Centar Informacijske Sigurnosti

Zaštita od prisluškivanja mrežnog prometa

listopad
2011.

CIS-DOC-2011-10-029

Upozorenje

Podaci, informacije, tvrdnje i stavovi navedeni u ovom dokumentu nastali su dobrom namjerom i dobrom voljom te profesionalnim radom CIS-ovih stručnjaka, a temelje se na njihovom znanju i petnaestak godina iskustva u radu u informacijskoj sigurnosti. Namjera je da budu točni, precizni, aktualni, potpuni i nepristrani.

Ipak, oni su dani samo kao izvor informacija i CIS ne snosi nikakvu izravnu ili posrednu odgovornost za bilo kakve posljedice nastale korištenjem podataka iz ovog dokumenta.

Ukoliko primijetite bilo kakve netočnosti, krive podatke ili pogreške u ovom dokumentu, ili imate potrebu komentirati sadržaj molimo Vas da to javite elektroničkom poštom na adresu info@CIS.hr.

O CIS-u

CIS izrađuje pregledne dokumente (eng. white paper) na teme iz područja informacijske sigurnosti koji će biti korisni zainteresiranoj javnosti, a u svrhu **podizanje njezine svijesti o informacijskoj sigurnosti** i **sposobnosti za čuvanje i zaštitu informacija i informacijskih sustava**. Pored toga, CIS razvija i održava mrežni portal www.CIS.hr kao referalnu točku za informacijsku sigurnost za cjelokupnu javnost; izrađuje obrazovne materijale namijenjene javnosti; organizira događaje za podizanje svijesti o informacijskoj sigurnosti u javnosti i pojedinim skupinama te djeluje u suradnji sa svim medijima.

CIS **okuplja mlade** zainteresirane za informacijsku sigurnost i radi na njihovom pravilnom odgoju i obrazovanju u području informacijske sigurnosti te pripremu za **profesionalno bavljenje informacijskom sigurnošću**.

Centar informacijske sigurnosti [CIS] nastao je 2010. godine na poticaj Laboratorija za sustave i signale[LSS] Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu, a kao posljedica 15togodišnjeg rada na istraživanju, razvoju i primjeni informacijske sigurnosti. LSS je među ostalim potaknuo osnivanje CARNetovog CERTa i sudjelovao u izradi Nacionalnog programa informacijske sigurnosti RH.

Smisao CISa je da bude **referentno mjesto za informacijsku sigurnost** za javnost, informatičare i posebno za mlade te da sustavno podiže njihovu svijest i sposobnosti u području informacijske sigurnosti.

Rad CISa podržava Ministarstvo znanosti, obrazovanja i sporta Republike Hrvatske, a omogućuju sponzori.

Prava korištenja

Sadržaj

1. Uvod

Prisluškivanje mrežnog prometa je vrlo slično prisluškivanju telefonskog razgovora: dvije strane komuniciraju, a treća strana prisluškuje njihovu komunikaciju. Kod prisluškivanja mrežnog prometa, treća strana presreće podatkovne pakete i čita njihov sadržaj. Kod lokalnih mreža je prisluškivanje vrlo jednostavno zbog činjenice da se koristi dijeljeni medij, tj. računalo može primiti podatke koji su namijenjeni drugim računalima.

Prisluškivanje mrežnog prometa u lokalnoj mreži je zapravo vrlo česta pojava. Većina administratora koristi prisluškivanje kako bi nadgledali rad mreže za koju su odgovorni. Ako prisluškuju mrežni promet, mogu uočiti probleme poput loše konfiguracije nekog mrežnog elementa te tako spriječiti neželjene posljedice.

Ipak, prisluškivanje mrežnog prometa se može koristiti i u druge, zlonamjerne svrhe. Ukoliko napadač ima pristup komunikacijskom kanalu, presretanjem i čitanjem paketa moguće je otkrivanje osjetljivih informacija. Dobivene informacije napadač može iskoristiti za neke kasnije napade (primjerice, napadač prisluškivanjem otkrije korisničku lozinku, a kasnije lozinku iskoristi za neovlašteni pristup sustavu). Zbog toga je potrebno zaštiti lokalnu mrežu od neželjenog prisluškivanja.

Prisluškivanje mrežnog prometa nije ograničeno samo na lokalnu mrežu. Napadač može prisluškivati mrežni promet i izvan lokalne mreže, ukoliko sudionike komunikacije na neki način prevari da sve pakete preusmjeravaju prema njemu. Jedan način je da se korisniku A predstavi kao korisnik B i obrnuto. Zbog toga će korisnik A slati podatke napadaču misleći da šalje svom sugovorniku (i obrnuto). Napadač čita podatke, a zatim ih šalje pravom primatelju kako sudionici razgovora ne bi posumnjali u njegovu prisutnost.

