linux, CSI Linux i CAINE
- Kreiranje USB uređaja sa kojih se može pokrenuti operativni sistem Kali Linux - Rufus i Etcher
- Kreiranje prenosive verzije operativnog sistema Kali Linux za Raspberry Pi - Imager (Pi Imager)
- Instalacija Windows alata u Kali - Wine
- Prikupljanje memorije - FTK Imager i Belkasoft RAM Capturer
- Prikupljanje dokaza i diskova - DD, DC3DD, Guymager i FTK Imager
- Oporavak datoteka i izdvajanje podataka - Foremost, Magic Rescue, DD-Rescue, Scalpel i Bulk_extractor
- PDF forenzika - pdfparser
- Oporavak NTFS diskova - scrounge-ntfs
- Analiza memorije/RAM memorije - Volatility 3
- Identifikacija operativnog sistema - p0f
- Linux forenzika uživo - Linux Explorer
- Otkrivanje artefakata - swap_digger, mimipenguin i pdgmail
- Forenzički alat zasnovan na pretraživaču - Autopsy Forensic Browser
- Kompletan forenzički alat - Autopsy 4
- Alati za otkrivanje mreže - netdiscover i nmap
- Pretraživač IoT uređaja - Shodan.io
- Analiza mrežnih paketa zasnovana na pregledaču - Xplico
- Automatizovana analiza mrežnih paketa - Network Miner i PcapXray
- Online alati za analizu Pcap datoteka - packettotal.com, apackets.com

Sledeći na redu je ljubičasti tim.

Koncept ljubičastog tima

Sada imamo zen trenutak računarske bezbednosti, jer smo stigli do ljubičastog tima. Termin **ljubičasti tim** ističe kombinaciju veština crvenog i plavog tima. Ljubičasta boja se dobija mešanjem crvene i plave boje, otuda naziv. Kada se osvrnemo na sve veštine i sertifikate potrebne za crveni i plavi tim, to može da deluje kao nemoguć poduhvat; međutim, garantujem vam da su mnogi pripadnici ljubičastog tima počeli od početka i završili kao profesionalci, uključujući i mene.

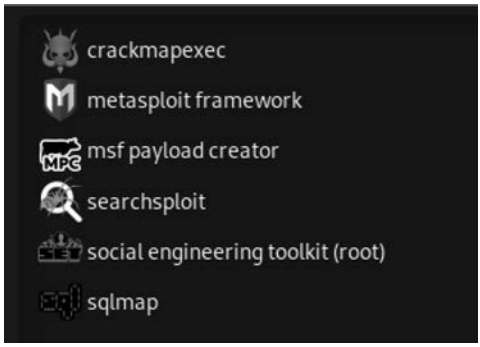
Kada sam zakoračio u svet računarske bezbednosti ranih 2000-ih godina, najviše sam bio zainteresovan za etičko hakovanje i testiranje proboja (crveni tim) i proveo sam mnoge noći ispred računara čitajući i istražujući pomoću ograničene palete dostupnih alata. Tek negde oko 2008. godine odlučio sam da se posvetim DFIR istrazi i analizi i postao veoma zainteresovan za oblast forenzike, do te mere da sam spojio CHFI i CEH kurseve.

Svaki put kada sam poželeo da se specijalizujem za određenu oblast, naišao bih na novi alat koji bi me usmerio ka nekoj drugoj. Srećom, to je išlo u moju korist jer sam ubrzo shvatio da se mnogi aspekti crvenog i plavog tima preklapaju i da nikada ne mogu reći da je ono što sam naučio dovoljno. Poenta je da je računarska bezbednost toliko dinamično polje, sa mnogo puteva, da nikada ne možete znati dovoljno. Uvek postoji neki novi softverski alat za iskorišćavanje ranjivosti, istražni alat ili procedura za odgovor na incidente koju treba naučiti, a na vama je da odlučite da li želite da se specijalizujete za jedno polje ili da nastavite da učite i usavršavate se, kao što sam ja radio, i da primenjujete svoje znanje kada je to potrebno.

Danas, ja sam vlasnik Instituta za računarsku forenziku i bezbednost, gde sam predvodnik ljubičastog tima i glavni tester proboja, kao i glavni istražitelj za forenziku i odgovor na incidente. Ponavljam, vrlo je moguće ovladati sa obe oblasti ako se tome posvetite.

