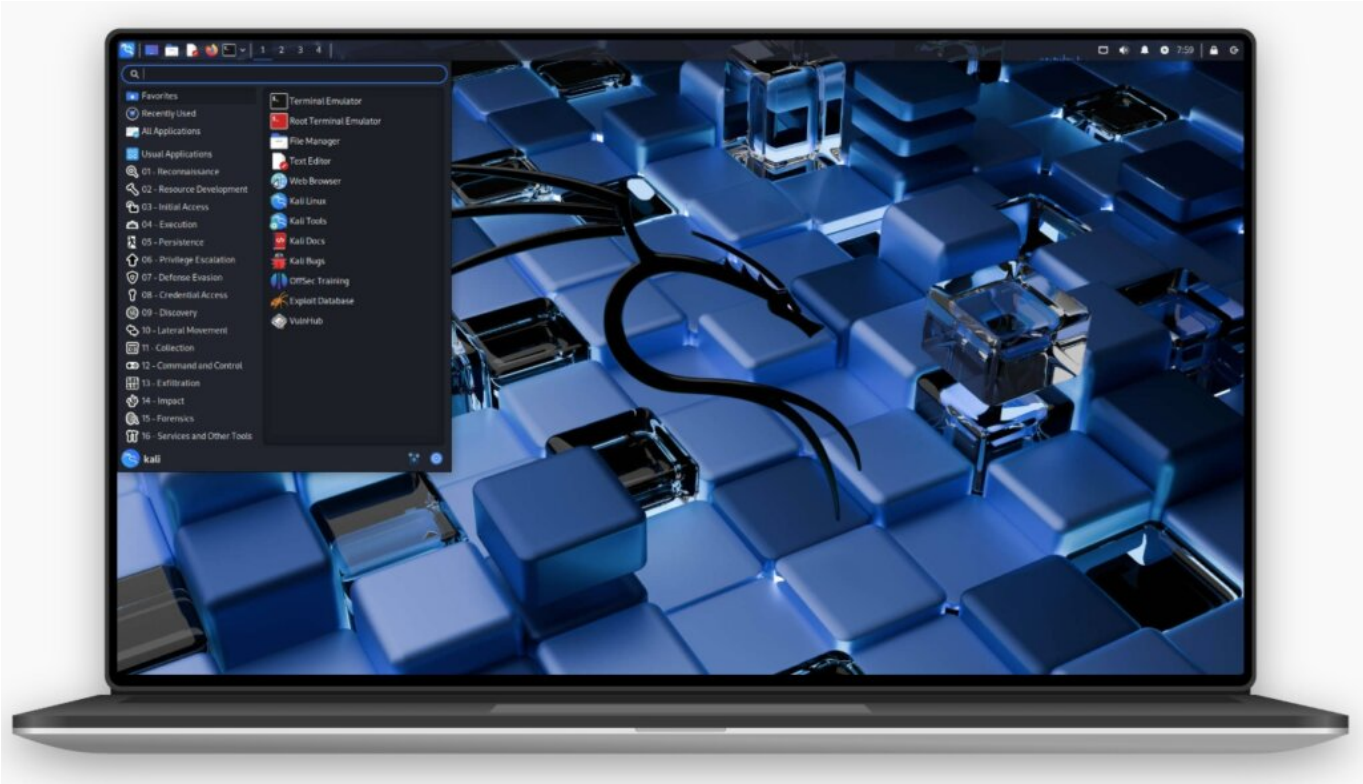
Etičko hakiranje za početnike i one naprednije – ključna Linux distribucija za laboratorije kibernetičke sigurnosti

Tihomir Katulić | 30 travnja, 2026

U doba uznapredovale digitalne transformacije, kako se društveni procesi sveobuhvatno sele iz fizičkog u virtualni, kibernetički prostor, proučavanje kibernetičke sigurnosti zauzima sve važniju poziciju u nizu obrazovnih programa. Da bi bilo učinkovito, treba cjelovito obuhvatiti teorijski, pravni, organizacijski i praktični okvir jer sigurnost kibernetičkih sustava, podataka i postupaka zahtijeva uvide i razumijevanje koji nadilaze samo tehnološku osnovicu.

