Iskorištavanje propusta u mrežnim protokolima i zaštita računalnih mreža

Ivoš, Venci

Sveučilište u Zadru

Odjel za informacijske znanosti

Stručni prijediplomski studij

Informacijske tehnologije

Venci Ivoš

Iskorištavanje propusta u mrežnim protokolima i zaštita računalnih mreža

Završni rad

Zadar, 2024.

Sveučilište u Zadru
Odjel za informacijske znanosti
Stručni prijediplomski studij
Informacijske tehnologije

Iskorištavanje propusta u mrežnim protokolima i zaštita računalnih mreža

Završni rad

Student/ica:
Venci Ivoš

Mentor/ica:
mag.ing.inf.et.comm.teh Marko Buterin

Zadar, 2024.

Izjava o akademskoj čestitosti

Ja, **Venci Ivoš,** ovime izjavljujem da je moj **završni** rad pod naslovom **Iskorištavanje propusta u mrežnim protokolima i zaštita računalnih mreža** rezultat mojega vlastitog rada, da se temelji na mojim istraživanjima te da se oslanja na izvore i radove navedene u bilješkama i popisu literature. Ni jedan dio mojega rada nije napisan na nedopušten način, odnosno nije prepisan iz necitiranih radova i ne krši bilo čija autorska prava.

Izjavljujem da ni jedan dio ovoga rada nije iskorišten u kojem drugom radu pri bilo kojoj drugoj visokoškolskoj, znanstvenoj, obrazovnoj ili inoj ustanovi.

Sadržaj mojega rada u potpunosti odgovara sadržaju obranjenoga i nakon obrane uređenoga rada.

Zadar, 30. rujna 2024.

Iskorištavanje propusta u mrežnim protokolima i zaštita računalnih mreža

SAŽETAK

Krajem 20-og stoljeća dolazi do široke primjene Internet tehnologije u društvu. Komercijalizacijom informatičke opreme dolazi do značajnog pada cijena informatičke opreme čime ista postaje dostupna i privatnim korisnicima. Masovno korištenje informatičke opreme dovodi do razvoja Interneta u svrhu brze povezanosti i izrade raznih informativnih sadržaja koji su brzo dostupni. Rastom podataka na Internetu dolazi do potrebe za povećanjem brzine i propusnosti prijenosa podataka te razvojem kvalitetnije mrežne opreme te izradom raznih protokola koji omogućuju opremi funkcioniranje bez potrebe za intervencijom stručnjaka pri kvaru pojedinog segmenta mreže ili pojedinog djela mrežne opreme. Općom dostupnosti Interneta dolazi do zlouporabe istog za iskorištavanje raznih sigurnosnih propusta u protokolima i aplikacijama. U ovom radu opisujemo radni okvir Yersinia koji služi za provjeru i iskorištavanje propusta u nekim protokolima koji se koriste pri radu mrežne opreme.

Ključne riječi: Računalne mreže, TCP/IP, OSI, Mrežni napadi, Yersinia

Exploiting loopholes in network protocols and protecting computer networks

SUMMARY

At the end of the 20th century, Internet technology was widely used in society. The commercialization of IT equipment leads to a significant drop in prices of IT equipment, which makes it available to private users as well. The mass use of IT equipment leads to the development of the Internet for the purpose of fast connection and the creation of various informational contents that are quickly available. With the growth of data on the Internet, there is a need to increase the speed and bandwidth of data transmission and to develop better quality network equipment and create various protocols that enable the equipment to function without the need for expert intervention in the event of failure of a particular segment of the network or a particular part of the network equipment. Due to the general availability of the Internet, it is misused to exploit various security flaws in protocols and applications. In this paper, we describe the Yersinia framework that is used to check and exploit vulnerabilities in some protocols used in the operation of network equipment.

Key words: Computer networks, TCP/IP, OSI, Network attacks, Yersinia

SADRŽAJ :

UVOD

Mrežna oprema koja se koristi u lokalnim mrežama posjeduje ugrađene razne protokole koji olakšavaju mrežnim administratorima rad. Svaki proizvođač mrežne opreme ima izrađena vlastita rješenja za standardne protokole.

Svi protokoli se mogu podešavati statično tako da novi korisnici u mreži nemaju pristup i ne mogu koristiti računalnu mrežu dok ne dobiju odobrenje od mrežnog administratora i on ih autorizira na mreži.

Da bi se olakšalo spajanje na takve mreže napravljeni su automatski načini rada protokola gdje se razmjenjuju paketi između mrežne opreme ili novog računala u mreži i na taj način se autorizira računalo ili mrežni dio opreme da funkcionira u mreži.

U ovom radu opisujemo radni okvir Yersinia koji ima ugrađene napade za neke protokole 2 sloja mreže.

1. Računalne mreže

Osnovni koncept komunikacije se sastoji od tri ključna elementa. Prvi element je postojanje dva entiteta koji će komunicirati, nazvana pošiljatelj i primatelj koji imaju potrebu za razmjenom informacija. Drugi element je medij preko kojeg će se prenijeti informacija. Treći i posljednji element je prihvaćeni skup pravila komunikacije ili protokola. Navedeni elementi su potrebni u bilo kojoj vrsti komunikacije[1].

Kad su se računala počela primjenjivati u poslovanju stvorila se i potreba za razmjenom podataka. U početku se razmjena vršila pomoću prenosivih medija za pohranu podataka koji su bili ograničeni svojim kapacitetom. Prijenos podataka na manjim udaljenostima je bio ograničen kapacitetom medija a na većim udaljenostima su se koristile i službe za dostavu što je povećalo vrijeme potrebno za prijenos podataka i postojala je mogućnost gubitka podataka u slučaju oštećenja medija za pohranu.

Potrebe za prijenosom podataka između računala su dovele do razvoja TCP/IP protokola. Istraživanje TCP/IP protokola je dovelo do razvoja više tipova mrežnih organizacija kao što su Talking Ring i Ethernet. Računalne mreže su u početku razvoja postizale niske brzine prijenosa podataka usporedno s brzinama koje su postignute u današnje vrijeme. Razmjena podataka se vršila u tekstualnom obliku te bi se u sekundi prenijelo nekoliko znakova[2].

Omogućavanjem spajanje više računala unutar jedne lokalne mreže dovelo je do razvoja raznih uređaja koji se mogu spajati na mrežu (kamere, hladnjaci, sustavi za grijanje kuća i razni strojevi) i raditi razmjenu podataka na malim i velikim udaljenostima. U konačnici dolazi do stvaranja novog pojma internet stvari (*eng. IOT – Internet of Things*). Povezivanjem raznih računalnih sustava u globalnu mrežu dovodi do razvoja raznih programa kojima je svrha omogućiti pristup sustavima, onesposobiti sustav ili zaključati podatke unutar sustava.

Najslabija karika pri napadima na računalne sustave je čovjek koji koristi taj sustav. Korisnik ima izravan pristup sustavu i njegovo nepoznavanje postojećih prijetnji i načina napada na sustav predstavlja prvu ranjivu točku svakog računalnog sustava. Poslodavci ne mogu očekivati od svih djelatnika da imaju visoku informatičku pismenost te da znaju samostalno prepoznati potencijalnu prijetnju ili napad na sustav, što je dovelo do potrebe za angažiranjem stručnjaka kojima je posao da podešavaju, održavaju i nadziru rad računalnog sustava. Razvojem tehnologija računalni sustav je doveo do potrebe da se podijele uloge zaštite računalnog sustava

[1] Kizza, Migga, Joseph. 2005. Computer Network Security. University of Tennessee-Chattanooga Chattanooga,: Springer.

[2] Bošnjaković, Robert. 2011. Model lokalnih i globalnih računalnih mreža. Sveu. J. J. Stross. Rad, Dipl.

(sistem administrator, mrežni administrator, administrator baze podataka itd.) jer jedna osoba ne može imati kvalitetno znanje iz svih područja informacijskih tehnologija.

2. Terminologija računalnih mreža

2.1 Pasivna oprema

Koaksijalni kabel sastoji od središnjeg bakrenog vodiča koji je obložen plastičnom izolacijom koja je obavijena upletenom bakrenom ovojnicom, te na kraju je sve obavijeno plastičnom izolacijom. Upletena bakrena ovojnica služi da apsorbira elektromagnetske smetnje i šumove da se ne miješaju s signalom koji prenosi podatke[3].

Uvrnuta parica sastoji se od osam isprepletenih žica u parovima. Ta četiri para su omotana vanjskom ovojnicom, a mogu biti omotani u zaštitu protiv smetnji i bez zaštite od vanjskih smetnji[3].

Optička vlakna – sastoje se od jezgre koja vodi svjetlo i skup ovojnica koji služe za zaštitu te jezgre. Može biti single mode (svjetlo ulazi pod samo jednim kutom) i multimode (svjetlost može ući u vodič pod više kutova u određenom rasponu.)[3].

Konektori za optička vlakna su SC-DC, LC, MT-RJ, Duplex SC, Volition, Fiber – Jack[3].

Patch panel – služi za koncentriranje dolaznih kablova kroz utičnice koje su razmještene po prostorijama koje pokriva lokalna mreža. Iz patch panela se kablovima povezuju računala spojena na dolazne kablove sa aktivnom opremom. Obično povezane sa preklopnikom[3].

Komunikacijski ormar služi za smještaj pasivne i aktivne mrežne opreme[3].

[3] Bošnjaković, Robert. 2011. Model lokalnih i globalnih računalnih mreža. Sveu. J. J. Stross. Rad, Dipl.

2.2 Aktivna oprema

2.2.1 Mrežna kartica

Mrežna kartica ili NIC (*eng. Network Interface Controller*) je uređaj koji služi za povezivanje računala sa računalnom mrežom. Svaka mrežna kartica ima jedinstvenu MAC - Kontrola pristupa medijima (eng. Media Access Control) adresu i zbog toga ovaj uređaj radi na drugom sloju referentnih modela OSI i TCP\IP. MAC adresa se sastoji od 48-bitne broja podijeljenog u šest okteta koji su prikazani u heksadekadskom sustavu. Prema IEEE - Institut inženjera elektrotehnike i elektronike (*eng. Institute of Electrical and Electronics Engineers*) standardu prva tri okteta određuju proizvođača dok druga tri određuju serijski broj kartice. U početku su se mrežne kartice proizvodile kao zaseban element računala dok su se kasnije počela integrirati u matičnu ploču. Mrežne kartice su koristile više konektora za spajanje AUI - Sučelje jedinice za pričvršćivanje (eng. Attachment Unit Interface), BNC (inicijali Bayonet Neill-Concelman) i RJ (Registered Jack) od kojih je RJ-45 trenutno najčešći u primjeni[4].

2.2.2 HUB

HUB je mrežni uređaj koji radi na prvom sloju referentnih modela OSI i TCP/IP. Na HUB - u se nalazi više priključaka na koje se spajaju računala, serveri ili oprema koja se spaja u računalnu mrežu. HUB funkcionira tako da podatke koje primi na jednom portu odašilje na sve preostale portove. Takva funkcionalnost predstavlja problem jer svako računalo u mreži može primiti podatke iako nisu namijenjeni za njih i dolazilo je do kolizije poslanih i primarnih podataka. Zbog takve funkcionalnosti imamo CSMA/CA „senzora“ koji ima višestruki pristup izbjegavanju protokola u mrežama. Razvijen je da se smanjio potencijalni sudar kada više stanica šalju svoje signale preko sloja podatkovne mreže. Dok CSMA/DC se koristi za poboljšanje performansi CSMA prekidanjem prijenosa čim se otkrije kolizija, čime se skraćuje vrijeme potrebno prije pokušaja ponovnog slanja.

[4] Lončar, Saša. 2015. Računarske mreže i umrežavanje Raspberry PI uređaja. Polit. Pula. Rad, Završni, Specijalistički.

Postoje dvije vrste HUB uređaja, aktivni i pasivni. Aktivni HUB ima funkcionalnost obnavljanja signala dok pasivni HUB samo ima spojene konektore koje dolaze od ostalih računala. Zbog svoje ograničene funkcionalnosti i pojeftinjenja preklopnika opreme prestao se koristiti[5].

2.2.3 Preklopnik

Preklopnik (*eng. Switch*) je mrežni uređaj koji radi na drugom sloju referentnih modela OSI i TCP/IP. Uređaji koji se spojene na preklopnik javljaju svoju MAC adresu te je preklopnik zapisuje su svoju ARP - Protokol za rješavanje adresa (*eng. Address Resolution Protocol*) tablicu. Komunikacija preko preklopnika se vrši od točke do točke gdje se paketi šalju sa jednog računala na drugo računalo koje je specificirano po MAC adresi, osim ako nije poslan paket emitiranja koji se šalje na sve uređaje u mreži. U zaglavlje podatkovnog paketa se zapisuje MAC adresa računala kojemu se šalje paket i adresa računala koje šalje paket, na osnovu čega računalo koje primi paket zna kome treba vratiti podatke. Naprednije verzije preklopnika imaju mogućnost smanjenja domene razašiljanja kreiranjem VLAN - ova i usmjeravanje prometa preko logičkih IP adresa[6].

2.2.4 Usmjerivač

Usmjerivač (*eng. Router*) je mrežni uređaj koji radi na trećem sloju referentnih modela OSI i TCP/IP. Uloga usmjerivača je da povezuje više različitih mreža. Usmjeravanje podatkovnih paketa vrši prema podatku o IP - Adresa internetskog protokola (*eng. Internet Protocol address*) adresi. Usmjerivač ima podatke o svim mrežama na koje je spojen i njih zapisuje u routing tablicu (tablicu usmjeravanja). Iz zaglavlja podatkovnog paketa usmjerivač iščitava odredišnu adresu i pomoću routing tablice znaju na koji port treba slati podatke. Ukoliko nema u routing tablici zapis o mreži za koju je namijenjen podatkovni paket on ga odbacuje. Usmjerivači imaju ugrađene protokole koji im služe da se dogovaraju međusobno o mrežama koje su na njih spojene te tako popunjavaju sami routing tablice[5].

---

[5] Kizza, Migga, Joseph. 2005. Computer Network Security. University of Tennessee-Chattanooga Chattanooga,: Springer.

[6] Bošnjaković, Robert. 2011. Model lokalnih i globalnih računalnih mreža. Sveu. J. J. Stross. Rad, Dipl.

2.2.5 Firewall

Vatrozid (*eng. Firewall*) je mrežni uređaj koji radi na četvrtom nivou referentnih modela OSI i TCP/IP. Uloga Vatrozida je da blokira promet između dvije točke po pravilima koja se definiraju unutar uređaja.Uređaj se najčešće postavlja između lokalne mreže i routera ali ima i drugih kombinacija gdje se koriste zonske mreže. Pravila propusnosti se definiraju u kojem smjeru smije ići promet po određenoj adresi i portu. Pomoću vatrozida se također može pratiti promet unutar mreže. Postoji i programski vatrozid ali njegova je uloga obrana i reguliranje prometa prema klijentu i od njega[7].

3. Podjela računalnih mreža

Razvojem računala dovelo je do razvoja računalnih mreža koje se sastoje od velikog broja povezanih računala. Računalne mreže možemo podijeliti po tehnologiji prijenosa, topologiji i veličini.

3.1 Podjela računalne mreže prema veličini

Prema veličini računalne mreže možemo podijeliti na LAN, MAN i WAN. Svaki tip mreže ima svoju veličinu odnosno koji prostor zauzima. Tako je LAN – Lokalna mreža (eng. Local Area Network) mreža koja je ograničena najčešće u jednoj prostoriji (soba). MAN (Metropolitan Area Network) je mreža koja svojom veličinom pokriva jedan grad ili naselje. WAN (Wide Area Network) je mreža koja se sastoji od više LAN – ova. Pokriva veće geografsko područje od LAN i MAN mreže. Služi za povezivanje računala u različitim gradovima, zemljama[7].

3.2 Podjela računalnih mreža prema tehnologiji prijenosa

Podjela prema tehnologiji prijenosa ima dvije vrste mreža:

1. Difuzijske mreže
2. Mreže od točke do točke

[7] Kizza, Migga, Joseph. 2005. Computer Network Security. University of Tennessee-Chattanooga Chattanooga,: Springer.

