Primjena Kali Linux distribucije za testiranje sigurnosnih ranjivosti u mreži

Mijić, Ivan

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU

FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA

Diplomski studij

PRIMJENA KALI LINUX DISTRIBUCIJE ZA TESTIRANJE SIGURNOSNIH RANJIVOSTI U MREŽI

Diplomski rad

Ivan Mijić

Osijek, 2017.

FERIT
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA OSIJEK

Obrazac D1: Obrazac za imenovanje Povjerenstva za obranu diplomskog rada

Osijek, 22.09.2017.

Odboru za završne i diplomske ispite

Imenovanje Povjerenstva za obranu diplomskog rada

Ime i prezime studenta:	Ivan Mijić
Studij, smjer:	Diplomski sveučilišni studij Elektrotehnika, smjer Komunikacije i informatika'
Mat. br. studenta, godina upisa:	D 970, 12.10.2015.
OIB studenta:	98716729679
Mentor:	Doc.dr.sc. Krešimir Grgić
Sumentor:	
Sumentor iz tvrtke:	
Predsjednik Povjerenstva:	Prof.dr.sc. Drago Žagar
Član Povjerenstva:	Dr.sc. Višnja Križanović-Čik
Naslov diplomskog rada:	Primjena Kali Linux distribucije za testiranje sigurnosnih ranjivosti u mreži
Znanstvena grana rada:	**Telekomunikacije i informatika (zn. polje elektrotehnika)**
Zadatak diplomskog rada:	Kali Linux distribucija predstavlja platformu koja na jednom mjestu objedinjava jako veliki broj aplikacija i alata koji se koriste u postupcima testiranja sigurnosnih ranjivosti, penetracijskih testiranja i sigurnosne analize različitih vrsta mreža. Potrebno je istražiti mogućnosti primjene Kali Linux distribucije u testiranju sigurnosnih ranjivosti u mreži, te je u tu svrhu primjeniti na više različitih primjera u lokalnom mrežnom okruženju. Prikupljene rezultate potrebno je analitički obraditi, te istaknuti smjernice i preporuke za povećanje razine mrežne sigurnosti.
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: 2 bod/boda Postignuti rezultati u odnosu na složenost zadatka: 2 bod/boda Jasnoća pismenog izražavanja: 2 bod/boda Razina samostalnosti: 3 razina
Datum prijedloga ocjene mentora:	22.09.2017.

Potpis mentora za predaju konačne verzije rada u Studentsku službu pri završetku studija:	Potpis:
	Datum:

FERIT
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA
I INFORMACIJSKIH TEHNOLOGIJA **OSIJEK**

IZJAVA O ORIGINALNOSTI RADA

Osijek, 09.10.2017.

Ime i prezime studenta:	Ivan Mijić
Studij:	Diplomski sveučilišni studij Elektrotehnika, smjer Komunikacije i informatika'
Mat. br. studenta, godina upisa:	D 970, 12.10.2015.
Ephorus podudaranje [%]:	1%

Ovom izjavom izjavljujem da je rad pod nazivom**: Primjena Kali Linux distribucije za testiranje sigurnosnih ranjivosti u mreži**

izrađen pod vodstvom mentora Doc.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:

Predgovor

Veliko hvala mentoru doc.dr.sc. Krešimiru Grgiću na savjetima, strpljenju i uloženom vremenu prilikom pisanja ovog rada. Također se zahvaljujem obitelji na strpljenju i podršci te svima koji su mi pripomogli pri izradi diplomskog rada.

Sažetak

1. UVOD

Računalne mreže su temelj informacijskih sustava. Pod računalnu mrežu spadaju različiti poslužitelji, radne stanice, sustavi za pohranu podataka, sustavi za pohranu rezervnih kopija, telefonski sustav, pisači itd. Jedna od glavnih uloga računalnih mreža je da povezuje informacijski sustav na Internet, a time je omogućen pristup na Internet, ali i s Interneta. Mrežni uređaji i komunikacijske veze čine glavne dijelove računalne mreže. Mnoštvo različitih protokola čine rad računalne mreže efikasnim. Različiti propusti i mane računalnih protokola dovode do sigurnosne ranjivosti računalne mreže i cijelog informacijskog sustava. U ovom radu testira se sigurnosna ranjivost u mreži pomoću Kali Linux distribucije.

Rad je koncipiran u dvije cjeline. U prvoj cjelini ukratko je opisana teorijska osnova o računalnim mrežama i sigurnosnim ranjivostima.

Druga cjelina opisuje penetracijsko testiranje, Kali Linux distribuciju, aplikacije i alate koje će se koristiti u postupcima testiranja sigurnosnih ranjivosti i analiza.

U zaključku su na temelju prikupljenih informacija smjernice i preporuke za povećanje mrežne sigurnosti.

Zadatak rada glasi: Kali Linux distribucija predstavlja platformu koja na jednom mjestu objedinjava jako veliki broj aplikacija i alata koji se koriste u postupcima testiranja sigurnosnih ranjivosti, penetracijskih testiranja i sigurnosne analize različitih vrsta mreža. Potrebno je istražiti mogućnost primjene Kali Linux distribucije u testiranju sigurnosnih ranjivosti u mreži, te je u tu svrhu primijeniti na više različitih primjera u lokalnom mrežnom okruženju. Prikupljene rezultate potrebno je analitički obraditi, te istaknuti smjernice i preporuke za povećanje razine mrežne sigurnosti.

2. RAČUNALNE MREŽE

Razvojem velike količine podataka, programa i multimedijalnog sadržaja, potreba za prijenosom informacije je rasla. Prije nego su se razvile računalne mreže, prijenos podataka se odvijao putem prijenosnih medija za pohranu podataka (npr. diskete, CD ROM). Ovakav način prijenosa podataka je bio pogodan za male udaljenosti i male količine informacija. Prijenos podataka na veće udaljenosti bio je spor i oduzimao je puno vremena budući da su se prijenosni mediji morali slati poštom. Zbog razvoja osobnih računala i potrebe za bržim slanjem podataka veće količine, javljaju se prve računalne mreže koje su bile povezane bakrenim vodovima. Prema tome može se reći da je računalna mreža skup dvaju ili više računala koji međusobno komuniciraju preko zajedničkog medija. Ubrzo se pojavila potreba za većim brzinama prijenosa. Veće brzine prijenosa podataka postignute su korištenjem optičkih vodova. Razvojem mobilnih uređaja javlja se potreba za fleksibilnošću koju omogućava bežični prijenos informacija. Prema tome medij kojim se prostire informacija može biti žični i bežični. Žični medij predstavljaju vodiči poput bakrenih vodiča i optičkih vlakana, dok bežični medij predstavlja zrak kojim se šire elektromagnetski valovi.

2.1. Vrste računalnih mreža

Postoje različite podjele računalnih mreža, a neke od njih su:

- prema veličini
- prema topologiji
- prema tehnologiji prijenosa
- prema funkcionalnoj povezanosti između pojedinih elemenata mreže

Računalne mreže prema veličini dijele se na nekoliko vrsta [1]. U praksi su najistaknutije:

- mreže lokalnog dosega (od jedne institucije)
- mreže srednjeg dosega (gradske)
- mreže globalnog dosega (Internet)

LAN (engl. *Local Area Network*) predstavlja lokalnu mrežu koja povezuje ograničen broj računala na ograničenom prostoru. Ograničenost prostora mreže određena je dužinom spojnih vodova, odnosno dosegom elektromagnetskog vala kod bežičnog medija. Dužina se kreće oko par kilometara ovisno o tome kome se pruža servis (tvrtka, kampus, regija). Karakteristike ove mreže su velika brzina, mala kašnjenja i male vjerojatnosti pogreške u prijenosu. Manji prostor i manji broj računala koji se povezuju omogućuju kvalitetniju izvedbu mrežne arhitekture. LAN je moguće povezati s drugim mrežama istih ili različitih komunikacijskih protokola pomoću usmjerivača (engl. *Router*) i pristupnika (engl. *Gateway*) U lokalnoj mreži komunikacija računala definirana je *Ethernet* (IEEE 802.3) standardom. *Ethernet* standard opisuje specifikacije koje se odnose na regulaciju pristupa mediju, fizičko adresiranje i interakcija računala s medijem za prijenos [1][2].

MAN (engl. *Metropolitan Area Network*) predstavlja mrežu koja se rasprostire duž par desetaka kilometara što je dovoljno za pokrivanje grada [1].

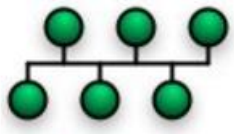
WAN (engl. *Wide Area Network*) predstavlja mrežu koja nema fizičkog ograničenja rasprostiranja. Predstavnik WAN mreže je Internet koji je nastao povezivanjem više mreža. Brzina prijenosa u WAN mrežama je manja u odnosu na LAN mreže. Kod LAN mreže brzine prijenosa su do 1 Gbps dok su kod WAN mreže nekoliko Mbps. WAN mreže su ograničene brojem raspoloživih adresa čvorova. Problem se nastoji riješiti povećanjem broja bitova koji tvore IP adresu. O novom Internet protokolu IPv6 govorit će se kasnije [1].

Druga podjela računalnih mreža je prema topologiji. Postoje dvije podjele prema topologiji, a to su logička i fizička [1]. Neki od tipova fizičke topologije su:

- sabirnička (engl. *Bus*)
- prstenasta (engl. *Ring*)
- zvjezdasta (engl. *Star*)
- hijerarhijska (engl. *Hierarchical*)
- isprepletena (engl. *Mesh*)

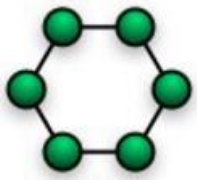
Sabirnička topologija (Slika 2.1.) je korištena u starijim mrežama koje su bile vezane koaksijalnim kabelima. Sastoji se od glavnog vodiča (sabirnice) na koju su povezani čvorovi koji komuniciraju. Čvorovi su uređaji koji tvore mrežu (računala, pisači, poslužitelji). Prednost

sabirničke topologije je jednostavnost spajanja i smanjen trošak korištenog medija. Nedostatak sabirničke topologije je da u slučaju oštećenja sabirnice mreža pada, a samim time otežan je postupak pronalaženja oštećenja. Drugi nedostatak je potreba za terminatorima koji se postavljaju na krajevima sabirnice. Ovim postupkom smanjena je refleksija i odbijanje signala čime se smanjuju smetnje u mreži. Sav promet koji se šalje kroz sabirnicu dostupan je svim čvorovima koji su spojeni na mrežu. Dužina vodiča i broj čvorova je ograničen [1][3].



Sl. 2.1. *Sabirnička mrežna topologija* [1]

Prstenastu topologiju (Slika 2.2.) čine čvorovi koji su povezani s dva susjedna čvora. Zadnji čvor u nizu i prvi su međusobno povezani tvoreći krug. Prijenos podataka se vrši jednim pravcem u krug. Odredišni čvor određen je IP ili MAC adresom. Svi čvorovi provjeravaju IP ili MAC adresu. Čvor na koji je adresiran paket će primiti informaciju, a ostali čvorovi će ignorirati. Prednost prstenaste topologije je da se povećanjem sustava smanjuje utjecaj na performanse, a samim time svi čvorovi imaju isti pristup. Prstenasta topologija može biti veća u odnosu na sabirničku zato što svaki čvor obnavlja signal. Nedostatak je visoka cijena, kompleksnost i osjetljivost na kvar. Ukoliko dođe do prekida u jednom čvoru, utjecaj će biti na ostalim čvorovima [3].



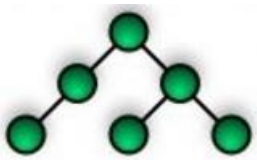
Sl. 2.2. *Prstenasta mrežna topologija* [1]

Zvjezdasta topologija (Slika 2.3.) je najčešći oblik povezivanja unutar lokalne mreže (LAN). Temelji se na središnjem uređaju na kojem su spojeni ostali čvorovi. Središnji uređaj može biti preklopnik (engl. *Switch*) ili koncentrator (engl. *Hub*). Ukoliko je središnji uređaj koncentrator, komunikacija je moguća između dva uređaja. Ako je središnji uređaj preklopnik komunikacija

je moguća između više parova čvorova istovremeno. Detaljniji opis rada preklopnika, koncentratora i ostalih mrežnih uređaja bit će opisano u idućem potpoglavlju. Prednost zvjezdaste topologije je jednostavnost spajanja i održavanja. Ukoliko dođe do oštećenja vodiča, kvar će osjetiti čvor koji je istim vodičem povezan. Nedostatak je veći zahtjev za prijenosnim medijem i ovisnost svih čvorova o središnjem uređaju [3].

Sl. 2.3. *Zvjezdasta mrežna topologija* [1]

Hijerarhijska topologija (Slika 2.4.) temelji se ne hijerarhijskom rasporedu čvorova. Na središnji čvor su spojeni čvorovi koji se nalaze u nižem sloju. Čvorovi nižeg sloja mogu imati grupu čvorova još nižeg sloja [1].



Sl. 2.4. *Hijerarhijska mrežna topologija* [1]

Isprepletena topologija (Slika 2.5.) temelji se na izravnim vezama između više ili svih čvorova u mreži. Zbog velike cijene i složenosti isprepletena topologija se koristi u krajnje nužnim mjestima (npr. nuklearne elektrane) [1].

Sl. 2.5. *Isprepletena mrežna topologija* [1]

Logička topologija se odnosi na način komunikacije između čvorova. Primjer logičke topologije je *Token Ring* topologija. Topologija se temelji na *token* (žeton) paketu koji se prenosi od čvora do čvora u prstenastoj topologiji. Ukoliko čvor posjeduje *token* paket omogućeno mu je slanje informacija. *Token Ring* komunikacijom spriječeno je nastajanje kolizije, odnosno zagušenje mreže [3].

Treća podjela računalnih mreža je prema tehnologiji prijenosa, a to su:

- difuzijske mreže (engl. *Broadcast network*)
- mreža od točke do točke (engl. *Point to Point*)

Difuzijska mreža koristi jedan zajednički kanal koji koriste sva računala u mreži. Kroz kanal se šalju paketi koji su označeni adresama. Svako računalo čita adresu. Ako se adresa podudara s korisnikovom adresom, paket se otvara, u suprotnom se ignorira.

Mreža od točke do točke je način komunikacije u kojoj korisnik ostvaruje vezu jedan s drugim. Paketi unutar ove mreže također imaju adresu čime je omogućena komunikacija s čvorovima koji nisu izravno povezani.

Četvrta podjela računalnih mreža je prema funkcionalnoj povezanosti između elemenata mreže, a to su:

- *Active networking*
- *Client – Server*
- *Peer to peer*

Active networking je komunikacijski model koji omogućava paketima koji prolaze kroz telekomunikacijsku mrežu dinamičku promjenu rada te mreže [1].

Client – Server je komunikacijski model u kojem postoji uloga klijenta i poslužitelja. Klijent upućuje zahtjev za podacima, a poslužitelj ih dostavlja. Svaki klijent i poslužitelj predstavljaju jedan čvor te mreže.

Peer to peer je komunikacijski model u kojem su svi članovi ravnopravni klijenti i poslužitelji.

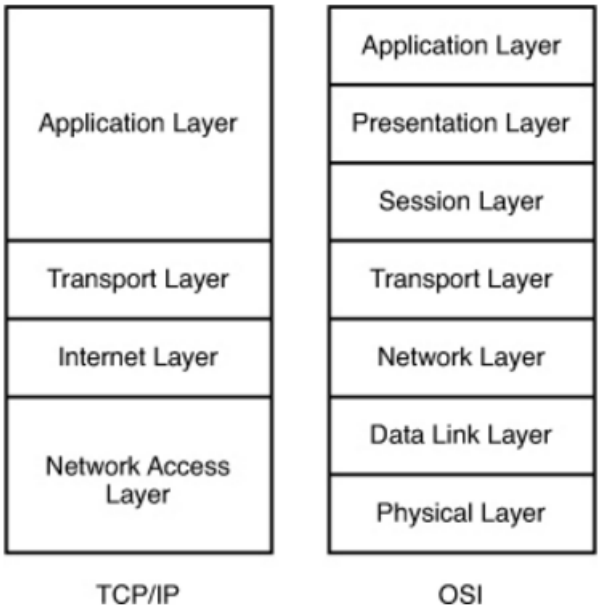
2.2. Referentni modeli računalne mreže i protokoli

Elemente računalnih mreža čine čvorišta i kanali koji ih povezuju. Čvorišta računalne mreže se dijele u dvije vrste: na one koje ostvaruju usluge prijenosa i one koje koriste usluge prijenosa. Čvorovi koji ostvaruju usluge prijenosa čine „unutrašnjost mreže“ i nazivaju se prijenosnicima. U prijenosnike se ubrajaju: usmjerivači (engl. *Router*), pristupnici (engl. *Gateway*), preklopnici (engl. *Switch*) i mostovi (engl. *Bridge*). Detaljnije o svakom elementu bit će opisano u podnaslovima slojeva OSI referentnog modela. Čvorovi na kojima rade mrežne aplikacije zovemo domaćinima (engl. *Host*) i nalaze se „na rubovima“ mreže. Domaćini mogu raditi kao klijenti (engl. *Client*) ili poslužitelji (engl. *Server*). Serveri su stalno aktivni u mreži. Na njima se nalaze web stranice, pretinci e-pošte i različite baze podataka koji se nude klijentima radi prijenosa informacija različitog sadržaja [4][5].

Kad su prednosti umrežavanja bile očigledne, veliki problem među proizvođačima *hardware*-a i *software*-a je bio nedostatak standardizacije. Različita idejna rješenja tvrtki su se miješala što je predstavljalo veliki problem umrežavanja. Kao rješenje problema načinjena su dva referentna modela. Jedan model načinjen od strane ISO (engl. *International Organization for Standardization*), a drugi od strane ministarstva obrane SAD-a. Kroz vrijeme su se oba modela usavršavala, što je dovelo do mreža kakve postoje danas. ISO organizacija je postala glavna organizacija za standardizaciju. Model načinjen od strane ISO organizacije je OSI (engl. *Open Systems Interconnection*) model [3]. Prednosti koje pružaju OSI model i TCP/IP model (model ministarstva obrane) su:

- Poticanje standardizacije radi definiranja funkcija koje se izvode na pojedinom sloju.
- Komunikacijski proces je rastavljen u slojevima što omogućava da svaki sloj obavlja svoju funkciju bez obzira na ostale slojeve.
- Promjene u jednom sloju ne uzrokuju potrebe za promjenama u drugim slojevima što ubrzava napredak i proizvodnju.
- Mogućnost komunikacije različitih tipova *hardware*-a i *software*-a kroz standardiziranu komunikaciju između slojeva.
- Potiču se različiti proizvođači za međusobnim razvitkom kroz razvoj zajedničkog okvira.

Cilj podjele komunikacijskog procesa u slojeve je izbjegavanje potrebe za razvojem novog komunikacijskog procesa ukoliko dođe do nadogradnje.



Sl. 2.6. *TCP/IP i OSI (ISO) model mreže* [6]

1970. ministarstvo obrane je razvilo TCP/IP (engl. *Transmission Control Protocol / Internet Protocol*). TCP/IP model je četveroslojni model i kasnije postaje standard za LAN protokole [3]. Modeli olakšavaju analizu razvoja protokola i komunikacije. Podjelom na slojeve omogućeno je da razvoj protokola na pojedinim slojevima ne ovisi o razvoju protokola na drugim slojevima. Na svakom sloju može djelovati više različitih protokola. Veza između dva susjedna sloja kojom oni komuniciraju zove se sučelje (engl. *Interface*). Zadaća sučelja je prilagoditi informaciju između protokola različitih slojeva. Komunikacija između slojeva iste razine vrši se protokolima [1]. OSI model sastoji se od sedam slojeva, nabrojani su od najvišeg prema najnižem, a to su:

1. Aplikacijski sloj (engl. *Application Layer*)
2. Prezentacijski sloj (engl. *Presentation Layer*)
3. Sesijski sloj (engl. *Session Layer*)
4. Prijenosni sloj (engl. *Transport Layer*)

5. Mrežni sloj (engl. *Network Layer*)
6. Sloj linka podataka (engl. *Data Link Layer*)
7. Fizički sloj (engl. *Physical Layer*)

Komunikacija između uređaja A i uređaja B započinje najvišim slojem. Aplikacijski sloj strane A poziva aplikacijski sloj strane B i uspostavlja se ravnopravan odnos. Aplikacijski sloj traži usluge nižeg sloja. Prezentacijski sloj strane A pomoću protokola uspostavlja ravnopravan odnos s prezentacijskim slojem na strani B. Ponavlja se postupak gdje viši sloj traži usluge nižeg sloja sve do najnižeg sloja. U fizičkom sloju razmjenjuju se podaci. Na prijemnoj strani podaci se šalju višim slojevima sve do odredišta. Prilikom komunikacije oba modela koriste tehnologiju komutacije paketa (engl. *Packet-switching*). Ovom tehnologijom određeno je da se jedinice podataka koje se šalju zovu paketi. Svaki paket sadrži odredišnu adresu pa se na taj način paketi preusmjeravaju. Paketi u svim slojevima OSI modela nisu isti. Za svaki sloj, oblik pakiranja paketa se zove PDU (engl. *Protocol Data Unit*). U aplikacijskom, prezentacijskom i sesijskom sloju podaci nisu zapakirani. U prijenosnom sloju podaci se dijele na segmente. Mrežni sloj segmente pakira u pakete. Sloj linka podataka pakete pakira u okvire, a u fizičkom sloju okviri se u obliku bitova prenose mrežom. Postupak pakiranja informacija u oblik pogodan za prijenos zove se enkapsulacija, a obrnuti postupak deenkapsulacija [1].

2.2.1. Aplikacijski sloj

U aplikacijskom sloju započinje proces enkapsulacije. Sloj pruža usluge aplikacijama. Kao primjer naveden je FTP (engl. *File Transfer Protocol*) kojeg ovaj sloj definira. FTP je protokol za prijenos podataka. Kako bi se prijenos izveo, krajnji korisnik mora pozvati i izvršiti aplikaciju. FTP protokol djeluje na modelu *client-server*, što znači da se aplikacija FTP klijenta koristi za traženje podataka, a FTP poslužitelja odgovara i šalje podatke. FTP koristi TCP *port* 21 kako bi uspostavio vezu s poslužiteljem, a *port* 20 za prijenos podataka. Ako se koristi pasivni način rada, prijenos će se vršiti slučajno odabranim portom od strane klijenta. Paketi za provjeru autentičnosti šalju se kao otvoreni tekst što čini FTP neprikladnim za sigurne prijenose. Postoji sigurna alternativa FTP-u kao što je SSH (engl. *Secure Shell*). SSH temelji se na uporabi

kriptografskih metoda koje omogućuju tajnost podataka koji se kreću kroz nesigurnu mrežu [3][7]. Protokol koji djeluje na ovom sloju je HTTP (engl. *Hypertext Transfer Protocol*) koji se koristi za prijenos web stranica preko mreže. Drugi primjeri protokola koji rade na ovom sloju su SMTP (engl. *Simple Mail Transfer Protocol*) za slanje e-pošte, DNS (engl. *Domain Name System*) za DNS upite. SMTP protokol ima mogućnost pohrane podataka i kasnijeg ponovnog slanja ukoliko dođe do neuspjeha prilikom slanja. SMTP poslužitelj odgovara klijentima pomoću POP (engl. *Post Office Protocol*) ili IMAP (engl. *Internet Message Access Protocol*) protokola. POP i IMAP su potrebni iz razloga što SMTP samo dostavlja e-poštu i nije u mogućnosti slati zahtjeve. SMTP koristi TCP *port* 25 [3]. DNS prevodi simbolička imena računala u njihove IP adrese i obratno. Sustav se sastoji od distribuirane baze podataka s imenima računala. Bez ovog servisa komunikacija među poslužiteljima bila bi moguća samo unošenjem IP adresa. DNS koristi TCP *port* 53 [8].

2.2.2. Prezentacijski sloj

Uloga prezentacijskog sloja je da informacije s izvorišnog aplikacijskog sloja uspješno prikaže odredišnom aplikacijskom sloju. Informacija se u izvorišnom prezentacijskom sloju transformira, šifrira i komprimira, dok se na odredišnom prezentacijskom sloju vrši obrnuti postupak. Transformacija informacije je ponekad potrebna budući da različiti uređaji koriste različite formate prikaza alfanumeričkih znakova (npr. ASCII, EBCDIC). Ukoliko je potrebna transformacija, sloj prezentacije dodaje informaciju koja će se nalaziti ispred podataka aplikacijskog sloja. Šifriranje služi kao zaštita od napadača koji žele presresti podatke. Šifriranje može biti primijenjeno u prezentacijskom sloju ili u sloju linka podataka. Primjeni li se u prezentacijskom sloju, podaci će biti šifrirani. Ukoliko se šifriranje primjeni u sloju linka podataka, cijeli će paket biti šifriran. Kompresija se vrši kako bi se uklonili redundantni podaci. Kompresijom se postiže efikasan prijenos podataka uz manje opterećenje mreže budući da se prenosi manja količina podataka uz jednaku kvalitetu [3].

2.2.3. Sesijski sloj

Sesijski sloj je odgovoran za koordinaciju razmjene informacija između aplikacija koji su u upotrebi. Sloj pokreće, održava i završava sesiju između aplikacija. Sesija je uspostavljena i prekinuta nakon fizičke sesije između računala. Da bi sesija bila uspješna, dodaju se relevantne informacije za upravljanje sesijom ispred informacija dobivenih iz prezentacijskog sloja [1][3].

2.2.4. Prijenosni sloj

Prijenosni sloj omogućava pouzdan prijenos podataka između uređaja. Sloj pruža spojnu i bespojnu vezu. Spojnu vezu pruža TCP (engl. *Transmission Control Protocol*), a bespojnu UDP (engl. *User Datagram Protocol*). TCP protokol prije slanja uspostavlja vezu s transportnim slojem odredišnog uređaja. Uspostava veze vrši se *three-way handshake* postupkom. Postupak se sastoji iz tri koraka. Prvi korak je zahtjev za uspostavu veze s drugim računalom (šalje se SYN paket). Drugi korak je da drugo računalo odgovara na primljeni SYN paket sa SYN ACK paketom. U trećem koraku nakon primanja SYN ACK paketa prvo računalo ulazi u stanje uspostavljene veze i šalje drugom računalu ACK paket. Nakon što drugo računalo primi ACK paket, također ulazi u stanje uspostavljene veze. Uspostavljenom vezom šalju se podaci. Ukoliko dođe do gubitka podataka, ponovno se šalju. Podaci su u transportnom sloju podijeljene na segmente gdje se svakom segmentu dodaje redni broj (engl. *sequence number*). Pomoću rednih brojeva olakšan je postupak dobivanja podataka iz segmenata kao i prepoznavanje ukoliko dođe do gubitka segmenta. UDP nema kontrolu nad gubicima segmenata pa se koristi gdje je brzina prijenosa na višoj razini od integriteta segmenata (multimedijalne aplikacije). Prijenosni sloj je zadužen za identifikaciju aplikacije na odredišnom računalu pomoću broja *port*-a. Brojevi *port*-a su standardizirani i ne radi se o fizičkim *port*-ovima (vratima) nego *software*-skim. Ako se radi o web stranici, prijenosni sloj će koristiti broj *port*-a koji je dodijeljen HTTP protokolu, a to je 80 [3].

Tab. 2.1. *Brojevi port-ova*

Usluga	TCP port
DNS – Domain Name Service	53
HTTP - Hypertext Transfer Protocol (Web)	80
HTTPS – Hypertext Transfer Protocol (Secure Web)	443
SMTP- Simple Mail Transport Protocol	25
POP – Post Office Protocol	109, 110
FTP – File Transfer Protocol	20, 21
SSH – Secure Shell	22

Prijenosni sloj ima mogućnost multipleksiranja više segmenata različitih poruka u jedan komunikacijski krug tako da se svakom segmentu dodaje oznaka kako bi se moglo raspoznati kojoj poruci segment pripada. Postoje tri vrste prijenosa u mreži, a to su: *unicast*, *broadcast* i *multicast*. *Unicast* je način prijenosa u kojem jedan izvorišni uređaj šalje informacije jednom odredišnom uređaju. *Broadcast* je način prijenosa u kojem jedan izvorišni uređaj šalje informacije svim uređajima koji su na mreži. *Multicast* je način prijenosa u kojem jedan izvorišni uređaj šalje podatke grupi uređaja koji su na mreži. Ukoliko se radi o *unicast* prijenosu, zastupljen je TCP, a ukoliko se radi o *broadcast* ili *multicast* načinu prijenosa, zastupljen je UDP.

2.2.5. Mrežni sloj

Mrežni sloj identificira odredišni uređaj pomoću logičke identifikacije. Logička identifikacija je IP adresa. IP adresa je jedinstvena za sve uređaje koji se nalaze na mreži. Protokol koji dodaje izvorišnu i odredišnu IP adresu paketima se zove IP (engl. *Internet Protocol*). Uređaj koji se nalazi u mrežnom sloju je usmjerivač. Usmjerivač je aktivni element mreže, što znači da je za njegov rad potrebno napajanje i vrši logičku funkciju. Preko IP adresa unutar tablice usmjeravanja, usmjerivač određuje prenosi li se paket unutar ili između mreža. Zbog sve većeg broja uređaja koji imaju pristup internetu, IPv4 adrese zamjenjuju IPv6 adrese. Razlika je u veličini adresa, odnosno količini podmreža i uređaja kojima je moguće dodijeliti ograničen broj IP adresa. IPv4 adresa je 32-bitni broj, dok je IPv6 128 bitni broj. Protokol koji se nalazi u mrežnom sloju je ICMP (engl. *Internet Message Control Protocol*) koji služi za slanje kontrolnih poruka. Također vrlo važan protokol koji se nalazi u ovom sloju je IPsec. IPsec je zaštitni protokol koji služi za autentifikaciju uređaja, ali ne i korisnika. Koristi se u IPv6, a u IPv4 se ne koristi što predstavlja problem budući da postoje uređaji koji rade na IPv4, a prijelaz na IPv6 sporo traje.

2.2.6. Sloj linka podataka

Uloga sloja linka podataka je da pretvara logički identifikator (IP adresa) u fizički identifikator. Vrsta identifikacije ovisi o protokolu koji se koristi. Identifikator za *Ethernet* se zove MAC adresa (engl. *Media Access Control*). MAC adresa je određena od strane proizvođača za sve uređaje koji imaju mogućnost pristupa mreži. Kao primjer drugih korištenih identifikatora je DLCI (engl. *Data-Link Connection Identifier*) koji se koristi za identifikaciju krajnjih točaka u *Frame Relay* mreži. Kao što mrežni sloj logički identificira IP adresu i s njom označava paket, tako i sloj linka podataka čini isto dodavanjem MAC adrese. Pomoću ARP protokola (engl. *Address Resolution Protocol*) moguće je iz IP adrese dobiti traženu MAC adresu. Sloj linka podataka dodaje izvorišnu i odredišnu MAC adresu ispred podataka koje prima od mrežnog sloja. Osim dodanih MAC adresa, iza podataka iz mrežnog sloja dodaje se rep (engl. *Trail*). Rep sadrži CRC (engl. *Cyclic Redundancy Check*). CRC je zaštita od šumova

koje se generiraju u mediju kojim se prenosi informacija. Nastaje matematičkom povezanošću s podacima. Podaci se odnose na sve informacije iz slojeva 3 do 7. Aktivni elementi koji se nalaze na sloju linka podataka su preklopnik i most. Preklopnik koristi memoriju u koju sprema MAC adrese svih uređaja koji su povezani. Most dijeli mrežu na više dijelova. Glavna funkcija mosta je da odredi treba li okvir proslijediti na drugi segment [3].

2.2.7. Fizički sloj

Na fizičkom sloju informacije koje se primaju od sloja linka podataka pretvaraju se u bitove za prijenos. Način na koji se bitovi prenose ovisi o mediju kojim se prenose podaci. Ako se podaci prenose žičnim medijem, bitovi će biti predstavljeni električnim razinama. Ako se radi o bežičnom prijenosu, bitovi su predstavljeni različitim modulacijama elektromagnetskog vala. U optičkom mediju bitovi su predstavljeni sa stanjem svjetlosti (ima svjetlosti, nema svjetlosti). Mrežni uređaji koji su u fizičkom sloju su koncentrator, pojačalo (engl. *Repeater*), utičnice, kabeli itd. Signal koji koncentrator primi na jednoj priključnici obnavlja ga i šalje na sve priključnice. Pojačalo je uređaj koji obnavlja primljeni signal i prosljeđuje [4][5].

TCP/IP model i OSI model opisuju enkapsulaciju i deenkapsulaciju informacije. Sloj pristupa mreže TCP/IP modela objedinjuje fizički sloj i sloj linka podataka OSI modela. Aplikacijski sloj TCP/IP modela ima funkcije sesijskog, prezentacijskog i aplikacijskog sloja OSI modela [1]. Slojevi TCP/IP modela od najvišeg prema najnižem su [9]:

1. Aplikacijski sloj
2. Prijenosni sloj
3. Sloj interneta (engl. *Internet Layer*)
4. Sloj pristupa mreži (engl. *Network Access Layer*)

Neke detaljnije razlike u načinu obavljanja određenih operacija u TCP/IP modelu u odnosu na OSI model su sljedeće:

- U OSI modelu je predviđeno da sloj sesije uspostavlja i upravlja komunikacijsku sesiju između usluga koje se koriste. U TCP/IP ova se funkcija izvodi TCP/IP protokolom na transportnom sloju.

- Pretvorba podataka u prezentacijskom sloju OSI modela se vrši u aplikacijskom sloju TCP/IP modela.
- Identifikacija protokola se događa u transportnom sloju oba modela. Kod TCP/IP modela taj sloj je također mjesto gdje se pružaju konekcijske usluge (TCP ili UDP).
- Kada je razvijen TCP/IP model odlučeno je da je podjela sloja linka podataka i fizičkog sloja nepotrebna.

2.3. Sigurnost računalnih mreža

U današnjem svijetu sve je više informacija koje se koriste na različitim uređajima. Broj korisnika i način na koji se informacija dijeli raste. Zbog toga postoji sve veća opasnost od neovlaštene uporabe informacije, širenja krivih informacija i uništavanja informacije. Kako bi se spriječile negativne posljedice, proučavanje i zaštita sigurnosti računalnih sustava je jedno od najvažnijih područja kojima se računalni inženjeri bave. U praksi postoje različiti informacijski sustavi koji su od iznimne važnosti u različitim ljudskim djelatnostima, a neki od njih su: vojni, bankovni, zdravstveni, gospodarski, znanstveni informacijski sustav itd. Stoga informacijski sustavi moraju ispuniti sigurnosne zahtjeve kao što su [10][11]:

- Povjerljivost ili tajnost: pristup informacijama imaju samo ovlašteni korisnici
- Raspoloživost: usprkos različitim nepredvidivim utjecajima, informacija mora uvijek biti dostupna ovlaštenim korisnicima
- Besprijekornost: treba osigurati da su informacije poslane i primljene u nepromijenjenom obliku.
- Autentičnost: postupkom autentifikacije moraju se prepoznati ovlašteni korisnici
- Autorizacija: postupkom autorizacije dopušta se pristup korisnicima samo nekim sadržajima
- Neporecivost: zaštita od opovrgavanja poruka ovlaštenog korisnika.

Sigurnost računalnih sustava moguće je ugroziti na različite načine. Jedna od mogućih podjela sigurnosnih mehanizama je [10]:

- Zaštita od vanjskih utjecaja
- Zaštita ostvarena sučeljem prema korisniku
- Unutarnji zaštitni mehanizmi
- Komunikacijski zaštitni mehanizmi

Zaštita od vanjskih utjecaja bi bila zaštita od fizičkog djelovanja neovlaštenih korisnika na uređaje informacijskog sustava. Primjer fizičkih utjecaja bila bi mehanička oštećenja i krađa uređaja i medija na kojima su pohranjene informacije. Kako bi se uspješno zaštitili od vanjskih utjecaja potrebno je ograničiti pristup prostorijama u kojima se nalaze uređaji s pohranjenim

informacijama. U praksi se čuvaju kopije informacija na različitim sigurnim mjestima što dodatno povećava sigurnost sustava od vanjskih utjecaja.

Zaštita ostvarena sučeljem prema korisniku je izvedena tako da samo ovlašteni korisnici mogu koristiti računalni sustav. Preko sučelja provjerava se identitet i utvrđuje vjerodostojnost (autentičnost) identiteta korisnika. Prilikom prijave za rad provodi se identifikacija i autentifikacija korisnika. Unosom korisničkog imena korisnik vrši identifikaciju, a unosom pripadajuće lozinke autentifikaciju.

Nakon postupka autentifikacije korisnik može upotrebljavati sredstva koja mu računalni sustav pruža. Unutarnji zaštitni mehanizmi omogućuju pojedinom korisniku korištenje sredstava za koje ima pristup (autoriziran).

Zbog prijenosa informacije različitim medijima pristup medijima se ne može fizički zaštititi, što omogućuje lako narušavanje sigurnosti od strane napadača. Zbog toga komunikacijski zaštitni mehanizam štiti informacije kriptiranjem.