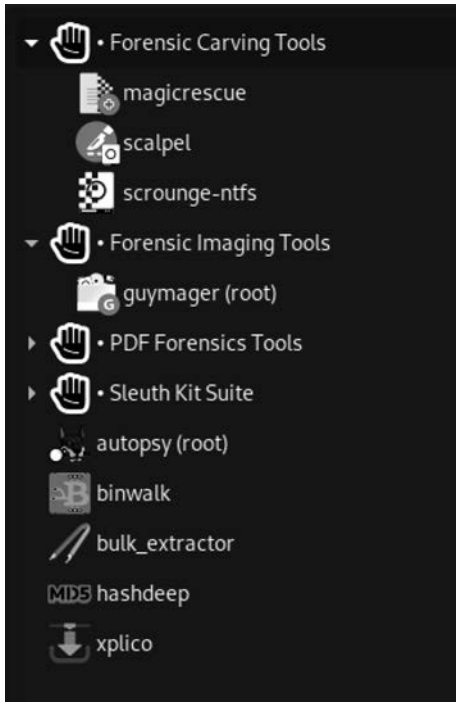
U tom smislu, mogu sa sigurnošću reći da je Kali Linux savršen za početak, jer nudi najbolje alate za ljubičasti tim. Hajde da pogledamo neke od dostupnih alata za eksploataciju (alati crvenog tima), koji su unapred instalirani uz bilo koju verziju Kali Linux operativnog sistema.

To je samo deo alata u meniju **Exploitation**; međutim, religiozno koristim alate **metasploit framework**, **msf payload creator** i **social engineering toolkit** (root) za procene crvenog tima.



Slika 1.2 – Kali Linux alati u meniju Exploitation

Sada hajde da pogledamo meni **Forensic**:



Slika 1.3 – Kali Linux alati u meniju Forensic

Ponavljam, ovo su samo neki od forenzičkih alata, dok je ostale moguće pronaći pregledom menija **All Applications**, koji ćemo razmotriti u *poglavlju 3, Instaliranje operativnog sistema Kali Linux*. Kali Linux je jedna od retkih platformi prilagođenih korisnicima koja nudi razne alate za ljubičasti tim i drago mi je što ću vam u narednim poglavljima pokazati kako da efikasno koristite mnoge od njih.

U *poglavlju 3, Instaliranje operativnog sistema Kali Linux*, pokazaću vam, korak po korak, kako da postavite Kali Linux u sigurnom, virtuelnom okruženju za testiranje gde možemo da koristimo naše alate i da preuzimamo uzorke datoteka za analizu. Iako će ova virtuelna mašina biti povezana na internet, koristićemo je u izolovanom okruženju da bismo osigurali da neće uticati na vaš proizvodni sistem. *U poglavlju 5, Instaliranje programa Wine na operativnom sistemu Kali Linux*, takođe ću vas provesti kroz proces instaliranja programa Wine na Kali Linux da bismo izgradili najbolji arsenal alata za plavi i ljubičasti tim, koji će sada biti kombinacija najboljih Windows i Linux alata otvorenog koda.

Sada kada smo sagledali razlike između crvenog, plavog i ljubičastog tima, preći ćemo na koncept digitalne forenzike, razmatranje drugih forenzičkih platformi i nekih komercijalnih alata i, što je vrlo važno, steći ćemo uvid u forenzičke radne okvire u *poglavlju 2, Uvod u digitalnu forenziku*.

Rezime

U ovom poglavlju smo upoznali Kali Linux operativni sistem zasnovan na Debian operativnom sistemu i njegove mogućnosti u svetu računarske bezbednosti. Takođe smo učili o različitim timovima za računarsku bezbednost, kao što su crveni timovi, koji se bave ofanzivnom bezbednošću i etičkim hakovanjem, poput testera proboja, i plavi timovi, koji se bave odbranom mreža i podataka, poput forenzičkih istražitelja. Takođe smo saznali da posedovanje veština i iskustva oba tima (crvenog i plavog) svrstava pojedinca u visoko kvalifikovani ljubičasti tim, što sugeriše da poznaje širok spektar alata za procenu ranjivosti, testiranje proboja, odgovor na incidente i digitalnu forenziku, od kojih se mnogi nalaze u operativnom sistemu Kali Linux.

U narednom poglavlju ćemo se detaljnije pozabaviti digitalnom forenzikom, pogledati druge forenzičke operativne sisteme i učiti o forenzičkim radnim okvirima i često korišćenim komercijalnim i alatima otvorenog koda. Vidimo se u sledećem poglavlju!