Difuzijske mreže koriste jedan komunikacijski kanal koji dijele svi uređaji na mreži. U ovom prijenosu postoji adresno polje koje određuje kojem uređaju je poslani paket namijenjen.

Mreže od točke do točke sastoje se od više međusobno povezanih uređaja, te paket na svom putu od izvora do odredišta može proći više čvorova.

Difuzijski pristup najčešće koriste lokalne mreže dok globalne koriste mreže od točke do točke[8].

3.3 Podjela računalnih mreža prema topologiji

Topologija označava geometrijski razmještaj veza i čvorova koji čine mrežu. Čvorovi su mjesta u mreži na koja je moguće priključiti mrežnu stanicu. Čvorovi međusobno komuniciraju kroz kombinaciju logičke i fizičke veze.

Logička veza je veza između dva čvora koja međusobno komuniciraju bez obzira da li postoji između njih direktna fizička veza ili ne[8].

3.3.1 Zvijezda

U zvjezdastoj mreži svi su čvorovi povezani na zajednički čvor. U ovoj topologiji glavnina složenosti mreže je u centralnom čvoru, preko kojeg se sve odvija. Centralni čvor može postati opterećen zbog velikog broja čvorova i zbog povećanog prometa. Zbog toga ova topologija nije prihvaćena u LAN mrežama[9].

3.3.2 Prsten

U prstenastoj mreži svi čvorovi su povezani pojedinačnim vezama tako da čine zatvorenu strukturu. Svaki čvor mora imati repetitor koji prima i odašilje poruku. Repetitor mora konstantno biti uključen jer poruke moraju slobodno cirkulirati mrežom. Repetitor služi kako bi svaki čvor prepoznao poruku, te ako poruka nije namijenjena njemu, šalje ju dalje[9].

[8] Testa, Ivan. 2019. Računalne mreže i umrežavanje. Dubrovnik: Dub. Sveu. Rad, Završni.

[9] Pralas, Toni. 2008. Računalne mreže – Mrežne topologije. sysportal.carnet.hr.

3.3.3 Sabirnica

Kod sabirničke mreže svi čvorovi su spojeni na jedan prijenosni medij to jest sabirnicu. Poruke stižu do svih čvorova koji prepoznaju poruke koje su njima upućene. Priključak na sabirnici je pasivan pa je domet sabirnice ograničen snagom odašiljača poruke. U ovakvoj topologiji kvar jednog čvora ne djeluje na druge[10].

3.3.4 Stablo

Ova mreža je modifikacija sabirnice na način da se prijenosni mediji dijele na više grana koji polaze od iste točke. Ova mreža zahtjeva upotrebu određenih aktivnih naprava za regeneriranje signala[10].

3.3.5 Isprepletena mreža

U isprepletenoj mreži uređaji su spojeni redundantnim vezama između čvorova. U ovoj mreži poslana poruka može putovati bilo kojim putem. U isprepletenoj mreži svaki čvor ima vezu s drugim čvorom[10].

4. Referentni modeli OSI i TCP/IP

U ranim danima mreža, većina sustava koristila je vlasnički softver i protokole koji bi omogućili samo komunikaciju s drugim uređajima istog proizvođača ili onih proizvođači koji su imali pristup tim protokolima. U to vrijeme to nije bilo problem jer bi organizacije kupovale svoju opremu od istog proizvođača i nije bilo pravih sredstava komunikacije izvan organizacija. Međutim, s vremenom se to promijenilo i sada postoji potreba za komunikacijom sa sustavima u vlasništvu drugih organizacija. Malo je vjerojatno da je druga organizacija imala opremu istog proizvođača, pa nije bilo načina da ti uređaji međusobno razgovaraju. Za borbu protiv toga, zahtjev je bio napravljeno za izradu standardnog modela koji će biti javno dostupan svima za korištenje.

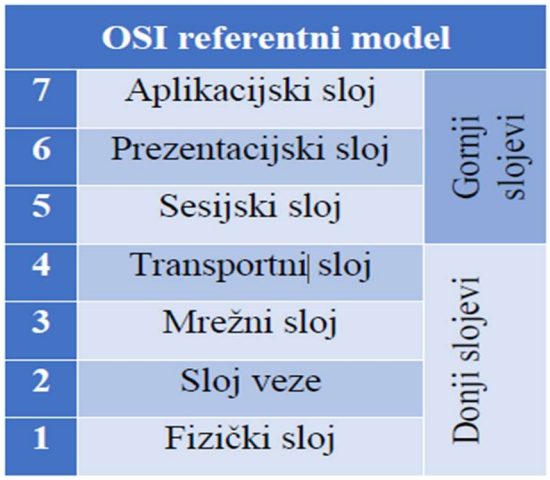
[10] Pralas, Toni. 2008. Računalne mreže – Mrežne topologije. sysportal.carnet.hr.

Dva modela koja su postala standard bila su sljedeća:

- Open Systems Interconnection (OSI) model koji je uvela Internacionalna Organizacija za standarde (ISO).
- TCP/IP model koji je rezultat istraživanja i razvoja protokola provedenog na eksperimentalnim komutiranim mrežnim paketima ARPANET, koju financira Agencija za napredne obrambene projekte (DARPA), i općenito se naziva skupom TCP/IP protokola. Ovaj skup protokola se sastoji od velike zbirke protokola koji su izdani kao Internet standardi od strane Odbora za Internet aktivnosti (*eng. IAB - Internet Activities Board*)[11].

4.1 Referentni model OSI

OSI model je mrežni model koji se sastoji od sedam pojedinačnih slojeva, kao što je prikazano na sljedeći dijagram. Svaki od ovih slojeva komunicira sa slojevima koji su mu susjedni i njegovom ekvivalentnom sloju na prijemnom uređaju:



Slika 1. OSI Model [Izvor: Obrada autora]

[11] Hunt, Craig, 2002. TCP/IP Network Administration. Gravenstein Highway North, Sebastopol: O'Reilly Media, Inc.

Gornja tri sloja (aplikacijski, prezentacijski i sesijski) nazivaju se gornjim slojevima. Navedena su četiri donja sloja (transportni, mrežni, sloj veza, fizički) kao niži slojevi. OSI model dopušta komunikacija sa susjednim slojevima. To znači da sloj aplikacije može razgovarati s prezentacijskim sloj, prezentacijski sloj može razgovarati s aplikacijskim slojem i sesijskim slojem, sloj sesije može razgovarati s prezentacijskim slojem i transportnim slojem i tako dalje. Ovaj slojeviti pristup pojednostavljuje proces razvoja[12].

Kako podaci prolaze kroz OSI model prolaze kroz proces naziva enkapsulacija. Enkapsulacija je jednostavno uzimanje podataka iz prethodnog sloja dodajući mu zaglavlje i prosljeđujući ga na sljedeći sloj gdje se proces se ponavlja. Na uređaju za primanje, zaglavlja se uklanjaju prije prosljeđivanja podataka do sljedećeg sloja. Ovaj proces se naziva dekapsulacija. Zaglavlja sadrže ključne informacije o obradi podataka.

4.1.1 Sloj 7 – Aplikacijski sloj

Aplikacijski sloj djeluje kao sučelje između aplikacije i mrežnog modela. Svaka aplikacija koja podržava mrežnu komunikaciju bit će razvijena pomoću sučelja aplikacijskog programiranja (*eng. API - Application Programming Interfaces*). API sadrži kod koji govori aplikaciji kako razgovarati s aplikacijskim slojem. Umjesto da je aplikacija na aplikacijskom sloju, postoji niz aplikacijskih protokola koje će aplikacija podržavati[13]. Neki od ovih uobičajenih protokola uključuju sljedeće:

- Jednostavan protokol prijenosa poruka (*eng. SMTP - Simple Message Transfer Protocol*)
- Protokol pošte (*eng. POP - Post Office Protocol*)
- Protokol za pristup internetskim porukama (*eng. IMAP - Internet Message Access Protocol*)
- Protokol prijenosa hiperteksta (*eng. HTTP - Hypertext Transfer Protocol*)
- Sustav naziva domene (*eng. DNS - Domain Name System*)
- Sigurna školjka (*eng. SSH - Secure Shell*)
- Protokol za prijenos datoteka (*eng. FTP - File Transfer Protocol*)

[12] Balchunas , Aaron. 2012. OSI Reference Model v1.31.

[13] CERT, CARNet. i LS&S. Sigurnosni model mreže računala. CCERT-PUBDOC-2009-01-253 Revizija 1.02.

4.1.2 Sloj 6 – Prezentacijski sloj

Prezentacijski sloj preuzima podatke koji su mu proslijeđeni iz aplikacijskog sloja i pretvara ga u generički format ili sintaksu. Neki od podataka koji se prevode bit će vrlo složeni i moraju se pretvoriti u plošnu datoteku, spremnu za prijenos primatelju. Ovaj serijaliziran tok podataka prima uređaj primatelj, deserializira ga i pretvara u njegov izvorni oblik. Pretvaranjem podataka u generički format, omogućuje svakom uređaju da razumije primljene podatke, prema prefiksu dokumenta će ih moći uzeti i pretvoriti u formatu koji aplikacija primatelj može razumjeti. Osim pretvaranja podataka, prezentacijski sloj također pruža kompresiju podataka i šifriranje/dešifriranje[14]. Neki od generičkih standarda koji se koriste na ovom sloju uključuju sljedeće:

- JPEG
- ASCII
- TIFF
- GIF

4.1.3. Sloj 5 – Sesijski sloj

Sloj sesije odgovoran je za upravljanje sesijama između uređaja. Upravljanje sesije uključuje uspostavljanje sesije, sinkronizaciju komunikacije između uređaja i prekid sesije[14]. Upravo na ovom sloju uređaji se dogovaraju o vrsti komunikacije koju će koristiti:

- Simpleks
- Polu-dupleks
- Puni dupleks

Protokoli koji su podržani na ovom sloju uključuju sljedeće:

- RPC
- SQL

Protokol tuneliranja od točke do točke (*eng. PPTP - Point-to-Point Tunneling Protocol*)

[14] Balchunas , Aaron. 2012. OSI Reference Model v1.31.

4.1.4. Sloj 4. – Transportni sloj

Transportni sloj odgovoran je za komunikaciju između korisnika i stvaranje logičkih vezu između dva uređaja. To uključuje pokretanje veze između uređaji, upravljanje protokom između uređaja, osigurava isporuka podataka i multipleks komunikaciju. Dva glavna protokola na transportnom sloju su sljedeća:

- TCP (*eng. Transmission Control Protocol*)
- UDP (*eng. User Datagram Protocol*)

Oba protokola uključuju kontrolni zbroj. Ovaj kontrolni zbroj je sredstvo za otkrivanje grešaka. Kada se podaci obrađuju za slanje, uređaj za slanje vrši izračun koji generira vrijednost na temelju podataka koji se šalju. Prijemni uređaj radi isto izračun, ako se vrijednost podudara, podaci su točni. Druga značajka koja im je zajednička je mogućnost obavljanja multipleks komunikacija. Druga zajednička značajka je korištenje logičkih portova[15].

4.1.4. Sloj 3. – mrežni sloj

Mrežni sloj OSI modela odgovoran je za logičko adresiranje uređaja korištenjem IP adresa. Također je odgovoran za odabir ruta za prijenos podataka, odnosno puta kojim dolaze od računala A do računala B. Što se tiče protokola na mrežnom sloju, najčešći su sljedeći:

- IP
- Internetska razmjena paketa (*eng. IPX - Internetwork Packet Exchange*)

Na ovom sloju, jedinica podataka protokola naziva se paketom i njegovo zaglavlje će uključivati izvornu i odredišnu IP adresu[15].

[15] Balchunas , Aaron. 2012. OSI Reference Model v1.31.

4.1.5. Sloj 2 – sloj veze

Moglo bi se tvrditi da je sloj veze relevantan samo unutar vaše pod mreže, iako je to u određenoj mjeri točno, još uvijek nam je potrebno za prijenos podataka izvan naših pod mreže. Sloj podatkovne veze stvara logičku vezu između čvorova na pod mreži. Ako su podaci za uređaj unutar iste pod mreže, veza će biti s tim uređajem, ako su podaci namijenjeni uređaju izvan pod mreže, veza će biti sa zadanim pristupnikom. Jedinica podataka protokola na sloju dva je okvir.

Sloj je podijeljen u dva podsloja:

Kontrola logičke veze (LLC - Logical Link Control): Zadatak LLC-a je da djeluje kao sučelje s mrežnim slojem i identificira koji se protokol mrežnog sloja koristi te pohranjuje te informacije unutar zaglavlja okvira. Ovo se događa iz razloga kada se podaci prime na drugom kraju, uređaj zna na koji protokol mrežnog sloja ga treba poslati.

Kontrola pristupa medijima (MAC - Media Access Control): MAC podsloj je odgovoran za kontrolu kako se podaci stavljaju na određene medije ili kako kontroliramo pristup podataka na medij. MAC podsloj može biti zauzet brojnim protokolima[16].

4.1.6. Sloj 1 – fizički sloj

Na ovom sloju se odvija fizički prijenos podataka u obliku bitova. Ovisno o vrsti medija i mrežnim karticama koje se koriste, način slanja podataka će se razlikovati. Važno je da se na oba kraja koristi ista metoda. Ti signali mogu biti u obliku varijacija napona ili svjetlosnih uzoraka koji se prenose. Na ovom sloju ne postoje protokoli u sekundi, ali postoje skupovi standarda i kriterija kojih se moraju pridržavati kablovi i mrežne kartice. Ovi standardi uključuju sljedeće:

- Naponi
- Brzine
- Ožičenje

[16] Balchunas , Aaron. 2012. OSI Reference Model v1.31.

4.2. Referentni model TCP/IP

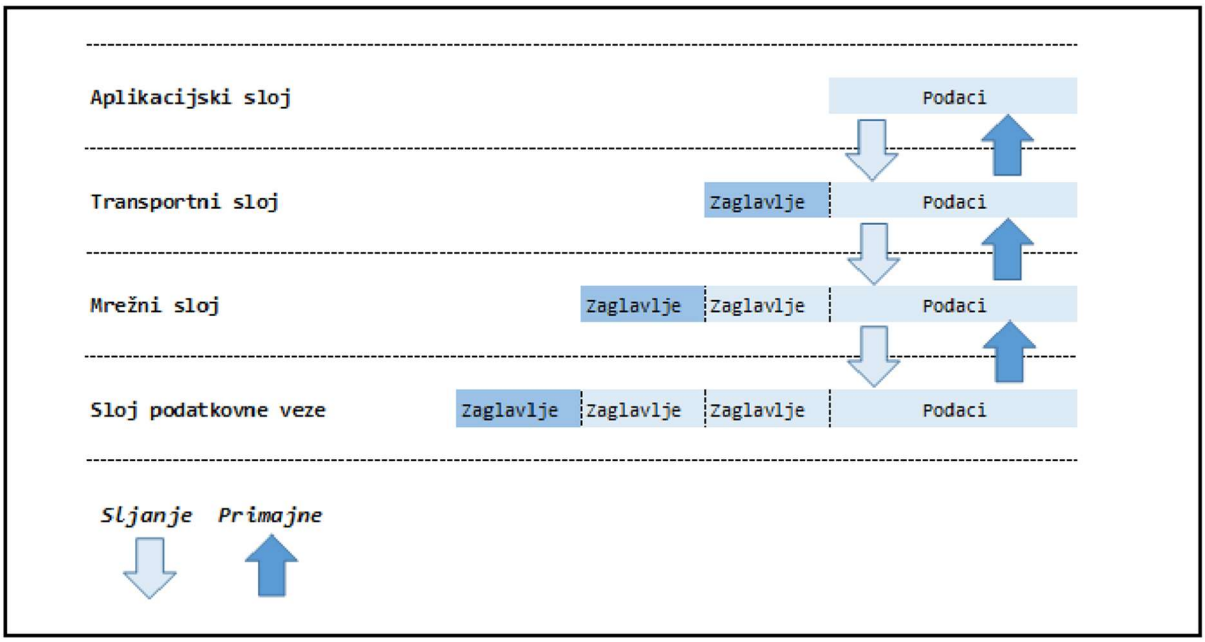
TCP/IP je sastavljen od manjeg broja slojeva u odnosu na OSI model. Većina opisa TCP/IP modela definiraju tri funkcionalne razine u arhitekturi protokola. Kao u OSI modelu, podaci se prosljeđuju niz stog kada se šalju u mrežu, i gore u stog kad se prima s mreže. Četveroslojna struktura TCP/IP-a se vidi u načinu na koji se podaci obrađuju dok prolaze niz stog protokola od sloja aplikacije do temeljne fizičke mreže. Svaki sloj unutra stog dodaje kontrolne informacije kako bi se osigurala ispravna isporuka. Ove kontrolne informacije nazivaju se zaglavljem jer se postavlja ispred podataka koji se prenose. Svaki sloj tretira sve informacije koje prima od sloja iznad kao podatke i postavlja im vlastito zaglavlje ispred te informacije[19].

