Aplikacije Kali Linux operativnog sustava

Brajković, Mateo

Sveučilište Jurja Dobrile u Puli

Fakultet informatike

MATEO BRAJKOVIĆ

Aplikacije Kali Linux operativnog sustava

Završni rad

Pula, listopad, 2022

Sveučilište Jurja Dobrile u Puli

Fakultet Informatike

MATEO BRAJKOVIĆ

Aplikacije Kali Linux operativnog sustava

Završni rad

JMBAG: 030308590,redoviti student

Studijski smjer: Informatika

Predmet: Informacijska tehnologija i društvo

Znanstveno područje: društvena znanost

Znanstveno polje: Informacijske i komunikacijske znanosti

Znanstvena grana: Informacijski sustavi i informatologija

Mentor: Prof. dr. sc. Snježana Babić

Pula, listopad, 2022.

IZJAVA O AKADEMSKOJ ČESTITOSTI

Ja, dolje potpisani_____Mateo_Brajković_____,kandidat za prvostupnika _____Informatike_____ ovime izjavljujem da je ovaj Završni rad rezultat isključivo mojega vlastitog rada, da se temelji na mojim istraživanjima te da se oslanja na objavljenu literaturu kao što to pokazuju korištene bilješke i bibliografija. Izjavljujem da niti jedan dio Završnog rada nije napisan na nedozvoljen način, odnosno da je prepisan iz kojega necitiranog rada, te da ikoji dio rada krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za koji drugi rad pri bilo kojoj drugoj visokoškolskoj, znanstvenoj ili radnoj ustanovi.

Student

_____

U Puli,_21.09.2022._ godine

IZJAVA

o korištenju autorskog djela

Ja, _____Mateo_Brajković_____ dajem odobrenje Sveučilištu Jurja Dobrile u Puli, kao nositelju prava iskorištavanja, da moj završni rad pod nazivom

_____Aplikacije Kali Linux operativnog sustava_____ koristi na način da gore navedeno autorsko djelo, kao cjeloviti tekst trajno objavi u javnoj internetskoj bazi Sveučilišne knjižnice Sveučilišta Jurja Dobrile u Puli te kopira u javnu internetsku bazu završnih radova Nacionalne i sveučilišne knjižnice (stavljanje na raspolaganje javnosti), sve u skladu s Zakonom o autorskom pravu i drugim srodnim pravima i dobrom akademskom praksom, a radi promicanja otvorenoga, slobodnoga pristupa znanstvenim informacijama.

Za korištenje autorskog djela na gore navedeni način ne potražujem naknadu.

U Puli, _21.09.2022._

Potpis _____

SADRŽAJ:

1. UVOD

Cilj rada je analiza Kali Linux i njegovih aplikacija u praksi, kao i u teoriji. Dobivenim istraživanjem izraditi rad koji prikazuje potencijalne aplikacije i mogućnosti koje nam donose razni alati implementirani u operativni sistem. Kali ima ogroman potencijal u informatičkom svijetu, ne samo u smislu da je baziran na Linuxu već da služi za penetracijsko testiranje i rješavanje dosta informatički orijentiranih problema. Takve aplikacije stvaraju cijeli novi svijet mogućnosti, u svakom aspektu moderne tehnologije.

Kali Linux koristi razne preinstalirane alate kojima se mogu riješiti mnogi problemi vezani uz informatiku. Kali Linux je open source os što znači da je besplatan i bilo tko ga može instalirati na svoje računalo kao i izmjenjivati mu kod kako bi postigao neke željene promjene i mogućnost primjene sustava prema svojoj udobnosti. Glavne značajke aplikacija su u svijetu cybersecurity-a ili ti penetracijskom testiranju. Kali Linux je među najpopularnijem sistemu koji se koriste u takve svrhe, osim ljudi koji su zaposleni kao testeri za sigurnost, mnogi koriste kali za hakiranje u ilegalne svrhe.

2. OPĆENITE APLIKACIJE U KALI LINUX-U SUSTAVU

Kali Linux ili skraćeno samo kali je distribucija linux operativnog sustava koja je razvijena za razne upotrebe u IT svijetu, među kojima je najpoznatija da se koristi u svrhe penetracijskog testiranja. Iako je prvenstveno korišten za provjeravati sigurnosti u sustavima ima koristi i u drugim aspektima informatike. Dolazi preinstalirana s brojnim alatima koji rade najbolje u linux okruženju. Prethodna inačica Kali Linux-a je bila backtrack; backtrack je stvoren spajanjem 3 različitih distribucija: IWHAX, WHOPPIX, Auditor. Kali po prvi put izlazi 2013. godine.

Slika 1. Kali Linux logo (https://www.kali.org/, 2022)

Kali Linux je baziran na Debian linux distribuciji, što znači da koristi skoro čitavu arhitekturu Debian softvera, neki od paketa su modificirani za poboljšanu sigurnost i smanjivanja ranjivosti. kali je isto tako i open-source što znači da je besplatan i dostupan svima koji ga žele koristiti. Isto jer je open-source korisnici imaju mogućnost uređivanja izvornog koda Kali Linux-a svojim potrebama. Dolazi preinstaliran s više od 600 aplikacija koje jedan tester može zatrebati. Pošto se koristi za testiranje sigurnosti, za testirati bežične mreže kali podržava veliki raspon podrške za bežične mrežne kartice i prilagođen kernel za "modifikaciju" mrežnih paketa.

3. UTJECAJ DRUŠTVA NA RAZVOJ APLIKACIJA KALI LINUX-A

Tijekom godina svi alati koji služe za nekakvu sigurnost ili testiranje sigurnosti su se razvijali sve više i više. Počevši od samog sustava prije nego li je uopće postojao, postojali su drugi sustavi koje su ujedinili da bi se kreirao Kali Linux. Kako se i sama kompleksnost sigurnosti sustava poboljšavala tako su i metode za prijeći preko te sigurnosti nekog sustava sve više razvijenije. Kako je potreba za sigurnost veća s vremenom tako treba više ljudi koji će radit na toj sigurnosti. Tako je nastala grana cyber sigurnosti gdje je cilj zaštititi nekakav sustav od zlonamjernih hakera. Tu dolazi i do pozicije penetracijskog testiranja gdje je svrha napadati sustav i tražiti mu ranjivosti kako bi se sve te ranjivosti uklonile. Kali Linux-u su sve više razvijene aplikacije za te grane informatike. Kako se sustavi probaju eksploatirati, jednom kad su pronađene te eksploatacije spremaju se u neku bazu svih postojećih eksploatacija. Tada postaju manje efektivne je će alati testirati i za te eksploatacije, također postoje još neotkrivenih eksploatacija koje se nazivaju „zero day exploits“.

U prošlosti kako bi haker uspio hakirati neki sustav ili ukrasti podatke nije bilo toliko sigurnosti da ga previše netko zaustavi, dok u sadašnjosti kako se tehnologija naglo razvila postaje sve više kompliciranо. Nije nemoguće već otežano, ako osoba koja je žrtva ne uzme dobre korake u zaštiti svojih podataka, napadač može lagano dobit pristup njihovim lozinkama i podacima. Današnji sustavi sadrže u sebi i dolaze ili se mogu instalirati razni programi za zaštitu od virusa i za sigurnost sustava koje stvaraju solidnu količinu zaštite. Također kako se web aplikacije razvijaju teško je napadati ili provaljivati u nečiji račun na tim aplikacijama, poznatije i veće web aplikacije imaju profesionalne osobe koje prate i testiraju sigurnost sustava na dnevnoj bazi. Isto većina web aplikacija zahtijeva pri odabiru lozinke veću kompleksnost kako bi se računi osigurali.

Kako je sva sigurnost veća s vremenom, razvijaju se također uređaji koji olakšavaju hakiranje nekoga, ali u većini slučaja zahtijevaju fizički pristup sustavu. Jednom kad ubačeni u sustav lagano se može dobiti nekakvi podaci ili napraviti „backdoor“ u sustave.

4. UTJECAJ APLIKACIJA KALI LINUX-A NA RAZVOJ DRUŠTVA

Kao osoba koja može provaljivati u sustave bira se hoće li se te vještine iskoristiti kao white hat haker gdje pomaže osigurati sustav kako bi imao što manje ranjivosti, ili kao black hat haker koji koristi te vještine za krađu podataka u svrhu da manipulira nekom žrtvom ili proda te podatke radi financijskog dobitka. Kako je tehnologija napredna postoji mnogo ljudi koji ne moraju niti znati se baviti Kali Linux-om kako bi prevarili ljude da pomoću socijalnog inženjeringa ukrali novce ili podatke nekoj osobi. Također osobe s vještinama hakiranja znaju koristiti svoje znanje u anarhističke svrhe samo da se kreira kaos i sruše veće korporacije. Hakeri imaju pristup „deepwebu“ gdje mogu svoje vještine prodavati za novce ili samovoljno prodavati već ukradene podatke.

Na drugu stranu netko može iskoristiti ove aplikacije za digitalnu forenziku, što se i koristi da se pronađu skriveni podaci ili obrisani podaci koje je jedan haker probao ukloniti. Aplikacije tijekom forenzike možete raditi na zadacima kao što su enkripcija, probijanje lozinki, forenzička analiza, napadi na bežičnu mrežu, obrnuti inženjering zlonamjernog softvera, procjena/testiranje ranjivosti i još mnogo toga koristeći Kali Linux. Potpodručje forenzičke znanosti poznato kao "digitalna forenzika" bavi se dohvaćanjem i ispitivanjem podataka iz opreme za obradu informacija kao što su računala, mobilni telefoni, mediji za pohranu i drugi uređaji.

Kako su sustavi mogući za provaliti i postaviti „backdoor“ u njih, hakeri imaju mogućnosti špijuniranja što se radi na tim sustavima. Jedan od najjednostavnijeg i najpoznatijeg načina toga je „keylogger“ koji omogućuje da pomoću sesije zabilježuju se udarci tipki, i time dobije što je sve žrtva upisivala pomoću tipkovnice uključujući osjetljive podatke i lozinke. Istom metodom haker može koristiti bilo koji aspekt računala žrtve, kao naprimjer kopiranje podatka s računala, manipuliranje tog sustave, korištenje uređaja povezanih na taj sustav kao što je kamera da bi se gledalo kroz nju i slične aplikacije.

5. APLIKACIJE PENETRACIJSKOG TESTIRANJA

Kali Linux ima najviše aplikacija kao sustav za ispitivanje penetracije ili penetracijsko testiranje, penetracijsko testiranje je proces koji uključuje simuliranje stvarnih napada radi procjene rizika potencijalnog kršenja sigurnosti. Na testiranju, za razliku od procjene ranjivosti, tester ne samo da otkriva ranjivosti koje bi napadači mogli koristiti, ali i iskoristiti ranjivost, gdje je to moguće, za procijeniti što bi napadač mogao dobiti nakon uspješne eksploatacije. Penetracijsko testiranje predstavlja kontinuirani ciklus istraživanja, i nakon nekog vremena napada na sustav. Napad mora biti strukturiran i proračunat, po mogućnosti testiran u laboratorijskom okruženju. Svako toliko, neke kompanije su izložene napadima zbog naprimjer loših verzija web aplikacija, to se zna događati zbog loše pokrpanih verzija softvera.

Velike tvrtke mogu biti žrtve napada raznim "SQL injection" napadima, socijalno inženjerstvima napadima na radnike, i probijanjem slabih lozinka. Testeri imaju svoju metodologiju penetracijskog testiranja, svaki profesionalac za sigurnost razvija svoju vlastitu metodologiju, temeljenu na općoj tehnici i svojim tehničkim vještinama.

5.1. Vrste penetracijskog testiranja

Tester može biti tražen da provjeri ranjivosti jedne ili više klijentno prilagođenih web aplikacija. Moguće su potrebe za izvođenje napada socijalnim inženjerstvom i napadi sa strane klijenta za dobiti pristup klijentovoj internoj mreži. Neki testovi će zahtijevati da se testira unutar sustava, kao zloćudan zaposlenik ili napadač koji je već probio perimetar. Dok neki zahtijevaju da se simulira napad s interneta (Baloch, 2014).

Može se još od nekih slučajeva dogoditi da zahtjeva da se testira i klijentova bežična mreža u uredima ili čak i procjena sigurnosti klijentove fizičke sigurnosti sustava. Postoje razni načini pristupa, dva najčešća koja su prihvaćena od strane industrija su white box(tester je upoznat sa sustavom) i black box(tester nije upoznat sa sustavom) pristup.

5.1.1. Black box pristup

Kod ovog pristupa, tester nije upoznat s implementiranim tehnologijama i mrežnom infrastrukturom ciljane organizacije. Kroz primjenu raznih tehnika hakiranja i testiranjem, ranjivosti se mogu potencijalno iskoristiti. Kad tester otkrije ranjivosti mora ih klasificirati i odrediti im prioritet prema razini rizika. Rizik se određuje prema veličini prijetnje koju pojedina ranjivost predstavlja (Baloch, 2014).

U idealnom slučaju tester pronalazi sve napade vektora koji ugrožavaju kompaniju. Poslije izvođenja testiranja, stvara se report u kojem su zapisane potpune informacije za sigurnosti, kategorizaciji i prebacivanje postotka sigurnosti u korporativni smisao. Black box pristup je obično skuplja usluga nego white box.

5.1.2. White box pristup

Za razliku od pristupa crne kutije, tester u pristupu bijele kutije upoznat je s infrastrukturom tvrtke i svim internim tehnologijama. Ovaj pristup pruža testeru mogućnost postizanja boljeg aspekta pregleda i identifikacije sigurnosnih rizika uz minimalan napor i maksimalnu točnost. Organizaciji pruža bolju korist od pristupa crne kutije, budući da se mogu pronaći i popraviti sve ranjivosti povezane s internim okruženjem organizacije, eliminiraju se sigurnosne rupe, što zlonamjernim korisnicima otežava prodor izvana. Koraci pristupa bijele kutije slični su koracima pristupa crne kutije (Baloch, 2014).

Pristup bijele kutije dobar je način za uklanjanje potencijalnih ranjivosti u ranim fazama organizacije tako da se otkriju što je prije moguće i da ih uljezi ne mogu iskoristiti. Ovaj pristup zahtijeva manje znanja, vremena i troškova nego pristup crne kutije.

5.2. Metodologije kod ispitivanja sigurnosti

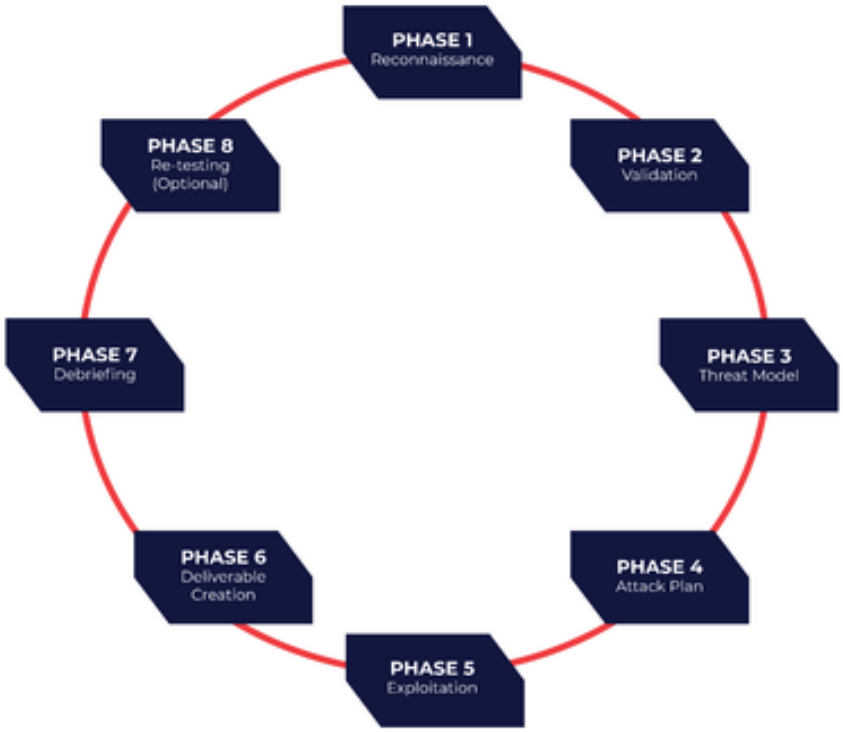
Postoji nekoliko metoda za procjenu sigurnosti. Primjenom ovih metoda mogu se planski otkloniti rizični i kompliciranі problemi sigurnosne procjene unatoč njihovoj veličini i složenosti. Neke od ovih metoda koriste tehničke aspekte testiranja, dok su druge usredotočene na upravljačke vještine i rijetko se temelje na oboje. Glavna prednost takvih metoda je izvođenje testiranja korak po korak kako bi se točno odredila sigurnost sustava (Allen, 2016).