Prilikom prijenosa informacije od izvorišta do odredišta, različite vrste napada mogu narušiti sigurnost mreže, a neki od njih su [10][11]:

- Prisluškivanje (engl. *Eavesdropping*) ili presretanje (engl. *Interception*): napadač čita pakete koje su namijenjene nekom drugom i na taj način dolazi do osjetljivih informacija. Napad je pasivan ukoliko se ne djeluje na informacije. Prisluškivanjem se djeluje na povjerljivost i tajnost informacija.
- Prekidanje (engl. *Interruption*): napad prekidanjem komunikacijskog kanala između izvorišta i odredišta čime se narušava raspoloživost informacija.
- Promjena sadržaja poruke: napadač prekida komunikacijski kanal i predstavlja se kao izvorište. Na taj način mijenja sadržaj poruke i djeluje na integritet informacije.
- Izmišljanje poruka: napadač se lažno predstavlja kao izvorište i uspostavlja komunikacijski kanal s odredištem. Na taj način šalju se izmišljene poruke i narušava se integritet informacije.
- Lažno predstavljanje: napadač se predstavlja kao neki drugi korisnik na način da je provalio u tuđi korisnički račun.
- Poricanje (engl. *Repudiation*): nakon poslane poruke korisnik se može predomisliti i poricati autorstvo poruke tvrdeći da se netko lažno predstavio.

Na sigurnost mogu utjecati pojedine komponente računalnih sustava. Sklopovlje računala utječe na sigurnosni zahtjev raspoloživosti informacija. Nedopuštenom uporabom i krađom programa utječe se na tajnost, besprijekornost i raspoloživost informacija. Način na koji se ostvaruje neovlašteno djelovanje na programe jesu napadi: virusima, programskim crvima (engl. *Worms*), trojanskim konjima i zlоćudnim programima koji djeluju na datoteke operacijskog sustava (engl. *Rootkit*). Podacima koji su smješteni u datoteke i baze podataka narušena je raspoloživost neovlaštenim brisanjem, tajnost neovlaštenim čitanjem sadržaja i besprijekornost neovlaštenom promjenom sadržaja.

2.3.1. Sigurnost na razini aplikacija

Osim fizičkog sloja, na svim slojevima OSI modela moguće je implementirati protokole i sigurnosnu zaštitu. Na razini aplikacije sustav sigurnosti se ostvaruje za svaku aplikaciju posebno pa se samim time može reći da se sigurnosni sustav smatra dijelom te aplikacije. Sigurnost i zaštita koji se mogu ostvariti na nižim razinama mreže ne udovoljavaju svim sigurnosnim zahtjevima viših razina, a posebno se odnosi na specifične potrebe pojedinih aplikacija. Kao primjer navodi se sustav sigurnosti za utvrđivanje autentičnosti i integriteta poruka na razini aplikacija. On nije pogodan u sustavu sigurnosti na razini linka podataka s okvirima ili na mrežnoj razini s IP paketima. Oblici sigurnosne zaštite na aplikacijskom sloju su važni kod financijskih transakcija preko web sjedišta. Dakle, sustav zaštite je moguće ostvariti na nižim slojevima, ali nisu dovoljne za potrebe protokola viših slojeva. Dodatni razlog zbog kojeg se sustav sigurnosti i zaštite postavlja na višim razinama je zbog jednostavnosti oblikovanja i realizacije sustava. Sigurnosni sustavi koji udovoljavaju potrebama protokola viših razina je jednostavnije oblikovati i realizirati od jednog univerzalnog sustava na nižim razinama koji je složen i opsežan kako bi izvršavao isti zadatak [5].

2.3.2. Sigurnost na razini prijenosa

Sigurnost i zaštita na razini prijenosa ostvaruje se na način da se TCP protokol nadopuni elementima pomoću kojih se ostvaruje povjerljivost, autentičnost i integritet. Postupkom šifriranja ostvaruje se povjerljivost, autentičnost i integritet. Tako nadopunjena verzija TCP naziva se slojem sigurnih utičnica (engl. *Secure socket layer* – SSL). SSL je posebno važan kod poslovnih web sjedišta kod kojih se izvodi trgovina, financijske transakcije, prijenos brojeva kreditnih kartica i drugi povjerljivih informacija. Pokazatelj da web sjedište koristi SSL je znak „*s*“ u URL adresi kod oznake „*https*“. Komunikacija preko SSL sastoji se iz tri koraka: rukovanje strana koje komuniciraju (engl. *Handshake*), izvođenje ključeva sesije i prijenos podataka. Ovaj rad neće opisivati detalje ova tri koraka [5][7].

2.3.3. Sigurnost na mrežnoj razini i niže

IPsec (engl. *IP security*) protokol definira sigurnost i zaštitu na mrežnom sloju. Sigurnost i zaštita je na razini prijenosa IP paketa koji se prenose od čvora do čvora, odnosno od izvora do odredišta. IPsec je jedan od tri VPN protokola (engl. *Virtual Private Network*). VPN koristi usluge mrežnog prijenosa javne mreže, ali tvore zatvorene sustave koji sprečavaju pristup drugim subjektima. Povezivanjem više udaljenih mreža pomoću posebnih vrata koja izvode dvostruka pakiranja IP paketa nastaju virtualne privatne mreže. IPsec šifrira ne samo podatke paketa, već i informacije o zaglavlju. Također ima zaštitu od neovlaštenog ponovnog slanja paketa. Važnost šifriranja zaglavlja je u tome što napadač nije u mogućnosti presresti informacije o prijenosu. Ostala dva VPN protokola su PPTP (engl. *Point to Point Tunneling Protocol*) i L2TP (engl. *Layer 2 Tunneling Protocol*) [12].

PPTP je najstariji VPN protokol koji je služio šifriranju paketa i autentifikaciji korisnika na starim mrežama od točke do točke (engl. *Point to Point*). Koristi dvije različite metode autentifikacije korisnika, a to su EAP (engl. *Extensible Authentication Protocol*) i CHAP (engl. *Challenge Handshake Authentication Protocol*). EAP je posebno dizajniran za PPTP. CHAP je proces autentifikacije koji se sastoji iz tri koraka, a to su da korisnik šalje šifru poslužitelju,

poslužitelj autentificira korisnika i šalje odgovor. CHAP periodično vrši ponovnu autentifikaciju korisnika iako je uspostavljena veza [12].

L2TP je dizajniran kao dodatak PPTP. Oba protokola djeluju na sloju linka podataka OSI modela. Za razliku od PPTP-a koji pruža dvije metode autentifikacije, L2TP pruža pet metoda, a to su: CHAP, EAP, PAP (engl. *Password Authentication Protocol*), SPAP (engl. *Shiva Password Authentication Protocol*) i MS-CHAP (engl. *Microsoft Challenge Handshake Authentication Protocol*). PAP je najjednostavniji oblik autentifikacije. Korisnička imena i lozinke se šalju nešifrirano kao otvoreni tekst. SPAP je dodatak PAP-u koji šifrira korisničko ime i lozinku koje se šalje Internetom.MS-CHAP je specifični Microsoft-ov dodatak CHAP-u. Za razliku od PPTP koji radi na standardnim IP mrežama, L2TP radi i na X.25 mrežama (protokol sustava telefonije) i ATM (engl. *Asynchronous Transfer Mode*) sustavima. ATM su mrežne tehnologije velikih brzina. L2TP koristi IPsec za šifriranje [12].

Zaštita i sigurnost kod sloja linka podataka kod bežičnih mreža je potrebna budući da se prijenos podataka vrši elektromagnetskim valovima. Valovi se šire na sve strane i mogu ih primati oni za koje sadržaj nije namijenjen. Protokol bežične mreže definiran je IEEE standardom 802.11 u kojem je definiran sigurnosni protokol WEP (engl. *Wired Equivalent Privacy*). WEP definira šifriranje i utvrđivanje autentičnosti strana koje komuniciraju uz upotrebu simetričnog ključa. U početku WEP je imao niz slabosti u području sigurnosne zaštite. Kriptografski ključevi su bili standardnih duljina od 64, 128 i 256 bita. Slabost WEP-a je bila u enkripciji podataka. U mreži kroz koju prolazi velika količina prometa 24-bitnih inicijalizacijskih vektora, postoji vjerojatnost ponavljanja istog niza. Zbog slabe sigurnosne zaštite usvojena je nova verzija standarda oznake 802.11i u kojoj je definiran sigurnosni protokol WPA2 koji se danas koristi. WPA2 za razliku od WEP-a uvodi povećanu vrijednost inicijalizacijskog vektora i ključa na 128 bita, onemogućuje korištenje loših oblikovanih inicijalizacijskih vektora i mijenja ključeve dinamički [12].

2.4. Sigurnosne opasnosti

Sigurnosne opasnosti su kategorizirane u šest vrsta, a to su [12]:

- Zlonamjerni software (engl. *Malware*): ovo je opći pojam za *software* koji ima zlonamjernu svrhu, a to uključuje viruse, crve, *adware*, trojanske konje i *spyware*.
- Narušavanje sigurnosti: uključuje svaki pokušaj dobivanja neovlaštenog pristupa sustavu. To uključuje provalu lozinki, mijenjanje privilegija, provala poslužitelja itd.
- DoS napadi (engl. *Denial Of Service*): sprječavaju legitiman pristup sustavu.
- Web napadi: bilo koji napad kojim se pokušava narušiti sigurnost web stranice. Dva najčešća napada su *SQL injection* i *cross-site scripting*.
- Preuzimanje sesije: napredni napadi koji pokušavaju preuzeti sesiju.
- DNS trovanje: vrsta napada kojim se pokušava ugroziti DNS poslužitelj. Na taj način korisnike se preusmjerava na zlonamjerne web stranice, uključujući web stranice za krađu identiteta.

Virus je program koji se replicira i krije unutar drugih programa bez znanja žrtve. Poput biološkog virusa, računalni virus se širi i to najčešće e-poštom prema kontaktima žrtve. Trojanski konj se pojavljuje kao bezopasan *software* koji potajno preuzima virus ili neki drugi zlonamjerni *software* na računalo. *Spyware* je *software* koji prati što žrtva čini na računalu. *Spyware* može biti kolačić (engl. *Cookie*), tekstualna datoteka koju Internet pretraživač sprema na tvrdi disk. Datoteka može biti otvorena od Internet pretraživača ili drugih pretraživača čime je moguće praćenje povijesti pretraživanja. „Logička bomba“ je *software* koji se aktivira ukoliko su ispunjeni određeni uvjeti kao što su vrijeme i datum. Kada se uvjeti ispune zlonamjerni *software* izvršava radnje poput brisanja datoteka, izmjene sustavnih konfiguracija ili aktivacija virusa. Vrsta *Spyware*-a je *Key logger* koji sprema upisane riječi. Neki *key logger*-i periodično slikaju radnu površinu računala. Podaci se spremaju za kasniju upotrebu ili se šalju e-poštom napadaču [11][12].

Aktivnost narušavanja sigurnosti se obično naziva „hakiranje“. Svaki neovlašteni pristup koji krši sigurnost, bilo preko operacijskog sustava ili drugog načina zove se provala. Tehnika za kršenje sigurnosti sustava korištenjem ljudske prirode zove se socijalno inženjerstvo. Počinitelj

dobiva informacije o ciljanoj organizaciji i koristi ih za dobivanje dodatnih informacija od korisnika sustava [11].

Napadač u ovoj vrsti napada ne pristupa sustavu, već sprječava pristup legitimnih korisnika. Način na koje se ostvaruje sprečavanje pristupa uslugama je pretrpavanje cilja napada s lažnim zahtjevima za komunikaciju čime se sprečavaju zahtjevi legitimnih korisnika. DoS napad je jedan od najčešćih napada na Internetu.

Po svojoj prirodi, web poslužitelji dopuštaju komunikaciju. Neke web stranice dopuštaju korisnicima interakciju što ih čini potencijalnim žrtvama web napada. *SQL injection* odnosi se na SQL (engl. *Structured Query Language*) naredbe u autentifikacijskim obrascima koje poslužitelj izvršava. Svrha naredbi je omogućiti napadaču pristup sustavu iako napadač nema legitimno korisničko ime i lozinku [11].

Preuzimanje sesije je složen napad za izvođenje pa nije čest oblik napada. Napadač preuzima praćenu autentificiranu sesiju između klijenta i poslužitelja.

DNS prevodi imena domena u IP adrese koju računala i usmjerivači koriste prilikom usmjeravanja prometa. DNS trovanje koristi preusmjeravanje na zlonamjernu stranicu u korist krađe osobnih informacija žrtve [8][11].

2.5. Sigurnosna zaštita

Kako bi se zaštitilo od različitih sigurnosnih prijetnji, potrebni su odgovarajući računalni programi, kao što su [11]:

- Pretraživač virusa
- Vatrozid (engl. *Firewall*)
- *Antispyware*
- Sustavi za otkrivanje napada (engl. *Intrusion Detection System* – IDS)
- *Honey pot*

Pretraživač virusa je *software* čiji je zadatak spriječiti zarazu sustava virusom. Dva su načina na koji rade pretraživači virusa. Prvi način je da sadrže bazu podataka svih poznatih virusa. Baza podataka sadrži informacije o veličini datoteke, svojstva i ponašanja. Usluge koje pružaju dobavljači pretraživača virusa je ažuriranje baze podataka o virusima. Drugi način je da pretraživač virusa prati postoje li određena djelovanja koja su tipična za virus. Tipična djelovanja su pokušaji promjene sustavnih datoteka, automatsko pokretanje e-pošte, širenje itd. Jedan od načina na koji se otkrivaju virusi su pomoću *sandbox*-a. *Sandbox* predstavlja odvojeni sustav od operacijskog sustava u kojem se pokreću nesigurne datoteke kako bi se pratilo njeno djelovanje. Ukoliko je datoteka zaražena neće djelovati na operacijski sustav. Ukoliko datoteka nije zaražena, može se koristiti u sustavu.

Vatrozid predstavlja sigurnosnu prepreku između privatne i vanjske mreže. Zadatak vatrozida je da filtrira dolazeće pakete prema parametrima kao što su: veličina paketa, izvorišna IP adresa, protokol, odredišni *port*. Vatrozid je najbolji način obrane od DoS napada i sprječavanje napadača da pretraži detalje unutrašnjosti mreže. Postoje tri tipa filtriranja, a to su: filtriranje paketa (engl. *Screening firewall*), aplikacijski pristupnici (engl. *Application gateway*) i kružni pristupnici (engl. *Circuit-level gateway*). Filtriranje paketa radi se na mrežnom sloju OSI modela. Postoje ulazni i izlazni filteri kojima se prema određenoj konfiguraciji određuje koje informacije se prosljeđuju unutar, a koje van mreže. Primjer gdje se koristi aplikacijski pristupnici je kod web pretraživača koji uspostavlja vezu s odredišnim poslužiteljem. Ovaj proces uspostavlja dvije veze. Prva veza je između klijenta i *proxy* poslužitelja, a druge između *proxy* poslužitelja i odredišta. *Proxy* poslužitelj uspostavlja vezu s odredištem iza vatrozida i djeluje u ime klijenta. Na taj način se skrivaju i štite računala na mreži iza vatrozida. Kod kružnog pristupnika provjerava se korisničko ime prije nego se uspostavi veza s usmjerivačem. Virtualni „krug“ je uspostavljen između korisnika i *proxy* poslužitelja. Internet zahtjevi prosljeđuju se krugom *proxy* poslužitelju koji nakon izmjene IP adrese prosljeđuje na Internet. Vanjskim korisnicima je vidljiva IP adresa *proxy* poslužitelja i na taj je način unutarnji sustav zaštićen [11][12].

Antispyware je program koji pretražuje sustav za *spyware* programima. Programi koje prate rad korisnika mogu zloupotrijebiti osobne i poslovne podatke, što dovodi do posljedica bez znanja korisnika. Najčešći izvor *spyware* programa su različiti dodaci na web preglednik koji se čine privlačni korisnicima [11].

Software za otkrivanje upada pregledava sve ulazne i izlazne aktivnosti na računalu, na vatrozidu te na sustavu radi uzoraka koje ukazuju na pokušaj upada. Primjer uzoraka može biti slijed poslanih ICMP paketa svakom portu u nizu što ukazuje na vjerojatnost analiziranja sustava. Najčešći tipovi IDS sustava su:

- Otkrivanje zloupotrebe i otkrivanje anomalije
- Pasivni sustavi i reaktivni sustavi
- Sustav temeljen na mreži i sustav temeljen na računalu.

IDS sustav, koji otkriva zloupotrebu slično kao pretraživači virusa, analiziraju bazu podataka o napadima. Sustav otkrivanja anomalija uključuje *software* za otkrivanje pokušaja upada i obavještavanje administratora. Način na koji se otkriva pokušaj upada je otkrivanjem anomalija. Anomalijama se smatra djelovanje koje ne odgovara normalnom pristupu korisnika. U pasivnom sustavu IDS otkriva potencijalno kršenje sigurnosti, bilježi informacije i signalizira upozorenje. U reaktivnom sustavu IDS reagira na sumnjivu aktivnost odjavom korisnika i reprogramiranjem vatrozida kako bi blokirao promet od sumnjivog zlonamjernog izvora. U sustavu temeljen na mreži (NIDS) analiziraju se pojedinačni paketi koji prolaze kroz mrežu. Sustav može otkriti pakete koji su namijenjeni da ostanu neotkriveni od sustava vatrozida. Sustav temeljen na računalu (HIDS) pregledava aktivnost svakog pojedinog računala [11][12].

Honey pot je sustav namijenjen odvraćanja pozornosti napadača od podataka koje se želi zaštititi, otkrivanje što napadača zanima i zadržavanje napadača kako bi se mogao pratiti. Način na koji se to postiže je postavljanjem ranjivog servera s lažnim podacima. Kako nitko od ovlaštenih korisnika ne pristupa lažnim podacima, ugrađen je software za praćenje i upozorenje ukoliko netko pristupi [12].

3. TESTIRANJE SIGURNOSNE RANJIVOSTI

Kada je u svijetu porasla svjesnost prijetnje koje izazivaju različiti računalni napadi, računalni i sigurnosni stručnjaci izumili su različite sigurnosne mjere. Jedna od najistaknutijih među takvim mjerama je proces koji se naziva penetracijsko testiranje. Penetracijsko testiranje je postupak kojim se kontroliranim napadima na računalni sustav bilježe slabe točke. Namjera napada je utvrditi učinkovitost sigurnosnih zaštitnih mjera u sustavu. Cilj penetracijskog testiranja je otkrivanje sigurnosne ranjivosti i njihovo rješavanje prije nego ih ugrozi bilo kakva vanjska prijetnja. Ključna područja koja se testiraju u bilo kakvom penetracijskom testiranju su *software, hardware*, računalna mreža i procesi. Penetracijsko testiranje se može obaviti dvjema metodama, a to su automatizirana i ručna metoda. Automatizirana metoda se odnosi na korištenje *software*-a koji se koristi u testiranju sustava i mreže. Automatiziranom metodom nije moguće otkriti sve ranjivosti pa je potrebno izvršiti ručnu metodu. Ova metoda je posebno značajna kod tvrtki. Ručna metoda obuhvaća ranjivosti u sustavu zbog ljudskih pogrešaka kao što su nedostatak standarda sigurnosti zaposlenika, neispravne povlastice zaposlenicima itd. Iako postoje različite vrste penetracijskih testiranja, dva najčešća pristupa su testiranje „crne kutije“ (engl. *Black box*) i testiranje „bijele kutije“ (engl. *White box*).

Prilikom testiranja crne kutije sigurnosni revizor procjenjuje mrežnu infrastrukturu i nije svjestan bilo kakvih internih tehnologija koje su implementirane. Upotrebom različitih metoda i prolaskom kroz organizirane testne faze potencijalno se mogu otkriti ranjivosti te ih iskoristiti. Važno je da ispitivač razumije, klasificira i određuje prioritet ranjivosti prema njihovoj razini rizika (niska, srednja ili visoka). Rizik se mjeri prema prijetnji koja ugrožava ranjivost. Idealni ispitivač bi odredio sve napadačke vektore koji bi mogli ugroziti cilj. Po završetku testiranja generira se izvješće koje sadrži sve potrebne informacije o stvarnom sigurnosnom stanju cilja [13].

Testiranje bijele kutije podrazumijeva da sigurnosni revizor treba biti svjestan svih internih tehnologija koje koristi ciljano okruženje. Ovim pristupom ispitivaču je omogućen pregled i kritički vrednovanje sigurnosnih propusta uz minimalne napore i najveću točnost. Vrijeme, trošak i razina znanja koja je potrebna za pronalazak i rješavanje sigurnosnih propusta je manja nego kod pristupa crnoj kutiji uz veću efikasnost [13].

3.1. Faze penetracijskog testiranja

Kali Linux je operacijski sustav koji dolazi s nizom sigurnosnih alata za penetracijsko testiranje. Izvođenje i prakticiranje alata bez odgovarajućeg slijeda koraka može dovesti do neuspjelog testiranja i rezultirati nezadovoljavajućim rezultatima. Postoji početna, medijalna i završna faza testiranja, a one uključuju sljedeće korake [13]:

- Područje primjene (engl. *Target scoping*)
- Prikupljanje informacija (engl. *Information gathering*)
- Otkrivanje ciljanog područja (engl. *Target discovery*)
- Enumeracija područja (engl. *Enumerating target*)
- Utvrđivanje ranjivosti (engl. *Vulnerability mapping*)
- Društveno inžinjerstvo (engl. *Social engineering*)
- Iskorištavanje cilja (engl. *Target exploitation*)
- Eskalacije privilegija (engl. *Privilege escalation*)
- Zadržavanje pristupa (engl. *Maintaining access*)
- Dokumentacija i izvješćivanje (engl. *Documentation and reporting*)

Bez obzira primjeni li se bilo koja kombinacija koraka s crnim ili bijelim kutijama, revizor odlučuje o strategiji penetracijskog testiranja na temelju poznavanja ciljane okoline.

Prije početka tehničke procjene sigurnosti važno je razumjeti zadano područje primjene ciljanog mrežnog okruženja. Opseg se može odrediti za jedinstveni entitet ili skup entiteta koji se daju revizoru. U prvom koraku područja primjene treba odrediti [13]:

- Što se testira?
- Na koji način testirati?
- Pod kojim uvjetima se testira?
- Što će ograničiti proces testiranja?
- Koliko dugo će trajati testiranje?
- Koji ciljevi su ispunjeni testiranjem?

Nakon faze određivanja područja primjene slijedi prikupljanje informacija. Revizor koristi brojne javno dostupne informacije kako bi naučio što više o svom cilju. Informacije se mogu preuzeti s izvora na internetu kao što su: forumi, bilteni, vijesti, članci, blogovi, društvene

mreže, komercijalne ili nekomercijalne web stranice itd. Osim prikupljanja informacija različitim tražilicama (Google, Yahoo!, MSN, Bing itd), revizor koristi alate u Kali Linuxu kako bi izdvojio mrežne informacije o ciljnom okruženju. Alati vrše prikupljanje informacija putem: DNS poslužitelja, praćenjem ruta, „Whois“ baze podataka, adrese e-pošte, telefonskih brojeva, osobnih podataka i korisničkih podataka. Prikupljanjem više informacija povećava se vjerojatnost provođenja uspješnog probijanja [13].

Faza otkrivanja ciljanog područja obuhvaća identifikaciju karakteristika mreže, operacijskog sustava i mrežne arhitekture. Na taj način revizor ima predodžbu povezanih uređaja i tehnologija. Samim time poznate su usluge koje se pokreću preko mreže.

Faza enumeracije područja pronalazi otvorene *port-ove* na ciljanim sustavima. Iako je ciljano područje zaštićeno vatrozidom i sustavom za otkrivanje upada (IDS), korištenjem brojnih tehnika skeniranja *port-ova* kao što su otvoreno, poluotvoreno i skriveno skeniranje mogu pomoći u otkrivanju vidljivosti *port-ova*. Budući da usluge koje su povezane s otvorenim *port-ovima* mogu biti korisne u svrhu daljnjeg istraživanja, ova faza služi kao temelj pronalaska ranjivosti na različitim mrežnim uređajima [13].

Nakon prikupljenih informacija iz prethodne faze slijedi faza utvrđivanja ranjivosti. U ovoj fazi na temelju prikupljenih podataka identificira se i analizira ranjivost na temelju otvorenih *port-ova* i usluga.

Ukoliko za revizora nema otvorenog načina za upad u ciljno područje, koriste se različiti načini prijevare. Neki od načina su zavaravanje korisnika u izvršavanje zlonamjernog koda koji bi trebao omogućiti revizoru stražnji (engl. *Backdoor*) pristup ciljanog područja. Društveno inženjerstvo dolazi u različitim oblicima. Takvi oblici mogu biti bilo koji način kojima se napadač predstavlja kao ovlaštena osoba i nastoji otkriti podatke o računu, e-pošti itd. Za uspješnu penetracijsko testiranje potrebno je razumjeti ljudsku psihologiju i državne zakone s obzirom na društveno inženjerstvo prije bilo kakvog postupka zavaravanja [13].

Nakon ispitivanja otkrivenih ranjivosti moguće je prodrijeti u ciljni sustav pomoću nekoliko vrsta zlonamjernih kodova (engl. *Exploits*). Ponekad su potrebna dodatna istraživanja i izmjene postojećih kodova kako bi se preuzela kontrola nad ciljnim sustavom.

Uspješnom penetracijom revizor djeluje unutar sustava, ovisno o privilegiji pristupa. Privilegije mogu eskalirati pomoću zlonamjernog koda. Revizor je u mogućnosti pokrenuti daljnje napade

na lokalni mrežni sustav, analizirati promet, prikupljati lozinke različitih usluga. Svrha faze eskalacije povlastica je postići što veću razinu pristupa sustavu.

Ponekad se od revizora traži zadržavanje pristupa sustavu na određeno vremensko razdoblje. Korištenjem različitih metoda tunela koji koriste protokoli uspostavlja se stražnji pristup kojim se zadržava revizor u ciljnom sustavu. Faza zadržavanja pristupa pruža jasan uvid kako napadač može održati svoju prisutnost bez sumnjivih aktivnosti.

Penetracijsko testiranje završava dokumentacijom, izvještavanjem i predstavljanjem otkrivenih, provjerenih i iskorištenih ranjivosti kako bi se sigurnosni propusti mogli popraviti. Izvješća mogu služiti kao usporedba integriteta ciljanog sustava prije i poslije procesa penetracije [13].

3.2. Kali Linux

Operacijski sustav je sastavni dio svakog računalnog sustava. Moglo bi se reći da je operacijski sustav skup programskih proširenja računalnog sklopovlja koji potpomaže izvođenje raznovrsnih operacija potrebnih za izvođenje korisničkih programa. Dva su osnovna zadatka, a to su [10]:

- Omogućivanje što prikladnije uporabe računala,
- Omogućivanje što djelotvornijeg iskorištavanja svih sklopovskih i programskih komponenti računalnih sustava.

Poput Windows XP, Windows 7, Windows 8, Mac OS X, Linux je operacijski sustav. Operacijski sustav Linux se sastoji od [14]:

- Pokretač operacijskog sustava (engl. *Bootloader*): *software* koji upravlja procesom pokretanja sustava.
- Jezgra (engl. *Kernel*): upravlja CPU (engl. *Central Processing Unit*), memorijom i perifernim uređajima.
- *Daemons*: pozadinske usluge koje se pokreću tijekom pokretanja i prijave na radnu površinu (ispis, zvuk itd).
- *The Shell*: omogućuje rad na računalu putem naredbi upisanih u tekstualno sučelje.

- Grafički poslužitelj (engl. *Graphical Server*): podsustav koji prikazuje grafiku na monitoru. Obično se naziva X poslužitelj ili samo „X“.
- Radna površina (engl. *Desktop Environment*): radno okruženje s kojom korisnici stupaju u interakciju. Svako radno okruženje uključuje ugrađene aplikacije kao što su: upravitelji datoteka, alati za konfiguraciju, web preglednici, igre itd. Neka radna okruženja su: Unity, GNOME, Cinnamon, Enlightenment, KDE, XFCE itd.
- Aplikacije (engl. *Applications*): radna okružena nude niz aplikacija. Baš kao Windows i Mac, Linux nudi mnoštvo visoko kvalitetnih *software*-a koji se lako mogu pronaći i instalirati.

Linux se distribuira besplatno, a to znači da je moguće:

- Korištenje programa u bilo koju svrhu.
- Sloboda proučavanja i mogućnost izmjene kako bi dobili željenu svrhu.
- Sloboda redistribucije kopija.
- Sloboda distribucije izmijenjenih kopija.

Linux ima niz različitih verzija koje odgovaraju gotovo svakoj vrsti korisnika. Verzije se nazivaju distribucije. Gotovo svaka distribucija je besplatna. U ovom radu biti će korištena Kali Linux distribucija o kojoj će biti u idućem potpoglavlju. Poznate Linux distribucije su: Elementary OS, Fedora, Linux Mint, Ubuntu, CentOS, Debian, Manjaro, openSUSE, Arch Linux, CoreOS, Kali Linux, Puppy Linux itd.

Kali Linux (Kali) je Linux distribucijski sustav koji je razvijen s naglaskom na testiranje sigurnosne ranjivosti, penetracijskih testiranja i sigurnosne analize različitih mreža. Kali je bio poznat kao BackTrack koji je nastao spajanjem tri različite Linux distribucije: IWHAX, WHOPPIX i Auditor. Kali se temelji na Debian Linux distribuciji. Ima više od 300 aplikacija za penetracijska testiranja. Svi Kali *software* paketi su GPG potpisani od razvojnih programera. Korisnici mogu sebi prilagoditi Kali kako bi odgovarao njihovim potrebama. Kali podržava ARM sustave. Kali sadrži niz alata koji se mogu koristiti tijekom procesa testiranja penetracije. Alati za testiranje penetracije u Kali Linux mogu se svrstati u sljedeće kategorije [15]:

- Prikupljanje informacija: ova kategorija sadrži nekoliko alata koji se mogu koristiti za prikupljanje informacija o DNS-u, IDS/IPS-u, mrežno skeniranje, operacijskim sustavima, usmjeravanju, SSL-u, SMB-u, VPN-u, VoIP, SNMP, adrese e-pošte.

- Procjena ranjivosti: u ovoj kategoriji nalaze se alati za skeniranje ranjivosti, za procjenu Cisco mreže i alati za procjenu ranjivosti nekoliko poslužitelja baze podataka. Također ova kategorija sadrži alate za provjeru ugroženosti *software*-a.
- Web aplikacije: ova kategorija sadrži alate vezane uz web aplikacije kao što je skener sustava za upravljanje sadržajem, eksploataciju baze podataka, ugroženost web aplikacija.
- Napad na lozinke: ova kategorija sadrži alate za izvođenje napada na lozinke.
- Alati za eksploataciju: ova kategorija sadrži alate koji se mogu koristiti za otkrivanje ranjivosti koje se nalaze u ciljanom okruženju.
- Detektiranje i lažiranje: sadrži alate za detekciju web prometa. Uključuje alate za lažiranje kao što su Ettercap i Yersinia.
- Održavanje pristupa: Alati u ovoj kategoriji omogućuju održavanje pristupa ciljanom okruženju. Također mogu se pronaći alati za tuneliranje.
- Alati za izvješćivanje: alati koji pomažu dokumentirati proces i rezultate penetracijskih testiranja
- Sustavne usluge: kategorija sadrži nekoliko usluga koje mogu biti korisne tijekom zadatka penetracijskog testiranja, kao što su Apache usluga, MySQL usluga, SSH usluga i Metasploit usluga.

Osim što sadrži alate koji se koriste za penetracijsko testiranje, Kali Linux također ima nekoliko alata koji služe za:

- Napad na bežične mreže: ova kategorija uključuje alate za napad na Bluetooth, RFID/NFC i bežične uređaje.
- Obrnuto inžinjerstvo: uključuje alate za ispravljanje (engl. *Debug*) programa i rastavljanje izvršnih datoteka.
- Ispitivanje otpornosti: sadrži alate koji ispituju otpornost mreže, weba i VoIP okruženja.
- Hakiranje *hardware*-a: alati koji se koriste želi li se raditi s Android i Arduino aplikacijama.
- Forenzika: u ovoj kategoriju alati koji mogu koristiti za digitalnu forenziku, stjecanje stanja i analiza tvrdog diska itd.

3.3. Primjena Kali Linux alata za otkrivanje sigurnosnih ranjivosti

Za otkrivanje sigurnosnih ranjivosti koristi se virtualni laboratorij. Virtualni laboratorij se postavlja u programu *Oracle VM Virtual Box*. U virtualnom laboratoriju se nalaze tri uređaja. Prvi uređaj radi na Kali Linux operacijskom sustavu i vrši testiranje ostalih uređaja. IP adresa Kali Linux uređaja je 192.168.5.134. Drugi uređaj radi na Windows XP operacijskom sustavu s IP adresom 192.168.5.135. Treći uređaj je Metasploitable2 Linux uređaj s IP adresom 192.168.5.133. O postupku kako namjestiti virtualni laboratorij neće biti govora. Alati koji se koriste za izviđanje su *theHarvester* i *DNSRecon*. Alati koji se koriste za otkrivanje su: *Nmap*, *Scapy*, *Dmitry*, *Netcat* i *Masscan*. Za otkrivanje i analizu sigurnosne ranjivosti koristi se *OpenVAS*.

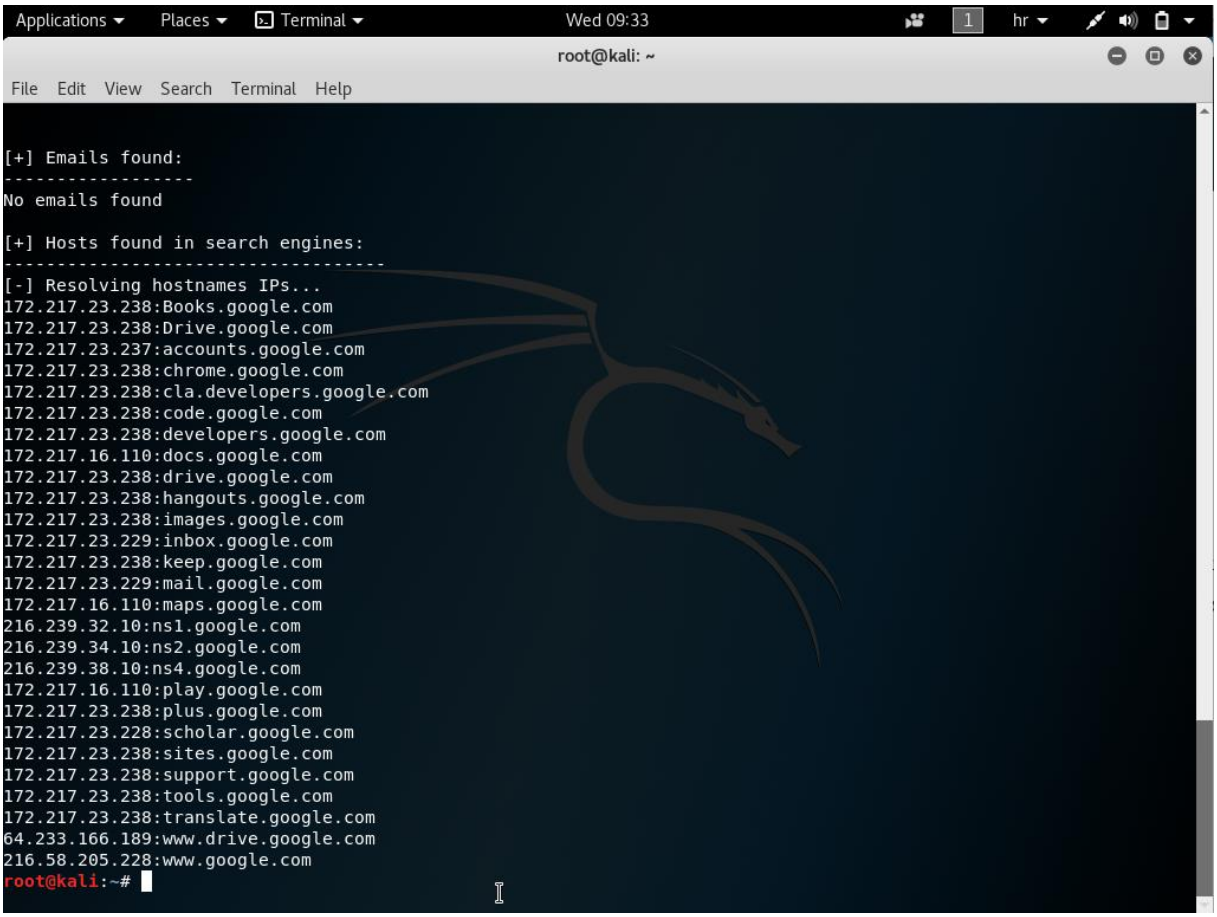
3.3.1. theHarvester

TheHarvester je program za prikupljanje adresa e-pošte, poddomena, domaćina, imena zaposlenika, otvorenih portova iz različitih javnih izvora kao što je tražilica. Alat je namijenjen za pomoć penetracijskim ispitivačima u ranoj fazi penetracijskog testiranja kako bi saznao o tragu (engl. *Footprint*) na internetu ispitivanog klijenta. Također koristi kako bi se saznalo što napadač može vidjeti o klijentu [15].

Za primjer potreban je uređaj s Kali Linux operacijskim sustavom. Pokretanje alata u Kali Linuxu se vrši otvaranjem komandnog prozora i upisivanjem *theharvester*. Pri pokretanju alata prikazana je lista uputa i primjera za korištenje (Slika 3.1.).

Sl. 3.1. *Pokretanje theHarvester*

Kao primjer korištenja *theHarvester*, traže se adrese e-pošte s *google.com* koristeći Google tražilicu. Upisana je naredba *theharvester -d google.com -l 1000 -b google*. Upisivanjem *-d* označava se domena koja se pretražuje, *-l* ograničava broj rezultata, a *-b* označava izvor koji se koristi. Moguće je koristiti *-f* kako bi se rezultati pretrage spremili u datoteku.