TCP/IP referentni model	
4	Aplikacijski sloj
3	Transportni sloj
2	Mrežni sloj
1	Sloj podatkovne veze

Slika 2. Slojevi TCP/IP Modela [Izvor: Obrada autora]

Kod slanja dodatak podataka o dostavi na svaki sloj naziva se enkapsulacija. Kod primanja podataka, događa se suprotno. Svaki sloj skida zaglavlje prije prolaska podatke na gornji sloj. Svaki sloj ima svoje nezavisne strukture podataka. Konceptualno, sloj nije svjestan strukture podataka koje koriste slojevi iznad i ispod njega. U stvarnosti, strukture podataka sloja dizajnirane su tako da budu kompatibilne sa strukturama koje koristi okruženje slojeva radi učinkovitijeg prijenosa podataka. Ipak, svaki sloj ima vlastitu strukturu podataka i vlastitu terminologiju koja opisuje tu strukturu. Aplikacije koje koriste TCP odnose se na podatke kao na tok, dok aplikacije koje koriste UDP odnose se na podatke kao na poruku. TCP naziva svoje podatke segmentom, a UDP naziva svoje podatke paket. Internetski sloj sve podatke promatra kao blokove koji se nazivaju datagrami. TCP/IP koristi mnogo različitih tipova temeljnih mreža, od kojih svaka može imati različite terminologije za podatke koje prenosi. Većina mreža prenosi podatke kao paketi ili okviri[17].

[17] Hunt, Craig, 2002. TCP/IP Network Administration. Gravenstein Highway North, Sebastopol: O'Reilly Media, Inc.



Slika 3. Protokol TCP/IP Prijenosa podataka [Izvor: https://litux.nl/Books/Books/www.leothreads.com/e-book/oreillybookself/tcpip/tcpip/ch01_03.html]

4.2.1. Sloj podatkovne veze

Sloj mrežnog pristupa najniži je sloj hijerarhije TCP/IP protokola. Protokoli u ovom sloju osiguravaju sredstva sustavu za isporuku podataka drugom uređaja na izravno spojenoj mreži. Ovaj sloj definira kako koristiti mrežu za prenijeti IP datagram. Za razliku od protokola više razine, protokoli sloja podatkovne veze moraju poznavati detalje osnovne mreže (njezinu strukturu paketa, adresiranje, itd.) za ispravno formatiranje podataka koji se prenose u skladu s mrežnim ograničenjima. TCP/IP sloj podatkovne veze može obuhvatiti funkcije sva tri donja sloja OSI referentnog modela (mrežni sloj, sloj veze i fizički sloj). Sloj podatkovne veze korisnici često zanemaruju. Dizajn TCP/IP-a skriva funkcije nižih slojeva, a poznatiji protokoli (IP, TCP, UDP itd.) su svi protokoli viših slojeva. Pristupni protokoli moraju biti razvijeni tako da TCP/IP mreže mogu koristiti novi hardver. Funkcije koje se izvode na ovoj razini uključuju enkapsulaciju IP datagrama u okvire koji se prenose mrežom i preslikavanje IP adresa u fizičku adresu koje koristi mreža. Jedna od prednosti TCP/IP-a je njegova univerzalna shema adresiranja. IP adresa se mora pretvoriti u adresu koja je prikladna za fizičku mrežu preko kojom se datagram prenosi.

Dva RFC-a standarda koja definiraju protokole sloja podatkovne veze su:

- RFC 826, Protokol za rješavanje adresa (ARP - Address Resolution Protocol), koji preslikava IP adrese na Ethernet adrese.
- RFC 894, Standard za prijenos IP datagrama preko Ethernet mreža, koji specificira kako se IP datagrami enkapsuliraju za prijenos preko Ethernet mreže[18].

4.2.2. Mrežni sloj

Sloj iznad sloja podatkovne veze u hijerarhiji protokola je mrežni sloj. Internetski protokol (IP) najvažniji je protokol u ovom sloju[18].

Protokoli:

- IP
- Internetski protokol kontrolnih poruka (ICMP - Internet Control Message Protocol)

4.2.3. Transportni sloj

Protokolski sloj neposredno iznad mrežnog sloja je transportni sloj. Dva najvažnija protokola u transportnom sloju su protokol upravljanja prijenosom (TCP) i protokol korisničkih datagrama (UDP). Oba protokola dostavljaju podatke između aplikacijskog sloja i mrežnog sloja. Programeri aplikacija mogu odabrati onu uslugu koja je prikladnija za njihove specifične potrebe[18].

Logički portovi

Svrha logičkog priključka je omogućiti prijemnom uređaju da identificira za koju aplikaciju ili usluga su podaci namijenjeni. Dostupno je 65.536 logičkih brojeva portova (s brojevima od 0 do 65 535). Ovi brojevi su dodijeljene od strane Autoriteta za dodijeljene brojeve na internetu (IANA - Internet Assigned Numbers Authority) i raščlanjeni su u rasponima:

Dobro poznati portovi (0-1.023): To su portovi koji se uobičajeno dodjeljuju korištene mrežne usluge.

[18] Hunt, Craig, 2002. TCP/IP Network Administration. Gravenstein Highway North, Sebastopol: O'Reilly Media, Inc.

Registrirani portovi (1.024-49.151): Ovi brojevi portova dodijeljeni su aplikacijama ili uslugama od strane IANA-e na zahtjev programera.

Dinamički portovi (49.152-65.535): ove portove ne dodjeljuje IANA i obično ih koriste klijentski strojevi kao izvorne portove[19].

TCP

TCP se naziva protokolom orijentiranim na vezu. To znači da, prije slanja podataka potrebno je uspostaviti vezu između uređaja. Na taj način uređaj za slanje je siguran da je primatelj spreman za primanje podataka. Za ostvarivanje veze, TCP provodi proces poznat kao trosmjerno rukovanje, što je prikazano na sljedećem dijagramu. Proces je sljedeći:

1. SYN: Uređaj za slanje šalje zahtjev za sinkronizaciju odredišnom računalu. Ova sinkronizacija uključuje redni broj. Za primjer recimo da je redni broj 101.

2. SYN/ACK: Prijemni uređaj odgovara potvrdom SYN zahtjeva. Ovo potvrda je u osnovi potvrda slijeda sljedećeg broj koji primatelj očekuje. U ovom slučaju, to je 102. Također šalje svoj zahtjev za sinkronizaciju prema izvornom uređaju. Za primjer ćemo koristit 201. U ovoj fazi, uređaji pristaju na parametre koje će koristiti za komunikaciju.

3. ACK: Izvorni uređaj potvrđuje zahtjev za sinkronizaciju od uređaj primatelja. Šalje sljedeći redni broj koji uređaj očekujući primiti. U ovom primjeru to je broj 202.

Nakon što je rukovanje završeno, podaci se mogu razmjenjivati između dva uređaja. TCP jamči dostavu podataka kroz proces korištenja rednih brojeva i priznanja. Podaci koji se prenose dijele se na segmente, a svaki od njih posjeduje redni broj. To primatelju omogućuje ponovnu izgradnju podataka po primitku. Osim toga, omogućuje primatelju da identificira je li primio sve podatke. Kada primi podatke, uređaj šalje potvrdu o primitku. Kao dio procesa sinkronizacije, oba uređaja će se dogovoriti o tome koliko segmenta će biti poslano prije nego što se potvrda o primitku šalje natrag. To pomaže u smanjenju mrežnog prometa smanjenjem broja potvrda koje se šalju. Ovo je proces poznat kao klizni prozor i fleksibilan je. Za primjer uređaji se dogovore da se tri segmenta mogu poslati prije nego što se kao odgovor šalje potvrda. Ako uređaj primatelja ne primi sva tri segmenta i stoga ne šalje potvrde, uređaj koji šalje, nakon

[19] Contributors, Wikipedia. 2022. List of TCP and UDP port numbers. Pristupljeno: 20. ožujak 2022. https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

određenog vremenskog razdoblja, shvatit će da nije primio potvrdu i ponovno će poslati podatke. Ako se to dogodi nekoliko puta, dva uređaja će pristati na manji prozor kako bi pokušali smanjiti gubitak podataka i zahtjev za ponovno slanje. TCP također uključuje značajku koja se zove kontrola protoka. Ovo je proces koji je osmišljen za smanjenje zagušenja. Ako se uređaj primatelja trudi držati korak s količinom primljenih podataka, može poslati poruku "nije spreman" pošiljatelju. Nakon što je izbrisao međuspremnik na mrežnoj kartici, uređaj će poslati poruku "spreman" i komunikacija će se nastaviti. Kada uređaji žele prestati komunicirati, slijedi proces četverosmjerno rukovanje.

1. Računalo A više ne treba slati nikakve podatke računalu B, pa šalje FIN paket.
2. Računalo B prima FIN zahtjev i kao odgovor šalje natrag ACK.
3. Nakon što računalo B nema više podataka za slanje šalje FIN paketa na računalo A.
4. Računalo A prima FIN zahtjev i šalje natrag ACK kao odgovor:
5. Nakon što je četverosmjerno rukovanje završeno, uređaji zatvaraju sučelja.

Korištenjem rednih brojeva, kontrole toka i potvrda, korištenje TCP-a osigurava zajamčenu dostavu do odredišta (sve dok spojna infrastruktura radi). Ovo jamstvo, međutim, ima svoju cijenu. TCP zaglavlje dodaje na dodatnih 20-60 bajtova podataka po poslanom segmentu, a potvrde dodaju dodatnu potrošnju propusnog opsega što osim čekanja na potvrde dovodi do sporijeg prijenosa podataka. Stoga se TCP koristi kada je imperativ da podaci budu u potpunosti preneseni, kao što je dijeljenje datoteka ili transakcije baze podataka[20].

UDP

Dok je TCP bio protokol orijentiran na vezu, UDP je protokol bez povezivanja. To znači da nema trosmjernog rukovanja prije prijenosa podataka. Uređaj za slanje doslovno šalje podatke na žicu i nada se da će ih primiti odredišni uređaj. Često se naziva protokolom najboljeg truda, nije važno jesu li podaci stigli ili ne. To je brži protokol jer ima manje zaglavlje (samo osam bajtova) i nema potrebe dodavati potvrde na propusnost. UDP se također koristi za multicast i odašiljanje prijenosa. Bilo bi nemoguće provesti trosmjerno rukovanje s toliko uređaja prije slanja podataka. Bit će slučajeva u kojima će protokol koristiti i TCP i UDP, ovisno o tome koju funkciju obavlja u tom trenutku.

[20] Hunt, Craig, 2002. TCP/IP Network Administration. Gravenstein Highway North, Sebastopol: O'Reilly Media, Inc.

Ukratko, kada je isporuka podataka kritična i vrijeme nije ograničenje, onda bi se trebao koristiti TCP protokol, kada isporuka podataka nije važna a vrijeme je bitno, trebao bi se koristiti UDP[21].

4.2.4. Aplikacijski sloj

Na vrhu arhitekture TCP/IP protokola je aplikacijski sloj. Ovaj sloj uključuje sve procese koji koriste protokole transportnog sloja za isporuku podataka. Aplikacijski sloj TCP/IP modela djeluje kao sučelje između samih aplikacija i mrežnog stoga[21].

5. Protokoli i servisi

U nastavku će biti opisan rad protokola i servisa od kojih će na nekima biti objašnjeni napadi pomoću radnog okvira Yersinia.

5.1. IP

Internet protokol (*eng. IP - Internet Protocol*) je dio 3 sloja OSI i TCP/IP referentnih modela. Postoje tri verzije IPv4, IPv5 i IPv6. Internetski protokol (IP) najvažniji je protokol u ovom sloju. Verzija IP-a koja se trenutno koristi na Internetu je IP verzija 4 (IPv4), koja je definirana u RFC 791 standardu. Postoje novije verzije IP-a, IP verzija 5 je eksperimentalna Stream Transport (ST) protokol koji se koristi za dostavu podataka u stvarnom vremenu. IPv5 nikad nije ušao u operativna upotrebu. IPv6 je IP standard koji pruža znatno proširen kapacitet adresiranja. Budući da IPv6 koristi potpuno drugačiju adresnu strukturu, nije kompatibilan s IPv4. Iako je IPv6 standardna verzija IP-a, još se ne koristi široko operativno i u komercijalnim mrežama. IPv4 je protokol koji ćete konfigurirati na svom sustavu kada želite razmjenjivati podatke s udaljenim sustavima. Internetski protokol je srce TCP/IP-a. IP pruža osnovnu uslugu dostave paketa na kojima su izgrađene TCP/IP mreže. Svi protokoli, u slojevima iznad i ispod IP-a koristite internetski protokol za isporuku podataka. Svi dolazni i odlazni TCP/IP podaci teku kroz IP, bez obzira na svoje konačno odredište. Internetski protokol je građevni blok interneta. Njegove funkcije uključuju:

[21] Hunt, Craig, 2002. TCP/IP Network Administration. Gravenstein Highway North, Sebastopol: O'Reilly Media, Inc.

- Definiranje datagrama, koji je osnovna jedinica prijenosa na Internetu
- Definiranje sheme internetskog adresiranja
- Premještanje podataka između pristupnog sloja i transportnog sloja
- Usmjeravanje datagrama na udaljene hostove
- Izvođenje fragmentacije i ponovnog sastavljanja datagrama

IP je protokol je protokol za veze bez spajanja. To znači da ne razmjenjuje kontrolu informacije nazvanu "rukovanje"(handshake) za uspostavljanje veze između dvije točke prije prijenos podataka. Nasuprot tome, protokol orijentiran na povezivanju razmjenjuje kontrolne informacije s udaljenim sustavom kako bi provjerio je li spreman za primanje podataka prije slanja podataka. Kada je rukovanje uspješno, kaže se da su sustavi uspostavili vezu. Internetski protokol se za uspostavljanje oslanja na protokole u višim slojevima ako zahtijevaju uslugu orijentiranu na povezivanje[22].

5.1.1. Subnet

Struktura IP adrese može se lokalno modificirati korištenjem bitova mrežne adrese. To je "linija podjele" između mreža, bitovi adrese i bitovi adrese hosta se pomiču, stvarajući dodatne mreže, ali smanjujući maksimalan broj hostova koji mogu pripadati svakoj mreži. Ovi novi određeni mrežni bitovi definiraju adresni blok unutar većeg adresnog bloka, koja se naziva Pod mrežom (Subnet). Organizacije se obično odlučuju na pod mrežu kako bi prevladale topološke ili organizacijske probleme. Pod mreža omogućuje decentralizirano upravljanje adresiranjem hostova. Uz standardnu shemu adresiranja, središnji administrator je odgovoran za upravljanje adresama hostova za cijelu mrežu. Subnetiranjem administrator može delegirati adresiranje zadataka manjim organizacijama unutar cjelokupne organizacije. IP usmjerivači mogu međusobno povezati različite fizičke mreže, ali samo ako svaka fizička mreža ima svoju jedinstvenu mrežnu adresu. Maska podmreže koristi se samo lokalno. Izvana se adresa još uvijek tumači pomoću maske adresa poznatih vanjskom svijetu[22].