Najčešće metodologije kod procjene sigurnosti koje prikazuju veći aspekt tijekom procjene sigurnosti mreže su: Open Source Security Testing Methodology Manual, Open Web Application Security Project Testing Guide, Web Application Security Consortium Threat Classification, Penetration Testing Execution Standard, Information Systems Security Assessment Framework.

Ovakve metodologije pomažu stručnjacima za izabrati najefikasniji način koji je najučinkovitija sa zahtjevima klijenta. Metodologija 1 i 2 daju općenita uputstva i načine za ispitati sigurnost za skoro svaku vrstu informacija. Metode OWASP i WASC većinom se koriste za web aplikacije da im se provjeri sigurnost. PTES daje uputstva za sve načine penetracijskog testiranja. Važno je reći da za sigurnost sustava je potreban stalni nadzor i da je test "snimka" prikaz sigurnost sustava samo tijekom testiranja. Isto tako uporaba jedne metodologije ne mora značiti da će se pružati potpunu sliku proces procjene rizika. Ima dovoljno metodologija za testiranje sigurnosnosti, za odabrati pravu metodu zahtjeva se oprezan selektivan proces kojim su određeni kvaliteta testiranja i njegov trošak.

5.3. Opći model pri penetracijskom testiranju

Kali Linux je opremljen što se tiče penetracijskog testiranja opremljen s mnogo alata i procjenu ranjivosti.Ti alati su veoma korisni kad se koriste neki postupci, bez dobrog modela može doći do neuspjeha testiranja i loših rezultata. Zato je bitno kod testiranja da postoji dobro strukturiran model koji je izuzetno bitan iz tehničke i upravljačke pozicije. Ovakav model testiranja je najviše viđen korištenjem tehnika testiranja penetracije „black box“ i „white box“.



Slika 2. Faze penetracijskog testiranja (https://www.redlegg.com/penetration-testing/physical-penetration-testing, 2022)

Ovaj opći model omogućuje pregled nekih temeljnih faza koje bi tester trebao proći kroz tijekom testiranja. Ovisno o fazi testiranja, ispitivač mora slijediti određene postupke u modelu kako bi učinkovito dovršio procjenu sigurnosti.

Koraci koje tester treba proći tijekom testiranja su:

1. definiranje opsega - Prije procjene tehničke sigurnosti, temeljito razumijte i upoznajte se s mrežnim okruženjem koje ćete testirati. Kako bi ocjenjivač uspješno proveo testove, treba dobro poznavati tehnologiju koja se testira, njezine funkcije i način rukovanja mrežnim okruženjem.

2. prikupljanje informacija - U ovoj fazi ispitivač koristi mnoge javno dostupne izvore kako bi saznao što više o svojoj meti. Ove podatke moguće je pronaći putem internetskih izvora (forumi, oglasne ploče, blogovi, društvene mreže...) kao i putem raznih tražilica (google, yahoo!...). Revizor koji prikuplja informacije također može koristiti Kali Linux alate za prikupljanje mrežnih informacija o DNS poslužiteljima, bazama podataka, adresama e-pošte, osnovnim informacijama i računima. Što je veća količina informacija, to je veći postotak vjerojatnosti da se penetracijski test može uspješno izvesti (Weidman, 2014).

3. detekcija ciljanog područja - glavni zadaci su identificirati status mreže, operativni sustav i stvoriti sliku mrežne arhitekture koja nam daje pregled međusobno povezanih tehnologija i uređaja. Korištenjem naprednih alata Kali Linux dobiva uvid u hostove i računala spojena na mrežu, njihove operativne sustave koje koriste te karakterizira svaki uređaj prema njegovoj ulozi u mreži. Alati koriste aktivne i pasivne tehnike otkrivanja mrežnog protokola za izdvajanje korisnih informacija.

4. Nabrajanje - Glavni cilj ove faze je stvoriti popis otvorenih portova na ciljnom sustavu. Kada se pronađu otvoreni portovi, jedan se port može povezati s protokolom na tom portu. Portovi se mogu skenirati uz pomoć brojnih tehnika koje daju čak i ako je računalo zaštićeno vatrozidom ili sustavom za otkrivanje upada, pregled stanja portova (IDS). Usluge mapiranja uspostavljenih veza pomažu u istraživanju potencijalnih slabosti u mrežnoj infrastrukturi. Ova faza se koristi za identifikaciju ranjivosti mrežnih uređaja koje potencijalno mogu omogućiti upad u sustav. Uz korištenje Kali Linux alata, revizor može automatizirati ovu fazu.

5. mapiranje ranjivosti - U ovoj fazi ranjivosti se identificiraju i analiziraju na temelju otvorenih portova. Ovaj se postupak može izvesti pomoću mnogih automatiziranih alata za testiranje ranjivosti mreže i web stranica. Procjena se može raditi i ručno, ali zahtijeva više vremena i više stručnog znanja. Također postoji pristup u kojem revizor kombinira oba procesa

kako bi proizveo točniju procjenu ranjivosti za sve poznate i nepoznate ranjivosti u mrežnom sustavu.

6. društveni inženjering - igra važnu ulogu kada nema alternativnog pristupa mreži. Za razliku od procjene ranjivosti, ovo koristi ljudski vektor za prodor u sustav. Korisnik je prevaren da izvrši zlonamjerni kod koji procjenitelju daje pristup stvaranjem "stražnjih vrata" na nekakav sustav, čak i ako nema ranjivosti u protokolima ili uslugama. Postoji mnogo načina društvenog inženjeringa, od kojih neki uključuju osobu koja glumi administratora koji pomaže "phishing" stranici da natjera korisnika da unese svoje podatke i na taj način osoba dobije te podatke ili slanjem e-pošte natjera korisnika da preuzme zlonamjerni kod koji, kada se pokrene, daje osobi udaljeni pristup kompromitiranom računalu. Prilikom izvođenja ove faze imajte na umu da zahtijeva razumijevanje ljudske psihologije kao i dobro poznavanje državnih zakona koji se odnose na društveni inženjering.

7. iskorištavanje ranjivosti - Nakon proučavanja otvorenih ranjivosti, može se odrediti točka upada na temelju dostupnih "iskorištavanja". Postoji nekoliko repozitorija koji sadrže gotove "eksploatacije". Također je moguće modificirati kod ovih eksploatacija tako da ispravno rade na sustavu koji se testira, pod uvjetom da na tom sustavu postoji ranjivost za koju eksploatacija postoji. Korištenje društvenog inženjeringa kako bi iskorištavanje lakše došlo do kupca.8. eskalacija privilegija - Ako se testeru odobri pristup ciljnom sustavu, test se može proglasiti uspješnim. Ovisno o privilegijama korisnika preko kojeg je tester dobio pristup sustavu, moguće je obavljati određene aktivnosti. Privilegije se mogu podići pomoću lokalnih eksploatacija koje, ako se uspješno izvrše, mogu podići privilegije na administratorsku razinu gdje su mogući daljnji napadi.

8. održavanje pristupa - Ako revizor treba ponovno dobiti pristup sustavu kako bi se olakšao proces testiranja ponovnog prodora korištenjem različitih protokola tuneliranja, proxyja ili "end-to-end" veza, može se uspostaviti "stražnja vrata" kako bi se osiguralo pristup koliko god je potrebno.

9. dokumentiranje i izvješćivanje - S etičkog stajališta, ova faza je važna jer daje timu pregled za metode korištene za prodor u sustav i uputstva za popravljanje sigurnosnih nedostataka. Izvješća se mogu iskoristiti u usporedbi integriteta sustava prije i nakon testa prodora.

6. APLIKACIJE U IZVIĐANJU MREŽNOG PROMETA

Kali Linux ima najbitniju aplikaciju možda u izviđanju. Izviđanje je prva stvar koja se radi kada se obavlja nekakvo testiranje pomoću Kali Linuxa. Što su opsežnije informacije prikupljene, to je veća šansa za pronalaženje i iskorištavanje ranjivosti. Što više informacija se uspije prikupiti tu postoji više potencijalnih napadačkih vektora za moguće penetracije sustava Cilj izviđanja je prikupljanje informacija o aplikacijama, bazama podataka, korisnicima, poslužiteljima i interakciji između aplikacija i korisnika (Hixon, Hutchens, 2017).

Iako svi žele preuzeti sustav, izviđanje može biti najvažniji korak u procesu hakiranja. U određenim slučajevima, izviđanje može oduzeti do 80% vremena procesa hakiranja. Vaši pokušaji hakiranja mogu biti neučinkoviti bez temeljitog izviđanja. Tehnologija koja se koristi ima vrlo specifične ranjivosti ili iskorištavanja. Operativni sustav (OS), aplikacije koje se koriste, priključci i usluge, pa čak i jezik sustava mogu potpasti pod ovu kategoriju. Prije nego što odaberemo najbolju strategiju za iskorištavanje prednosti sustava, prvo moramo pribaviti sve te informacije, a ponekad i više (https://www.hackers-arise.com, 2022).

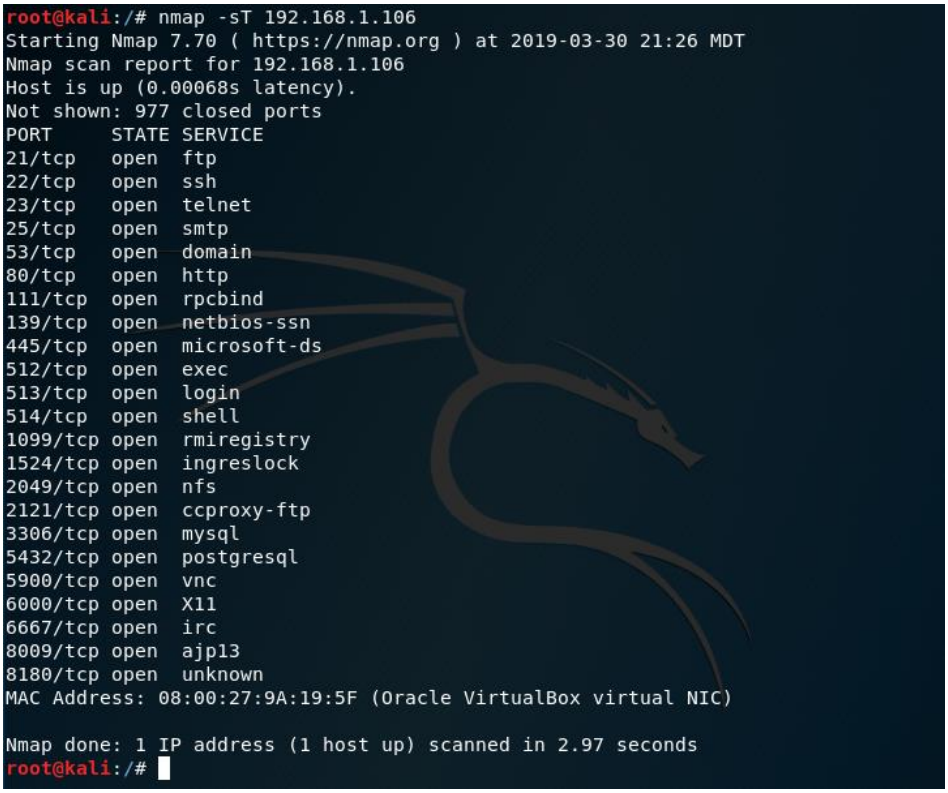
Ključna faza u protivničkom ciklusu je izviđanje. Hakeri često troše puno više vremena na planiranje svojih napada nego na njihovu provedbu. Osim toga, neprecizno ili nedostatno izviđanje može dovesti do katastrofe za napad. Izviđanje se može provoditi aktivnom ili pasivnom strategijom. Ove dvije tehnike često koriste testeri kako bi procijenili ranjivosti i zaustavili opasno iskorištavanje. Tehnike aktivnog izviđanja kao što su ping sonde, skeniranje portova i traceroute primjeri su iz stvarnog svijeta. Kako bi identificirali podatke koji se mogu iskoristiti, napadači rade izravno s uređajima koje su odabrali. Naprotiv, pasivno izviđanje. Neizravne metode koje napadači koriste za dobivanje informacija uključuju fizički nadzor zgrada, prisluškivanje razgovora, lociranje dokumenata koji sadrže prijave i lozinke, Google štrebere, open source intelligence (OSINT) i napredni Shodan, packet sniffer, pretraživanja i WHOIS informacije (https://www.esecurityplanet.com/threats/how-hackers-use-reconnaissance/. 2022).

6.1. Korištenje alata Nmap

Što se tiče izviđanja Nmap je jedan od najboljih i najpoznatijih alata za to, ima veliki raspon mogućnosti koje bi mogle zatrebati nekoj osobi. Nmap služi za otkrivanje statusa poslužitelja, provjeru otvorenih TCP i UDP portova i otkrivanje vatrozida, otkrivanje servera i njihove verzije, itd. Nmap ima vrlo jednostavnu sintaksu za koristiti:

nmap {Scan type(s)] [Options] {target specification}

Najbolje i najjednostavnije skeniranje se može izvesti pomoću nmap je TCP skeniranje. Radi tako da pokušava stvoriti „TCP 3-way handshake" na svakom portu koji skenira. Ako uspije port je smatran otvorenim. Sintaksa za TCP skeniranje je jednostavna: nmap -sT <IP adresa>



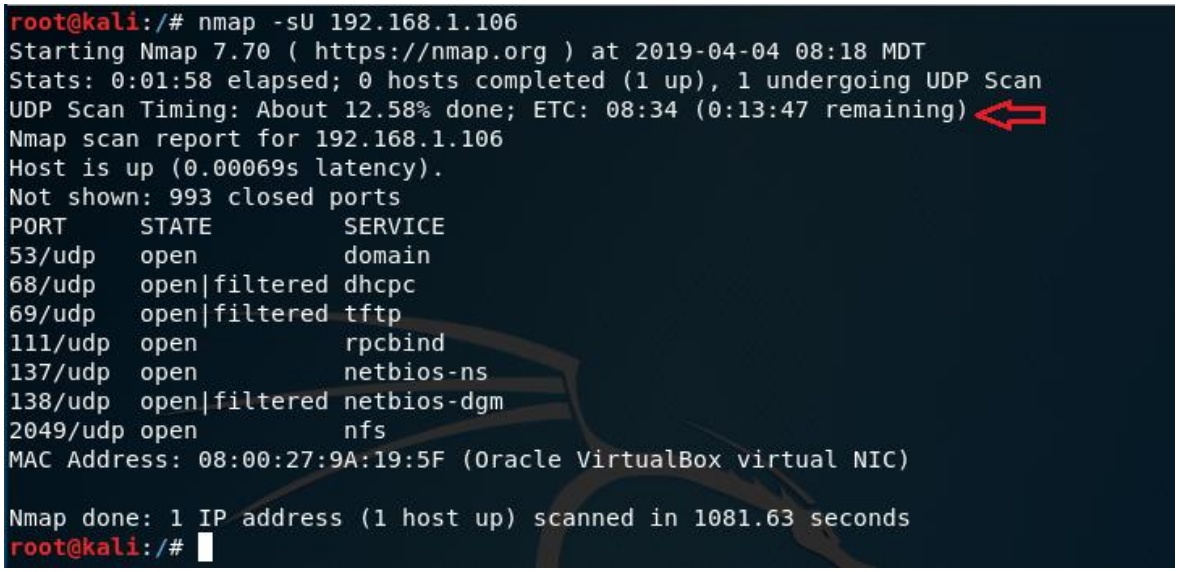
Slika 3: Prikaz rada TCP skeniranja (https://www.hackers-arise.com, 2022.)