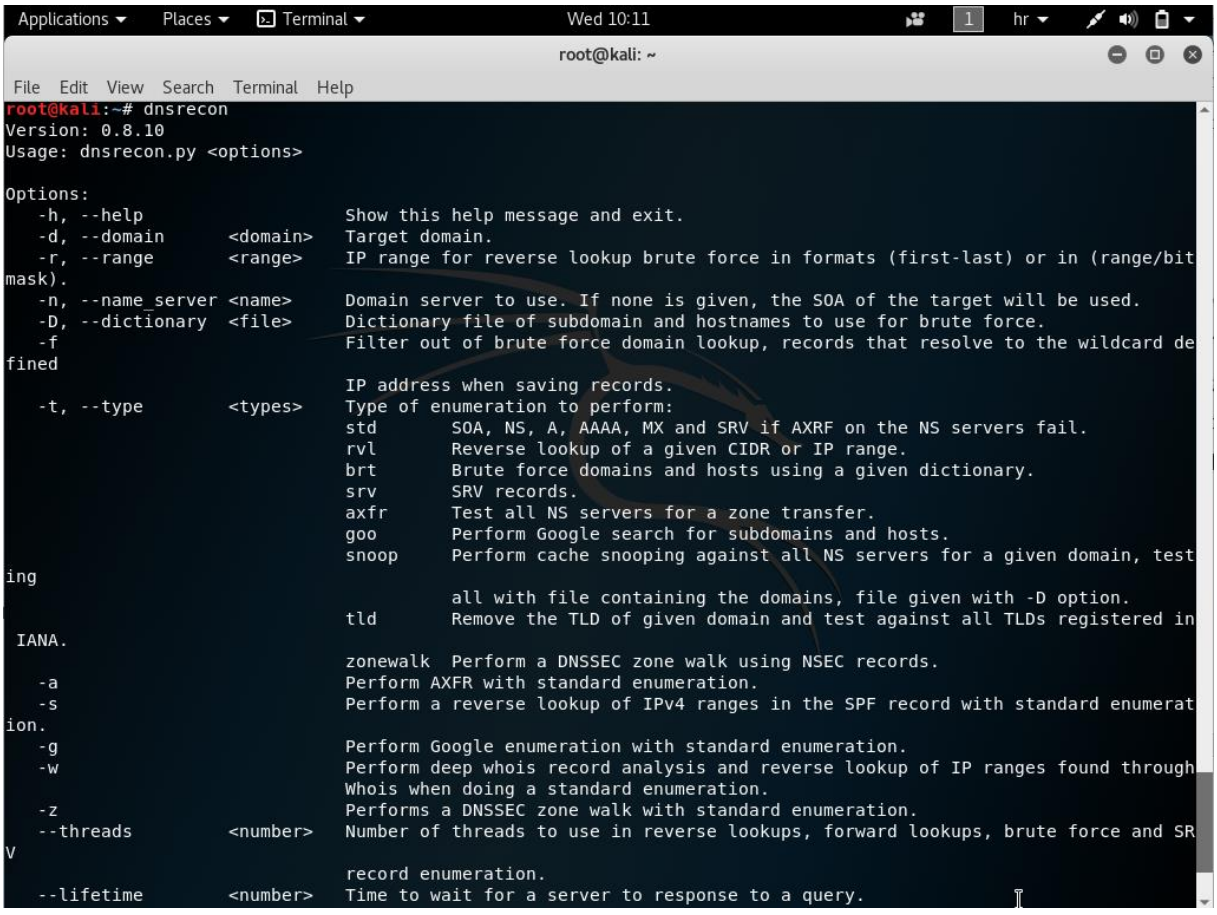


Sl. 3.2. *Primjer korištenja navedene naredbe theHarvester*

Izvršavanjem naredbi nisu se mogle pronaći adrese, ali zato su pronađeni *host*-ovi s IP adresama (Slika 3.2). U prethodnoj naredbi moguće je upisati *all* kao izvor pretrage, čime se vrši pretraga iz svih izvora.

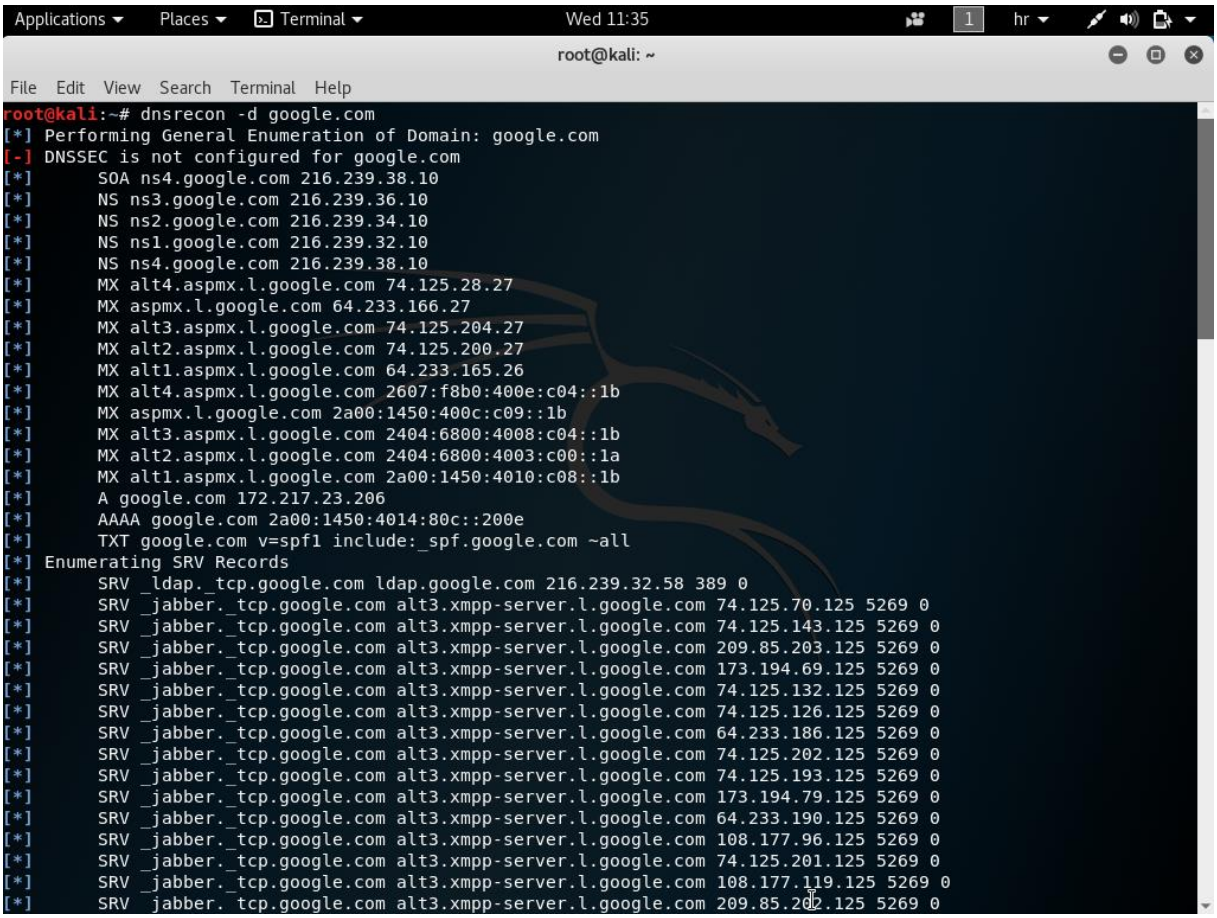
3.3.2. DNSRecon

Postoje programi za DNS izviđanja što znači da se provodi identificiranje DNS poslužitelja ciljanog klijenta i DNS zapisa koji se nalazi u njima. Jedan od takvih programa je *DNSRecon*. *DNSRecon* može enumerirati DNS zapise, obavljati prijenos zona (engl. *Zone transfer*), reverznu pretragu (engl. *Reverse lookups*) i primijeniti grubu silu (engl. *Bruteforce)* poddomena među ostalim funkcijama [15]. U primjeru korišten je uređaj s Kali Linux operacijskim sustavom. Pokretanje alata u Kali Linuxu se vrši otvaranjem komandnog prozora i upisivanjem *dnsrecon* (Slika 3.3).



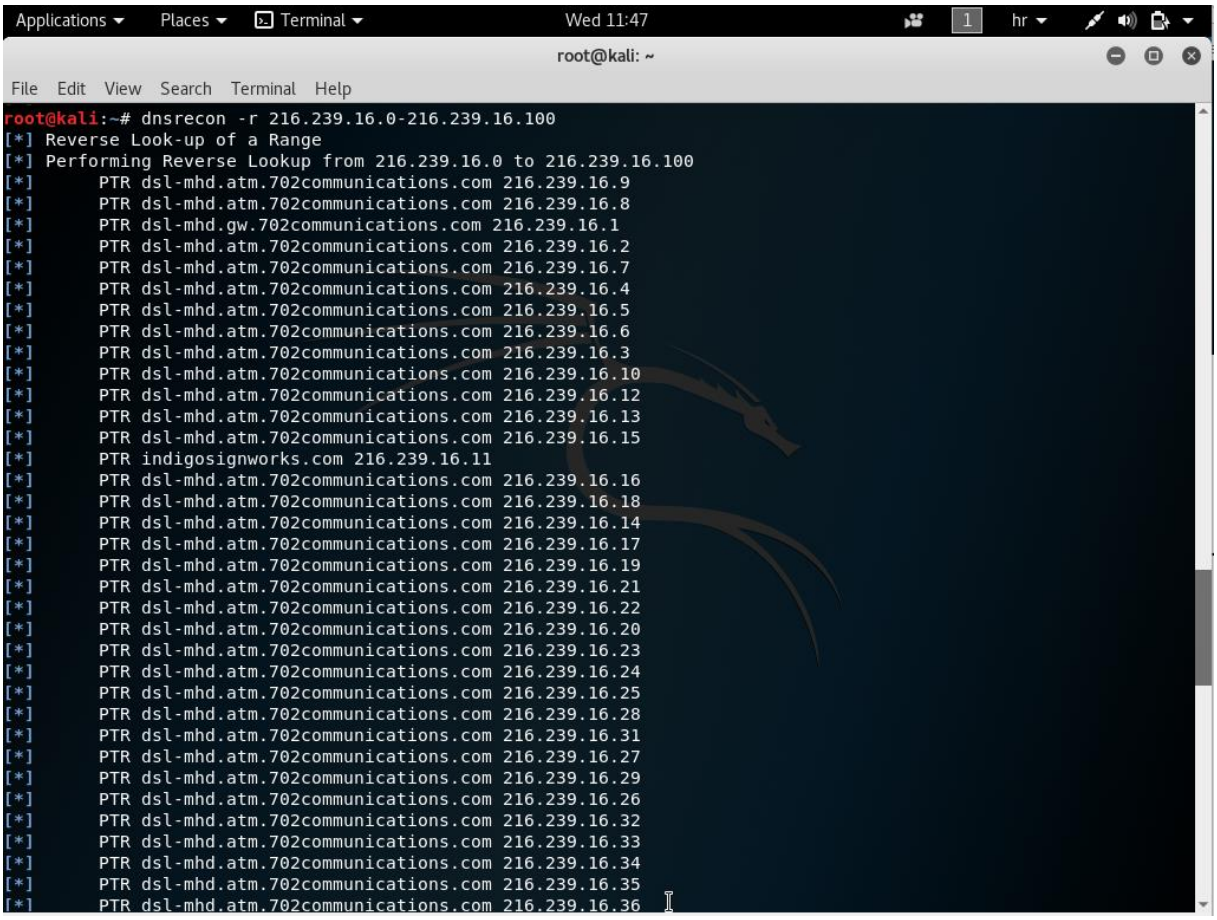
Sl. 3.3. *Pokretanje DNSRecon*

Pokrene li se *DNSRecon* bez unosa zastavice o vrsti (*-t*) izvršit će se standardna enumeracija. Standardna enumeracija pruža SOA, NS, A, AAAA, MX i SRV zapise. Da bi se proslijedila domena koja se želi skenirati koristi se *-d* zastavica. Kako bi se pokrenula standardna enumeracija na ciljanu domenu (*google.com*) unosi se naredba *dnsrecon -d google.com* (Slika 3.4).



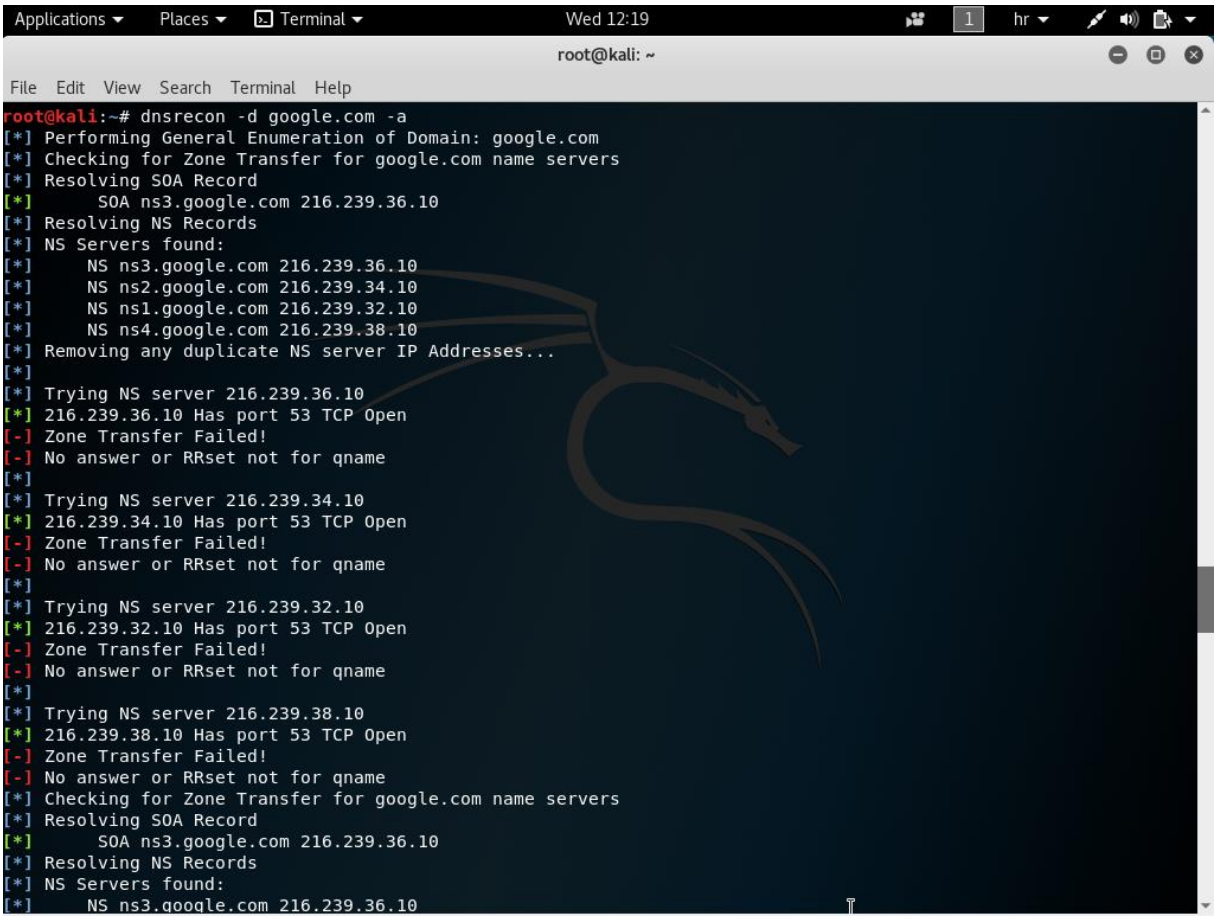
Sl. 3.4. *DNSRecon standardna enumeracija*

DNSRecon može pokrenuti reverznu pretragu unosom raspona IP adresa. Naredba se vrši korištenjem *-r* zastavice i rasponom IP adresa: *dnsrecon -r 216.239.32.0-216.239.32.100* (Slika 3.5).



Sl. 3.5. *DNSRecon reverzna pretraga*

DNS prijenos zona je proces u kojem DNS server predaje kopiju baze podataka (zonu) sekundarnom DNS serveru što može uzrokovati otkrivanje informacije o infrastrukturi neke organizacije. DNS poslužitelji su konfigurirani da ne dopuštaju prijenos zone. Naredba za prijenos zone: *dnsrecon -d google.com -a*



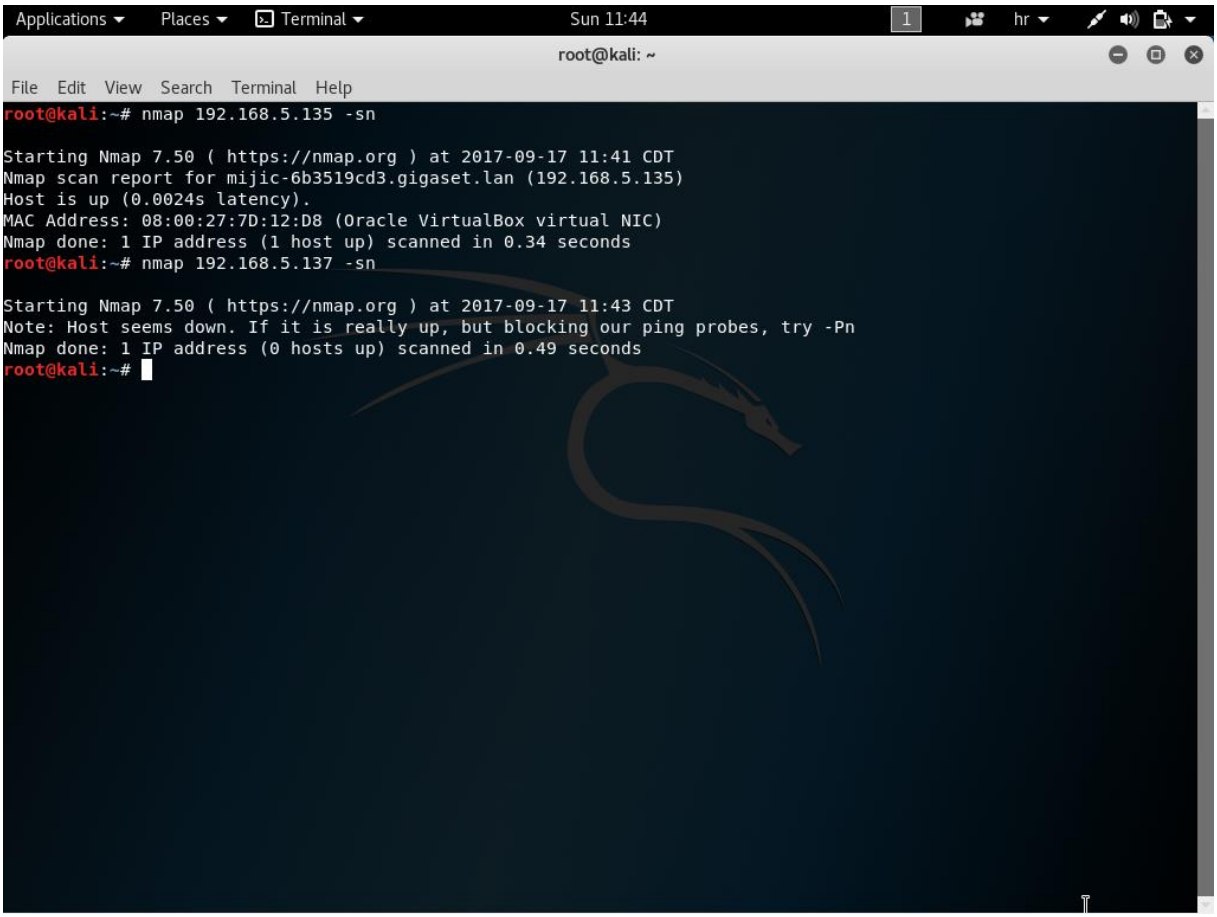
Sl. 3.6. *DNSRecon prijenos zona*

U primjeru pokušaj prijenosa zona nije uspio. Uvijek postoji vjerojatnost nailaska na DNS poslužitelj koji nije dobro konfiguriran kako bi spriječio prijenos zona.

3.3.3. Nmap

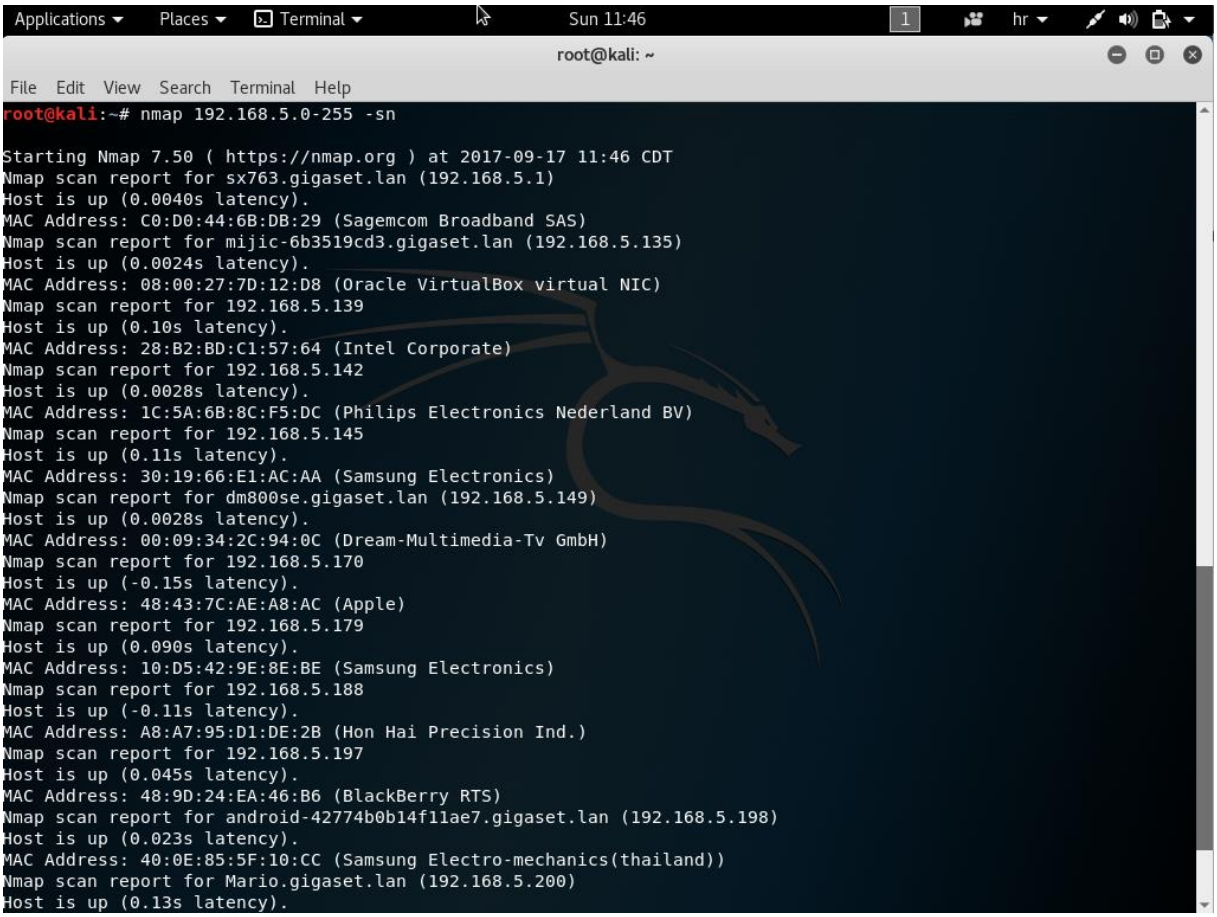
Nmap (engl. *Network mapper*) je alat za otkrivanje mreže i sigurnosnu reviziju. Program koristi IP pakete kako bi utvrdio koji su domaćini dostupni na mreži, koje usluge nude (aplikacija i verzija), na kojem operacijskom sustavu rade, koji se filtri paketa i vatrozid koristi itd. Osmišljen je za brzo skeniranje velikih mreža. Dobro radi za skeniranje jednog domaćina. *Nmap* radi na svim većim operativnim sustavima, a službeni binarni paketi dostupni su za Linux, Windows i Mac OS X. Osim klasičnog *Nmap* koji se vrši naredbama iz komandnog prozora, *Nmap* paket uključuje napredni GUI (engl. *Graphic user interface*) i preglednik rezultata (*Zenmap*), fleksibilni alat za prijenos podataka, preusmjeravanje i ispravljanje pogrešaka (*Ncat*), uslužni program za usporedbu rezultata skeniranja (*Ndiff*) i alata za analizu i generiranje paketa (*Nping*) [15].

Testiranjem *Nmap*-a korišteni su uređaji s Kali Linux i Windows XP operacijskim sustavom. U primjeru korištenja *Nmap* alata biti će prikazano otkrivanje domaćina pomoću ARP zahtjeva, otkrivanje operacijskog sustava i vatrozida. Opcija kojom se pokreće ARP zahtjev je *-sn* koja označava *ping scan.*



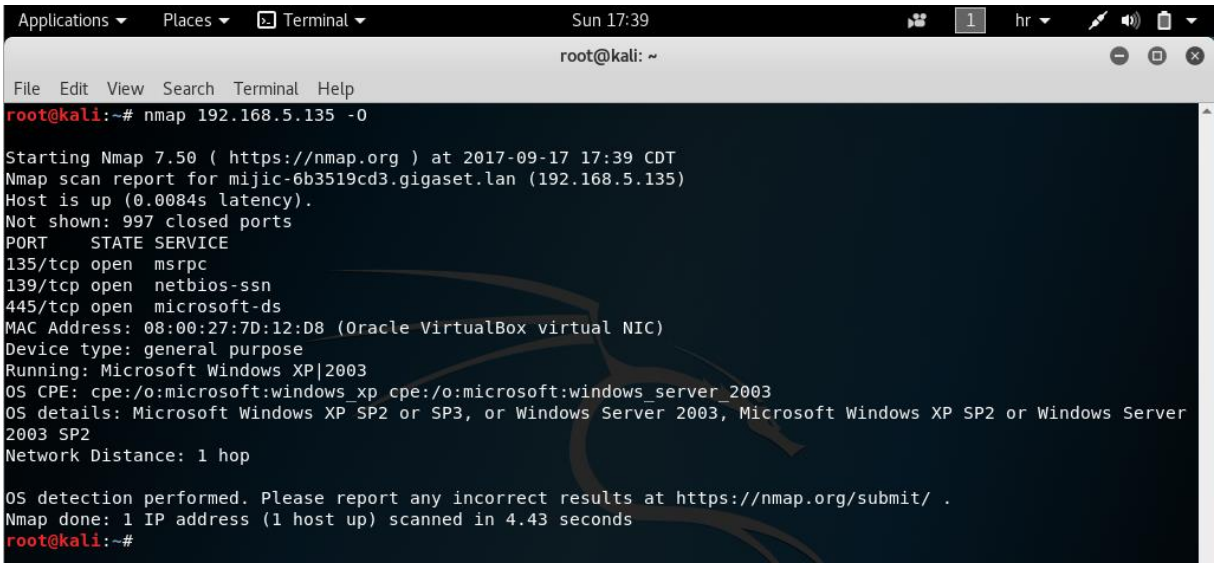
Sl. 3.7. *Nmap otkrivanje domaćina na drugom sloju OSI modela*

Naredba šalje ARP zahtjev upisanoj adresi Windows XP uređaja. Ukoliko je zahtjev uspješan, kao odgovor biti će poznata MAC adresa. Ukoliko je zahtjev neuspješan, ispisat će se poruka da domaćin nije aktivan (Slika 3.7). *Nmap* alatom je moguće pretražiti podmrežu unosom intervala IP adresa (Slika 3.8).



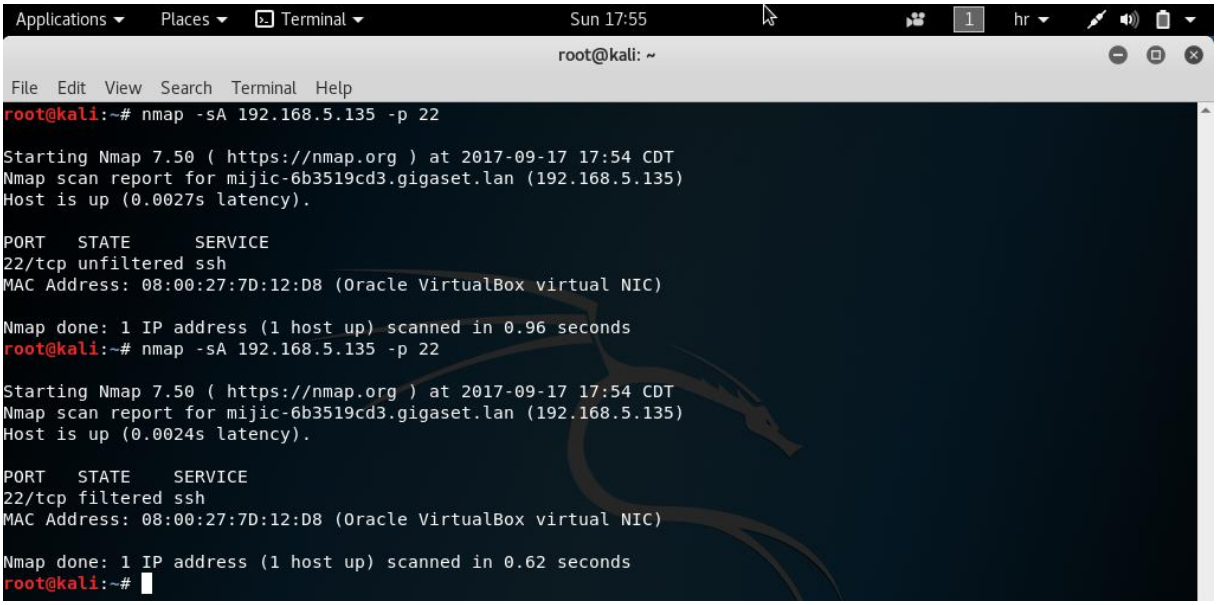
Sl. 3.8. *Nmap otkrivanje domaćina u podmreži na drugom sloju OSI modela*

Nmap može koristiti *-O* opciju za otkrivanje operacijskog sustava domaćina koji se skenira. U primjeru je skeniran i otkriven Windows XP operacijski sustav (Slika 3.9).



Sl. 3.9. *Nmap otkrivanje operacijskog sustava domaćina*

Kako bi se provjerilo da li postoji vatrozid kod domaćina koristi se -*sA* opcija (Slika 3.10). U primjeru korišten je Windows XP operacijski sustav u slučaju kada je uključen i isključen vatrozid.



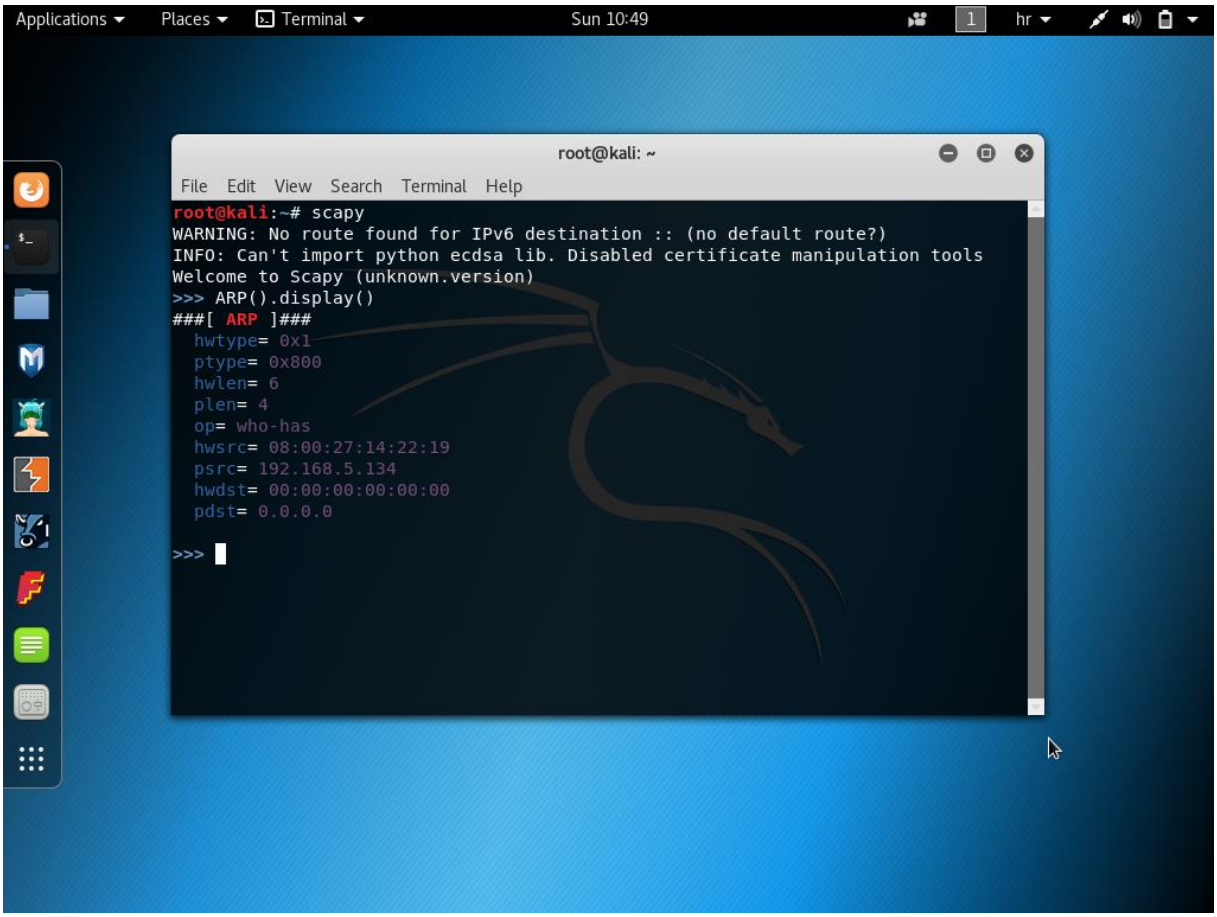
Sl. 3.10. *Nmap provjera vatrozida*

U odgovoru na prvu provjeru TCP *port* 22 (SSH) nije filtriran što znači da nema vatrozida. U drugoj provjeri ima vatrozid je uključen što dokazuje da je *port* 22 filtriran.

3.3.4. Scapy

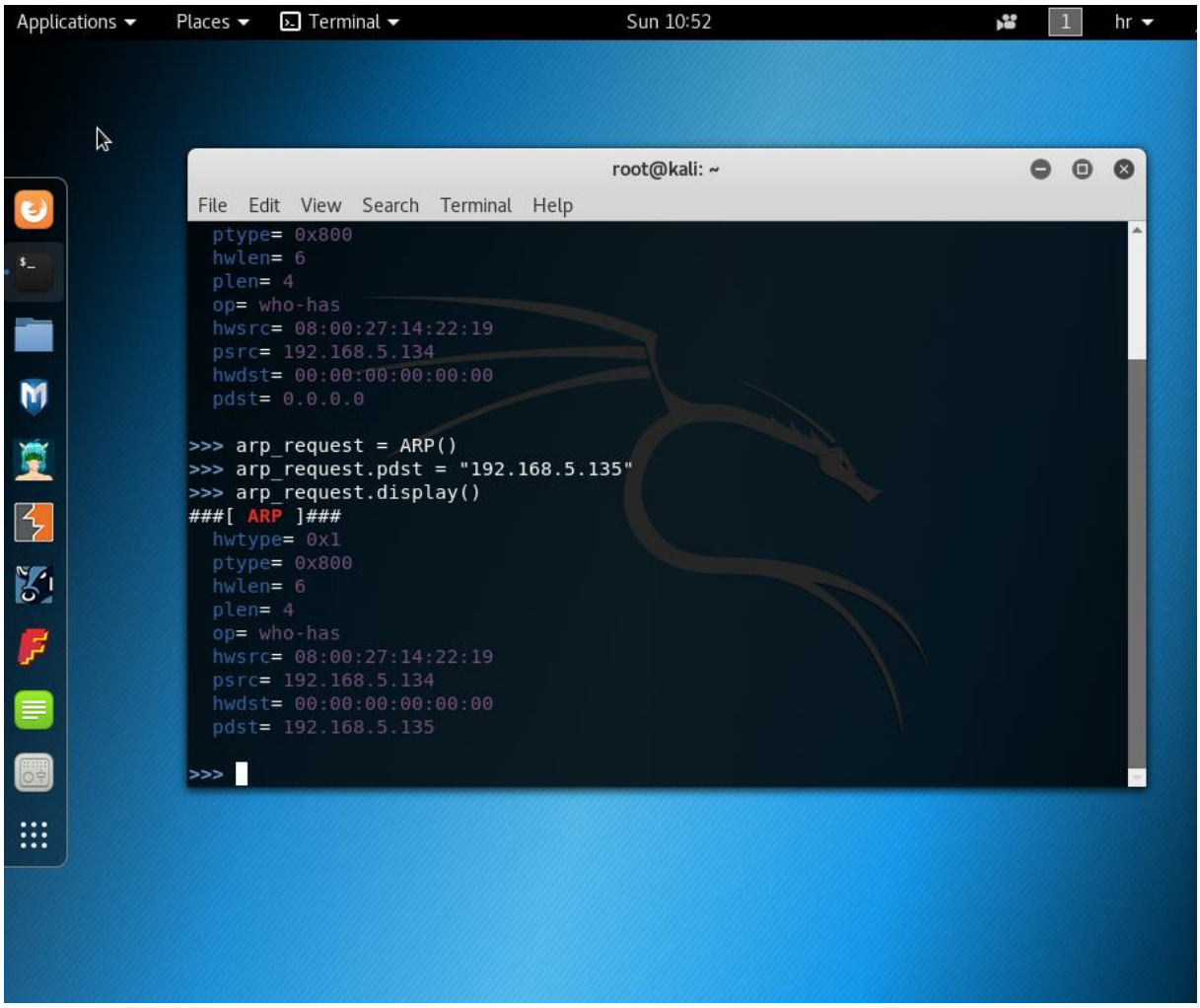
Scapy je alat za snimanje, analizu, manipulaciju i stvaranje mrežnog prometa sukladan protokolu. *Scapy* je također biblioteka koja se koristi u *Python*-u i time nudi mogućnost stvaranja visoko učinkovitih skripti za manipulaciju i upravljanjem mrežnim prometom. U primjeru pokazano je kako koristiti *Scapy* za otkrivanje domaćina pomoću protokola drugog, trećeg i četvrtog sloja referentnog OSI modela [15].