[22] Hunt, Craig, 2002. TCP/IP Network Administration. Gravenstein Highway North, Sebastopol: O'Reilly Media, Inc.

5.1.2. Gateway

Pristupnik (eng. Gateway) je mrežna adresa koja je dodijeljena usmjerivaču da usmjerava podatke između mreža, svi mrežni uređaji moraju donositi odluke o usmjeravanju. Za većinu hostova odluke o usmjeravanju su jednostavne:

- Ako je odredišni host na lokalnoj mreži, podaci se isporučuju na odredišni host.
- Ako je odredišni host na udaljenoj mreži, podaci se prosljeđuju lokalnom gatewayu

Odluke o IP usmjeravanju su jednostavno traženje u tablici usmjeravanja. Paketi se usmjeravaju prema svojim odredištima prema uputama tablice usmjeravanja (koja se naziva i tablica prosljeđivanja). Tablica usmjeravanja preslikava odredišta na usmjerivač i mrežno sučelje koje IP mora koristiti za doći do tog odredišta[23].

5.2. DHCP

Protokol dinamičke konfiguracije glavnog računala (DHCP - Dynamic Host Configuration Protocol) protokol pruža sve informacije koje se obično koriste za konfiguriranje TCP/IP-a, od IP adresa klijenta do IP adresa servera za ispis koje bi klijent trebao koristiti. DHCP radi preko UDP portova 67 i 68. Ispravno konfiguriran, DHCP poslužitelj može podržati sve mrežne klijente. DHCP poslužitelj pruža kompletan skup TCP/IP konfiguracijskih parametara. Mrežni administrator može upravljati cijelom konfiguracijom za korisnike. DHCP poslužitelj može dati stalne adrese ručno, trajne adrese automatski, a privremene adrese dinamički. Mrežni administrator može prilagoditi dodjelu adresa prema potrebama mreže i klijentskom sustavu[24].

5.3. DNS

Sustav naziva domene (DNS - Domain Name System)je servis 5 sloja TCP/IP referentnog modela. Ova aplikacija preslikava IP adrese na imena dodijeljen mrežnim uređajima. DNS

[23] Kizza, Migga, Joseph. 2005. Computer Network Security. University of Tennessee-Chattanooga Chattanooga,: Springer.

[24] Hunt, Craig, 2002. TCP/IP Network Administration. Gravenstein Highway North, Sebastopol: O'Reilly Media, Inc.

trenutno pruža informacije o približno 100.000.000 domaćina. DNS jamči da će novi podaci o hostu biti proslijeđeni ostatku mreže koliko je potrebno.

Informacije se automatski distribuiraju i to samo onima koji su zainteresirani. Ako DNS poslužitelj primi zahtjev za informacijama o hostu za koje nema informacija, prosljeđuje zahtjev autoritativnom poslužitelju. Autoritativni poslužitelj je svaki poslužitelj odgovoran za održavanje točnih informacija o domeni koja se ispituje. Kada autoritativni poslužitelj odgovori,lokalni poslužitelj sprema odgovor za buduću upotrebu. Sljedeći put lokalni poslužitelj zaprimi zahtjev za tim informacijama, on sam odgovara na zahtjev. Usluzi DNS name dodjeljuje se port 53 i naziva se domena[25].

5.4. VLAN

Iako su nam preklopnici omogućili da naše mreže učinimo učinkovitijima kroz segmentaciju, korištenjem VLAN-ova može nam omogućiti da još više segmentiramo mrežu. Kada uređaj šalje emitirani prijenos, on se šalje svakom uređaju na lokalnoj mreži. Svi uređaji koji primaju taj prijenos emitiranja su na istoj domeni emitiranja. Usmjerivači nisu dizajnirani za prosljeđivanje emitiranih prijenosa zbog čeg su ograničeni na lokalnu mrežu.

Kada implementiramo VLAN-ove, kaže se da je svaki VLAN za sebe domena emitiranja. VLAN-ovi nam omogućuju daljnje razbijanje mreže. Umjesto da ovo radim fizički, ovo se obavlja virtualno konfiguriranjem preklopnika. Rastavljanje mreže na VLAN-ove će se razlikovati od organizacije do organizacije. Neki primjeri kako se može rastavljati LAN-a na VLAN-ove su sljedeći:

- Po jedan za svaki kat zgrade
- Po jedan za svaki odjel
- Po jedan za svaku učionicu u školi
- Jedan za različite razine sigurnosti
- Jedan za podatkovnu i jedan za govornu komunikaciju

VLAN-ovi se obično identificiraju brojem. Implementacija VLAN-ova pruža izvrsne rezultate u smislu sigurnosti i performansi. Možemo segmentirati mrežu na različita područja

[25] Hunt, Craig, 2002. TCP/IP Network Administration. Gravenstein Highway North, Sebastopol: O'Reilly Media, Inc.

osjetljivosti podataka. Budući da je svaki VLAN u vlastitoj domeni emitiranja, mreža postaje učinkovitija[26].

5.5. STP

Protokol razapinjućeg stabla (STP - Spanning Tree Protocol) ima ulogu spriječiti petlje između preklopnika kada postoje implementirane redundantne veze. Petlje (eng. Broadcast storm) treba spriječiti jer zbog njih dolazi do efekta lavinskog multipliciranja informacija između mrežnih elemenata što je posljedica „zauzetog kanala“. Informacije koje je potrebno poslati ne mogu biti poslane radi zagušenosti kanala. Između preklopnika se održavaju izbori kako bi se odlučilo koji prekidač će se klasificirati kao korijenski most (eng. Root Bridge). Jednom identificirani, preklopnici identificiraju koji od njihovih sučelja je najbliži korijenskom mostu i nazivaju ga korijenskim sučeljem (eng. Root Port). Ova sučelja će uvijek biti na raspolaganju. Ostala sučelja se nazivaju određenim sučeljima (eng. Designated Ports) i neodređena sučelja (eng. Non Designated Ports). Neodređenim sučeljima je onemogućeno slanje podataka osim ako nešto na mreži ne funkcionira što od njih zahtijeva da preuzmu ulogu slanja podataka[27].

5.6. ARP tablica

Protokol rješavanja adresa (ARP - Address Resolution Protocol) je dio drugog sloja TCP/IP i OSI referentnih modela , njegova uloga je mapiranje IP adresa sa fizičkim MAC adresama u mreži[28].

5.7. HSRP

Visoko stanje pripravnosti (HSRP - Hot Standby Router Protocol) je vlasnički Ciscov protokol redundancije za uspostavljanje zadanog mrežnog prolaza tolerantnog na kvarove. Jedan od načina za postizanje gotovo 100-postotne dostupnosti mreže je korištenje HSRP-a, koji osigurava redundantnost mreže za IP mreže, osiguravajući da se korisnički promet odmah

[26] CERT, CARNet. i LS&S. Sigurnosni model mreže računala. CCERT-PUBDOC-2009-01-253 Revizija 1.02.

[27] Nikola, Jelečki. Turkalj, Vedran. 2019. Spanning-tree-protokol. POLYTECHNIC & DESIGN Vol. 7, No. 1, 2019.

[28] Hunt, Craig, 2002. TCP/IP Network Administration. Gravenstein Highway North, Sebastopol: O’Reilly Media, Inc.

i transparentno oporavlja od kvarova prvog skoka u mrežnim rubnim uređajima ili pristupnim krugovima. Dijeleći IP adresu i MAC (Layer 2) adresu, dva ili više usmjerivača mogu djelovati kao jedan "virtualni" usmjerivač. Članovi grupe virtualnih usmjerivača neprestano razmjenjuju statusne poruke. Na ovaj način jedan usmjerivač može preuzeti odgovornost za usmjeravanje drugog ako prestane raditi iz planiranih ili neplaniranih razloga. Domaćini nastavljaju prosljeđivati IP pakete na dosljednu IP i MAC adresu, a promjena uređaja koji usmjeravaju je transparentna. Koristeći HSRP, skup usmjerivača radi zajedno kako bi domaćinima na LAN-u prikazao iluziju jednog virtualnog usmjerivača. Ovaj skup je poznat kao HSRP grupa ili pripravna grupa. Jedan usmjerivač izabran iz grupe odgovoran je za prosljeđivanje paketa koje domaćini šalju virtualnom usmjerivaču. Ovaj usmjerivač je poznat kao aktivni usmjerivač. Drugi usmjerivač je izabran kao Standby usmjerivač. U slučaju da aktivni usmjerivač pokvari, Standby preuzima dužnost prosljeđivanja paketa aktivnog usmjerivača. Iako proizvoljan broj usmjerivača može pokretati HSRP, samo aktivni usmjerivač prosljeđuje pakete poslane virtualnom usmjerivaču. Kako bi se smanjio mrežni promet, samo aktivni i standby usmjerivači šalju periodične HSRP poruke nakon što protokol završi izborni proces. Ako aktivni usmjerivač ne uspije, usmjerivač u stanju pripravnosti preuzima funkciju aktivnog usmjerivača. Ako usmjerivač u stanju pripravnosti pokvari ili postane aktivni usmjerivač, tada se drugi usmjerivač bira kao usmjerivač u stanju pripravnosti. Na određenom LAN-u može koegzistirati i preklapati se više grupa u stanju pripravnosti. Svaka skupina u stanju pripravnosti emulira jedan virtualni usmjerivač. Pojedinačni usmjerivači mogu sudjelovati u više grupa. U tom slučaju, usmjerivač održava zasebno stanje i mjerače vremena za svaku grupu. Svaka skupina u stanju pripravnosti ima jednu, dobro poznatu MAC adresu, kao i IP adresu. Značajka HSRP omogućuje usmjerivaču s najvišim prioritetom da odmah postane aktivni usmjerivač. Kada usmjerivač višeg prioriteta preduhitri usmjerivač nižeg prioriteta, on šalje poruku o prekidu. Kada aktivni usmjerivač nižeg prioriteta primi poruku o prekidu ili pozdravnu poruku od aktivnog usmjerivača višeg prioriteta, prelazi u stanje govora i šalje poruku o ostavci[29].

[29] Contributors, Wikipedia. 2021. Hot Standby Router Protocol. Pristupljeno: 20. ožujak 2022. https://en.wikipedia.org/wiki/Hot_Standby_Router_Protocol

5.8. CDP

Ciskov protokol identifikacije (eng. *CDP - Cisco Discovery Protocol*) je protokol sloja 2, neovisan o medijima i mreži, koji mrežne aplikacije koriste za učenje o obližnjim, izravno povezanim uređajima. Svaki uređaj konfiguriran za Ciskov protokol identifikacije oglašava barem jednu adresu na koju uređaj može primati poruke i šalje povremene oglase (poruke) na dobro poznatu multicast adresu 01:00:0C:CC:CC:CC. Uređaji se međusobno otkrivaju slušajući na toj adresi. Oni također slušaju poruke kako bi saznali kada su sučelja na drugim uređajima uključena ili isključena. Oglasi sadrže informacije o vremenu trajanja, koje označavaju duljinu vremena u kojem bi uređaj za primanje trebao zadržati informacije Ciskov protokol identifikacije prije nego što ih odbaci. Oglasi podržani i konfigurirani u softveru Cisco šalju se prema zadanim postavkama svakih 60 sekundi na sučelja koja podržavaju zaglavlja SNAP (eng. *Subnetwork Access Protocol*). Cisco uređaji nikada ne prosljeđuju Ciskov protokol identifikacijske pakete. Cisco uređaji koji podržavaju Ciskov protokol identifikacije pohranjuju primljene informacije u tablicu. Informacije u ovoj tablici osvježavaju se svaki put kada se primi oglas, a informacije o uređaju se odbacuju nakon što se propuste tri oglasa s tog uređaja[30].

5.9. DTP

Dinamički kanalni protokol (*eng. DTP - Dynamic Trunking Protocol*) je kanalni protokol koji je razvijen i vlasništvo tvrtke Cisco i koji se koristi za automatsko pregovaranje o kanalima između Ciscovih preklopnika. Pregovorima o kanalu upravlja DTP samo ako su portovi međusobno izravno povezani. Ethernet kanal sučelja podržavaju različite načine kanala. Ta se sučelja mogu konfigurirati kao trunk ili ne-trunk, ili za pokretanje pregovaračkog trunkinga na susjedno sučelje ili čeka da primi poruku pregovaranja o trunkovima od drugog izravno povezanog sučelja. Većina današnjih Cisco preklopnika koristi IEEE 802.1Q kao svoj izbor tipa trunkinga zbog manjeg opterećenja u usporedbi s ISL (Inter Switch Link)[31].

[30] Admin, Cisco. 2020. Cisco Discovery Protocol. Pristupljeno: 20. ožujak 2022.
https://learningnetwork.cisco.com/s/article/cisco-discovery-protocol-cdp-x

[31] Contributors, Wikipedia. 2022. Dynamic Trunking Protocol Wikipedia. Pristupljeno: 20. ožujak 2022.
https://en.wikipedia.org/wiki/Dynamic_Trunking_Protocol

6. Mrežna sigurnost

Danas, zbog široke u upotrebe interneta od strane ljudi jedan od najvažnijih aspekata mreža je njena sigurnost. Mrežna sigurnost u današnjem svijetu igra vrlo važnu ulogu, na tu temu se vode mnoga istraživanja kako bi se pružila bolja sigurnost postojećim mrežama. Mrežna sigurnost i vatrozid dvije su riječi koje su usko povezane jedna s drugom, činjenica da vatrozid pruža sigurnost za učinkovito umrežavanje u organizaciji. Potreba za vatrozidom nije velika ako se mreža temelji samo na intranetu, u usporedbi s scenarijem u kojem se svi korisnici povezuju s internetom koji djeluje kao medij odakle promet (podaci) putuju izvana prema unutra i obrnuto. U tom slučaju vatrozid je prva linija obrane. U ovom odjeljku opisujemo neke od klasičnih napada koji su iskoristili tipične ranjivosti računalne mreže i rješenja koja se koriste za borbu ili smanjenje mogućnosti nekih od ovih napada.

6.1. Vrste mrežnih napada

6.1.1. Prijetnje u tranzitu

Kartica mrežnog sučelja (NIC) svakog hosta u mreži jedinstveno je identificirana s hardverskom adresa. NIC će biti programiran da pokupi samo pakete adresirane na:

- adresa koja odgovara hostu
- adresa višestrukog prijenosa koja odgovara multicast grupi u kojoj je domaćin član
- adresu emitiranja

Sposoban uljez može reprogramirati NIC s hardverskom adresom drugog hosta i prihvatiti pakete adresirane za taj host. Kako ne bi bio uhvaćen, uljez može vratiti kopiju paketa u mrežu.

Prisluškivanje (eng. Wiretapping) je proces izdvajanja informacija dok teku kroz žicu. Proces prisluškivanje se razlikuje ovisno o korištenom komunikacijskom mediju. U kablovima se može obaviti prisluškivanje korištenjem njuškala (eng. Sniffer) paketa ili putem induktivnosti. Njuškalo paketa je računalni softver ili hardver koji može presresti promet koji prolazi kroz kabel lokalne mreže (LAN)[32], može se koristiti u korisne i zlonamjerne svrhe:

- Za analizu mrežnih problema i praćenje korištenja mreže
- Za filtriranje sumnjivog sadržaja iz mrežnog prometa

[32] Meghanathan, Natarajan. A Tutorial on Network Security Attacks and Controls. Jackson: Jackson State University.

- Za proučavanje strukture paketa, zaglavlja različitih protokola koji se koriste preko mreže
- Za otkrivanje pokušaja upada u mrežu
- Za prikupljanje informacija za provođenje upada u mrežu.