Kako bi provjerili funkcionalnost servera to je izvedivo4 tako da provjerimo da li server odgovara na zahtjeve i to možemo provjeriti pomoću naredbe:

nmap -sn <ip adresa>

Ako je server funkcionalan, sljedeća stvar koju radimo je da pogledajmo ima li poslužitelj otvorene portove; to je zamislivo izvesti jednostavnom naredbom:

Nmap <ip adresa servera >

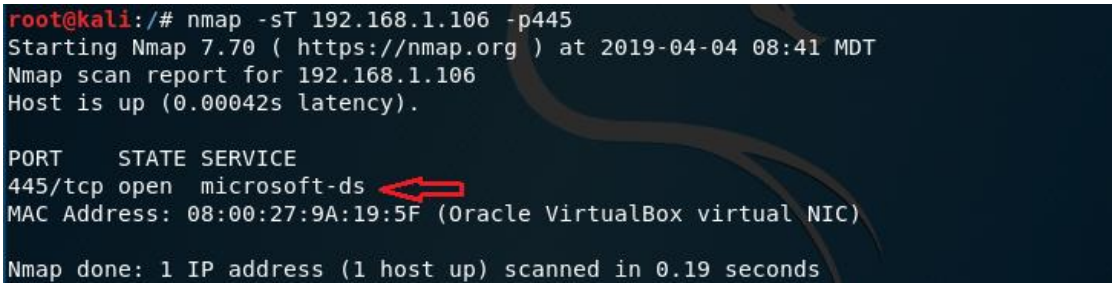


Slika 4. Prikaz rezultata UDP skeniranja (https://www.hackers-arise.com, 2022.)

Zbog nešto drugačije i nejasnije tehnike koju koristi UDP za označavanje zatvorenog porta u usporedbi s TCP-om, UDP skeniranja traju znatno dulje od TCP skeniranja. Vrijeme TCP skeniranja u mom slučaju bilo je 2,97 sekundi, dok je vrijeme UDP skeniranja bilo 1081,63 sekunde. Sintaksa za skeniranje UDP porta je slična kao i kod TCP-a, zapisuje se kao:

nmap -sU <IP adresa>

Ako jednostavno trebamo saznati je li jedan port otvoren. Budući da smo svjesni da napad EternalBlue cilja na SMB na portu 445, možemo razmisliti o njegovoj upotrebi protiv ovog stroja. Jednostavnim dodavanjem -p nakon ciljne IP adrese i broja porta, provjerimo ima li ovaj stroj otvoren port 445. Sintaksa glasi: nmap -sT <IP adresa> - p <broj porta> (https://www.hackers-arise.com, 2022.)



Slika 5. Prikaz skeniranja specifičnog porta (https://www.hackers-arise.com, 2022.)

Nakon što provjerimo otvorene portove, korak dalje je provjeriti verzije usluge i operativni sustav koji pokreću ti servisi izvode(Weidman, 2014)

Za provjeru verzije i operacijskog sustava možemo koristiti naredbu:

nmap -sV -O <ip adresa servera/ime servera>

U Nmap repozitoriju dostupno je nekoliko unaprijed napisanih skripti koje se mogu koristiti. WHOIS skripta jedna je od poznatijih; šalje zahtjev regionalnim internetskim registrima za WHOIS i pokušava dobiti pojedinosti poput raspona dodijeljenih IP adresa, IP adrese poslužitelja, kontakt podataka za domenu itd.

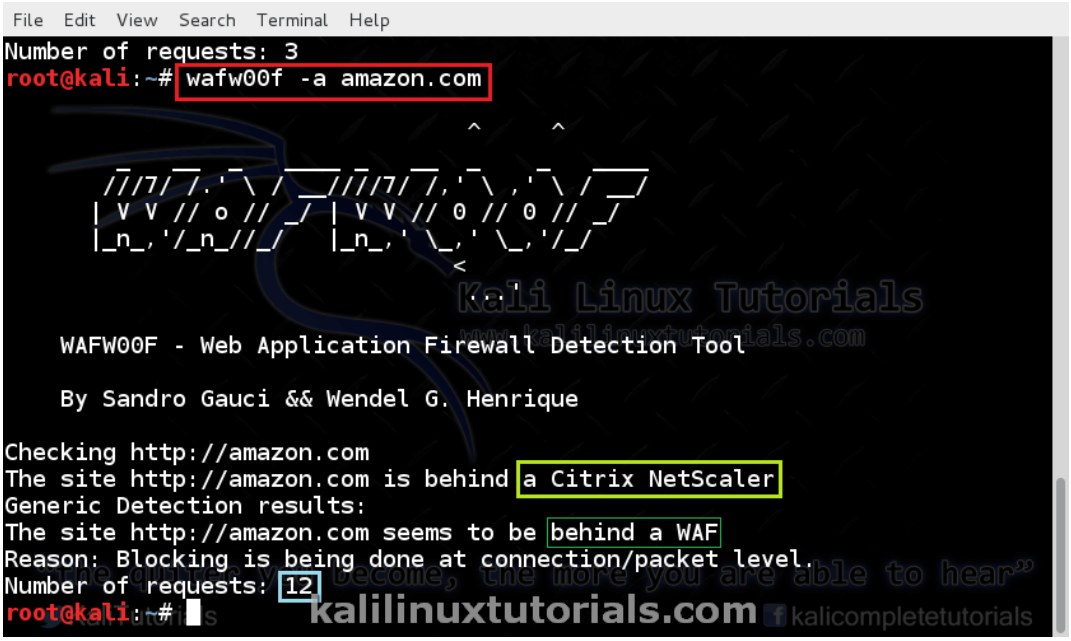
6.2. Otkrivanje "firewall"-a za sigurnost aplikacija

"Web application firewall" je aplikacija koja prati i provjerava mrežne paket obično na bazi potpisa ili reguliranih fraza koje dolaze do web servera da se identificira i blokira zlonamjerne pakete. Ako firewall blokira zahtjeve za server ili blokira pristup s IP adrese revizor se može suočiti s mnogim problemima. Kod izviđanja spadaju procesi otkrivanja i identifikacije firewall-a, IDS/IPS sustava, to se odrađuje da bi se moglo izviđalo neometano.

Postoje nekoliko skripta unutar Nmap repozitorija koje mogu poslužiti za provjeravanje prisutnosti firewall-a, jedan od skripta je:

Nmap -p80 --script=http-waf-detect <ip adresa servera/ime servera>

Nasuprot http-waf-detect skripte skripta http-waf-fingerprint daje informaciju o kojem se firewallu i IDS/IPS sustavu radi. Druga od skripta koja pomaže otkriti firewall unutar Nmap repozitorija je: Nmap –script=http-waf-fingerprint



Slika 6. Prikaz rada wafw00f alata na amazon web stranicu (https://kalilinuxtutorials.com/wafw00f/, 2022.)

Jedan od popularnijih alata za detekciju firewall-a je wafw00f, radi tako da šalje nekoj IP adresi normalni http zahtjev i analiziran odgovor. Ovo identificira broj WAF solucija. Ako nije uspješan, šalje brojne(potencijalno zlonamjerne) HTTP zahtjeve i koristi jednostavnu logiku da deducira o koje se WAF-u radi. Ako ni to ne uspije, analizira odgovore i koristi još jedan algoritam da proba pogoditi da li WAF ili zaštitna mjera aktivno reagira na napade (http-waf-fingerprint NSE script—Nmap Scripting Engine documentation, 2022). Primjenjuje se na načina:

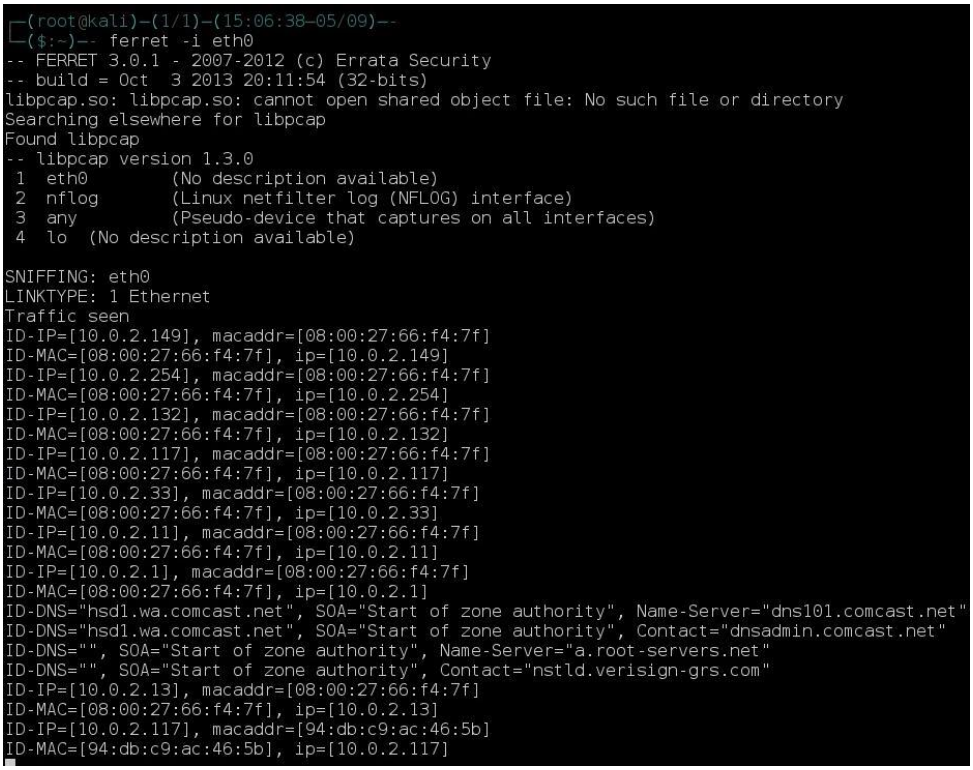
Wafw00f <IP adresa>

6.3. Izviđanje "source code"-a web aplikacije

Prilikom analize "izvornog koda" osoba može vidjeti programsku logiku web stranice ili aplikacije koja se na njoj izvodi i steći uvid u to postoje li ranjivosti koje se mogu iskoristiti. Stoga je analiza izvornog koda bitan korak u izviđanju. Vanjske datoteke i poveznice koje koriste mogu se pronaći analizom. Za bolji pregled možemo koristiti i Firebug alat. Ovo je proširenje web preglednika koje se može koristiti za analizu internih dijelova internet stranica kao što su CSS klase, tablice, okviri itd. Također može prikazati DOM objekte, kodove grešaka i izmjenu informacija između preglednika i poslužitelja.

6.4. Dohvaćanje cookie-a i njegova modifikacija

Kolačići su informacije koje web poslužitelj šalje klijentu (pregledniku) kako bi lokalno pohranio određene informacije o određenom korisniku. U novijim web aplikacijama kolačići se koriste za pohranu korisničkih podataka, kao što su konfiguracija teme, raspored objekata na web stranici, prethodne aktivnosti i (što je najvažnije za testera) identifikatori sesije (Najera-Gutierrez, 2016).



Slika 7. Prikaz rada ferret sučelja (https://www.wonderhowto.com, 2022)

Fantastičan mali alat koji radi s Hamsterom zove se Ferret. Otima kolačiće sesije koji putuju LAN-om. Svim čime se Ferret dočepa "manipulira" Hamster, koji djeluje kao opunomoćenik. Jedini nedostatak je što Ferret ne uključuje 64-bitnu verziju Kali. Moramo dodati i386 (32-bitno) spremište kako bismo ga instalirali. Kad se sve instalira, prvo se pokreće ferret s naredbom ferret -i interface. Nakon pokrećemo hamster s naredbom hamster u terminalu. Tu se počinju dohvaćati cookie-i koje može se pregledati na pregledniku tako da se upiše localhost:1234, tu također se može postaviti na kojem sučelju da hamster sluša kao naprimjer eth0 (https://www.wonderhowto.com, 2022).

6.5. Pronalaženje datoteka na serveru pomoću DirBuster alata

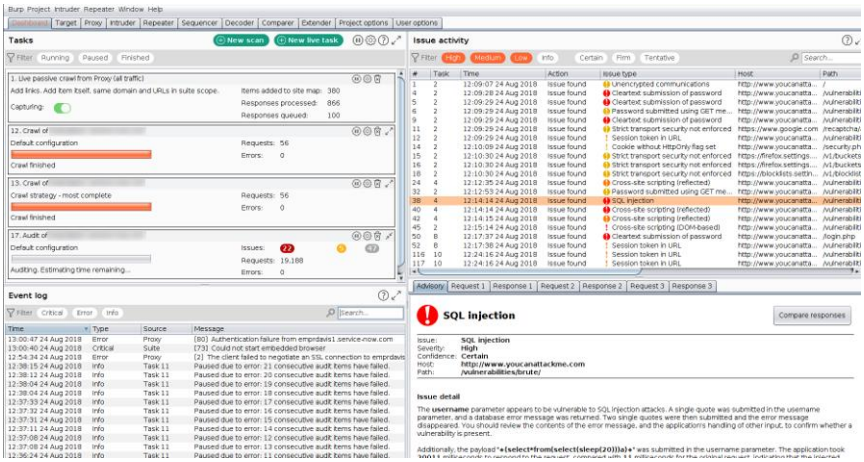
DirBuster je alat sustava Kali Linux za lociranje postojećih datoteka i direktorija na web poslužitelju. Alat DirBuster koristi se na sljedeći način: Prvo se mora odrediti cilj, tj. web poslužitelj za koji će se izvršiti pretraga postojećih datoteka i direktorija. Zatim morate odrediti treba li alat koristiti rječnik korisnički definiranih ključnih riječi za pretraživanje direktorija (Brute Force na temelju popisa) ili bi alat trebao sam generirati rječnik (Pure Brute Force). Nakon toga trebate odabrati druge opcije ovisno o tome što želite postići. Kada je sve konfigurirano, možete započeti pretragu (https://null-byte.wonderhowto.com/how-to/hack-like-pro-find-directories-websites-using-dirbuster-0157593/, 2022).

Slika 8. Korištenje alata na webscantest.com web stranicu (https://www.hackers-arise.com, 2022)

DirBuster možemo koristiti jednostavnom sintaksom kao što je dirb <IP adresa>. No ako se želi upotrijebiti specifična lista riječi koja se želi iskoristiti samo se nadodaje s putanjom na tu listu u nastavku sintakse.

