MEĐIMURSKO VELEUČILIŠTE U ČAKOVCU

STRUČNI STUDIJ RAČUNARSTVA

Jelena Lepoglavec

PRIKAZ SIGURNOSNIH MEHANIZMA KROZ OSI I TCP/IP MODEL

ZAVRŠNI RAD

Čakovec, 2015.

MEĐIMURSKO VELEUČILIŠTE U ČAKOVCU

STRUČNI STUDIJ RAČUNARSTVA

Jelena Lepoglavec

PRIKAZ SIGURNOSNIH MEHANIZMA KROZ OSI I TCP/IP MODEL

OVERVIEW OF SECURITY MECHANISM THROUGH OSI AND TCP / IP MODEL

ZAVRŠNI RAD

Mentor:
Jurica Trstenjak, dipl. ing.

Čakovec, 2015.

Zahvaljujem profesoru Jurici Trstenjaku, dipl.ing. i asistentu Bruni Palašeku, struč.spec.ing.el. na vodstvu, pomoći i savjetima tijekom izrade završnog rada.

Jelena Lepoglavec

Sažetak

Završni rad opisuje sigurnosti na fizičkom, mrežnom, transportnom i aplikacijskom sloju uz pomoć današnjih najnovijih tehnologija. Na početku su objašnjene dvije današnje najpoznatije mrežne arhitekture - OSI referentni model (eng. Open System Interconnection) i TCP/IP (eng. Transmission Control Protocol/Internet Protocol) model. Slojevi na OSI mrežnoj arhitekturi, aplikacijski, prezentacijski, sesijski, transportni, mrežni, podatkovni i fizički sloj, detaljno su objašnjeni. Aplikacijski sloj, transportni, mrežni i sloj pristupa medija kod TCP/IP modela također su detaljno razrađeni i objašnjeni. Kod usporedbe OSI i TCP/IP modela navedene su razlike između tih mrežnih arhitektura. Sigurnost mreža na fizičkom, mrežnom, transportnom i aplikacijskom sloju OSI i TCP/IP modela ispitana je pomoću Cisco Packet Tracer[1] alata. Vježbom Layer 2 Security i Layer 2 VLAN Security ispitana je sigurnost na fizičkom sloju, a na mrežnom sloju sigurnost je ispitana vježbom ISO Intrusion Prevention System. Vrste napada na mrežnom sloju, poput Skeniranja IP adrese, lažiranje IP adrese, ICMP napadi i lažiranje poruka usmjerivačkih protokola, objašnjeni su te su spomenute i obrane protiv navedenih napada. Ispitivanje sigurnosti na transportnom sloju odrađeno je pomoću ACL (eng. Access Control List). Objašnjeni su i najčešće korišteni protokoli i servisi koji se koriste na aplikacijskom sloju za upravljanjem mrežom te je konfiguracijom Syslog-a, NTP-a (eng. Network Time Protocol) i SSH (eng. Secure Shell) ispitana sigurnost na navedenom sloju. Osim toga, prikazan je i objašnjen rad sigurnosnih mehanizma koji se implementiraju na različitim slojevima OSI i TCP/IP modela. Na kraju se spominju najčešće korištene i najbolje zaštite korisnika od potencijalnog napada, a tu se podrazumijevaju vatrozidi (eng. Firewall), zaštita od virusa, zaštita od špijunskog i drugog zlonamjernog softvera i Windows ažuriranja.

KLJUČNE RIJEČI: mrežne arhitekture, sigurnost mreže, sigurnosni mehanizmi, napadi, zaštita korisnika

[1] Cisco Packet Tracer: Inovativni mrežni konfiguracijski alat dizajniran od strane Cisco Networking Academy.

Sadržaj

1. Uvod

Međusobna razmjena podataka između dva računala dokaz je da su ona povezana u mreži. Mreže se obično povezuju da bi se stvorile veće mreže. Internet je najpoznatiji primjer mreže najrazličitijih računarskih mreža. To je svjetska mreža koja se sastoji od međusobno povezanih (pod)mreža te omogućava komunikaciju među računalima i pristup različitim uslugama na njima (Rengel i dr., 2008). Mrežom putuju podaci koje je potrebno zaštiti. Ako podaci ostanu nezaštićeni, neautorizirane osobe ih mogu pročitati, izmijeniti ili preusmjeriti na neko drugo odredište.

Danas korišteni sigurnosni mehanizmi štite korisnika od napadača na različitim slojevima mreže. Pitanje sigurnosti postavlja se već na fizičkom sloju. Ukoliko napadač ima fizički pristup mrežnom uređaju ima mogućnost provođenja čitavog niza drugih napada.

2. Mrežne arhitekture

Mrežna arhitektura potpuni je okvir organizacije računalne mreže. Upotpunjenu sliku uspostavljene mreže s detaljnim pregledom svih dostupnih resursa pruža dijagram mrežne arhitekture. To uključuje hardverske komponente koje se koriste za komunikaciju, kabliranje, izgled mreže i topologije, fizičke i bežične veze te provode područja i planove za budućnost. Softver pravila i protokoli također su utemeljeni na mrežnoj arhitekturi. Mrežna arhitektura uvijek je dizajnirana od strane upravitelja, odnosno administratora mreže s koordinacijom mreže inženjera i drugih projektanata.

Mrežna arhitektura pruža pregled pojedinosti o mreži. To se koristi za klasifikaciju svih mrežnih slojeva korak-po-korak u logičkom obliku opisujući svaki korak u detalje. Također se temelji na kompletnim radnim definicijama protokola. Arhitektura u računalnom okruženju i njezina složenost ne može se razumjeti bez okvira. Stoga postoji potreba za razvojem aplikacija ili metoda za pregled mreže.

Okvir je, u arhitekturi mreže, podatak koji se prenosi između mrežnih točaka kao cjelina zajedno sa adresiranjem i potrebnim informacijama.

Nad informacijskim jedinicama u čvorovima informacijske mreže se provode operacije komutacije i procesiranja. Operacijom transmisije, informacijske jedinice premještaju se između čvorova. Komutiranje informacijskih jedinica provodi se samo u nekim mrežnim čvorovima, dok se u nekima vrši procesiranje, koje može biti iznimno složeno. Neki čvorovi generiraju informacijske tokove koji putuju mrežom i koje drugi čvorovi u mreži apsorbiraju. Intuitivno je jasno da ne provode svi čvorovi iste operacije nad informacijskim jedinicama te da u nekim čvorovima postoji više „inteligencije“ za obradu informacijskih jedinica nego u drugima (Jukić i Heđi, 2012.). Informacijske jedinice putovat će mrežnim granama i biti preusmjeravane vrlo vjerojatno kroz više mrežnih čvorova bez procesiranja sadržaja informacijskih jedinica. Tek će odredišni čvor imati u sebi dovoljno „inteligencije“ da u potpunosti procesira korisnički zahtjev. Kako bi se naznačila ovakva arhitektura, u kojoj nemaju svi čvorovi iste kapacitete za provođenje operacija na informacijskim jedinicama, arhitektura informacijske mreže prikazuje se slojevito. Slojevi su smješteni jedan iznad drugog po vertikali, pri čemu viši slojevi imaju više „inteligencije“.

Današnje najpoznatije mrežne arhitekture su :

1. OSI referentni model
2. TCP/IP model

2.1. OSI referentni model

Organizacija ISO (eng. *International Organization for Stadardization*) definirala je 1984. godine OSI referentni model (eng. *Open System Interconnection*). On označava model pomoću kojeg aplikacije mogu komunicirati preko mreže. Referentni model je konceptualni okvir za razumijevanje odnosa. Svrha OSI referentnog modela je voditi dobavljačima i programerima digitalne komunikacijske proizvode i softverske programe koje oni stvaraju, tako da rade jedni s drugima i olakša jasne usporedbe između komunikacijskih alata. Njime je moguće opisati svaki otvoreni sustav pomoću slojeva složenih po vertikali. Glavni koncept OSI modela jest da je on proces komunikacije između dviju krajnjih točaka u telekomunikacijskoj mreži te se može podijeliti u sedam različitih skupina, povezanih funkcija ili slojeva. Svako komuniciranje korisnika ili program na računalu mora proći sedam slojeva funkcije. Dakle, određenom porukom između korisnika održat će se protok podataka kroz slojeve u izvornom računalu, preko mreže, a zatim kroz slojeve u prijamnom računalu. Sedam slojeva funkcija pružaju kombinaciju aplikacija, operativnih sustava, mrežne kartice upravljača i umrežavanje hardvera koji omogućuju u sustav postaviti signal preko mrežnog kabla ili preko Wi-Fi-a[2]. OSI model dijeli arhitekturu mreže u sedam logičkih razina te daje spisak funkcija, servisa i protokola koji funkcioniraju na svakoj razini. Logičke razine OSI modela su aplikacijski sloj, prezentacijski sloj, sesijski sloj, transportni sloj, mrežni sloj, podatkovni sloj i fizički sloj.

OSI-model ili referentni model je najkorišteniji apstraktni opis arhitekture mreže.

[2] Wi-Fi: zaštitni znak koji se postavlja na certificirane proizvode za bežičnu lokalnu računalnu mrežu (WLAN) zasnovane na specifikacijama IEEE 802.11.

2.1.1. Aplikacijski sloj

Aplikacijski sloj (eng. *application layer*) je sloj koji podržava aplikacije i krajnje procese korisnika. Na njemu su identificirani partneri u komunikaciji te kvaliteta usluge, autentikacija korisnika i privatnost te su identificirana ograničenja sintakse podataka. Ovaj sloj pruža aplikacijske usluge za prijenos datoteka, e-maila i drugih mreža softverskih usluga. Telnet i FTP su aplikacije koje postoje u potpunosti na razini aplikacijskog sloja.

2.1.2. Prezentacijski sloj

Ovaj sloj pruža neovisnost od razlike u zastupljenosti podataka (primjerice šifriranje) prevođenjem iz aplikacije na mrežnom formatu i obrnuto. Prezentacijski sloj (eng. *Presentation Layer*) radi tako da transformira podatke u oblik koji aplikacijski sloj može prihvatiti. Ovaj sloj preoblikuje i šifrira podatke koji se šalju preko mreže, pružajući slobodu od problema s kompatibilnošću. To se ponekad naziva sintaksa sloj.

2.1.3. Sesijski sloj

Ovaj sloj uspostavlja, upravlja i prekida veze između lokalne i udaljene aplikacije. Sjednica sloj (eng. *Session Layer*) uspostavlja, koordinira i završava razgovore te vodi razmjenu i dijalog između aplikacija na svakom kraju.