Kako obična žica emitira zračenje tijekom prolaska električnih signala kroz nju, uljez može dodirnuti žicu i pročitati izračene signale kroz induktivitet bez fizičkog kontakta s kabelom. Uljez koji presreće signale na širokopojasnom kabelu mora odvojiti ciljani signal od svih multipleksiranih signala. Bežični signali se emitiraju kroz otvoreni prostor i osjetljiviji su na prisluškivanje. Put mikrovalnih signala mora biti prilično širok kako bi se osiguralo da će antena prijemnika biti pogođen odaslanim signalom. Ali, što je širi put signala, to je lakše uljezu ometati liniju vidljivosti prijenosa između pošiljatelja i primatelja te također pokupiti cijeli prijenos s antene koja se nalazi blizu prijemnika. Otisak stopala (eng. Footprint) je definiran kao uzorak proizveden na površini zemlje od satelitskog odašiljača. A širi otisak je potreban kako bi se povećala pokrivenost jer se signali mogu pokupiti u velikoj regiji. S druge strane, manji otisak je poželjan kako bi se smanjio rizik od presretanja. Kut disperzije je parametar koji se može kontrolirati za podešavanje širenja otiska.

Optičko vlakno, napravljeno od tankih staklenih niti, može prenositi svjetlosne impulse na velike udaljenosti, a da nije pod utjecajem električnih smetnji. Optička vlakna su sigurnija od bilo kojeg drugog prijenosnog medija zbog sljedeća dva razloga:

- Optička vlakna su fino podešena kako bi se postigao ukupan unutarnji odraz. Cjelokupna mreža treba biti ponovno podešena kako bi se omogućilo prisluškivanje i presretanje

- Optička vlakna nose svjetlosnu energiju, a ne električne signale. Dakle, prisluškivanje temeljeno na induktivnosti nije moguće.

6.1.2. Otmica TCP sesije

Otmica TCP sesije odnosi se na čin preuzimanja već uspostavljene TCP sesije i ubacivanje paketa u tok koje primatelj obrađuje kao da paketi dolaze iz autentičnog vlasnika sesije. TCP sesija je identificirana četverostruko:

- IP adresa klijenta
- Broj porta klijenta
- IP adresa poslužitelja
- Broj porta poslužitelja

Svaki paket koji dođe do bilo kojeg stroja s gore navedenim identifikatorima se smatra dijelom postojeće sesije. Ako napadači mogu lažirati ove stavke, mogu slati TCP pakete klijentu ili poslužitelju i ti se paketi obrađuju kao da dolaze s drugog stroja te sesije. Da bi uspješno oteo postojeću TCP sesiju, napadač mora prvo desinkronizirati sesiju i zatim unijeti predviđene naredbe. Za desinkronizaciju postojeće TCP sesije između klijenta i poslužitelja, napadač mora prvo predvidjeti redni broj koji će klijent koristiti (ili poslužitelj) i upotrijebite taj redni broj prije nego što klijent (ili poslužitelj) dobije priliku za korištenje istog. Ako napadač ima pristup mreži, njuškalo paketa može se koristiti za pregled paketa koji pripadaju TCP sesiji i može se točno predvidjeti očekivani redni broj iz razmijenjenih ACK paketa.

Ako napadač ne može pronaći TCP sesiju između klijenta i poslužitelja mora pogoditi očekivani redni broj. Kada napadač uspješno otme TCP sesiju i ubacuje vlastite lažirane pakete podataka (kao da paketi podataka dolaze iz izvornog klijenta), poslužitelj će potvrditi primitak paketa podataka izvornog klijenta tako što će mu poslati ACK paket. Kako će ovaj ACK paket najvjerojatnije nositi redni broj koji se od njega ne očekuje, izvorni klijent pokušat će se ponovno sinkronizirati s poslužiteljem tako što će mu poslati ACK paket s rednim brojem koji se očekuje. Ovaj ACK paket zauzvrat će sadržavati redni broj koji poslužitelj ne očekuje i stoga će poslužitelj ponovno poslati svoj zadnji ACK paket. Ovaj ciklus će se nastaviti i brzo slanje ACK paketa naprijed-nazad stvara TCP ACK oluju. Napadač ubacuje sve više i više paketa podataka, veličina ACK oluje se povećava i može brzo doći do smanjenje performansi mreže. Nakon određenog broja neuspješnih pokušaja resinkronizacije, izvorni klijent na kraju se iscrpi i zatvori vezu s poslužiteljem[33].

[33] Meghanathan, Natarajan. A Tutorial on Network Security Attacks and Controls. Jackson: Jackson State University.

6.1.3. Čovjek u sredini

Uz napad Čovjek u sredini (*MITM - Man-In-The-Middle*) napadač može čitati, modificirati i umetati poruke između dvije strane u komunikaciji, a da nijedna strana ne zna da je veza između njih kompromitirana. Za uspješno izvođenje ovog napada potrebno je znati promatrati i presresti poruke između dvije žrtve. Sada opisujemo primjer MITM napada na kriptografiju s javnim ključem. Neka su A i B dvije strane u komunikaciji i neka je M napadač koji želi isporučiti lažnu poruku B. Za početak, B šalje svoj javni ključ A. Ako M može presresti komunikacijski kanal između A i B, tada M dobiva pristup javnom ključu B. Zatim, M šalje A, lažnu poruku koja tvrdi da je došla od B. U ovoj poruci, M šalje svoj javni ključ, ali A misli da je primio javni ključ B. Kada A šalje paket podataka B, on šifrira paket s (onim što A smatra) javni ključ B i ubacuje šifriranu poruku u kanal. M presreće poruku i dešifrira sa svojim privatnim ključem za izdvajanje stvarne poruke koju je A poslala B. M zatim šifrira poruku pomoću javni ključ B. Svrha ovakvog napada je da M modificira poruku prije nego što je ponovno šifrira. M umeće novu šifriranu poruka natrag u kanal kako bi poruka mogla otići do B. B dešifrira poruku koristeći vlastiti privatni ključ i čita poruku pod pretpostavkom da dolazi od A[34].

6.1.4. Smurf napad

Počinitelj može pokrenuti napad Štrumpfa slanjem lažirane Echo-Request poruke na mrežnu IP adresu za emitiranje. Lažna poruka Echo-Request ima IP adresu žrtve kao izvornu IP adresu. Stoga će svaki host koji primi emitiranu poruku Echo-Request poslati Echo-Reply poruku žrtvi. Žrtva će biti preplavljena Echo-Reply porukama. Dakle, Štrumpf napad je vrsta napada uskraćivanja usluge (DoS)[34].

6.1.5. Preusmjeravanje prometa

Kompromitirani usmjerivač može slati poruke o ažuriranju rute svim susjednim usmjerivačima informirajući ih da leži na najkraćem putu do svake mreže na Internetu. Susjedni usmjerivači prosljeđuju sve njihove dolazne pakete podataka na ovaj kompromitirani

[34] Meghanathan, Natarajan. A Tutorial on Network Security Attacks and Controls. Jackson: Jackson State University.

usmjerivač, koji će na kraju biti preplavljen paketima podataka te ih počne ispuštati. Paketi podataka ne stižu do odredišta[35].

6.1.6. Napadi na uslugu naziva domene (DNS)

DNS poslužitelj je stroj koji drži tablicu (nazvanu DNS cache) koja mapira nazive domena sa IP adresama. Poslužitelj postavlja upite drugim DNS poslužiteljima koji su viši u hijerarhiji naziva domene kako bi saznao imena domena za koje nema unos IP adrese u svojoj DNS predmemorije i ažurirao svoju predmemoriju s novim mapiranjem. Trovanje DNS predmemorije je napad u kojem se DNS poslužitelj navodi da vjeruje u autentičnost mapiranja imena domene i IP adresa, dok u stvarnosti nije. Nakon što je DNS cache zatrovan, unos ostaje neko vrijeme u predmemoriji i utječe na klijente koji koriste DNS poslužitelj. Na primjer, napadač može zamijeniti informacije o IP adresi za ciljni poslužitelj datoteka sa IP adresom kompromitiranog poslužitelja datoteka kojim napadač kontrolira. Napadač stvara lažne unose na kompromitiranom poslužitelju s nazivima datoteka koji odgovaraju onima na ciljnom poslužitelju. Ove datoteke mogu sadržavati zlonamjerni sadržaja poput crva ili virusa. Korisnici koji žele preuzeti datoteke s ciljnog poslužitelja datoteka mogu nesvjesno preuzeti datoteka sa zlonamjernim sadržajem s ugroženog poslužitelja datoteka[35].

[35] Meghanathan, Natarajan. A Tutorial on Network Security Attacks and Controls. Jackson: Jackson State University.

6.1.7. Distribuirani napadi uskraćivanja usluge (DDoS)

DDoS napadi uključuju provalu u stotine ili tisuće strojeva diljem Interneta. Napadač instalira zlonamjerni softver na sve te kompromitirane strojeve (zvane zombiji) i kontrolira pokretanje koordiniranog napade na žrtvinu stranicu. DDoS napadi obično imaju za cilj iscrpljivanje propusnosti mreže, nadjačavajući kapacitet obrade usmjerivača i prekidajući mrežnu povezanost žrtve. Napadač koristi bilo koju prikladnu metodu (kao što je iskorištavanje napada preljeva međuspremnika ili prevari žrtvu da otvori i instalira nepoznati kod iz privitka e-pošte) za postavljanje trojanca na ciljnom stroju i transformira ga u zombija tako što ćete instalirati rootkit softver.

Trojanac je računalni program kojem je namjena inficirati računalo i uzrokovati na njemu zlonamjerne aktivnosti. Ovakvi programi koriste se za krađu osobnih podataka, širenje drugih virusa i remećenje performansi računala.

Rootkit pomaže prikriti prisutnost trojanca i sakriti njegove zlonamjerne aktivnosti. Nakon formiranja dovoljnog broj zombija, napadač šalje signal svim zombijima da pokrenu DDoS napad na odabrani stroj. Svaki zombi može pokrenuti istu ili drugu vrstu napada na žrtvu[36].

6.1.8. Syn Flood Attack

Tijekom procesa uspostavljanja TCP veze, poslužitelj održava red čekanja SYN_RECV koji treba zadržati praćenje zahtjeva za povezivanjem za koje je dodijelio resurse i odgovorio sa SYN/ACK porukom, ali odgovarajući ACK od klijenta još nije primljen. Poslužitelj na kraju istekne vrijeme čekanja ACK paketa i uklanja nepotpuni zahtjev za povezivanje iz svog reda čekanja. Napadač može pokrenuti DDOS napad slanjem nekoliko poruka zahtjeva za SYN povezivanje pomoću lažirane nepostojeće IP adrese i nikad ne odgovara ACK porukama. SYN_RECV red čekanja na poslužitelju se popunjava nepotpunim porukama zahtjeva za povezivanje. Iako ovi nepotpuni zahtjevi za povezivanje se odbacuju nakon isteka vremena, ako pravi klijent pokuša uspostaviti TCP vezu s poslužiteljem u međuvremenu, poslužitelj odbacuje SYN zahtjev od tog klijenta[36].

[36] Meghanathan, Natarajan. A Tutorial on Network Security Attacks and Controls. Jackson: Jackson State University.

7. Zaštitne mjere mreža

Postoji nekoliko sigurnosnih kontrola mreže koje su usvojene u modernim računalnim mrežama za borbu protiv prijetnji i sprječavanje ili smanjenje šanse za napad. Neke od ranjivosti mogu se spriječiti pomoću stvaranje pravila za dopuštenu upotrebu mreže.

7.1. Šifriranje veze naspram end-to-end enkripcije

Enkripcija koja se primjenjuje između svakog para domaćina povezanih vezom naziva se enkripcija link-to-link. Šifriranje veze je poželjno kada su svi hostovi u mreži sigurni, ali komunikacijski medij je podijeljen među nekoliko korisnika i nije siguran. Zbog toga imamo Protokol prijenosa hiperteksta (*HTTPS - HyperText Transfer Protocol Secure*) komunikacijski protokol koji se koristi kako bi se uspostavila veza između WWW servera i proslijedile se HTML stranice direktno to klijentskog preglednika. Ovaj protokol omogućava kriptiranu komunikaciju i sigurnu identifikaciju web poslužitelja mreže.

Gotovo sve komponente podatkovnog okvira (osim izvorne i odredišne hardverske adrese u zaglavlju okvira) šifriraju se prije umetanja okvira na fizičku komunikacijsku vezu. Kada okvir stigne do sljedećeg prijamnika (može biti usmjerivač ili krajnji host), okvir se dešifrira na donjem sloju protokola i šalje višim slojevima na dalje obradu i prosljeđivanje. Budući da je enkripcija na donjem sloju protokola, poruka je izložena kao otvoreni tekst na svim slojevima. Dakle, šifriranje veze štiti poruku u tranzita između dva računala. Enkripcija koja se primjenjuje između dva aplikacijska programa koja se izvode na krajnjim hostovima komunikacije je naziva end-to-end enkripcija. Ovdje je samo podatkovni dio paketa šifriran na najvišoj razini (aplikacijskom sloju) i paket se prenosi s podacima u šifriranom obliku kroz Internet. Dakle, end-to-end enkripcija štiti podatke od otkrivanja tijekom prijenosa[37].

[37] Meghanathan, Natarajan. A Tutorial on Network Security Attacks and Controls. Jackson: Jackson State University.

7.2. Virtualne privatne mreže

Postoje dvije vrste IP adresa: javne i privatne. Javna IP adresa je globalno jedinstvena i samo jedan stroj spojen na javni Internet može imati javnu IP adresu. Privatne IP adrese su jedno od rješenja za smanjenje iscrpljenosti IP adresnog prostora. Privatna IP adresa mora biti jedinstvena samo unutar skupa mreža određene organizacije. Domaćini na različitim mjestima organizacije mogu se identificirati s jedinstvenom privatnom IP adresom. Ali isti skup privatnih IP adresa može se koristiti u mrežama različite organizacije. Tehnologija virtualne privatne mreže (VPN) koristi IP-in-IP tuneliranje za šifriranje i enkapsuliranje IP datagram koji ima privatne IP adrese dva krajnja hosta s drugim IP zaglavljem koje ima izvornu i odredišnu IP adresu od javne IP adrese usmjerivača za ova dva privatne mreže[38].

7.3. Secure Shell

SSH - Secure Shell je mrežni protokol koji omogućuje korisniku sigurnu interakciju s udaljenim strojevima uspostavljanjem sigurnog kanala za razmjenu podataka. SSH je zamijenio TELNET i druge nesigurne shell programe koji su se u prošlosti koristili za slanje informacija u otvorenom tekstu, uključujući slanje lozinke na udaljene sustave. SSH šifrira informacije poslane preko ne sigurnog interneta i na taj način pruža povjerljivost i integritet podataka[38].

7.4. Sigurnost transportnog sloja

Sigurnost transportnog sloja (*TLS - Transport Layer Security*) je nasljednik Sloj sigurnih utičnica (*SSL - Secure Sockets Layer*) kriptografskog protokola i osigurava sigurnu komunikaciju datagrama protokola transportnog sloja kao dio end-to-end veze preko mreže. TLS se koristi u raznim aplikacijama poput pregledavanja weba, elektroničke pošte, glasovnog prijenosa preko IP-a, razmjene trenutnih poruka itd[38].

[38] Meghanathan, Natarajan. A Tutorial on Network Security Attacks and Controls. Jackson: Jackson State University.

7.5. IP Sigurnost

IP Paket sigurnosnih protokola (*IPSec - Security Protocol suite*) implementiran je na IP sloju, tako da ne zahtijeva nikakve promjene za postojeće protokole transportnog sloja i aplikacijskog sloja. IPSec je prvenstveno dizajniran za temeljne nedostatke IP sloja kao što su lažiranje IP adrese, prisluškivanje i otmica sesije[39].

