

ANALIZA SIGURNOSTI JAVNIH DNS POSLUŽITELJA

Torbar, Josip

Undergraduate thesis / Završni rad

2023

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **Algebra University College / Visoko učilište Algebra**

Permanent link / Trajna poveznica: <https://um.nsk.hr/um:nbn:hr:225:468509>

Rights / Prava: [In copyright](#)/[Zaštićeno autorskim pravom.](#)

Download date / Datum preuzimanja: **2024-07-28**



Repository / Repozitorij:

[Algebra University - Repository of Algebra University](#)



VISOKO UČILIŠTE ALGEBRA

ZAVRŠNI RAD

**ANALIZA SIGURNOSTI JAVNIH DNS
POSLUŽITELJA**

Josip Torbar

Zagreb, veljača 2023.

Predgovor

U predgovoru bi htio zahvaliti svim osobama koje su bile dio mog studija, posebice profesorima Zlatanu Moriću, Vedranu Dakiću i Jasminu Redžepagiću. Hvala vam što ste me naučili razmišljati na drugačiji način. Također bih se htio zahvaliti svojoj obitelji koja mi je pružala podršku tokom tog procesa. Hvala vam na svemu što ste mi pružili tokom mog studija. Ovaj rad posvećujem svojoj baki.

Sažetak

Sustav domenskih imena (DNS) kritična je komponenta interneta koja pretvara adrese računala u ljudima pamtljiva imena. DNS ima dugu povijest koja datira do ranih dana interneta, kada se jednostavna tablica hostova koristila u te svrhe. S vremenom se ovaj sustav razvio u ogromnu distribuiranu bazu podataka koja je postala neophodna za funkcioniranje interneta. Razvitkom interneta i porastom kibernetičkih prijetnji, sigurnost DNS-a postala je od kritične važnosti za održavanje njegove stabilnosti. Kako bi se podigla razina sigurnost DNS-a, implementirane su razne sigurnosne mjere od kojih su neke obrađene u ovome radu.

The Domain Name System (DNS) is a critical component of the Internet that converts computer addresses into humanly memorable names. DNS has a long history dating back to the early days of the Internet, when a simple host file was used for this purpose. Over time, this system developed into a huge, distributed database that became essential for the functioning of the Internet. With the development of the Internet and the rise of cyber threats, DNS security has become critical to maintaining its stability. In order to raise the level of DNS security, various security measures have been implemented, some of which are discussed in this paper.

Ključne riječi: DNS, TCP/IP, ARPANET, DNS, Kibernetička sigurnost, DNSSEC.

Sadržaj

1.	Uvod	1
2.	Povijest DNS-a	2
2.1.	ARPANET	2
2.2.	TCP/IP	4
2.3.	DNS - Sustav domenskih imena	5
3.	DNS ranjivosti	8
3.1.	Lažiranje/Trovanje DNS-a	8
3.2.	Napadi uskraćivanja usluge	9
3.3.	DNS tuneliranje	10
4.	Sigurnosne mjere za zaštitu DNS-a	13
4.1.	Liste za kontrolu pristupa (ACLOvi)	13
4.2.	Šifriranje DNS zahtjeva	14
4.2.1.	DNSSEC	14
4.2.2.	DNS-over-HTTPS (DoH) i DNS-over-TLS (DoT)	16
4.3.	DNS vatrozid	17
4.4.	DNS sigurnosne politike i revizije	18
5.	Implementacija DNS servisa	20
5.1.	Konfiguracija infrastrukture u oblaku	20
5.2.	Konfiguracija BIND DNS servisa	26
6.	Analiza razine sigurnosti implementiranog DNS rješenja	36
6.1.	Testiranje prijenosa datoteka DNS zona	36
6.2.	Testiranje DNS razlučivanja	37
6.3.	Testiranje DNSSEC funkcionalnosti	39

Zaključak	44
Popis kratica	46
Popis slika.....	48
Popis tablica.....	49
Popis kôdova	Pogreška! Knjižna oznaka nije definirana.
Literatura	50

1. Uvod

Sustav domenskih imena (kasnije u tekstu: DNS) ključna je komponenta interneta koja korisnicima omogućuje pristup web stranicama i drugim mrežnim resursima koristeći imena domena koja se lako pamte. Međutim, kao i svaki sustav koji rukuje osjetljivim informacijama, DNS je ranjiv na razne sigurnosne prijetnje koje mogu ugroziti njegov integritet i dostupnost. Iz tog razloga bitno je primijeniti snažne sigurnosne mjere za zaštitu DNS-a od zlonamjernih napada.

Cilj ovog rada je podizanje svijesti o važnosti sigurnosti i zaštite DNS-a.. Konkretno, ovaj rad pokriva povijest DNS-a, njegovo porijeklo i razvoj raznih popratnih protokola. Nakon toga su ispitane uobičajene ranjivosti DNS-a, kao što su lažiranje/trovanje DNS-a, napadi uskraćivanja usluge i DNS tuneliranje, te su obrađene neke od sigurnosnih mjera koje se mogu koristiti za zaštitu DNS-a. Te mjere uključuju liste kontrole pristupa, šifriranje, DNS vatrozid i sigurnosna politike i revizije. U radu će se također pokriti implementacija DNS servisa, uključujući konfiguraciju infrastrukture oblaka i konfiguraciju BIND DNS servisa. Konačno, uključit će analizu razine sigurnosti implementiranog DNS rješenja, uključujući testiranje razlučivosti DNS-a i DNSSEC funkcionalnosti.

2. Povijest DNS-a

U ovom poglavlju razrađene su teme ARPANET-a, TCP/IP-a i DNS-a. Te tri tehnologije odigrale su ključnu ulogu u razvoju interneta. ARPANET je bila jedna od prvih operativnih mreža za komutaciju paketa i preteča samog interneta. Tu mrežu je razvilo Ministarstvo obrane Sjedinjenih Američkih Država kasnih 1960-ih i ranih 1970-ih, a korištena je prvenstveno za razna istraživanja i eksperimente. Zatim, kao komunikacijski protokol za ARPANET razvijen je TCP/IP. On je osmišljen kako bi pružio standardiziranu metodu za prijenos podataka između različitih vrsta računalnih sustava. TCP/IP postao je okosnica internetske komunikacije te je usvojen kao standard za sve računalne sustave povezane putem internetskog protokola (IP). DNS je razvijen kao rješenje problema sve većeg broj računala povezanih na internet.

2.1. ARPANET

1957. godine Sovjetski Savez je uspješno lansirao Sputnik 1, te je SAD shvatio da su Sovjeti razvili sposobnost veoma brzog razvoja vojne tehnologije. Uspješno lansiranje bilo je šok za stručnjake i građane u Sjedinjenim Državama, koji su se nadali da će oni prvi postići ovaj znanstveni napredak. Činjenica da su Sovjeti bili uspješni potaknula je strahove da je američka vojska općenito zaostala u razvoju nove tehnologije. Tadašnji Američki predsjednik Eisenhower 1958. odobrio je Ministarstvu obrane stvaranje Agencije za napredne istraživačke projekte (ARPA) kako bi ubrzali razvoj vojne tehnologije. 1969. godine ARPA-in Ured za tehnike obrade informacija (IPTO) financirao je 4 sveučilišta u SAD-u kako bi razvili učinkovitu mrežu računala koja omogućava brzu razmjenu informacija između geografski udaljenih lokacija. Razvojem te mreže značajno se poboljšala razmjena informacija o znanstvenim istraživanjima i radovima između tih sveučilišta te su samim time ubrzali znanstveni napredak cijele nacije. J.C.R. Licklider, profesor s MIT-a, je u više svojih dopisa (RFC) spominjao koncept „Galaktičke mreže“. (Licklider, 1965.) U tim dopisima njegova vizija računalnih mreža bila je u mnogočemu slična današnjem internetu. Bob Taylor 1966. na temelju Lickliderovih dopisa dobiva

odobrenje direktora ARPA-e za početak programa ARPANET. Kao voditelja projekta postavio je Larryja Robertsa.

ARPANET je bio mreža računalnih terminala koji mogu međusobno komunicirati i razmjenjivati informacije. Ta mreža je preteča svih današnjih računalnih mreža zbog čega se često i naziva „začetkom svih mreža“. ARPANET se u početku sastojao od iznajmljenih međugradskih telefonskih linija i paketnih preklopnika na koje su bila povezana računala. Takva arhitektura omogućila je računalu da s jedne lokacije putem paketnog preklopnika komunicira s računalom na drugoj, udaljenoj lokaciji, koje je isto tako spojeno na preklopnik. 29. listopada 1969. godine prvi je put uspješno uspostavljena veza između dva računala putem ARPANET mreže. Bill Duvall, programer s Istraživačkog instituta Stanford (SRI) i student Sveučilišta u Kaliforniji Charley Kline toga su dana povezali računala SDS Sigma 7 (UCLA) sa SDS 940 (SRI). Prva stalna ARPANET veza uspostavljena je 21. studenog između ta dva čvorišta, a 5. prosinca uspostavljena je prva mreža s četiri čvora (Slika 2.1).



The ARPANET in December 1969

Slika 2.1 Čvorovi ARPANETa u prosincu 1969. Godine (TechTarget Arpanet Definition)

Već na samom početku ARPANET-a pojavio se problem u uspostavljanju mrežne komunikacije između većeg broja računala. Svako računalo se služilo zasebnim programskim jezikom te je stoga prvotno bilo potrebno međusobno uskladiti jezike povezanih računala kako bi međusobno mogli razmjenjivati informacije. Taj problem potaknuo je projekt za razvitak jedinstvenog načina komunikacije računala putem mreže.

2.2. TCP/IP

Dva znanstvenika ARPA-e, Vinton Cerf i Robert Kahn, 1973. su započeli istraživanje o pouzdanoj komunikaciji preko radijskih mreža po uzoru na protokol za upravljanje mrežom (NCP). Razvili su sljedeću generaciju tog protokola te ga nazvali Protokol kontrole prijenosa (TCP), koji se koristi i dan danas. (Cerf, Kahn, 1974.) Tijekom razvoja TCP-a koristili su koncept kirkada, odnosno koncept mreže za komutaciju paketa koji je dizajnirao francuski znanstvenik Louis Pouzin. Koncept je zasnovan na ideji da su mrežne komponente odgovorne samo za učinkovit i brz prijenos podataka između krajnjih čvorova, dok su za integritet informacija zaduženi sami krajnji čvorovi, odnosno računala. Korištenjem tog jednostavnijeg dizajna, postalo je moguće spojiti gotovo bilo koju mrežu na ARPANET bez obzira na njene lokalne karakteristike. TCP/IP podijeljen je u četiri sloja, od kojih svaki uključuje specifične protokole, oni su sljedeći:

1. Aplikacijski sloj – sloj TCP/IP modela koji je odgovoran za pružanje usluga korisniku. Ovi protokoli pružaju potrebnu funkcionalnost za aplikacije kao što su web preglednici, klijenti e-pošte i programi za prijenos datoteka.
2. Transportni sloj – sloj odgovoran za pružanje pouzdane veze između aplikacija koje se izvode na različitim uređajima. Najčešće korišteni protokol u ovom sloju je TCP koji omogućuje provjeru i ispravljanje pogrešaka, kontrolu toka i ponovni prijenos izgubljenih paketa.
3. Mrežni sloj – ovaj sloj je odgovoran za usmjeravanje paketa podataka između različitih mreža. Najčešće korišteni protokol u ovom sloju je IP. On omogućuje usmjeravanje paketa podataka.
4. Sloj podatkovne veze – to je najniži sloj TCP/IP modela koji je odgovoran za pružanje pouzdane veze između uređaja na istoj mreži. Najčešće korišteni protokol u ovom sloju je Ethernet, koji omogućuje fizičko adresiranje (MAC adrese) i kontrolu podatkovne veze.

Godine 1975. provedeno je testiranje TCP/IP komunikacije s dvije mreže između Sveučilišta Stanford i Sveučilišta u London (UCL). Nekoliko drugih TCP/IP prototipova razvijeno je u više istraživačkih centara između 1978. i 1983. Migracija ARPANET-a na TCP/IP službeno je završena 1. siječnja 1983., kada su novi protokoli trajno aktivirani. Nakon toga je TCP/IP postao standardni komunikacijski protokol koji računala omogućuje komunikaciju s drugim računalima na velikim udaljenostima.

Internet je najbolji primjer mreže koja koristi komutaciju paketa u kojoj se informacije rastavljaju u male pakete, zatim šalju pojedinačno putem više različitih ruta u isto vrijeme, a potom ponovno sastavljaju na primateljskom kraju. TCP je komponenta koja razdvaja, šalje i ponovno sastavlja pakete podataka, dok je IP odgovoran za isporuku tih paketa na ispravno odredište.