U primjeru korišteni su Kali Linux i Windows XP uređaji. Za otkrivanje domaćina protokolom drugog sloja OSI modela koristi se ARP zahtjev. Kako bi se pokrenuo program u komandnom prozoru je potrebno upisati *scapy*. Upotrebom funkcije *display()* prikazat će se postavke ARP objekta (Slika 3.11).



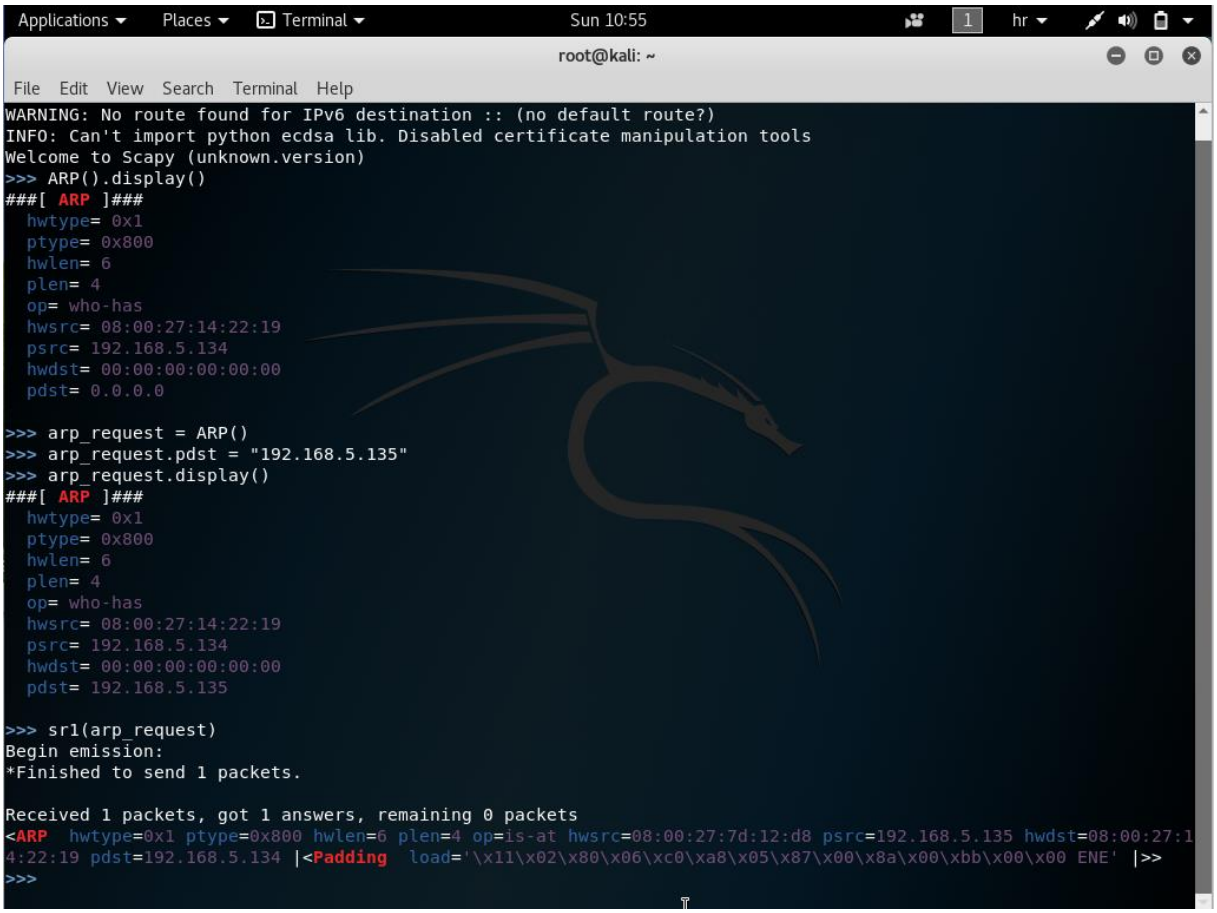
Sl. 3.11. *Scapy ARP objekt*

Izvorišna IP i MAC adresa ARP objekta su podešeni adresama uređaja s kojeg se pokreće program. U ARP objekt je potrebno upisati odredišnu IP adresu kako bi se otkrila odredišna MAC adresa. Kako bi podesili IP adresu potrebno je stvoriti ARP objekt i postaviti varijable. ARP objektu je dodijeljeno ime *arp_request*. Postupak postavljanja odredišne IP adrese i prikaz stvorenog ARP objekta prikazan je na slici 3.12.



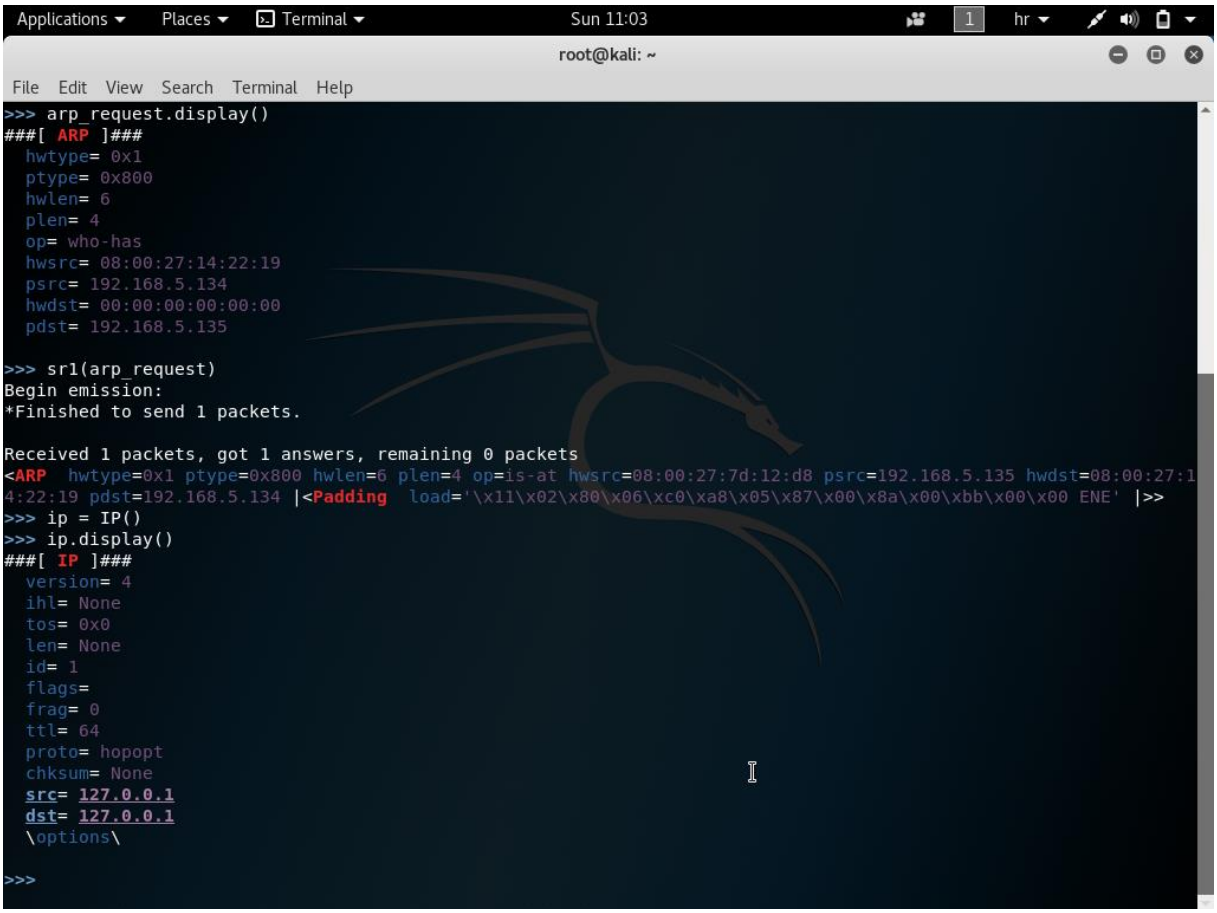
Sl. 3.12. *arp_request objekt*

Kako bi se poslao ARP objekt i dobila povratna informacija koristi se *sr1()* funkcija (Slika 3.13). Iz povratne informacije poznata je odredišna MAC adresa: 08:00:27:14:22:19



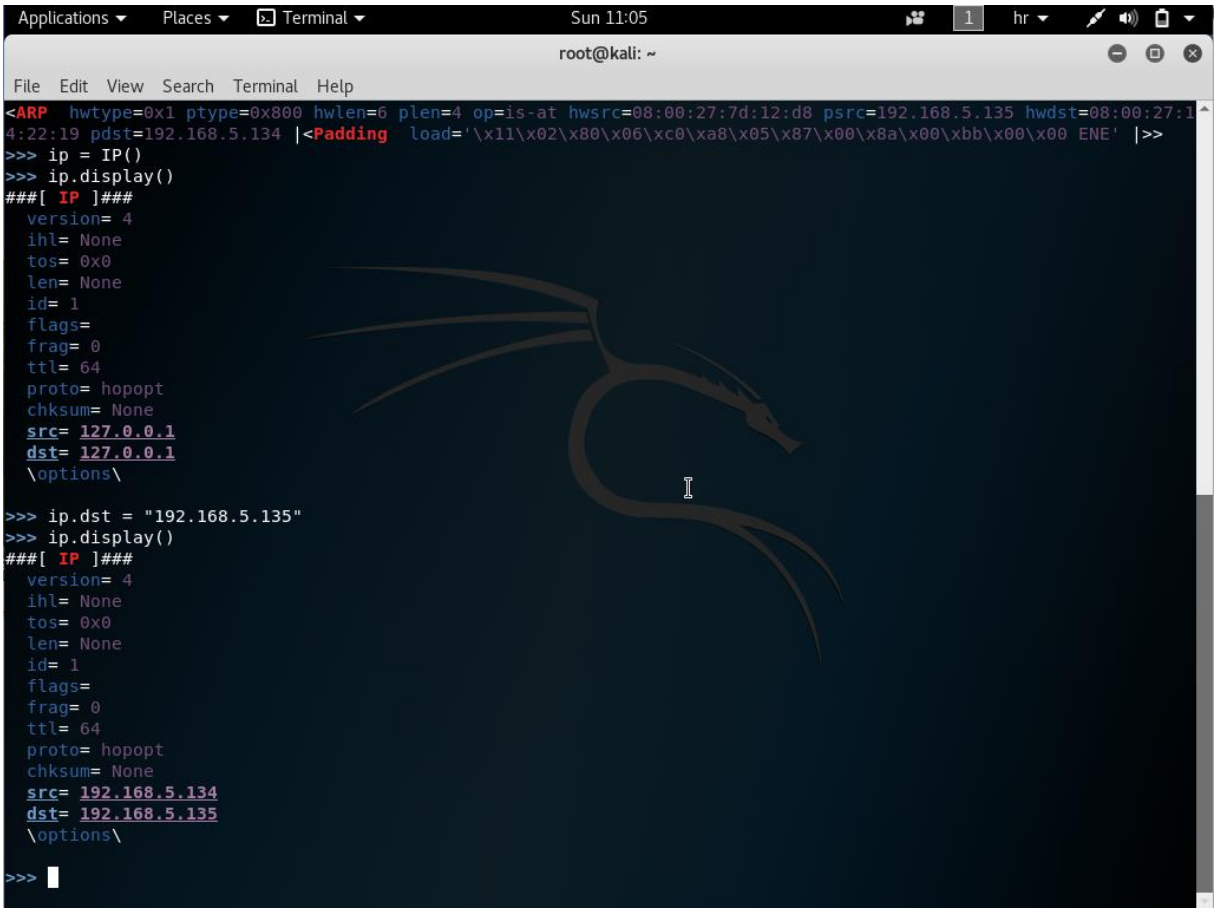
Sl. 3.13. *Slanje ARP objekta pomoću sr1() funkcije*

U *Scapy*-u je moguće pomoću *Python* skripte podesiti interval IP adresa koje se pretražuju. U ovom radu neće biti objašnjen rad s *Python* skriptama. Za otkrivanje domaćina protokolom trećeg sloja OSI modela koristi se ICMP zahtjevi. Nakon što se pokrene *scapy* potrebno je stvoriti IP objekt (Slika 3.14).



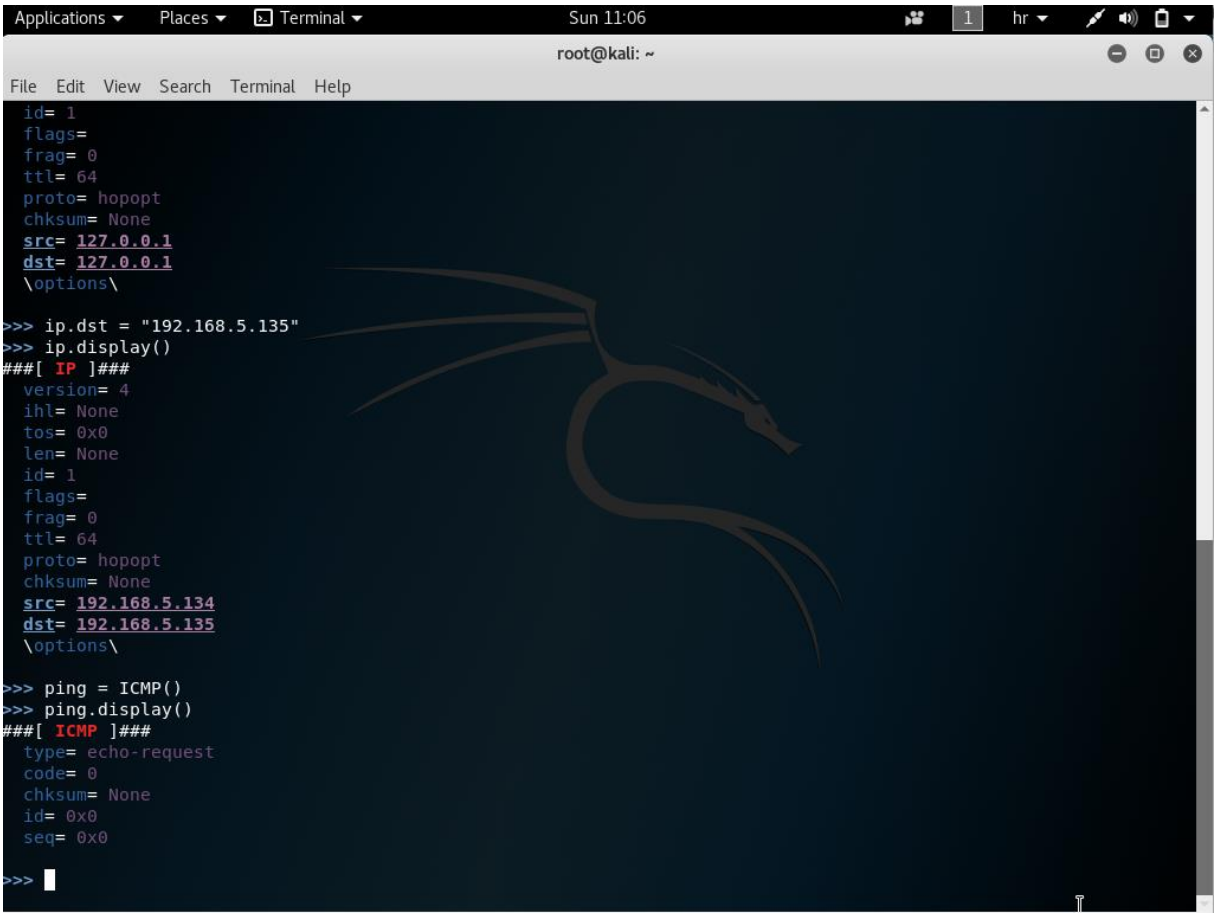
Sl. 3.14. *Stvaranje IP objekta*

Na isti način kao kod ARP objekta potrebno je podesiti odredišnu IP adresu (Slika 3.15).



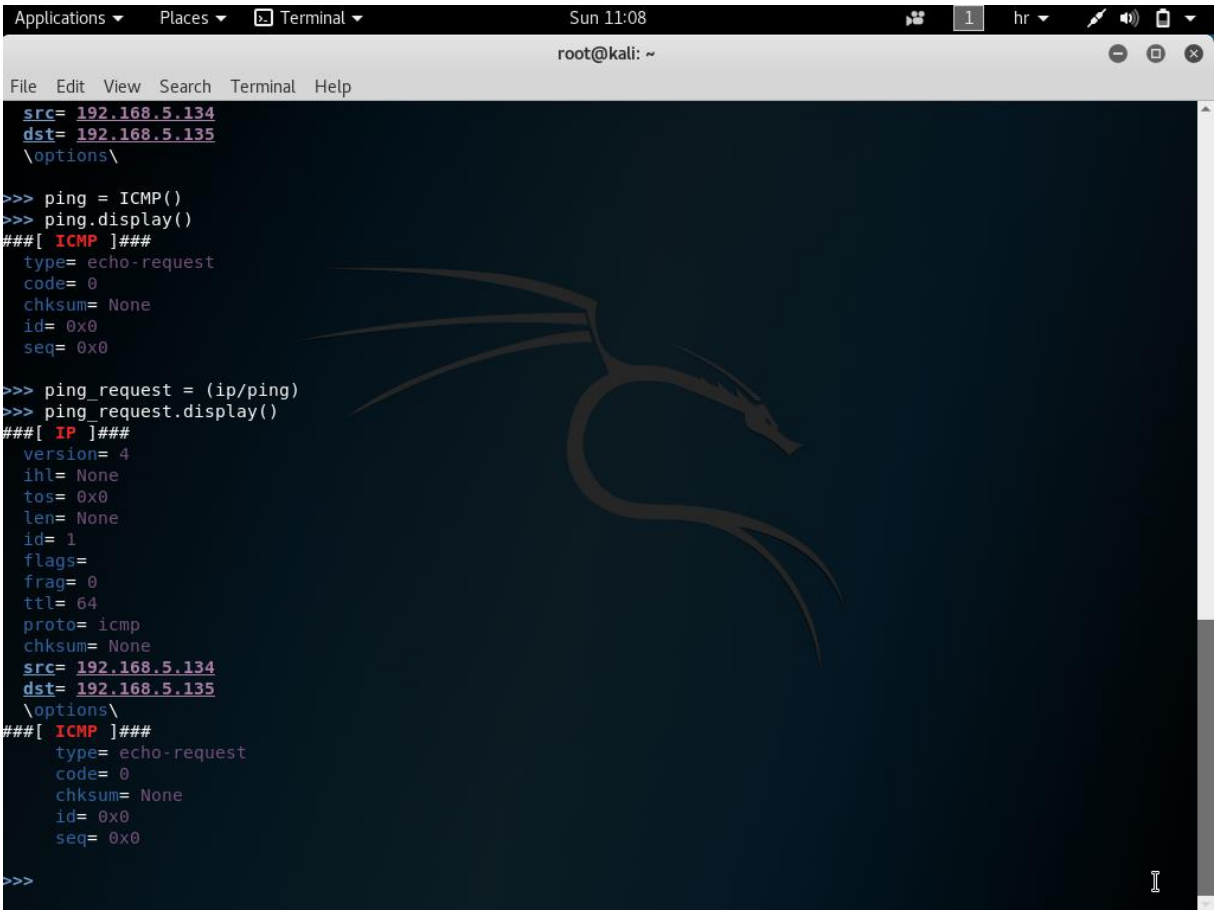
Sl. 3.15. *Podešavanje IP objekta*

Nakon što je podešen IP objekt potrebno je stvoriti ICMP objekt koji se zajedno šalje s IP objektom (Slika 3.16).



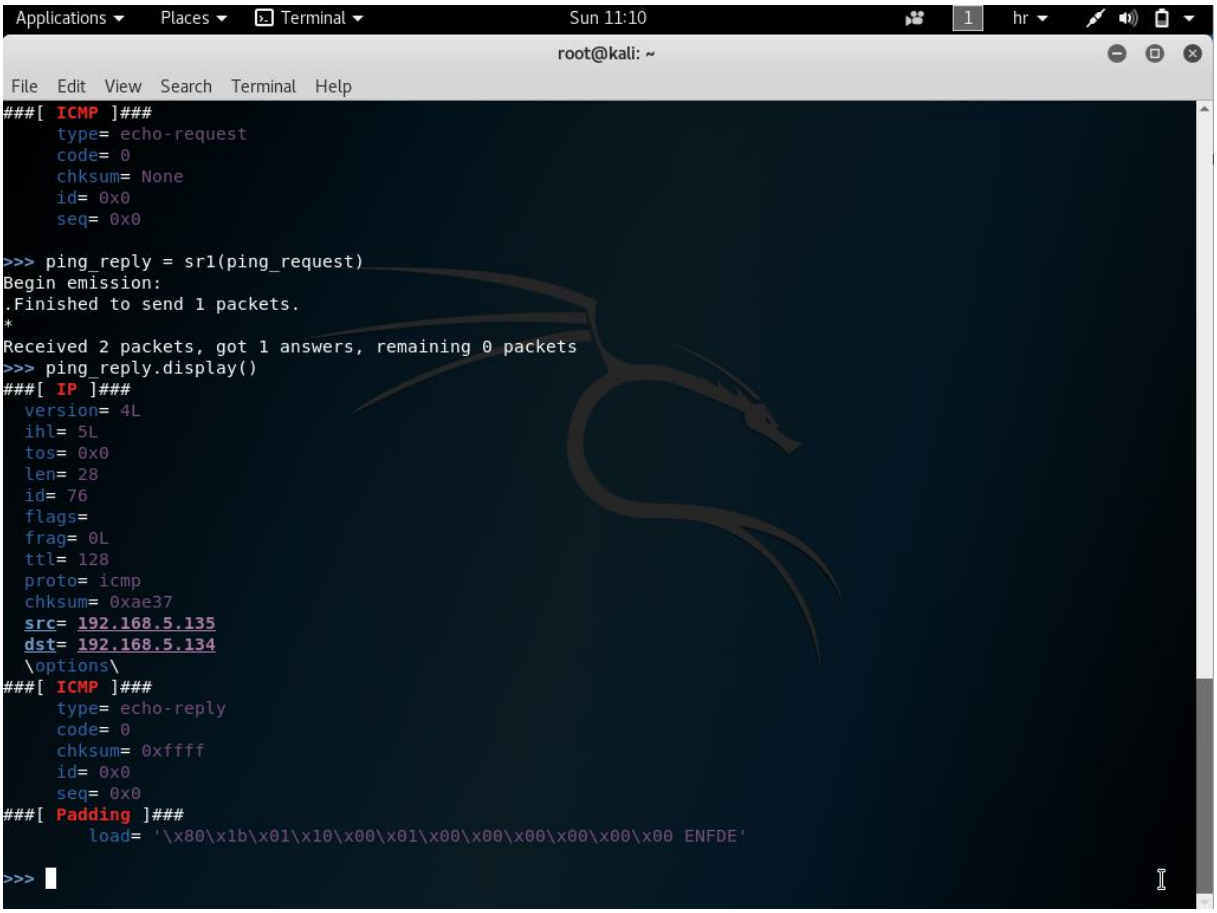
Sl. 3.16. *Stvaranje ICMP objekta*

Kako bi se izvršio ICMP zahtjev, dovoljne su početne postavke. Za ICMP zahtjev potrebno je stvoriti *ping_request* objekt koji sadrži prethodno stvorene IP i ICMP objekte (Slika 3.17).



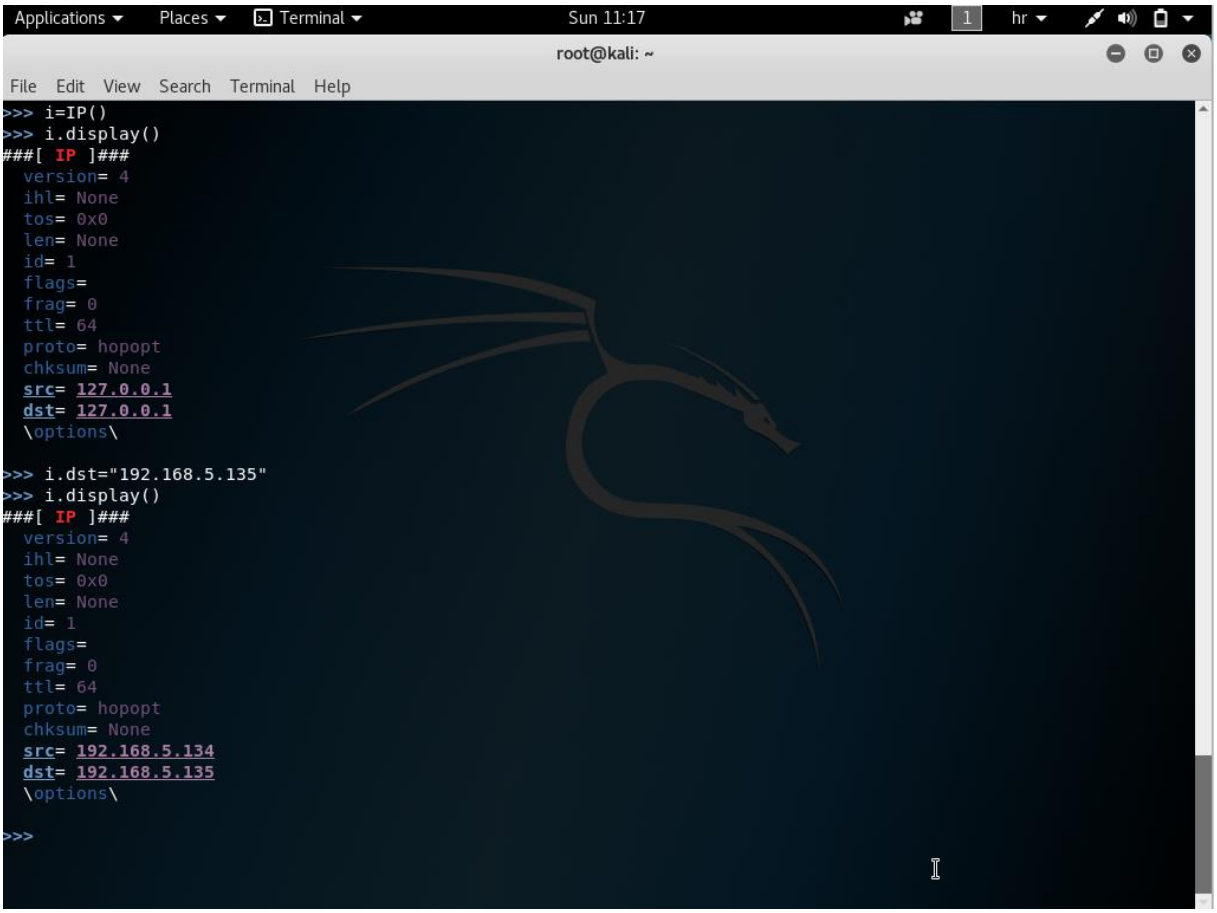
Sl. 3.17. *Stvaranje ping_request objekta*

Za slanje *ping_request* objekta koristi se *sr1()* funkcija koja je dodijeljena *ping_reply* varijabli. Nakon što se objekt pošalje, pomoću *display()* funkcije je moguće prikazati sadržaj odgovora (Slika 3.18).



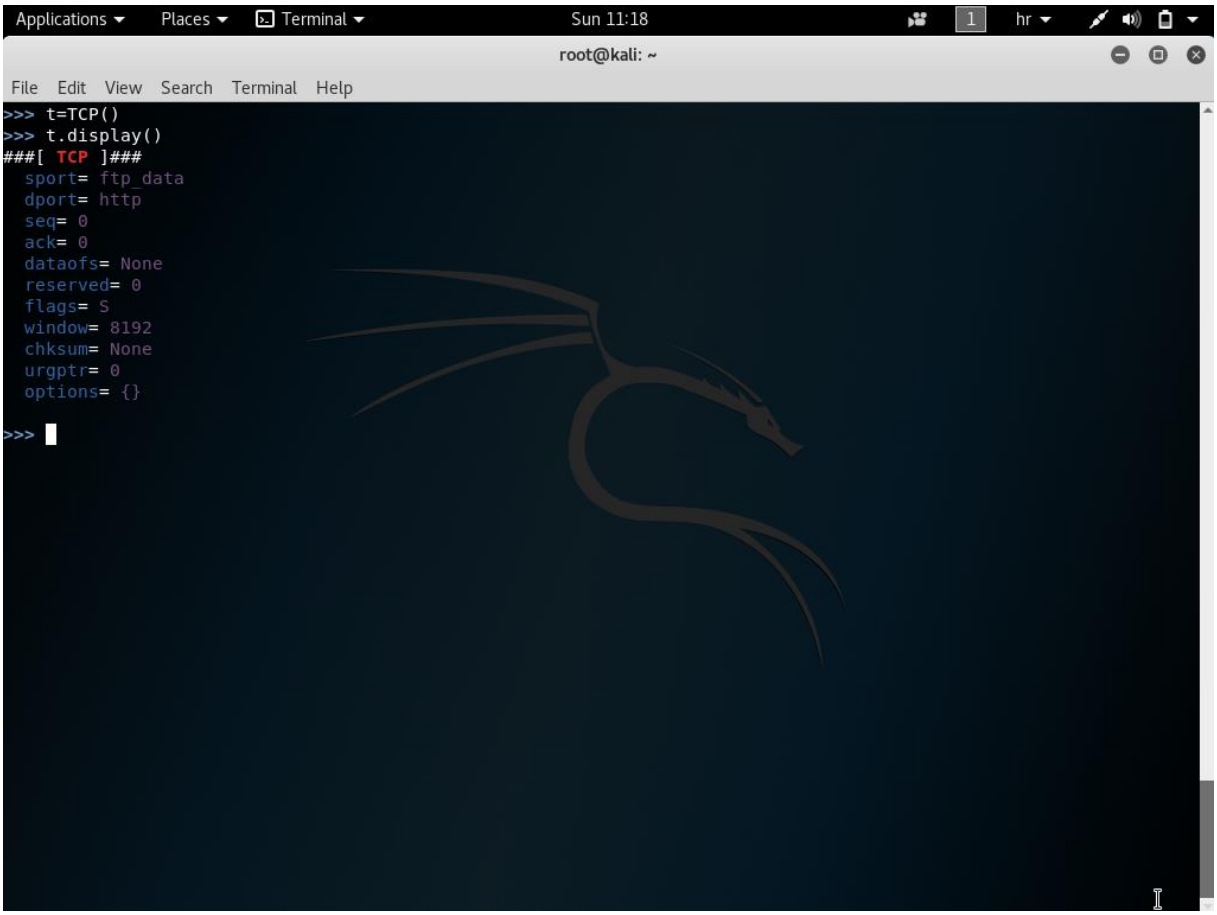
Sl. 3.18. *Sadržaj ping_reply objekta*

Za otkrivanje domaćina protokolom četvrtog sloja OSI modela koristi se TCP i UDP protokol. Kako bi bili sigurni o primljenom RST odgovoru od traženog domaćina, *Scapy* omogućuje slanje TCP ACK paketa. U primjeru ACK paket se šalje na odredišni TCP *port* 80. Kao u prethodnom primjeru potreban je IP objekt s odredišnom IP adresom (Slika 3.19).



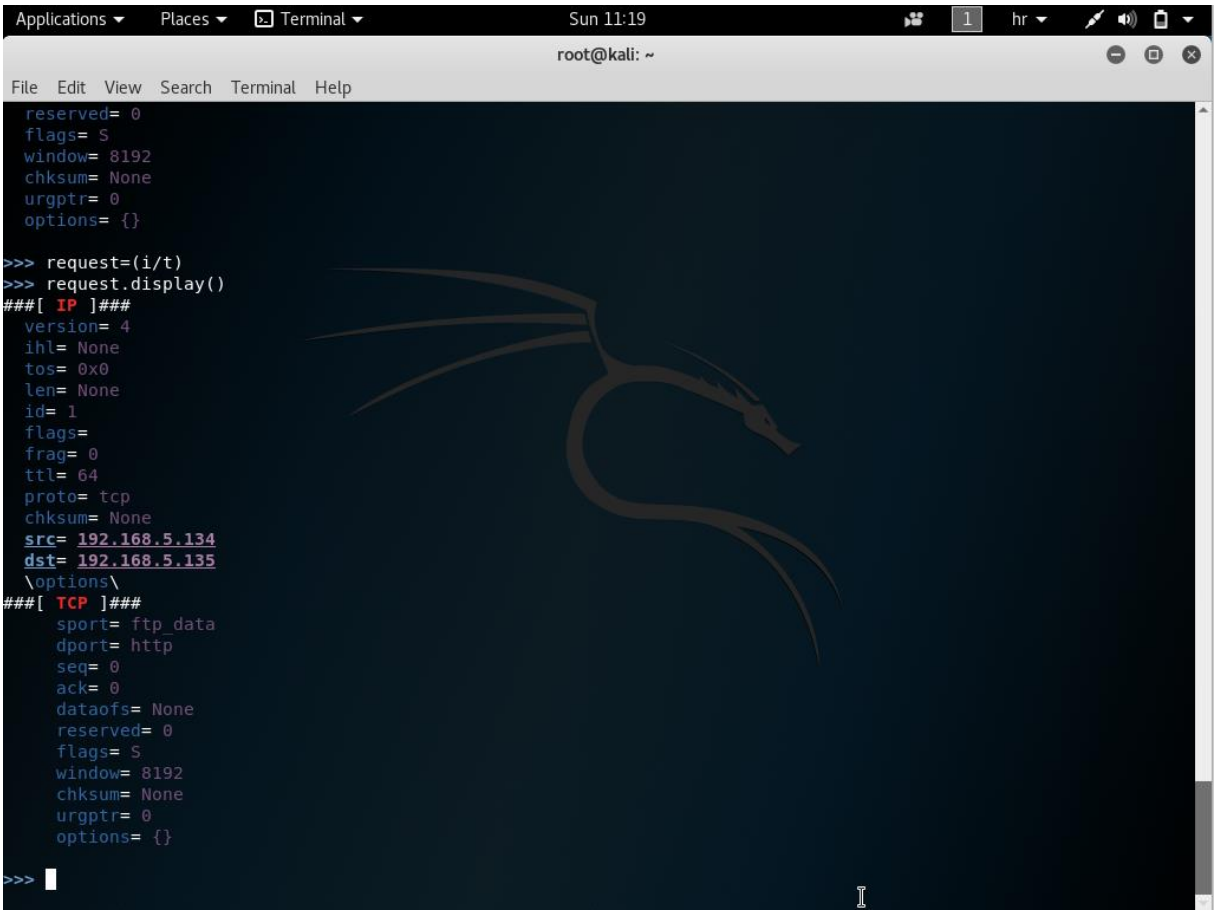
Sl. 3.19. *Stvaranje IP objekta za otkrivanje domaćina na četvrtom sloju*

Idući objekt koji je potrebno stvoriti je TCP objekt (Slika 3.20).



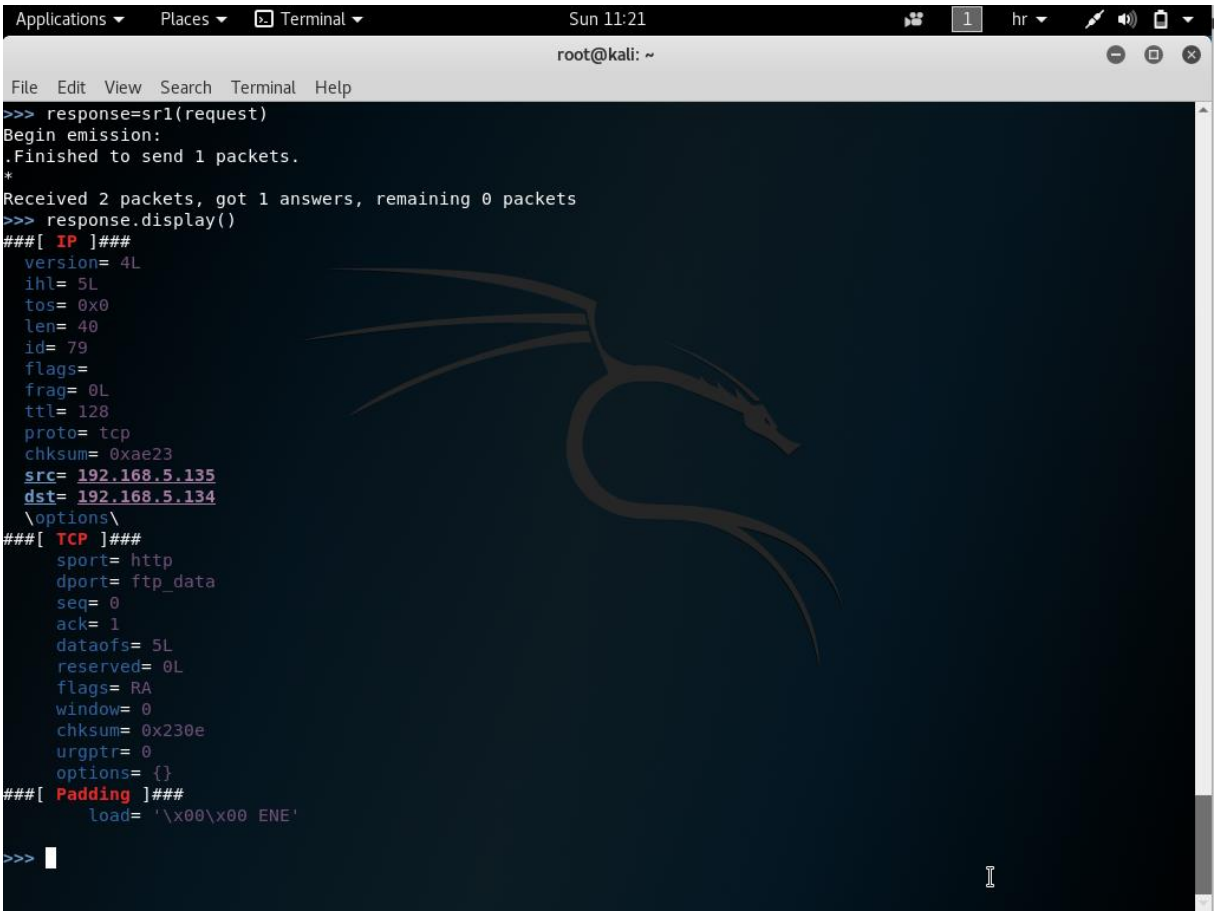
Sl. 3.20. *Stvaranje TCP objekta*

Prilikom stvaranja TCP objekta početna postavka *port*-a je HTTP ili *port* 80. Idući korak je stvoriti *request* objekt u kojem se IP i TCP objekti zajedno šalju (Slika 3.21).