7.6. Yersinia

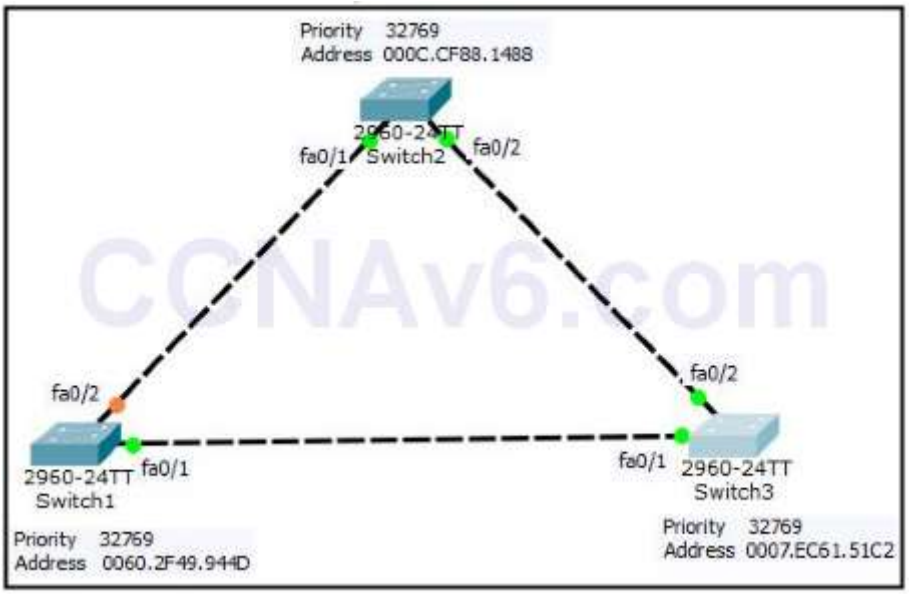
Yersinia je mrežni alat dizajniran da iskorištava neke slabosti u različitim mrežnim protokolima. Okvir (eng. Framework) je napisan u jeziku C a izvodi se na Linux, BSD i Solaris operacijskim sustavima. Višenitni okvir (eng. Framework) podržava kreiranje više korisnika i napada po korisniku. Pretendira da bude osnovan (eng. Framework) za testiranje, analizu mreža i sustava. Sastoji se od raznih napada koji iskorištavaju slabosti različitih protokola 2 sloja. Pomoću ovog (eng. Frameworka) administrator može identificirati ranjivosti u 2 sloju mreže. Tijekom pen testiranja, yersinia se koristi za pokretanje napada na uređaje 2 sloja kao što su preklopnici, STP protokol itd. Neki od implementiranih napada uzrokovat će DoS u mreži, drugi će pomoći u izvođenju bilo kojeg drugog naprednijeg napada, ili oboje. Yersinia će zasigurno pomoći i pentesterima i mrežnim administratorima u njihovim svakodnevnim zadacima[40].

[39] Meghanathan, Natarajan. A Tutorial on Network Security Attacks and Controls. Jackson: Jackson State University.
[40] Tomac. i Slay. 2017. Yersinia Kali. Pristupljeno: 20. ožujak 2022. https://www.kali.org/tools/yersinia

8. Napadi na računalne mreže

8.1. STP i RSTP napad

STP radi prema sljedećem principu. U L2 domeni je odabran korijenski preklopnik naziva korijenski most. Odabir se temelji na prioritetu (zadano 32768). Što je niži prioritet, to bolje. Svi preklopnici imaju zadanu vrijednost, izbor se vrši po prioritetu + MAC linku. Preklopnik s nižom MAC vrijednošću postat će korijenski most, što će utjecati na performanse mreže. Nadalje, svaki ne-korijenski premosni preklopnik odabire jedan port koji vodi do korijenskog mosta, portove koji se koriste za promet i portove koji moraju biti isključeni kako bi se izbjegle preklopne petlje.

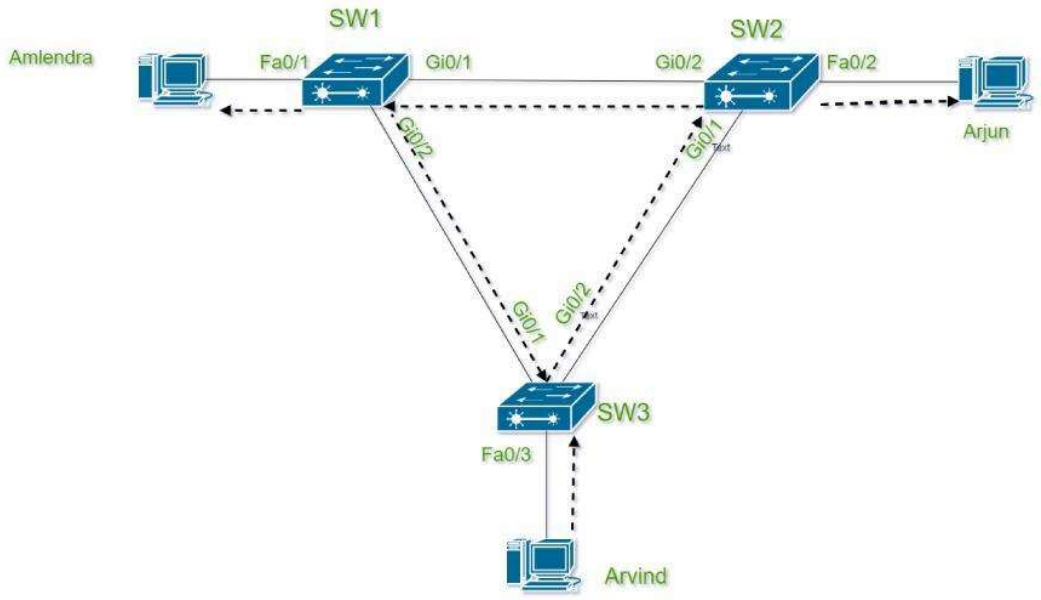


Slika 4. STP Protokol [Izvor: https://itexamanswers.net/lab-124-configuring-spanning-tree-protocol.html]

U STP-u nema sigurnosnih mehanizama tijekom procesa odabira root preklopnika. Također mu nedostaju ugrađeni mehanizmi provjere autentičnosti, lozinke ili provjere izvora. STP vjeruje svima. Kada se na mreži pojavi novi preklopnik čiji je prioritet niži od prioriteta trenutnog korijenskog preklopnika, odabire se novi korijenski uređaj. Manipuliranjem takvim scenarijima možemo promijeniti optimalne prometne putove, pa čak i pokušati ih presresti, spamati mrežu posebnim STP – TCN porukama, koje će obrisati komutacijske tablice svakog preklopnika i uzrokovati gubitke, pogoršanje performansi mreže i druge probleme.

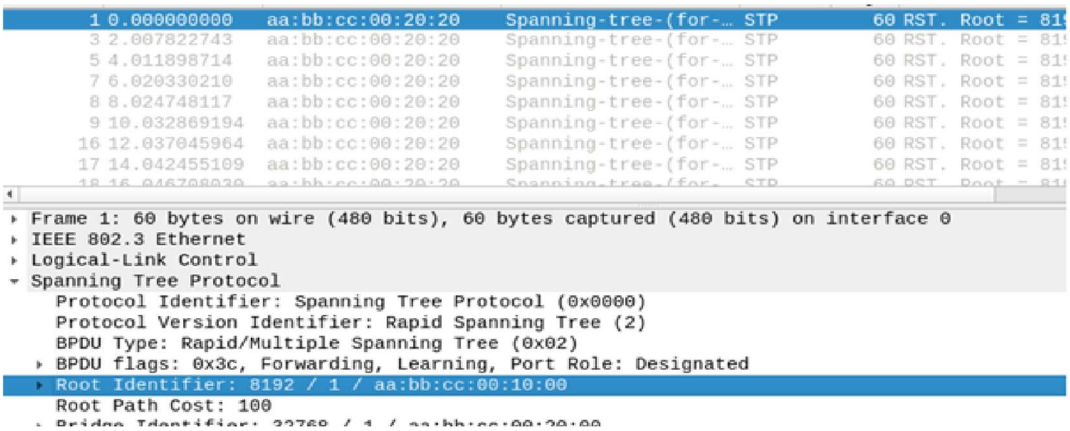
Za korištenje ovog napada dovoljno je povezati Linux računalo i Yersinia okvir (eng. Framework) na mrežu, što će nam omogućiti pokretanje STP-a na našem domaćinu, lažno predstavljajući preklopnik. To će nam omogućiti da manipuliramo našim L2 segmentom.

Topologija u virtualnom laboratoriju koristi dio standardne topologije koja se najčešće koristi u korporativnom segmentu. SW1 djeluje kao korijenski most, SW2 i SW3 su ne-root premosnici. Portovi SW1 0/0, 0/1 SW2 0 / 1.0 / 3 SW3 0 / 0.0 / 2 se koriste za promet, 0/0 i 0/1 na SW2 i SW3 su blokirani kako bi se izbjegle petlje. Promet se odvija stazom SW2 – SW1 – SW3. Zatim povezujemo naš Linux stroj na dva pristupna preklopnika SW2 i SW3 i vidimo da primamo STP poruke.

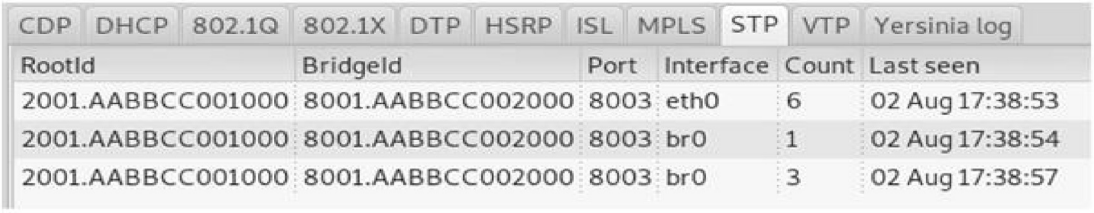


Slika 5. STP i RSTP Protokol [Izvor: https://www.geeksforgeeks.org/introduction-of-spanning-tree-protocol-stp/]

Pregled prometa u Wiresharku, ove poruke znače da je STP na preklopnicima pokrenut i da nije blokiran na portovima povezanim s nama. Kombiniramo naša sučelja u most kako bi promet prošao kroz naš uređaj, pokrećemo Yersinia okvir (eng. Framework) i vidimo da nam je STP dostupan na oba sučelja.

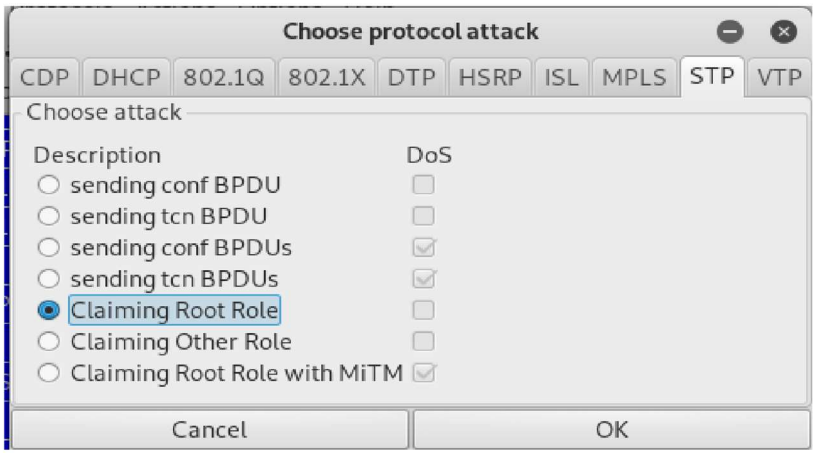


Slika 6. Pregled prometa u Wireshark-u [Izvor: https://spy-soft.net/stp-attack-and-defense/]



Slika 7. Pregled prometa Wireshark programu [Izvor: https://spy-soft.net/stp-attack-and-defense/]

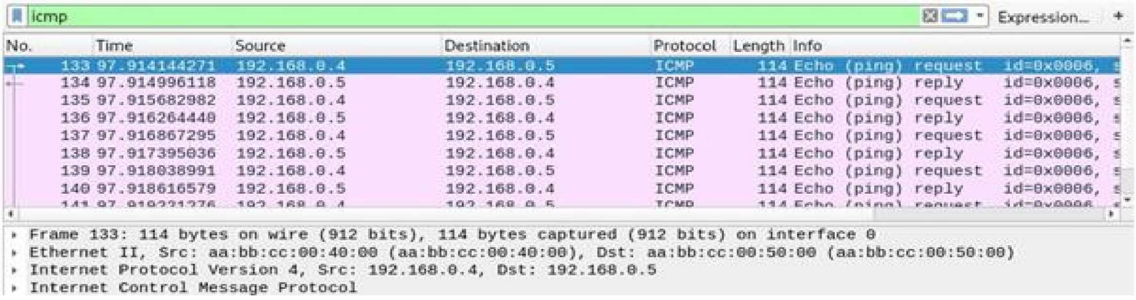
Informacije o primljenim STP BPDU-ovima, pokrećemo napad i biramo tip napada sa zahtjevom Korijenska uloga (eng. Root Role), što znači da ćemo se početi oglašavati kao preklopnik s nižim prioritetom, što će prisiliti STP stablo da se obnovi.



Slika 8. Odabir tipa napada [Izvor: https://spy-soft.net/stp-attack-and-defense/]

Postavili smo korijeski preklopnik (eng. Root switch) za naš mrežni segment i sada možemo vidjeti promet koji je prethodno prošao kroz SW1.

Za provjeru šaljemo ICMP pakte s računala 192.168.0.5 prema računalu 192.168.0.4. U Wireshark programu vidimo da su paketi prošli kroz naše računalo koje je preuzelo ulogu korijenskog mosta.



Slika 9. Pregled paketa [Izvor: https://spy-soft.net/stp-attack-and-defense/]

Yersinia tip napada izgleda ovako:

Poslat ćemo BPDU jednom, što će prisiliti preklopnike u našem L2 segmentu da ponovno izgrade stablo i vrate se na izvornu shemu budući da se BPDU-ovi više ne šalju s našeg računala. Korijenski most šalje konfiguraciju BDPU u intervalu od dvije sekunde, koja specificira glavne parametre, prioritet trenutnog preklopnika, njegov MAC, MAC sučelje s kojeg je poslan BPDU, informacije o tome treba li mehanizam FLUSH početi ispirati CAM tablice. Budući da smo u ovom scenariju pokušali imitirati korijenski most, šaljemo konfiguracijski BPDU s prioritetom jednakim onom trenutnog korijenskog mosta, ali s nižom MAC adresom. Slanje TCN BPDU će prisiliti korijenski most da pokrene mehanizam za brisanje CAM tablica s MAC adresama, s kojih promet ne dolazi dulje od 15 sekundi. Prema zadanim postavkama, vrijeme u kojem je MAC adresa pohranjena u tablici je 300 sekundi. Kada se stanje sučelja promijeni iz isključenog u uključeno, preklopnik koji sudjeluje u STP-u mora poslati TCN (obavijest o promjeni topologije) servisni okvir prema korijenskom mostu kako bi ga obavijestio da je došlo do promjene u mreži. Ostali preklopnici ne znaju koje su MAC adrese bile iza ovog sučelja određenog preklopnika, zbog čega počinje proces čišćenja CAM tablice. Sve adrese koje nisu naučene unutar 15 sekundi bit će izbrisane. Ovakav napad nam omogućuje povećanje opterećenja mreže i CPU-a preklopnika. TCN se šalje jednom.

8.1.1. Zaštita STP i RSTP protokola

STP protokol sadrži mehanizme koji vam omogućuju da suzbijete pojavu novih uređaja kao korijenskog mosta, blokirate portove koji su primili BPDU-ove ili omogućite potpuno BPDU filtriranje.

• ROOT GUARD

Nakon primanja prioritetnog BPDU – a od trenutnog, sučelje koje prima ovaj BPDU bit će stavljeno u korijen-nedosljedan način rada.

• BPDU GUARD

Omogućuje vam da ograničite L2 domenu. Po primitku bilo kojeg BPDU-a, port se stavlja u stanje greške err - disable BPDU guard.

• BPDU filter

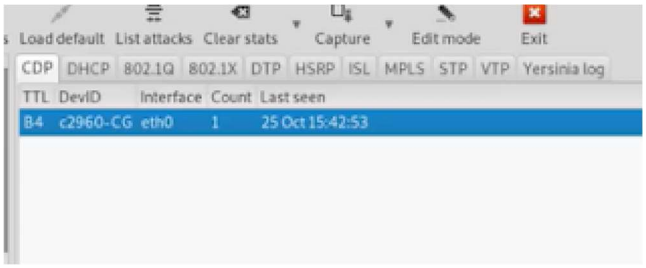
BPDU filter ne šalje niti prima BPDU-ove na sučelju. Drugim riječima, STP je onemogućen na ovom sučelju.