2.1.4. Transportni sloj

Transportni sloj (eng. *Transport Layer*) pruža transparentan prijenos podataka između krajnjih sustava, prihvaća podatke od viših slojeva, rastavlja ih na dijelove i šalje mrežnom sloju. On osigurava da segmenti ispravno stignu na drugi kraj. Transportni sloj određuje koji će se tip usluge pružati sesijskom sloju i samim time koji će se stupanj zaštite primjenjivati za prijenos podataka.

2.1.5. Mrežni sloj

Ovaj sloj pruža preklopniku i usmjerivaču tehnologije stvaranje logičkih staza, poznatih kao virtualni krugovi, za prijenos podataka od čvora do čvora. Usmjeravanje i prosljeđivanje su funkcije mrežnog sloja (eng. *Network Layer*), kao i rješavanje, umrežavanje, rukovanje pogreškama, kontrola zagušenja i sekvenciranja paketa. Mrežni sloj koristi logičko adresiranje (jedan od primjera je i IP adresa) kako bi znao na koje

odredište se šalje paket. Ovisno o parametrima u mreži, paketi mogu putovati različitim putanjama kroz mrežu. Pomoću metode najboljeg mogućeg prijenosa (eng. *best effort*), prenose se podaci na mrežnom sloju što i ujedno znači da se ne vodi računa o sigurnoj dostavi paketa.

2.1.6. Podatkovni sloj

Osnovna zadaća podatkovnog sloja je pouzdan prijenos podataka preko medija. Brine se o pristupu mediju za prijenos podataka i otkriva pogreške u prijenosu preko fizičkog sloja. U podatkovnom sloju (eng. *Data Link Layer*) paketi podataka su kodirani i dekodirani u komadiće. Tijekom prijenosa podataka pošiljatelj rastavi ulaznu poruku na dijelove koji se nazivaju okviri (eng. *frame*) i pošalje ih slijedno po fizičkom sloju. Ako pošiljatelj šalje više informacija nego što ih primatelj može obraditi, podatkovni sloj sprječava zastoj pomoću signalizacije i međuspremnika za privremeno pohranjivanje podataka. Podatkovna razina je podijeljena u dva pod sloja: MAC (eng. *The Media Access Control*) sloj i LLC (eng. *Logical Link Control*) sloja.

2.1.7. Fizički sloj

Fizički sloj (eng. *Physical Layer*) prenosi bitove – električke impulse, svjetlosne ili radio signale – preko mreže na električnu i mehaničku razinu. On definira fizičke i električne specifikacije uređaja i fizičkog medija po kojem se prenose podaci.

RS-232 je primjer standarda na fizičkom sloju kojim se točno definira što je potrebno za serijsku komunikaciju između dva mrežna uređaja na fizičkom sloju.

2.2. TCP/IP model

Slično OSI referentnom modelu, postoji i referentni model za TCP/IP arhitekturu koji je znatno jednostavniji. TCP/IP protokol kartu do četiri sloja konceptualnog modela poznatog kao DARPA model čine aplikacijski, transportni, mrežni i sloj pristupa mediju. DARPA model stvoren je od strane Ministarstva obrane SAD-a (*DoD, Department of Defense*) želeći stvoriti mrežu koja će "preživjeti" bilo kakve uvjete, pa čak i nuklearni rat.

TCP/IP (eng. *Transmission Control Protocol/Internet Protocol*) je osnovna komunikacija jezika ili protokol interneta. Također se može koristiti kao komunikacijski protokol u privatnoj mreži. Kada se računalo spoji izravno na internet, ono se isporučuje sa kopijom TCP/IP programa kao i svako drugo računalo koje može slati poruke ili dobiti informacije, a da također ima kopiju TCP/IP-a.

TCP/IP je program sa dva sloja. Viši sloj, TCP (eng. *Transmission Control Protocol*), upravlja tako da sastavlja poruke ili datoteke u manje pakete koji se prenose preko interneta i prima TCP sloj koji šalje pakete s izvornom porukom. Donji sloj, IP (eng. *Internet protokol*), obrađuje adresu svakog dijela paketa, tako da se dobiva na pravo odredište. Svaki pristupnici na računalu na mreži provjere ovu adresu kako bi vidjeli gdje proslijediti poruku. Iako su neki paketi iz iste poruke preusmjereni drugačije od drugih, oni će biti ponovno poslani na odredište.

2.2.1. Aplikacijski sloj

Ovo je mjesto gdje TCP/IP govori izravno sa krajnjeg korisnika aplikacije. Aplikacijski sloj upravlja sa protokolima višeg nivoa, kontrolom dijaloga, problematikom prikaza i enkodiranjem.
TCP/IP kombinira svu problematiku vezanu uz aplikativni dio u jednom sloju (aplikacijskom) i osigurava ispravno pakiranje podataka za sljedeći sloj.

2.2.2. Transportni sloj

Ovaj sloj pretvara podatke u pakete i upravljanje protokom paketa preko mreže između aplikacija i korisnika. Brine se o kvaliteti usluge, problematici pouzdanosti, protoku podataka i ispravljanu grešaka.

2.2.3. Mrežni sloj

Mrežni sloj ili sloj pristupa mreži je odgovoran za sastavljanje TCP/IP paketa na mrežnom mediju i primanje TCP/IP paketa izvan mreže medija. To je mjesto gdje je mrežna komunikacija uspostavljena i odvijaju se IP adresiranje i usmjeravanje. TCP/IP je dizajniran da bude neovisan o metodi mrežnog pristupa, okvira formata i medija. Na ovaj način, TCP/IP se može koristiti za povezivanje različite vrste mreža. To uključuje LAN tehnologije kao što su *Ethernet* i *Token Ring* i WAN tehnologije, kao što su X.25 i *Frame Relay*. Neovisnost od bilo koje specifične mrežne tehnologije pruža TCP/IP mogućnost da se prilagoditi novim tehnologijama, kao što su asinkroni način prijenosa (ATM).

2.2.4. Sloj pristupa medija

Sloj pristupa mediju ili internet sloj odgovoran je za adresiranje, pakiranje i usmjeravanje funkcija. Internet sloj je analogan mrežnom sloju OSI modela. Temeljni protokoli interneta sloju IP, ARP, ICMP, i IGMP.

IP (eng. *Internet Protocol*) je usmjeravanje protokola odgovornog za IP adresiranje, usmjeravanje i fragmentacije.

ARP (eng. *Adresa Resolution Protocol*) odgovoran je za rješavanje internet sloja obraćanju mrežnog sučelja sloja adrese, kao što je hardver adresa.

ICMP (eng. *Internet Control Message Protocol*) je odgovoran za pružanje dijagnostičkih funkcija i izvješćivanje pogrešaka zbog neuspješne isporuke IP paketa.

IGMP (eng. *Internet Group Protokol*) odgovoran je za upravljanje IP *multicast* skupine.

2.3. Usporedba OSI i TCP/IP modela

Referentni modeli TCP/IP i OSI imaju mnogo zajedničkoga. Oba se zasnivaju na konceptu skupa nezavisnih protokola i funkcionalnost slojeva im je prilično slična. Usprkos navedenim načelima sličnosti između modela postoje i mnoge razlike.

OSI referentni model sastoji se od sedam slojeva, dok TCP/IP referentni model čine četiri sloja kao što je prikazano slikom 1.

OSI model jasno je povukao granicu između tri ključna koncepta, a to su: usluge, sučelje i protokoli. Svaki sloj obavlja određene usluge za sloj iznad sebe (Tanenbaum i Wetherall 2012). Sučelje između slojeva ukazuje procesima iz gornjeg sloja kako da pristupe daljnjem sloju. Podređeni protokoli koji se koriste unutar sloja tiču se samo toga sloja. TCP/IP na početku nije povukao jasnu granicu između ta tri koncepta i zbog toga su protokoli u OSI modelu bolje skriveni i mogu se lakše zamijeniti s napretkom tehnologije nego protokoli kod TCP/IP-a.

Druga razlika odnosi se na komunikaciju sa uspostavljanjem direktne veze i bez nje. Nudeći korisnicima izbor, TCP/IP model u transportnom sloju podržava oba skupa komunikacije za razliku od OSI modela koji podržava kod transportnog sloja samo komunikaciju s uspostavljanjem direktne veze.

Kod OSI modela transportni sloj jamči isporuku paketa i slijedi horizontalni pristup, dok kod TCP/IP modela transportni sloj ne jamči isporuku paketa i slijedi vertikalni pristup. OSI je opći model za razliku od TCP/IP modela koji se ne može koristiti u bilo kojoj drugoj primjeni.

<table>
<tr><th>Primjer</th><th>TCP/IP sloj</th><th>OSI-RM sloj</th></tr>
<tr><td rowspan="2">SMTP, SSH, FTP, HTTP</td><td rowspan="2">4. Aplikacija</td><td>7. Aplikacija</td></tr>
<tr><td>6. Prezentacija</td></tr>
<tr><td rowspan="2">UDP, TCP</td><td rowspan="2">3. Transport</td><td>5. Sesija</td></tr>
<tr><td>4. Transport</td></tr>
<tr><td>Segment</td><td>2. Internet</td><td>3. Mreža</td></tr>
<tr><td rowspan="2">Bit</td><td rowspan="2">1. Sloj podatkovne veze</td><td>2. Podatkovna veza</td></tr>
<tr><td>1. Fizički sloj</td></tr>
</table>

Slika 1. Usporedba TCP/IP slojeva sa OSI-RM modelom [1]

3. Sigurnost mreža na slojevima OSI i TCP/IP modela

Sigurnosni model računalne mreže je samo jedan od mogućih modela koji postoje. On mora biti smisleno oblikovan kako bi omogućio sigurnosnoj zajednici metode istraživanja, primjene i održavanja mrežne sigurnosti koja se može primijeniti na bilo koju mrežu. Prilikom istraživanja sigurnosni model, podjelom po slojevima, može se koristiti kao alati za analizu mrežne sigurnosti. Kod postavljanja mrežne sigurnosti, model se može iskoristiti za stvaranje mrežne arhitekture. U smislu održavanja postojećih mreža može se koristiti za razvoj rasporeda pregleda sigurnosnih mjera. Organizacija sigurnosti po slojevima je svakako dobar način osiguravanja optimalne zaštite mrežnog sustava. Uz to, sigurnosni model računalne mreže može se upotrijebiti za otkrivanje neovlaštenih provala te za smanjivanje mogućnosti da se oni ponovno pojave.

Sigurnost komunikacijskih sustava kontinuirano se suočava s novim izazovima. Ljudi postaju sve više ovisni o bežičnim tehnologijama za prijenos osobnih podataka, kao što su Internet bankarstvo putem bežične pristupne točke ili mobilnih plaćanja putem uređaj-na-uređaj vezu. Unatoč praktičnosti bežičnih mreža, emitiranje čini bežični medij ranjivim na napade od neovlaštenog prisluškivanja. Izazovan problem sigurne bežične

komunikacije već je privukao značajnu pažnju iz različitih istraživačkih zajednica u komunikaciji, obrada signala i cyber-sigurnosti. Ovi istraživački napori kulminirali su u ogromna poboljšanja u postojećim kriptografskim tehnikama i još važnije, u uvođenju nove sigurnosne paradigme za bežične mreže, nazvan kao fizički sloj sigurnosti.