U ovom dokumentu će biti objašnjeni napadi prisluškivanjem mrežnog prometa koji iskorištavaju propuste u protokolima ARP (eng. *Address Resolution Protocol*) i DNS (eng. *Domain Name System*). Budući da je najbolji način zaštite poznavanje ranjivosti protokola i načina na koji se te ranjivosti iskorištavaju, u prva dva poglavlja će biti objašnjen način rada protokola ARP i DNS te metode koje napadači okoriste pri svojim napadima. Ranjivosti ARP-a i DNS-a rezultiraju prisluškivanjem prometa, ali, kao što će biti pokazano, mogu imati i druge posljedice poput lažiranja podataka ili izvođenja DoS (eng. *Denial of Service*) napada. U zadnjem poglavlju su navedene metode zaštite od prisluškivanja mrežnog prometa koje ujedno štite i do ostalih oblika napada (npr. lažiranje podataka, DoS, itd.)

2. Ranjivi mrežni protokoli

Kao što je rečeno u uvodu, prisluškivanje mrežnog prometa je takav oblik napada kod kojeg napadač presreće podatkovne pakete koje dva računala izmjenjuju te čita njihov sadržaj.

Ovaj oblik napada je u lokalnoj mreži moguće izvesti koristeći propuste u protokolu ARP. Način rada protokola ARP biti će objašnjen u poglavlju 2.1.

Kako bi izveo napad iskorištavanjem protokola ARP, napadač mora imati pristup lokalnoj mreži. Udaljeni napadač može izvesti napad prisluškivanjem mrežnog prometa i iskorištavajući ranjivosti u sustavu domenskih imena ili DNS-u. Način rada DNS-a je objašnjen u poglavlju 2.2.

Prije objašnjena ARP i DNS protokola objasnit će se OSI (eng. *Open Systems Interconnection*) model kako bi se olakšalo razumijevanje rada ARP i DNS protokola. OSI model je predložen kako bi se standardizirali telekomunikacijski protokoli. Model je podijeljen u sedam slojeva (slika 1.), a svaki sloj ima određenu zadaću. Svaki sloj može komunicirati sa susjednim slojem preko unaprijed definiranih sučelja. Najviši je aplikacijski sloj koji predočuje aplikacije i usluge za korisnike, a najniži je fizički sloj kojim se obavlja prijenos informacija fizičkim medijem.

7	Aplikacijski sloj
6	Prezentacijski sloj
5	Sjednički sloj
4	Transportni sloj
3	Mrežni sloj
2	Sloj podatkovne poveznice
1	Fizički sloj

Slika 1. OSI model

Zadaci pojedinih slojeva su:

1. Fizički sloj: prijenos bitova podataka fizičkim medijem, npr. žica, optičko vlakno
2. Sloj podatkovne poveznice: fizičko adresiranje
3. Mrežni sloj: usmjeravanje paketa
4. Transportni sloj: povezivanje s kraja na kraj
5. Sjednički sloj: usklađivanje sustava koji komuniciraju
6. Prezentacijski sloj: prikaz informacija koje se šalju
7. Aplikacijski sloj: računalni procesi koje korisnik vidi.

Kada se govori o komunikaciji preko Interneta, sjednički, prezentacijski i aplikacijski sloj se najčešće objedinjuju u jedan, aplikacijski, sloj (osjenčani zeleno na slici 1).

2.1. ARP

ARP je komunikacijski protokol koji djeluje između mrežnog sloja i sloja podatkovne poveznice u OSI modelu. Koristi se za pretvorbu adresa iz mrežnog sloja u adrese sloja podatkovne poveznice i obrnuto.