Razumijevanje pravnog okvira osigurava svijest o obvezama, osobito postupcima, tehničkim i organizacijskim mjerama, ali i nadzornim ovlastima i potencijalnim kaznama kao mehanizmu generalne prevencije neželjenog ponašanja. U kontekstu kibernetičke sigurnosti to znači prevenciju nemarnog i nepažljivog uvođenja, korištenja i održavanja kritičnih sustava pod prijetnjom značajnih financijskih (prekršajnih) sankcija. S druge strane, u kontekstu kibernetičkog kriminaliteta to znači razvoj kaznenopravnih sankcija koje se razvijaju radi njegovog sprečavanja i progona počinitelja.

Organizacijski aspekt kibernetičke sigurnosti analizira sigurnost kao proces, a ne samo konačni rezultat odnosno proizvod, obuhvaćajući područja kao što su upravljanje rizicima, izrada internih sigurnosnih politika te, u konačnici vjerojatno najvažnije, izgradnju sigurnosne kulture u organizaciji. Desetljeća uvida u sigurnosnu praksu uče nas kako je najslabija točka često ljudski faktor pa je ključno educirati zaposlenike i osigurati da se sigurnosne mjere dosljedno provode na svim razinama poslovanja. Takva edukacija treba biti interdisciplinarna, cjelovita, s pristupom koji uključuje tehničko znanje, regulatornu usklađenost i ljudske organizacijske procese kako bi se osigurala učinkovita kibernetička sigurnost. Konačno, sve ove aspekte treba nekako prenijeti odnosno pretvoriti u primjenjive vještine, a za to su potrebni odgovarajući alati s obzirom da profil suvremenih prijetnji, kao i složenost suvremenih informacijskih sustava zahtjeva moderne alate i tehničku sofisticiranost. Tome mogu poslužiti razni sigurnosni alati kojih svakim danom ima sve više budući da svijest o kibernetičkoj sigurnosti postaje sastavni dio i opće mjesto poslovne kulture. Tih je alata uistinu puno pa nekad nije jednostavno odabrati na koje se usredotočiti. Ponekad je stoga najjednostavnije u edukacijske svrhe posegnuti za nekom od kolekcija slobodno dostupnih alata, kao što je kolekcija koja je i predmet ovog prikaza – najpopularnija Linux distribucija za etičko hakiranje pod imenom Kali Linux.