Lako je pretpostaviti da pri korištenju ovih funkcija napadi koji koriste Yersinia framework neće biti dostupni. STP je prilično jednostavan protokol bez sigurnosnih značajki prema zadanim postavkama. Mnogi ljudi zanemaruju instaliranje zaštitnih mehanizama u L2 domeni, što može dovesti do prilično ozbiljnih posljedica.

8.2. CDP napad

Ciscov protokol identifikacije (CDP - Cisco Discovery Protocol) je protokol sloja podatkovne veze koji se koristi za dijeljenje informacija između uređaja izravno povezanih na preklopnik. Ovo je vrsta DoS napada - Uskraćivanje usluge (eng. Denial of Service). Pomoću CDP poplave cijeli preklopnik je preopterećen, MAC tablica se također prelijeva i to može uzrokovati da preklopnik prosljeđuje okvire sa svih sučelja te se ponaša kao koncentrator (HUB). A kada se to dogodi, možete pokrenuti program Wiresharka i pratiti sve podatke na mreži jer se svi okviri prosljeđuju iz svih sučelja dok ispravni preklopnik prosljeđuje samo na ispravno sučelje po MAC adresi.

Kad se otvori sučelje Yersinia okvira (eng. Frameworka) i odabere CDP kartica prikazani su nam svi preklopnici u mreži na koju smo spojeni.



Slika 10. CDP kartica [Izvor: https://medium.com/@suppaboy/cdp-flood-attack-on-cisco-switches-da1ccb0fd28f]

Prvo u cilju izvođenja napada odabire se "Launch Attack" i pošalje CDP paket na preklopnik kao što je prikazano u nastavku.

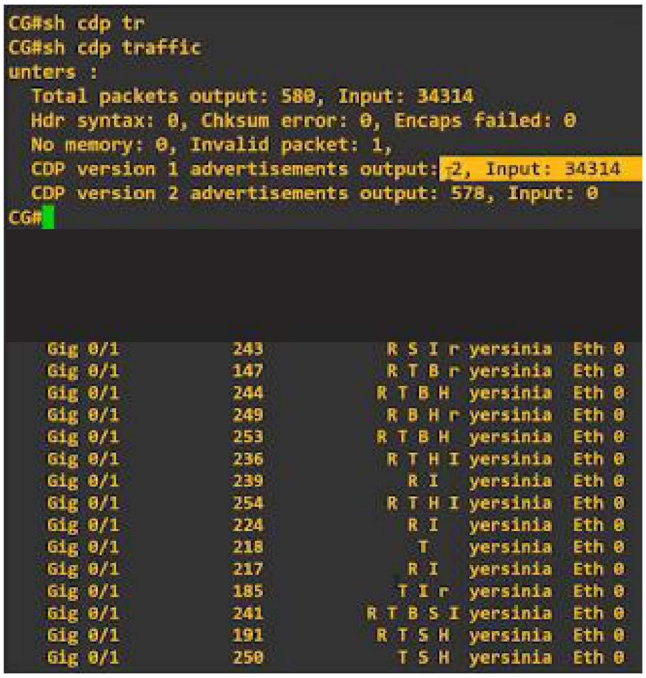
Tada se može provjeriti Yersinia dnevnik i vidjeti da je napad pokrenut kao što je prikazano u nastavku.

Slika 11. Yersinia log [Izvor: https://medium.com/@suppaboy/cdp-flood-attack-on-cisco-switches-da1ccb0fd28f]

Niže je prikaz preljeva paketa koji se šalju.

Slika 12. Prikaz preljeva paketa [Izvor: https://medium.com/@suppaboy/cdp-flood-attack-on-cisco-switches-da1ccb0fd28f]

U komandnoj maski preklopnika se upiše "show CDP Traffic" i vidi se puno CDP ulaza. Na preklopniku će početi treptati sva svjetla.



Slika 13. Komandna maska [Izvor: https://medium.com/@suppaboy/cdp-flood-attack-on-cisco-switches-da1ccb0fd28f]

8.2.1. Zaštita od CDP poplave

Za onemogućavanje CDP poplava dobro je isključiti CDP na preklopniku, ne samo na sučeljima već na cijelom preklopniku.

8.3. DHCP napad

DHCP ima pouzdan port. To su pouzdani priključci koji čine izvor nečije poruke DHCP poslužitelja pouzdane.

Napad na DHCP poslužitelj se vrši korištenjem DHCP izgladnjivanja, koji iscrpljuje cijeli IP popis adresa predviđenih da DHCP poslužitelj dodjeli računalima u mreži.

Princip rada ovog napada je vrlo jednostavan:

- Napravi se upit za IP adresom prema DHCP poslužitelju i dobije se adresa.
- Promijeni se MAC adrese i zatraži nova IP adresa. Promjenom MAC adresa računalo se maskira kao novi klijent.
- Radnja se ponavlja sve dok se ne istroši cijeli skup IP adresa na DHCP poslužitelju predviđen za dodjelu računalima.

Napad izgladnjivanja DHCP-a događa se kada napadač DHCP poslužitelju neprestano šalje krivotvorene DHCP zahtjeve koristeći različite MAC adrese u polju chaddr. Time se iscrpljuju resursi IP adrese DHCP poslužitelja tako da legitimni DHCP klijenti ne mogu dobiti IP adrese. DHCP poslužitelj također možda neće raditi zbog iscrpljenosti resursa sustava.

8.3.1. Zaštita od DHCP izgladnjivanja

Ublažili napad DHCP izgladnjivanja koji koristi DHCP pakete enkapsulirane s različitim izvornim MAC adresama možemo ako ograničimo broj MAC adresa koje mogu biti spojene na sučelje preklopnika.

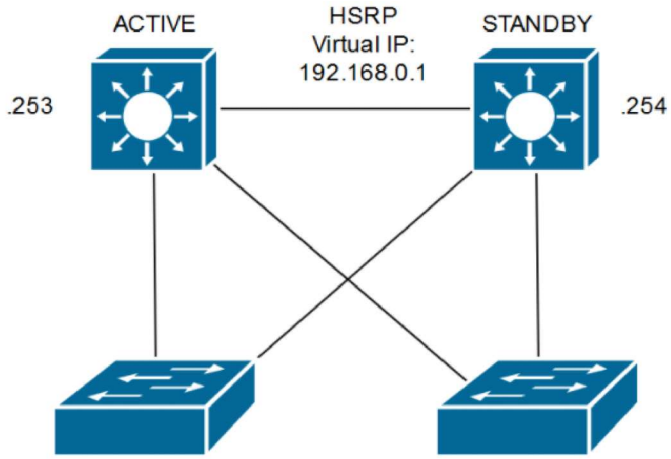
Za sprječavanje DHCP napada izgladnjivanjem koji koristi DHCP zahtjeve enkapsulirane s istom izvornom MAC adresom, treba omogućiti provjeru MAC adrese na DHCP poslužitelju. Kada je ova funkcija omogućena, DHCP poslužitelj uspoređuje polje CHADDR primljenog DHCP zahtjeva s izvornim poljem MAC adrese okvira. Ako su isti, zahtjev se smatra valjanim i prosljeđuje se DHCP poslužitelju, ako nije zahtjev se odbacuje.

8.4. HSRP napad

Protokol visokog stanja pripravnosti (HSRP - Hot Standby Router Protocol) je Ciscov vlasnički protokol koji osigurava redundantnost mreže u slučaju kvara usmjerivača zadanog pristupnika. To je jedan od najčešćih protokola, međutim, sadrži ranjivost koja može dovesti do uskraćivanja usluge ili hvatanja podataka od strane napadača.

HSRP konfiguracija

U simulaciji ćemo koristiti dva Cisco usmjerivača. Osigurat ćemo redundanciju zadanog pristupnika za Vlan 10. Usmjerivač R1-NETVEL bit će primarni usmjerivač, a R2-NETVEL će služiti kao rezervna kopija.



Slika 14. Konfiguracija HSRP [Izvor: https://netvel.sk/hsrp-attack/]

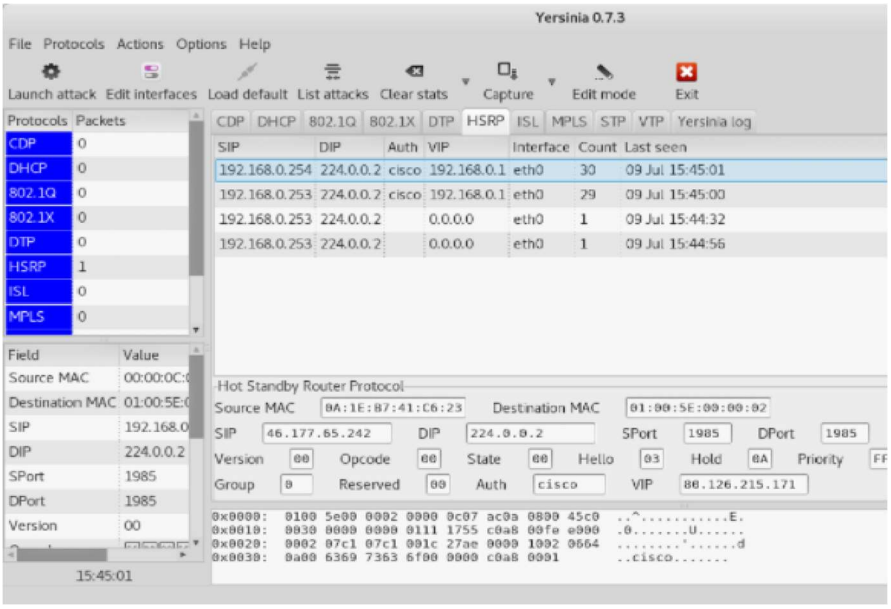
Kao što možemo vidjeti u izlazu naredbe "show standby brief" u nastavku, R1-NETVEL usmjerivač je postao aktivan zbog višeg prioriteta, koji je implicitno 100. R2-NETVEL usmjerivač je u stanju pripravnosti jer je postavljena niža vrijednost prioriteta od 95.

```
R1-NETVEL#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Vl10        10   100 P Active  local           192.168.0.253   192.168.0.1

R2-NETVEL#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Vl10        10   95    Standby 192.168.0.254   local           192.168.0.1
```

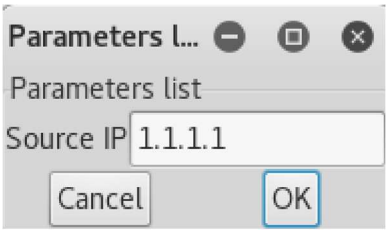
Slika 15. Komandna maska [Izvor: https://netvel.sk/hsrp-utok/]

Cilj ovog napada je preuzeti ulogu HSRP aktivnog usmjerivača od strane naše napadačke stanice, što će uzrokovati uskraćivanje usluge ili preuzimanje podataka na mreži.



Slika 16. HSRP napad [Izvor: https://netvel.sk/hsrp-utok/]

Kada pokrenemo HSRP napad, potrebno je unijeti izvornu IP adresu pod kojom želimo izvesti napad. Adresa ne mora biti u istoj podmreži (eng. subnet).



Slika 17. Unošenje izvorne IP adrese [Izvor: https://netvel.sk/hsrp-utok/]

Ako pokrenemo debug HSRP-a na usmjerivaču, vidjet ćemo kako R1-NETVEL usmjerivač mijenja svoj status u stanje govora, a zatim u stanje pripravnosti.

```
R1-NETVEL#
*Jul  9 13:08:41.535: %HSRP-5-STATECHANGE: Vlan10 Grp 10 state Active -> Speak
*Jul  9 13:08:48.427: %HSRP-5-STATECHANGE: Vlan10 Grp 10 state Speak -> Standby
```

Slika 18. Pokrenut debug HSRP-a [Izvor: https://netvel.sk/hsrp-utok/]

Rezultat napada će se vidjeti nakon izvršavanja "show standby brief" naredbe. Vidimo da su oba usmjerivača proglasila našu napadačku stanicu aktivnim usmjerivačem.

```
R1-NETVEL#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Vl10        10   100 P Standby 1.1.1.1         local           192.168.0.1

R2-NETVEL#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Vl10        10   95    Listen  1.1.1.1         192.168.0.254   192.168.0.1
```

Slika 19. Usmjerivači proglasili našu napadačku stanicu aktivnom [Izvor: https://netvel.sk/hsrp-utok/]

8.4.1. Zaštita od HSRP napada

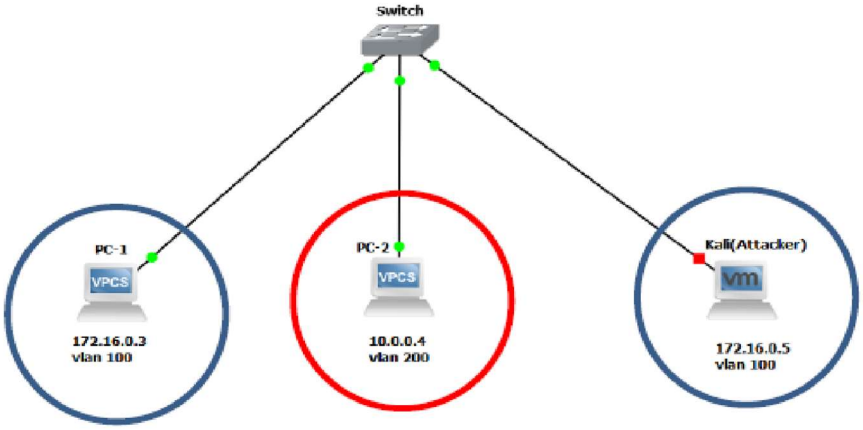
Prije uvođenja HSRP MD5 provjere autentičnosti, HSRP je provjeravao autentičnost paketa protokola jednostavnim nizom običnog teksta. HSRP MD5 provjera autentičnosti je poboljšanje za generiranje MD5 sažetka za HSRP dio višesmjernog paketa HSRP protokola. Ova funkcija pruža dodatnu sigurnost i štiti od prijetnje softvera za lažiranje HSRP-a. MD5 provjera autentičnosti pruža veću sigurnost od alternativne sheme provjere autentičnosti običnog teksta. MD5 provjera autentičnosti omogućuje svakom članu HSRP grupe korištenje tajnog ključa za generiranje ključnog MD5 hasha koji je dio odlaznog paketa. Generira se hash s ključem dolaznog paketa i ako se hash unutar dolaznog paketa ne podudara s generiranim hashom, paket se zanemaruje. HSRP provjera autentičnosti štiti od lažnih HSRP hello paketa koji uzrokuju napad uskraćivanja usluge.

HSRP paketi bit će odbijeni u bilo kojem od sljedećih slučajeva:

- Sheme provjere autentičnosti razlikuju se na uređaju, i u dolaznim paketima.
- MD5 digesti se razlikuje na uređaju i u dolaznom paketu.
- Tekstualni nizovi za provjeru autentičnosti razlikuju se na uređaju, i u dolaznom paketu

8.5. DTP napad

Svrha napada je promjena VLANa na koje je računalo spojeno. Da bi napad bio uspješan, sučelje na preklopniku mora biti podešeno u dinamički ili trunk način rada, tako da preklopnici mogu razgovarati i slati DTP pakete. Prema osnovnim postavkama, sučelja na Cisco preklopnicima su postavljena u dinamički način rada. Za demonstraciju napada korišten je sljedeći scenarij, mala mreža koja ima tri klijenta (napadač i dvije žrtve) u istoj mreži spojeni zajedno na preklopnik.
Imamo preklopnik na koji su spojeni na PC-1 (IP: 172.16.0.3), PC-2 (IP: 10.0.0.4) i Napadač (IP: 172.16.0.5).