3.1. Sigurnost mreža na fizičkom sloju

Fizički sloj je najslabija točka bilo koje mreže. Ako je fizički sloj napadnut neće biti pomoći u sprečavanju napada. U tom slučaju napadač može neovlašteno pristupiti podacima.

Fizička sigurnost uključuje projektiranje sigurnosti ustanove, postavljanje uređaja za kontrolu pristupa, alarma i kamera.

Poslužitelj, mrežna oprema i klijent su mrežne sastavnice na fizičkom sloju te se na njih prvenstveno odnosi sigurnost na fizičkom sloju. Ukoliko jedna od ovih sastavnica nije fizički osigurana napadač može preuzeti nezaštićenu sastavnicu te otuđiti podatke, ako je riječ o poslužitelju ili klijentu, odnosno konfiguraciju mrežnog uređaja.

Fizički sloj sigurnosti je prvo sigurnosno rješenje koja se fokusira na iskorištavanje fizičkog sloja svojstava bežičnog kanala, kao što je gubljenje signala kod prijenosa (eng. *multi-path fading*) i interferencije, za zaštitu povjerljivih informacija prijenosa protiv prisluškivanja. On također može lijepo nadopuniti trenutne kriptografske tehnike kao dva pristupa koji djeluju u različitim područjima - jedan štiti fazu komunikacije dok drugi štiti obradu podataka nakon faze komunikacije.

Fizički je sloj najlakše osigurati jer ne zahtjeva napredne tehničke koncepte. Moguće je unajmiti tvrtku koja će postaviti alarmni sustav te zaposliti zaštitara.

3.1.1. Ispitivanje sigurnosti na fizičkom sloju

Ispitivanje sigurnosti pomoću Layer 2 Security

Vježbom *Layer 2 Security* ispitana je sigurnost na fizičkom sloju. Za optimalne performanse i sigurnost trebalo je osigurati da *je root bridge 3560 Central* prekidač (eng. *switch*). Kako bi se spriječila manipulacija napada na *spanning-tree*, trebalo je osigurati parametre STP. Omogućena je kontrola kako bi se spriječile oluje (eng. *storms*) ili emitiranje oluja. Kako bi se spriječili napadi protiv MAC adresa,

konfigurirani je *port* sigurnosti koji ograničava broj MAC adresa. Ako broj MAC adresa premašuje zadanu granicu, *port* treba biti zatvoren.

Prvi zadatak u ovoj vježbi je konfiguracija *Root Bridge*. Od *Central* prekidača izdana je *show spanning-tree* naredba za određivanje trenutnog *Root Bridge* i za prikaz portova koji se koriste te njihov status. Trenutni *root-bridge* je bio prekidač SW-1. Kod drugog koraka u ovom zadatku centralnom prekidaču dodijeljen je zadatak da bude osnovni *root-bridge*, pomoću naredbe *spanning-tree vlan 1 root primary*. Nakon toga, prekidaču SW-1 dodijeljen je, pomoću naredbe *spanning-tree vlan 1 root secondary*, zadatak da bude sporedan *root-bridge*. Četvrtim korakom provjerena je konfiguracija *spanning-tree*. Izdavanjem naredbe *show spanning*-tree provjereno je da li je 3560 Centralni preklopnik *root-bridge*. Da, 3560 Centralni preklopnik je *root-bridge*.

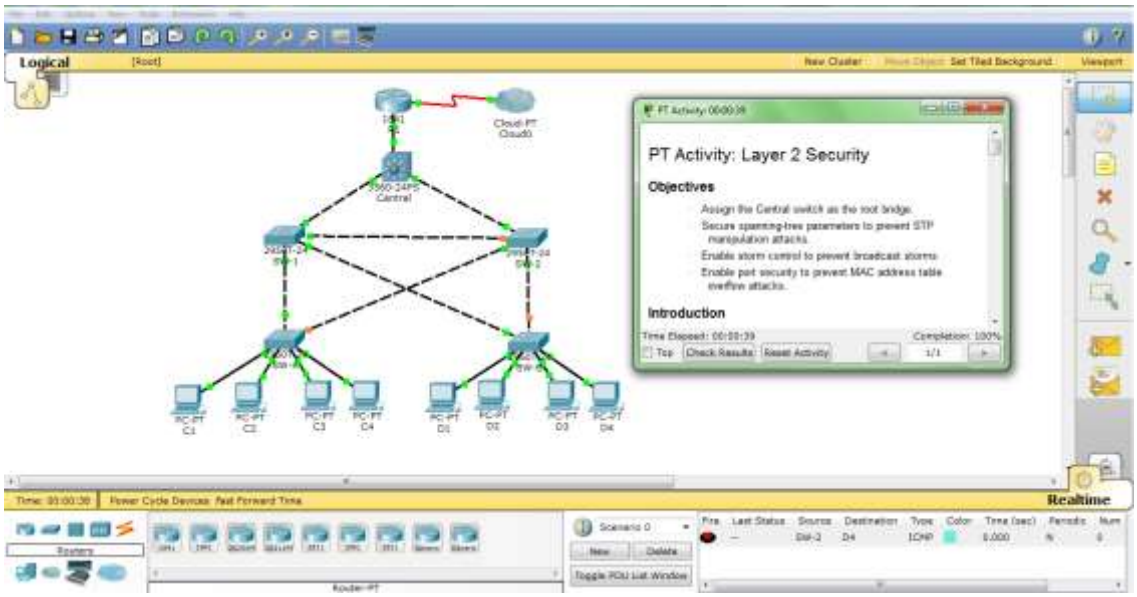
Drugi zadatak bio je zaštita od STP (eng. *Spanning Tree Protocol***)** napada. STP sprječava formiranje petlji kada su prekidači ili mostovi međusobno povezani preko višestrukih mjesta. Osigurani su parametri STP-a kako bi spriječili STP manipulacije napada. Prvi korak je da se osigura *PortFast* za sve pristupne portove. *PortFast* je konfiguriran na pristupnim točkama portova koje su povezane na jednu radnu stanicu ili poslužitelja koji će im omogućiti da postanu brže aktivne. Na povezanim pristupnim portovima od preklopnika SW-A i SW-B korištena je naredba *spanning-tree portfast*. Na svim pristupnim portovima omogućena je BPDU straža (eng. *Guard*). BPDU stražar je značajka koja može spriječiti loše prekidače i podvale na pristupnim portovima. Preko naredbe *spanning-tree bpduguard enable* omogućena je BPDU straža na SW-A i SW-B pristupnim portovima.

Kod trećeg zadatka omogućena je kontrola emisije oluja (eng. *Storm*). Postavljena je 50 posto viša razina suzbijanja pomoću naredbe *storm-control broadcast*. Nakon toga provjerena je konfiguracija *storm-controle*, korištenjem naredbe *show storm-control broadcast* i naredbe *show run*.

Konfiguriran je priključak sigurnosti (eng. *Port Security*) i onemogućeni su neiskorišteni portovi.

Prvi korak kod četvrtog zadatka bilo je konfigurirati osnove sigurnosti na svim portovima koji su povezani na glavni (eng. *Host*) uređaj. Taj postupak proveden je na svim pristupnim portovima preklopnika SW-A i SW-B. Korištenjem naredbe *switchport port-security maximum* 2 postavljen je maksimalan broj MAC adresa te da se MAC

adresa saznaje dinamički. Postavljeno je narušavanje (eng. *Violation*) na zaustavljanje. Port-sigurnosti na drugim usmjerivačima i preklopnicima nisu omogućeni jer portovi koji su povezani na druge preklopnike i usmjerivače mogu i trebali bi imati mnoštvo MAC adresa za taj jedan port. Limitirati broj MAC adresa koje mogu biti na tim portovima mogu značajno utjecati na funkcionalnost mreže. Kod drugog koraka napravljena je provjera porta-sigurnosti. Na preklopniku SW-A, izdana je naredba *show port-security interface fa0/1* kako bi se provjerilo je li konfiguriran port-sigurnosti. Za kraj, onemogućeni su neiskorišteni portovi na preklopnicima SW-A i SW-B, korištenjem naredbi *interface fa0/5, interface fa0/*6 i naredbe *shutdown.* Slika broj dva prikazuje da je vježba odrađena sto posto.



Slika 2. Vježba Layer 2 Security.[2]

Ispitivanje sigurnosti pomoću Layer 2 VLAN Security

Ispitivanje sigurnosti na fizičkom sloju ispitano je pomoću Layer 2 VLAN Security. U ovoj vježbi ciljevi su sljedeći: spajanje na novu suvišnu vezu između preklopnika SW-1 i SW-2, omogućivanje kanala i konfiguriranje sigurnosti na novim kanalnim vezama između preklopnika SW-1 i SW-2, stvaranje novog upravitelja VLAN 20 te provođenje ACL- a kako bi se spriječilo vanjske korisnike u pristupu upravljanja VLAN-om.

Mrežna tvrtka trenutačno je postavljena pomoću dva odvojena VLAN-a: VLAN 5 i VLAN 10. Osim toga, svi kanalni priključci su konfigurirani s izvornim VLAN 15. Mrežni administrator dodaje suvišne vezu između prekidača SW-1 i SW-2. Veza mora imati omogućene kanale i svi sigurnosni uvjeti trebaju biti na mjestu. Osim toga, mrežni administrator spaja upravitelja, PC na preklopnika SW-A. Administrator omogućuje upravljanje PC računala tako da će ono imati mogućnost spajanja na sve prekidače i usmjerivače, uz uvjet da se drugim uređajima zabrani spajanje na upravitelja, PC ili ostale prekidače. Administrator stvara novi VLAN 20 za potrebe upravljanja.

Prvi zadatak u ovoj vježbi odnosi se na provjeru povezivanja. Provjeravanja povezanosti između C2 (VLAN 10) i C3 (VLAN 10) i provjera povezanost između C2 (VLAN 10) i D1 (VLAN 5). Ako se koriste jednostavni PDU GUI paket, treba pingati dva puta kako bi se omogućio ARP.

Zadatak dva je stvaranje suvišnih veza između prekidača SW-1 i SW-2. Prvi korak je da se pomoću križnog kabela spoje priključak Fa0/23 na preklopniku SW-1 sa priključkom Fa0 / 23 na preklopniku SW-2. Korak dva je omogućiti kanale i uključiti sve kanale sigurnosti na vezama između preklopnika SW-1 i SW-2. Kanali su konfigurirani na svim već postojećim kanalima sučelja. Nova veza mora biti konfigurirana za armaturu, uključujući sve kanale sigurnosnih mehanizama. Na oba preklopnika SW-1 i SW-2 potrebno je postaviti port za prtljažnik, dodijeliti izvorni VLAN 15 do kanalnih portova i onemogućiti automatsko pregovaranje uz pomoć naredbe *switchport nonegotiate*.