2.3. DNS - Sustav domenskih imena

U ranim danima računalnih mreža, računala su se oslanjala na statičke, tekstualne datoteke, zvane hosts, kako bi znala poslati neku informaciju na njoj namijenjeno odredište. To su jednostavne datoteke koje sadrže popis IP adresa i njima odgovarajuće nazive računala. Kada bi korisnik htio pristupiti nekom mrežnom resursu, računalo bi potražilo ime računala u hosts datoteci i pronašlo njemu odgovarajuću IP adresu. Međutim, kako je razvoj ARPANET-a činio sustav sve kompleksnijim, hosts datoteke postajale su sve manje praktične i učinkovite. S povećanjem broja resursa dostupnih na mreži, veličina svake hosts datoteke je porasla u veličini, što je otežalo njeno održavanje i distribuciju. Osim toga, kako su novi resursi dodavani na mrežu, hosts datoteke su se morale ažurirati na svakom računalu, što je bio dugotrajan proces sklon pogreškama. Iz tih nedostataka, stvorila se potreba za centraliziranim sustavom koji će imati aktualne informacije o uređajima na mreži i njima pripadajućim IP adresama.

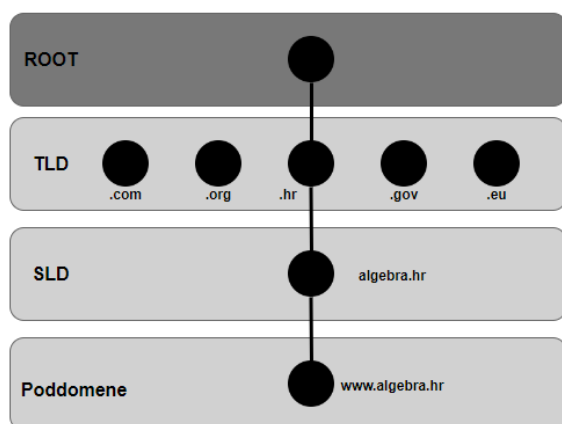
1971. godine Elizabeth Feinler stvorila je ARPANET imenički servis. ARPANET imenički servis bila je centralizirana imenička usluga koja je pratila sve resurse na ARPANET mreži. Umjesto čuvanja lokalne kopije hosts datoteke na svakom računalu, korisnici su mogli pristupiti ARPANET imeničkom servisu kako bi pronašli IP adresu bilo kojeg mrežnog resursa. ARPANET imenički servis pružio je brojne prednosti u odnosu na hosts datoteke. Prvo, bio je skalabilniji jer se središnja imenička usluga mogla ažurirati na jednom mjestu, što je olakšalo dodavanje i uklanjanje zapisa mrežnih resursa. Drugo, bio je centraliziran sustav koji je mogao pružiti više informacija o resursima na mreži (osim imena računala i IP adrese), kao što su informacije o vrsti resursa, njegovoj lokaciji i statusu. Međutim, iako je ARPANET imenički servis bio poboljšanje u odnosu na hosts datoteke ni on nije mogao pratiti brzinu razvitka ARPANET mreže, odnosno sve većeg broja povezanih računala. Oslanjao se samo na jedan centralizirani poslužitelj, koji je stvorio jednu točku kvara. Također, sustav je bio ranjiv na „uska grla“ u radu budući da je

velik broj korisnika pristupao tom jednom poslužitelju. Kao rješenje navedenih ograničenja ARPANET imeničkog servisa, razvijen je DNS.

DNS je osmislio Paul Mockapetris 1983. godine, dok je radio na Institutu informacijskih znanosti na Sveučilištu Južne Kalifornije. Mockapetris je razvio izvorni koncept DNS-a i napisao prvu implementaciju takvog sustava. Mockapetrisovo rješenje bilo je uvođenje koncepta domenskih imena, kao što je **algebra.hr**, koji se mogu koristiti za identifikaciju računala na mreži. (Mockapetris, 1987.) On je definirao hijerarhijsku strukturu imenovanja, gdje su nazivi domena organizirani u strukturu poput stabla. DNS funkcionira tako da naziv domene rastavlja na više razina ranije spomenute hijerarhije, a one su:

1. **Domena najviše razine (TLD):** TLD je najviša razina DNS hijerarhije i nalazi se u korijenu stabla. To je dio naziva domene desno od točke, kao što su **.com**, **.org** i **.edu**. Domene najviše razine podijeljene su u dvije glavne kategorije:
 - generičke domene najviše razine (gTLD)
 - domene koda države najviše razine (ccTLD)
2. **Domena druge razine (SLD):** SLD je sljedeća razina u hijerarhiji i nalazi se odmah ispod TLD-a. To je dio naziva domene koji identificira vlasnika ili organizaciju povezanu s domenom, kao što je **algebra** unutar **algebra.hr**.
3. **Domena treće razine (Poddomene):** Poddomene se nalaze ispod SLD-a i dalje dijele naziv domene na manje dijelove. Poddomene se često koriste za organiziranje web stranice u različite odjeljke, kao što je **www** u **www.algebra.hr**.

Hijerarhijska struktura DNS-a prikazana je na slici 2.3.



Slika 2.2 Hijerarhijska struktura DNS-a

DNS se često naziva i telefonskim imenikom interneta budući da je njegova glavna funkcija prevođenje IP adresa uređaja u imena računala koja su ljudima lakša za zapamtiti. Proces razlučivanja naziva domene u IP adresu započinje tako što klijent, kao što je web preglednik, šalje zahtjev lokalnom DNS razlučivaču. Njega krajnjem korisniku obično osigurava davatelj internetskih usluga (ISP) i odgovoran je za razlučivanje naziva domena u IP adrese. Kada lokalni DNS razlučivač zaprimi zahtjev za naziv domene, prvo pristupa svojoj predmemoriji kako bi provjerio postoji li tamo već IP adresa povezana s tim nazivom domene. Ukoliko uspije pronaći IP adresu povezanu s tim imenom, odmah je javlja klijentu. Ako ne uspije, šalje zahtjev korijenskom DNS poslužitelju. On je odgovoran za održavanje popisa domena najviše razine i njihovih odgovarajućih autoritativnih DNS poslužitelja. Kada korijenski poslužitelj zaprimi zahtjev za naziv domene, vraća IP adresu autoritativnog poslužitelja za TLD tog naziva. Nakon što TLD poslužitelj zaprimi taj zahtjev, vraća IP adresu autoritativnog poslužitelja za SLD. Potom autoritativni poslužitelj za domenu zaprimi zahtjev za naziv poddomene, traži IP adresu povezanu s tim nazivom i vraća je kao povratnu informaciju klijentskom računalu. Na kraju, lokalni DNS razlučivač pohranjuje IP adresu u svoju priručnu memoriju tako da može brzo odgovoriti na buduće zahtjeve za istim nazivom domene. Ovaj proces razlučivanja naziva domene u IP adresu poznat je kao DNS resolution.

Zaključno, povijest DNS-a usko je povezana s razvojem ARPANET-a i kasnije interneta. Od svojih prvih dana, do svoje trenutne uloge danas, DNS je sastavni dio razvoja i održavanja interneta kakvog danas poznajemo.

3. DNS ranjivosti

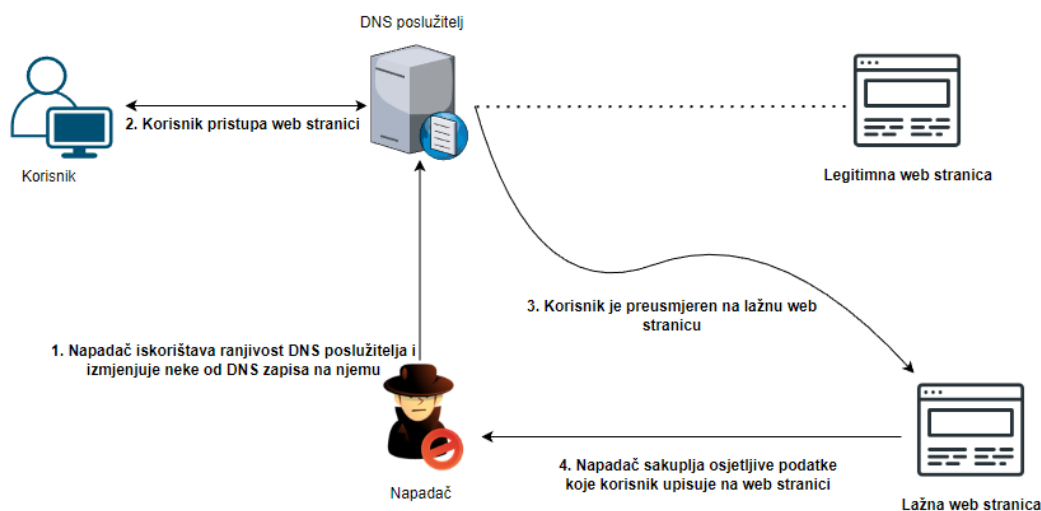
U početku razvoja DNS-a, nije postojala svijest o potrebi za razvojem sigurnosnih značajki. S vremenom su uočeni mnogi nedostaci koji narušavaju njegovu sigurnost. DNS ranjivosti stoga mogu poprimiti mnoge oblike, poput napada koji iskorištavaju slabosti u DNS protokolu, napada koji ciljaju DNS poslužitelje i dr. Ovi napadi mogu imati ozbiljne posljedice, kao što su: krađa osjetljivih informacija, prekid mrežnih usluga i širenje zlonamjernog softvera. Jedan od ključnih razloga ranjivosti DNS-a je taj što je DNS decentraliziran sustav koji se oslanja na model temeljen na uspostavljenom povjerenju. To znači da svaki zlonamjerni akter s pristupom DNS poslužitelju potencijalno može ugroziti podatke koje on sadrži i koristiti ih u zlonamjerne svrhe. Još jedan čimbenik koji pridonosi ranjivosti DNS poslužitelja je korištenje nešifrirane komunikacije između klijenata i poslužitelja. To napadačima može omogućiti presretanje i modificiranje DNS mrežnog prometa. Pojedinci i organizacije trebali bi primjenjivati najbolje sigurnosne prakse, redovno ažurirati softver i nadzirati DNS promet za neuobičajene aktivnosti kako bi se što više zaštitili od potencijalnih ugroza. U nastavku su obrađene neke od poznatih vrsta napada na DNS.

3.1. Lažiranje/Trovanje DNS-a

Lažiranje DNS-a je vrsta kibernetičkog napada u kojem napadač mijenja DNS podatke pohranjene na poslužitelju, uzrokujući isporuku netočnih informacija prema krajnjim korisnicima. To se može koristiti za preusmjerenje prometa prema legitimnim web stranicama na one zlonamjerne kao i za potpuno blokiranje pristupa web stranicama. Lažiranje DNS-a također se može koristiti za krađu osjetljivih informacija. To je itekako ozbiljna prijetnja koja može imati teške posljedice za pojedince i organizacije.

Lažiranje DNS-a može se postići na nekoliko načina, primjerice: kompromitiranje DNS poslužitelja (Slika 3.1), presretanje DNS prometa ili korištenje zlonamjernog DNS poslužitelja. Nakon što se korisnik usmjeri na zlonamjerno mjesto, od njega se može tražiti da unese osjetljive informacije kao što su vjerodajnice za prijavu. Također, korisnik može

svoje računalo izložiti zlonamjernom (malicioznom) softveru. Ova vrsta napada veoma je opasna jer korisnicima može biti teško otkriti da pristupaju lažnoj web stranici.



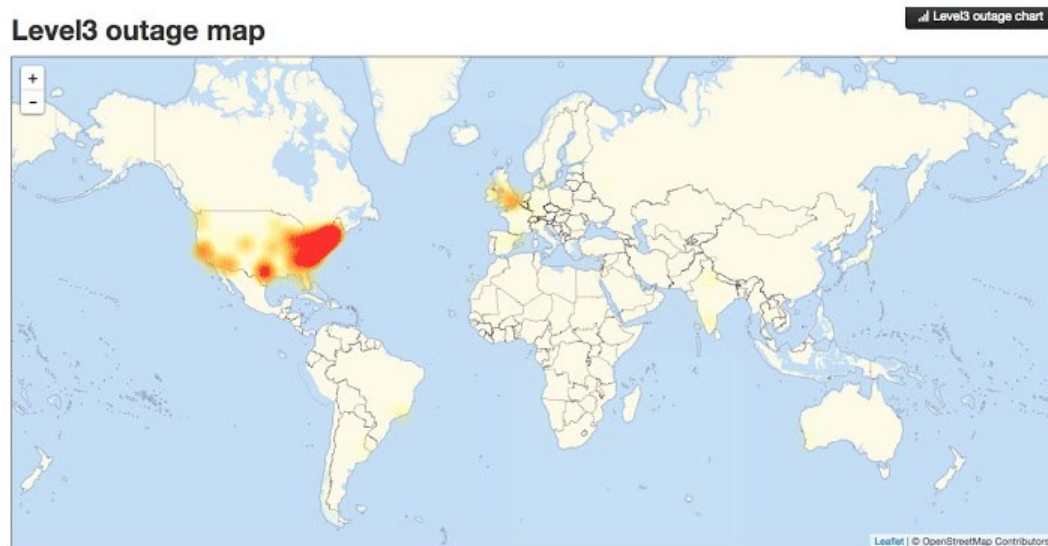
Slika 3.1 Primjer kompromitacije DNS poslužitelja

Dobar primjer napada lažiranja DNS-a je izveden 2011. u Pakistanu. Hakeri su napali državni TLD **.pk**. Grupa hakera kompromitirala je nekoliko DNS poslužitelja koji su bili odgovorni za razlučivanje imena **.pk** domena. Napadači su potom izmijenili DNS zapise nekih od popularnih web stranica, uključujući Google, Yahoo i Bing, kako bi preusmjerili korisnike na lažnu web stranicu koju oni kontroliraju. Lažna stranica izgledala je kao i ona legitimna, a od korisnika se tražilo da unesu svoje vjerodajnice za prijavu. Međutim, nakon što su korisnici unijeli svoje podatke, napadači su ih mogli ukrasti i koristiti u zlonamjerne svrhe. Napad je utjecao i na druge web-stranice, poput banaka i vladinih web-mjesta, te je izazvao rašireni prekid internetskih usluga u Pakistanu.