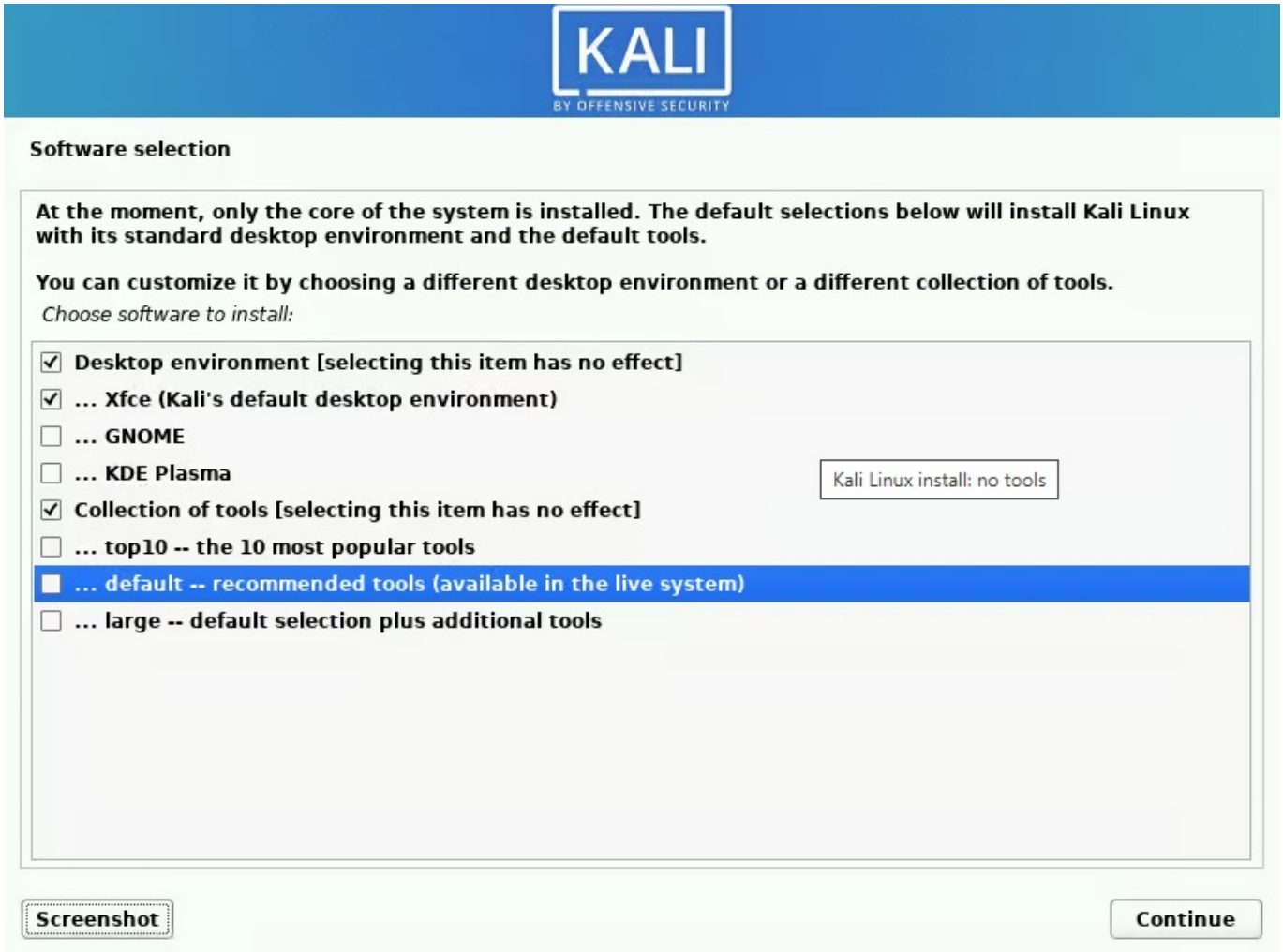


Prije nego prikažemo neke od sastavnih dijelova odnosno alata koje ova distribucija sadrži, potrebno je ponoviti klasično upozorenje koje se odnosi na sve tehnologije dvostruke namjene. Upotreba alata koje ova distribucija sadrži može značiti ozbiljne pravne i etičke implikacije. Alati unutar Kalija mogu poslužiti za edukaciju o sigurnosti, ali i za počinjenje napada, jer isti alat koji administrator koristi za popravak mreže, napadač može koristiti za njezino ometanje, neovlašteni pristup, presretanje podataka i slično. Zbog toga linija između legitimnog istraživanja i kaznenog djela može biti tanka, stoga korisnici trebaju poduzeti odgovarajuće korake kako bi dokumentirali svoju akademsku, istraživačku ili edukacijsku namjeru i ishodili potrebne dozvole za takvo postupanje.

Što je Kali Linux?

Kali Linux je besplatna i *open-source* distribucija operativnog sustava Linux posebno prilagođena i namijenjena digitalnoj forenzici i testiranju otpornosti i pristupa sustavima (engl. *penetration testing*). Kroz više od deset godina razvoja, ova je kolekcija izrasla u prilično zaokružen skup alata koji stručnjacima omogućuju provedbu sigurnosne revizije i testiranje otpornosti sustava, mreža i aplikacija na stvarne napade.