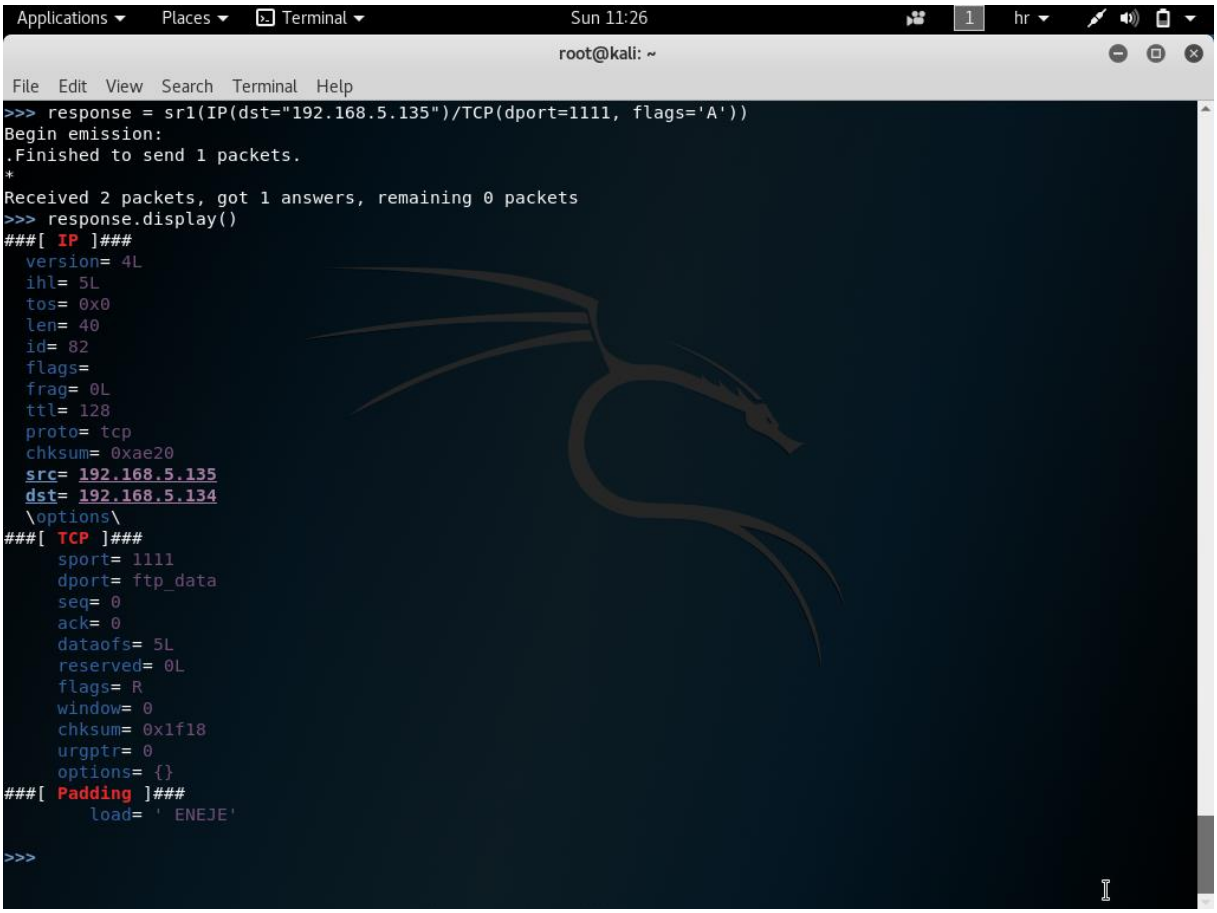
Sl. 3.21. *Stvaranje request objekta*

Nakon stvaranja objekta potrebno je promijeniti TCP zastavicu sa SYN (S) na ACK (A). Nakon slanja objekta, *display()* funkcijom se prikazuje odgovor. U odgovoru zastavica je postavljena na RST (Slika 3.22).



Sl. 3.22. *Prikaz uspješnog TCP zahtjeva*

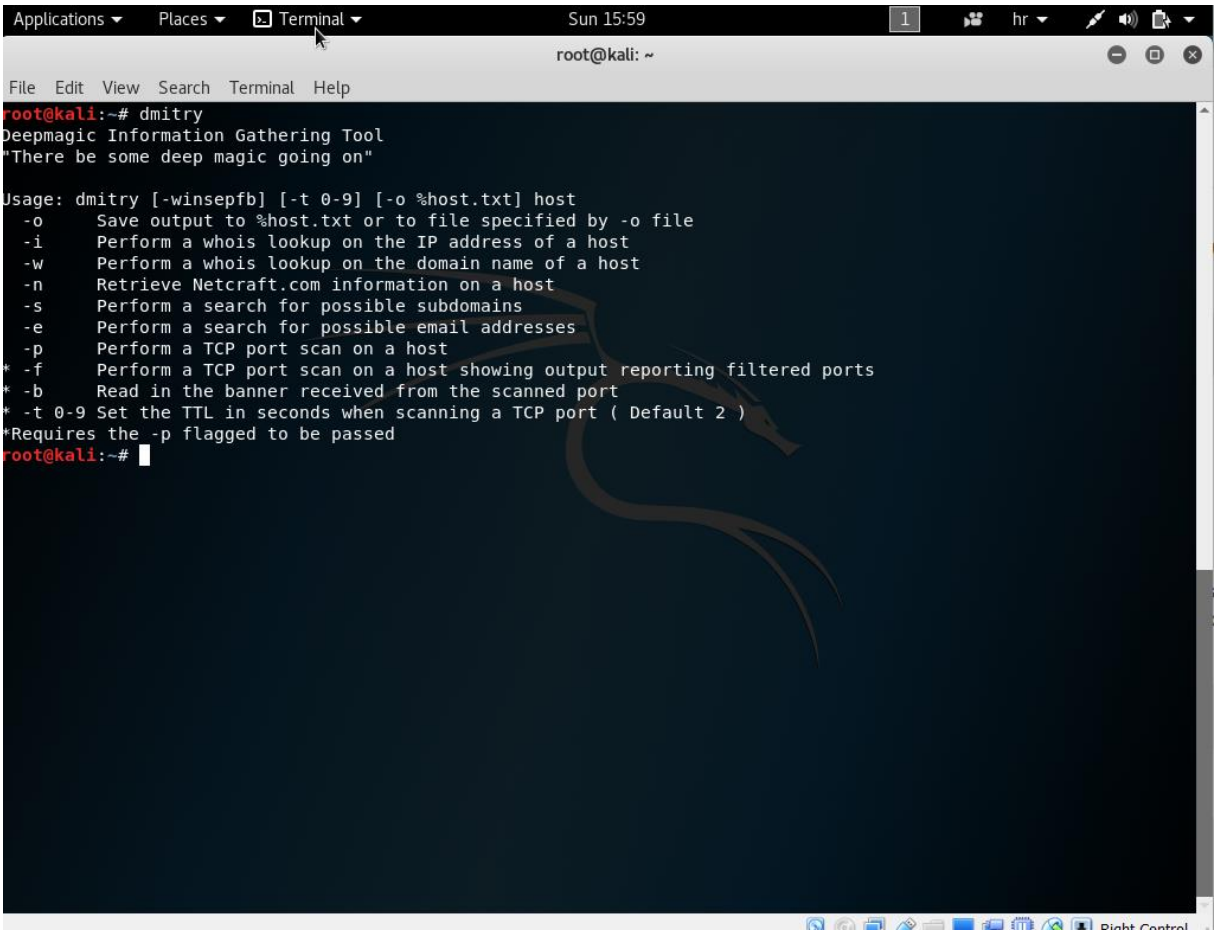
U idućem primjeru TCP *port* je promijenjen na *port* 1111 (*port* na kojem nije pokrenuta usluga). Podešavanje je moguće napraviti u jednom retku koda (Slika 3.23). Može se primijetiti kako je odgovor isti kod oba *port*-a bio on otvoren ili zatvoren.



Sl. 3.23. *TCP zahtjev na port 1111*

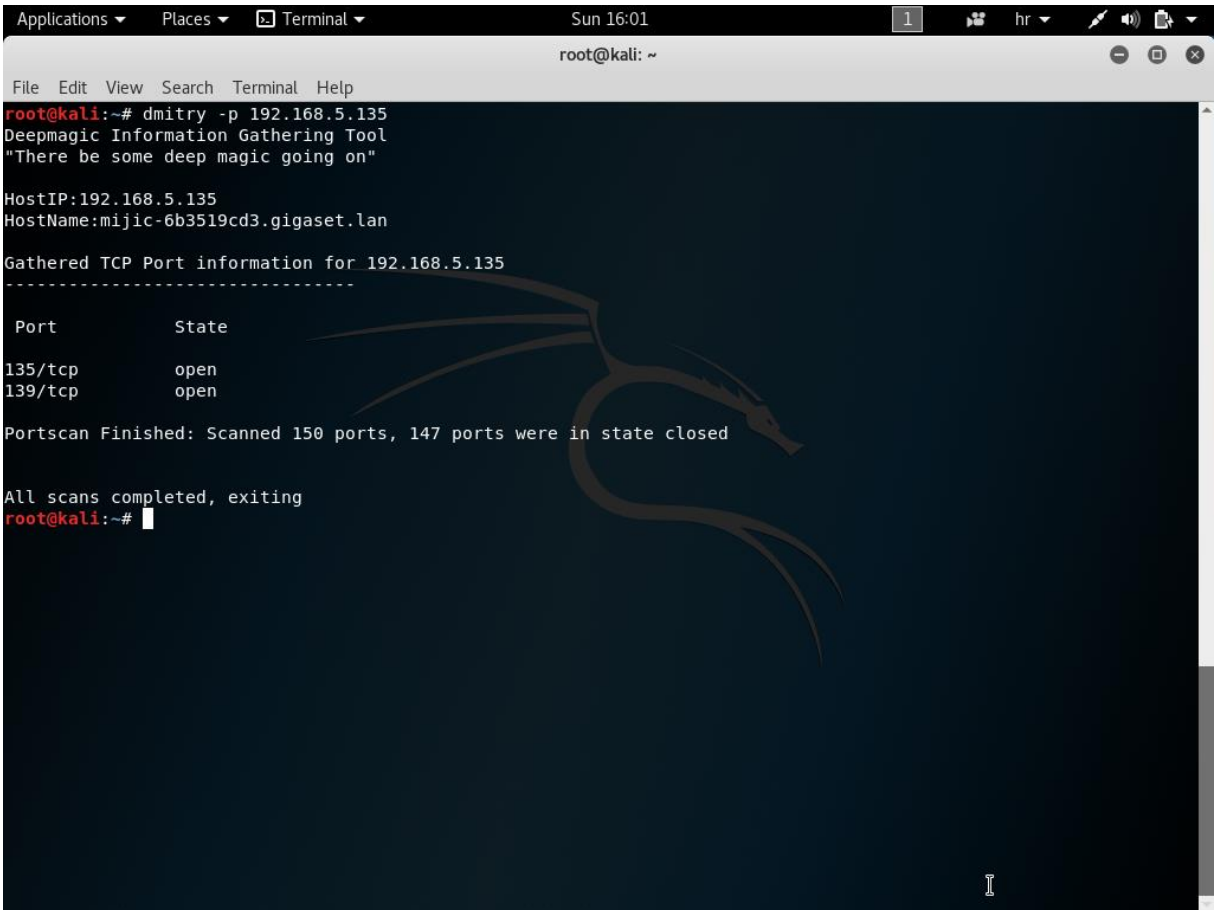
3.3.5. Dmitry

Dmitry je UNIX/(GNU) Linux aplikacija kodirana u C-u. Programom je moguće prikupiti što više informacija o domaćinu. Osnovne funkcionalnosti su prikupljanje poddomena, adrese e-pošte, skeniranje TCP *port*-ova itd [15]. U primjeru će biti objašnjeno skeniranje TCP *port*-ova. Koriste se Kali Linux i Windows XP uređaj. Za pokretanje programa u komandnoj liniji je potrebno upisati *dmitry* (Slika 3.24).



Sl. 3.24. *Dmitry izbornik*

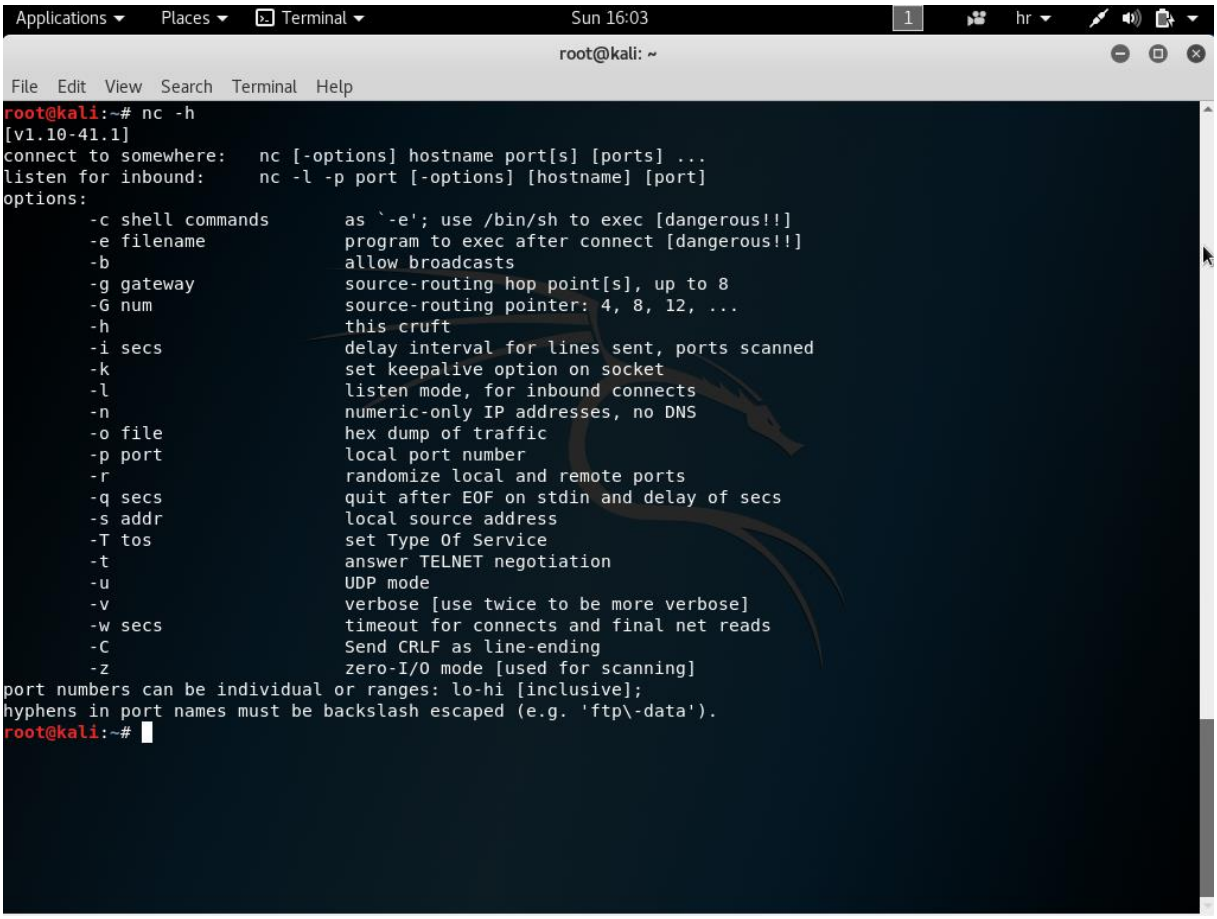
Kako bi izvršili skeniranje *port*-ova domaćina, potrebno je odabrati *-p* opciju skeniranja TCP *port*-ova. Opcija se koristi s IP adresom sustava koji se skenira. *Dmitry* za skeniranje koristi 150 najčešće korištenih i unaprijed definiranih *port*-ova koje će prikazati ukoliko su otvoreni (Slika 3.25). Rezultate skeniranja je moguće spremiti unutar tekstualne datoteke *-o* opcijom i nazivom datoteke.



Sl. 3.25. *Dmitry skeniranje*

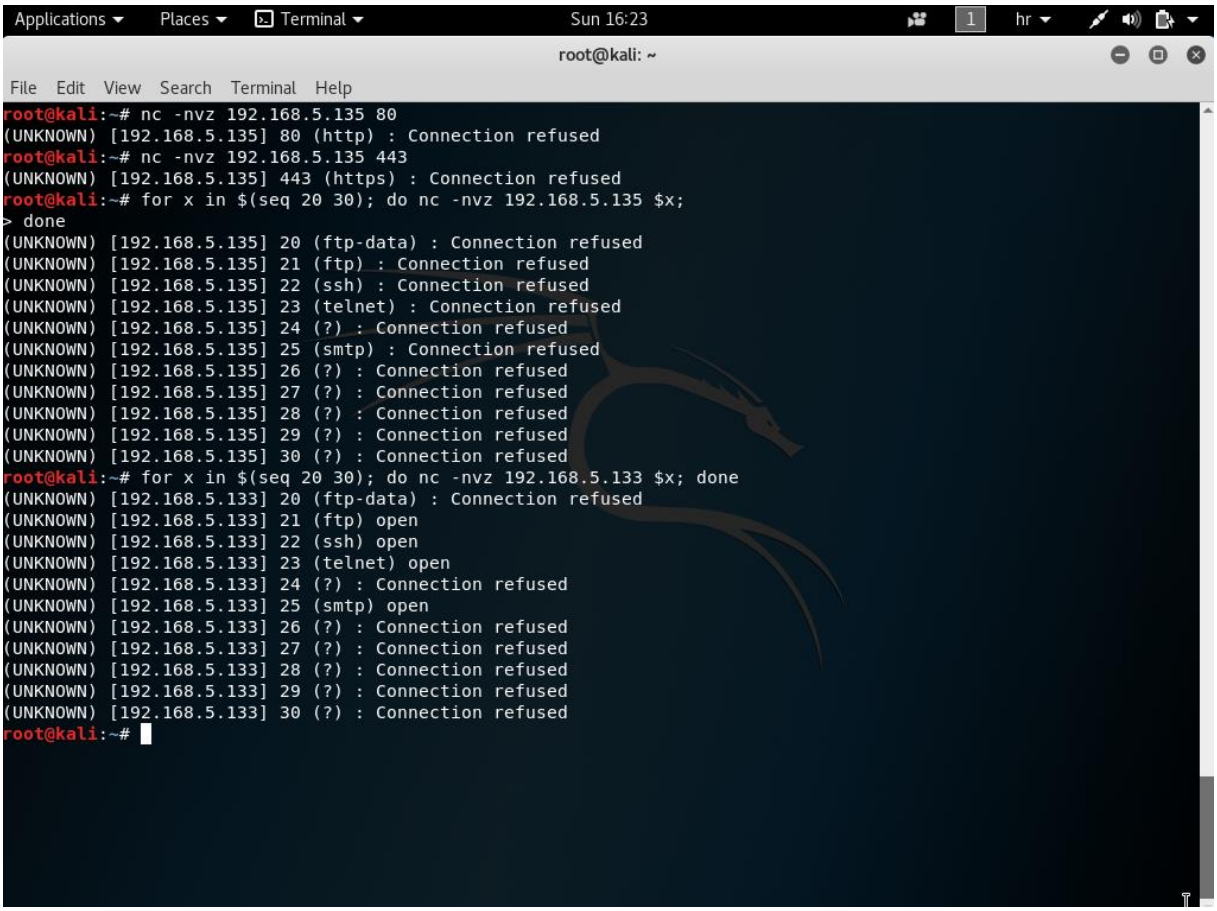
3.3.6. Netcat

Netcat je koristan višenamjenski alat za umrežavanje i može služiti za mnoge svrhe. Jedna od njih je skeniranje *port*-ova [15]. Kako bi se koristio *Netcat* potrebno je pokrenuti program naredbom *nc* uz *-h* opciju (Slika 3.26).



Sl. 3.26. *Netcat*

Kao što je prikazano *-z* opcija se koristi za skeniranje. Kako bi se skenirao TCP *port* 80 ciljanog sustava, koristi se *-n* opcija za IP adresu koja će se koristiti. Opcija *-v* se koristi za opširan izlaz skeniranja. U primjeru sa slike 3.27. prvo je skeniran Windows XP sustav (192.168.5.135) gdje su svi *port*-ovi zatvoreni. U drugom slučaju je skeniran Metasploitable2 (192.168.5.133) u kojem se nalaze otvoreni *port*-ovi.

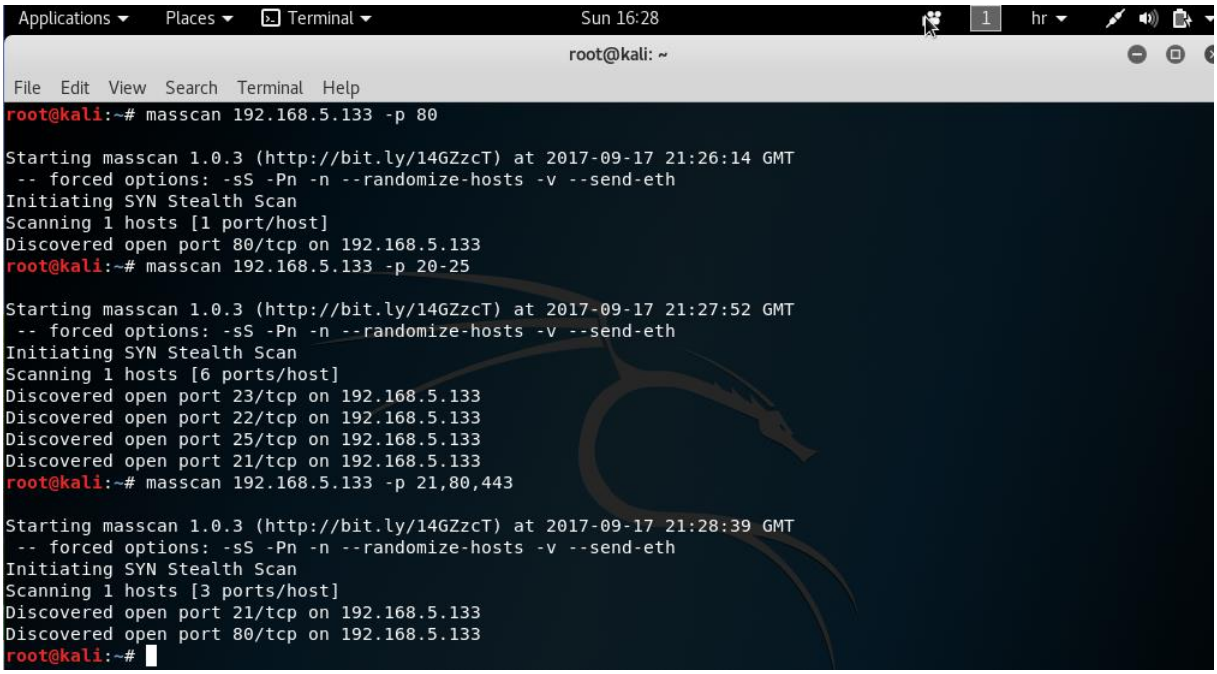


Sl. 3.27. *Netcat skeniranje port-ova*

Alati koji izvršavaju TCP konekcijska skeniranja izvode *three-way handshake* kako bi uspostavili vezu sa svim *port*-ovima skeniranog sustava. Ako se veza uspostavi *port* je otvoren. Ukoliko se veza ne uspostavi, *port* je zatvoren.

3.3.7. Masscan

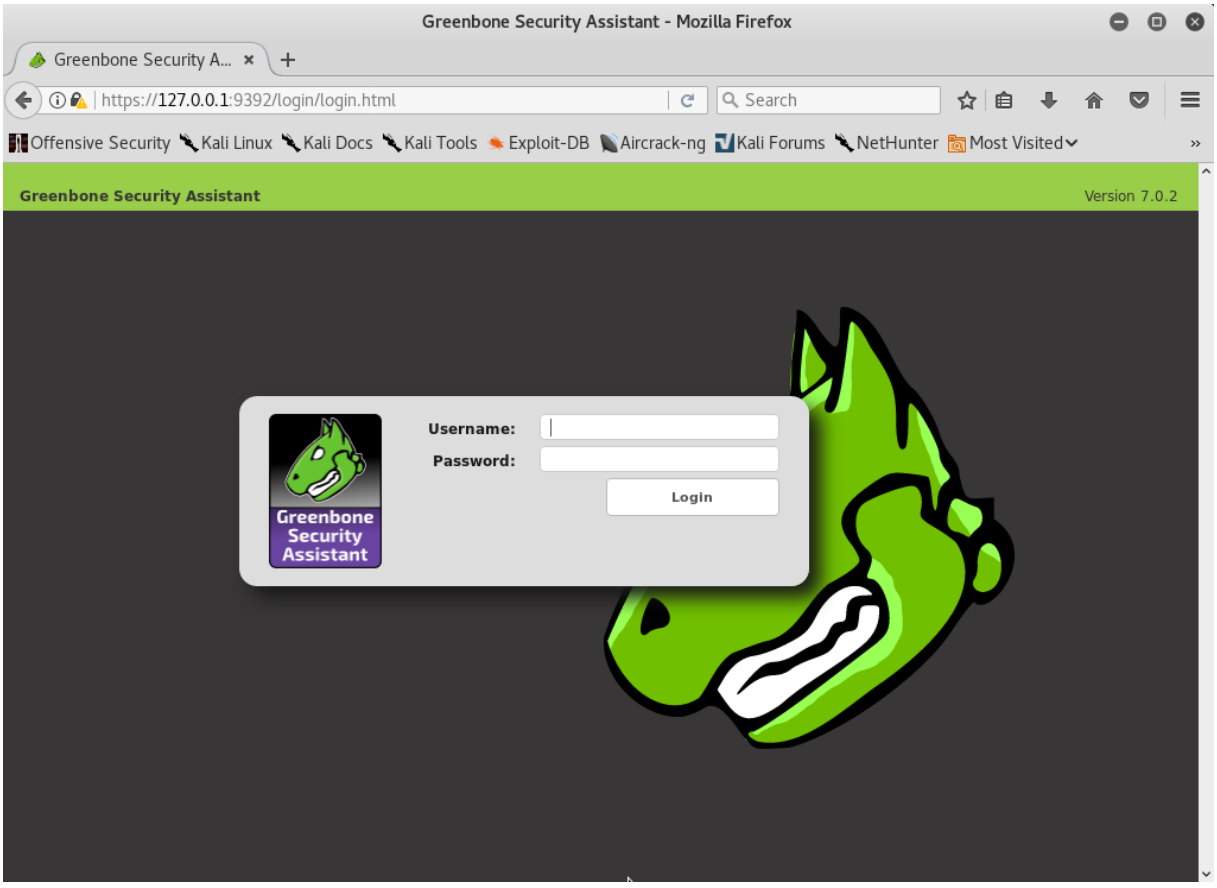
Masscan je najbrži skener *port*-ova. Program koristi asinkroni prijenos čime je omogućeno brzo skeniranje [15]. Kako bi se pokrenuo *Masscan* potrebno je upisati *masscan* u komandnu liniju, IP adresu sustava koji se skenira i opcija *-p* koja označava *port*-ove koji se skeniraju (Slika 3.28). U primjeru se skenira Metasploitable2 na tri načina odabira *port*-ova.



Sl. 3.28. *Masscan skeniranje port-ova*

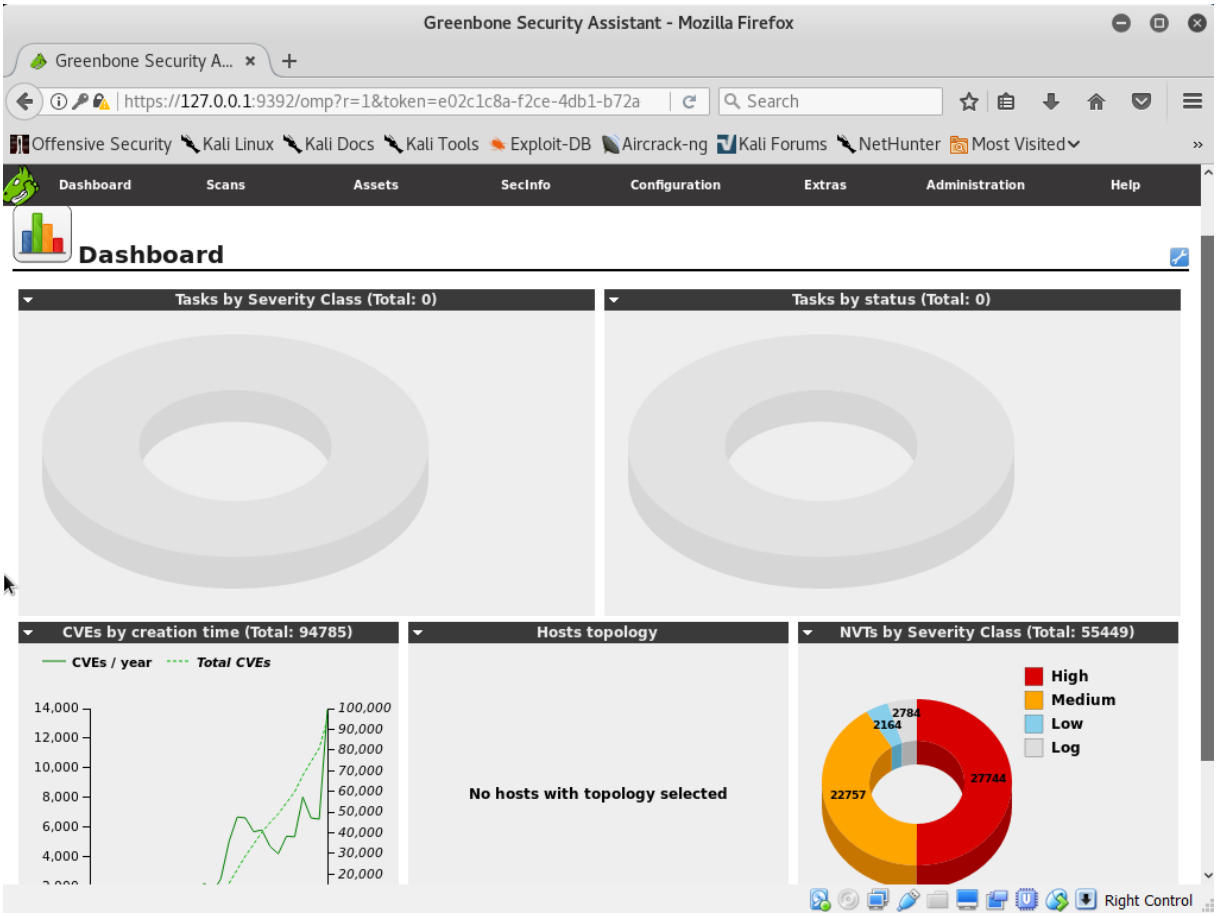
3.3.8. OpenVAS

OpenVAS (engl. *Open Vulnerability Assessment System*) je program koji se koristi za otkrivanje sigurnosne ranjivosti [16]. Proces otkrivanja sigurnosne ranjivosti je glavni dio penetracijskog testiranja. U primjeru korištenja *OpenVAS* programa testira se Metasploitable2 kako bi se pronašle sigurnosne ranjivosti. *OpenVAS* se pokreće s uređaja koji radi na Kali Linux. Kako bi se koristio *OpenVAS* u Kali Linux okruženju, potrebno je pokrenuti instalaciju naredbom *apt-get install openvas*. Nakon uspješne instalacije pokreće se naredba *openvas-setup* kojom se instaliraju i podešavaju skripte za testiranje ranjivosti. Nakon što se instaliraju i podese skripte, ispisat će se lozinka za pristup *OpenVAS* web sučelju (Slika 3.29).



Sl. 3.29. *OpenVAS web sučelje-registracija*

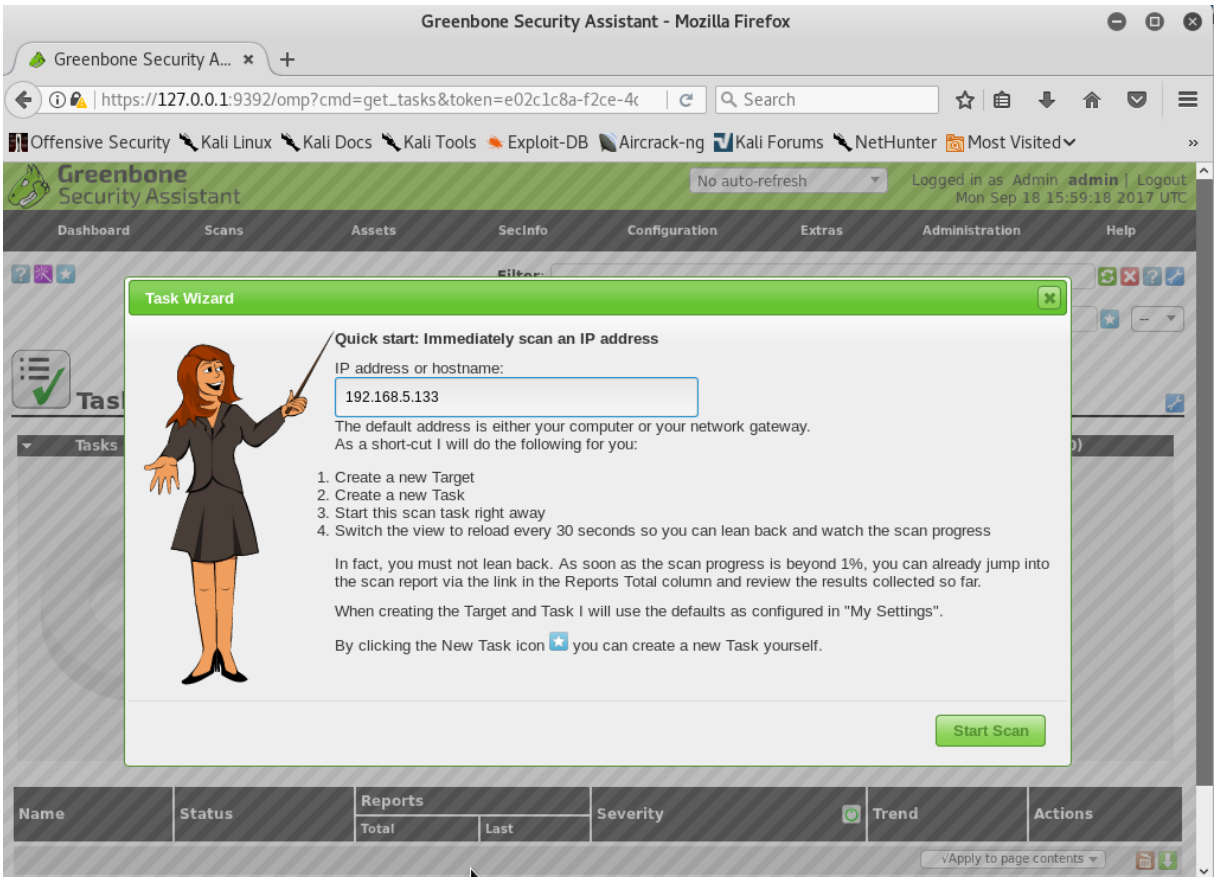
Kako bi se koristio *OpenVAS* potrebno je u komandnom prozoru upisati *openvas-start*. Kako bi se otvorilo web sučelje potrebno je u web pregledniku upisati adresu https://127.0.0.1:9392/. Za registraciju potrebno je upisati korisničko ime i lozinku koje se dobiju izvršavanjem *openvas-setup*. Nakon uspješne registracije slijedi prikaz *OpenVAS* web sučelja na kojem su prikazane statistike testiranja ranjivosti koje su izvedene (Slika 3.30).