7. APLIKACIJE PRI INDEKSIRANJU WEB APLIKACIJA I NJENIH DIREKTORIJA

Dok istražujete, dobra je ideja provjeriti svaku vezu na stranici i vidjeti koje su datoteke prikazane na vezama. Kali Linux ima aplikacije za indeksiranje web aplikacija s alatima kao što su Web Crawler i Web Spider koji automatiziraju i ubrzavaju ovaj rad. Oni rade tako da alati provjeravaju web stranicu za sve poveznice i reference na vanjske datoteke, ponekad ispunjavaju obrasce i šalju ih na poslužitelj, dok istovremeno lokalno pohranjuju sve zahtjeve prema poslužitelju i odgovore poslužitelja, tako da kontrolor može kasnije provjeriti datoteke bez potrebe za internetom. Najčešće korišteni alat za puzanje i paukanje je Burb Suite.

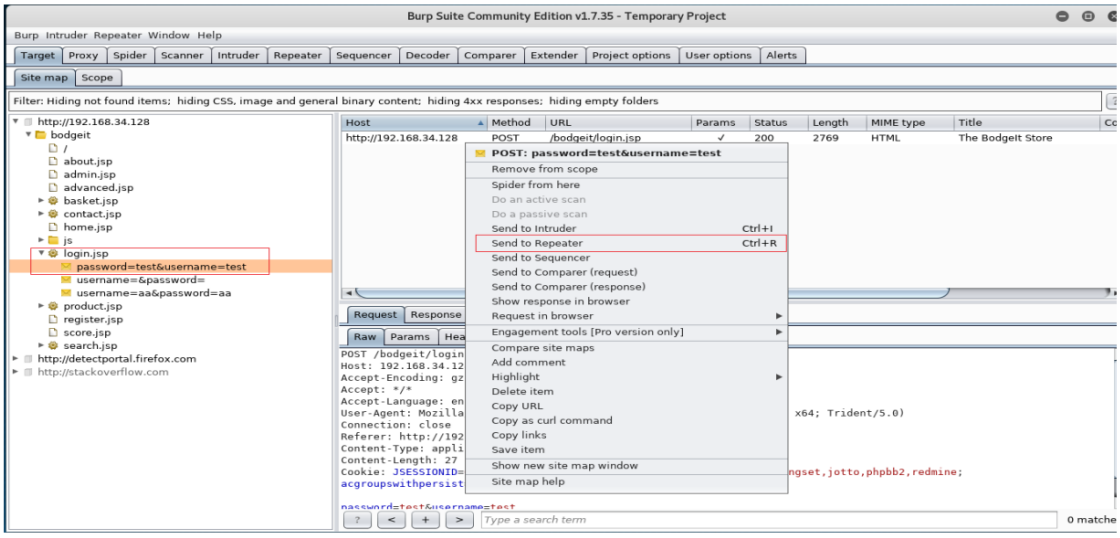


Slika 9. Sučelje burp suite-a (https://www.pentestgeek.com/web-applications/burp-suite-2-0-beta-review, 2022)

Jedan od najboljih sigurnosnih paketa za etičko hakiranje i pentestiranje je Burp. Iako su profesionalna i poslovna izdanja na prodaju, možete preuzeti i besplatno koristiti izdanje zajednice izravno iz Kali Linuxa (https://www.esecurityplanet.com/networks/getting-started-with-burp-suite-pentest-tutorial/#How-Do-You-Intercept-Requests-Using-Burp, 2022).

7.1. Ponavljanje zahtjeva uz Burp repeater

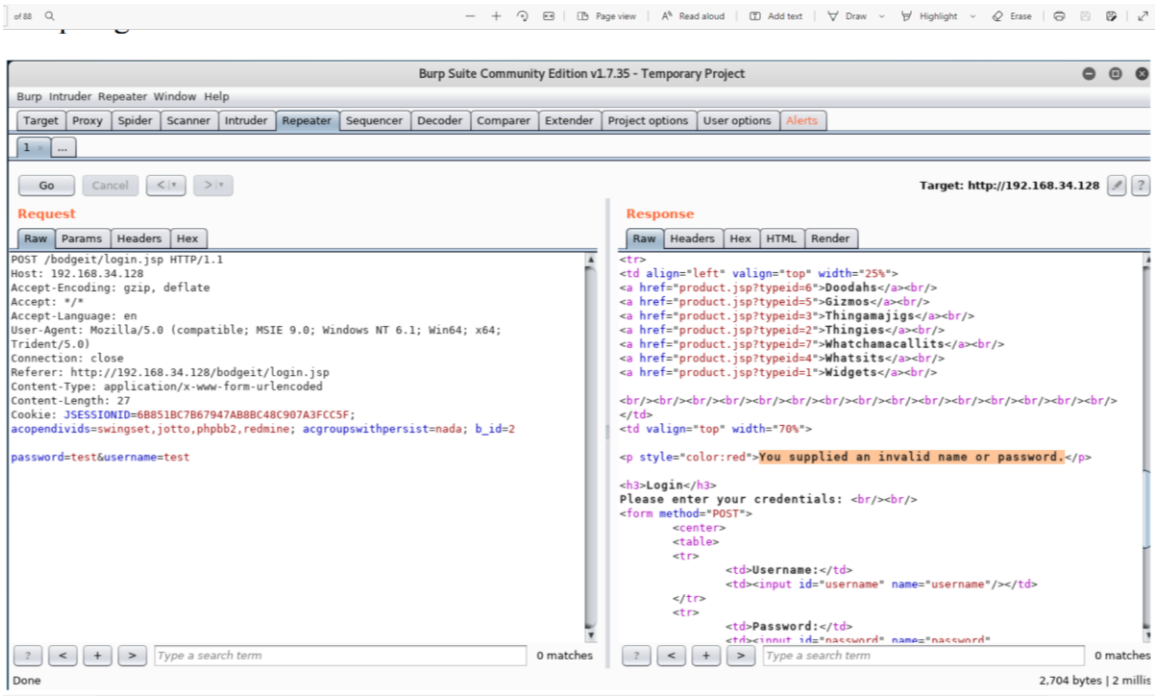
Tijekom analize rezultata Burp spider može slati isti zahtjev različitih verzija gdje se za svaki zahtjev promjene neki određen parametri. Prvo se odlazi na karticu Target, zatim na zahtjev koji je Burp Spider napravio za obrazac na koji se prijavljuje na web stranicu tj. obrazac u kojemu za parametre prijave je definirana vrijednost test.



Slika 10.1.Slanje zahtjeva na Burp repeater

(https://portswigger.net/burp/documentation/desktop/tools/repeater/getting-started, 2022)

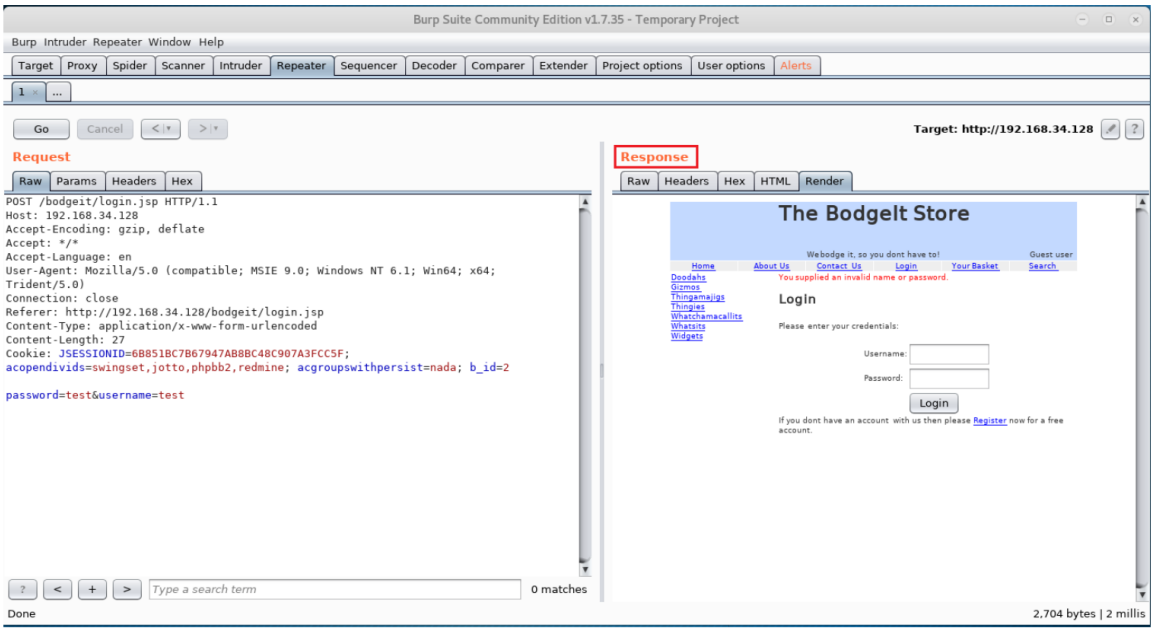
Nakon toga morate odabrati karticu repetitora i zatim pritisnuti gumb za pokretanje da biste započeli ponavljanje zahtjeva.



Slika 10.2. Ponavljanje zahtjeva

(https://portswigger.net/burp/documentation/desktop/tools/repeater/getting-started, 2022)

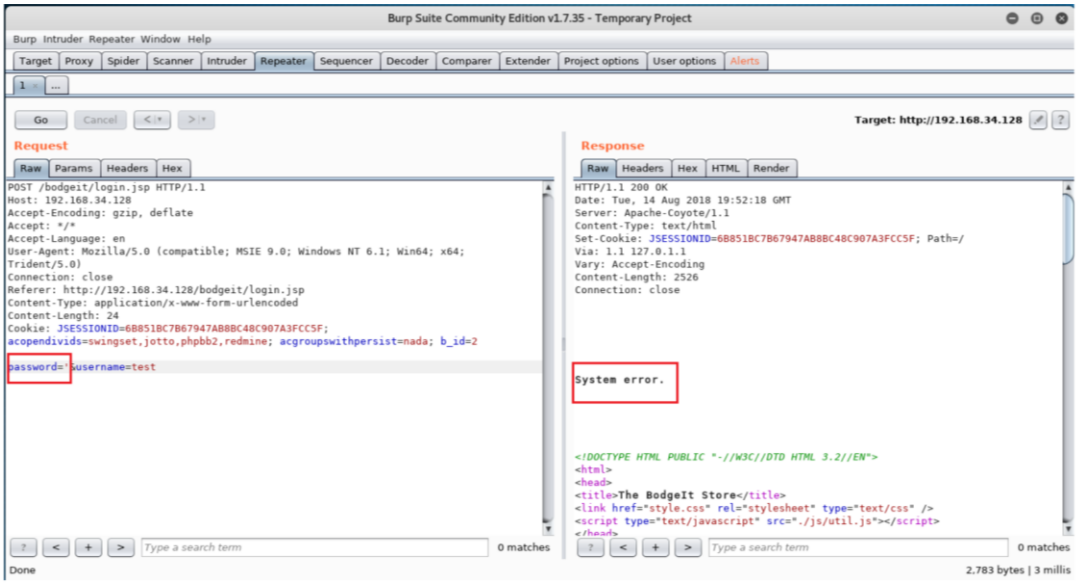
U dijelu zahtjeva može se vidjeti neobrađeni zahtjev koji se šalje na server. U prvim linijama se vide metode koje se koriste, URL i protokol. Sve linije nakon do linije cookie prikazuju parametre zaglavlja, i nakon POST parametri s vrijednostima koje se šalju obrscu za prijavu. U odgovoru su prikazane kartice: Raw, Header, Hex, HTML i Render. Render daje prikaz istih podatka u drugačijim formatima.



Slika 10.3.Prikaz web stranice u Render modu

(https://portswigger.net/burp/documentation/desktop/tools/repeater/getting-started, 2022)

U zahtjevu se može izmijeniti vrijednost parametra i izdati novi zahtjev na temelju serveru. Kao primjer ako se zamjeni vrijednost parametra lozinka s apostrofom nakon slanja zahtjev će generirati sljedeći odgovor:



Slika 10.4. Slanje izmijenjenog zahtjeva i odgovora zahtjeva (https://portswigger.net/burp/documentation/desktop/tools/repeater/getting-started, 2022)

Kao rezultat prema zahtjevima koje šaljemo dobivamo odgovor koji prikazuje istu informaciju u drugim formatima. Slanje modificiranog zahtjeva izazvana je greška na serveru što može značiti da postoji moguća ranjivost u web aplikaciji.

7.2. Pronalaženje datoteka iz rezultata indeksiranja

Kada Burb napravi spisak datoteka i direktorija web stranice treba pronaći koje informacije su relativne i sadrže potencijalne ranjivosti (Najera-Gutierrez, 2016).

Način filtriranja je se odrađuje na sljedeći način:

1. Web stranice za "Login" i "SignIn"-stranice na kojima se može postati korisnik ili pomoću "brute-force" napadom dobiti ime i lozinku nekog postojećeg korisnika
2. Web stranice za resetirati lozinku
3. Web stranice za administraciju web stranice
4. Sustavi za upravljanje bazama podacima
5. Aplikacije koje se još razvijaju i testiraju-obično su slabije zaštićene i sadrže više ranjivosti
6. Konfiguracijske datoteke i datoteke koje imaju informacije o web poslužitelju

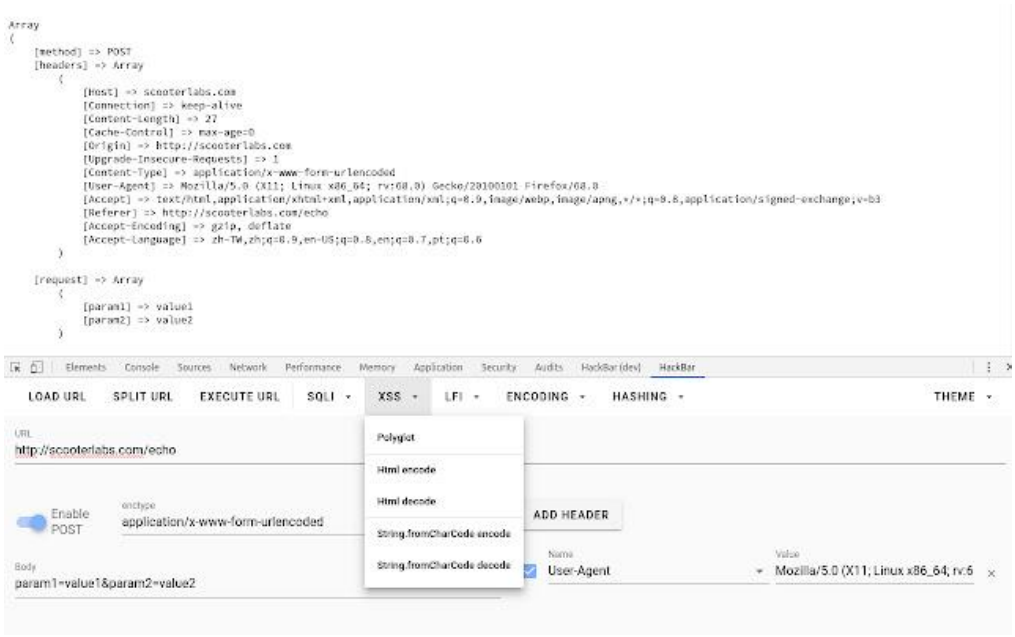
8. APLIKACIJE TIJEKOM IDENTIFIKACIJA RANJIVOSTI

Kada je faza izviđanja gotova i kad su prikupljene informacije o serveru, okruženju na kojem funkcioniraju i moguće slabe točke, prelazi se na fazu testiranja i pronalaženja ranjivosti. Ranjivost je slabost koja ima potencijal potkopati povjerljivost, integritet ili dostupnost informacijskog sustava. Proces pronalaženja ranjivosti i njihovog katalogiziranja u dokumentaciju unutar ciljnog okruženja je identifikacija ranjivosti. Postoji zabilježena zbirka tipičnih ranjivosti i poznata je kao lista ranjivosti. Identificirane ranjivosti često dobivaju broj, opis i reference od šire javnosti. Otkriveno je da se ti nedostaci često pojavljuju i često rezultiraju iskorištavanjem internetskih sustava.