Privlačnost Kali Linuxa leži u njegovom skladištu alata. Za razliku od standardnih operativnih sustava (poput Windowsa ili standardnog Ubuntu Desktopa) koji zahtijevaju ručnu instalaciju i konfiguraciju stotinu specijaliziranih alata, Kali Linux, kao vodeća distribucija namijenjena digitalnoj forenzici i penetracijskom testiranju, u svojoj osnovnoj instalaciji sadrži impresivan arsenal od nekoliko stotina predinstaliranih alata. Dostupni alati pažljivo su organizirani u kategorije koje prate tijek standardne sigurnosne procjene, omogućujući stručnjacima da slijede metodologiju od početnog prikupljanja informacija pa sve do pisanja završnih izvještaja. Alati su organizirani u kategorije poput alata za prikupljanje informacija (engl. *information gathering*), alata za analizu ranjivosti (engl. *vulnerability analysis*), alata za ispitivanje sigurnosti bežičnih mreža (*wireless network sniffing*), alata za iskorištavanje ranjivosti (engl. *exploitation tools*) i alata za digitalnu forenziku (*digital forensics*).



Najpopularniji alati

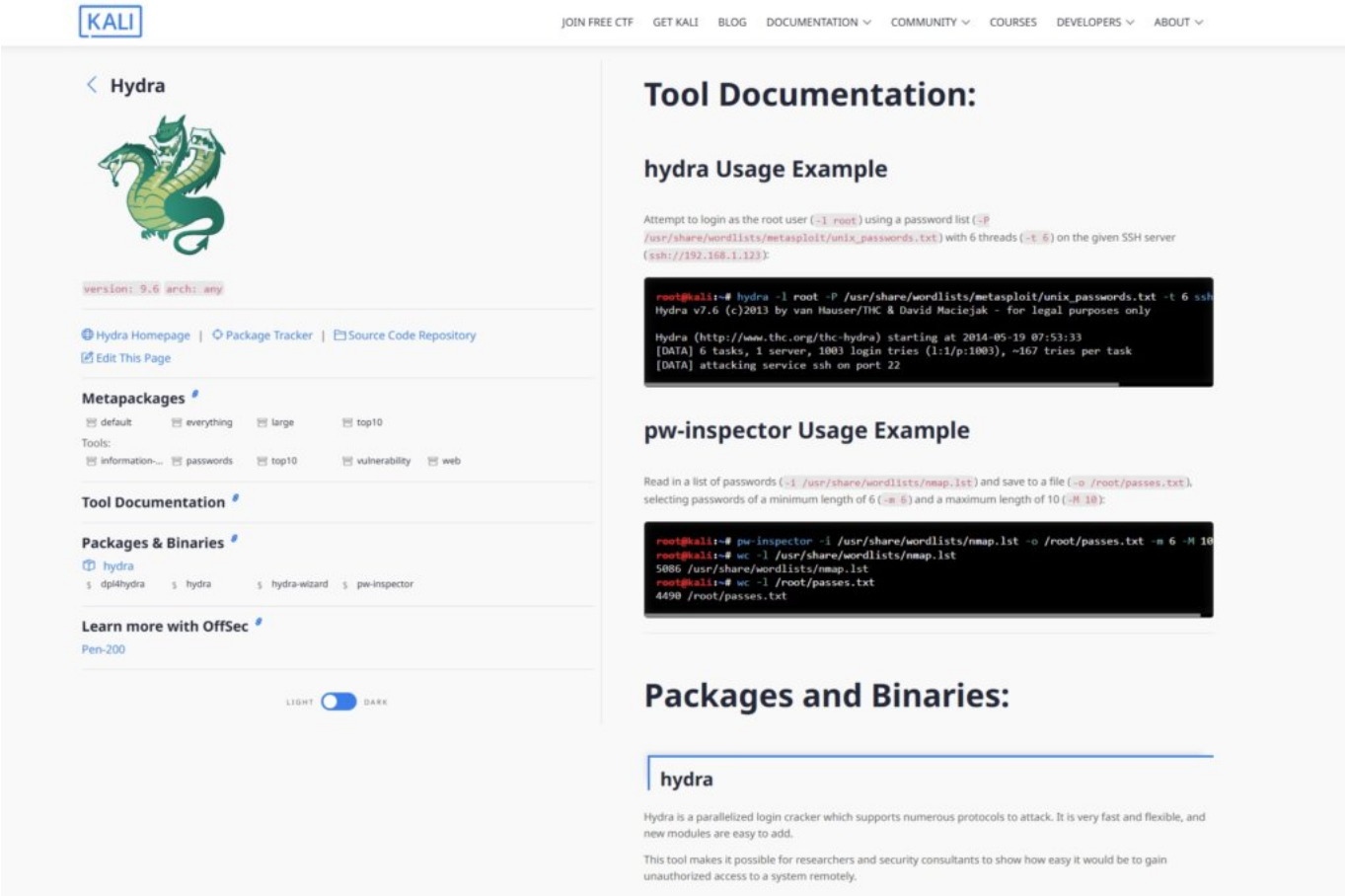
Prvi korak svake sigurnosne revizije započinje prikupljanjem informacija, a u tu svrhu Kali nudi niz alata dobro poznatih sigurnosnim stručnjacima, od starih provjerenih alata kao što je Nmap, legendarni mrežni skener koji služi za otkrivanje aktivnih uređaja, otvorenih portova i verzija operativnih sustava do alata kao što su Maltego (alat za rudarenje podataka i vizualizaciju veza između subjekata, primjerice pojedinaca, grupa, mrežnih stranica, domena, mreža, internetske infrastrukture i povezanosti s online uslugama i čvorovima računalnih platformi kao što su Twitter i Facebook), theHarvester (*open-source* OSINT alat za pasivno prikupljanje informacija o nekoj domeni ili organizaciji – najčešće u ranoj fazi *pentestinga* ili sigurnosne analize) i Recon-ng (*open-source* OSINT / *reconnaissance framework* koji služi za automatizirano prikupljanje informacija iz javnih izvora, uglavnom vezanih uz mrežne ciljeve poput domena i mrežnih aplikacija).