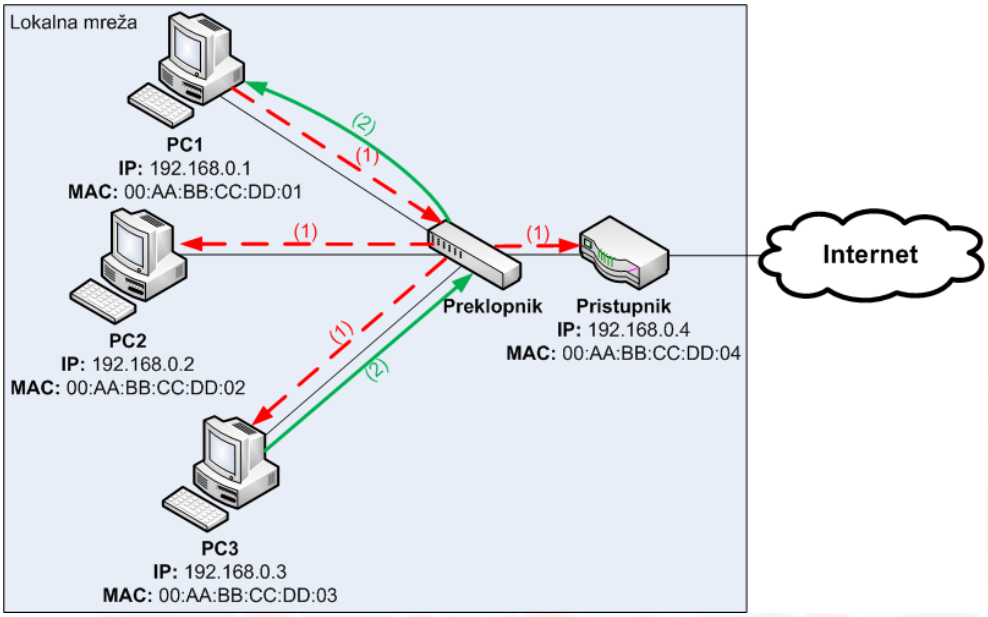
Najčešće se radi o pretvorbi IP (eng. *Internet Protocol*) adresa s mrežnog sloja u MAC (eng. *Media Access Control*) adrese na sloju podatkovne poveznice. IP adrese se koriste za usmjeravanje paketa u mreži, ali kako bi se paketi dostavili do odredišnog računala potrebno je

poznavati i njegovu MAC[1] adresu. ARP omogućuje dinamičko povezivanje IP adresa s odgovarajućim MAC adresama (i obrnuto) u jednoj lokalnoj mreži.

ARP je vrlo jednostavan protokol koji se sastoji od četiri vrste poruka:

1. ARP zahtjev,
2. ARP odgovor,
3. Obrnuti ARP zahtjev ili RARP (eng. *Reverse ARP Request*) te
4. RARP odgovor.

Rad protokola ARP će biti objašnjen na primjeru. Slika 2. prikazuje malu lokalnu mrežu koja se sastoji od tri računala (PC1, PC2 i PC3), jednog preklopnika (eng. *switch*) i jednog pristupnika (eng. *gateway*) koji povezuje lokalnu mrežu s Internetom.



Slika 2. Primjer rada protokola ARP

Primjerice, neka računalo PC1 želi poslati paket računalu PC3. Računalo PC1 zna IP adresu računala PC3 (192.168.0.3), ali ne i njegovu MAC adresu (00:AA:BB:CC:DD:03). Kako bi ju saznao, koristi se ARP protokol. Pri tome se koriste dvije ARP poruke:

1. ARP zahtjev (šalje PC1): „Tko ima IP adresu 192.168.0.3?“
2. ARP odgovor (šalje PC3): „Ja imam IP adresu 192.168.0.3. Moja MAC adresa je 00:AA:BB:CC:DD:03“

Dakle, na početku računalo PC1 šalje ARP zahtjev. Budući da ne zna kome poslati zahtjev, PC1 ga šalje svim računalima u lokalnoj mreži (na slici 2. je ARP zahtjev označen s crvenim strelicama). Nakon što sračunalo PC3 primi ARP zahtjev od računala PC1 i prepozna da se u zahtjevu spominje njegova IP adresa, ono šalje ARP odgovor. Budući da PC3 zna kome mora poslati odgovor, on se više ne šalje sveodredišnim razašiljanjem (eng. *broadcast*), nego izravno do računala PC1 (na slici 2. je ARP odgovor označen sa zelenim strelicama).

Druge dvije ARP poruke se koriste za otkrivanje IP adrese na temelju poznate MAC adrese, a princip rada je isti kao u prethodnom primjeru.

Budući da se pri radu protokola ARP često koristi sveodredišno razašiljanje koje zagušuje mrežu, uvedene su ARP tablice koje privremeno spremaju parove IP i MAC adresa, a svako računalo se brine o podacima u svojoj ARP tablici. Time se smanjuje broj ARP poruka koje se razmjenjuju jer se potrebne informacije nalaze u ARP tablici. Parovi adresa u ARP tablici imaju određeno vrijeme života. Nedostatak je što se ARP tablice mogu iskoristiti za izvođenje napada prisluškivanjem mrežnog prometa kao što će biti objašnjeno u poglavlju 3.1.