Sl. 3.30. *OpenVAS web sučelje*

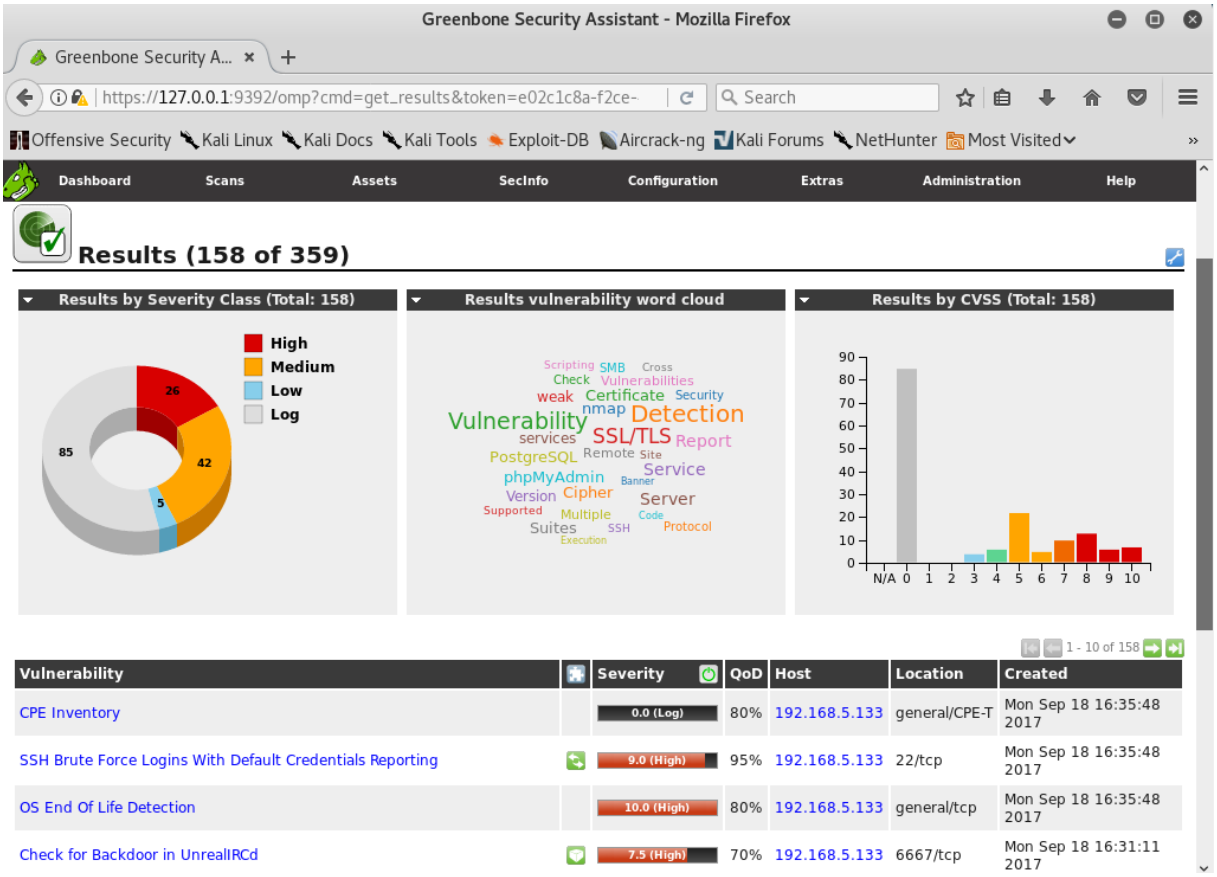
Budući da se *OpenVAS* prvi put koristi, nema informacija o prethodnim sigurnosnim testiranjima. Kako bi se pokrenulo sigurnosno testirane potrebno je u izborniku odabrati *Scans->Tasks*. Na prikazanoj *Tasks* stranici potrebno je kliknuti ikonu čarobnog štapića i odabrati *Task Wizard*. U *Task Wizard* prozoru upisuje se IP adresa domaćina koji se želi skenirati. U

primjeru upisana je IP adresa Metasploitable2, a to je 192.168.5.133 (Slika 3.31). Za pokretanje testiranja potrebno je kliknuti na *Start Scan*.



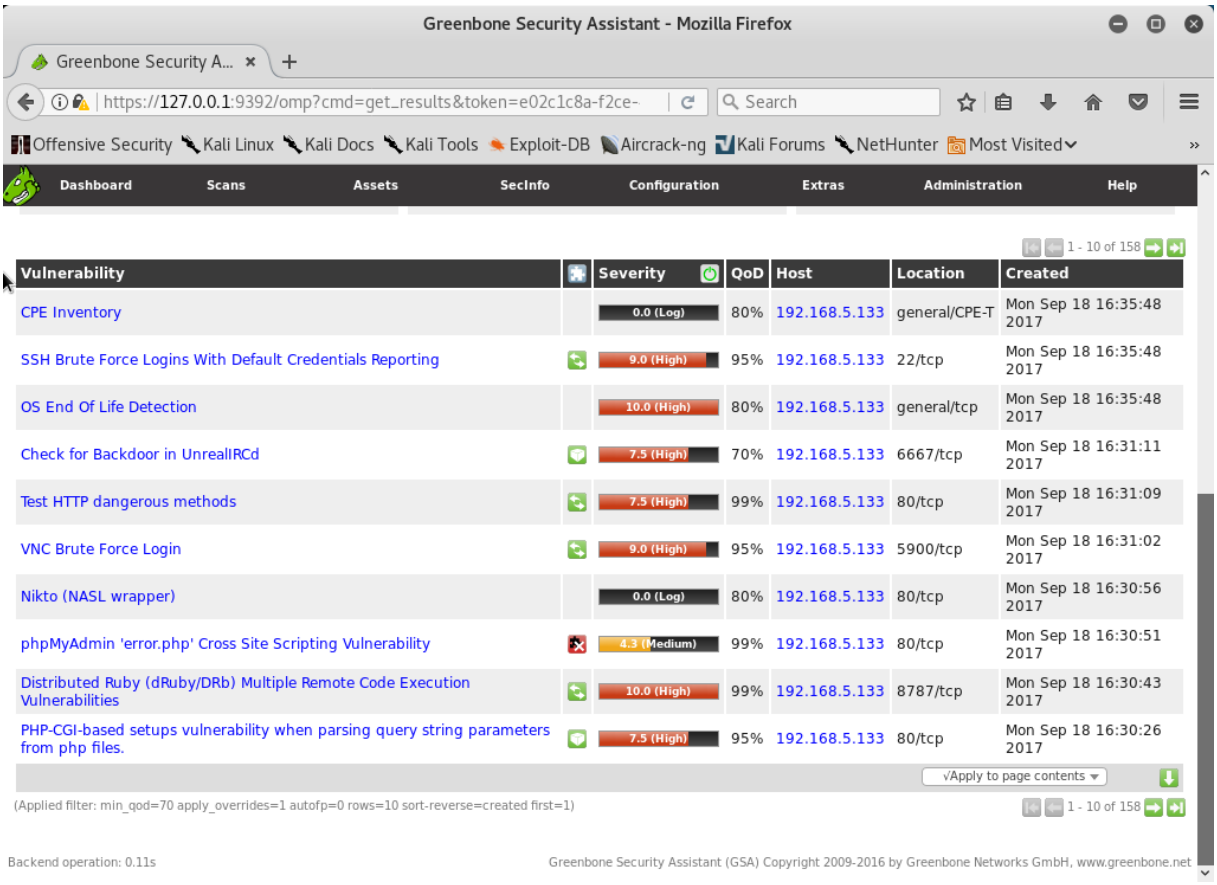
Sl. 3.31. *OpenVAS Task Wizard prozor*

Nakon uspješnog testiranja sigurnosne ranjivosti, za prikaz rezultata testiranja potrebno je u izbornik odabrati *Scans->Results*. U *Results* prozoru su prikazani dijagrami razine ozbiljnosti. U kružnom dijagramu razine ozbiljnosti su prikazane crvenom (visoka razina ozbiljnosti), žutom (srednja razina ozbiljnosti), plavom (niska razina ozbiljnosti) i sivom bojom(nema razine ozbiljnosti). Stupčasti dijagram prikazuje razinu ozbiljnosti prema vrijednostima CVSS (engl. *Common Vulnerability Scoring System*). Vrijednosti CVSS kreću se od nule do deset. Deset predstavlja najveću razinu ozbiljnosti, a nula najmanju. (Slika 3.32).



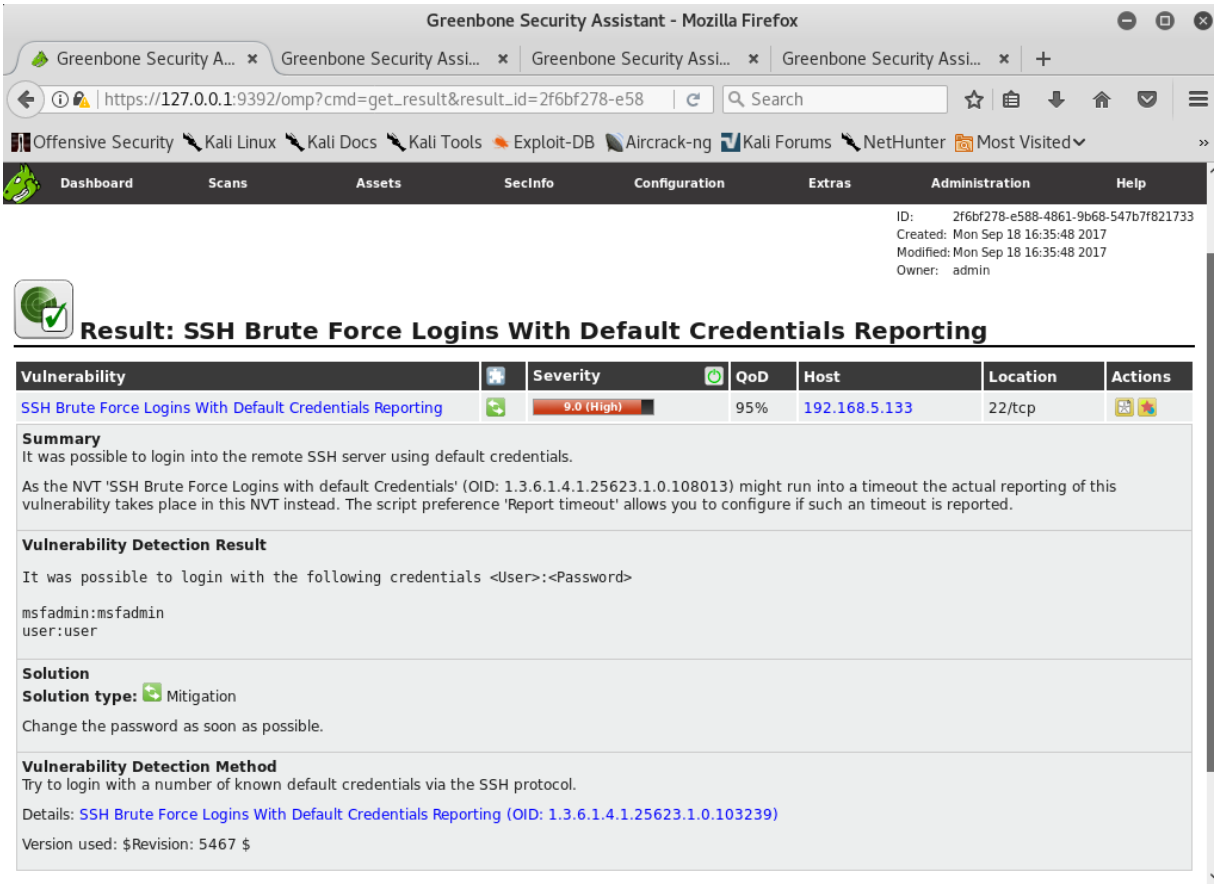
Sl. 3.32. *OpenVAS Results prozor*

Ispod dijagrama se nalazi tablica koja sadrži: ranjivost, ozbiljnost, QoD, IP adresu testiranog domaćina, lokaciju i vrijeme testiranja. QoD je vrijednost izražena u postocima od nula do sto koja opisuje pouzdanost otkrivanja ranjivosti (Slika 3.33).



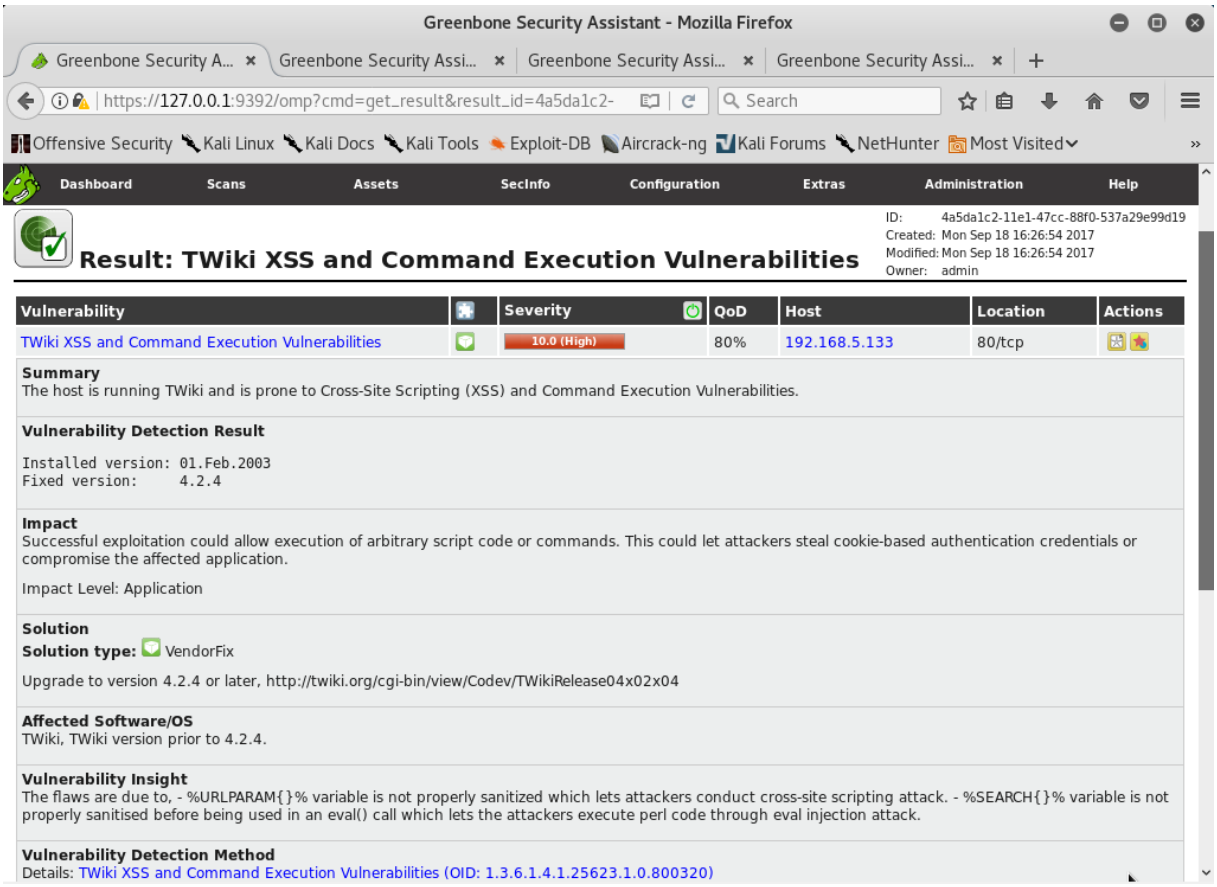
Sl. 3.33. *OpenVAS Results prozor-tablica*

U prilogu se nalazi tablica svih testova ranjivosti za Metasploitable2. Klikom na ranjivost otvara se prozor s detaljima testiranja odabrane ranjivosti. Kao primjer prikaza detalja odabrana je *SSH Brute Force Logins With Default Credentials Reporting*. Odabrana ranjivost se odnosi na pokušaj prijave u sustav grubom silom uz postojeću listu podataka o prijavi putem SSH protokola. Razina ranjivosti je visoka uz CVSS vrijednost devet. U detaljima se navodi otkriveno korisničko ime i lozinka. Kao rješenje sigurnosne ranjivosti se preporučuje promjena lozinke (Slika 3.34).



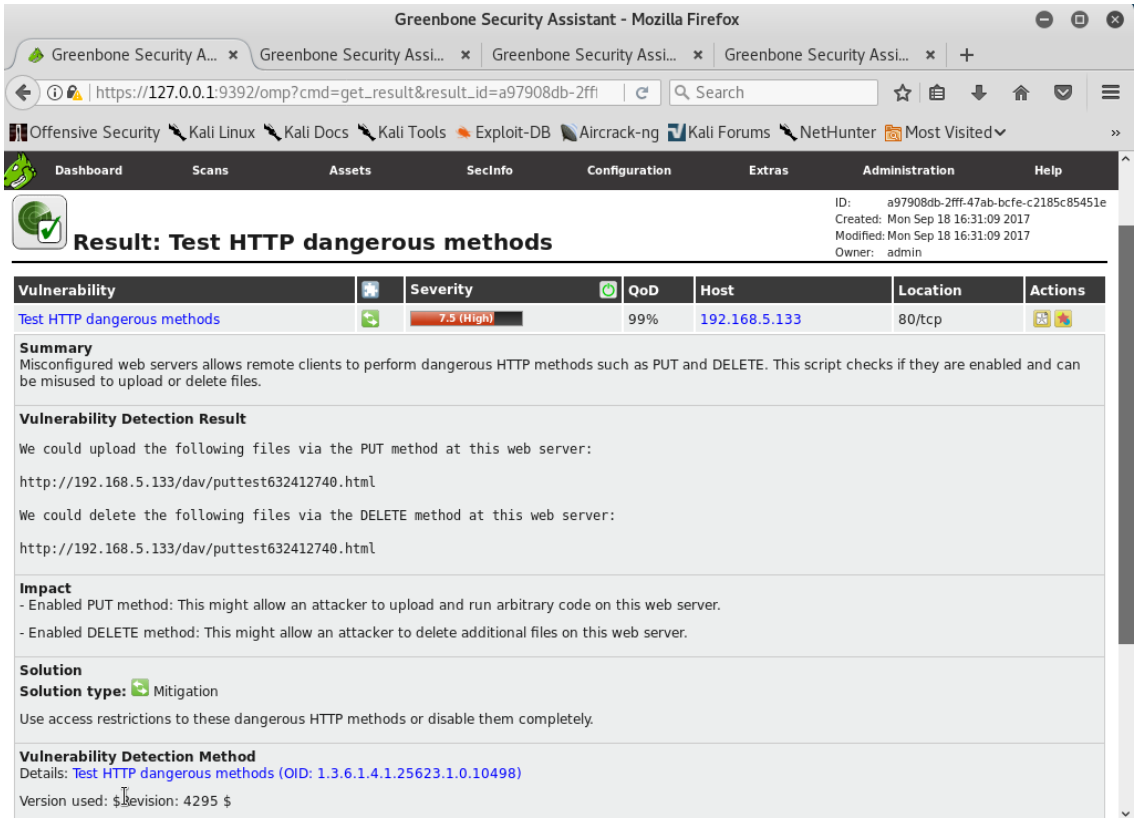
Sl. 3.34. *Detaljan pregled odabrane sigurnosne ranjivosti*

Na slici 3.35. prikazan je detaljan pregled *TWiki XSS and Command Execution Vulnerability*. Radi se o *cross-site scripting* i ranjivosti u izvršavanju naredbi. Napadač je u mogućnosti izvršavati štetne skripte koje su u mogućnosti ukrasti autentifikacijske kolačiće. Kao rješenje navodi se ažuriranje *software*-a.



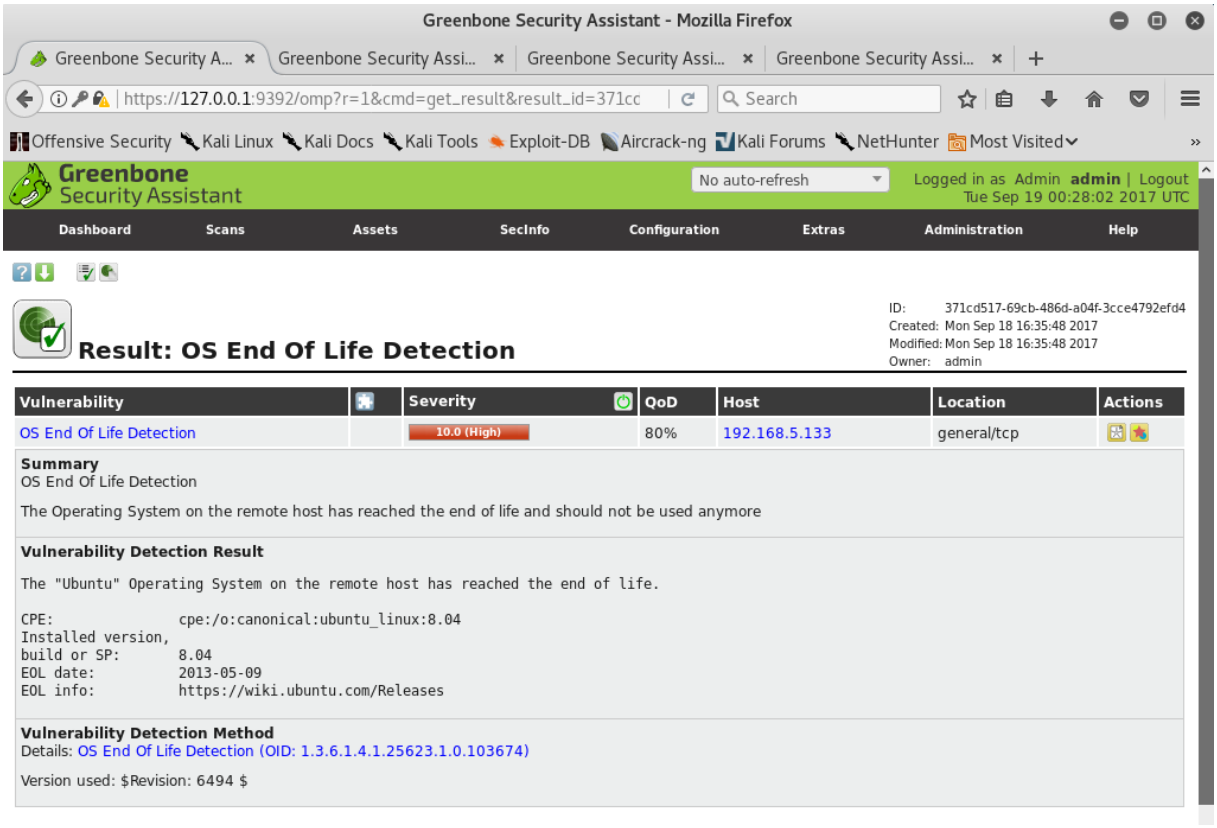
Sl. 3.35. *Detaljan pregled TWiki XSS and Command Execution Vulnerability*

Ranjivost s visokom CVSS varijablom je *Test HTTP dangerous methods*. Ova ranjivost podrazumijeva da nepravilno konfigurirani web poslužitelji omogućuju udaljenim klijentima izvođenje opasnih HTTP metoda kao što su PUT i DELETE. Ovim metodama napadaču je omogućeno postavljanje i pokretanje štetne skripte kao i brisanje datoteka. Kao rješenje predloženo je uvesti zabrane opasnim HTTP metodama ili ih onemogućiti u potpunosti (Slika 3.36).



Sl. 3.36. *Detaljan pregled Test HTTP dangerous methods*

Testiranje sigurnosti je u rezultatima pokazalo o dotrajalom operacijskom sustavu (Slika 3.37). Kako bi se dobio detaljan pregled potrebno je odabrati *OS End Of Life Detection*.



Sl. 3.37. *Detaljan pregled OS End Of Life Detection*

ZAKLJUČAK

Kao zaključak istaknuo bih smjernice za povećanje razine mrežne sigurnosti. Jedna od njih je redovno ažuriranje operacijskog sustava. Različite verzije operacijskih sustava su podlegle napadima. Ažuriranje je potrebno provoditi jednom mjesečno ili kako dolazi nova poboljšana inačica što drastično smanjuje rizik sigurnosne opasnosti. Također vrlo važno je ažurirati *software*. Osim što nove verzije *software*-a pružaju bolju učinkovitost i praktičnost, one također imaju bolje ugrađene sigurnosne značajke. Stoga je vrlo važno osigurati ažuriranje programa i preglednika. Za mrežnu sigurnost potreban je dobar i učinkovit antivirusni *software*, pogotovo ukoliko postoji povezanost s internetom. Postoji mnogo antivirusnih programa dostupni na tržištu koji mogu biti besplatni ili plaćeni s različitim stupnjevima učinkovitosti. Kao i svaki drugi program, najveća važnost antivirusne zaštite je ažuriranje kako bi se pohranile informacije o novim virusima i spriječile njihov utjecaj. *Antispyware* je jednako važan kao antivirus iz istih razloga. Za učinkovitu zaštitu mrežne sigurnosti potrebno je izbjegavati sumnjive web stranice. Web stranice koje se predstavljaju uslugama besplatnog sadržaja su često praćeni od hakera. Sadržaj koji se preuzima s tih web stranica može sadržavati zlonamjerni *software* koji ugrožava sigurnost računala i mreže. Ako postoji više od jednog računalnog sustava koji djeluje pod jednom mrežom, preporučljivo je instalirati vatrozid. Vatrozid dolazi u svim verzijama sustava Windows počevši od XP do najnovije verzije. U poslužiteljima e-pošte postoji filtri koji poruke sumnjivog sadržaja premještaju u *spam* ili ih odbacuju. Postoji mogućnost da e-pošta sumnjivog sadržaja prođe filtar. U takvim situacijama treba biti na oprezu i ne pokušavati čitati poruke, a to se odnosi posebno na one koje imaju privitke. Različiti zlonamjerni *software*-i mogu potpuno preoteti podatke i učiniti ih nepovratnima. Kako bi se spriječila navedena situacija, potrebno je stvoriti sigurnosnu kopiju podataka. Kopije svih važnih podataka spremljene na sustavu potrebno je spremiti na vanjsku memoriju, kao što je samostalni tvrdi disk ili neki drugi sličan uređaj. Ažuriranje kopija podataka potrebno je vršiti što češće. Jedan od najvažnijih sigurnosnih aspekata su lozinke. Lozinke su najčešće prve i posljednje „linije obrane“ od bilo kakvih vanjskih prijetnji. Pri odabiru lozinke nikada ne unositi datume rođendana, godišnjice, imena članova obitelji, brojeve bankovnog računa, telefonski broj, broj registracije automobila itd. Lozinke se nikad ne zapisuju u osobni dnevnik, mobitel ili na bilo koji drugi način. U odabir lozinke koristiti kombinaciju pomiješanih pisama i brojeva koji ne znače ništa u osobnom i poslovnom životu. Posljednja preporuka bi bila isključivanje računala ukoliko se ne koristi jer je nemoguće upasti u sustav koji nije uključen.

LITERATURA

[1] T. Pralas, E. Mujarić, Računalne mreže, CARNet, 2017.

[2] CARNet Computer Emergency Response Team, URL: http://www.cert.hr/sites/default/files/CCERT-PUBDOC-2009-06-267.pdf , 6/2009.

[3] T. McMillan, Cisco networking essentials, Indianapolis (SAD), Sybex, 2011.

[4] R. Mario, Računalne mreže (1), Digital Point Tiskara, Rijeka, 2010.

[5] R. Mario, Računalne mreže (2) prijenos, mrežne usluge i zaštita, Digital Point Tiskara, Rijeka, 2011.

[6] J. Casad, Teach yourself TCP/IP in 24 Hours 5th Edition, Sams, Indianapolis (SAD), 2011.

[7] CARNet Computer Emergency Response Team, URL: http://www.cert.hr/sites/default/files/CCERT-PUBDOC-2009-08-272.pdf , 8/2009.

[8] CARNet Computer Emergency Response Team, URL: http://www.cert.hr/sites/default/files/CCERT-PUBDOC-2006-02-149.pdf , 2/2006.

[9] T.G. Robertazzi, Introduction to Computer Networking, SAD, Springer, 2017.

[10] L. Budin, M. Golub, D. Jakobović, L. Jelenković, Operacijski sustavi, Zagreb, Element, 2010.

[11] W. Stallings, Cryptography and Network Security: Principles and Practice, Prentice Hall, 2011.

[12] C. Easttom, Computer security fundamentals, Indianapolis, Pearson, 2012.

[13] L. Allen, S. Ali, T. Heriyanto, Kali Linux – Assuring Security by Penetration Testing, Packt Publishing, Birmingham, 2014.

[14] www.linux.com

[15] www.kali.org/kali-linux-documentation

[16] www.openvas.org

SAŽETAK

Naslov: Primjena Kali Linux distribucije za testiranje sigurnosnih ranjivosti u mreži

Diplomski rad podijeljen je u dvije cjeline. Prva cjelina sadrži teoriju o računalnim mrežama, podjelu, OSI referentni model, protokoli i sigurnost računalnih mreža. U drugoj cjelini opisan je postupak penetracijskog testiranja i primjena pojedinih alata iz Kali Linux distribucije. U zaključku su istaknute smjernice i preporuke za povećanje razine mrežne sigurnosti.

Ključne riječi: Računalne mreže, Sigurnost računalnih mreža, Kali Linux, Penetracijsko testiranje, ranjivost

SUMMARY

Title: Application of Kali Linux distribution for testing network security vulnerabilities

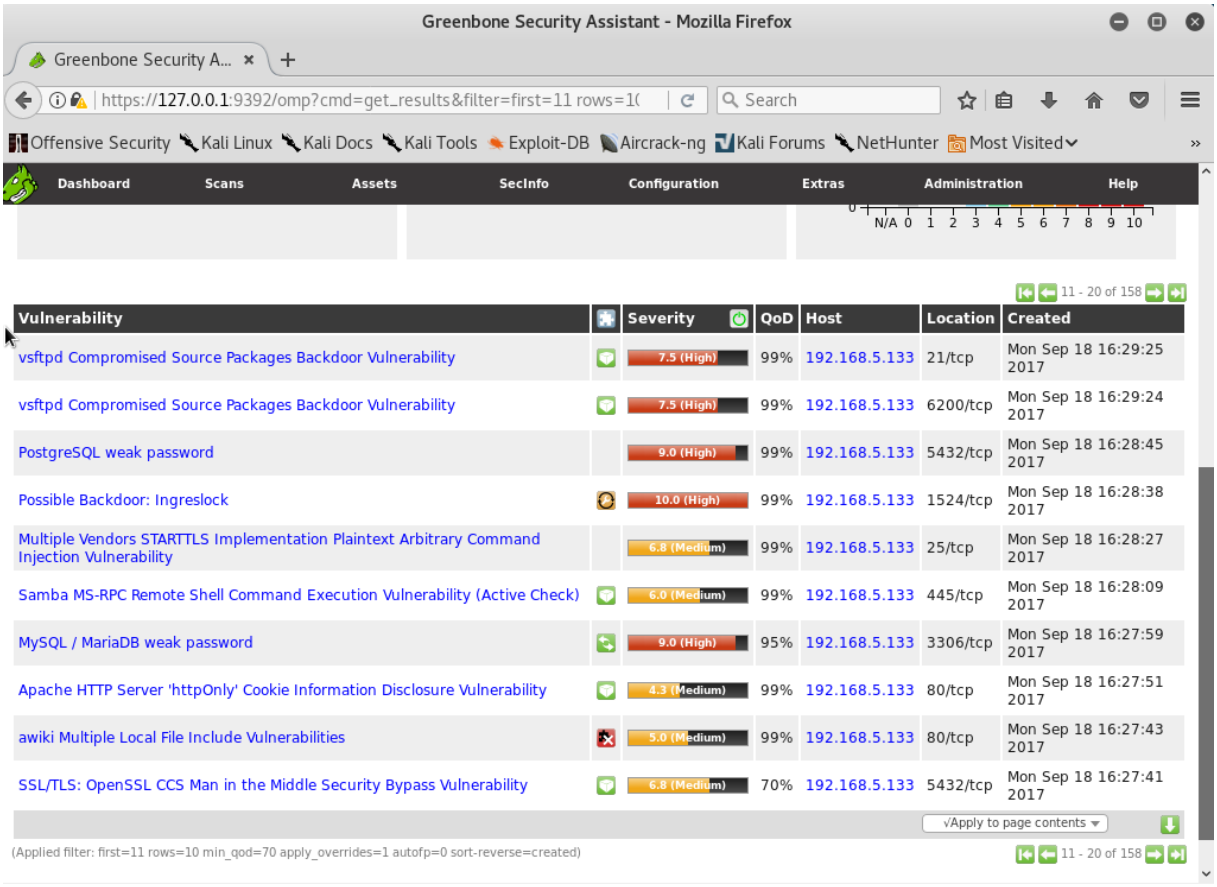
Masters thesis is divided into two units. The first unit contains the theory of computer networks, types, OSI reference model, protocols and computer network security. The second unit describes the procedure of penetration testing and application of some tools from Kali Linux distribution. In conclusion, the guidelines and recommendations for incrasing the level of network security are outlined.