Potrebno je uzeti u obzir niz čimbenika kako bi se ispravno identificirala i kategorizirala ranjivost. Proces skeniranja počinje, a kada se završi, ranjivosti se objavljuju pomoću identifikatora industrijskih standarda kao što su CVE kodovi, EDB-ID-ovi i savjeti dobavljača. Razina rizika može se odrediti pomoću ovih ID-ova i CVSS rezultata ranjivosti. Bilo bi nemoguće identificirati ranjivosti koje postoje unutar mreže bez identifikacije ranjivosti. Ključno je živjeti u stalnom strahu da bi vaša mreža mogla biti ugrožena (https://resources.infosecinstitute.com/topic/ethical-hacking-what-is-vulnerability-identification/, 2022).

8.1. Hackbar alat

Tijekom testiranja neizbježno je naići na adresnu traku preglednika, a koristi se za dodavanje, i izmjenu parametra i urla. Neki serveri odgovaraju preusmjeravanjem na druge stranice kod ponovnog učitavanja stranice ili promjenom parametra. Da bi se process ubrzao i zamijenio ručnim testiranjem promjenom parametra koriste se razni alati koji pomažu ubrzati i olakšati ovaj proces. Jedan od tih alata je Hackbar.



Slika 11. Prikaz rada hackbar ekstenzije
(https://chrome.google.com/webstore/detail/hackbar/ginpbkfigcoaokgflihfhhmglmbchinc, 2022)

Hackbar je dodatak za preglednik Mozilla FireFox koji radi na istom principu kao i adresna traka, ali ne reagira na preusmjeravanja ili promjene u odgovoru poslužitelja, što ga čini savršenim alatom za testiranje web aplikacija. Na primjer, ako unesete ID vrijednosti i pošaljete ga putem gumba Pošalji, kao odgovor ćete dobiti prezime i ime korisnika, ovisno o identifikatoru. Ako pritisnete tipku F9, otvorit će se adresna traka Hackbara. URL i njegove parametre kopira Hackbar (Najera-Gutierrez, 2016).

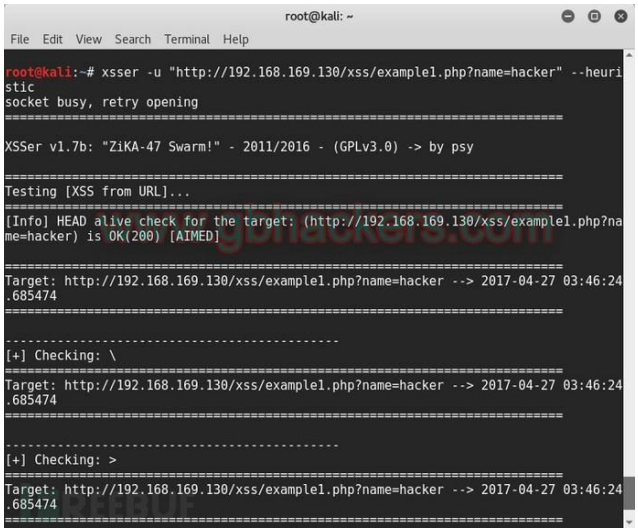
8.2. Presretanje zahtjeva uz burp suite alat i njegova modifikacija

Kako bi obišao sustav i provjerio unos klijenta, Burp može upotrijebiti proxy za presretanje i promjenu zahtjeva. Na primjer, ako su znakovi stavljeni u polje imena na stranici za pretraživanje korisnika koja koristi korisničko ime i lozinku "user@@", a u polje za lozinku "tajna@@", aplikacija zatim izdaje upozorenje da se radi o nedopuštenim i potencijalno opasnim znakovima, zaključuje se da aplikacija ne dopušta unos znakova u polja te se vrši provjera valjanosti unosa. Za dodatnu provjeru, postoji li sustav koji kontrolira da se zahtjev ne upisuje u Burp Proxy HTTP mapu povijesti. Ovo se može zaobići ispunjavanjem zahtjeva s točnim podacima. burpproxy presreće ovaj zahtjev i dopušta promjenu parametara imena i lozinke. Zaobilaženje sustava za

provjeru valjanosti unosa uspješno je jer proxy omogućuje izmjenu zahtjeva nakon što prođe mehanizam za provjeru valjanosti unosa.

8.3. Pronalaženje XSS slabosti sustava

Zlonamjerne skripte ubacuju se u inače pouzdane i nevine web stranice u napadima Cross-Site Scripting (XSS). XSS napadi se događaju kada napadač pošalje zlonamjerni kod, obično u obliku skripte na strani preglednika, zasebnom krajnjem korisniku pomoću online aplikacije. Sve veća upotreba tehnologija temeljenih na webu povećala je popularnost napada na ljude koji koriste internetske aplikacije. Kada napadač umetne zlonamjerni JavaScript kod na web stranicu, preglednik svakog korisnika koji posjeti tu stranicu pokrenut će kôd. Ovo je primjer XSS napada. Napadač može upotrijebiti ovaj kod za izvođenje bilo koje željene radnje, poput krađe povjerljivih podataka ili preusmjeravanja korisnika na zlonamjerno web mjesto (https://www.systranbox.com/how-to-perform-xss-attack-using-kali-linux/, 2022).



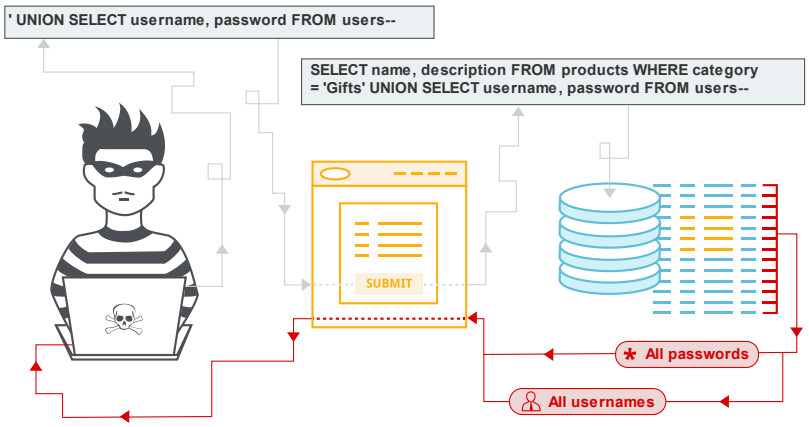
Slika 12. Rad XSSer alata (https://www.systranbox.com/how-to-perform-xss-attack-using-kali-linux/, 2022))

Alat za testiranje penetracije nazvan XSSer koristi se za prepoznavanje i iskorištavanje XSS ranjivosti. Može se pronaći u spremištima i sastavni je dio distribucije Kali Linuxa. Prvi korak u testiranju XSS ranjivosti je promatranje normalnog odgovora aplikacije. U web aplikaciji korisnički unos koristi se za oblikovanje izraza. Međutim, ako posebni znakovi kao što je <'test'>? koriste umjesto ispravnog unosa, može se zaključiti da će se sve što korisnik unese u tekstualno

polje odraziti na odgovor web aplikacije i postati dio HTML koda web stranice. Gore navedeno može se potvrditi analizom izvornog koda weba. Analizom izvornog koda može se utvrditi da se prilikom odgovora na zahtjev korisnika ne vrši filtriranje znakova, te se znakovi koje šalje klijent projiciraju na web stranicu bez prethodne obrade. Budući da se u HTML-u znakovi < > koriste za definiranje HTML oznaka, postoji mogućnost umetanja koda na web stranicu. Na primjer, web-mjesto uspješno pokreće skriptu kada korisnik upiše regularnu vrijednost nakon koje slijedi običan HTML kod, pokazujući da je web-mjesto definitivno osjetljivo na XSS (Fogie, 2007).

8.4. Pronalaženje SQL injection slabosti

Injekcije ranjivosti su među najčešćim sigurnim web aplikacijama ranjivosti. Jedan od najčešće korištenih primarnih ransomware alata je SQL ubacivanje. Suvremene online aplikacije koriste lokalne ili globalne baze podataka, ovisno o aplikaciji. SQL baze podataka su najnovije. U SQL napadu, korisnik pokušava zlouporabiti komunikaciju između aplikacije i baze podataka navode web aplikaciju da pošalje modificirane upite baze podataka umetanjem SQL naredbe u obrasce za unos podataka ili druge. Prva ključna točka je promicanje aplikacija na uzlaznoj vezi. Aplikacija je inicijalno bila postavljena u bazi s pitanje postoji ili korisnik s ID-om, a zatim je omogućila pristup korisničkom upitu. Kako biste ispravno implementirali SQLi ranjivosti, trebali biste izraditi novu web aplikaciju, ali i ova će raditi pomoću dva apostrofa. Web-aplikacija je obradila korisnički upit, što ukazuje da postoji SQL injekcija u ovoj web-aplikaciji. Unos "ili 1"="1 u polje User ID to će potvrditi (Najera-Gutierrez, 2016).

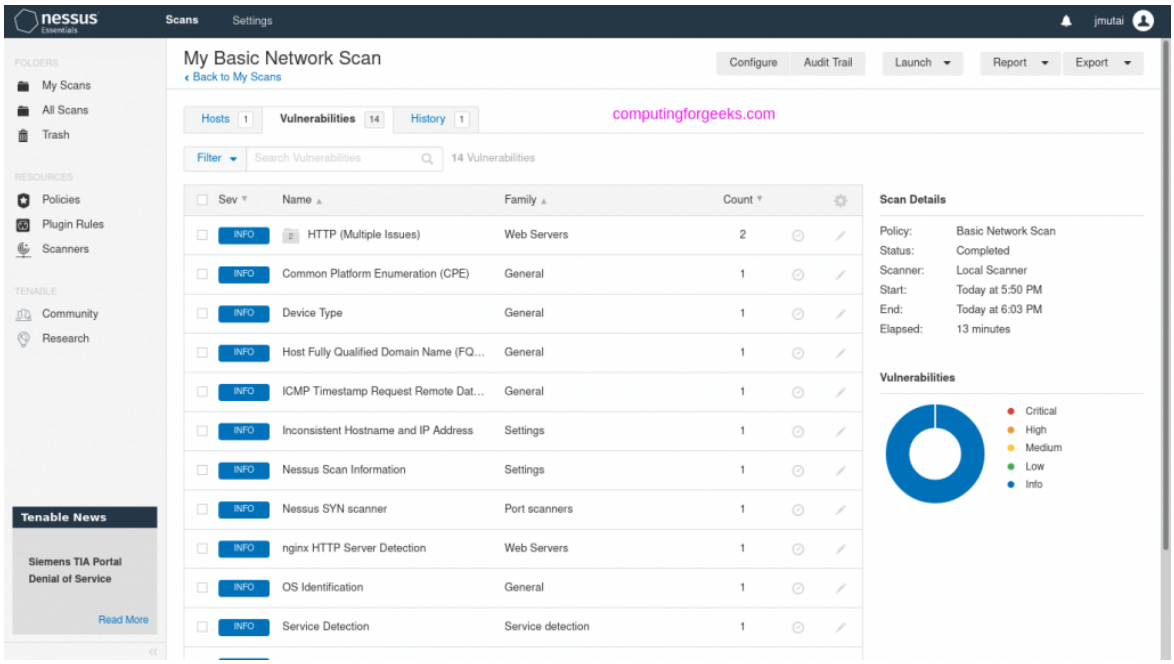


Slika 13. Primjer krađe podatka pomoću SQL injectiona (https://portswigger.net/web-security/sql-injection, 2022)

Lozinkama, brojevima kreditnih kartica i drugim osjetljivim podacima može se neispravno pristupiti kao rezultat uspješnog napada SQL injekcijom. Napadi SQL injekcijom bili su uzrok nekoliko kršenja podataka visokog profila posljednjih godina, što je rezultiralo narušavanjem ugleda i pravnim kaznama. U nekim okolnostima, napadač može dobiti pristup trajnim stražnjim vratima, što može rezultirati dugotrajnim kršenjem koje može ostati neotkriveno dugo vremena (https://portswigger.net/web-security/sql-injection, 2022).

8.5. Nessus alat

Kako bi se u kratkom vremenskom razdoblju proveli različiti testovi na web aplikacijama kako bi se identificirao što je moguće više ranjivosti, automatizirani alati za skeniranje ranjivosti idealni su za ovaj zadatak. Jedan od najomiljenijih i najpouzdanijih alata za automatsko skeniranje ranjivosti je Nessus. Može testirati lozinke koje je lako provaliti, neispravno konfigurirane web aplikacije, DDoS ranjivosti i ranjivosti koje korisnicima omogućuju daljinski pristup sustavu i osjetljivim podacima. . Otvorite URL https:// localhost:8834 u web-pregledniku, zatim se prijavite koristeći svoj Nessus korisnički račun za pristup grafičkom korisničkom sučelju alata (Allen, 2016).



Slika 14. Prikaz rezultata skeniranja pomoću nessusa (https://computingforgeeks.com/install-nessus-vulnerability-scanner-on-kali-linux/, 2022)

Odaberite "Novo skeniranje" iz izbornika na korisničkom sučelju. Aplikacija tada nudi niz unaprijed napravljenih predložaka za skeniranje ranjivosti, a ako korisniku ne odgovaraju, može izraditi vlastiti predložak. Kao što vidite, postoji nekoliko gotovih predložaka za skeniranje sustava. Kao primjer koristi jednostavno skeniranje mreže. Drugi prozor će se pojaviti kada odaberete predložak, omogućujući vam da odredite temeljne postavke skeniranja. Prije početka skeniranja potrebno je postaviti naziv, opis i odredište skeniranja. Recenzent može prilagoditi svaku od ovih postavki kako bi odgovarale njihovim individualnim zahtjevima za skeniranje. Morate spremiti predložak nakon konfiguriranja postavki skeniranja. tada će navedeni predložak biti prikazan na početnoj stranici alata. Skeniranje cilja započet će kada kliknete ikonu Play +. Detaljniji popis otkrivenih ranjivosti dostupan je ako kliknete na IP adresu poslužitelja (host kartica). Novi prozor koji sadrži više informacija o ranjivosti pojavljuje se kada kliknete na određenu ranjivost. Ove informacije uključuju pojedinosti o ranjivosti, kao i utvrđivanje jesu li već razvijena iskorištavanja.

9. APLIKACIJE PRI NAPADIMA NA LOZINKE

Kali Linux ima ogromne aplikacije pri pokušavanju probijanja lozinka. Čak i ako sustav ima jake sigurnosne programe koje je otežano zaobići, korisnici znaju imati nedostatke. Pogađanjem se može upasti u sustav bez direktnog napada. Većina aplikacija za zaštitu koristi lozinke, ali to se može zaobići brute-force napadom ili pogađanjem i tako upasti u sustav. Neke modernije aplikacije znaju kao sigurnost koristiti biometrijske podatke(skeniranje mrežnice, otisak prsta) ili dvofaktorsku provjeru autentičnosti(slanje sigurnosnog koda na mobitel ili email).