Treći zadatak temelji se na omogućavanju VLAN-a 20 kao upravitelja VLAN-om. Administrator mreže je u mogućnosti pristupiti svim preklopnicima i usmjerivačima koristeći upravitelja PC-a. Administrator osigurava sigurnost tako da su svi uređaji za

upravljanje na posebnom VLAN-u. Prvi korak je omogućiti upravljanje VLAN (VLAN 20) na preklopniku SW-a. Pomoću naredbe *vlan 20,* koja se upisuje u ikonu *Command Prompt* na preklopniku SW-A, omogućuje se VLAN 20. Korištenjem naredbe *interface vlan 20* i *ip address* 129.168.20.1 255.255.255.0 stvara se novo sučelje VLAN 20 i dodjeljuje mu se IP adresa unutar 192.168.20.0/24 mreže. Drugi korak je omogućiti isti VLAN upravljanja na svim ostalim prekidačima. Na primjer, na prekidaču SW-B:

SW-B(config)# vlan 20

SW-B(config-vlan)# exit

SW-B(config)# interface vlan 20

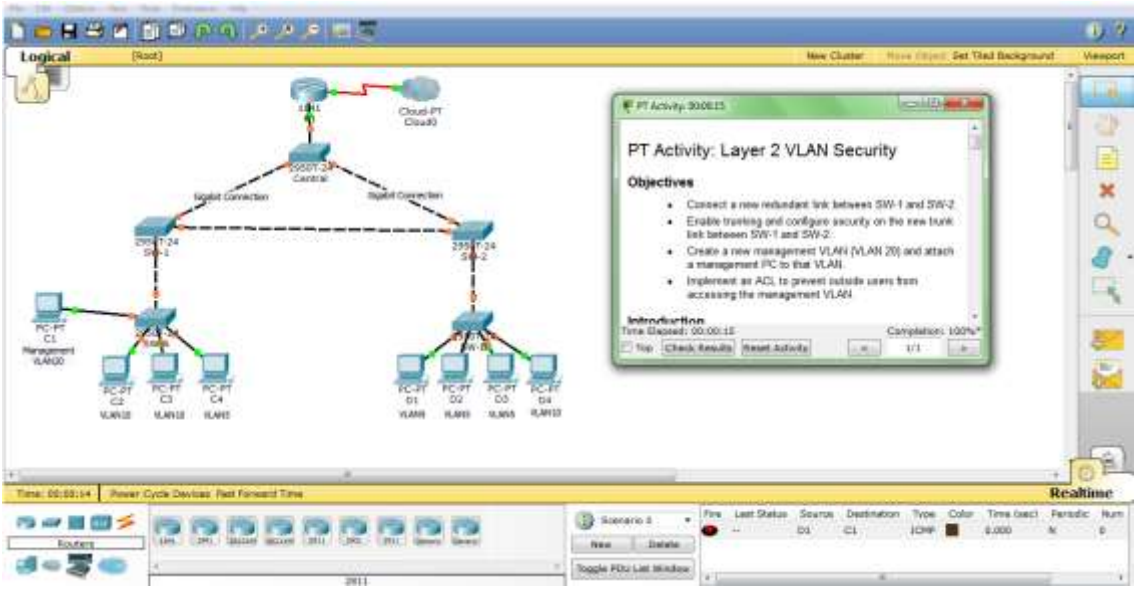
SW-B(config-if)# ip address 192.168.20.2 255.255.255.0

Treći korak je konfiguracija upravitelja PC-a te spajanje PC-a na prekidač SW-A port Fa0 /1. Na prekidaču SW-A se provjerava je li upravitelj PC-a dio VLAN 20. Sučelje Fa0 / 1 mora biti dio VLAN 20. Kod petog koraka provjerava se povezanost upravitelja PC-a sa ostalim preklopnicima. Upravitelj PC je u mogućnosti pingati SW-A, SW-B, SW-1, SW-2 i Central.

Četvrti zadatak je omogućiti upravitelju, PC-u pristup usmjerivaču R1. Prvi korak je da se omogući novo pod sučelje na usmjerivaču R1. Stvara se novo pod sučelje Fa0 / 0,3 i dodjeljuje IP adresu unutar 192.168.20.0/24 mreže. Korištenjem *naredbe encapsulation dotlq 20* postavlja se enkapsulacija na račun za VLAN 20. Drugi korak je provjeravanje povezanosti između upravitelja, PC-a i usmjerivača R1. zatim slijedi konfiguriranje zadanog pristupnika (eng. *Default Gateway*) na upravitelja PC-a kako bi se omogućilo povezivanje. Omogućiti sigurnost dio je trećeg koraka. Dok upravitelj PC mora biti u mogućnosti pristupiti usmjerivaču, ni jedno drugo računalo ne bi trebalo biti u mogućnosti pristupiti upravljanju VLAN-a. Stvori se ACL koji negira bilo kakvu mrežu iz 192.168.20.0/24 mreže, ali omogućuje svim drugim mrežama pristup jedna drugoj.

Postoji više načina na koji ACL može biti stvoren kako bi ostvarili potrebnu sigurnost. Iz tog razloga, ocjenjivanje na ovom dijelu aktivnosti temelji se na ispravnim zahtjevima povezivanja. Upravitelj PC mora imati mogućnost spajanja na svim prekidačima i usmjerivačima. Sva ostala računala ne bi trebala imati mogućnost

spajanja na sve uređaje u sklopu upravljanja VLAN. Posljednji korak je provjera sigurnosti. Upravitelj PC pinga preklopnik SW-A, SW-B i usmjerivač R1. Ping je uspješan jer svi uređaji sa 192.168.20.0 mrežom su u mogućnosti pingati jedni druge. Nakon toga, D1 pinga upravitelja PC-a, a taj ping nije uspješan. Da bi uređaji sa različitim VLAN-on bili uspješno pingani sa uređajima koji imaju VLAN 20, moraju biti usmjerivači. Usmjerivač ima ACL koji sprječava svim paketima da pristupe 192.168.20.0 mreži. Slikom 3. prikazana je vježba koja je odrađena sto posto.



Slika 3. Prikaz vježbe: Ispitivanje sigurnosti uz Layer 2 VLAN Security [3]

3.2. Sigurnost mreža na mrežnom sloju

Tijekom 20. stoljeća tehnologija se razvijala u smjeru prikupljanja, obrade i distribucije informacija. Između ostalog, razvijene su svjetske telefonske mreže, radio i televizija, osobna računala i komunikacijski sateliti. Kao rezultat ubrzanog tehnološkog napretka spomenuta su se područja međusobno približila, a razlike između prikupljanja, prijenosa, pohrane i obrade informacija nestaju.

Vrste napada na mrežnom sloju OSI modela:

- Skeniranje IP adresa
- Lažiranje IP adresa

- ICMP[3] napadi
- Lažiranje poruka usmjerivačkih protokola

3.2.1. Skeniranje IP adresa

Skeniranje IP adresa je vrsta napada čija zadaća je otkriti adresnu shemu napadnute mreže kako bi se znalo gdje se koji klijent nalazi u mreži. (Grupa autora, 2014) Izvršavanje ovog napada postiže se u dva koraka:

1. upit prema DNS[4] poslužitelju - zahtjeva IP adresu poslužitelja na nekoj domeni i
2. na internetskim registrima preko dobivene adrese saznati za dodijeljene javne IP adrese.

3.2.2. Lažiranje IP adresa

IP address spoofing, odnosno lažiranje IP adresa provodi se često u spoju s nekim od DoS[5] napada da se sakrije trag od onoga koji šalje te pakete. Mijenja se izvorišna adresa da bi se prikrio trag nekog napada ili da bi se preskočilo IP filtre.

3.2.3. ICMP napadi

Osim IP protokola koji se koristi za prijenos podataka s jednog računala na drugo, na mrežnom sloju, razvijen je i ICMP (eng. *Internet Control Message Protocol*) protokol za kontrolu toka podataka. Budući da IP protokol nije konekcijski orijentiran i ne omogućuje kontrolu toka, javila se potreba za ICMP protokolom.

ICMP protokol mrežnim administratorima pomaže u otkrivanju i otklanjanju problema u komunikaciji te se često koristi i za otkrivanje mreže.(Grupa autora,2014)

Neki od čestih ICMP napada su: *Ping of Death, ICMP Ping flood attack i ICMP smurf attack.*

[3] ICMP (engl. *Internet Control Message Protocol*): komunikacijski protokol koji je ugrađen u svaki IP modul da bi omogućio mrežnim prolazima(usmjerivačima) ili računalima slanje kontrolnih poruka o greškama.

[4] DNS (eng. *Domain Name System*): distribuirani hijerarhijski sustav Internet poslužitelja u kojem se nalaze informacije povezane s domenskim nazivima, tj. o povezanosti IP adresa i njihovih logičkih (simboličkih) imena.

[5] DoS (eng. Denial of Service) napad: napad na neki računalni servis s ciljem da se korisnicima onemogući njegovo korištenje.

3.2.4. Lažiranje poruka usmjerivačkih protokola

Routing protocols, odnosno usmjerivački protokoli su ključni dijelovi svake mreže jer oni određuju putove kojima će paketi prolaziti kroz mrežu i obavještavaju ostale usmjerivače gdje se koja mreža nalazi.(Grupa autora,2014)

Uz pomoć usmjerivačke obavijesti (eng. *routing update*) koja služi za čitanje ključnih informacija o topologiji i rasporedu mreže, napadač može doći do potrebnih informacija za izvršenje napada.

3.2.5. Ispitivanje sigurnosti na mrežnom sloju

Ispitivanje sigurnosti na mrežnom sloju pomoću IOS *Intrusion Prevention System*.

Zadatak je konfigurirati usmjerivač R1 za IPS (eng. *Intrusion Prevention System)* koji bi skenirao promet unosom 192.168.1.0 mreže. Poslužitelj s oznakom „*Syslog Server* " koristi se za prijavu IPS poruke. U zadatku je trebalo konfigurirati usmjerivač tako da identificira *syslog* poslužitelja kako bi razumio zapisivanje poruka. Prikaz točnog vremena i datuma u *syslog* porukama je bitno kod korištenja *syslog-a* za praćenje mreže. Trebalo je postavite sat i konfigurirati *timestamp* servis za prijavu na usmjerivač, omogućiti IPS-u proizvoditi upozorenja i ispustiti ICMP *echo* odgovore paketa na istoj razini.