3.2. Napadi uskraćivanja usluge

Napad uskraćivanjem usluge (DoS) je vrsta kibernetičkog napada kojemu je u cilju učiniti neku web uslugu nedostupnu korisnicima kojima je namijenjena. DoS napad iscrpljuje hardverske resurse poslužitelja, sprječavajući odgovore na legitimne zahtjeve korisnika. Jedna od podvrsta DoS napada jest distribuirani napad uskraćivanja usluge (DDoS), koji uključuje korištenje više zaraženih računala (*botnet*) kako bi učinio web uslugu nedostupnom.

Napadač maliciozni promet može generirati korištenjem različitih metoda kao što su UDP, TCP SYN ili HTTP preplavlivanja. DoS napad također može koristiti razne tehnike izbjegavanja otkrivanja, kao što je korištenje lažnih IP adresa ili korištenje nestandardnih protokola. Jedan od najznačajnijih primjera DNS DDoS napada je napad na davatelja usluga, Dyn, 2016. godine u kojemu su napadači koristili *botnet* uređaja interneta stvari (IoT), kako bi preplavio DNS poslužitelje s mrežnim prometom. Napad je rezultirao prekidom interneta velikih razmjera, koji je utjecao na glavne web stranice poput Twittera, Netflix i Reddita. Također, napad je utjecao i na druge pružatelje DNS-a te je izazvao rašireni prekid internetskih usluga. Slika 3.2 predstavlja toplinsku kartu prekida internetske usluge tijekom napada na Dyn.



Slika 3.2 Toplinska karta koja prikazuje nedostupnost interneta tijekom napada na Dyn (Khandelwal, 2016.)

DoS napadi nisu novi, prisutni su godinama. Zabrinutost stvara njihova učestalost te sve viša razina sofisticiranosti i složenosti. Također, porast broja IoT uređaja olakšao je napadačima izgradnju velikih *botneta* koji mogu generirati ogromne količine mrežnog prometa. To predstavlja veliku prijetnju sigurnosti internetske infrastrukture koja može imati značajan utjecaj na dostupnost interneta.

3.3. DNS tuneliranje

Izvorno, DNS tuneliranje je bilo zamišljeno kao jednostavan način za zaobilazanje zatvorenih portala i dobivanje besplatnog pristupa internetu u ograničenim mrežama. DNS

tuneliranje djeluje tako da kriptira i skriva podatke unutar DNS zahtjeva i odgovora. DNS tuneliranje je postala metoda koju napadači koriste za zaobilazanje sigurnosnih mjera i izvlačenje podataka iz infiltriranih mreža. DNS tuneliranje napadačima omogućava uspostavljanje zapovjednog i kontrolnog (C&C¹) kanala korištenjem DNS protokola. Ova tehnika obično zahtijeva da kompromitirani sustav ima vanjsku mrežnu vezu, a napadač također mora kontrolirati domenu i poslužitelj koji može djelovati kao autoritativni DNS poslužitelj za istoimenu domenu. Isto tako, važno je napomenuti kako DNS tuneliranje ne iskorištava nikakve ranjivosti u samom DNS-u, samo ga koristi kao način zaobilazanja sigurnosnih mjera.

Operacija ShadowHammer je kampanja kibernetičkog napada koja je prvi put otkrivena početkom 2019. Napad je uključivao kompromitaciju popularnog softvera za upravljanje mrežom, ASUS Live Update, i korištenje DNS tuneliranja za isporuku zlonamjernog softvera sustavima korisnika koji ništa ne sumnjaju. Napadači su u ASUS Live Update softver implementirali zlonamjerni kod, koji je zatim distribuiran korisnicima putem službenog ASUS servera za ažuriranje. Jednom kada je taj softver instaliran na sustav, *malware* bi koristio DNS tuneliranje za komunikaciju s udaljenim poslužiteljem i primanje daljnjih uputa. To je napadačima omogućilo trajnu prisutnost na kompromitiranim sustavima i krađu osjetljivih informacija. Primarni cilj operacije ShadowHammer bila je određena skupina od 600 korisnika, identificiranih po njihovim jedinstvenim MAC adresama. Napadači su do tih informacija dolazili na razne načine, uključujući korištenje *phishing* e-pošte i taktike društvenog inženjeringa. Ciljajući ovu specifičnu grupu korisnika, napadači su mogli izvesti svoj napad s visokim stupnjem preciznosti i minimizirati rizik otkrivanja. Utjecaj operacije ShadowHammer bio je dalekosežan i značajan. Procjenjuje se da je više od milijun korisnika ASUS-a bilo pogođeno napadom, iako je samo mali broj korisnika bio posebno ciljan. Zlonamjerni softver je uspio ukrasti osjetljive podatke iz kompromitiranih sustava, koji bi se potencijalno mogli koristiti za daljnje kibernetičke napade i kibernetičku špijunažu. Otkriće operacije ShadowHammer izazvalo je zabrinutost oko sigurnosti lanca nabave softvera i istaknulo potrebu za proaktivnim mjerama od strane organizacija kako bi zaštitile svoje sustave od istih ili sličnih napada. To uključuje pažljivo praćenje i osiguravanje

¹ Zapovjedni i kontrolni kanal je komunikacijski kanal koji zlonamjerni softver koristi za primanje uputa i prijenos podataka udaljenom napadaču.

procesa ažuriranja softvera te provjere i validacije softvera prije njegove instalacije. Isto tako, ovaj napad služi kao podsjetnik na važnost održavanja sigurnosti DNS poslužitelja i zaštite od napada DNS tuneliranja.

4. Sigurnosne mjere za zaštitu DNS-a

Sigurnost DNS-a kritičan je aspekt kibernetičke sigurnosti i postaje sve važniji kako broj prijetnji DNS sustavima nastavlja rasti. Važno je održavati DNS poslužitelje što sigurnijima kako bi se osigurala stabilnost i pouzdanost interneta. Kompromitacija DNS poslužitelja može imati dalekosežne posljedice, utječući ne samo na klijente koji se oslanjaju na poslužitelj, već i na druge poslužitelje i mreže koje se oslanjaju na taj poslužitelj za svoje operacije. Kompromitacija DNS poslužitelja može se koristiti kao „odskočna daska“ za daljnje napade, omogućujući napadačima da steknu uporište u mreži te izvedu sofisticiranije i štetnije napade. Stoga, administratori DNS-a implementiraju razne sigurnosne mjere kako bi podigli razinu sigurnosti DNS-a. DNS sigurnosne mjere mogu se podijeliti u dvije kategorije, tehničke i ne-tehničke. Tehničke mjere uključuju implementaciju sigurnosnih protokola i korištenje DNS vatrozida. Ne-tehničke mjere uključuju obuku zaposlenika i redovite sigurnosne revizije za prepoznavanje i rješavanje ranjivosti.

4.1. Liste za kontrolu pristupa (ACL-ovi)

ACL-ovi se koriste za kontrolu pristupa DNS poslužiteljima i informacijama koje oni sadržavaju. Koriste se za određivanje kojim klijentima je dopušteno izvoditi određene radnje na DNS poslužitelju, kao što je postavljanje DNS upita ili ažuriranje DNS baze podataka. To omogućuje administratorima podizanje razine sigurnosti DNS-a tako da ograničavaju samo ovlaštenim klijentskim računalima pristup informacijama.

DNS ACL-ovi stvaraju se definiranjem skupa ili raspona IP adresa i određivanjem vrsta radnji koje su dopuštene ili zabranjene za te IP adrese. Na primjer, ACL može dopustiti svim klijentima upite prema DNS poslužitelju, ali samo određenim klijentima dopustiti ažuriranje DNS baze podataka. ACL se primjenjuje na DNS poslužitelj, a poslužitelj koristi ACL za određivanje radnji koje neki klijent može izvršiti. Kontrolirajući koji korisnici i sustavi imaju pristup određenim resursima, ACL-ovi pomažu spriječiti neovlašteni pristup osjetljivim informacijama, dopuštajući samo pouzdanim korisnicima i sustavima pristup određenim resursima. ACL-ovi mogu pomoći i kod poboljšanja

performansi sustava te u smanjivanju rizika od pojedinih sigurnosnih incidenata. To je zato što poslužitelj neće trošiti svoje resurse na obradu zahtjeva iz nepouzdatih izvora. Organizacije se često moraju pridržavati raznih sigurnosnih politika i propisa te im ACL-ovi pomažu za implementaciju tih pravila. Liste za kontrolu pristupa osiguravaju da je pristup resursima ograničen u skladu s propisima i zahtjevima za postizanje usklađenosti s regulativama.

Ukratko, ACL-ovi definiraju točne dozvole koje bi svaki korisnik ili sustav trebao imati, dopuštajući administratorima da odrede tko bi trebao imati pristup kojim resursima, a tko ne. Time pomažu smanjiti rizik od pojave sigurnosnih incidenata.

4.2. Šifriranje DNS zahtjeva

Šifriranje je važna tehnologija koja služi za poboljšanje sigurnosti DNS-a. U ovom kontekstu, šifriranje se odnosi na osiguravanje podataka koji putuju mrežom, što otežava neovlaštenim stranama presretanje i/ili izmjenu istih. Kada se podaci prenose putem interneta, često se šalju u običnom tekstu, što znači da ih može presresti i pročitati svatko tko ima pristup mreži. Iz tog razloga ti su podaci ranjivi na razne sigurnosne prijetnje, poput prisluškivanja, neovlaštenog mijenjanja i krađe. Kako bi se odgovorilo na te prijetnje, koristi se šifriranje. Ono se koristi za kodiranje podataka, čineći ih nečitljivima svima koji nemaju ključ za dešifriranje. Kako bi se riješile navedene i slične prijetnje DNS sustavima, razvijeno je nekoliko protokola za održavanje pouzdanosti i integriteta informacija, od kojih su najučestaliji: DNSSEC, DNS-over-HTTPS i DNS-over-TLS. Ove tehnologije vrlo su slične i usko povezane te rade zajedno kako bi se postigla što veća sigurnost DNS prometa.

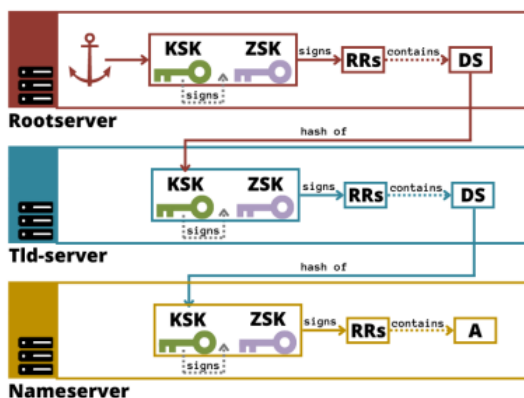
4.2.1. DNSSEC

Sigurnosna proširenja DNS-a (DNSSEC) su skup značajki DNS protokola koje pružaju šifriranje DNS podataka s kraja na kraj. Primarni cilj DNSSEC-a je osigurati internetsku infrastrukturu i spriječiti različite vrste napada na DNS kao što su trovanje predmemorije, napadi "čovjeka u sredini" i preusmjerenje prometa na zlonamjerne mjesta. DNSSEC sastoji se od kriptografskih mehanizama i protokola koji se koriste za osiguranje podataka u prijenosu. (Network Working Group, 2005.) Srž DNSSEC-a je skup

digitalnih potpisa koji se koriste za provjeru autentičnosti DNS podataka i za otkrivanje bilo kakvih neovlaštenih promjena.

DNSSEC funkcioniра na način da potpisuje DNS podatke pohranjene na autoritativnom poslužitelju, a zatim distribuira potpisane podatke podređenim poslužiteljima, uključujući razlučivače i *caching* poslužitelje. Potpisane podatke tada razlučivač može provjeriti koristeći digitalne potpise za provjeru autentičnosti podataka primljenih od drugih poslužitelja. Tim putem može saznati jesu li ti podaci izmijenjeni te ako jesu, je li to bila ovlaštena promjena ili ne. Svatko tko je autoritativan za naziv domene na internetu može zaštititi svoje podatke pomoću DNSSEC-a.