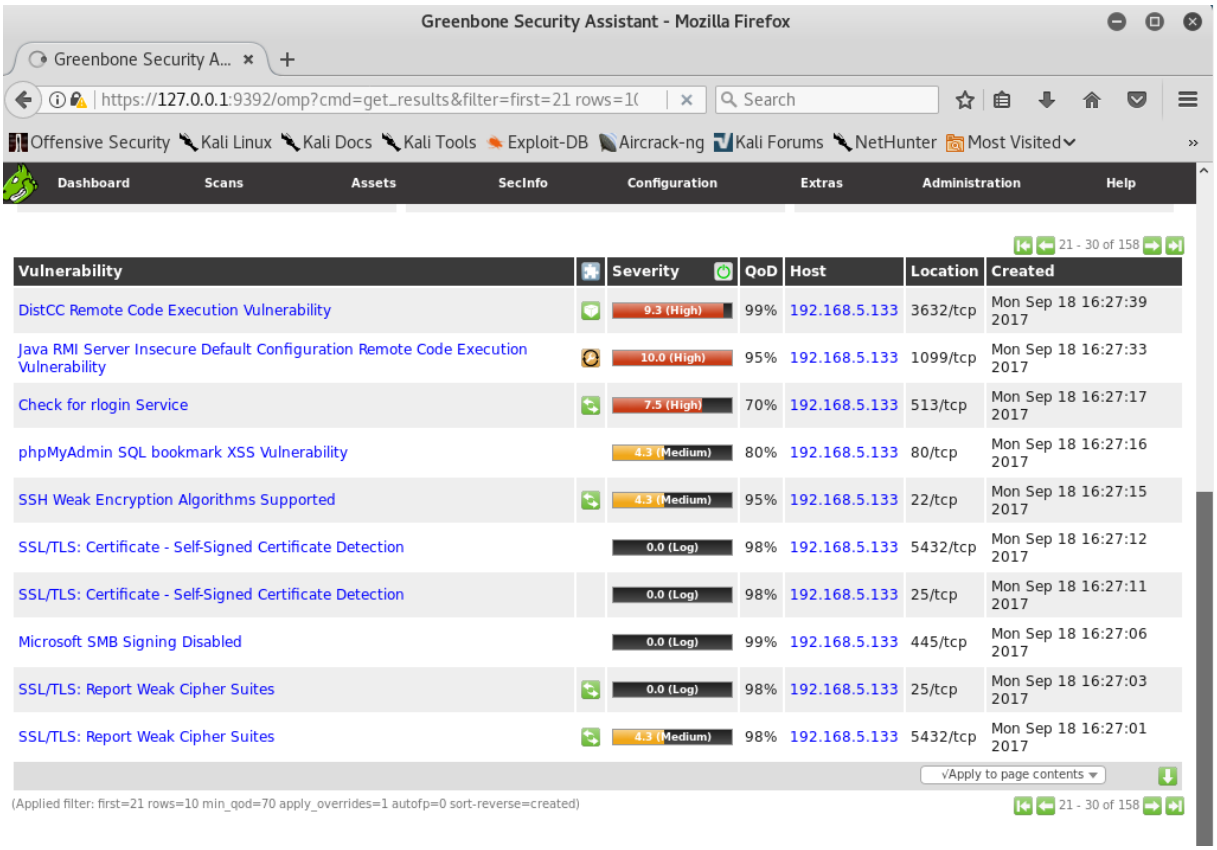
Key words: Computer network, Network security, Kali Linux, Penetration testing, Vulnerability

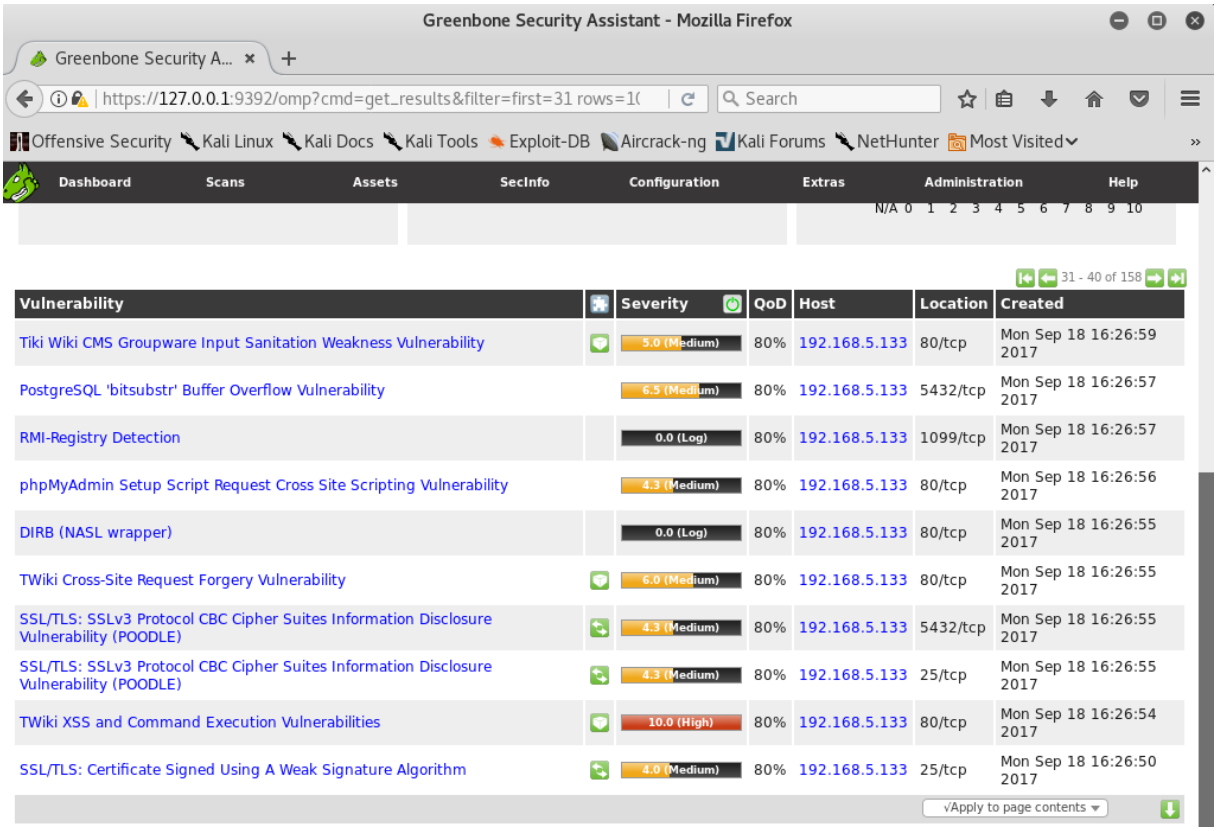
ŽIVOTOPIS

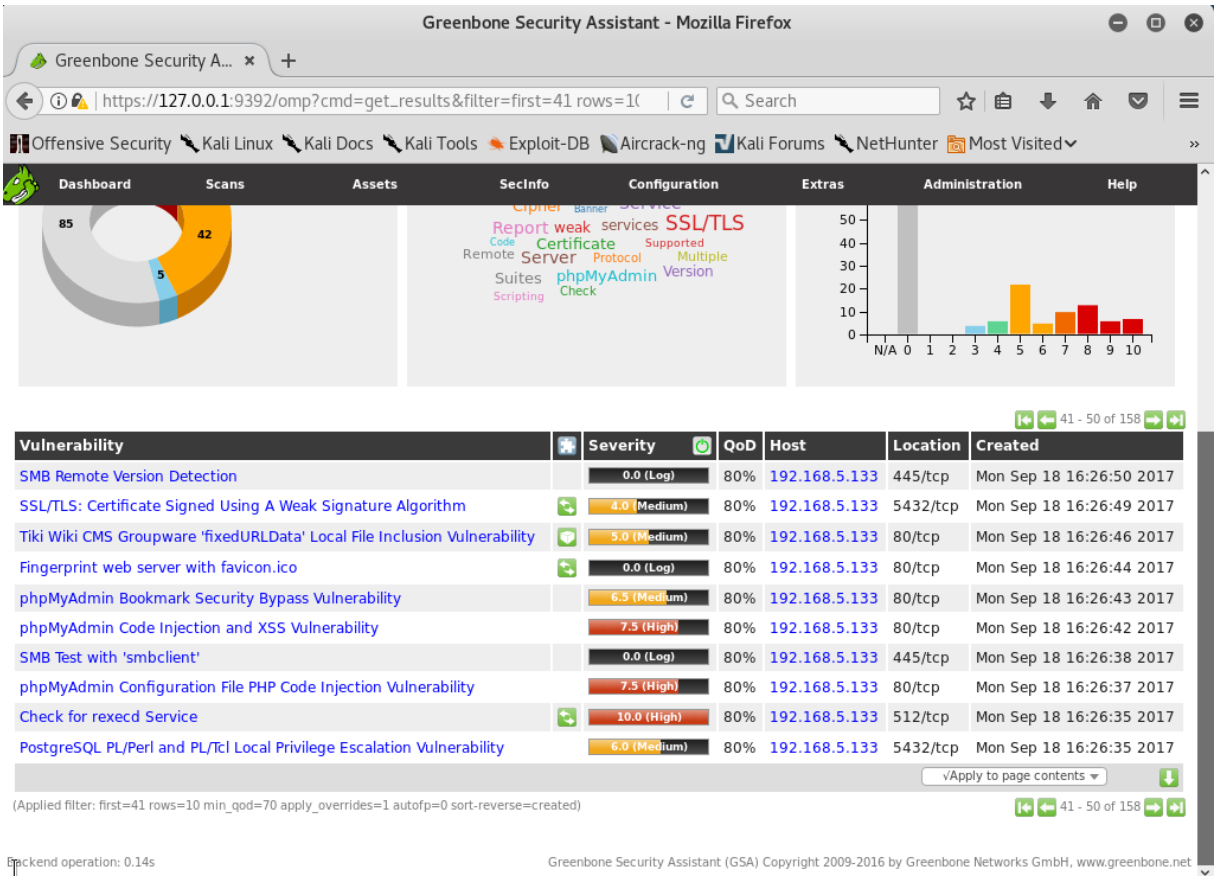
Ivan Mijić je rođen 18. listopada 1993. u Heidelbergu (Njemačka). Osnovnu školu je završio u OŠ Stjepan Radić Domaljevac (BiH). 2008. godine upisuje Elektrotehničku i prometnu školu u Osijeku. Sudjelovao je na gradskom i županijskom natjecanju iz fizike, gradskom natjecanju iz matematike. Završetkom srednje škole stekao je srednju školsku spremu, profil: elektrotehničar. Zbog zalaganja i odličnog uspjeha, 2012. godine ostvaruje izravan upis na Fakultet elektrotehnike, računarstva i informacijskih tehnologija u Osijeku. U slobodno vrijeme bavi se sportom i volontiranjem. Kroz studij održavao je demonstrature iz kolegija: Programiranje 1, Elektronika 1 i Sigurnost računalnih sustava. Odlično se služi njemačkim i engleskim jezikom.

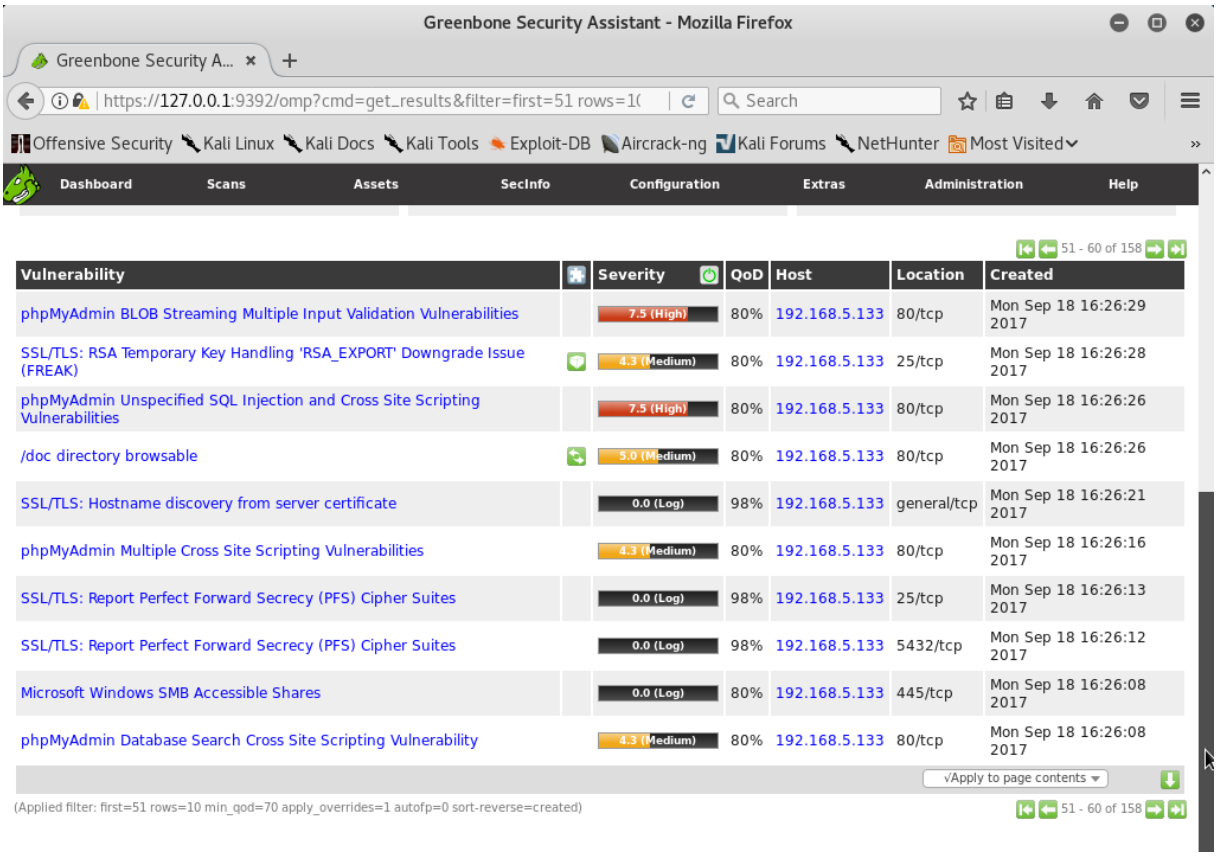
PRILOZI

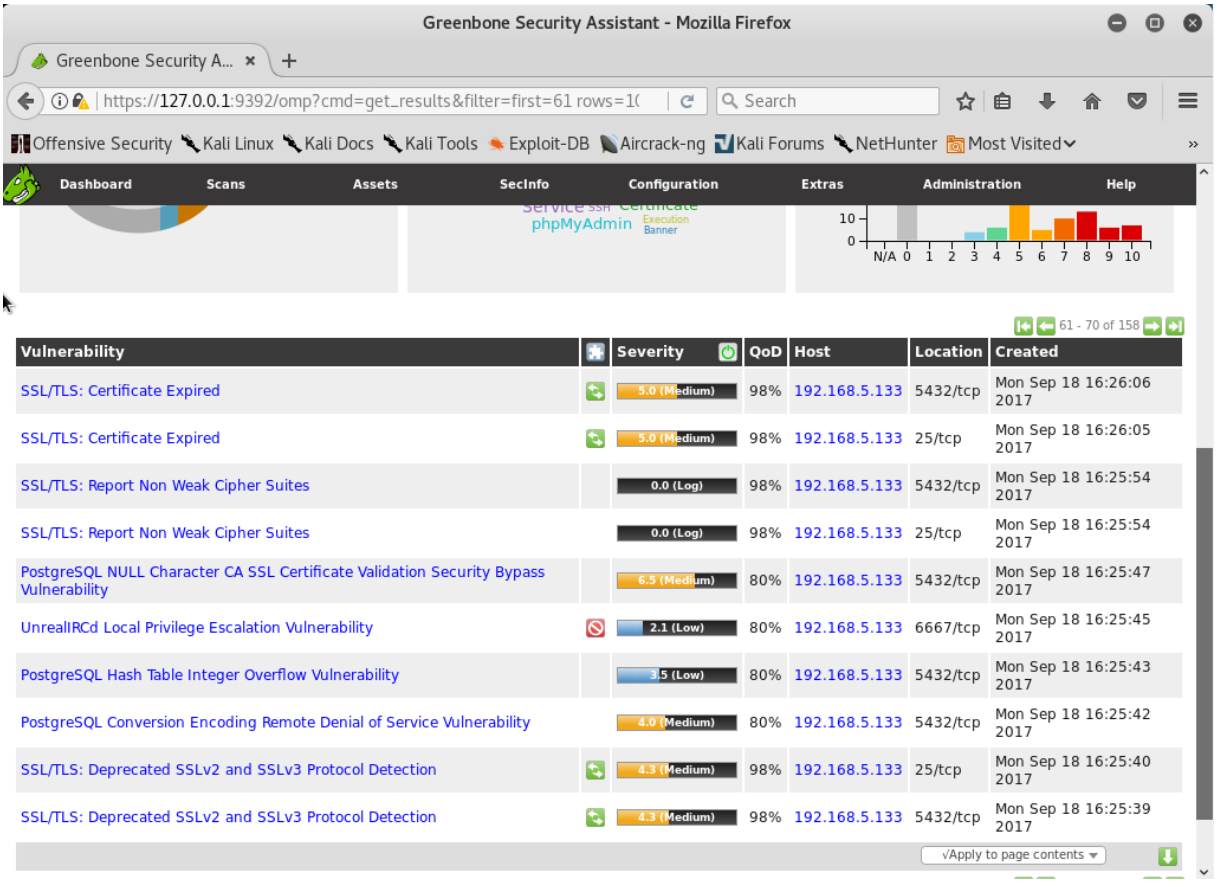

Greenbone Security Assistant - Mozilla Firefox
Greenbone Security A...
https://127.0.0.1:9392/omp?cmd=get_results&filter=first=11 rows=1(
Search
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Most Visited
Dashboard
Scans
Assets
SecInfo
Configuration
Extras
Administration
Help
N/A 0 1 2 3 4 5 6 7 8 9 10
11 - 20 of 158
Vulnerability
Severity
QoD
Host
Location
Created
vsftpd Compromised Source Packages Backdoor Vulnerability
7.5 (High)
99%
192.168.5.133
21/tcp
Mon Sep 18 16:29:25 2017
vsftpd Compromised Source Packages Backdoor Vulnerability
7.5 (High)
99%
192.168.5.133
6200/tcp
Mon Sep 18 16:29:24 2017
PostgreSQL weak password
9.0 (High)
99%
192.168.5.133
5432/tcp
Mon Sep 18 16:28:45 2017
Possible Backdoor: Ingreslock
10.0 (High)
99%
192.168.5.133
1524/tcp
Mon Sep 18 16:28:38 2017
Multiple Vendors STARTTLS Implementation Plaintext Arbitrary Command Injection Vulnerability
6.8 (Medium)
99%
192.168.5.133
25/tcp
Mon Sep 18 16:28:27 2017
Samba MS-RPC Remote Shell Command Execution Vulnerability (Active Check)
6.0 (Medium)
99%
192.168.5.133
445/tcp
Mon Sep 18 16:28:09 2017
MySQL / MariaDB weak password
9.0 (High)
95%
192.168.5.133
3306/tcp
Mon Sep 18 16:27:59 2017
Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability
4.3 (Medium)
99%
192.168.5.133
80/tcp
Mon Sep 18 16:27:51 2017
awiki Multiple Local File Include Vulnerabilities
5.0 (Medium)
99%
192.168.5.133
80/tcp
Mon Sep 18 16:27:43 2017
SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability
6.8 (Medium)
70%
192.168.5.133
5432/tcp
Mon Sep 18 16:27:41 2017
√Apply to page contents
(Applied filter: first=11 rows=10 min_qod=70 apply_overrides=1 autofp=0 sort-reverse=created)
11 - 20 of 158

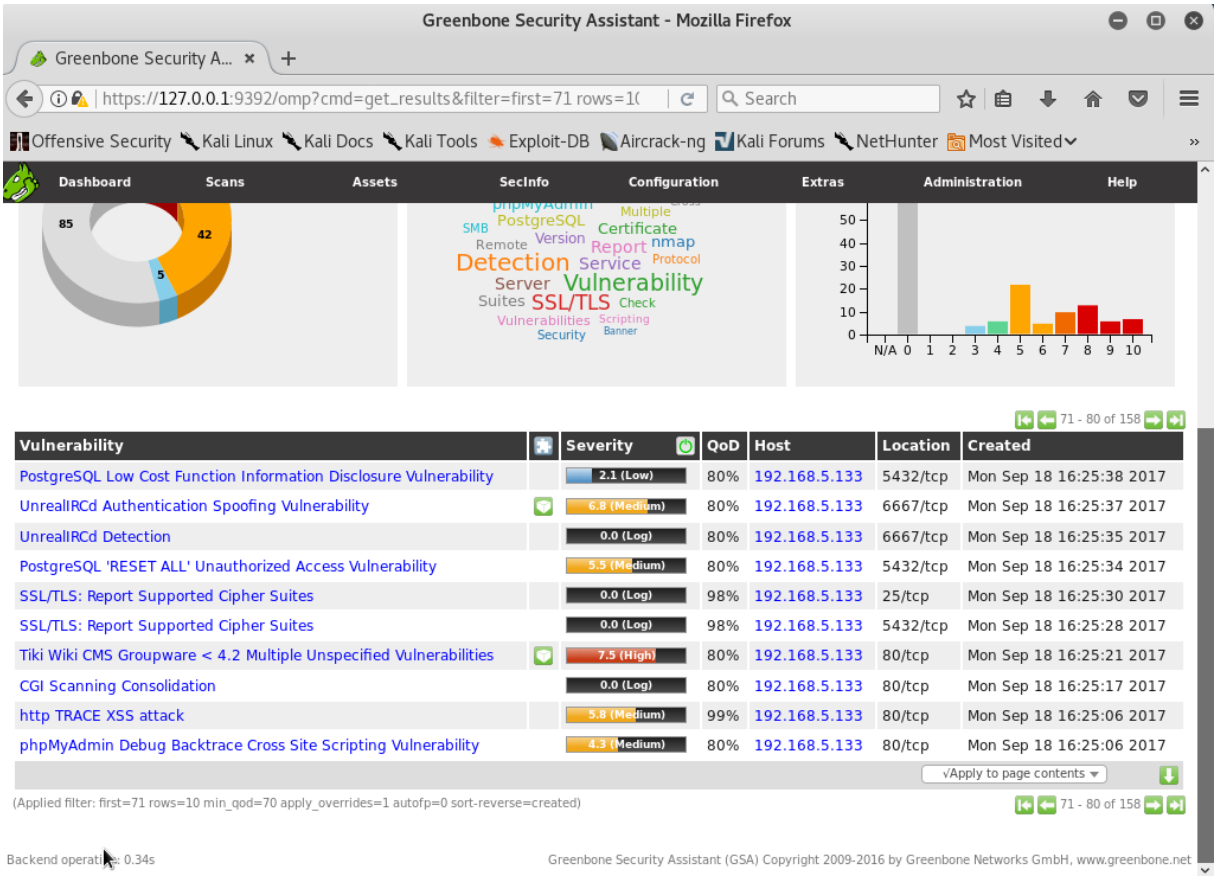

Greenbone Security Assistant - Mozilla Firefox
Greenbone Security A...
https://127.0.0.1:9392/omp?cmd=get_results&filter=first=21 rows=1(
Search
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Most Visited
Dashboard
Scans
Assets
SecInfo
Configuration
Extras
Administration
Help
21 - 30 of 158
Vulnerability
Severity
QoD
Host
Location
Created
DistCC Remote Code Execution Vulnerability
9.3 (High)
99%
192.168.5.133
3632/tcp
Mon Sep 18 16:27:39 2017
Java RMI Server Insecure Default Configuration Remote Code Execution Vulnerability
10.0 (High)
95%
192.168.5.133
1099/tcp
Mon Sep 18 16:27:33 2017
Check for rlogin Service
7.5 (High)
70%
192.168.5.133
513/tcp
Mon Sep 18 16:27:17 2017
phpMyAdmin SQL bookmark XSS Vulnerability
4.3 (Medium)
80%
192.168.5.133
80/tcp
Mon Sep 18 16:27:16 2017
SSH Weak Encryption Algorithms Supported
4.3 (Medium)
95%
192.168.5.133
22/tcp
Mon Sep 18 16:27:15 2017
SSL/TLS: Certificate - Self-Signed Certificate Detection
0.0 (Log)
98%
192.168.5.133
5432/tcp
Mon Sep 18 16:27:12 2017
SSL/TLS: Certificate - Self-Signed Certificate Detection
0.0 (Log)
98%
192.168.5.133
25/tcp
Mon Sep 18 16:27:11 2017
Microsoft SMB Signing Disabled
0.0 (Log)
99%
192.168.5.133
445/tcp
Mon Sep 18 16:27:06 2017
SSL/TLS: Report Weak Cipher Suites
0.0 (Log)
98%
192.168.5.133
25/tcp
Mon Sep 18 16:27:03 2017
SSL/TLS: Report Weak Cipher Suites
4.3 (Medium)
98%
192.168.5.133
5432/tcp
Mon Sep 18 16:27:01 2017
√Apply to page contents
(Applied filter: first=21 rows=10 min_qod=70 apply_overrides=1 autofp=0 sort-reverse=created)
21 - 30 of 158

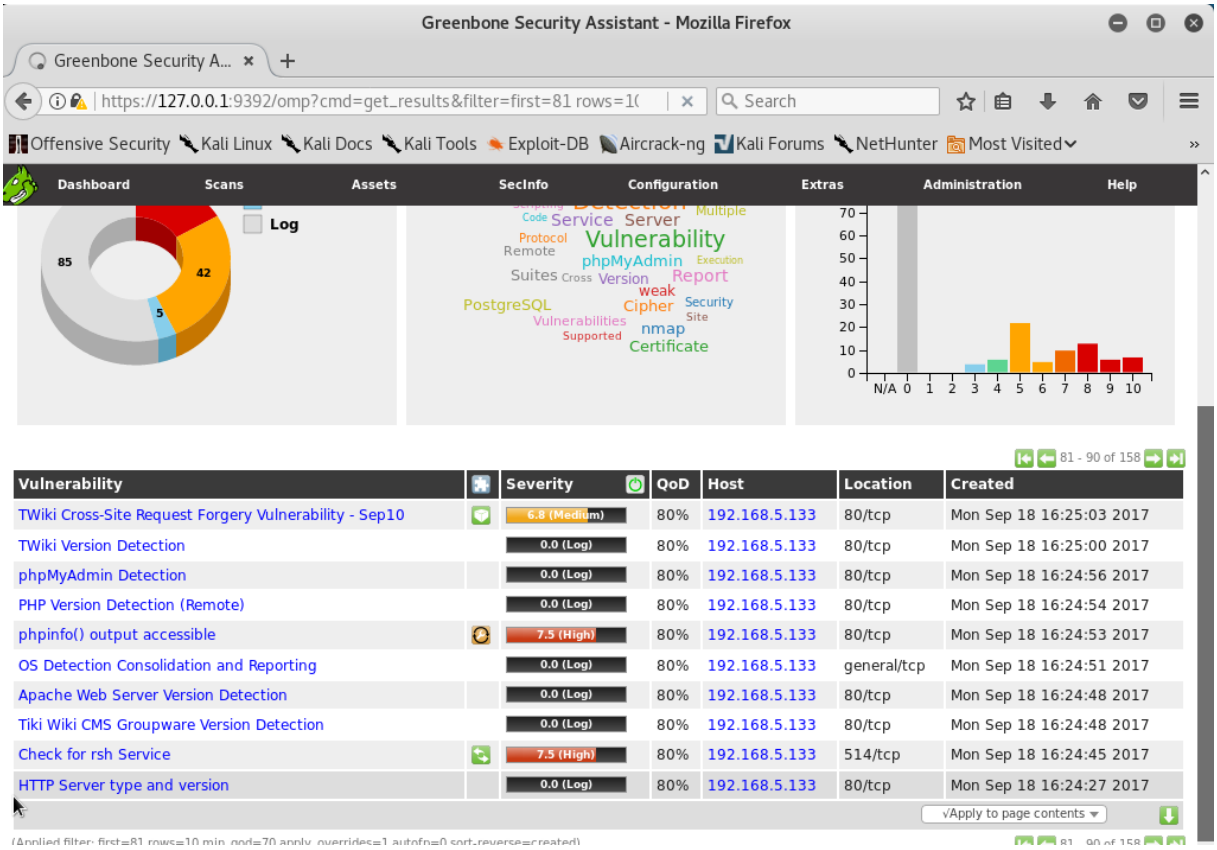

Greenbone Security Assistant - Mozilla Firefox
Greenbone Security A...
https://127.0.0.1:9392/omp?cmd=get_results&filter=first=31 rows=1(
Search
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Most Visited
Dashboard
Scans
Assets
SecInfo
Configuration
Extras
Administration
Help
N/A 0 1 2 3 4 5 6 7 8 9 10
31 - 40 of 158
Vulnerability
Severity
QoD
Host
Location
Created
Tiki Wiki CMS Groupware Input Sanitation Weakness Vulnerability
5.0 (Medium)
80%
192.168.5.133
80/tcp
Mon Sep 18 16:26:59 2017
PostgreSQL 'bitsubstr' Buffer Overflow Vulnerability
6.5 (Medium)
80%
192.168.5.133
5432/tcp
Mon Sep 18 16:26:57 2017
RMI-Registry Detection
0.0 (Log)
80%
192.168.5.133
1099/tcp
Mon Sep 18 16:26:57 2017
phpMyAdmin Setup Script Request Cross Site Scripting Vulnerability
4.3 (Medium)
80%
192.168.5.133
80/tcp
Mon Sep 18 16:26:56 2017
DIRB (NASL wrapper)
0.0 (Log)
80%
192.168.5.133
80/tcp
Mon Sep 18 16:26:55 2017
TWiki Cross-Site Request Forgery Vulnerability
6.0 (Medium)
80%
192.168.5.133
80/tcp
Mon Sep 18 16:26:55 2017
SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)
4.3 (Medium)
80%
192.168.5.133
5432/tcp
Mon Sep 18 16:26:55 2017
SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)
4.3 (Medium)
80%
192.168.5.133
25/tcp
Mon Sep 18 16:26:55 2017
TWiki XSS and Command Execution Vulnerabilities
10.0 (High)
80%
192.168.5.133
80/tcp
Mon Sep 18 16:26:54 2017
SSL/TLS: Certificate Signed Using A Weak Signature Algorithm
4.0 (Medium)
80%
192.168.5.133
25/tcp
Mon Sep 18 16:26:50 2017
√Apply to page contents

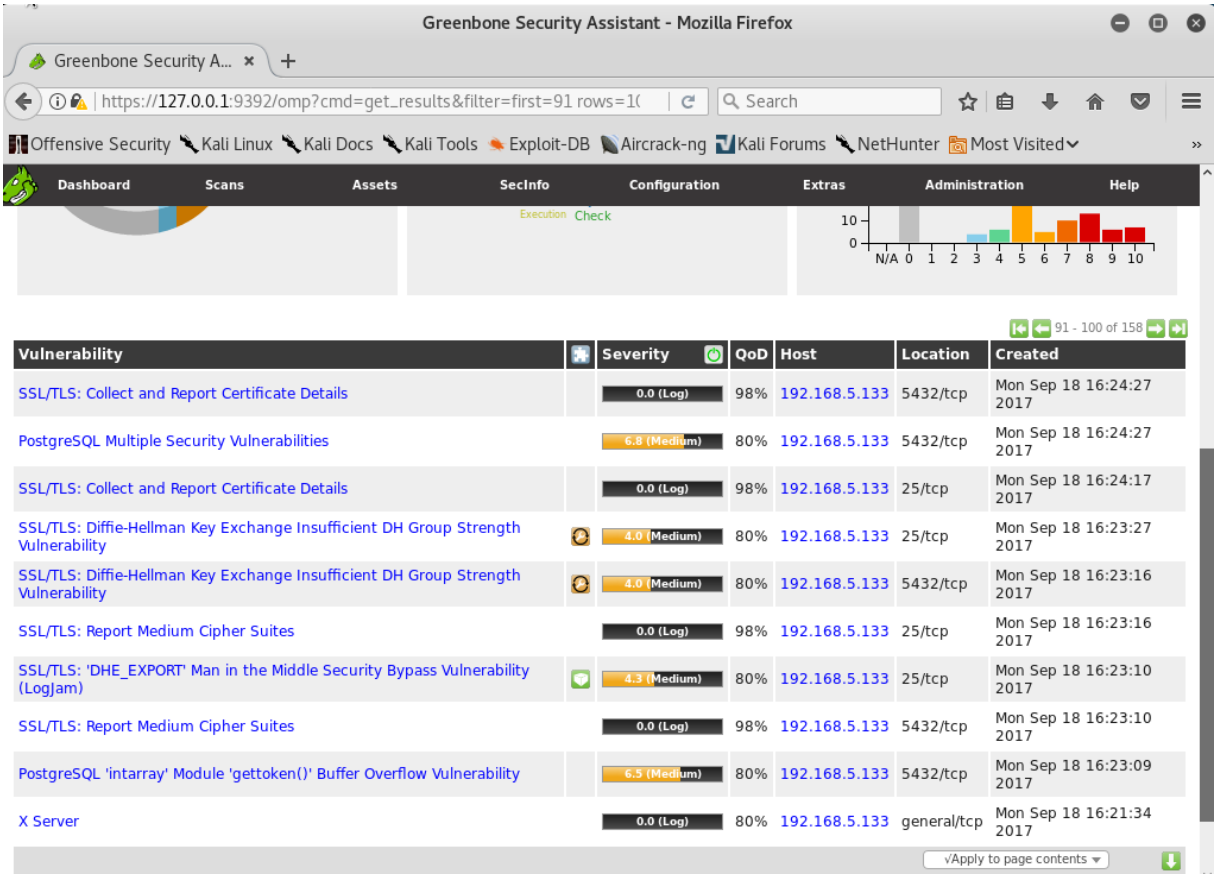

Greenbone Security Assistant - Mozilla Firefox
Greenbone Security A...
https://127.0.0.1:9392/omp?cmd=get_results&filter=first=41 rows=1(
Search
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Most Visited
Dashboard
Scans
Assets
SecInfo
Configuration
Extras
Administration
Help
85
42
5
Report weak services SSL/TLS
Certificate
Server
Suites
phpMyAdmin
Version
Check
Scripting
50
40
30
20
10
0
N/A 0 1 2 3 4 5 6 7 8 9 10
41 - 50 of 158
Vulnerability
Severity
QoD
Host
Location
Created
SMB Remote Version Detection
0.0 (Log)
80%
192.168.5.133
445/tcp
Mon Sep 18 16:26:50 2017
SSL/TLS: Certificate Signed Using A Weak Signature Algorithm
4.0 (Medium)
80%
192.168.5.133
5432/tcp
Mon Sep 18 16:26:49 2017
Tiki Wiki CMS Groupware 'fixedURLData' Local File Inclusion Vulnerability
5.0 (Medium)
80%
192.168.5.133
80/tcp
Mon Sep 18 16:26:46 2017
Fingerprint web server with favicon.ico
0.0 (Log)
80%
192.168.5.133
80/tcp
Mon Sep 18 16:26:44 2017
phpMyAdmin Bookmark Security Bypass Vulnerability
6.5 (Medium)
80%
192.168.5.133
80/tcp
Mon Sep 18 16:26:43 2017
phpMyAdmin Code Injection and XSS Vulnerability
7.5 (High)
80%
192.168.5.133
80/tcp
Mon Sep 18 16:26:42 2017
SMB Test with 'smbclient'
0.0 (Log)
80%
192.168.5.133
445/tcp
Mon Sep 18 16:26:38 2017
phpMyAdmin Configuration File PHP Code Injection Vulnerability
7.5 (High)
80%
192.168.5.133
80/tcp
Mon Sep 18 16:26:37 2017
Check for rexecd Service
10.0 (High)
80%
192.168.5.133
512/tcp
Mon Sep 18 16:26:35 2017
PostgreSQL PL/Perl and PL/Tcl Local Privilege Escalation Vulnerability
6.0 (Medium)
80%
192.168.5.133
5432/tcp
Mon Sep 18 16:26:35 2017
√Apply to page contents
(Applied filter: first=41 rows=10 min_qod=70 apply_overrides=1 autofp=0 sort-reverse=created)
41 - 50 of 158
Backend operation: 0.14s
Greenbone Security Assistant (GSA) Copyright 2009-2016 by Greenbone Networks GmbH, www.greenbone.net

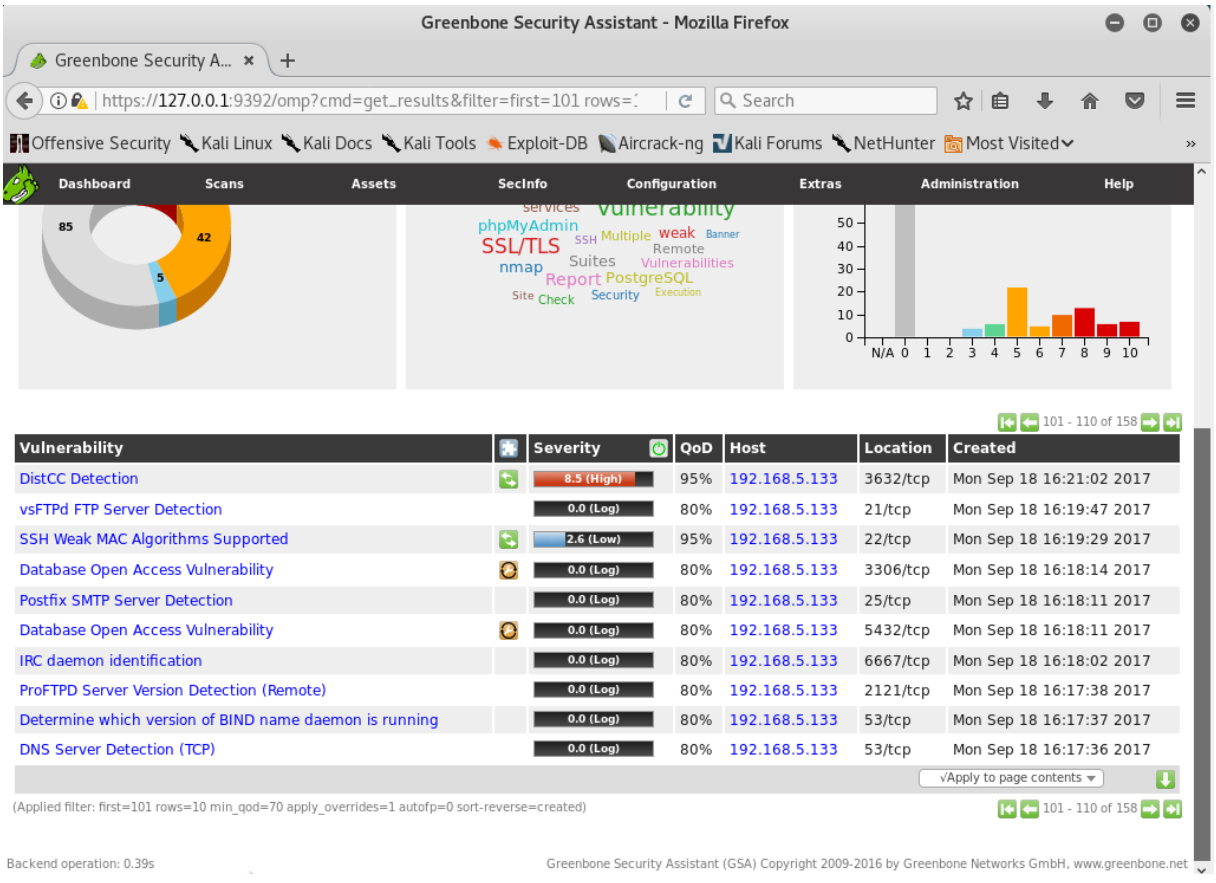

Greenbone Security Assistant - Mozilla Firefox
Greenbone Security A...
https://127.0.0.1:9392/omp?cmd=get_results&filter=first=51 rows=1(
Search
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Most Visited
Dashboard
Scans
Assets
SecInfo
Configuration
Extras
Administration
Help
51 - 60 of 158
Vulnerability
Severity
QoD
Host
Location
Created
phpMyAdmin BLOB Streaming Multiple Input Validation Vulnerabilities
7.5 (High)
80%
192.168.5.133
80/tcp
Mon Sep 18 16:26:29 2017
SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)
4.3 (Medium)
80%
192.168.5.133
25/tcp
Mon Sep 18 16:26:28 2017
phpMyAdmin Unspecified SQL Injection and Cross Site Scripting Vulnerabilities
7.5 (High)
80%
192.168.5.133
80/tcp
Mon Sep 18 16:26:26 2017
/doc directory browsable
5.0 (Medium)
80%
192.168.5.133
80/tcp
Mon Sep 18 16:26:26 2017
SSL/TLS: Hostname discovery from server certificate
0.0 (Log)
98%
192.168.5.133
general/tcp
Mon Sep 18 16:26:21 2017
phpMyAdmin Multiple Cross Site Scripting Vulnerabilities
4.3 (Medium)
80%
192.168.5.133
80/tcp
Mon Sep 18 16:26:16 2017
SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites
0.0 (Log)
98%
192.168.5.133
25/tcp
Mon Sep 18 16:26:13 2017
SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites
0.0 (Log)
98%
192.168.5.133
5432/tcp
Mon Sep 18 16:26:12 2017
Microsoft Windows SMB Accessible Shares
0.0 (Log)
80%
192.168.5.133
445/tcp
Mon Sep 18 16:26:08 2017
phpMyAdmin Database Search Cross Site Scripting Vulnerability
4.3 (Medium)
80%
192.168.5.133
80/tcp
Mon Sep 18 16:26:08 2017
√Apply to page contents
(Applied filter: first=51 rows=10 min_qod=70 apply_overrides=1 autofp=0 sort-reverse=created)
51 - 60 of 158