Prvi zadatak u ovoj vježbi bio je uključiti IOS IPS. Provjera mrežnog povezivanja je prvi korak. Znači, od PC-C trebalo je pingati PC-A i on je bio uspješan. Nakon toga, trebalo je pingati od PC-A do PC-C koji je isto bio uspješan. U drugom koraku je trebalo napraviti IOS IPS konfiguraciju *directory in flash*. Na usmjerivač R1 stvoriti direktorij pomoću *mkdir* naredbe. Naziv direktorija je ipsdir. Treći korak je bila konfiguracija *IPS signature storage location*. Na usmjerivaču R1 konfigurirana je *IPS signature storage location* pomoću naredbe *ip ips config location flash:isdir*. Na usmjerivaču R1 stvoren je IPS *rule* ime pomoću naredbe *ip ips name* u globalnom konfiguracijom modu. Ime za IPS pravilo je iosips.

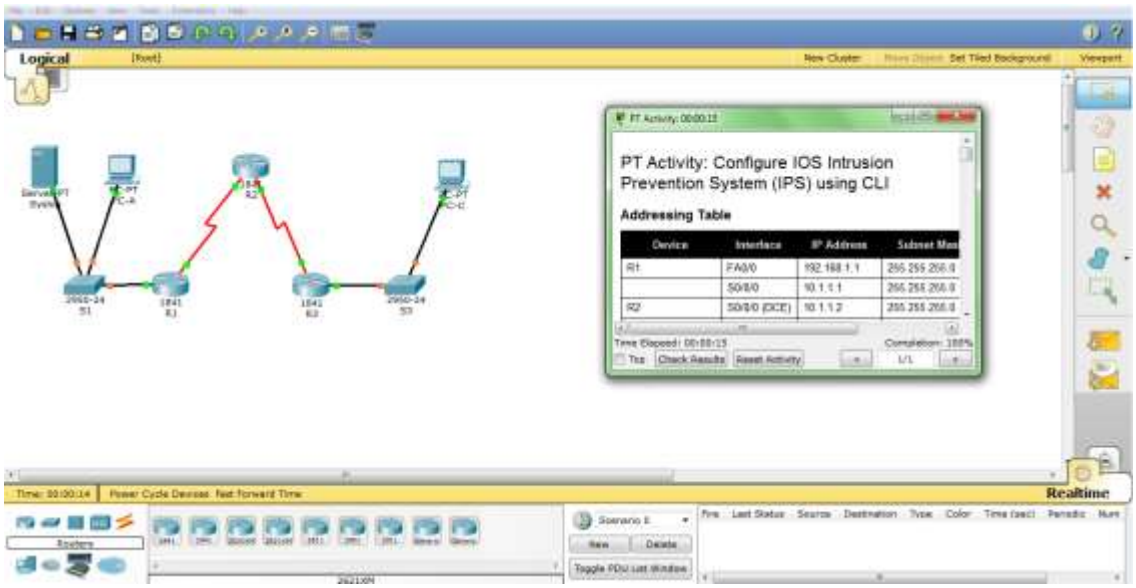
Kod petog koraka trebalo je omogućiti logiranje. IOS IPS podržava upotrebu *syslog* za slanje obavijesti o događajima. *Syslog* obavijest je omogućena po *defaultu*. Ako je omogućena prijavom konzola, mogu se vidjeti IPS *syslog* poruke. Nakon toga trebalo je omogućiti *syslog* ako nije omogućeno.

Koristiti *Clock Set* naredbu iz povlaštenog EXEC načina za resetiranje sata ako je potrebno. Nakon toga trebalo je provjeriti je li *timestamp* servis za prijavu omogućen na usmjerivaču pomoću *show run* naredbe. Nije bio omogućen te ga je trebalo omogućiti. Sa usmjerivača R1 trebalo je poslati log poruke na *Syslog* poslužitelja na IP adresu 192.168.1.50. Kod šestog koraka trebalo je konfigurirati IOS IPS kako bi koristio kategorije potpisa. Zatim je trebalo povući sve *signature* kategorije sa *retired true* naredbom. *Unretire IOS-IPSBasic* kategoriju sa *retired false* naredbom. Postaviti *IPS rule* na sučelje bio je dio koji je odrađen kod sedmog koraka.

Postavljen je *IPS rule* na sučelje sa naredbom *IP IPS name direction* u konfiguracijskom sučelju. Primijenjeno je pravilo izlaza na FA0 / 0 sučelja na usmjerivaču R1. Nakon što je omogućen IPS, neka log poruka bila je poslana na konzolne linije (eng. *console line*) i bilo je prikazano da su IPS *engines* inicijalizirani. Smjer *in* znači da IPS pregledava samo promet koji ide u sučelje. Isto tako, *out* znači samo promet koji izlazi iz sučelja.

Kod drugog zadatka trebalo je izmijeniti potpis. Korištenjem naredbe *ip ips signature-definition*, promijenjen je događaj akcije od potpisa. Nakon toga korišten je *show ip ips all* kako bi se vidio IPS sažetak o stanju konfiguracije. Na sučelje *Fa 0/0* i direktorij *outbound* se primijenio *iosips rule*. Treći korak bio je provjeriti radi li IPS ispravno.

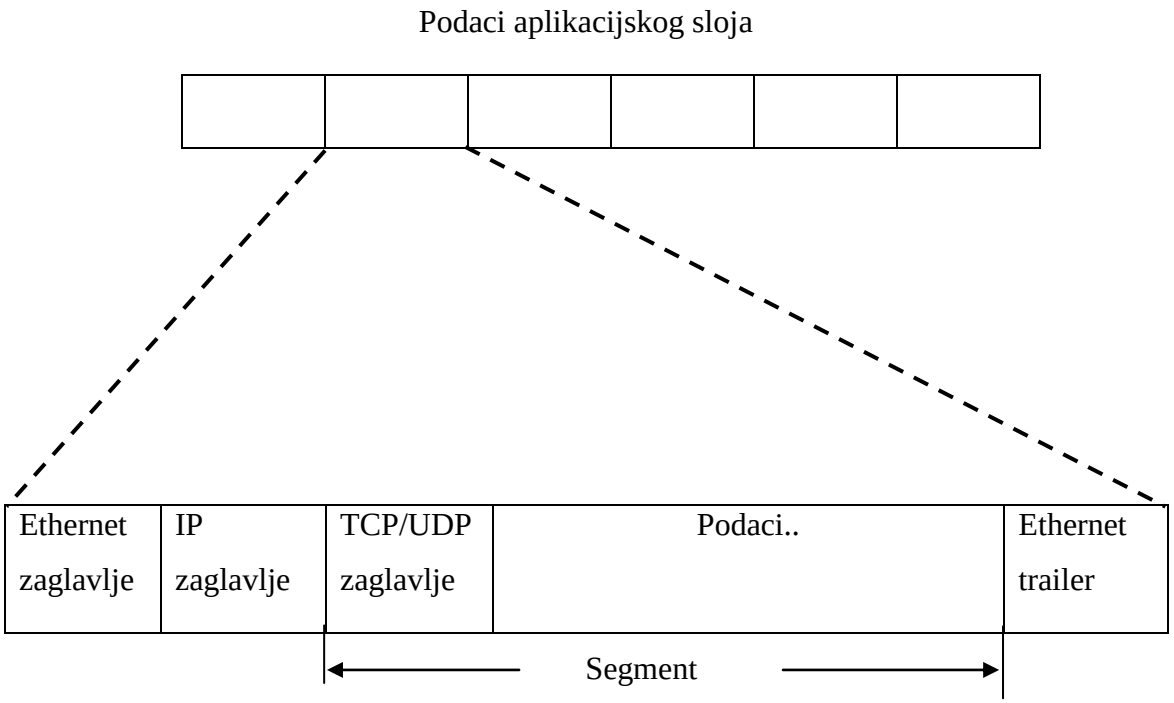
Od PC-C pingan je PC-A. *Ping* nije bio uspješan zato jer je *IPS rule* za *event-action* od *echo* zahtjeva bio poslan na *"deny-packet-inline"*. Zatim je od PC-A pingan PC-C. *Ping* je bilo uspješan zato jer *IPS rule* ne pokriva *echo* odgovor. Kada PC-A pinga PC-C, PC-C odgovara sa *echo* odgovorom. Četvrti korak bio je pogledati *syslog* poruke. Klikom na *Syslog* poslužitelja odabrana je karticu *Config*. U lijevom navigacijskom izborniku odabran je *syslog* za pregled log datoteke. Vježba je odrađena sto posto što je i prikazano slikom broj 4.



Slika 4. Prikaz vježbe: Ispitivanje sigurnosti na mrežnom sloju pomoću IOS Intrusion Prevention System [4]

3.3. Sigurnost mreža na transportnom sloju

Transportni sloj omogućava pouzdan prijenos podataka između krajnjih komunikacijskih točaka u mreži. Primjeri protokola na transportnom sloju su TCP (eng. *Transmission Control Protocol*) i UDP (eng. *User Datagram Protocol*). Nakon kreiranja na aplikacijskim slojevima, podatkovni niz se segmentira i odvoji u zasebne segment te preuzima zaglavlja TCP ili UDP protokola. Kao što je prikazano na slici 5., oba protokola prenose informaciju izvorišnog i odredišnog porta, kojim se povezuju aplikacije na dva računala tako da se portom označi neka aplikacija. TCP protokol prenosi podatke na pouzdan način tako da prati i kontrolira svaki poslani segment, dok UDP šalje podatke bez ikakve kontrole prijenosa podataka.



Slika 4. Prikaz segmenata [5]

Napadi na TCP i UDP protokole su česti. UDP je podložan raznim DoS napadima što kod TCP protokola nije slučaj. Neki od napada na TCP protokol je skeniranje SYN bitom, skeniranje FIN bitom, TCP SYN *flood* napad, TCP *reset* napad i drugi.

Kako UDP protokol nije konekcijski orijentiran, podložan je UDP skeniranju, pa se tako mogu saznati aktivni servisi i aplikacije na nekom računalu.

3.3.1. Ispitivanje sigurnosti na transportnom sloju

Standardni operativni postupak je primjena ACL (eng. *Access Control List*) na rubnim usmjerivačima za ublažavanje zajedničkih prijetnji. U ovoj aktivnosti, stvoren je ACL na rubovima usmjerivača R1 i R3. Zatim je provjerena ACL funkcionalnost od unutarnjih i vanjskih *hostova*.

Prije konfiguracije IP ACL-a trebalo je u ovoj vježbi provjeriti mrežnu vezu. Od PC-C koristeći ikonu *Command Prompt* trebalo je pingati PC-A poslužitelja. Od PC-C trebalo je otvoriti web-preglednik na PC-A poslužitelju (eng. *Server*), korištenjem IP adrese, za prikaz web stranice. Nakon toga, naredbom ping u *Command Prompt-u* od PC-A poslužitelja pingati PC-C.