Prvi korak u DNSSEC provjeri valjanosti jest potpisivanje svih zapisa za pojedinu domenu. Za svaku domenu postoji barem jedan par privatnih i javnih ključeva, pri čemu privatni ključ – prema nazivu – ostaje privatnа, а javni ključ postaje dio DNSKEY zapisa koji je javan. Privatni ključ potpisuje zapise, pri čemu se javni ključ koristi za provjeru potpisa. Ovi su potpisi sami po sebi DNS zapisi i nazivaju se RRSIG. Budući da ovaj par ključeva potpisuje zone, naziva se ključ za potpisivanje zone (ZSK). S kombinacijom DNSKEY, javnog ZSK i A ili AAAA zapisa, razlučivač može provjeriti valjanost A ili AAAA zapisa. Međutim, javlja se problem povjerenja: kako znamo da je DNSKEY zapis doista točan? Kako bismo potvrdili integritet zapisa, možemo upotrijebiti lanac povjerenja korijenskog poslužitelja. (Slika 4.1) Korijenski poslužitelj ponovno ima dva para ključeva, ZSK par i drugi par koji se naziva ključ za potpisivanje ključa (KSK) i zajedno se koriste za neizravno potpisivanje KSK-a TLD poslužitelja, raspršivanjem DS zapisa. Ovime se mogu potvrditi KSK i ZSK TLD poslužitelja, а zajedno mogu potvrditi KSK i ZSK poslužitelja imena domene. (Kreuger, 2023.)



Slika 4.1 DNSSEC lanac povjerenja (Kreuger, 2023.)

DNSSEC uključuje i skup protokola koji se koriste za osiguranje komunikacije između autoritativnog poslužitelja i razlučivača. To uključuje korištenje sigurnih komunikacijskih protokola koji pružaju E2E šifriranje i autentifikaciju za podatke koji se prenose u DNS-u. Ti protokoli su detaljnije opisani u sljedećem poglavlju.

4.2.2. DNS-over-HTTPS (DoH) i DNS-over-TLS (DoT)

DNS putem HTTPS-a (DNS-over-HTTPS) i DNS putem TLS-a (DNS-over-TLS) su sigurnosni protokoli za šifrirani prijenos DNS upita i odgovora preko interneta. Oba protokola dizajnirana su za pružanje privatnosti i sigurnosti za DNS komunikaciju i za sprječavanje različitih vrsta DNS napada. Njihova arhitektura sastoji se od niza mehanizama koji se koriste za osiguranje prijenosa DNS podataka. Oba protokola koriste šifriranje i autentifikaciju za zaštitu podataka tijekom njihovog prijenosa. I DoH i DoT pružaju nekoliko važnih sigurnosnih prednosti. Prvo, oba protokola pružaju E2E šifriranje podataka, što sprječava prisluškivanje i manipulaciju nad podacima tokom prijenosa. Drugo, oba protokola omogućuju uzajamnu autentifikaciju između klijenta i poslužitelja, čime se osigurava da klijent komunicira sa željenim poslužiteljem i da je poslužitelj doista autoritativni poslužitelj za traženu domenu. DoH koristi HTTPS protokol, koji je posebno dizajniran za sigurnu web komunikaciju, dok DoT koristi TLS protokol, koji je sigurnosni protokol opće namjene koji se može koristiti za više različitih vrsta mrežne komunikacije. Slika prikazuje pojednostavljeni prikaz komunikacije između klijenta i DNS poslužitelja koristeći navedene protokole.



Slika 4.2 Pojednostavljeni prikaz DNS komunikacije putem HTTPS/TLS protokola (Infoblox, How to configure DoT/DoH)

DoH funkcionira na sljedeći način: klijent šalje DNS upit DoH razlučivaču preko sigurne HTTPS veze. Razlučivač zatim koristi šifrirani kanal za prosljeđivanje upita autoritativnom DNS poslužitelju. Autoritativni poslužitelj odgovara na upit DNS odgovorom, koji se šalje natrag u razlučivač preko sigurne HTTPS veze. Klijent tada prima šifrirani odgovor i dešifrira ga kako bi dobio tražene informacije. (Hoffmann, ICANN, McManus, 2018.) Skoro pa identično funkcionira i DoT, gdje DNS klijent šalje DNS upit DoT razlučivaču preko TLS veze te se ostatak komunikacije odvija na isti način kao i kod DoH-a. (Hu, Zhu, Heidemann et al, 2016.)

DoH i DoT su opcionalne komponente DNS infrastrukture koje pružaju privatnost i sigurnost DNS komunikacije šifriranjem i provjerom autentičnosti podataka tijekom njihovog prijenosa mrežom. Oba protokola imaju svoje prednosti i mane, a izbor između DoH i DoT ovisit će o specifičnim potrebama i zahtjevima organizacije ili pojedinca koji ih primjenjuje.

4.3. DNS vatrozid

DNS vatrozid mrežno je sigurnosno rješenje osmišljeno za zaštitu DNS-a od prijetnji, kao što su kibernetički napadi, povrede podataka i druge vrste zlonamjernih aktivnosti. Dizajniran je da djeluje kao zaštitna barijera između interne mreže i interneta, filtrirajući i blokirajući DNS promet koji se smatra zlonamjernim ili neovlaštenim. DNS vatrozidi postaju sve važniji kako se sve više organizacija oslanja na internet i digitalne sustave za vođenje svojih poslovnih operacija. Sukladno tome, sve je veći broj napada na takve organizacije. DNS vatrozid može pomoći organizacijama da postignu višu razinu sigurnosti pružajući sveobuhvatno rješenje koje uz već spomenute sigurnosne značajke pomaže spriječiti napade i povrede podataka.

DNS vatrozidi rade tako da analiziraju DNS promet u stvarnom vremenu i blokiraju svaki promet koji se smatra zlonamjernim ili neovlaštenim. Specifične metode koje se koriste za utvrđivanje je li određeni DNS zahtjev zlonamjernan ovisit će o specifičnom rješenju DNS vatrozida koje se koristi. Neka rješenja mogu koristiti algoritme strojnog učenja za prepoznavanje zlonamjernog prometa, dok druga mogu koristiti tradicionalniji pristup temeljen na pravilima. Nakon što se identificira zlonamjerni DNS zahtjev, DNS vatrozid će ga blokirati, sprječavajući zahtjev da dosegne željeni cilj. Osim toga, DNS vatrozidi također mogu pružiti dodatne sigurnosne značajke, kao što su:

- Kontrole pristupa – sigurnosne značajke koje organizacijama omogućuju ograničavanje pristupa određenim resursima na temelju danih kriterija.
- Bilježenje i izvješćivanje – značajke koje omogućuju organizacijama praćenje DNS prometa i prepoznavanje potencijalnih sigurnosnih incidenata.
- Integracija s postojećim sigurnosnim rješenjima - DNS vatrozidi mogu se integrirati s postojećim sigurnosnim rješenjima, kao što su drugi vatrozidi, sustavi za otkrivanje i prevenciju upada (IDS/IPS) i rješenja za upravljanje sigurnosnim informacijama i događajima (SIEM).

4.4. DNS sigurnosne politike i revizije

Sigurnosne politike i revizije ključni su dio održavanja ukupne sigurnosti organizacije pa tako i DNS-a. Sigurnosna politika pruža jasan i koncizan okvir za zaštitu DNS infrastrukture i podataka organizacije te pomaže osigurati da svi zaposlenici razumiju svoje uloge i odgovornosti u održavanju njene sigurnosti. Redovite sigurnosne revizije s druge strane pomažu u identifikaciji ranjivosti, osiguravanju ažurnosti i relevantnosti sigurnosnih politika, također pomažu u sprječavanju neovlaštenog pristupa osjetljivim informacijama. Sigurnosna revizija DNS-a procjena je DNS infrastrukture, uključujući njezine sustave, uređaje i konfiguracije. Cilj revizije je identificirati sigurnosne slabosti, pogrešne konfiguracije i druge ranjivosti koje bi napadači mogli iskoristiti. Revizija bi trebala obuhvatiti sve aspekte infrastrukture, uključujući njezine poslužitelje, vatrozide, usmjerivače i druge mrežne uređaje.

Da bi provela reviziju sigurnosti DNS-a, organizacija treba započeti s provođenjem sveobuhvatne procjene rizika kako bi identificirala potencijalne sigurnosne prijetnje i utjecaj koji bi one imale na organizaciju ako bi bile iskorištene. Nakon toga treba uslijediti temeljita procjena sigurnosnih politika i procedura organizacije, kao i procjena trenutnih sustava i uređaja kako bi se identificirale potencijalne ranjivosti sustava. Kada se revizija dovrši, potrebno je razviti detaljan plan za rješavanje svih identificiranih sigurnosnih slabosti, što može uključivati: ažuriranje sigurnosnih pravila, implementaciju novih sigurnosnih tehnologija i/ili izmjenu postojećih konfiguracija. Plan bi također trebao uključivati buduće sigurnosne revizije kako bi se osiguralo da organizacija ostane u toku s prijetnjama koje će se razvijati tokom vremena.

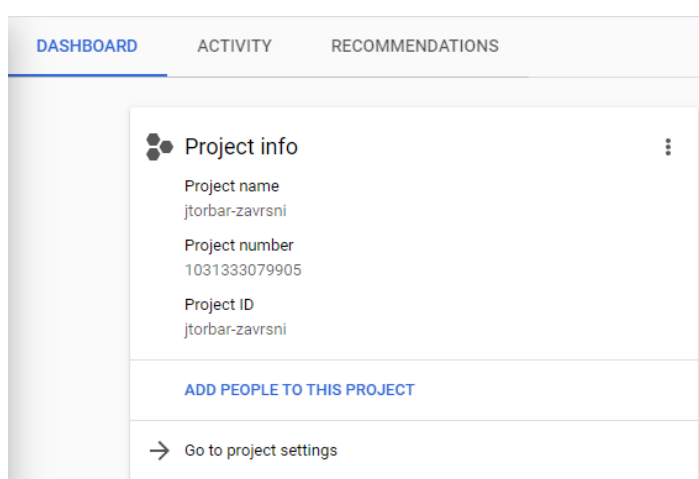
Zaključno, redovite sigurnosne revizije i ažurne sigurnosne politike bitan su dio održavanja ukupne sigurnosti DNS infrastrukture organizacije. Implementacija spomenutih tehnologija i procedura u sigurnosnu strategiju neke organizacije zahtijeva sveobuhvatan pristup i predanost redovitim revizijama sigurnosti. To će joj pomoći u pružanju snažne zaštite od širokog spektra prijetnji povezanih s DNS-om.

5. Implementacija DNS servisa

U praktičnom dijelu ovoga rada razrađena je implementacija DNS servisa. Implementacija sadržava instalaciju i konfiguraciju stabilne verzije ISC BIND servisa. BIND je jedan od najčešće korištenih softverskih rješenja za DNS, a koriste ga mnoge organizacije i pružatelji usluga. BIND 9 je najnovija verzija BIND-a. Ona omogućuje niz novih značajki i poboljšanja u odnosu na prethodne verzije, uključujući povećanu sigurnost, performanse i nove funkcionalnosti. BIND 9 podržava širok raspon platformi, što ga čini prikladnim za korištenje u jednostavnim, ali i u složenim okruženjima. Također uključuje brojne alate i pomoćne programe za upravljanje i nadzor DNS poslužitelja, što administratorima olakšava upravljanje i održavanje DNS infrastrukture temeljene na BIND 9 softveru.

5.1. Konfiguracija infrastrukture u oblaku

BIND DNS poslužitelji instalirani su na Google Cloud platformi. Kao operacijski sustav na kojem je implementiran BIND servis, koristi se Rocky Linux verzije 9. Za potrebe ovog rada, kreiran je projekt unutar GCP-e, naziva „jtorbar-zavrzni“ (Slika 5.1).



Slika 5.1 Nadzorna ploča projekta „jtorbar-zavrzni“ unutar Google Cloud platforme

Za potrebe razvoja i implementacije DNS servisa korištene su dvije E2 instance. Tablica ispod opisuje njihove specifikacije.