Nakon faze izviđanja, slijedi analiza ranjivosti gdje alati poput Nikta skeniraju mrežne poslužitelje tražeći zastarjele verzije softvera, loše konfiguracije i poznate sigurnosne propuste, dok se Nmapove skripte (NSE) često koriste za dublju inspekciju specifičnih servisa. Nikto je *open-source* alat namijenjen provjeri sigurnosti mrežnih poslužitelja, koji se najčešće koristi u kontekstu etičkog hakiranja, sigurnosnih audita i edukacije. Pokreće se iz komandne linije i radi kao skener ranjivosti s ciljem prikazivanja poznatih slabosti u konfiguraciji i softveru koji stoje „iza“ mrežne stranice ili mrežne aplikacije. Kada se pokrene protiv određenog mrežnog poslužitelja, Nikto sustavno prolazi kroz velik skup unaprijed definiranih testova. U praksi to znači da traži opasne ili barem „zanimljive“ datoteke i skripte – primjerice stara administracijska sučelja, ostavljene testne skripte, *backup* datoteke ili direktorije s uključenim *listingom* sadržaja. Uz to, provjerava koristi li se zastarjela verzija mrežnog servera (poput Apachea, Nginxa ili IIS-a) i pokušava utvrditi postoje li poznate ranjivosti vezane upravo uz tu verziju. Zbog ovakvog načina rada Nikto se vrlo često pojavljuje u ranim fazama