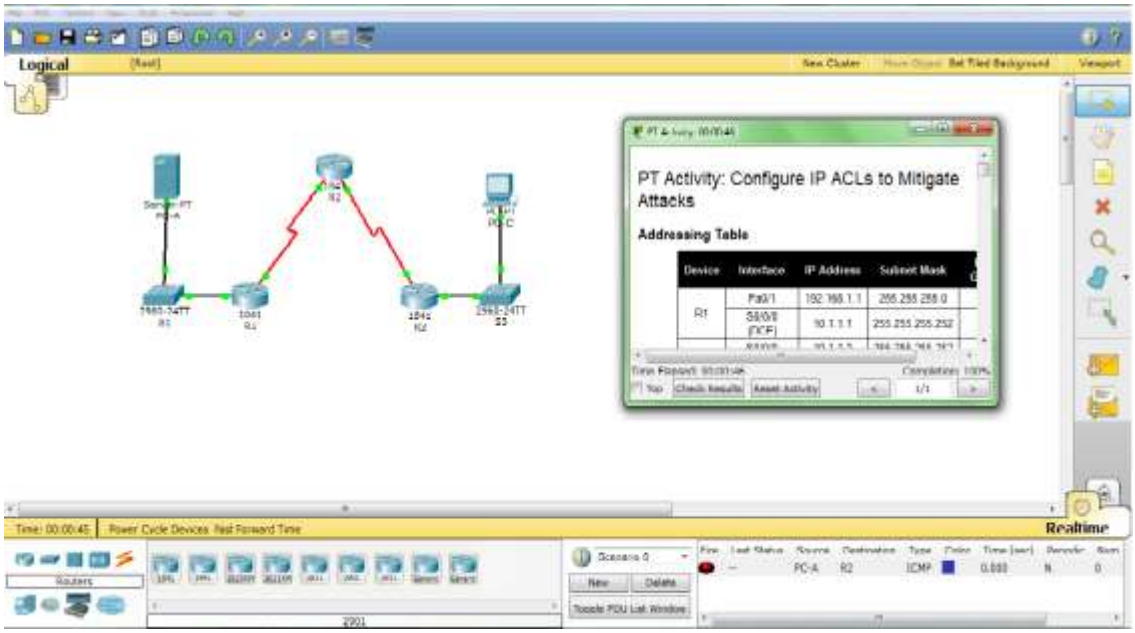
Drugi zadatak bio je osigurati siguran pristup usmjerivačima. Prvi korak kod toga je da se konfigurira ACL 10 koji blokira sav udaljeni pristup na usmjerivače osim od PC-C. Korištena je naredba *access-list* kako bi se kreirao broj IP ACL-a na usmjeriovaču R1, R2 i R3. Korištenjem naredbe *access-class* na usmjerivačima R1, R2 i R3, primijenjen je pristupni popis za dolazni promet na VTY linijama. Nakon toga, provjeren je ekskluzivan pristup od PC-, upravitelja stanice. Na PC-C, korištenjem ikone *Command Prompt*, upisana je naredba *ssh –l SSHadmin 192.168.2.1* te pritiskom na *enter* dobio se rezultat da je SSH uspješan. Taj postupak ponovljen je iz PC-A koji je dao rezultat da SSH nije uspješan.

Treći zadatak u ovoj vježbi bio je stvaranje broja IP ACL 100. Dakle, na usmjerivaču R3 treba blokirati sve pakete koji sadrže izvor IP adrese iz sljedećeg bazena adresa: 127.0.0.0/8 bilo kojeg RFC 1918 privatnih adresa i bilo kojih IP *multicast* adresa. Prvi korak je konfiguracija ACL 100 tako da blokira sav promet primljen od vanjske mreže. Korištena je naredba *access-list* za stvaranje numeriranih IP ACL-a na usmjerivaču R3. Primijenjen je ACL na sučelje *Serial 0/0/1* korištenjem naredbe *ip access-group*. Kod trećeg koraka potvrđeno je da je navedeni ulazni promet sučelja *Serial 0/0/1* pao. Od PC-C u ikoni *Command Prompt* pingan je PC-A poslužitelja. ICMP *echo* odgovori su bili blokirani od strane ACL jer su podrijetlom iz adresnog prostora 192.168.0.0/16. Nakon toga, potrebno je bilo skinuti ACL iz sučelja *Serial 0/0/1* iz razloga jer će inače sav promet od vanjske mreže, koji je upućen s privatnih izvora IP adresa, biti odbijen za ostatak PT aktivnosti. Taj dio odrađen je koristeći naredbu no *ip access-group* za sučelje *Serial 0/0/1*.

Kod četvrtog zadatka trebalo je zabraniti sve izlazne pakete s izvorne adrese koji su izvan raspona internih IP adresa. Prvi korak je bilo konfiguriranje ACL 110 tako da dopusti promet samo od unutarnje mreže. Korištenjem naredbe *access-list* stvoren je numeriran IP ACL. Nakon toga, postavljen je ACL na sučelje *Fa0/1* pomoću naredbe *ip access-group*. Peti zadatak bio je da se dopusti bilo kojem vanjskom *hostu* da pristupi DNS, SMTP i FTP poslužitelju na PC-A, da odbije bilo koji vanjski *host* pristup HTTPS poslužitelja na PC-A i da dozvoli PC-C da pristupi usmjerivaču R1 preko SSH. Kod prvog koraka trebalo se uvjeriti da PC-C može pristupiti PC-A preko HTTPS pomoću web preglednika. Na serveru PC-A onemogućiti HTTP i omogućiti HTTPS. Naredba *access-list* korištena je za stvaranje numeriranih IP ACL na usmjerivaču R1. Nakon toga, potrebno je bilo na sučelje *Serial 0/0/0* nanijeti ACL koristeći se naredbom

ip access-group. PC-C nije mogao pristupiti PC-A preko HTTPS koristeći se web preglednikom.

Izmjena postojećeg ACL-a je bio dio koji je odrađen u šestom zadatku. Dopušteni su ICMP *echo* odgovori i odredišta nedostupnih poruka izvan mreže. PC-A nije mogao uspješno pingati sučelje na usmjerivaču R2. Korištenjem naredbe *access-list* napravljene su potrebne promjene u ACL 120 da se onemogući i uskrati određeni promet. Nakon toga, PC-A je uspješno pingao povratno sučelje na usmjerivaču R2. Vježba ispitivanje sigurnosti na transportnom sloju pomoću ACL-a odrađena je sto posto što je i prikazano slikom pod brojem šest.



Slika 6. Prikaz vježbe: Ispitivanje sigurnosti na transportnom sloju pomoću ACL(eng. Access Control List) [6]

3.4. Sigurnost mreža na aplikacijskom sloju

Posljednji, odnosno najviši sloj mrežnog modela omogućava korisniku pristup mrežnom modelu. Najčešće korišteni protokoli i servisi koji se koriste za upravljanje mrežom su TELNET, TFTP, SNMP, HTTP i drugi.

3.4.1. TELNET

Jedan od prvih protokola razvijen za TCP/IP mreže i namijenjen za upravljanje udaljenim računalima ili uređajima u mreži putem komandne linije.(Grupa autora, 2014)

Telnet prenosi samo tekst koji korisnik upisuje odnosno tekst koji mu se pokazuje na zaslonu. Nedostatak mu je što prenosi u čistom tekstu bez enkripcije pa svatko tko ima pristup tim podacima i presluša tu komunikaciju MITM (eng. *man-in-the-middle*[6]) vidi sve što korisnik upisuje i dobiva na zaslonu. Najbolja zaštita udaljenog pristupa je umjesto Telnet protokola koristiti SSH (eng. *Secure Shell*) protokol koji ima ugrađenu enkripciju podataka.

3.4.2. TFTP

TFTP (eng. *Trivial File Transfer Protocol*) je protokol koji se koristi u mrežama za spremanje konfiguracije i operativnih sustava na jedan centralni datotečni poslužitelj zbog lakšeg upravljanja i održavanje mreže.(Grupa autora, 2014)

3.4.3. SNMP

SNMP (eng. *Simple Network Management Protocol*) je UDP usmjereni mrežni protokol čija je namjena praćenje rada mrežnih uređaja i konfiguracija. SNMP protokol verzije 3 je treća verzija SNMP-a te ga je poželjno koristiti na mreži jer enkripcijom štiti sav SNMP promet na mreži.

Pored svih tih protokola potrebno je spomenuti i HTTP (eng. *HyperText Transfer Protocol*) koji se koristi za udaljenu konfiguraciju mrežnih uređaja pomoću grafičkog sučelja GUI (eng. *Graphical User Interface*).

3.4.4. Ispitivanje sigurnosti na aplikacijskom sloju

Ispitivanje sigurnosti na aplikacijskom sloju odrađen je tako da je konfiguriran usmjerivač kao NTP (eng. *Network Time Protocol*) klijent i da ažurira hadverski sat preko NTP-a. Konfiguriran je usmjerivač tako da prijavi poruku na *syslog* poslužitelja, konfigurirani su lokalni korisnici te VTY linije da prihvate samo SSH konekciju. Na SSH serveru konfiguriran je *RSA key pair*.

Mrežna topologija prikazuje tri usmjerivača, R1, R2, R3. Usmjerivače R1 i R3 konfigurirani su kao NTP klijente i syslog poslužitelje, a na usmjerivač R3 konfiguriran je SSH.

[6]MITM (eng. man-in-the-middle) : napad gdje napadač postavlja svoje računalo u logički put između ostalih dvaju računala koja međusobno komuniciraju.

NTP dozvoljava usmjerivačima na mreži da sinkroniziraju svoje vremenske postavke sa NTP serverom. On može pomoći kod rješavanja problema na mreži i različitih napada na mrežu. Kada je NTP implementiran na mrežu, on može biti postavljen tako da sinkronizira privatni glavni sat ili na javni slobodan NTP server na internetu.

U ovoj vježbi konfiguriran je usmjerivač tako da dopusti softver satu da bude sinkroniziran od NTP-a te je konfiguriran usmjerivač tako da periodično ažurira hardverski sat.

Syslog poslužitelj će pružiti poruke prijavom u ovom laboratoriju. Konfiguriran je usmjerivač za identifikaciju udaljenog računala koji će primati *logging* poruke. Konfigurirane su *timestamp* usluge za logiranje na usmjerivače. Prikazivanje točnog vremena i datuma u *syslog* poruci je vitalan kada se koristi *syslog* da prati mrežu. Ako je nepoznato točno vrijeme i datum poruke biti će teško odrediti koji su mrežni događaji izazvali poruke.