Slika 20. DTP napad [Izvor: https://www.securitylab.ru/analytics/495927.php]

Pretpostavili smo da je napadač dobio pristup mreži i da su u istoj domeni razašiljanja, te da je spojen s PC – 1 koji je u VLAN 100 (ista pod mreža i VLAN) što znači da mogu komunicirati jedan s drugim. PC – 2 koji se nalazi u drugoj podmreži i ima VLAN 200 ne može komunicirati ni s PC – 1 i sa napadačem.

Sučelja G0/0, G0/1 dodijeljena su VLAN-u 100, a to su Napadač i PC-1, a sučelje (G0/2) je dodijeljeno VLAN-u 200. Kao što smo već rekli, da bi napad bio uspješan, preklopnik mora imati osnovnu konfiguraciju sučelja (u Dynamic Desirable).

```
vIOS-L2-01#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi0/3, Gi1/0, Gi1/1, Gi1/2
                                                Gi1/3, Gi2/0, Gi2/1
100  VLAN100                          active    Gi0/0, Gi0/1
200  VLAN0200                         active    Gi0/2
```

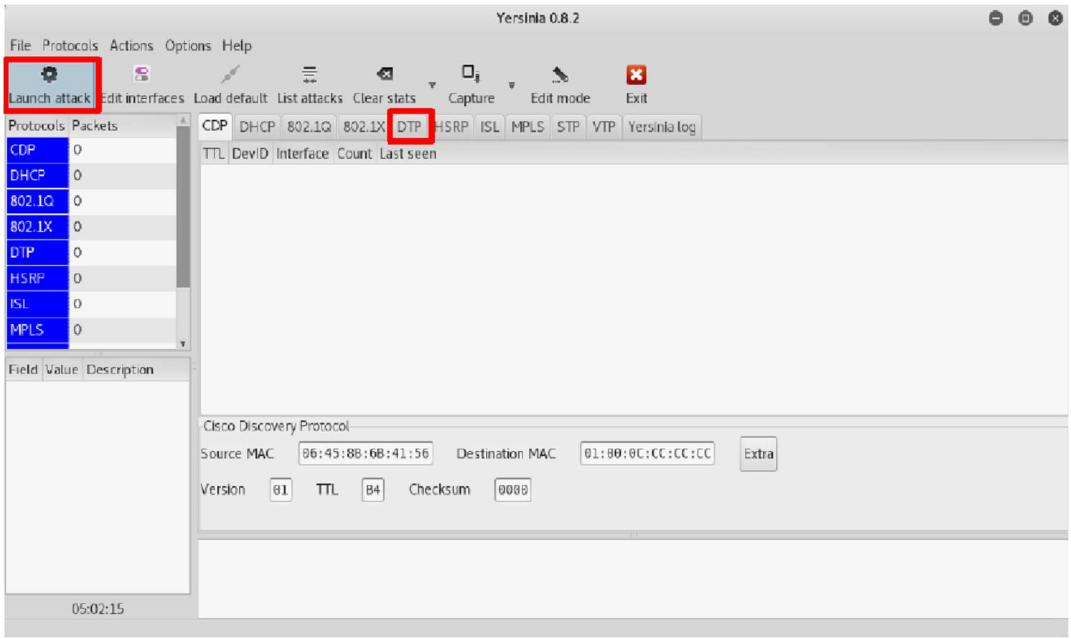
Slika 21. Sučelje G0/0, G0/1 [Izvor: https://www.securitylab.ru/analytics/495927.php]

Pregledom konfiguracije sučelja preklopnika vidimo da je postavljeno na Dinamički poželjno (eng. Dynamic Desirable), tako da se o VLAN-ovima može pregovarati.

```
vIOS-L2-01#show interfaces g0/0 switchport
Name: Gi0/0
Switchport: Enabled
Administrative Mode: dynamic desirable
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 100 (VLAN100)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
```

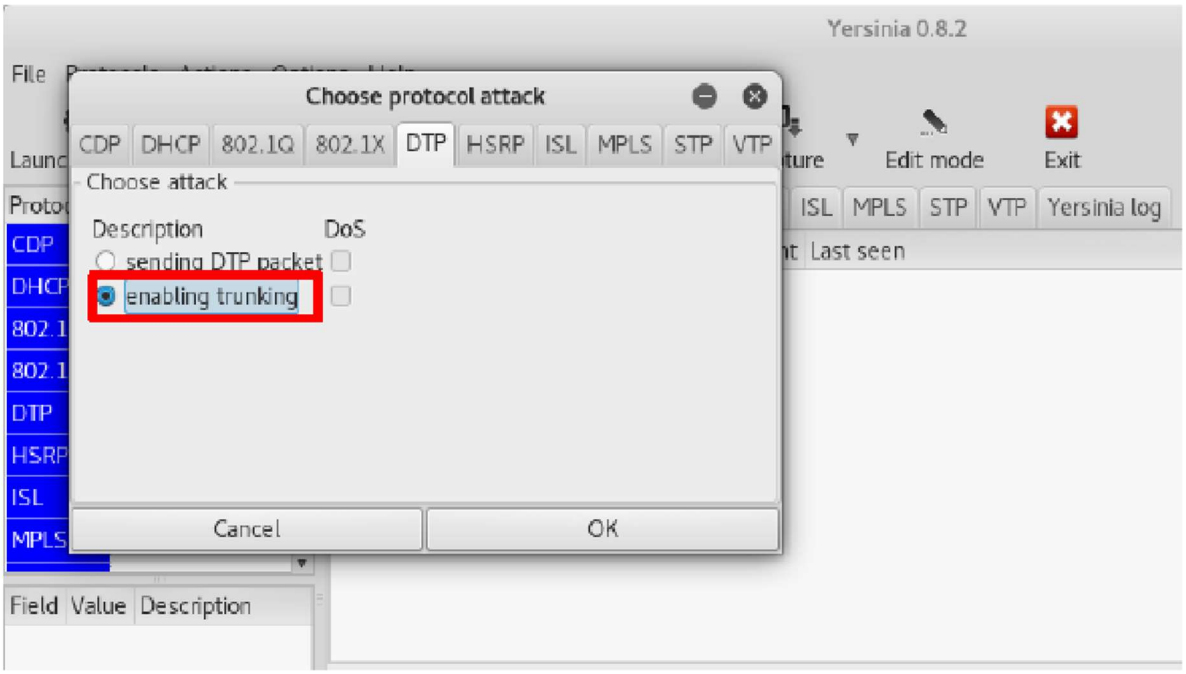
Slika 22. Pregled konfiguracije sučelja preklopnika [Izvor: https://www.securitylab.ru/analytics/495927.php]

Sada pokrećemo okvir (eng. Framework) Yersinia kako bismo omogućili način rada TRUNK, odabirom DTP kartice i pokretanjem napada.



Slika 23. Pokretanje okvira (eng. Framework) Yersinia [Izvor: https://www.securitylab.ru/analytics/495927.php]

Sljedeći korak je odabir napada gdje odabiremo uključivanje trunk moda.



Slika 24. Odabir napada [Izvor: https://www.securitylab.ru/analytics/495927.php]

Pregledom konzole preklopnika možemo vidjeti da su paketi poslani kao DTP događaji.

```
vIOS-L2-01#
*Jul 17 00:46:25.890: DTP-event:Gi0/0:Received packet event ../dyntrk/dyntrk_process.c:2213
```

Slika 25. Pregled konzole preklopnika [Izvor: https://www.securitylab.ru/analytics/495927.php]

Pregledom VLAN tablice vidimo da je sučelje (G0/0) postavljeno u trunk mod što znači da možemo prelaziti u druge VLAN-ove.

```
vIOS-L2-01#show interfaces status

Port      Name               Status       Vlan       Duplex  Speed Type
Gi0/0                        connected    trunk        auto    auto unknown
Gi0/1                        connected    100          auto    auto unknown
Gi0/2                        connected    200          auto    auto unknown
Gi0/3                        connected    1            auto    auto unknown
Gi1/0                        connected    1            auto    auto unknown
Gi1/1                        connected    1            auto    auto unknown
Gi1/2                        connected    1            auto    auto unknown
Gi1/3                        connected    1            auto    auto unknown
Gi2/0                        connected    1            auto    auto unknown
Gi2/1                        connected    1            auto    auto unknown
vIOS-L2-01#
```

Slika 26. Pregled VLAN tablice [Izvor: https://www.securitylab.ru/analytics/495927.php]

Možemo vidjeti da su svi VLAN - ovi dopušteni na sučelju (g0/0).

```
vIOS-L2-01#show interfaces g0/0 trunk

Port        Mode             Encapsulation  Status        Native vlan
Gi0/0       desirable        n-802.1q       trunking      1

Port        Vlans allowed on trunk
Gi0/0       1-4094

Port        Vlans allowed and active in management domain
Gi0/0       1,100,200,300

Port        Vlans in spanning tree forwarding state and not pruned
Gi0/0       1,100,200,300
vIOS-L2-01#
```

Slika 27. Dopušteni VLAN-ovi na sučelju [Izvor: https://www.securitylab.ru/analytics/495927.php]

Da bi napad bio izvršen do kraja potrebno je na računalu dodati novo VLAN sučelje i zadati mu ID=200 čime smo mu definirali da pripada VLAN - u 200. Zatim smo postavili novu IP adresu i dodijelili novo kreirano VLAN sučelje sučelju eth0.200.

```
root@kali:~# modprobe 8021q
root@kali:~# vconfig add eth0 200
Added VLAN with VID == 200 to IF -:eth0:-
root@kali:~# ifconfig eth0.200 up
root@kali:~# ifconfig eth0.200 10.0.0.6 up
root@kali:~#
```

Slika 28. Konfiguracija novog VLAN-a [Izvor: https://www.securitylab.ru/analytics/495927.php]

Konačno možemo pingati PC – 2 koji je u istoj domeni razašiljanja, koji ranije nije bio dostupan i koji je bio na drugom VLAN – u.

```
root@kali:~# ping 10.0.0.4
PING 10.0.0.4 (10.0.0.4) 56(84) bytes of data.
64 bytes from 10.0.0.4: icmp_seq=1 ttl=64 time=18.4 ms
64 bytes from 10.0.0.4: icmp_seq=2 ttl=64 time=21.4 ms
64 bytes from 10.0.0.4: icmp_seq=3 ttl=64 time=33.9 ms
64 bytes from 10.0.0.4: icmp_seq=4 ttl=64 time=24.9 ms
^C
--- 10.0.0.4 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3007ms
rtt min/avg/max/mdev = 18.434/24.680/33.933/5.812 ms
```

Slika 29. Ping prema PC-2 koji ranije nije bio dostupan [Izvor: https://www.securitylab.ru/analytics/495927.php]

8.5.1. Zaštita od napada na DTP

Preskakanje VLAN-a može se iskoristiti samo kada su sučelja postavljena da pregovaraju o trunk modu. Spriječiti nepoželjno VLAN skakanje možemo ako poduzmemo sljedeće mjere:

- Osigurajte da portovi nisu postavljeni da automatski pregovaraju o trunk modu tako što se onemogućiti DTP.
- Nikad se ne koristi VLAN 1.
- Onemogućite neiskorištena sučelja i stavite ih u nekorišteni VLAN.

ZAKLJUČAK

Svi propusti koji su prikazani na protokolima 2 nivo TCP/IP stoga su mogli biti iskorišteni pomoću radnog okvira Yersinia dok su podešeni na automatsku razmjenu postavki. Ako se protokoli kvalitetno podese da rade statično i zahtijevaju intervenciju mrežnog administratora da dopusti spajanje novog računala u mrežu ili se zabrane prometi na mreži koji stvaraju zagušenje prometa paketa, radni okvir Yersinia ne bi bila u mogućnosti iskorištavati propuste istih. Statično podešavanje mrežnih protokola zahtijeva naprednije znanje mrežnog administratora ali za uzvrat se kreira sigurnije mrežno okruženje što i je cilj u kompanijama koje posjeduju osjetljive podatke i koriste informacijski sustav u svakodnevnom radu. Radni okvir Yersinia je napravljen da olakša rad mrežnim administratorima pri pronalasku propusta na mreži.

PRILOZI

LITERATURA

- Bejtlich, Richard. 2013. *The practice of network security monitoring*. San Francisco: no starch press.
- Seder, Lovro. i Ilić, Željko. i Kos, Mladen. 2011. *Sigurno usmjeravanje u ad hoc mrežama.* Automatika, 52:3, 269-278, DOI: 10.1080/00051144.2011.11828425.
- Cisco Systems, 2006. *Moving from concepts to real solutions: Vulnerability Analysis and Best Practices for Adopting IP Communications.* Cisco Systems, Inc.
- Werlinger, Rodrigo. i Hawkey, Kirstie. i Muldner, Kasia. i Jaferian, Pooya. i Beznosov, Konstantin. 2008. *The Challenges of Using an Intrusion Detection System:Is It Worth the Effort?.* Vancouver, Canada: University of British Columbia.
- Balchunas , Aaron. 2012. *OSI Reference Model v1.31.*
- Ignou 2017. *Unit-2 OSI and TCP/IP Models.*
- Nieles, Michael. i Dempsey, Kelley. Pillitteri, Yan, Victoria. 2017. *An Introduction to Information Security*. Computer Security Division Information Technology Laboratory: NIST Special Publication 800-12 Revision 1.
- Stallings, William. 2010. *APPENDIX L TCP/IP and OSI TCP/IP and OSI.*
- Siddique, Nasir. i Ali, Mustafa. i Zubair, Mubeen. 2015. *DATA LINK LAYER SECURITY PROBLEMS AND SOLUTIONS*. Halmstad: Bachelor's Thesis in Computer Network Engineering.
- Mehić, Damir. i Žigman, Dubravko. i Pongrac, Danijela. 2014. *VIRTUALNE LOKALNE RAČUNALNE MREŽE.* POLYTECHNIC & DESIGN. Vol. 2, No. 2, 2014.
- Hunt, Craig, 2002. *TCP/IP Network Administration.* Gravenstein Highway North, Sebastopol: O'Reilly Media, Inc.
- Testa, Ivan. 2019. *Računalne mreže i umrežavanje.* Dubrovnik: Dub. Sveu. Rad, Završni.
- Kizza, Migga, Joseph. 2005. *Computer Network Security.* University of Tennessee-Chattanooga
  Chattanooga: Springer.
- Bošnjaković, Robert. 2011. *Model lokalnih i globalnih računalnih mreža.* Sveu. J. J. Stross. Rad, Dipl.
- Lončar, Saša. 2015. *Računarske mreže i umrežavanje Raspberry PI uređaja.* Polit. Pula. Rad, Završni, Specijalistički.

- CERT, CARNet. i LS&S. *Sigurnosni model mreže računala.* CCERT-PUBDOC-2009-01-253 Revizija 1.02.
- Pralas, Toni. 2008. *Računalne mreže – Mrežne topologije*. sysportal.carnet.hr.
- Nikola, Jelečki. Turkalj, Vedran. 2019. *Spanning-tree-protokol.* POLYTECHNIC & DESIGN Vol. 7, No. 1, 2019.
- Meghanathan, Natarajan. *A Tutorial on Network Security Attacks and Controls.* Jackson: Jackson State University.
- Contributors, Wikipedia. 2022. *List of TCP and UDP port numbers*. Pristupljeno: 20. ožujak 2022. https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers
- Contributors, Wikipedia. 2021. *Hot Standby Router Protocol.* Pristupljeno: 20. ožujak 2022. https://en.wikipedia.org/wiki/Hot_Standby_Router_Protocol
- Admin, Cisco. 2020. *Cisco Discovery Protocol*. Pristupljeno: 20. ožujak 2022. https://learningnetwork.cisco.com/s/article/cisco-discovery-protocol-cdp-x
- Contributors, Wikipedia. 2022. *Dynamic Trunking Protocol Wikipedia*. Pristupljeno: 20. ožujak 2022. https://en.wikipedia.org/wiki/Dynamic_Trunking_Protocol
- Tomac. i Slay. 2017. *Yersinia Kali*. Pristupljeno: 20. ožujak 2022. https://www.kali.org/tools/yersinia