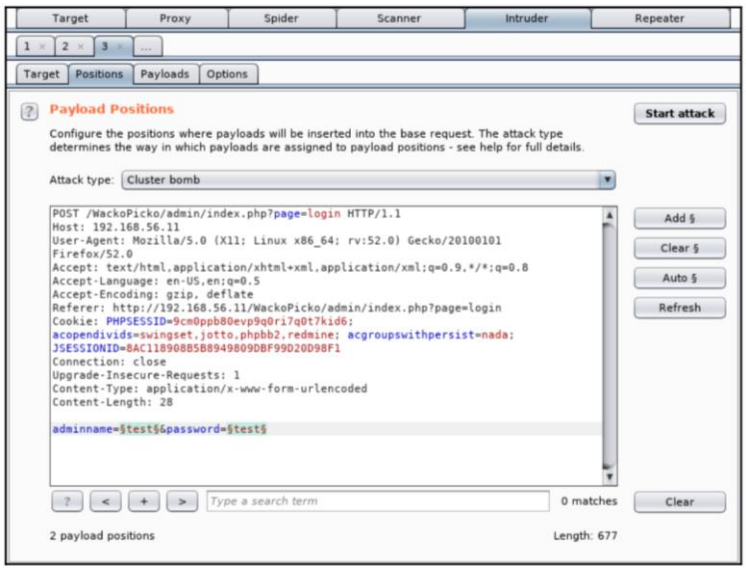
9.1. Napadi na mrežne lozinke

Korisnik može napisati skriptu za prijavu u sustav u slučaju napada, koristeći metodu brute force napada. Brute force je metoda dobivanja podataka o lozinki ili PIN-u putem pokušaja i pogrešaka. Kada se alat prvi put pokrene, pokušava sve moguće kombinacije korisničkog imena i lozinke i, kada prođe dovoljno vremena, otkriva legitimne vjerodajnice. Nedostatak metode brute force je taj što može potrajati neko vrijeme za razbijanje velikih i složenih lozinki (Weidman, 2014).

9.1.1. Probijanje lozinka pomoću rječnika

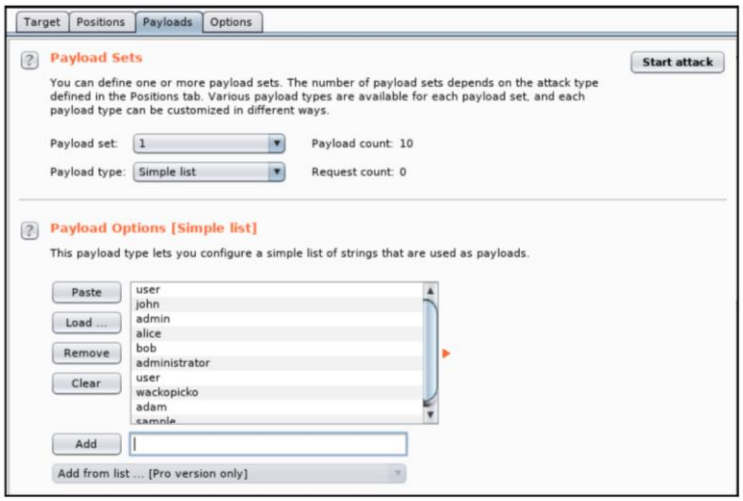
Potreban mu je rječnik ili popis parametra koji će poslužiti kao početna točka za pogađanje lozinki prije nego što može pogoditi lozinke. Unaprijed napravljeni rječnik može se preuzeti s web stranice, rječnik se može generirati pomoću alata kao što je John the Ripper ili možete prikupiti popis potencijalnih pojmova koje bi kupac mogao koristiti kao lozinku. Alat WL može se koristiti za pretraživanje web stranice i izradu popisa pojmova za dodavanje u rječnik ako je pogađanje dovoljno neuspješno. Preporučljivo je koristiti alat Crunch kada sastavljate popise riječi za popis svih mogućih kombinacija danog niza ili popis svih kombinacija znakova za određeni broj znakova, a naravno potrebno je više prostora na disku što je više opcija. Izrada popisa svih mogućih kombinacija od sedam znakova koji uključuju slova A i B je jedan primjer kako koristiti Crunch. Na sličan način, naredba crunch 7 8 generira popis svih mogućih kombinacija znakova za niz između sedam i osam znakova koristeći dani skup znakova, ali malim slovima. Poznavanje kretanja duljine znakova koda ključna je vještina koja vam može pomoći da radite brže i učinkovitije (https://null-byte.wonderhowto.com/how-to/brute-force-nearly-any-website-login-with-hatch-0192225/, 2022).

Za primjer će se koristiti burp suite. Prvi korak je probati se prijaviti na neku web stranicu pomoću nekih parametra. Jednom kad se zahtjev zapisao može ga se pregledati i modificirati s burp Suiteom. Kao vrstu napada koristi će se "Cluster bomb" napad (Najera-Gutierrez, 2016).



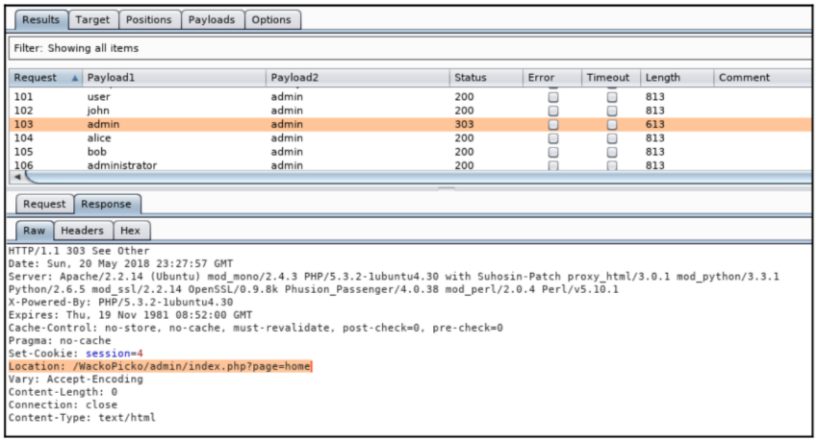
Slika 15.1. Odabir napada u burp suite-u (Najera-Gutierrez, 2016)

Kada se odabere žrtva i vrsta napada, mora se prvo maknuti već spremljene parametre i dodati nove. U novim parametrima možemo postaviti željene liste riječi s kojima se želi probati pronaći akreditacije nekog računa (Najera-Gutierrez, 2016).



Slika 15.2. Unos željenih lista za jedan parameter (Najera-Gutierrez, 2016)

Pri izboru bira se specifična lista za svaki parameter ili se ručno može zapisati određene parametre koje se žele testirati. Nakon toga se može započeti napad, ako je jedan od unosa ispravan, napadač je prebačen na željenu web stranicu s ukradenim akreditacijama (Najera-Gutierrez, 2016).



Slika 15.3. Prikaz rezultata napada rječnikom (Najera-Gutierrez, 2016)

9.1.2. Korištenje alata za automatsko testiranje lozinka

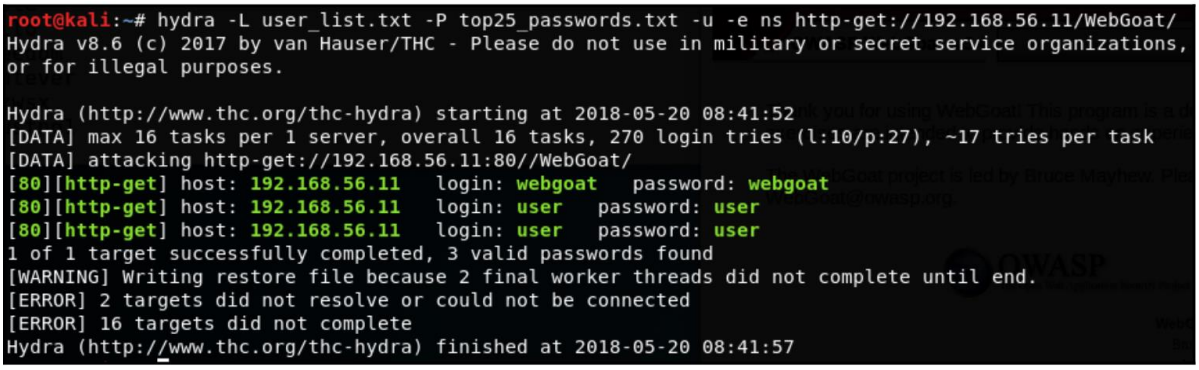
Kako bi se izbjeglo ručno upisivanje dobivenih akreditacija jednog po jednog automatizira se proces korištenjem alata, najbolji primjer tih alata je Hydra. Hydra je alat za oporavak lozinke koji vam omogućuje testiranje korisničkih imena i lozinki. Kao primjer, hydra se koristi za pogađanje korisničkih imena i lozinki provjerom korisničkih imena i lozinki za važeće POP3 vjerodajnice pomoću naredbe:

hydra -L popis korisnika.txt -P datoteka lozinke.txt pop3

Oznaka -l predstavlja popis korisničkih imena, zastavica -p predstavlja popis lozinki. Ako se lozinka nauči tijekom korištenja POP3 ranjivosti, može se prijaviti na isti POP3 poslužitelj s valjanim vjerodajnicama i pokrenuti daljnje napade. U stvarnosti, tvrtke dopuštaju određeni broj pokušaja upada i mogu "zaključati" profil koji je napravio mnogo grešaka prilikom prijave u sustav. . Da bi se izbjegli takvi slučajevi, koristi se nešto gdje pokušavate pogoditi kod prije pokušaja prijave u sustav (Weidman, 2014).

Mrežni mrežni kreker za prijavu, kao što je THC Hydra, može se koristiti za dobivanje vjerodajnica za prijavu grubim forsiranjem aktivnih mrežnih usluga. Možemo locirati HTTP

provjeru autentičnosti obrasca i HTTP osnovnu prijavu među različitim uslugama koje Hydra pruža (Najera-Gutierrez, 2016).



Slika 16. Prikaz rada Hydra alata (Najera-Gutierrez, 2016)

Osnovna provjera autentičnosti jedinstvena je u onome što pruža poslužitelju, kako to prenosi i odgovoru koji od nje očekuje, za razliku od drugih strategija provjere autentičnosti poput one temeljene na obrascu. To štedi napadačima i testerima penetracije dragocjeno analitičko vrijeme olakšavajući određivanje koji parametri sadrže prijavu i lozinku, kako se ti parametri obrađuju i prenose te kako razlikovati uspješan i neuspješan odgovor. Ovo je samo jedan od nekoliko argumenata protiv jednostavne provjere autentičnosti kao sigurnog pristupa (Najera-Gutierrez, 2016).

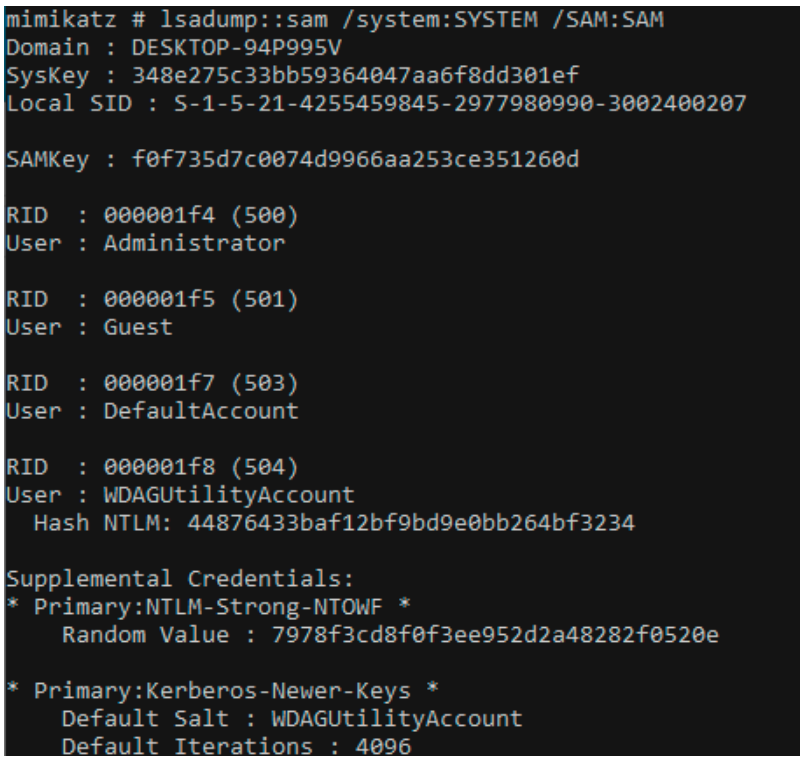
9.2. Offline napadi na lozinke

Dobivanje kopije hash-a i njegovo pretvaranje natrag u izraze običnog teksta važno je kako bi se spriječilo "zatvaranje" profila tijekom pogađanja. Hash funkcija se može koristiti za izračunavanje izlaza iz ulaza, ali kada je izlaz poznat, nemoguće je točno otkriti ulaz. U stvarnosti će većina lozinki biti šifrirana i teško ih je čitati u običnom tekstu. Jednosmjerna hash funkcija može se koristiti za kombiniranje lozinke s pretpostavkom, a rezultati se zatim mogu usporediti s poznatim hashom. Legitimna zaporka je otkrivena ako se dva hash-a podudaraju (Weidman, 2014).

Za dobivene hash kodove možete koristiti naredbu hashdump u meterpreteru koja ispisuje hash lozinku i alat. John the Ripper da ga dešifrira. Zatim morate usporediti ova 2 hash-a s onima koje ste pronašli pomoću naredbe hashdump. Ako se hashevi pronađu za ostale korisnike osim onih pronađenih s hashdumpom, može se reći da su ti korisnici stvoreni nakon sigurnosne kopije datoteke SAM.

9.3. Nabavljivanje hash lozinki pri fizičkom pristupu

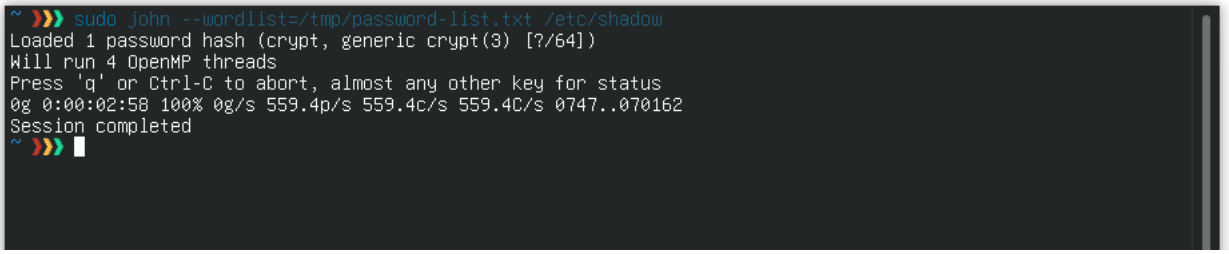
Možemo koristiti CD ili USB za instalaciju operativnog sustava Kali Live na računalo kako bismo prešli sigurnosne mjere sustava Windows. Naredba mkdir -p, na primjer, u sustavu može se koristiti za stvaranje direktorija s imenom /mnt/sda1 kada se pristupa montiranju sustava datoteka Windows. Kako biste pristupili datotekama SAM i SYSTEM, premjestite ih u mape / mnt / sda1 / Windows / System32 / config pomoću naredbe cd. Ove se datoteke nalaze u C: Windows System32 konfiguracijskom direktoriju u sustavu Windows. Ovdje Samdump2 i Bkhive mogu pristupiti datotekama SAM i SYSTEM bez prethodnog spremanja i prijenosa u sustav Kali. Konačno, nakon dovršetka ovih procesa, primit ćete raspršene lozinke.