Tablica 1 – dimenzije korištenih virtualnih strojeva (instanci) unutar Google Cloud platforme

	rocky-1	rocky-2
OS	Rocky Linux 9	Rocky Linux 9
CPU	2	2
RAM	4	4
Disk	20GB	20GB

Za kreiranje ovih virtualnih strojeva korišten je python kod koji komunicira s Google Cloud API-jem. Prije početka razvoja python koda, treba kreirati i aktivirati python virtualnu okolinu, to je postignuto sljedećim naredbama:

```
pip -m venv jtorbar-zavrzni && .\jtorbar-zavrzni\Scripts\activate
```

Kako bi bilo moguće pristupiti Google Cloud API-ju, potrebno je instalirati python google paket. Također, za potrebe kreiranja i manipulaciju virtualnim strojevima, potrebno je instalirati google-cloud-compute i google-api-python-client pakete.

```
pip install google google-cloud-compute google-api-python-client
```

Nakon što su instalirani potrebni paketi, potrebno je kreirati i konfigurirati vjerodajnice za prijavu. Unutar Google Cloud web sučelja kreiran je servisni račun koji se koristio za sve radnje na infrastrukturi u oblaku. Nakon što je kreiran servisni račun, pomoću google.auth python biblioteke uspostavljena je autentikacija s API-jem. Vjerodajnice servisnog računa postavljene su u credentials.json datoteci. Ispod se nalazi dio koda koji odrađuje autentikaciju s Google Cloud API-jem.

```
import google.auth

# Authenticate with the Google Cloud API
credentials, project = google.auth.default()

compute = compute_v1.ComputeClient(credentials=credentials)
```

Nakon uspješne prijave, moguće je kreirati instance navedene u tablici 1. Za kreiranje virtualnih strojeva isto je korišten python. Priloženi kod sadržava python rječnik koji se koristi za definiranje konfiguracije Rocky Linux instanci. Vrijednost metapodatka „ssh-keys“ je uklonjena iz koda ispod.

```
config = {
    "name": instance_name,
    "machineType": f"zones/{zone}/machineTypes/{instance_type}",
    "disks": [
        {
            "boot": True,
            "autoDelete": True,
            "initializeParams": {
                "sourceImage": f"projects/rocky-linux-
cloud/global/images/family/rocky-linux-9",
                "diskSizeGb": boot_disk_size,
                "diskType":
f"zones/{zone}/diskTypes/{boot_disk_type}"
            }
        }
    ],
    "networkInterfaces": [
        {
            "network":
f"projects/{project}/global/networks/zavrsni-vpc",
            "subnetwork":
f"projects/{project}/regions/{region}/subnetworks/zavrsni-subnet",
            "accessConfigs": [
                {
                    "name": "External NAT",
                    "type": "PRIVATE"
                }
            ]
        }
    ]
}
```

```

        ]
    }
],
"serviceAccounts": [
    {
        "email": "default",
        "scopes": [
            "https://www.googleapis.com/auth/cloud-platform"
        ]
    }
],
"metadata": {
    "items": [
        {
            "key": "ssh-keys",
            "value":
        }
    ]
}
}

```

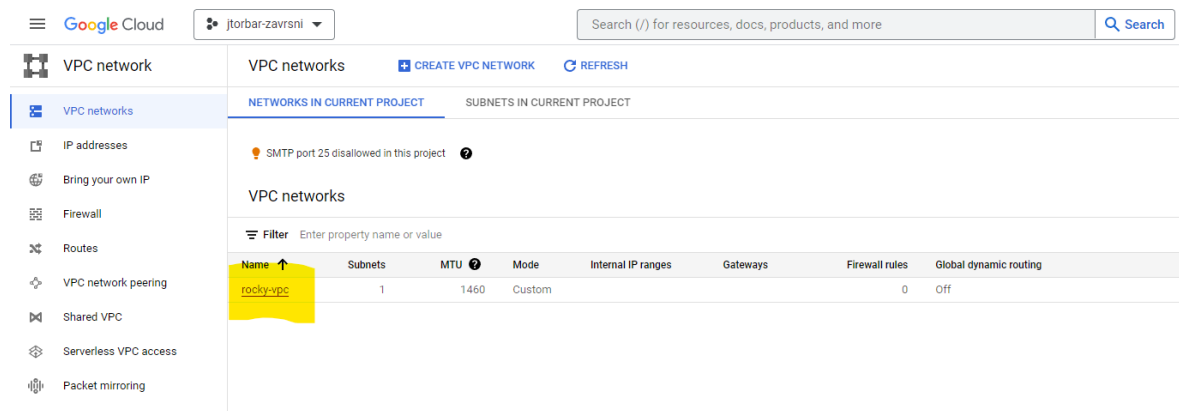
Kada se kod za kreiranje infrastrukture u oblaku izvrši (skripta main.py), u terminalu je moguće vidjeti sljedeći ispis:

```

(jtorbar-zavrsni) > python.exe .\main.py
=== Connection to Google Cloud API succeeded ===
=== Creating VPCs ===
VPC 'zavrsni-vpc' and subnet 'zavrsni-subnet' created successfully
=== Creating Rocky Linux 9 instances ===
Enter the number of Rocky instances to create: 2
VM instances are being created: rocky-0, rocky-1

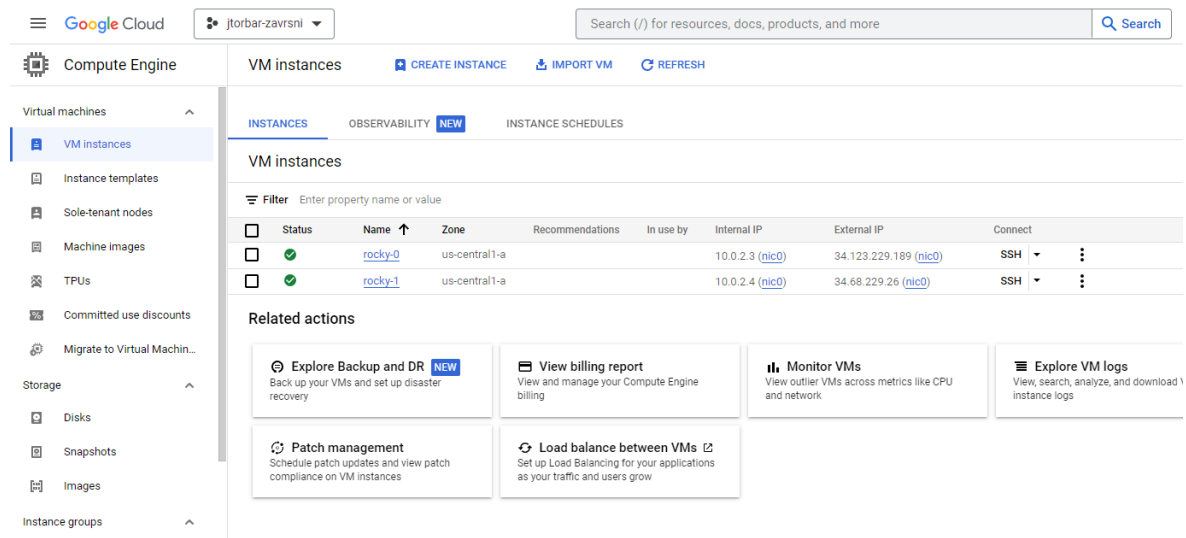
```

Unutar Google Cloud konzole možemo provjeriti je li se infrastruktura u oblaku ispravno kreirala. Prvo možemo provjeriti je li kreirana `zavrnsni-vpc` VPC mreža. To se može provjeriti u VPC network sučelju:



Slika 5.2 VPC network sučelje unutar GCP konzole

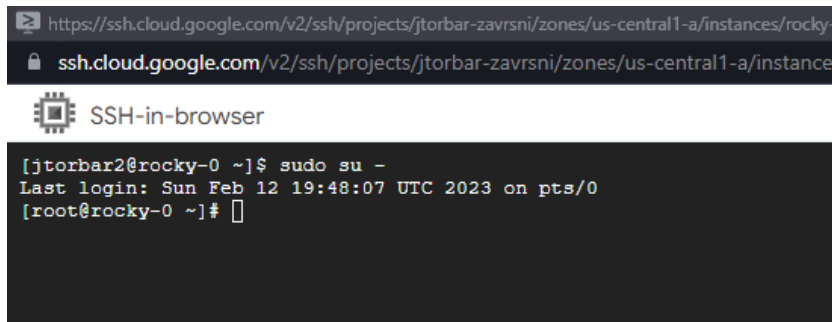
Kako bi provjerili jesu li se kreirale Rocky Linux instance, trebamo pristupiti Compute Engine sučelju. Tu možemo vidjeti kako su kreirane dvije instance virtualnih strojeva, **rocky-0** i **rocky-1**.



Slika 5.3 Compute Engine sučelje unutar GCP konzole

Nakon što je utvrđeno da je infrastruktura kreirana očekivano, potrebno je kreirati pravilo na vatrozidu kako bi bilo moguće pristupiti virtualnim strojevima putem SSH protokola. Pravilo za SSH je kreirano putem web konzole GCP-e te je nakon odrađenih radova na poslužiteljima uklonjeno.

SSH konekcije uspostavljane su kroz Compute Engine web sučelje, pristikom na gumb „SSH“. Web preglednik tada uspostavlja WebSocket vezu s poslužiteljem GCP konzole, koji djeluje kao proxy za SSH vezu s instancom virtualnog stroja. GCP konzola nakon toga autentificira korisnika i prosljeđuje zahtjev za SSH vezu ciljanoj instanci. Zatim instanca provjerava zahtjev za SSH vezom i uspostavlja SSH vezu s korisnikom. Korisnik tada može upravljati virtualnim strojem putem prozora SSH terminala koji se prikazuje u pregledniku.



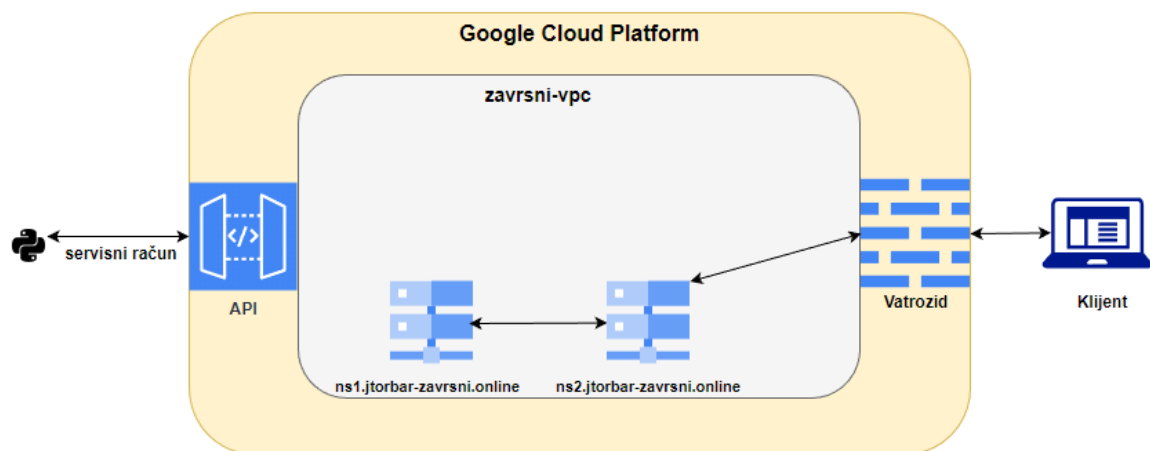
Slika 5.4 SSH veza prema virtualnom stroju uspostavljena putem web preglednika

Kada je uspješno uspostavljena SSH konekcija prema virtualnim strojevima, moguća je daljnja modifikacija i konfiguracija istih.

5.2. Konfiguracija BIND DNS servisa

Domena koja je korištena za implementaciju BIND servisa je **jtorbar-zavrsni.online**. Domena je registrirana putem servisa **domain.com**². DNS servis implementiran je u hidden master³ infrastrukturi, korištenjem prethodno kreiranih virtualnih strojeva na Google Cloud platformi. U takvoj konfiguraciji, datoteke DNS zona na glavnom poslužitelju ne sadrže nikakve specifične informacije o IP adresi za sam glavni poslužitelj. Umjesto toga, te datoteke sadrže samo mjerodavne DNS informacije za resurse pojedine domene.

Infrastruktura se sastoji od jednog glavnog i jednog podređenog DNS poslužitelja. Glavni poslužitelj je primarni poslužitelj te on drži mjerodavne datoteke DNS zona, dok je podređeni poslužitelj sekundarni poslužitelj koji dobiva kopiju datoteka DNS zona. Glavni poslužitelj odgovoran je za izmjene u datotekama DNS zona, dok podređeni poslužitelji dobivaju ažuriranja kada su promjene napravljene. Skica infrastrukture vizualno je prikazana na slici ispod.



Slika 5.5 Skica virtualne infrastrukture u oblaku

Prije instalacije paketa potrebnih za uspostavljanje DNS servisa, potrebno je preimenovati virtualne strojeve **rocky-0** i **rocky-1** u **ns1.jtorbar-zavrsni.online** i **ns2.jtorbar-zavrsni.online**. To je odrađeno korištenjem naredbe `hostnamectl`.