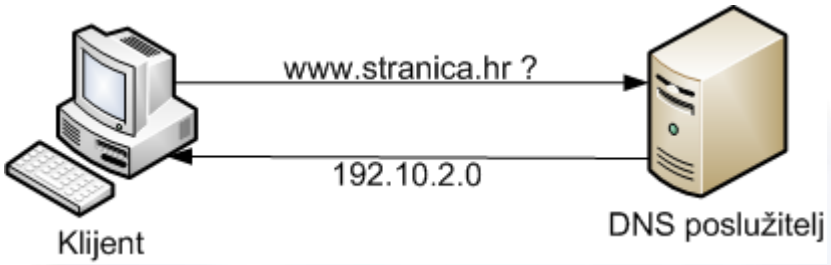
[1] MAC adresa je jedinstveni identifikator mrežnog sučelja nekog uređaja koji se ne može mijenjati budući da je tvornički ugrađen u uređaj pri njegovoj proizvodnji.

Važno je uočiti da protokol ARP djeluje samo u jednoj lokalnoj mreži[2]. Zbog toga je napad koji iskorištava ranjivosti u protokolu ARP ograničen samo na lokalnu mrežu.

2.2. DNS

Protokol ARP se koristi za uparivanje MAC i IP adresa kako bi se adrese mrežnog sloja (IP adrese) preslikale u adrese sloja podatkovne poveznice (MAC adrese) i obrnuto. Slično, DNS se također koristi za uparivanje adresa s različitih slojeva OSI modela, ali DNS djeluje na višim slojevima. Točnije, DNS uparuje domenska[3] imena s pripadajućim IP adresama.

Slika 3. prikazuje pojednostavljenu upotrebu DNS-a. Neka klijentsko računalo želi pristupiti *web* stranici čija je URL (eng. *Uniform Resource Locator*) adresa oblika *www.stranica.hr*. Računalo ne može pristupiti željenoj stranici, dok ne sazna njenu IP adresu. Pomoću DNS upita na DNS poslužitelj, računalo saznaje traženu IP adresu poslužitelja na kojem je stranica *www.stranica.hr*. Tek tada računalo može početi slati pakete prema poslužitelju na dobivenoj IP adresi.



Slika 3. Pojednostavljeno korištenje DNS-a

DNS se često uspoređuje s telefonskim imenikom jer uparuje domenska imena (koja su ljudima lako pamtljiva) s nizom brojeva IP adrese (koja su razumljiva računalima) što je jako slično traženju telefonskog broja prema nečijem imenu i prezimenu.