Slika 17. Prikaz datoteka SAM i SYSTEM pomoću mimikat alata (https://www.wonderhowto.com, 2022)

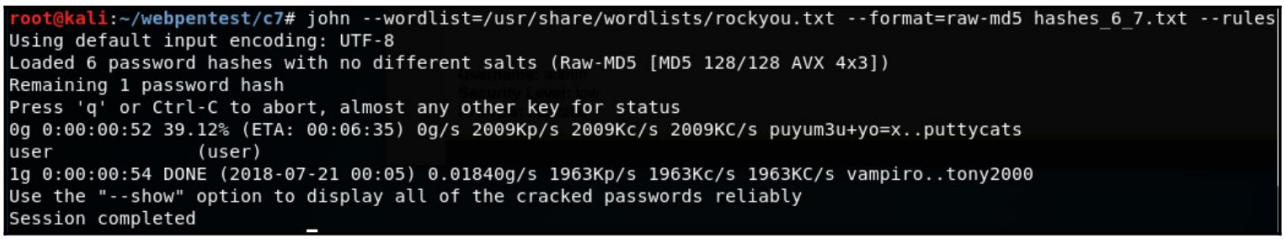
9.4. John the ripper

Alat za probijanje lozinki pod nazivom John the Ripper traži slabe lozinke. John the Ripper je sposoban izvući razne lozinke i hashove. Ovaj je alat također koristan za resetiranje lozinka, razbijanje LM šifre nije problem čak ni na Kali virtualnom računalu s ograničenom CPU snagom i memorijom. Ako su hashovi sustava pohranjeni u datoteci pod nazivom xphashes.txt, jednostavno se šalju alatu John Ripper (Weidman, 2014).



Slika 18. John the ripper terminal (https://en.wikipedia.org/wiki/John_the_Ripper, 2022)

Na primjer, ako trebate pronaći lozinku za korisnike (tajna, Lusiana, administrator). Uz određeno predznanje, npr. kod korisnika Lusiana, prva polovica lozinke bit će LOZINK, a druga A321 Šifra za tajnog korisnika je drugačija i glasi PASSWORD. Hash LM-a pokazao je ispravnu lozinku, no još uvijek se ne zna je li sva velika, mala ili miješana, a daljnje dešifriranje zahtijeva dodatne napore. Da biste saznali sadrži li lozinka velika, mala ili miješana slova, trebali biste pogledati četvrto polje NTLM hash-a. Sam NTLM hash teško je dešifrirati korištenjem grube sile i tehnika rječnika. Iako se NTLM lozinka od pet znakova koja sadrži samo mala slova i nema druge složenosti može probiti jednako brzo kao i LM hash. S druge strane, za probijanje NTLM lozinke od 30 znakova i visoke složenosti trebat će godine.



Slika 19. Prikaz rada i sintakse alata John the Ripper (Najera-Gutierrez, 2016)

Svaki izvanmrežni kreker za probijanje lozinki, uključujući Johna, radi tako što raspršuje riječi na popisu (ili one koje proizvodi) i uspoređuje ih s raspršivačima koje treba probiti; kada postoji podudaranje, pretpostavlja se da je lozinka pronađena. Opcija —wordlist koristi se u prvoj naredbi za davanje uputa Johnu koje riječi da koristi. Proizvodi vlastiti popis za stvaranje napada brutalnom silom ako je izostavljen. Ako opcija —format nedostaje, John pokušava pogoditi metodu, obično uspješno. Opcija —format nam govori koji je algoritam korišten za izradu hashova. Datoteka koja sadrži hashove koje želimo razbiti je zadnja stvar koju uključujemo (Najera-Gutierrez, 2016).

10. APLIKACIJE TIJEKOM EKSPLOATACIJE

Eksploatacije se koriste protiv ranjivosti koje se otkriju tijekom izviđanja kako bi se pristupilo određenom ciljanom sustavu. Kali Linux ima aplikacije pri kreiranju eksploatacija, koristeći mnogo dostupnih alata za kreiranje vlastitih eksploatacija ili lakšim načinom koristeći alata koji automatski kreiraju eksploatacije koristeći već nekih postavljenih šablona. Najbolje je koristiti alat Metasploit za iskorištavanje većinu ranjivosti.

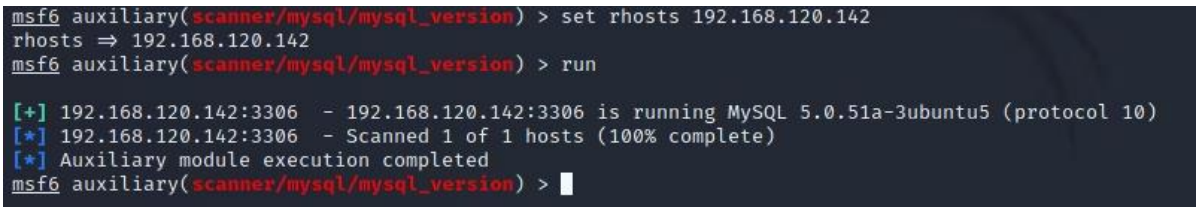
Iskorištavanja su metoda za dobivanje pristupa sustavu putem sigurnosne rupe i korištenje te rupe za vlastitu korist ili njezino iskorištavanje. Eksploatacije obično koriste skriptu, dio koda ili dio softvera koji je razvijen. Često se šalju u obliku kompleta, koji je zbirka trikova. Posjetite web-mjesta koja su napadači postavili u zamku za najpopularniji način povezivanja s eksploatacijama. Najgori aspekt je to što su web stranice s velikim prometom kao što su nytimes.com, msn.com i yahoo.com često stavljene u zamku napadača. Dvije kategorije poznatih i neotkrivenih eksploatacija čine najširu klasifikaciju eksploatacija. Poznate eksploatacije su one koje su istraživači već otkrili i prijavili. Budući da se često popravljaju u kasnijim sigurnosnim nadogradnjama, etički hakeri imat će veće šanse poraziti ih. Zero-day eksploatacije, koji se obično nazivaju nepoznate eksploatacije, još nisu pronađeni niti katalogizirani. Ažuriranja vas neće zaštititi od ovih ranjivosti, koje povremeno mogu godinama ostati neotkrivene (https://resources.infosecinstitute.com/topic/ethical-hacking-what-are-exploits/, 2022).

10.1. Metasploit framework

Okvir za testiranje penetracije pod nazivom Metasploit čini hakiranje jednostavnim. Za mnoge napadače i one koji brane sustav, to je ključni alat. Način na koji radi je da Metasploit odabire exploit, određuje kako ga pokrenuti, a zatim usmjerava na cilj. Sustav koji je iskorišten može djelovati u naše ime zahvaljujući Metasploit korisnim sadržajima. Većina korisnih opterećenja su obvezujuće skripte koje se pokreću na lokalnom priključku ciljnog računala ili obrnute ljuske koje se pozivaju iz napadačevog sustava; drugi korisni tereti obavljaju određene zadatke. Glavne komponente Metasploita su msfconsole i moduli koje nudi.

Najpopularnije sučelje nalik shellu na jednom mjestu za pristup svim funkcijama Metasploita zove se msfconsole. Budući da pruža automatsko dovršavanje naredbi, tabiranje i

druge bash prečace, ima podršku za naredbeni redak sličnu Linuxu (https://www.makeuseof.com/beginners-guide-metasploit-kali-linux/, 2022).



Slika 20. Prikaz odabira eksploatacije za neku IP adresu (https://www.makeuseof.com/beginners-guide-metasploit-kali-linux/, 2022)

10.2. Payload

Korisni teret paketa ili druge podatkovne jedinice za prijenos naziva se korisnim teretom. Fraza, koja ima vojne korijene, često se koristi u vezi sa zloćudnim kodom koji se može izvršiti i uzrokovati štetu. Zlonamjerni kôd koji šteti ciljnoj žrtvi obično se naziva sadržajem kada se govori o zlonamjernom softveru (Weidman, 2014).

Korištenjem naredbe display payloads kao root u Msfconsole (Metasploitovo administrativno sučelje), možete vidjeti većinu korisnih opterećenja dostupnih u Metasploitu. Windows/shell/obrnuti tcp korisni teret, koji je korisni teret stupnja zbog prisutnosti / koji odvaja ljusku od obrnutog tcp korisnog opterećenja, jedan je od najpoznatijih korisnih opterećenja.

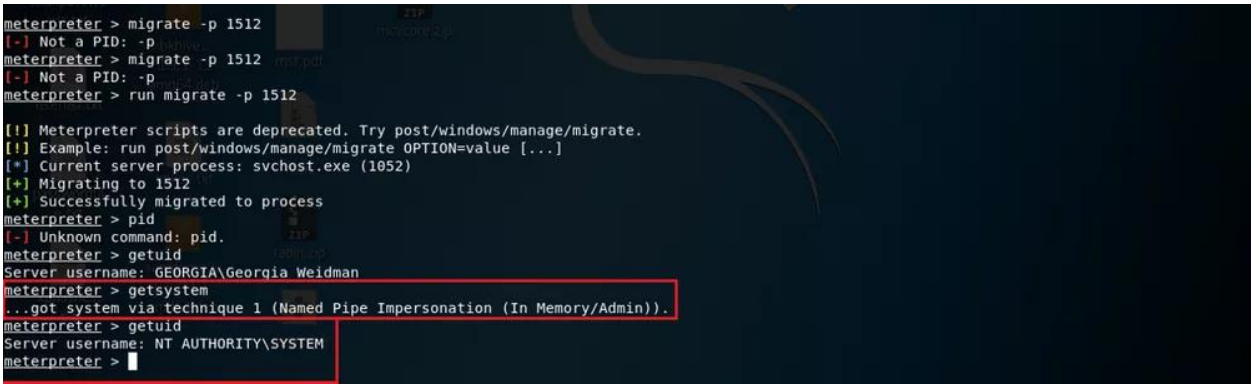
Stage payload označava da nisu prisutne sve upute potrebne za vraćanje obrnute ljuske. Umjesto toga, informacije o stupnju mogu se koristiti za povezivanje s napadačevim sustavom i traženje dodatnih uputa od Metasploita. Ostatak korisnog opterećenja općenito izvršava rukovatelj koji se ponovno povezuje s napadačevim strojem. Iako inkrementalni korisni teret nema ograničenje memorije, često koristi manje memorije od "inline" korisnog opterećenja. Sve informacije koje su potrebne za pružanje napadaču obrnute ljuske sadržane su u umetnutom sadržaju. Obično su stabilniji, troše manje memorije od samih stupnjevanih korisnih opterećenja i obično sadrže sve informacije. Slojevite i inline varijacije nosivosti označene su kosom crtom (/).

10.3. Meterpreter

Nakon što se iskoristi sustav pomoću naredbe session može se micati između sesija i naći onaj koji ima najveće privilegije. Tester pomoću curl ili Wget može preuzeti podatke sa servera i ne može dobiti kvalitetnu sliku ranjivog sustava, moguće je da se mogu poslati datoteke pomoću komande upload čak i ako nema cijelu sliku sustava. Najčešće Meterpreter koristi iskorištene procese ili korisnike. Kao primjer pomoću eksploatacije MS08-067 na uspješno iskorištenom serveru može se vidjeti privilegije s komandom getuid na meterpreter sesiji (Weidman, 2014).

Reflexive DLL injection je postupak koji se koristi za izravno učitavanje u memoriju procesa. Stoga Meterpreter ne zapisuje ništa na disk i umjesto toga ostaje u memoriji. radi unutar memorije glavnog računala umjesto da započne novi proces koji bi bio ranjiv na sustav za otkrivanje upada (Weidman, 2014).

Na sustavu Kali Linux, skripte meterpreter nalaze se ispod područja metasploit skripti. Skripta koja uspješno demonstrira naknadno iskorištavanje, kao ilustracija, je kada se skripte premještaju u druge procese. Za to se može koristiti naredba za pokretanje. Dok vam alat ps može pokazati sve procese, možete otkriti jedan proces prema njegovom ID-u.



Slika 21. Meterpreter skripte korištene u terminalu (https://www.getastra.com/blog/security-audit/meterpreter-commands-post-exploitation/, 2022)

Direktorij za poslije eksploatacije u Metasploitu ima module kojima se mogu podići privilegije, sakupljati podatci, kontrolirati na udaljenost, itd, i to na više sustava odjednom. Kao primjer ako se iskoristi modul enum_logged_on_users može se dobiti informacija tko je trenutni

korisnik na iskorištenom sustavu. Nakon što se izvede eksploatacija prikažu se svi nedavni korisnici i ti podaci se također spremaju kao .txt dokument.

10.4. Metoda upornosti(persistence)

Kad završi testiranje za pronalazak ranjivosti u sustavu, testiranje još ima par koraka, nije dovoljno prikazati nekom klijentu koliko mu je ranjiv sustav kad tester dobije Meterpreter sesiju. Samo stvaranje sesije ne prikazuje klijentu dobar pogled ranjivosti sustava, tu je bitna faza poslije eksploatacije u penetracijskom testiranju. U testu prodora ili legalnom hakiranju, cilj poslije iskorištavanja je nastavak pristupa udaljenom računalu. Jednom kad se osoba osjeća opušteno, može upotrijebiti niz alata za nastavak pristupa i podizanje razine svojih prava na računalu. Alati koje ćemo promatrati pomoći će u očuvanju pristupa ciljnom računalu sve dok ne dođe vrijeme za prebacivanje na drugi cilj. Omogućuje vam održavanje veze s udaljenim računalom kako biste mu se mogli vratiti kasnije ili dok ne morate dovršiti sljedeći zadatak. Operacija je u opasnosti ako se ovaj upad ne pronađe i eliminira na proizvodnoj mreži. Ako se s njima ne postupa, štetni sadržaji mogu biti uneseni u okolinu, a podaci, lozinke i druge ključne informacije mogu se izlučiti. Kao rezultat toga, morate razumjeti kako prepoznati te situacije kako biste ih mogli ispravno ukloniti kada na njih naiđete (https://resources.infosecinstitute.com/topic/kali-linux-top-5-tools-for-post-exploitation/, 2022).

Kako je proces spremljen u cjelovitosti u memoriji, ako se sustav ugasi, gubi se i dobivena sesija koja neće više postojati ako se sustav opet pokrene. Također ako nema mrežne povezanosti, sesija isto može nestati. Da bi ostali na sustavu treba nam upornosti, to može biti lagano tako da se ubaci korisnik u sustav ili kompliciranija verzija gdje se instalira rootkit na terminal da je bolje sakriven i da ga Windows API ne može otkriti.

11. APLIKACIJE PRI SOCIJALNOM INŽENJERINGU

Socijalni inženjering je praksa uvjeravanja drugih da daju osjetljive informacije. Vrste informacija koje ti kriminalci traže mogu varirati, ali kada je osoba meta, kriminalci vas obično pokušavaju prevariti da im date podatke o vašoj banci ili zaporci ili pokušavaju dobiti pristup vašem računalu kako bi tajno instalirali zlonamjerni softver koji će im omogućiti pristup informacijama o vašoj banci i zaporci, kao i kontrolu nad vašim računalom. Hakeri koriste tehnike socijalnog inženjeringa jer je često jednostavnije iskoristiti svoju inherentnu tendenciju da vjerujete drugima nego smisliti kako hakirati vaš program. Na primjer, znatno je jednostavnije prevariti nekoga da vam da svoju lozinku nego da vi pokušate ukrasti njihovu lozinku (osim ako nisu imali veoma slabu)

Čak i ako sustav ima veliku sigurnost i skoro nikakve rupe u sistemu jedan od način za zaobići to je da radnika se prevari da preda bitne podatke o firmi i poremetiti svoju sigurnost. Neki od najčešćih hakerskih napada ne zahtijevaju eksploataciju sustava. Naprimjer Kevin Mitnick popularni haker bi samo ušao u kompaniju tako da dokaže stražarima da je djelatnik i da dobije pristup nekom željenom dijelu kompanije, i jednom kad unutra samo iskoristi sustav. Ovaj napad koristi ljudske ranjivosti i naziva se socijalni inženjering. Iste rezultate se može dobiti phishing napadom tako da ako je dostupno preko lažiranje povjerljivih osoba nagovoriti da promjeni nešto u sustavu ka naprimjer lozinku ili promjeni neke postavke (Weidman, 2014).