² <https://www.domain.com/>

³ Arhitektura koja uključuje primarni DNS poslužitelj koji nije javno dostupan i koristi se za privatno upravljanje ažuriranjima DNS zona prije njihovog prijenosa na javno dostupan sekundarni poslužitelj.

```
rocky-0$ sudo hostnamectl set-hostname ns1.jtorbar-zavrnsni.online
rocky-1$ sudo hostnamectl set-hostname ns2.jtorbar-zavrnsni.online
```

Sljedeće što je bilo potrebno napraviti jest konfigurirati `/etc/hosts` datoteku tako da njen sadržaj izgleda ovako:

```
<privatna-ip-adresa-ns1> ns1.jtorbar-zavrnsni.online ns1
<privatna-ip-adresa-ns2> ns2.jtorbar-zavrnsni.online ns1
```

Nakon što su postavljena imena virtualnih strojeva i `hosts` datoteka kako bi oni znali međusobno komunicirati, instalirani su paketi potrebni za implementaciju DNS servisa. Instaliran je BIND verzije 9.16, koja je ujedno i zadnja stabilna verzija u trenutku pisanja ovog rada. Uz sam paket **bind**, instalirana su dva dodatna paketa koja pružaju dodatne funkcionalosti. Oni su **bind-chroot** i **bind-utils**.

```
sudo dnf install bind bind-chroot bind-utils
```

Kada se paketi instaliraju, u `/etc/sysconfig/named` datoteku dodana je opcija „-4“ koja limitira BIND servis na način da on pri pokretanju može slušati samo na IPv4 adresama. Ispod se nalazi spomenuta datoteka nakon dodavanja opcije.

```
# BIND named process options
# ~~~~~
# OPTIONS="whatever"      -- These additional options will be passed to named
#                          at startup. Don't add -t here, enable proper
#                          -chroot.service unit file.
# NAMEDCONF=/etc/named/alternate.conf
#                          -- Don't use -c to change configuration file.
#                          Extend systemd named.service instead or use this
#                          variable.
# DISABLE_ZONE_CHECKING  -- By default, service file calls named-checkzone
#                          utility for every zone to ensure all zones are
#                          valid before named starts. If you set this option
#                          to 'yes' then service file doesn't perform those
#                          checks.
OPTIONS="-4"
```

Glavni poslužitelj konfiguriran je sa raznim sigurnosnim značajkama. Njegova konfiguracija uključuje ACL-ove, IP adrese za pokretanje BIND servisa, postavljanje parametara za DNSSEC i dr. Postavljene su i DNS zone za domenu **jtorbar-zavrzni.online**. Prije same konfiguracije DNS servisa, kreirano je chroot okruženje koje omogućava „zatvoriti“ DNS servis na određenu putanju na datotečnom sustavu. Ovo je jedna od implementiranih sigurnosnih značajki te ona služi za sprječavanje pristupa potencijalnih napadača drugim dijelovima sustava. Sljedeća naredba montira sve BIND konfiguracijske datoteke u chroot lokaciju:

```
/usr/libexec/setup-named-chroot.sh /var/named/chroot on
```

Konfiguracija glavnog DNS poslužitelja nalazi se na lokaciji */var/named/chroot/etc/named.conf*. Ispod su navedene najrelevantnije implementirane značajke za podizanje razine sigurnosti sustava.

1. ACL – primijenjena je lista za kontrolu pristupa **dozvoli-kopiranje** koja dozvoljava isključivo računalima iz zavrzni-vpc pod mreže kopiranje podataka iz datoteka DNS zona.

```
acl "dozvoli-kopiranje" {
    <zavrzni-vpc-subnet>/30; # zavrzni-vpc, ali samo prve 4 adrese
};

options {
    ...
    allow-query { any; };
    allow-transfer { "dozvoli-kopiranje"; };
    ...
};
```

2. Zapisivanje informacija o upitima korisnika

```
logging {
    channel query_log {
        file "/var/log/query.log" versions 3 size 50M;
        severity info;
        print-time yes;
        print-severity yes;
        print-category yes;
    };
};
```

```
};  
  
category queries { query_log; };  
  
};
```

3. DNSSEC – DNSSEC je uključen bez potrebe za dodatnom konfiguracijom u novijim verzijama BIND-a. Opcija **dnssec-validation** postavljena je na vrijednost **yes** kako bi se omogućila DNSSEC provjera valjanosti kriptografskih ključeva.

```
options {  
  
    ...  
  
    dnssec-validation yes;  
  
    ...  
  
};
```

4. TSIG – korišten je tajni ključ **tajni-kljuc** koji je definiran SHA512-MD5 algoritmom za šifriranje i dijeljene tajne u Base64 šifriranom formatu. Ona je uklonjena u primjeru ispod. Kopiranje datoteka omogućeno je samo računalima koja se mogu autentificirati putem tog ključa.

```
key "tajni-kljuc" {  
  
    algorithm hmac-sha512;  
  
    secret "<ovdje-se-nalazi-tajna>";  
  
};  
  
options {  
  
    ...  
  
    allow-transfer {  
  
        key "tajni-kljuc";  
  
    };  
  
    ...  
  
};
```

5. Rate limit – ograničen je broj upita koju jedan klijent (jedna IP adresa) može postaviti unutar određenog vremenskog perioda. Broj upita je postavljen na 5 u jednoj sekundi. Ako klijent premaši ovo ograničenje, opcija **slip** će odgoditi sljedeće upite za 10 sekundi. Opcija **ipv4-prefix-length** postavljena je na 32 kako bi se postavilo ograničenje postavljanja upita na pojedinačne IP adrese, a ne na cijele pod mreže.

```
options {  
    ...  
    rate-limit {  
        responses-per-second 5;  
        window 1;  
        errors-per-second 5;  
        log-only no;  
        slip 10;  
        ipv4-prefix-length 32;  
    };  
};
```

6. Sakrivanje verzije softvera - opcija verzije postavljena je na vrijednost **nepoznata verzija** kako bi se spriječilo da BIND poslužitelj otkrije informacije o svojoj verziji u odgovoru poslužitelja.

```
options {  
    ...  
    version "nepoznata verzija";  
    ...  
};
```

Nakon postavljanja konfiguracije BIND servisa, moguće je provjeriti ispravnost sintakse naredbom `named-checkconf -t /var/named/chroot/etc/named.conf`. Servis je pokrenut naredbom `systemctl enable --now named-chroot` koja ujedno i omogućava njegovo pokretanje pri podizanju sustava.

Status servisa provjeren je naredbom `systemctl status named-chroot`:

```
$ systemctl status named-chroot
• named-chroot.service - Berkeley Internet Name Domain (DNS)

   Loaded: loaded (/usr/lib/systemd/system/named-chroot.service; enabled;
 vendor preset: disabled)

   Active: active (running) since Mon 2023-02-13 19:52:17 UTC; 6s ago

   Process: 62024 ExecStartPre=/bin/bash -c if [ ! "$DISABLE_ZONE_CHECKING" ==
 "yes" ]; then /usr/sbin/named-checkconf -t /var/named/chroot -z "$NAMEDCONF";
 else echo "Checking of zone files is disabled"; fi (code=exited,
 status=0/SUCCESS)

   Process: 62026 ExecStart=/usr/sbin/named -u named -c ${NAMEDCONF} -t
 /var/named/chroot $OPTIONS (code=exited, status=0/SUCCESS)

  Main PID: 62027 (named)

    Tasks: 6 (limit: 23104)

   Memory: 18.5M

      CPU: 79ms

   CGroup: /system.slice/named-chroot.service
           └─62027 /usr/sbin/named -u named -c /etc/named.conf -t
 /var/named/chroot -4

Feb 13 19:52:17 nsl.jtorbar-zavrsni.online named[62027]: all zones loaded
Feb 13 19:52:17 nsl.jtorbar-zavrsni.online named[62027]: running
Feb 13 19:52:17 nsl.jtorbar-zavrsni.online systemd[1]: Started Berkeley Internet
Name Domain (DNS).
Feb 13 19:52:17 nsl.jtorbar-zavrsni.online named[62027]: managed-keys-zone:
Initializing automatic trust anchor management for zone '.'; DNSKEY ID 20326 is
now trusted, waiving the normal 30-day waiting period.
Feb 13 19:52:17 nsl.jtorbar-zavrsni.online named[62027]: resolver priming query
complete
```

Nakon što je glavni DNS poslužitelj ispravno konfiguriran i DNS servis pokrenut, kreiran je kriptografski ključ i DNS forward-lookup zona **jtorbar-zavrsni.online** koja sadrži informacije o zoni i A zapis. Kod ispod prikazuje konfiguraciju DNS forward-lookup zone.

```
$TTL 1D
@      IN SOA  jtorbar-zavrsni.online  root (
                                0      ; serial
```

```

                                1D      ; refresh
                                1H      ; retry
                                1W      ; expire
                                3H )    ; minimum

                                IN NS   ns1.jtorbar-zavrsni.online.
                                IN NS   ns2.jtorbar-zavrsni.online.
ns2                                IN A   104.197.65.23

```

Nakon što je zona konfigurirana, potrebno ju je dodati u BIND konfiguracijsku datoteku i ponovno učitati konfiguraciju. Sljedeća direktiva je dodana u konfiguracijsku datoteku:

```

zone "jtorbar-zavrsni.online" IN {
    type master;
    dnssec-policy default;
    inline-signing yes;
    file "jtorbar-zavrsni.online";
    allow-update { none; };
};

```

Uz forward-lookup zonu, kreirana je i reverse-lookup zona koja sadržava PTR zapis za ns2 poslužitelj, za tu zonu je isto tako generiran DNSSEC kriptografski ključ te je ona potpisana istim.

Sekundarni DNS poslužitelj je konfiguriran na veoma sličan način. Kreirano je chroot okruženje, postavljena tajna i sigurnosni ključ za BIND servis, postavljene su kontrole pristupa, DNSSEC validacija, ograničenja na klijentske upite i zapisivanje informacija o klijentskim upitima. Sve potrebne datoteke koje zahtjeva konfiguracija kopirane su na sekundarni poslužitelj. Ispod se nalazi konfiguracija sekundarnog poslužitelja:

```

[root@ns2 chroot]# cat etc/named.conf
key "tajni-kljuc" {
    algorithm hmac-sha512;
    secret "<ovdje-se-nalazi-tajna>";
};
acl "dozvoli-kopiranje" {
    <zavrsni-vpc-subnet>/30; # zavrsni-vpc, ali samo prve 4 adrese

```

```

};

options {
    listen-on port 53 { 127.0.0.1; <privatna-ip-adresa-ns2>; };
    directory          "/var/named/";
    dump-file           "/var/named/data/cache_dump.db";
    statistics-file     "/var/named/data/named_stats.txt";
    memstatistics-file  "/var/named/data/named_mem_stats.txt";
    recursing-file      "/var/named/data/named.recursing";
    secroots-file       "/var/named/data/named.secroots";
    allow-query         { localhost; any; };
    allow-query-cache   { localhost; any; };
    /* Rate limiting */
    rate-limit {
        responses-per-second 5;
        window 1;
        errors-per-second 5;
        log-only no;
        slip 10;
        ipv4-prefix-length 32;
    };
    recursion yes;
    /* DNSSEC */
    dnssec-validation yes;
    /* Zone transfer */
    allow-transfer{"dozvoli-kopiranje"; key "tajni-kljuc";};
    /* Path to ISC DLV key */
    bindkeys-file "/etc/named.iscdlv.key";
    managed-keys-directory "/var/named/dynamic";
    pid-file "/run/named/named.pid";
    session-keyfile "/run/named/session.key";
    /* Hide version number */
    version "nepoznata verzija";
}

```



```

};

logging {

    channel default_debug {

        file "data/named.run";

        severity dynamic;

    };

    channel query_log {

        file "/var/log/query.log" versions 3 size 50M;

        severity info;

        print-time yes;

        print-severity yes;

        print-category yes;

    };

    category queries { query_log; };

};

zone "." IN {

    type hint;

    file "named.ca";

};

zone "jtorbar-zavrsni.online" IN {

    type secondary;

    file "jtorbar-zavrsni.online";

    masters { <privatna-ip-adresa-ns1>; };

};

zone "65.197.104.in-addr.arpa" IN {

    type secondary;

    file "65.197.104.in-addr.arpa";

    masters { <privatna-ip-adresa-ns1>; };

};

include "/etc/named.rfc1912.zones";

include "/etc/named.root.key";

```

Nakon konfiguracije sekundarnog poslužitelja, na primarnom je povećan serijski broj u datotekama zona kako bi obavijestio sekundarni o svojim DNS zonama. U tom trenutku su datoteke kopirane na sekundarni poslužitelj. Ovime je konfigurirano željeno DNS okruženje i ono je spremno za testiranje implementiranih sigurnosnih značajki.

6. Analiza razine sigurnosti implementiranog DNS rješenja

Sigurnosna analiza je proces procjene sigurnosti DNS infrastrukture domene, uključujući njene DNS poslužitelje, DNS zapise i mrežnu infrastrukturu koja podržava DNS. Primarni cilj sigurnosne analize DNS-a je identificirati potencijalne ranjivosti ili slabosti koje bi napadači mogli iskoristiti za kompromitiranje integriteta ili dostupnosti DNS-a ili za krađu osjetljivih informacija. U ovom poglavlju odabrani su i odrađeni pojedini testovi DNS-a kako bi se ispitala razina njegove sigurnosti. Svi testovi odrađeni su pomoću virtualnog stroja na kojemu je instaliran operacijski sustav Kali Linux verzije 2022.4.