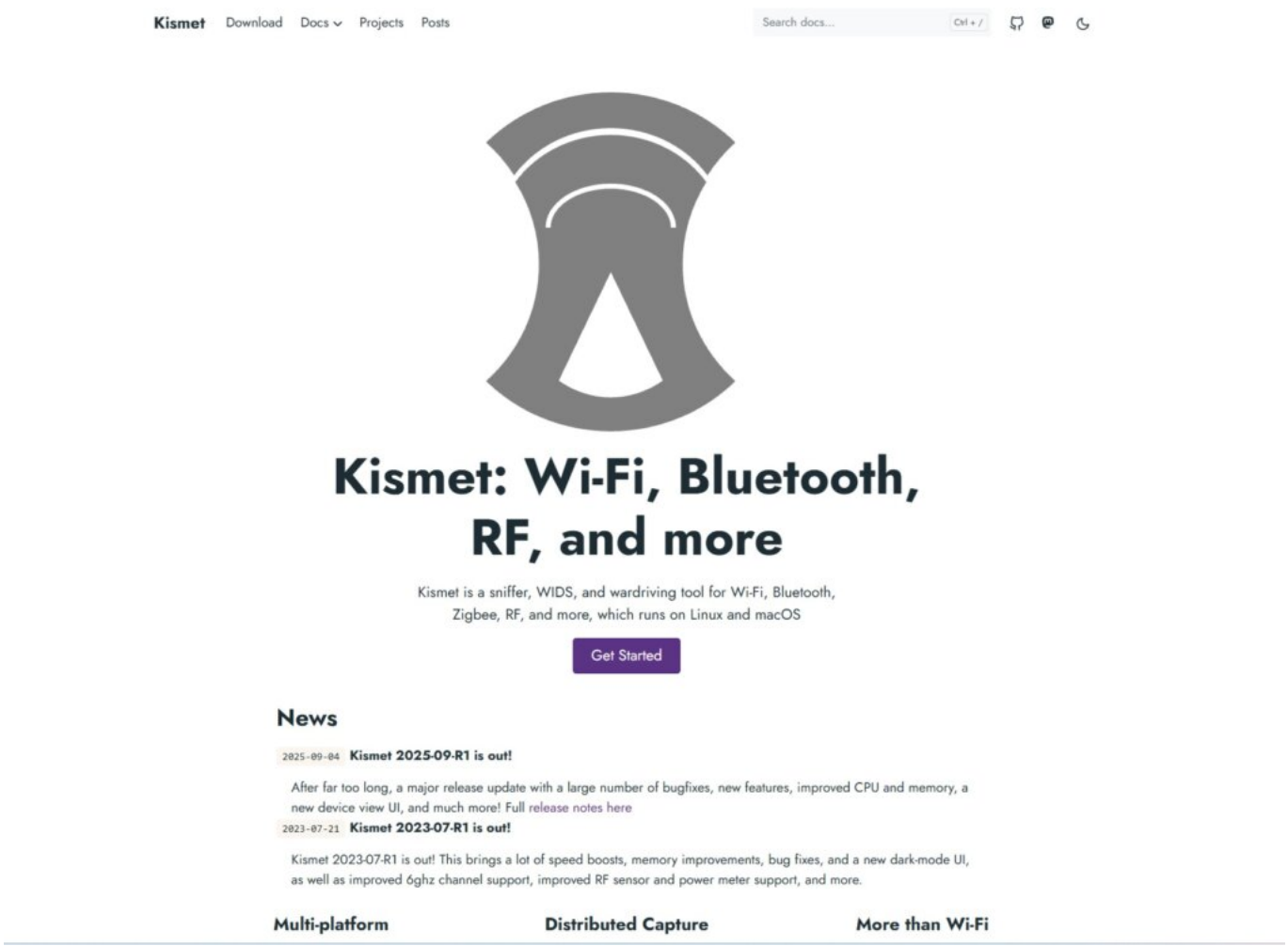
sigurnosnog testiranja. Tzv. pentesteri ga koriste kao brzi „prvi prolaz“ kojim dobivaju sliku o tome koliko je neki mrežni poslužitelj izložen već poznatim problemima. Rezultati skeniranja služe kao polazište za daljnje, dublje analize – ako Nikto otkrije staru verziju softvera, javno dostupnu administraciju ili zaboravljene skripte, to su odlične točke za nastavak istraživanja potencijalnih ulaza u sustav.