11.1. Alati koji se koriste za socijalno inženjerstvo

SET je najpoznatiji alat za društveni inženjering. Napade društvenog inženjeringa jednostavno je razviti pomoću programiranja Python otvorenog koda. Sastoji se od niza metoda, uključujući phishing napad o kojem smo ranije govorili, web napad u kojem se web stranica često kopira, a meta se na prijevaru natjera da unese informacije na njoj. Naredba settoolkit može se koristiti za pokretanje alata SET (Weidman, 2014).

Slika 22. Prikaz sučelja SET-a i svih njegovih napada (https://shah-hassan.medium.com/social-engineering-se-toolkit-set-8cdbb375f001, 2022)

11.2. Spear-phishing napad

Spear-phishing napad omogućuje stvoriti zlćudne datoteke koje se šalju klijentu kao dio napada, u datoteku se također odmah i postavlja Metasploit handler s kojim se poveže za payload. Kod ovakvih napada mogu se slati ili jednom specifičnoj žrtvi, ili se mogu poslati na veći broj e-mail adresa skupa sa Metasploit "listenerom" za odabrani payload. Ostali izbori se koriste kreiranje zlonamjernih datoteka s payloadom od strane Metasploita, i zadnji izbor služi za kreirati predložak za napad preko alata (Weidman, 2014).

Slika 23. Odabir Phishing napada u set terminalu (https://null-byte.wonderhowto.com/how-to/hack-like-pro-spear-phish-with-social-engineering-toolkit-set-backtrack-0148571/, 2022)

Pri odabiru prve opcije odabrat će se izbor payloada, kao primjer iskoristi će se Adobe Collab.getIcon BufferOverflow payload, nakon još ostaje izbor kako izvesti taj payload za primjer najbolje je iskoristi Windows Reverse TCP Shell. Korištenjem ovog shella dobit će se upit za postaviti LHOST i LPORT koje nakon zapisujemo. Nakon što je sve postavljeno biramo svojevoljno naziv datoteke koja sadrži payload. i kao zadnji upit alat će postaviti opciju na jednu ili više žrtva.

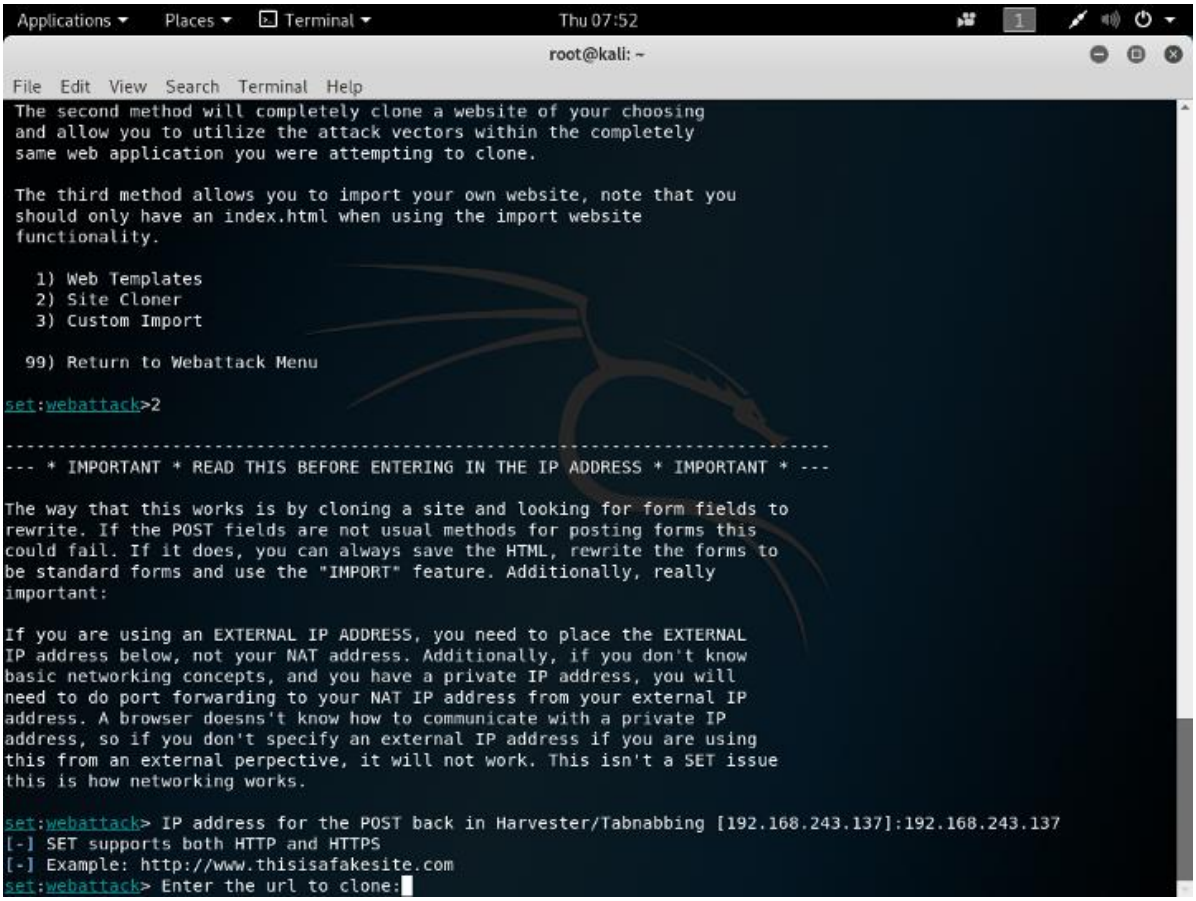
11.2.1. Aplikacije pri kreiranju predložaka

Kod kreiranja predloška e-maila može se iskoristiti već postojeći od alata ili unijeti svoj nekakav predložak. Uz to postoji opcija da se kreira predložak će moć opet iskoristiti tako da izabrati "kreiraj predložak za društveni inženjering". Kad se kreira predložak ostaje samo za izabrati kome poslati payload. Pri slanju se odabire postojeća e-pošta i njegova lozinka, alat nakon pokušava poslati poštu. Tu može doći do problema ako neka usluga poput Gmaila primijeti da datoteka je sumnjiva i zaustavi napad (Weidman, 2014).

U ovakvim situacijama mogu se dobiti bolji rezultati ako se iskoriste neki drugi poslužitelji e-pošte ili klijentovi neki podaci. Zadnja opcija koja je potrebna je postaviti vrijednost "listenera", to može biti ili da ili ne. Pri odabiru da, listener je postavljen i samo se čeka da korisnik pokrene zlonamjernu PDF datoteku gdje se dobiva sesija.

11.3. Web napadi

Ova vrsta napada uključuje društveni inženjering budući da nalikuje nekoliko stvarnih napada društvenog inženjeringa. Imamo brojne alternative pri odabiru vrsta napada: Opcija 1 automatizira proceduru napada pomoću Java-potpisanih apleta. Opcija 2 omogućuje korištenje svih Metasploit napada na strani klijenta bez potrebe za eksplicitnim postavljanjem parametara. Opcija 3 olakšava dizajn web stranica koje varaju ljude da otkriju svoje vjerodajnice. Posljednja opcija gradi grupu otvorenih kartica u pregledniku pomoću korisničkih postavki. Žrtva vidi obavijest da treba pričekati kada otvori karticu iz konačnog izbora, a napad web kloniranja počinje kada se korisnik vrati nakon prebacivanja na drugu karticu. Nakon unosa akreditiva, napad se smatra uspješnim (Weidman, 2014).



Slika 24. Set alat u terminalu tijekom odabira web napada (https://medium.com/@nancyjohn_95536/using-set-tool-kit-to-perform-website-cloning-in-kali-linux-67fa01c92af9, 2022)

Ovo je tip napada koji ima komponentu društvenog inženjeringa jer oponaša mnoge napade društvenog inženjeringa iz stvarnog svijeta. Prilikom odabira vrsta napada imamo nekoliko opcija: Opcija 1 automatizira proces napada s Java-potpisanim appletima. Opcija 2 omogućuje vam korištenje svih napada na strani klijenta koji koriste Metasploit bez potrebe za ručnim postavljanjem parametara. Opcija 3 pomaže u stvaranju web stranica kako bi se korisnici naveli da otkriju svoje vjerodajnice. Posljednja opcija koristi korisničke postavke za stvaranje zbirke otvorenih kartica u pregledniku. Kada žrtva otvori karticu iz zadnje opcije, prikazuje joj se poruka da pričeka, a napad u obliku kloniranih web stranica pokreće se kada korisnik prijeđe na drugu karticu i vrati se. Ako unese vjerodajnice, napad je bio uspješan.

11.4. Mass-mail napad

Da biste koristili SET za automatiziranje phishing napada putem e-pošte, prvo izradite datoteku i unesite nekoliko adresa e-pošte. Kada se vratite na izbornik, prikazat će vam se pogled u kojemu određujete put do datoteke koja sadrži e-poštu koja će se koristiti za izvršenje napada. Zatim se odabire server za napad (u ovom slučaju Gmail) i rade se sljedeći koraci od kojih je najvažniji izrada samog emaila. Kada program postavi pitanje "Šaljete li poruku kao html ili običnu?" odaberite 'h' ili 'p' za izradu e-pošte u kojoj je najbolje koristiti html, koji omogućuje korištenje svojih oznaka, na primjer, za skrivanje poveznice na koju će korisnik biti preusmjeren. Ako korisnik 'nasjedne' na ovaj trik, napadač mu krade vjerodajnice (Weidman, 2014).

11.5. Kombinirani napad

Posljednje, ali ne i najmanje važno, napad koji kombinira napad e-poštom napadom na webu može se koristiti za prevaru potrošača da kliknu na poveznice u e-pošti, što će ih zatim usmjeriti na web mjesto koje napadač kontrolira. Da bi se to postiglo, potrebno je promijeniti opciju u konfiguracijskoj datoteci SET. Ovo se može pronaći u Kali pod /usr/share/set/config/set config. WEB _ATTACK_ EMAIL je opcija koju treba promijeniti; trenutno je postavljen na ISKLJUČENO i treba ga uključiti. Tada će se, kao i u ovoj fazi, sve postaviti, iskoristit će se jedan od ranijih napada (Weidman, 2014).

12. ZAKLJUČAK

Dakle kali ima mnogo aplikacija u informatičkom svijetu, naravno najpopularniji je definitivno penetracijsko testiranje. Kali Linux dolazi s mnogobrojno alata koji su većinom službeno namijenjeni nekom djelu penetracijskog testiranja, no postoji još alata koji služe za neke druge korisne namjene. Kao naprimjer probijanje lozinka ili upravljanje tuđih uređaja pomoću ranih metoda infiltracije sustava. Kali Linux je veoma zahtjevan operativni sistem koji zahtjeva mnogo znanja iz informatičkog svijeta da bi se moglo upravljati njime na profesionalnoj razini. Čak i ako neki korisnik ima dovoljno znanja za upravljati kali-em i njegovim alatima u dosta situacija je potrebna kreativnost i improvizacija za uspjeti izvesti napad na sustav.

Također u dosta situacija napadi mogu proći neuspješno jer zlonamjerne datoteke je primijetio „firewall“ ili žrtva napada nije nasjela na napad. Postoje metode kojima možemo povećati šanse zaobilaženja neuspješnog napada, kao enkripcija ili pomoću Trojana. Kad govorimo o kreativnosti mislimo na to da za uspješan napad mora izgledati legitiman, što znači da mora izgledati kao da je poslana datoteka koju želimo poslati ili osoba koju se pokušava imitirati doista službena od neke kompanije kojoj će žrtva povjerovati.

Kali je opremljen također izvesti cijeli proces penetracijskog testiranja, što znači da je sposoban može pojedinačno izvesti sve procese za pojedine faze. Pod procese može izvesti izviđanja prometa mreža, otkrivanja ranjivosti, iskorištavanja tih ranjivosti za infiltraciju sustava, socijalni inženjering u potrebnim slučajevima, dostavljanje „payload“-a koji nose nekakve „exploit“-e na sustave, skrivanje svojih koraka, dodavanje privilegija na sustave i po potrebi ostavljanje nekakvog „backdoor“-a unutar sustava.

SAŽETAK

Kali Linux je vrlo jednostavan i u isto vrijeme kompleksan operativni sustav koji ima s informatičke strane uz najpopularniju aplikaciju što je penetracijsko testiranje ima još mnogo aplikacija kojima se može efikasno manipulirati nekakvim informatičkim sustavom. Ima aplikacije u bilo kojem aspektu informatike, sustav sadrži u sebi veliki broj alata koji služe za raznovrsne mogućnosti u svim poljima gdje Kali Linux može biti koristan. U radu je prikazano kakve aplikacije ima s ovim sustavom, čemu služe te aplikacije, i nekakvi najbolji načini i alati koji mogu biti korišteni za postići tu aplikaciju. Rad je namijenjen da bude vodič kroz sve mogućnosti koje daje, naravno da je tu penetracijsko testiranje na prvom mjestu i da kad podijelimo cijeli proces na manje dijelove dobijemo aplikacije koje nam mogu služiti zasebno za sebe, isto tako za prikaz aplikacija koje nisu dio penetracijskog testiranja već imaju svoju korist zasebno za sebe.

Ključne riječi: Kali, Linux, Aplikacije, penetracijsko testiranje, izviđanje, socijalni-inženjering, payloads, eksploatacije, ranjivosti, napadi

SUMMARY

Kali Linux is a very simple and at the same time complex operating system that has, on the IT side, in addition to the most popular application, because penetration testing has many other applications that can effectively manipulate some kind of IT system. It has applications in any aspect of IT, the system contains a large number of tools that serve for various possibilities in all fields where Kali Linux can be useful. The paper shows what applications there are with this system, what these applications are for, and some of the best ways and tools that can be used a little to achieve this application. The work is intended to be a guide through all the possibilities it provides, of course, penetration testing is in the first place and when we divide the whole process into smaller parts, we get applications that can serve us separately on their own, as well as for displaying applications that are not part of penetration testing they already have their benefit separately for themselves.

Keywords: Kali, Linux, Applications, penetration testing, reconnaissance, social-engineering, payloads, exploits, vulnerabilities, attacks

LITERATURA

Gilberto Najera-Gutierrez, *Kali Linux Web Penetration Testing Cookbook*, 2016.

Michael Hixon, Justin Hutchens, *Kali Linux Network Scanning Cookbook Second Edition*, 2017.

Lee Allen, Gerard Johansen, Tedi Heriyanto, Shakeel Ali, *Kali Linux 2 – Assuring Security by Penetration Testing Third Edition*, 2016.

Seth Fogie, *Cross Site Scripting Attacks: XSS Exploits and Defense*, 2007.

Georgia Weidman, *Penetration Testing: A Hands-On Introduction to Hacking*, 2014.

url: https://www.hackers-arise.com, 2022.

url: https://www.wonderhowto.com, 2022.

https://www.esecurityplanet.com/, 2022.

https://portswigger.net, 2022.

https://resources.infosecinstitute.com/, 2022.

https://kalilinuxtutorials.com/, 2022.

https://www.systranbox.com/, 2022.