6.1. Testiranje prijenosa datoteka DNS zona

Ovo je veoma važan test u procjeni sigurnosti DNS-a jer nam on može pomoći u prepoznavanju bilo kakvih neovlaštenih promjena ili nedosljednosti u DNS zapisima. Tijekom prijenosa zone, cijela datoteka zone se kopira s primarnog DNS poslužitelja na jedan ili više sekundarnih DNS poslužitelja. Taj prijenos bi trebao biti omogućen samo autoritativnim DNS poslužiteljima koji su definirani listom za kontrolu pristupa, što znači da u ovom slučaju klijent (Kali Linux) nebi trebao biti u mogućnosti prenijeti datoteku DNS zone na svoje računalo. Prijenos zone testiran je pomoću `dig` naredbe. Javna IP adresa `ns2` poslužitelja u trenutku testiranja je **104.197.65.23**.

```
└─(j0p4@kali) - [~]
└─$ dig axfr jtorbar-zavrsni.online @104.197.65.23
; <<>> DiG 9.18.11-2-Debian <<>> axfr jtorbar-zavrsni.online @104.197.65.23
;; global options: +cmd
; Transfer failed.

└─(j0p4@DESKTOP-OGJOI5P) - [~]
└─$ dig axfr 65.197.104.in-addr.arpa @104.197.65.23
; <<>> DiG 9.18.11-2-Debian <<>> axfr 65.197.104.in-addr.arpa @104.197.65.23
```

```
;; global options: +cmd
; Transfer failed.
```

Rezultatom **Transfer failed** možemo zaključiti kako je DNS poslužitelj prošao ovaj test budući da klijent nije mogao prenijeti datoteku zone **jtorbar-zavrsni.online**.

6.2. Testiranje DNS razlučivanja

Test DNS razlučivanja način je provjere funkcionalnosti i performansi DNS razlučivača. U ovom testu očekivani rezultat je uspješno razlučivanje DNS zapisa **ns2.jtorbar-zavrsni.online** i **104.197.65.23** i neuspješno razlučivanje **ns1.jtorbar-zavrsni.online**.

1. Test razlučivanja ns2.jtorbar-zavrsni.online

```
└─(j0p4@kali)-[~]
└─$ dig ns2.jtorbar-zavrsni.online @104.197.65.23
; <<>> DiG 9.18.11-2-Debian <<>> ns2.jtorbar-zavrsni.online @104.197.65.23
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8502
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: fab96b9e8cbf77750100000063effa7091e39bdeb865386b (good)
;; QUESTION SECTION:
;ns2.jtorbar-zavrsni.online.      IN      A
;; ANSWER SECTION:
ns2.jtorbar-zavrsni.online. 86400 IN      A      104.197.65.23
;; Query time: 140 msec
;; SERVER: 104.197.65.23#53(104.197.65.23) (UDP)
;; WHEN: Fri Feb 17 23:06:40 CET 2023
;; MSG SIZE rcvd: 99
```

Status **NOERROR** i odgovor **104.197.65.23** predstavljaju uspješno razlučivanje postavljenog upita.

2. Test razlučivanja 104.197.65.23

```
└─(j0p4@kali)-[~]
└─$ dig -x 104.197.65.23 @104.197.65.23
; <<>> DiG 9.18.11-2-Debian <<>> -x 104.197.65.23 @104.197.65.23
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61090
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: c26c9edfe3e628e60100000063eff8e1f9cbb73beaa1b7d2 (good)
;; QUESTION SECTION:
;23.65.197.104.in-addr.arpa.      IN      PTR
;; ANSWER SECTION:
23.65.197.104.in-addr.arpa. 86400 IN      PTR      ns2.jtorbar-zavrsni.online.
;; Query time: 129 msec
;; SERVER: 104.197.65.23#53(104.197.65.23) (UDP)
;; WHEN: Fri Feb 17 23:00:01 CET 2023
;; MSG SIZE rcvd: 123
```

Status NOERROR i odgovor ns2.jtorbar-zavrsni.online predstavljaju uspješno razlučivanje postavljenog upita.

3. Test razlučivanja ns1.jtorbar-zavrsni.online

```
└─(j0p4@kali)-[~]
└─$ dig ns1.jtorbar-zavrsni.online @104.197.65.23
; <<>> DiG 9.18.11-2-Debian <<>> ns1.jtorbar-zavrsni.online @104.197.65.23
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 25225
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
```

```

; COOKIE: dc7220db952c5b5c0100000063eff8ee90b275bb08ff4bc5 (good)

;; QUESTION SECTION:

;ns1.jtorbar-zavrsni.online.      IN      A

;; AUTHORITY SECTION:

jtorbar-zavrsni.online. 10800    IN      SOA      jtorbar-zavrsni.online.jtorbar-
zavrsni.online. root.jtorbar-zavrsni.online. 2 86400 3600 604800 10800

;; Query time: 129 msec

;; SERVER: 104.197.65.23#53(104.197.65.23) (UDP)

;; WHEN: Fri Feb 17 23:00:14 CET 2023

;; MSG SIZE rcvd: 169

```

Status NXDOMAIN i odgovor vrijednosti 0 predstavljaju neuspješno razlučivanje postavljenog upita.

Dobivenim rezultatima testiranja možemo zaključiti kako je DNS poslužitelj prošao i ovaj test budući da je odgovorio očekivano na upite o sekundarnom poslužitelju i nije otkrio privatnu IP adresu ns1 poslužitelja.

6.3. Testiranje DNSSEC funkcionalnosti

Testiranje DNSSEC-a odrađeno je u više koraka. Prvo je provjerena konfiguracija RRSIG zapisa za domenu jtorbar-zavrsni.online:

```

└─(j0p4@kali)-[~]
└─$ dig +dnssec ns2.jtorbar-zavrsni.online @104.197.65.23

; <<>> DiG 9.18.11-2-Debian <<>> +dnssec ns2.jtorbar-zavrsni.online
@104.197.65.23

;; global options: +cmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27418

;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:

; EDNS: version: 0, flags: do; udp: 1232

; COOKIE: 77df2458a7db58bc0100000063f017000cf85a8e8254e442 (good)

;; QUESTION SECTION:

```

```

;ns2.jtorbar-zavrsni.online.      IN      A
;; ANSWER SECTION:
ns2.jtorbar-zavrsni.online. 86400 IN      A      104.197.65.23
ns2.jtorbar-zavrsni.online. 86400 IN      RRSIG   A 13 3 86400 20230226042614
20230217230416 59069 jtorbar-zavrsni.online.
8XyM7Pg/r98Rf2UtFEv1Qt0jLot8CCy/Ws9NUxeJJy0tRRkUVorWLLa7
mlw+0LuvXBBcwVTfYtXOTUDKzhYP5A==
;; Query time: 140 msec
;; SERVER: 104.197.65.23#53(104.197.65.23) (UDP)
;; WHEN: Sat Feb 18 01:08:32 CET 2023
;; MSG SIZE rcvd: 217

```

Prisutnost zapisa RRSIG u sekciji odgovora označava da je DNS odgovor potvrđen pomoću DNSSEC-a. Točnije, RRSIG zapis se koristi za potpisivanje A zapisa za jtorbar-zavrsni.online domenu i pruža kriptografski dokaz da je zapis autentičan te da nije mijenjan.

Nakon RRSIG provjere, potrebno je provjeriti DNSKEY zapis za domenu.

```

└─(j0p4@kali)-[~]
└─$ dig +dnssec jtorbar-zavrsni.online DNSKEY @104.197.65.23
; <<>> DiG 9.18.11-2-Debian <<>> +dnssec jtorbar-zavrsni.online DNSKEY
@104.197.65.23
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29044
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 1232
; COOKIE: 3a25d049f70e16340100000063f01a566be182aacc0633f (good)
;; QUESTION SECTION:
jtorbar-zavrsni.online.      IN      DNSKEY

;; ANSWER SECTION:
jtorbar-zavrsni.online. 3600    IN      DNSKEY  257 3 13
VtdcWJahkP4u1t8CYTVVaCfQBn+M7aeEj4Wa3IVmm20Ups1V1ylQC5fj
IYrK02SABhGFotspS8lgraF+ZJqKDQ==

```

```

jtorbar-zavrsni.online. 3600 IN RRSIG DNSKEY 13 2 3600 20230304000416
20230217230416 59069 jtorbar-zavrsni.online.
tgby93w3TlVntZEhAJ+qE/WtPenIY01oNKossEWToS6QZ7ROJY5/CqCA
hKpAmRBo265VOWW1lSyh3df7+2vekA==

;; Query time: 140 msec
;; SERVER: 104.197.65.23#53(104.197.65.23) (UDP)
;; WHEN: Sat Feb 18 01:22:46 CET 2023
;; MSG SIZE rcvd: 277

```

Odgovor na DNS upit daje zapis DNSKEY i njegov odgovarajući RRSIG zapis. DNSKEY zapis sadrži javni ključ za zonu, a RRSIG zapis digitalni potpis DNSKEY zapisa privatnim ključem zone. Ove informacije upućuju na to da je odgovor autentičan.

Još je ostalo za provjeriti kompletan lanac povjerenja DNSSEC-a:

```

└─(j0p4kali)-[~]
└─$ dig +dnssec +trace jtorbar-zavrsni.online @104.197.65.23
; <<>> DiG 9.18.11-2-Debian <<>> +dnssec +trace jtorbar-zavrsni.online
@104.197.65.23
;; global options: +cmd
.                515174  IN      NS      d.root-servers.net.
.                515174  IN      NS      b.root-servers.net.
.                515174  IN      NS      j.root-servers.net.
.                515174  IN      NS      h.root-servers.net.
.                515174  IN      NS      a.root-servers.net.
.                515174  IN      NS      f.root-servers.net.
.                515174  IN      NS      l.root-servers.net.
.                515174  IN      NS      e.root-servers.net.
.                515174  IN      NS      m.root-servers.net.
.                515174  IN      NS      c.root-servers.net.
.                515174  IN      NS      k.root-servers.net.
.                515174  IN      NS      g.root-servers.net.
.                515174  IN      NS      i.root-servers.net.
.                515174  IN      RRSIG   NS 8 0 518400 20230302170000
20230217160000 951 . hY6cob4Q6WHk9LFmzVSwicnbeiuff3dNJ8xykB7K5EbTPhHw423ejKY4
Eg8PjnTFNIVnwO98ghJZclp8xjCgBOPxwmsnVQu+n5LNxvoeEjkkZAQK

```



```

FLvdY27ZA2IveXU/zyaJR194vOcdDtxdIz4zX2fYDjVkAwSqOAgMn8gP
pWO++LsCIemS1HmdVyLWXxFUNfC3UcxelEypQpGMyX427BRS8IPVRyG+
g/cnMIDHlohKg724wcJ/a9WPLyCsVWHSivy2hZx5EUxfiSt2LS2GQKfd
XcvB/NG58tmDkgUFG9GjvLuCYjHgDstWBMhEtv6wQXaYX2fq9XUM/9MF dP4sdw==

;; Received 1137 bytes from 104.197.65.23#53(104.197.65.23) in 139 ms
online.                172800  IN      NS      b.nic.online.
online.                172800  IN      NS      a.nic.online.
online.                172800  IN      NS      f.nic.online.
online.                172800  IN      NS      e.nic.online.
online.                86400   IN      DS      4267 8 2
66D7010609CB19E99AD1DA2833DDAB8CA2E7ACC1CE870CC28D29E76E B53D39BA
online.                86400   IN      DS      4267 8 1
A038DA06A96AD8E9BFE2BA78C392FF7804B4CD2B
online.                86400   IN      RRSIG   DS 8 1 86400 20230302170000
20230217160000 951 . RUD4pooF RKlYBcHjTDZXD4jXDs9osi7FrEmSojy6rb7sudMI/R5IXcz9
vcaJnH56mRvbHnYChoxT3fOBuVQIfikhVH1MIiYmQS+ctcoY+luFI45/
DW01KUtEMyC33tBDVrlYu3rs75KITwQNIueJirgX3qmbZC4/IJ4xMz2g
08ajEnca/4rlwFMundR4YlZnWVrLYeTGVivlt4nsyvH3E2VXqnRTW6Kr
tRFZU07TN+RqdmXV/Ahzf/OgradIi7sUvIb/KO97tihOFDoT1OJ3RuB9
h77EqkBS54QhtypH3+wXhA78jcn8zu4seR4/i8JJ+B/QAhHhwsSvShxN 8AftWA==

;; Received 700 bytes from 192.112.36.4#53(g.root-servers.net) in 40 ms
jtorbar-zavrsni.online. 3600   IN      NS      ns2.domain.com.
jtorbar-zavrsni.online. 3600   IN      NS      ns2.jtorbar-zavrsni.online.
1ribnbjb5koke6vekotivtq00v2eqsdj.online. 3600 IN NSEC3 1 1 0 -
1RIID8G9TUQKKQ0G8DOH8LU6FDDM3PU9 NS SOA RRSIG DNSKEY NSEC3PARAM
0ijfeo69mdnupn9b438c9p0mbjatu5if.online. 3600 IN NSEC3 1 1 0 -
0IKGVRDKR99EABON4TFF3SNJDIE1KTNK NS DS RRSIG
1ribnbjb5koke6vekotivtq00v2eqsdj.online. 3600 IN RRSIG NSEC3 8 2 3600
20230313152703 20230211125333 28569 online.
zPtMfGX2i115fRX47AGVFxRk0amMfIAu74qLZfRftly6bbbPVHt4d7Nk
bg0tX/bN7tN+ZLOWqln1FF2XBGAPJumz9vf841yyPcJiStCjffVf//oh
zMShOhNciAXW87R1nBS/5QcQBR3qaDElC4J7LOmoPlnb7EaFOYjPA3L3 AnQ=
0ijfeo69mdnupn9b438c9p0mbjatu5if.online. 3600 IN RRSIG NSEC3 8 2 3600
20230313084747 20230211105451 28569 online.
zBpSjPfkBRnMjtMz8uvX55WfqD8y0q3NP+louP5DEV6yoqLwZg/2Dz2
2wP3lABb9S/PPTB52e3UzsKUT5LFjgxTXiQDa8Az27KBTZxrB85PxqqL
raXyiUSLnXkUjNemzEfG3Rum3wfxMV82ULCGSQu5/sh1CP2CjrcKc5M rvM=

;; Received 626 bytes from 212.18.248.54#53(e.nic.online) in 39 ms

```

```
jtorbar-zavrsni.online. 10800 IN SOA jtorbar-zavrsni.online.jtorbar-  
zavrsni.online. root.jtorbar-zavrsni.online. 2 86400 3600 604800 10800  
;; Received 165 bytes from 104.197.65.23#53(ns2.jtorbar-zavrsni.online) in 129 ms
```

U svim ovim testovima korištena je `+dnssec` opcija koja omogućava DNSSEC validaciju. Kao što smo mogli vidjeti, u sva tri odrađena testa DNSSEC je validan. U zadnjem testu, korištenjem `+trace` opcije, izvršeno je praćenje kompletnog procesa razlučivanja DNS-a. Na njemu možemo vidjeti kako sve razine DNS hijerarhije imaju implementiran DNSSEC čime možemo potvrditi integritet dobivenog odgovora.