Posebno značajna kategorija u kontekstu suvremenih trendova u pogledu izvora i objekata napada je analiza sigurnosti mrežnih aplikacija. Prema podacima koje već više od desetljeća objavljuje Europska agencija za kibernetičku sigurnost – ENISA, mrežne aplikacije su stalno pri vrhu objekata napada. U kolekciji Kali Linux zastupljeno je nekoliko alata koji mogu pomoći u analizi ranjivosti na ovakve napade kao što su SQLMap, alat za automatizirano otkrivanje i iskorištavanje SQL injekcija ili WPSscan, alat za specifičnu analizu WordPress stranica. Kada je riječ o napadima na baze podataka, Kali nudi alate koji se nadovezuju na mrežnu analizu, ali i specifične alate poput SQLiteBrowsera za izravnu manipulaciju lokalnim bazama.

Kali sadrži i niz alata za otkrivanje odnosno pogađanje pristupnih lozinki. Ova kategorija podijeljena je na *online* i *offline* alate. Hydra i Medusa su primjeri alata za brze online *brute-force* napade na mrežne servise poput SSH-a ili FTP-a. S druge strane, za *offline* razbijanje *hashova* lozinki mogu se koristiti alati kao što su John the Ripper, ili noviji i iznimno brzi Hashcat, koji može koristiti suvremene moćne grafičke procesore za ubrzanje procesa dešifriranja.



Za testiranje sigurnosti bežičnih mreža, Kali Linux sadrži industrijski standard, paket alata Aircrack-ng. Ovaj skup programa omogućuje praćenje prometa, lažiranje pristupnih točaka i razbijanje WEP i WPA/WPA2 enkripcije. Uz njega, popularan je i Kismet kao pasivni detektor bežičnih mreža te WiFite koji automatizira proces napada na bežične mreže.



Što se tiče digitalne forenzike, Kali Linux sadrži niz alata kao što su Autopsy, Guymager, Volatility, ExifTool i drugi. Iako se Kali Linux često primarno doživljava kao ofenzivna platforma namijenjena penetracijskom testiranju, distribucija posjeduje raznovrstan ekosustav alata namijenjenih digitalnoj forenzici. Sam sustav moguće je podići u posebnom forenzičkom načinu rada koji osigurava da se prilikom pokretanja sustava ne montiraju unutarnji diskovi niti koristi *swap* particija, čime se jamči očuvanje integriteta digitalnih dokaza i sprječava njihovo slučajno kontaminiranje.

Za forenzičke potrebe, korisnicima je na raspolaganju Sleuth Kit (često označen kao TSK – The Sleuth Kit). TTSK je *open-source* skup alata za digitalnu forenziku, namijenjen analizi diskova i datotečnih sustava te oporavku podataka u forenzički prihvatljivom obliku. Riječ je o zbirci alata naredbenog retka koja omogućuje detaljnu inspekciju datotečnih sustava, no većina istražitelja preferira korištenje njegovog grafičkog sučelja poznatog pod nazivom Autopsy. Autopsy je grafički forenzički alat koji u pozadini koristi TSK kao *engine* za rad s datotečnim sustavima, ali dodaje i dodatne funkcionalnosti te funkcionira kao digitalni preglednik koji stručnjacima omogućuje vizualizaciju strukture diska, pretragu ključnih riječi, analizu elektroničke pošte te generiranje vremenskih crta događaja, čineći ga konkurentnim vodećim (vrlo skupim) komercijalnim rješenjima.