Usmjerivač R2 je ISP povezan sa dvije udaljene mreže: usmjerivačem R1 i usmjerivačem R3. Lokalni administrator može na usmjerivaču R3 izvoditi najviše usmjerivačkih konfiguracija i može rješavati njegove probleme. Usmjerivač R3 je upravitelj i ISP treba pristup od njega kako bi povremeno rješavao probleme i ažurirao. Kako bi pružao taj pristup na siguran način, administrator se mora dogovoriti da koristi SSH (eng. *Secure Shell*).

Pomoću CLI konfiguriran je usmjerivač kako bi uspio sigurno koristiti SSH umjesto Telnet-a. SSH je mrežni protokol koji uspostavlja sigurnosni terminal veza na usmjerivače ili druge mrežne uređaje. SSH šifrira sve informacije koje prolaze mrežnom vezom i pružaju autentifikaciju udaljenom uređaju (eng.*Computer*).

Prvi zadatak je bila konfiguracija usmjerivača kao NTP klijenta. Kao uvod u taj dio zadatka trebalo je testirati povezanost između PC-C i usmjerivača R3 koja se pokazala uspješnom. Isto tako, trebalo je testirati povezanost između usmjerivača R2 i R3 što na kraju rezultira uspješnim povezivanjem. Drugi korak je konfiguracija usmjerivača R1, R2 i R3 kao NTP klijenta. Pomoću *ISO Command Line Interface* na svaki usmjerivač doda se NTP server ip adrese 192.168.1.5. Zatim se pomoću naredbe *show ntp* status provjeri konfiguracija klijenta.

Nakon konfiguracije NTP klijenta potrebno je, u trećem koraku, konfigurirati usmjerivače R1, R2 i R3 kako bi povremeno ažurirali hardverski sat. To se radi pomoću

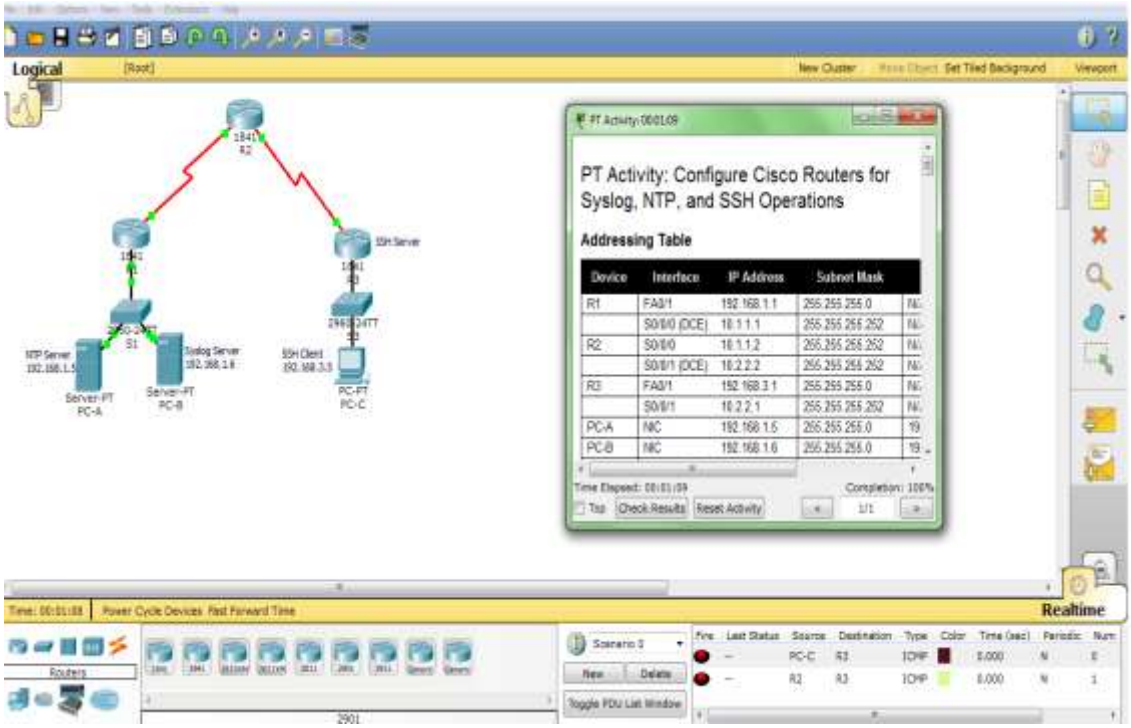
ISO Command Line Interface tako da se upisuje u svaki usmjerivač naredba *ntp update-calendar*. Nakon toga provjeri se pomoću naredbe *show clock* da li je ažurirani hadverski sat. Kod četvrtog koraka potrebno je konfigurirati usmjerivače za timestamp log poruke. Preko CLI u svaki usmjerivač upisuje se naredba *service timestamps log datetime msec.*

Drugi zadatak se odnosi na konfiguraciju usmjerivača za log poruke na *Syslog* poslužitelja (eng. *Syslog server*). Prvi korak temelji se na konfiguraciji usmjerivača za identifikaciju udaljenog računala (Syslog poslužitelja) koji će primati log poruke. Kod svakog usmjerivača u CLI upisuje se naredba *logging host* uz ip adresu *syslog* servera, koja je u ovom primjeru 192.168.1.6. Nakon toga provjerava se konfiguracija prijave pomoću naredbe *show loggin*g. Kod trećeg koraka ispituje se *logs* od *Syslog* poslužitelja. Na kartici *Config* od syslog dijaloškog okvira, odabire se *Syslog services* gumb. Nakon toga promatraju se logging poruke primljene od usmjerivača. Log poruke mogu biti generirane na poslužitelja obavljanjem naredbi na usmjerivaču. Na primjer, ulazom i izlazom globalni konfiguracijski oblik rada će generirati informativne konfiguracijske poruke.

Konfiguracija usmjerivača R3 za podršku SSH veze je dio koji se obavlja u trećem zadatku. Kod prvog koraka, na usmjerivač R3, konfigurira se ime domene ccnasecurity.com. To se obavlja pomoću CLI tako da se koristi naredba *ip domain-name* te kraj toga upiše naziv domene. Drugi korak je konfiguracija korisnika za prijavu SSH klijenta na usmjerivač R3. Kreira se korisnički ID *SSHadmin* sa najvišom razinom mogućih povlastica i tajnom lozinkom *ciscosshpa55*. Korisnički ID i lozinka zajedno se upisuju u usmjerivač R3 pomoću naredbe *username SSHadmin privilege 15 secret ciscosshpa55*. Korištenjem lokalnog korisničkog računa za obveznu prijavu i provjeru, uspješno je obavljen i treći korak. Kod njega je trebalo konfigurirati dolazni *VTY lines* na usmjerivač R3. Upisom naredbe *transport input ssh* u CLI treba prihvatiti samo SSH vezu. Brisanje postojećih RSA ključa na usmjerivačima odrađuje se pomoću CLI naredbe *crypto key zeroize rsa*. Ako nekim slučajem ključevi ne postoje prikazat će se poruka: `% No Signature RSA Keys found in configuration.`

Usmjerivač koristi RSA ključ za autentifikaciju i šifriranje prenosivih SSH podataka. Konfiguriraju se RSA ključevi sa koeficijentom od 1024. Pritiskom tipke *Enter* prilikom upisa naredbe *crypto key generate rsa* u CLI dobije se ime od ključa koje je R3.ccnsecurity.com te je potrebno odabrati veličinu ključa modula u rasponu od 360 do

2048 bitova. Generiranjem 1024 bitni RSA ključ, ključ neće biti izvozni. Kod koraka pod brojem šest potrebno je provjeriti SSH konfiguraciju. Koristeći naredbu *show ip ssh* vidljive su bile trenutne postavke. Kod sedmog koraka potrebno je konfigurirati SSH *timeout* (stanku) i parametre autentičnosti. Zadani SSH *timeout* i parametri autentičnosti mogu se mijenjati. Sa naredbom *ip ssh time-out 90* postavlja sa stanka na 90 sekundi. Korištenjem naredbe *ip ssh authentication-retries* 2 na usmjerivaču R3 postavlja se broj pokušaja provjere autentičnosti na dva, a pomoću naredbe *ip ssh version 2* postavlja se SSH verzija za dva. Izdavanjem *show ip ssh* naredbe ponovno se potvrđuje da su promijenjene vrijednosti. Preko *Telneta* spaja se R3 sa PC-C. Otvaranjem ikone *Desktop* na PC-C odabire se ikona *Command Prompt*. U ikonu *Command Prompt* upisuje se naredba *telnet 192.168.3.1* pomoću koje se preko *telneta* povezuje PC-C sa usmjerivačem R3. Ova veza nije uspjela jer je usmjerivač R3 konfiguriran da prihvati samo SSH veze. U sljedećem koraku spaja se na usmjerivač R3 koristeći SSH na PC-C. Otvaranjem ikone *Desktop* na PC-c odabrana je ikona *Command Prompt* u koju se upisuje naredba *ssh –l SSHadmin 192.168.3.1* i povezuje se na usmjerivač R3. Nakon toga unosi se lozinka *ciscosshpa55*. Posljednji korak u ovoj vježbi odnosi se na povezivanje s usmjerivača R3 pomoću SSH na usmjerivač R2. Od CLI usmjerivača R2 unosi se naredba *ssh -v 2 L SSHadmin 10.2.2.1* uz pomoć koje se povezuje na usmjerivač R3 preko SSH verzija 2 koristeći *SSHadmin* korisnički račun. Upisom lozinke konfigurirane za administratora - *ciscosshpa55*- uspješno se povezuje na usmjerivač R2. Vježba u kojoj je trebalo konfigurirati Syslog, NTP i SSH odrađena je sto posto što je vidljivo slikom pod brojem sedam.



Slika 7. Prikaz vježbe: Ispitivanje sigurnosti na aplikacijskom sloju konfiguracijom Syslog, NTP i SSH. [7]

4. Sigurnosni mehanizmi koji se implementiraju na različitim slojevima OSI i TCP/IP modela

Najniži sloj OSI ili TCP/IP modela je fizički sloj, a njegova sigurnost uključuje projektiranje sigurnosti ustanove, postavljanje uređaja za kontrolu pristupa, alarma i kamera.

Podešavanje sigurnosnih mehanizma na uređajima i zaključavanje portova na preklopnicima (eng. *switch*) su najvažniji mehanizmi zaštite sloja podatkovne veze.

Sa prvog stajališta podrazumijeva se pravilno konfiguriranje portova za određenu vrstu filtriranja.

Zaštita od potencijalnog napada s kojim napadač ima mogućnost pretvoriti običan korisnički preklopnik (eng. *switch*) u *root switch* te bi mu se time pružila mogućnost manipulacije nad svim podacima koji kroz njega prolaze je *root guard*. On se

omogućava na *root switch*-u i vrši isključivanje porta na *switch*-u na koji dođe zahtjev za postavljanjem novog *switch*-a kao *root*-a.