Na temelju rezultata sigurnosnog testiranja DNS-a, koje je uključivalo test prijenosa zone, testove razlučivanja DNS upita i DNSSEC testove, može se zaključiti da je testirani poslužitelj prošao i da se može smatrati sigurnim. Test prijenosa zone, koji se koristi za utvrđivanje može li napadač prenijeti popis svih DNS zapisa neke zone s poslužitelja, nije pokazao nikakvu naznaku ranjivosti. Testovi razlučivanja DNS upita, koji provjeravaju sposobnost poslužitelja za razlučivanje imena domena, pokazali su da je poslužitelj pouzdan i da može bez ikakvih problema obraditi DNS upite. Osim toga, DNSSEC testovi, koji provjeravaju je li poslužitelj pravilno konfiguriran za podršku sigurnosnih proširenja potvrdili su da poslužitelj ima implementiran DNSSEC i može pružiti sigurne i provjerene DNS odgovore.

Sve u svemu, rezultati sigurnosnog testiranja DNS-a daju uvjerenje da su u sklopu testiranog poslužitelja implementirane potrebne sigurnosne mjere kako bi osigurao integritet i dostupnost svojih DNS usluga.

Zaključak

Povijest DNS-a, ranjivosti, sigurnosne mjere i metode implementacije doprinose složenoj i ključnoj ulozi koju DNS igra u funkcioniranju interneta. Sigurnost DNS-a veoma je bitan aspekt kibernetičke sigurnosti. Kako bi se umanjio rizik od iskorištavanja potencijalnih ranjivosti te poboljšala zaštita DNS-a, implementirane su razne sigurnosne mjere. Isto tako, implementacija DNS usluga složen je proces koji zahtijeva pažljivo planiranje pa i izvođenje kako bi se minimalizirao rizik od napada koji bi mogli imati velik utjecaj na sustav. Uz specifične teme obrađene u prethodnim poglavljima, postoje mnoge druge implikacije kada je u pitanju sigurnost DNS-a.

Jedna od ključnih stavki je sve veća važnost interneta u svakodnevnom životu. Kako se sve više usluga seli online, sigurnost DNS-a postaje tim više relevantnijom. Kibernetički napadi mogu prouzročiti značajnu štetu ne samo pojedinačnim korisnicima, već cijelim organizacijama, pa čak i vladama. Ovo naglašava potrebu za snažnim sigurnosnim mjerama DNS-a te redovitim testiranjem njegove sigurnosti. Internet je globalna mreža, a prekidi DNS usluga mogu imati značajan utjecaj na korisnike širom svijeta. Naglasak je na potrebi za međunarodnom suradnjom i standardizacijom kada je u pitanju DNS sigurnost, kako bi se osiguralo da svi korisnici mogu pristupiti sigurnijem i pouzdanijem internetu. Sigurnost DNS-a kritično je pitanje sa širokim implikacijama koje se odnose na sve ljude diljem svijeta.

Bitna stvar za naglasiti je važnost obrazovanja i podizanje svijesti o kibernetičkoj sigurnosti. Kako kibernetički napadi postaju sve sofisticiraniji i češći, veoma je važno da pojedinci i organizacije budu informirani o najnovijim prijetnjama te implementacijama sigurnosnih mjera kontra istih. Obrazovanjem o najboljim praksama kibernetičke sigurnosti, pojedinci i organizacije mogu smanjiti vjerojatnost uspješnih napada.

Zaključno, valja napomenuti da je DNS sigurnost samo jedan dio veće slagalice kibernetičke sigurnosti. Organizacije moraju zauzeti čvrst pristup prema sigurnosti, uzimajući u obzir ne samo DNS već i druge komponente svoje mrežne infrastrukture.

Student vlastoručno potpisuje Završni rad na prvoj stranici ispred Predgovora s datumom i oznakom mjesta završetka rada te naznakom:

„Pod punom odgovornošću pismeno potvrđujem da je ovo moj autorski rad čiji niti jedan dio nije nastao kopiranjem ili plagiranjem tuđeg sadržaja. Prilikom izrade rada koristio sam tuđe materijale navedene u popisu literature, ali nisam kopirao niti jedan njihov dio, osim citata za koje sam naveo autora i izvor, te ih jasno označio znakovima navodnika. U slučaju da se u bilo kojem trenutku dokaže suprotno, spreman sam snositi sve posljedice uključivo i poništenje javne isprave stečene dijelom i na temelju ovoga rada“.

U Zagrebu, datum.

Ime Prezime

Popis kratica

DNS	<i>Domain Name System</i>	Sustav domenskih imena
DDoS	<i>Distrubuted Denial of Service</i>	Distribuirano uskraćivanje usluge
ARPANET	<i>Advanced Research Projects Agency Network</i>	Mreža Agencije za napredne istraživačke projekte
ARPA	<i>Advanced Research Projects Agency</i>	Agencija za napredne istraživačke projekte
IPTO	<i>Information Processing Techniques Office</i>	Ured za tehnike obrade informacija
RFC	<i>Request for Comments</i>	Dopis
MIT	<i>Massachusetts Institute of Technology</i>	Tehnološki institut Massachusetts
SRI	<i>Stanford Research Institute</i>	Istraživački institut Stanford
UCLA	<i>University of California, Los Angeles</i>	Kalifornijsko sveučilište, Los Angeles
UCSB	<i>University of California, Santa Barbara</i>	Kalifornijsko sveučilište, Santa Barbara
SDS	<i>Scientific Data System</i>	Sustav znanstvenih podataka
NCP	<i>Network Control Protocol</i>	Protokol za upravljanje mrežom
TCP	<i>Transmission Control Protocol</i>	Protokol kontrole prijenosa
IP	<i>Internet Protocol</i>	Internetski protokol
UCL	<i>University College London</i>	University College London
TLD	<i>Top Level Domain</i>	Domena najviše razine
gTLD	<i>Generic Top Level Domain</i>	Generička domena najviše razine
ccTLD	<i>Country Code Top Level Domain</i>	Domena koda države najviše razine
SLD	<i>Secondary Level Domain</i>	Domena druge razine
DoS	<i>Denial of Service</i>	Uskraćivanje usluge
DDoS	<i>Distributed Denial of Service</i>	Distribuirano uskraćivanje usluge
UDP	<i>User Datagram Protocol</i>	User Datagram Protocol
HTTP	<i>Hyper Text Transfer Protocol</i>	Hyper Text Transfer Protocol
IoT	<i>Internet of Things</i>	Internet stvari
ACL	<i>Access Control List</i>	Lista za kontrolu pristupa
DNSSEC	<i>DNS Security Extensions</i>	DNS sigurnosna proširenja
E2E	<i>End-to-End</i>	S kraja na kraj
ZSK	<i>Zone Signing Key</i>	Ključ za potpisivanje zone

KSK	Key Signing Key	Ključ za potpisivanje ključa
DoH	DNS-over-HTTPS	DNS putem HTTPS-a
DoT	DNS-over-TLS	DNS putem TLS-a
IPS	Intrusion Prevention System	Sustav za sprječavanje upada
IDS	Intrusion Detection System	Sustav za detekciju upada
SIEM	Security information and Event Management	Sustav za sigurnosne informacije i upravljanje događajima
ISC	Internet Systems Consortium	Konzorcij internetskih sustava
BIND	Berkley Internet Name Domain	Berkley Internet Name Domain
GCP	Google Cloud Platform	Google Cloud platforma
API	Application Programming Interface	Sučelje za programiranje aplikacija
VPC	Virtual Private Cloud	Virtualni privatni oblak
SSH	Secure Socket Shell	Secure Socket Shell

Popis slika

Slika 2.1 Čvorovi ARPANETa u prosincu 1969. Godine (TechTarget Arpanet Definition)	3
Slika 2.2 Hijerarhijska struktura DNS-a.....	6
Slika 3.1 Primjer kompromitacije DNS poslužitelja	9
Slika 3.2 Toplinska karta koja prikazuje nedostupnost interneta tijekom napada na Dyn (Khandelwal, 2016.)	10
Slika 4.1 DNSSEC lanac povjerenja (Kreuger, 2023.).....	15
Slika 4.2 Pojednostavljeni prikaz DNS komunikacije putem HTTPS/TLS protokola [14]	16
Slika 5.1 Nadzorna ploča projekta „jtorbar-završni“ unutar Google Cloud platforme	20
Slika 5.2 VPC network sučelje unutar GCP konzole	24
Slika 5.3 Compute Engine sučelje unutar GCP konzole	24
Slika 5.4 SSH veza prema virtualnom stroju uspostavljena putem web preglednika	25
Slika 5.5 Skica virtualne infrastrukture u oblaku	26

Popis tablica

Tablica 1 – dimenzije korištenih virtualnih strojeva (instanci) unutar Google Cloud platforme.....	21
--	----

Literatura

- [1] LICKLIDER, J.C.R. *Libraries of the future*. Cambridge: MIT Press, 1965.
[Libraries of the future : Licklider, J. C. R. : Free Download, Borrow, and Streaming : Internet Archive](#)
- [2] TECHTARGET ARPANET Definition
<https://www.techtargget.com/searchnetworking/definition/ARPANET>
- [3] PELKEY J., *The History of Computer Communications*
<https://historyofcomputercommunications.info/>
- [4] CERF, V.G.; KAHN, R.E. *A Protocol for Packet Network Intercommunication*, 1974.
<https://www.cs.princeton.edu/courses/archive/fall06/cos561/papers/cerf74.pdf>
- [5] MOCKAPETRIS, P. RFC882, 1983.
[RFC 882 - Domain names: Concepts and facilities \(ietf.org\)](#)
- [6] MOCKAPETRIS, P. RFC883, 1983.
[RFC 883 - Domain names: Implementation specification \(ietf.org\)](#)
- [7] MOCKAPETRIS, P. RFC1034, 1987.
[RFC 1034 - Domain names - concepts and facilities \(ietf.org\)](#)
- [8] MOCKAPETRIS, P. RFC1035, 1987.
[RFC 1035 - Domain names - implementation and specification \(ietf.org\)](#)
- [9] KUMAR, M. *Pakistan Domain Registrar Hacked*
<https://thehackernews.com/2013/02/pakistan-domain-registrar-pknic-hacked.html>
- [10] KASPERSKY *Operation ShadowHammer*
https://www.kaspersky.com/about/press-releases/2019_operation-shadowhammer-new-supply-chain-attack
- [11] KHANDELWAL, S. *Massive DDoS Attack Against Dyn DNS Service Knocks Popular Sites Offline*
<https://thehackernews.com/2016/10/dyn-dns-ddos.html>
- [12] NETWORK WORKING GROUP RFC4033, 2005.
[RFC 4033 - DNS Security Introduction and Requirements](#)
- [13] KREUGER, R. *Review of social media traffic at the DNS resolvers and their security implementation, 2023*.
<https://essay.utwente.nl/94417/>
- [14] INFOBLOX How to configure DoT/DoH
<https://blogs.infoblox.com/security/how-to-configure-dot-doh/>

- [15] HOFFMAN, P.; ICANN; MCMANUS, P.; MOZILLA RFC8484, 2018.
[RFC 8484 – DNS Queries over HTTPS \(DoH\)](#)
- [16] HU Z.; ZHU, L.; HEIDEMANN, J. ET AL. RFC 7858, 2016.
[RFC 7858 – Specification for DNS over Transport Layer Security \(TLS\)](#)