S obzirom da je za forenzički nalaz presudno stvoriti vjernu kopiju izvornog medija kako se ne bi vršio izravan uvid na originalnom mediju, što bi moglo kompromitirati dokaze, važno je imati adekvatne alate za izradu forenzičkih kopija. Kali ih sadrži nekoliko, među popularnijima su Guymager i dc3dd, kao i alat Hashdeep čija je svrha provjeriti kriptografske sažetke (engl. *hashovi*) kako bi se osiguralo da se podaci nisu izmijenili tijekom forenzičke analize. U situacijama kada su podaci namjerno obrisani ili je datotečni sustav oštećen, potrebni su alati za oporavak/povrat podataka koji funkcioniraju na principu prepoznavanja zaglavlja i podnožja datoteka unutar sirovih podataka. Najpoznatiji alati u ovoj kategoriji su Foremost, izvorno razvijen u američkim zračnim snagama te njegova modernija i brža inačica Scalpel. Takvi alati sposobni su „izrezati“ specifične tipove datoteka, poput slika ili dokumenata iz naizgled praznog ili oštećenog prostora na mediju za pohranu. Uz analizu trajnih zapisa na disku, Kali Linux pruža i vrhunske mogućnosti za analizu radne memorije, što je ključno za otkrivanje sofisticiranih napada koji ne ostavljaju tragove na medijima za pohranu podataka kao što je Volatility Framework ili alat Binwalk koji se koristi kod mrežne opreme ili IoT uređaja.

Instalacija Kali Linuxa

Prije instalacije potrebno je s interneta preuzeti aktualnu verziju distribucije. Najpouzdaniji izvor za preuzimanje distribucije je službena mrežna stranica kali.org, budući da preuzimanje s neslužbenih izvora ponekad nosi povećan rizik od dobivanja kompromitirane verzije koja sadrži zlonamjerni softver. Nakon preuzimanja odgovarajuće datoteke, dobra je praksa provjeriti njezin integritet usporedbom SHA256 kriptografskog sažetka (engl. *hasha*) s onim koji je naveden na službenoj stranici, čime korisnik osigurava da datoteka nije mijenjana tijekom prijenosa. Tradicionalni način

instalacije je onaj pri kojem se Kali Linux instalira izravno na hardver računala kao primarni operativni sustav ili u tzv. *dual boot* konfiguraciji uz postojeći Windows ili macOS. S druge strane, najpopularnija i najsigurnija metoda za većinu korisnika je virtualizacija. Ovdje korisnik unutar svog postojećeg operativnog sustava instalira softver poput VirtualBoxa ili VMwarea te pokreće Kali Linux kao virtualni stroj. Kali nudi gotove, unaprijed konfigurirane virtualne slike (VMware i VirtualBox *images*) koje znatno pojednostavljuju ovaj postupak jer više nije potrebno prolaziti klasičnu instalacijsku proceduru. Prednost ovog pristupa je izolacija od glavnog sustava te mogućnost korištenja *snapshotova* koji omogućuju da se korisnik u slučaju greške jednim klikom vrati u prethodno, ispravno stanje sustava.

Zaključak

Temeljna vrijednost alata i kolekcija kao što je Kali Linux zapravo je u demokratizaciji pristupa i znanja. Većina alata koje kolekcija sadrži jest softver otvorenog koda ili drugi softver u pravnom režimu slobodnog korištenja za određene nekomercijalne namjene. Time se omogućuje svim zainteresiranim stranama – svakom studentu, nastavniku, entuzijastu i IT profesionalcu – isprobavanje i istraživanje njihove upotrebe, čime se uklanjaju financijske i tehničke barijere koje su nekoć ograničavale ulazak u ovo vitalno polje, ostavljajući ga rezerviranim za eksperte velikih kompanija ili državnih službi koje su imale pristup ključnim alatima.

Iz edukacijske perspektive treba naglasiti da se učinkovita sigurnosna kultura može izgraditi isključivo potpunim razumijevanjem ofenzivnih tehnika. Iako je većina stručnjaka za kibernetičku sigurnost okrenuta primarno zaštiti kibernetičkih sustava, razumijevanje rizika i načina napada je ključno. Umjesto suhoparnog učenja o definicijama ranjivosti, student u kontroliranom okruženju laboratorija može vidjeti ranjivost na djelu, što rezultira dubljim i trajnijim razumijevanjem. Integracija ovih alata u proces učenja služi kao ključan poligon za razvoj profesionalne etike i

odgovornosti jer dostupnost neizbježno suočava korisnika s ozbiljnim pravnim i moralnim posljedicama njihove upotrebe, potičući razvoj samodiscipline koja je preduvjet za svakog stručnjaka za kibernetičku sigurnost.