Sljedeća potencijalna prijetnja je potencijalni lažni DHCP server. Mehanizam zaštite obuhvaća zaštitu porta na taj način da se omogući odgovaranje samo na DHCP zahtjeve preko odgovarajućeg porta na kome bi trebalo i da se nalazi odgovarajući DHCP server.

Pored navedenih akcija koje se izvršavaju u cilju povećanja nivoa zaštite, postoji još jedan mehanizam, a to je grupiranje svih aktivnih portova na jedan SPAN (eng. *Switched Port ANalyzer*) port i prosljeđivanje prikupljenih paketa na IPS ili IDS uređaj, koji će onda vršiti analizu kompletnog saobraćaja koji je primio sa danog uređaja i nakon toga će donijeti odluku o potencijalnim akcijama ili o obavještavanju korisnika o prijetnjama.

Kako bi se, kod mrežnog sloja, zaštitilo skeniranje IP adresa potrebno je postaviti IP filtre koji klijentima brane pristup u neovlaštene dijelove mreže te implementiraju IPS (eng. *Intrusion Preventions System*) sustav koji će na vrijeme zaustaviti svaki pokušaj skeniranja mreže.

Kako bismo spriječili lažiranje izvorišnih IP adresa, potrebno je na svakom usmjerivaču (eng. *router*) postaviti IP filtar koji će filtrirati i odbaciti sve pakete s mreže koji nemaju izvorišnu IP adresu iz te mreže.

Kako bi se spriječilo ubacivanje klijentskog računala između usmjerivača te samim time i napad na komunikacijsku infrastrukturu, usmjerivački protokoli zaštićuju se autentifikacijom. Uz autentifikaciju zaštita od takvih napada postiže se i postavljanjem svih mreža u kojima se nalaze klijenti kao pasivne za usmjerivačke protokole da usmjerivači ne bi slali usmjerivačke poruke na te mreže.

Na transportnom sloju, za zaštitu od skeniranja portova, potrebno je imati IPS *(Instrusion Prevention System*) i instalirati dobre vatrozidove, kako na mreži, tako i na računalima.

Kod zaštite aplikacijskog sloja koriste se različiti protokoli i metode. SSH protokol se koristi za zaštitu aplikacijskog sloja, a ima ugrađenu enkripciju podataka.

Za zaštitu TFTP poslužitelja moraju se koristiti proširene pristupne kontrolne liste (eng. *Extended ACL*) u cijeloj mreži.

Kako bi se spriječilo lažiranje SNMP paketa, potrebno je spriječiti i lažiranje izvorišnih IP adresa koristeći IP filtre.

5. Najčešće korištene i najbolje zaštite korisnika na mreže

Načini poboljšanja zaštite računala od potencijalnih sigurnosnih rizika:

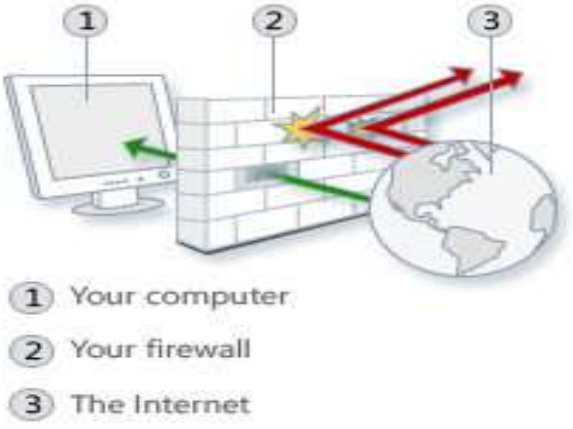
- Vatrozidi(eng.Firewall)
- zaštita od virusa
- Zaštita od špijunskog i drugog zlonamjernog softvera
- Windows ažuriranje (eng. Windows Update)

5.1. Vatrozid

Vatrozid je softver ili komad hardvera koji može pridonijeti zaštititi računala tako da onemoguće pristup hakerima, virusima i crvima koji pokušavaju doći do računala preko Interneta. To je sustav sigurnosti mreže koji kontrolira dolazni i odlazni mrežni promet i temelji se na skupu pravila.

Vatrozid koristiti 3 vrste mehanizama filtriranja:

- filtriranje paketa
- proxy
- inspekcija



Slika 8. Prikaz vatrozida[8]

5.1.1. Najbolji vatrozidi 2015.godine

1. *Barracuda Firewall* – pruža sve nove generacije kontrolne aplikacije i korisnikov identititet funkcije kao jednostavan za korištenje i povoljno je rješenje.
2. *ZoneAlarm Free Firewall 2015* – prvi osobni vatrozid koji je instalirani, novije izdanje 2015 nudi iste moćne značajke kao i uvijek, uz poboljšanja u nekim područjima.
3. *Comodo Firewall* –ima malo drugačiji pristup od ZoneAlarm u tome što se zaista osjeća kada Comodo pokušava preuzeti računalo - na dobar način naravno - i to je iznenađujuće koliko dobrih obilježja ima kao besplatni program.
4. *PeerBlock* – Peer Block je najbolji program za blokiranje određene IP adrese
5. *Privatefirewall* – je veličine minuskula koja obavlja posao na istoj razini kao i ostali vatrozidi na ovom popisu. To je samo običan i jednostavan vatrozid s glavnim izbornikom koji pokazuje status vatrozida (tj. je li uključen ili isključen), izbor različitih profila, ovisno o lokaciji, te popis mjesta da vjeruje ili blokira.
6. *Anti NetCut 3* – pokušava zaštititi programe prilikom pristupa internetskoj vezi tako da zaštiti mrežni adapter koji je spojen na računalo.

5.2. Zaštita od virusa

Protuvirusni softver može pomoći zaštititi računalo od virusa, crva i drugih sigurnosnih prijetnji.

5.3. Zaštita od špijunskog i drugog zlonamjernog softvera

Softver za zaštitu od špijunskih programa može pridonijeti zaštititi računala od špijunskog softvera i drugog potencijalno neželjenog softvera.

5.4. Windows ažuriranje (Windows Update)

Windows Update je Microsoft usluga koja se koristi za pružanje ažuriranja poput servisnih paketa i zakrpe za Windows operacijskih sustava i drugog softvera tvrtke Microsoft.

Windows može rutinski provjeravati postoje li ažuriranja namijenjena računalu i automatski ih instalirati. Windows Update može se koristiti za ažuriranje upravljačkih programa za popularne hardverske uređaje. Ažuriranja često uključuju poboljšanja značajki i sigurnosna ažuriranja za zaštitu od zlonamjernih programa i Windows zlonamjernih napada.

6. Zaključak

Sigurnost je vrlo složeno područje koje se još uvijek mnogo istražuje. Važno je razumjeti da kod pitanja sigurnosti, korisnik ne može jednostavno reći: „Koji je najbolji vatrozid?“. Sigurnost ne čini samo jedna stvar, već čitavo mnoštvo elemenata.

Razvojem i širenjem računalnih mreža te pojeftinjenjem opreme i njenim širenjem u sve pore društva, počeli su i sigurnosni problemi. Domena koja je do tada bila rezervirana za uski krug znanstvenika, tehnologa, tehničara i privilegiranih korisnika, u kratkom vremenu se otvorila za široke mase koje su u nju donijele i svoje oblike ponašanja. Stoga je bilo potrebno i razviti mrežnu sigurnost. Sigurnost računalnih mreža je složena tema kojom se, opet tradicionalno, bavio uzak krug specijaliziranih stručnjaka. Međutim, kako se sve više ljudi umrežuje, raste i broj ljudi koji moraju razumjeti osnove mrežne sigurnosti.

7. Literatura

1. A.S. Tanenbaum, D.J. Wetherall(2012): Računarske mreže. Beograd, Mikro knjiga, str. 48.
2. CARNet – Sigurnosni model mreže računala. http://www.cert.hr/sites/default/files/CCERT-PUBDOC-2008-01-253.pdf (svibanj 2015).
3. CISCO – Networking Academy.CCNA Security.
4. Grupa autora(2014): Sigurnost računalnih mreža. Zagreb, Algebra d.o.o.,str. 19-27.
5. http://en.wikipedia.org/wiki/Internet_protocol_suite (svibanj 2015).
6. Jukić, O., Heđi, I.(2012): Računalne mreže. Autorizirana predavanja i zbirka odabranih primjera, Visoka škola za menadžment u turizmu i informatici, Virovitica, str. 1–312.
7. Rengel, S., Safundžić, A., Safundžić, M., Jovanović, S.(2008): Računalne mreže – općenito, vrste (LAN, WAN, Internet, intranet, ekstranet). Informatika i informatičke tehnologije, Ekonomski fakultet u Osijeku, str. 1–13.
8. MICROSOFT – Firewall: https://www.microsoft.com/security/pc-security/firewalls-whatis.aspx (svibanj 2015).
9. WINDOWS – Update: http://pcsupport.about.com/od/keepingupwithupdates/p/windows-update.htm (svibanj 2015).

8. Reference

[1]Slika 1. Usporedba TCP/IP slojeva sa OSI-RM modelom-

https://www.google.hr/search?q=osi+referentni+model&espv=2&biw=1366&bih=667&source=lnms&tbm=isch&sa=X&ei=r7HdVJHpDsT8UqingogE&ved=0CAYQ_AUoAQ#imgdii=_&imgrc=3z1XklMmUG2K5M%253A%3BMH0xXdeQznIZwM%3Bhttp%253A%252F%252Fimage.slidesharecdn.com%252Fosireferentnimodel-090919065310-phpapp01%252F95%252Fosi-referentni-model-4-728.jpg%253Fcb%253D1253361255%3Bhttp%253A%252F%252Fwww.slideshare.net%252Fnik0la%252Fosi-referentni-model%3B728%3B546 (svibanj 2015).

[2] Slika 2. Vježba Layer 2 Security. – osobna arhiva

[3] Slika 3. Prikaz vježbe: Ispitivanje sigurnosti uz Layer 2 VLAN Security –osobna arhiva

[4] Slika 4. Prikaz vježbe: Ispitivanje sigurnosti na mrežnom sloju pomoću IOS Intrusion Prevention System –osobna arhiva

[5] Slika 5. Prikaz segmenata-osobna arhiva

[6] Slika 6. Prikaz vježbe: Ispitivanje sigurnosti na transportnom sloju pomoću ACL(eng. Access Control List) –osobna arhiva

[7] Slika 7. Prikaz vježbe: Ispitivanje sigurnosti na aplikacijskom sloju konfiguracijom Syslog, NTP i SSH. –osobna arhiva

[8] Slika 8. Prikaz vatrozida - Grupa autora(2014): Sigurnost računalnih mreža. Zagreb, Algebra d.o.o., str. 22.