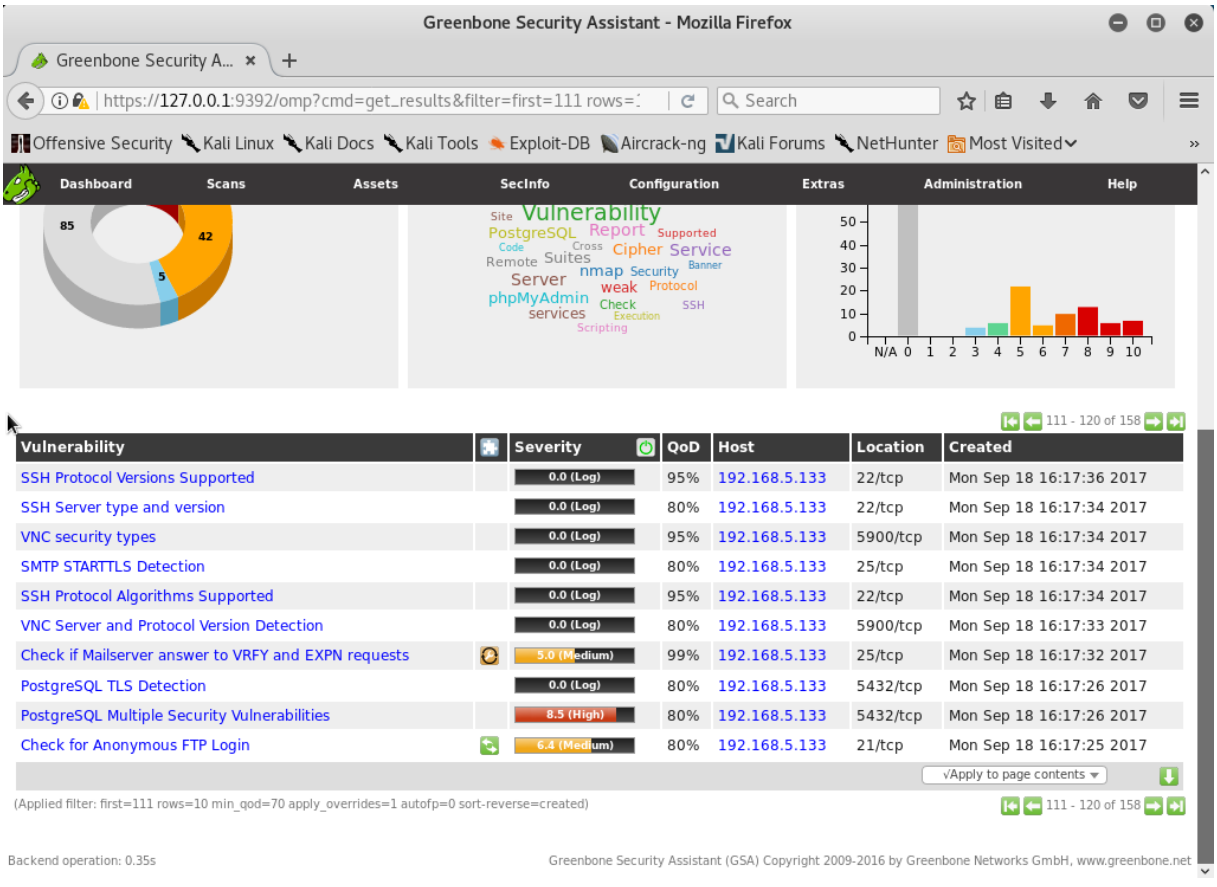

Greenbone Security Assistant - Mozilla Firefox
Greenbone Security A...
https://127.0.0.1:9392/omp?cmd=get_results&filter=first=61 rows=1(
Search
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Most Visited
Dashboard
Scans
Assets
SecInfo
Configuration
Extras
Administration
Help
phpMyAdmin
Execution
Banner
10
0
N/A 0 1 2 3 4 5 6 7 8 9 10
61 - 70 of 158
Vulnerability
Severity
QoD
Host
Location
Created
SSL/TLS: Certificate Expired
5.0 (Medium)
98%
192.168.5.133
5432/tcp
Mon Sep 18 16:26:06 2017
SSL/TLS: Certificate Expired
5.0 (Medium)
98%
192.168.5.133
25/tcp
Mon Sep 18 16:26:05 2017
SSL/TLS: Report Non Weak Cipher Suites
0.0 (Log)
98%
192.168.5.133
5432/tcp
Mon Sep 18 16:25:54 2017
SSL/TLS: Report Non Weak Cipher Suites
0.0 (Log)
98%
192.168.5.133
25/tcp
Mon Sep 18 16:25:54 2017
PostgreSQL NULL Character CA SSL Certificate Validation Security Bypass Vulnerability
6.5 (Medium)
80%
192.168.5.133
5432/tcp
Mon Sep 18 16:25:47 2017
UnrealIRCd Local Privilege Escalation Vulnerability
2.1 (Low)
80%
192.168.5.133
6667/tcp
Mon Sep 18 16:25:45 2017
PostgreSQL Hash Table Integer Overflow Vulnerability
3.5 (Low)
80%
192.168.5.133
5432/tcp
Mon Sep 18 16:25:43 2017
PostgreSQL Conversion Encoding Remote Denial of Service Vulnerability
4.0 (Medium)
80%
192.168.5.133
5432/tcp
Mon Sep 18 16:25:42 2017
SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection
4.3 (Medium)
98%
192.168.5.133
25/tcp
Mon Sep 18 16:25:40 2017
SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection
4.3 (Medium)
98%
192.168.5.133
5432/tcp
Mon Sep 18 16:25:39 2017
√Apply to page contents

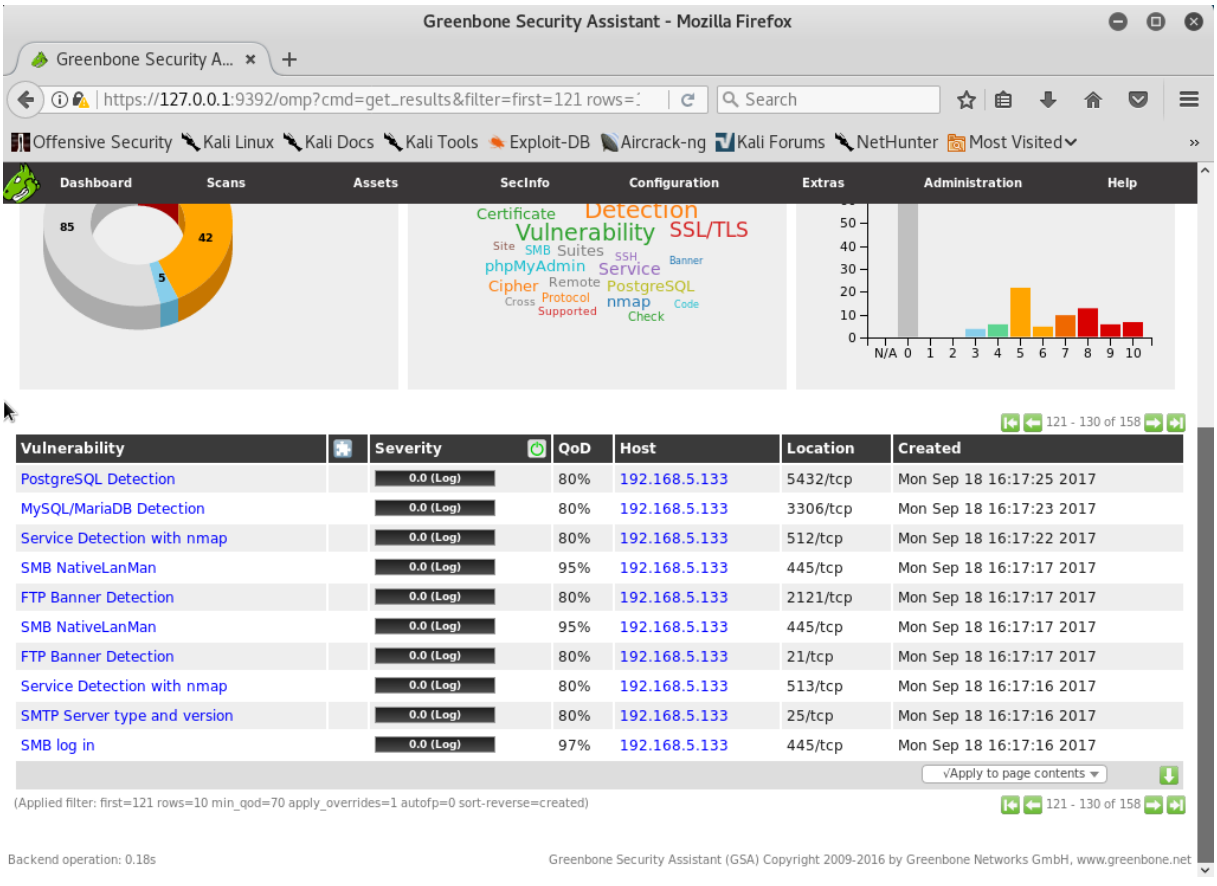

Greenbone Security Assistant - Mozilla Firefox
Greenbone Security A...
https://127.0.0.1:9392/omp?cmd=get_results&filter=first=71 rows=1(
Search
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Most Visited
Dashboard
Scans
Assets
SecInfo
Configuration
Extras
Administration
Help
71 - 80 of 158
Vulnerability
Severity
QoD
Host
Location
Created
PostgreSQL Low Cost Function Information Disclosure Vulnerability
2.1 (Low)
80%
192.168.5.133
5432/tcp
Mon Sep 18 16:25:38 2017
UnrealIRCd Authentication Spoofing Vulnerability
6.8 (Medium)
80%
192.168.5.133
6667/tcp
Mon Sep 18 16:25:37 2017
UnrealIRCd Detection
0.0 (Log)
80%
192.168.5.133
6667/tcp
Mon Sep 18 16:25:35 2017
PostgreSQL 'RESET ALL' Unauthorized Access Vulnerability
5.5 (Medium)
80%
192.168.5.133
5432/tcp
Mon Sep 18 16:25:34 2017
SSL/TLS: Report Supported Cipher Suites
0.0 (Log)
98%
192.168.5.133
25/tcp
Mon Sep 18 16:25:30 2017
SSL/TLS: Report Supported Cipher Suites
0.0 (Log)
98%
192.168.5.133
5432/tcp
Mon Sep 18 16:25:28 2017
Tiki Wiki CMS Groupware < 4.2 Multiple Unspecified Vulnerabilities
7.5 (High)
80%
192.168.5.133
80/tcp
Mon Sep 18 16:25:21 2017
CGI Scanning Consolidation
0.0 (Log)
80%
192.168.5.133
80/tcp
Mon Sep 18 16:25:17 2017
http TRACE XSS attack
5.8 (Medium)
99%
192.168.5.133
80/tcp
Mon Sep 18 16:25:06 2017
phpMyAdmin Debug Backtrace Cross Site Scripting Vulnerability
4.3 (Medium)
80%
192.168.5.133
80/tcp
Mon Sep 18 16:25:06 2017
Apply to page contents
(Applied filter: first=71 rows=10 min_qod=70 apply_overrides=1 autofp=0 sort-reverse=created)
71 - 80 of 158
Backend operation: 0.34s
Greenbone Security Assistant (GSA) Copyright 2009-2016 by Greenbone Networks GmbH, www.greenbone.net

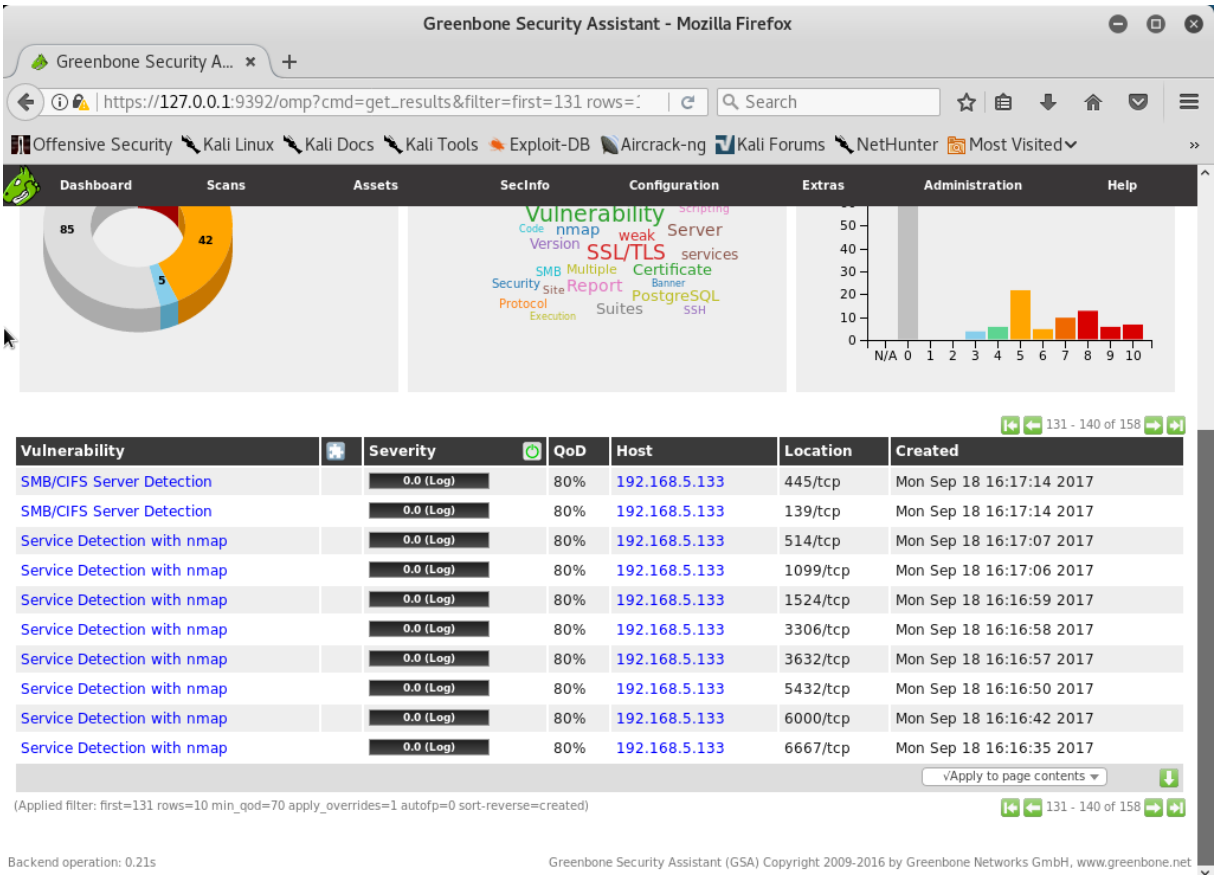

Greenbone Security Assistant - Mozilla Firefox
Greenbone Security A...
https://127.0.0.1:9392/omp?cmd=get_results&filter=first=81 rows=1(
Search
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Most Visited
Dashboard
Scans
Assets
SecInfo
Configuration
Extras
Administration
Help
Log
81 - 90 of 158
Vulnerability
Severity
QoD
Host
Location
Created
TWiki Cross-Site Request Forgery Vulnerability - Sep10
6.8 (Medium)
80%
192.168.5.133
80/tcp
Mon Sep 18 16:25:03 2017
TWiki Version Detection
0.0 (Log)
80%
192.168.5.133
80/tcp
Mon Sep 18 16:25:00 2017
phpMyAdmin Detection
0.0 (Log)
80%
192.168.5.133
80/tcp
Mon Sep 18 16:24:56 2017
PHP Version Detection (Remote)
0.0 (Log)
80%
192.168.5.133
80/tcp
Mon Sep 18 16:24:54 2017
phpinfo() output accessible
7.5 (High)
80%
192.168.5.133
80/tcp
Mon Sep 18 16:24:53 2017
OS Detection Consolidation and Reporting
0.0 (Log)
80%
192.168.5.133
general/tcp
Mon Sep 18 16:24:51 2017
Apache Web Server Version Detection
0.0 (Log)
80%
192.168.5.133
80/tcp
Mon Sep 18 16:24:48 2017
Tiki Wiki CMS Groupware Version Detection
0.0 (Log)
80%
192.168.5.133
80/tcp
Mon Sep 18 16:24:48 2017
Check for rsh Service
7.5 (High)
80%
192.168.5.133
514/tcp
Mon Sep 18 16:24:45 2017
HTTP Server type and version
0.0 (Log)
80%
192.168.5.133
80/tcp
Mon Sep 18 16:24:27 2017
Apply to page contents

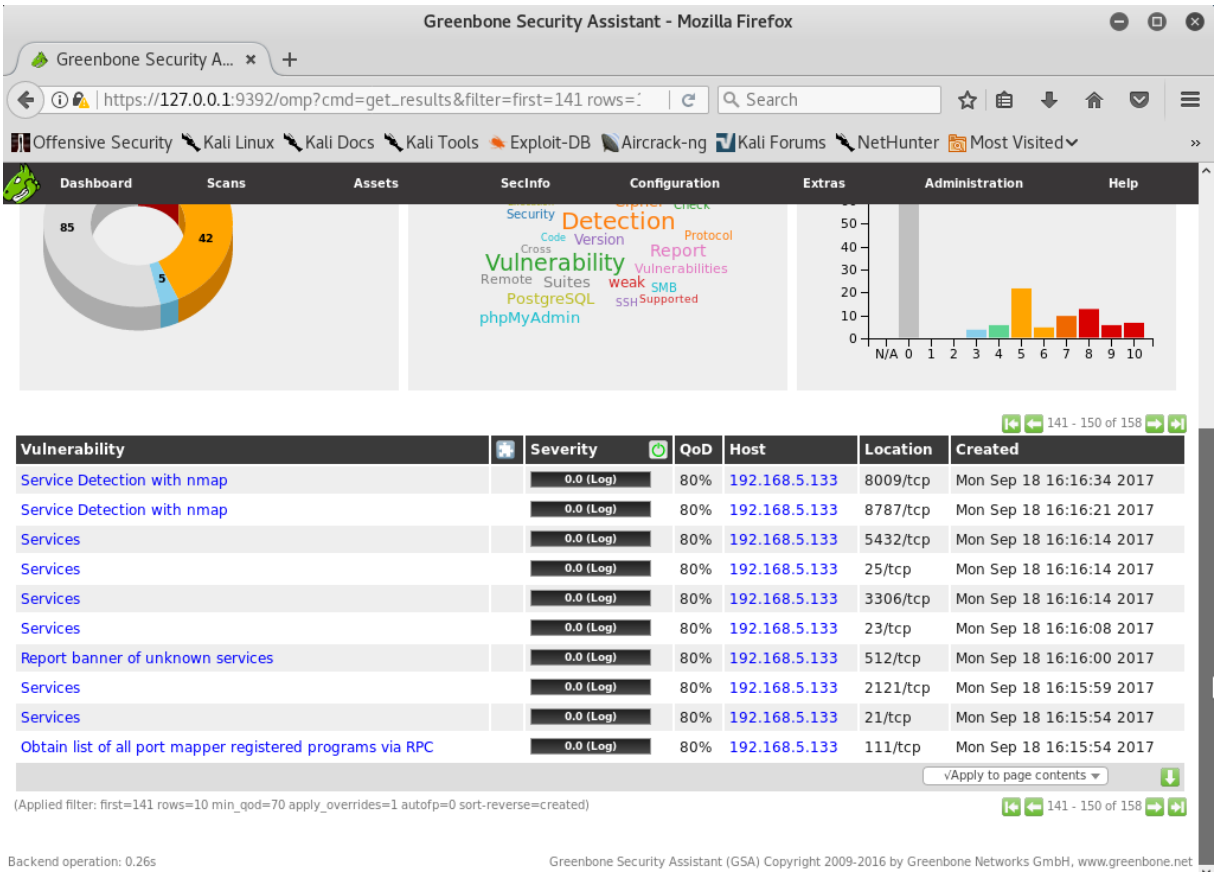

Greenbone Security Assistant - Mozilla Firefox
Greenbone Security A...
https://127.0.0.1:9392/omp?cmd=get_results&filter=first=91 rows=1(
Search
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Most Visited
Dashboard
Scans
Assets
SecInfo
Configuration
Extras
Administration
Help
Execution
Check
10
0
N/A 0 1 2 3 4 5 6 7 8 9 10
91 - 100 of 158
Vulnerability
Severity
QoD
Host
Location
Created
SSL/TLS: Collect and Report Certificate Details
0.0 (Log)
98%
192.168.5.133
5432/tcp
Mon Sep 18 16:24:27 2017
PostgreSQL Multiple Security Vulnerabilities
6.8 (Medium)
80%
192.168.5.133
5432/tcp
Mon Sep 18 16:24:27 2017
SSL/TLS: Collect and Report Certificate Details
0.0 (Log)
98%
192.168.5.133
25/tcp
Mon Sep 18 16:24:17 2017
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability
4.0 (Medium)
80%
192.168.5.133
25/tcp
Mon Sep 18 16:23:27 2017
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability
4.0 (Medium)
80%
192.168.5.133
5432/tcp
Mon Sep 18 16:23:16 2017
SSL/TLS: Report Medium Cipher Suites
0.0 (Log)
98%
192.168.5.133
25/tcp
Mon Sep 18 16:23:16 2017
SSL/TLS: 'DHE_EXPORT' Man in the Middle Security Bypass Vulnerability (LogJam)
4.3 (Medium)
80%
192.168.5.133
25/tcp
Mon Sep 18 16:23:10 2017
SSL/TLS: Report Medium Cipher Suites
0.0 (Log)
98%
192.168.5.133
5432/tcp
Mon Sep 18 16:23:10 2017
PostgreSQL 'intarray' Module 'gettoken()' Buffer Overflow Vulnerability
6.5 (Medium)
80%
192.168.5.133
5432/tcp
Mon Sep 18 16:23:09 2017
X Server
0.0 (Log)
80%
192.168.5.133
general/tcp
Mon Sep 18 16:21:34 2017
√Apply to page contents

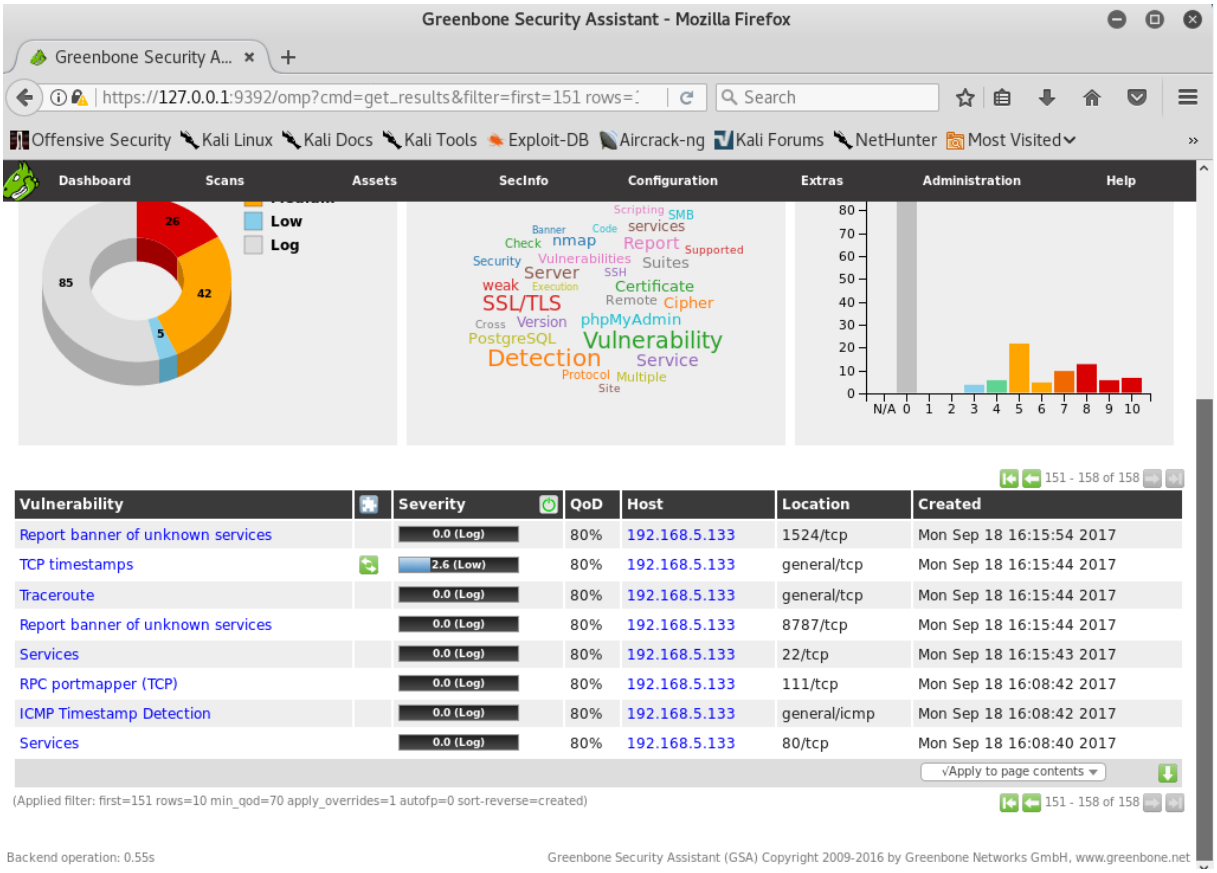

Greenbone Security Assistant - Mozilla Firefox
Greenbone Security A...
https://127.0.0.1:9392/omp?cmd=get_results&filter=first=101 rows=1
Search
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Most Visited
Dashboard
Scans
Assets
SecInfo
Configuration
Extras
Administration
Help
85
42
5
services
Vulnerability
phpMyAdmin
SSH
Multiple
weak
Banner
SSL/TLS
Remote
nmap
Suites
Vulnerabilities
Report
PostgreSQL
Site
Check
Security
Execution
50
40
30
20
10
0
N/A 0 1 2 3 4 5 6 7 8 9 10
101 - 110 of 158
Vulnerability
Severity
QoD
Host
Location
Created
DistCC Detection
8.5 (High)
95%
192.168.5.133
3632/tcp
Mon Sep 18 16:21:02 2017
vsFTPd FTP Server Detection
0.0 (Log)
80%
192.168.5.133
21/tcp
Mon Sep 18 16:19:47 2017
SSH Weak MAC Algorithms Supported
2.6 (Low)
95%
192.168.5.133
22/tcp
Mon Sep 18 16:19:29 2017
Database Open Access Vulnerability
0.0 (Log)
80%
192.168.5.133
3306/tcp
Mon Sep 18 16:18:14 2017
Postfix SMTP Server Detection
0.0 (Log)
80%
192.168.5.133
25/tcp
Mon Sep 18 16:18:11 2017
Database Open Access Vulnerability
0.0 (Log)
80%
192.168.5.133
5432/tcp
Mon Sep 18 16:18:11 2017
IRC daemon identification
0.0 (Log)
80%
192.168.5.133
6667/tcp
Mon Sep 18 16:18:02 2017
ProFTPD Server Version Detection (Remote)
0.0 (Log)
80%
192.168.5.133
2121/tcp
Mon Sep 18 16:17:38 2017
Determine which version of BIND name daemon is running
0.0 (Log)
80%
192.168.5.133
53/tcp
Mon Sep 18 16:17:37 2017
DNS Server Detection (TCP)
0.0 (Log)
80%
192.168.5.133
53/tcp
Mon Sep 18 16:17:36 2017
√Apply to page contents
(Applied filter: first=101 rows=10 min_qod=70 apply_overrides=1 autofp=0 sort-reverse=created)
101 - 110 of 158
Backend operation: 0.39s
Greenbone Security Assistant (GSA) Copyright 2009-2016 by Greenbone Networks GmbH, www.greenbone.net


Greenbone Security Assistant - Mozilla Firefox
Greenbone Security A...
https://127.0.0.1:9392/omp?cmd=get_results&filter=first=111 rows=
Search
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Most Visited
Dashboard
Scans
Assets
SecInfo
Configuration
Extras
Administration
Help
111 - 120 of 158
Vulnerability
Severity
QoD
Host
Location
Created
SSH Protocol Versions Supported
0.0 (Log)
95%
192.168.5.133
22/tcp
Mon Sep 18 16:17:36 2017
SSH Server type and version
0.0 (Log)
80%
192.168.5.133
22/tcp
Mon Sep 18 16:17:34 2017
VNC security types
0.0 (Log)
95%
192.168.5.133
5900/tcp
Mon Sep 18 16:17:34 2017
SMTP STARTTLS Detection
0.0 (Log)
80%
192.168.5.133
25/tcp
Mon Sep 18 16:17:34 2017
SSH Protocol Algorithms Supported
0.0 (Log)
95%
192.168.5.133
22/tcp
Mon Sep 18 16:17:34 2017
VNC Server and Protocol Version Detection
0.0 (Log)
80%
192.168.5.133
5900/tcp
Mon Sep 18 16:17:33 2017
Check if Mailserver answer to VRFY and EXPN requests
5.0 (Medium)
99%
192.168.5.133
25/tcp
Mon Sep 18 16:17:32 2017
PostgreSQL TLS Detection
0.0 (Log)
80%
192.168.5.133
5432/tcp
Mon Sep 18 16:17:26 2017
PostgreSQL Multiple Security Vulnerabilities
8.5 (High)
80%
192.168.5.133
5432/tcp
Mon Sep 18 16:17:26 2017
Check for Anonymous FTP Login
6.4 (Medium)
80%
192.168.5.133
21/tcp
Mon Sep 18 16:17:25 2017
Apply to page contents
(Applied filter: first=111 rows=10 min_qod=70 apply_overrides=1 autofp=0 sort-reverse=created)
111 - 120 of 158
Backend operation: 0.35s
Greenbone Security Assistant (GSA) Copyright 2009-2016 by Greenbone Networks GmbH, www.greenbone.net


Greenbone Security Assistant - Mozilla Firefox
Greenbone Security A...
https://127.0.0.1:9392/omp?cmd=get_results&filter=first=121 rows=
Search
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Most Visited
Dashboard
Scans
Assets
SecInfo
Configuration
Extras
Administration
Help
121 - 130 of 158
Vulnerability
Severity
QoD
Host
Location
Created
PostgreSQL Detection
0.0 (Log)
80%
192.168.5.133
5432/tcp
Mon Sep 18 16:17:25 2017
MySQL/MariaDB Detection
0.0 (Log)
80%
192.168.5.133
3306/tcp
Mon Sep 18 16:17:23 2017
Service Detection with nmap
0.0 (Log)
80%
192.168.5.133
512/tcp
Mon Sep 18 16:17:22 2017
SMB NativeLanMan
0.0 (Log)
95%
192.168.5.133
445/tcp
Mon Sep 18 16:17:17 2017
FTP Banner Detection
0.0 (Log)
80%
192.168.5.133
2121/tcp
Mon Sep 18 16:17:17 2017
SMB NativeLanMan
0.0 (Log)
95%
192.168.5.133
445/tcp
Mon Sep 18 16:17:17 2017
FTP Banner Detection
0.0 (Log)
80%
192.168.5.133
21/tcp
Mon Sep 18 16:17:17 2017
Service Detection with nmap
0.0 (Log)
80%
192.168.5.133
513/tcp
Mon Sep 18 16:17:16 2017
SMTP Server type and version
0.0 (Log)
80%
192.168.5.133
25/tcp
Mon Sep 18 16:17:16 2017
SMB log in
0.0 (Log)
97%
192.168.5.133
445/tcp
Mon Sep 18 16:17:16 2017
Apply to page contents
(Applied filter: first=121 rows=10 min_qod=70 apply_overrides=1 autofp=0 sort-reverse=created)
121 - 130 of 158
Backend operation: 0.18s
Greenbone Security Assistant (GSA) Copyright 2009-2016 by Greenbone Networks GmbH, www.greenbone.net


Greenbone Security Assistant - Mozilla Firefox
Greenbone Security A...
https://127.0.0.1:9392/omp?cmd=get_results&filter=first=131 rows=
Search
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Most Visited
Dashboard
Scans
Assets
SecInfo
Configuration
Extras
Administration
Help
85
42
5
Vulnerability
nmap
weak
Server
Version
SSL/TLS
services
SMB
Multiple
Certificate
Security
Site
Report
Banner
PostgreSQL
Protocol
Suites
SSH
Execution
N/A 0 1 2 3 4 5 6 7 8 9 10
131 - 140 of 158
Vulnerability
Severity
QoD
Host
Location
Created
SMB/CIFS Server Detection
0.0 (Log)
80%
192.168.5.133
445/tcp
Mon Sep 18 16:17:14 2017
SMB/CIFS Server Detection
0.0 (Log)
80%
192.168.5.133
139/tcp
Mon Sep 18 16:17:14 2017
Service Detection with nmap
0.0 (Log)
80%
192.168.5.133
514/tcp
Mon Sep 18 16:17:07 2017
Service Detection with nmap
0.0 (Log)
80%
192.168.5.133
1099/tcp
Mon Sep 18 16:17:06 2017
Service Detection with nmap
0.0 (Log)
80%
192.168.5.133
1524/tcp
Mon Sep 18 16:16:59 2017
Service Detection with nmap
0.0 (Log)
80%
192.168.5.133
3306/tcp
Mon Sep 18 16:16:58 2017
Service Detection with nmap
0.0 (Log)
80%
192.168.5.133
3632/tcp
Mon Sep 18 16:16:57 2017
Service Detection with nmap
0.0 (Log)
80%
192.168.5.133
5432/tcp
Mon Sep 18 16:16:50 2017
Service Detection with nmap
0.0 (Log)
80%
192.168.5.133
6000/tcp
Mon Sep 18 16:16:42 2017
Service Detection with nmap
0.0 (Log)
80%
192.168.5.133
6667/tcp
Mon Sep 18 16:16:35 2017
√Apply to page contents
(Applied filter: first=131 rows=10 min_qod=70 apply_overrides=1 autofp=0 sort-reverse=created)
131 - 140 of 158
Backend operation: 0.21s
Greenbone Security Assistant (GSA) Copyright 2009-2016 by Greenbone Networks GmbH, www.greenbone.net


Greenbone Security Assistant - Mozilla Firefox
Greenbone Security A...
https://127.0.0.1:9392/omp?cmd=get_results&filter=first=141 rows=
Search
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Most Visited
Dashboard
Scans
Assets
SecInfo
Configuration
Extras
Administration
Help
85
42
5
Security
Detection
Code
Version
Protocol
Cross
Report
Vulnerability
Vulnerabilities
Remote
Suites
weak
SMB
PostgreSQL
SSH
Supported
phpMyAdmin
N/A 0 1 2 3 4 5 6 7 8 9 10
141 - 150 of 158
Vulnerability
Severity
QoD
Host
Location
Created
Service Detection with nmap
0.0 (Log)
80%
192.168.5.133
8009/tcp
Mon Sep 18 16:16:34 2017
Service Detection with nmap
0.0 (Log)
80%
192.168.5.133
8787/tcp
Mon Sep 18 16:16:21 2017
Services
0.0 (Log)
80%
192.168.5.133
5432/tcp
Mon Sep 18 16:16:14 2017
Services
0.0 (Log)
80%
192.168.5.133
25/tcp
Mon Sep 18 16:16:14 2017
Services
0.0 (Log)
80%
192.168.5.133
3306/tcp
Mon Sep 18 16:16:14 2017
Services
0.0 (Log)
80%
192.168.5.133
23/tcp
Mon Sep 18 16:16:08 2017
Report banner of unknown services
0.0 (Log)
80%
192.168.5.133
512/tcp
Mon Sep 18 16:16:00 2017
Services
0.0 (Log)
80%
192.168.5.133
2121/tcp
Mon Sep 18 16:15:59 2017
Services
0.0 (Log)
80%
192.168.5.133
21/tcp
Mon Sep 18 16:15:54 2017
Obtain list of all port mapper registered programs via RPC
0.0 (Log)
80%
192.168.5.133
111/tcp
Mon Sep 18 16:15:54 2017
√Apply to page contents
(Applied filter: first=141 rows=10 min_qod=70 apply_overrides=1 autofp=0 sort-reverse=created)
141 - 150 of 158
Backend operation: 0.26s
Greenbone Security Assistant (GSA) Copyright 2009-2016 by Greenbone Networks GmbH, www.greenbone.net


Greenbone Security Assistant - Mozilla Firefox
Greenbone Security A...
https://127.0.0.1:9392/omp?cmd=get_results&filter=first=151 rows=
Search
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Most Visited
Dashboard
Scans
Assets
SecInfo
Configuration
Extras
Administration
Help
Low
Log
26
85
42
5
Scripting
SMB
Banner
Code
services
Check
nmap
Report
Supported
Security
Vulnerabilities
Suites
Server
SSH
weak
Execution
Certificate
SSL/TLS
Remote
Cipher
Cross
Version
phpMyAdmin
PostgreSQL
Vulnerability
Detection
Service
Protocol
Multiple
Site
80
70
60
50
40
30
20
10
0
N/A 0 1 2 3 4 5 6 7 8 9 10
151 - 158 of 158
Vulnerability
Severity
QoD
Host
Location
Created
Report banner of unknown services
0.0 (Log)
80%
192.168.5.133
1524/tcp
Mon Sep 18 16:15:54 2017
TCP timestamps
2.6 (Low)
80%
192.168.5.133
general/tcp
Mon Sep 18 16:15:44 2017
Traceroute
0.0 (Log)
80%
192.168.5.133
general/tcp
Mon Sep 18 16:15:44 2017
Report banner of unknown services
0.0 (Log)
80%
192.168.5.133
8787/tcp
Mon Sep 18 16:15:44 2017
Services
0.0 (Log)
80%
192.168.5.133
22/tcp
Mon Sep 18 16:15:43 2017
RPC portmapper (TCP)
0.0 (Log)
80%
192.168.5.133
111/tcp
Mon Sep 18 16:08:42 2017
ICMP Timestamp Detection
0.0 (Log)
80%
192.168.5.133
general/icmp
Mon Sep 18 16:08:42 2017
Services
0.0 (Log)
80%
192.168.5.133
80/tcp
Mon Sep 18 16:08:40 2017
√Apply to page contents
(Applied filter: first=151 rows=10 min_qod=70 apply_overrides=1 autofp=0 sort-reverse=created)
151 - 158 of 158
Backend operation: 0.55s
Greenbone Security Assistant (GSA) Copyright 2009-2016 by Greenbone Networks GmbH, www.greenbone.net