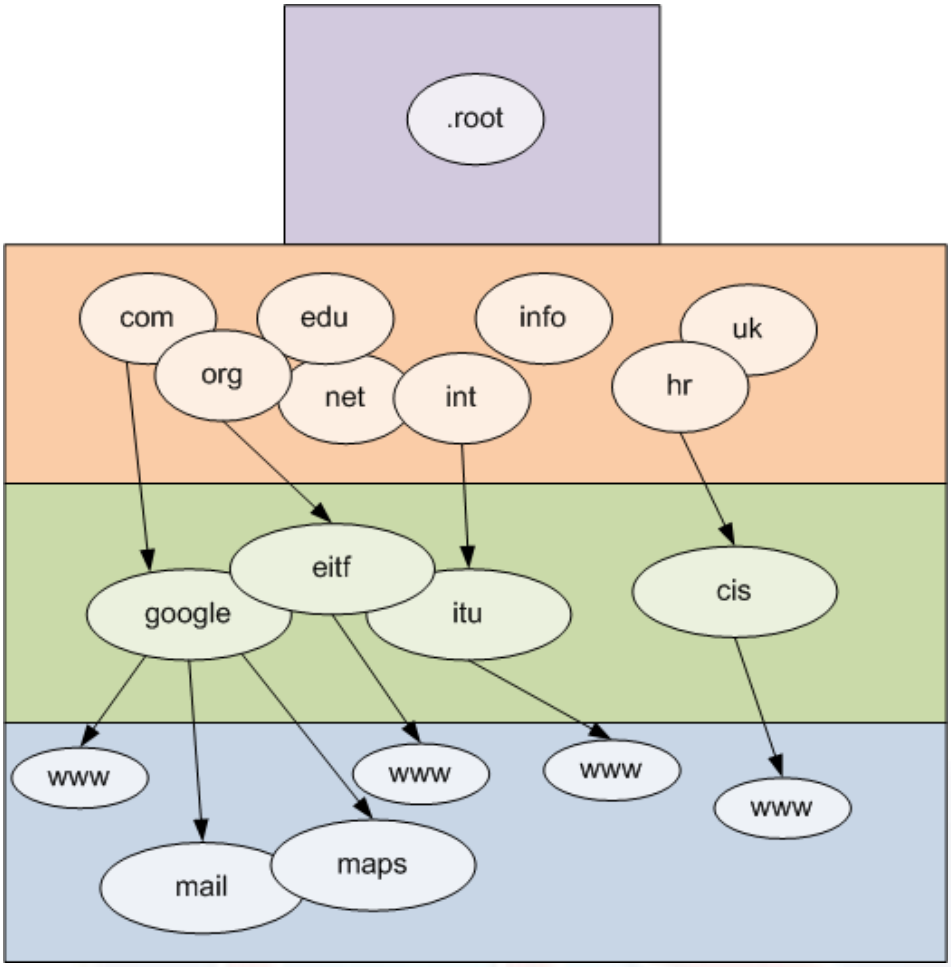
Budući da postoji jako veliki broj domena, s jednim DNS poslužiteljem ne bi bilo moguće obraditi sve klijentske zahtjeve. Zbog toga se koristi hijerarhijski sustav DNS poslužitelja (Slika 4). Na vrhu hijerarhije je korijenski (.root) DNS poslužitelj. Nakon njega slijede DNS poslužitelji zaduženi za vršne domene poput *.com*, *.org*, *.edu*, *.hr*, *.uk* itd. Nakon njih, slijede poslužitelji zaduženi za poddomene poput: *google.com* ili *cis.hr.* Hijerarhija može ići još niže ukoliko postoje dodatne poddomene, kao što su *mail.google.com*.

Kako bi se saznala IP adresa poslužitelja zaduženog za neku domenu, DNS upiti se šalju DNS poslužiteljima prema njihovom poretku u hijerarhiji. Primjerice, kako bi se saznala IP adresa poslužitelja zaduženog za domenu mail.google.com, po jedan DNS upit će primiti (tim redoslijedom):

- korijenski DNS poslužitelj,
- DNS poslužitelj vršne domene .com,
- DNS poslužitelj domene google.com i
- DNS poslužitelj domene mail.google.com.

[2] Lokalna mreža povezuje manji broj računala i drugih mrežnih uređaja na manjoj udaljenosti, najčešće unutar kuće ili zgrade.

[3] Domenu čini skup računala i mrežne opreme koji su (najčešće) vlasništvo jedne organizacije. Primjer domene je google.com koja može imati svoje poddomene (npr. mail.google.com, maps.google.com itd).



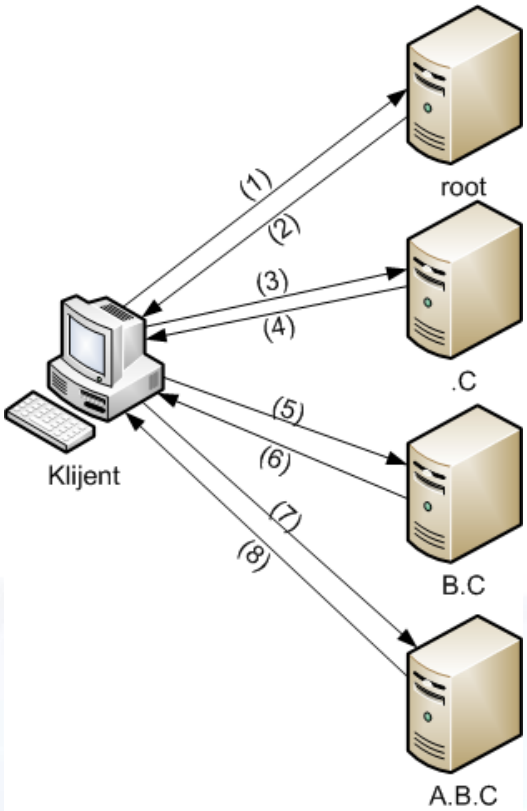
Slika 4. DNS hijerarhija

Postoje dva načina za razrješavanje DNS upita. To su:

1. iterativni način i
2. rekurzivni način.

Kod iterativnog načina klijent šalje sve DNS upite svakom od DNS poslužitelja. Primjer je prikazan na slici 5. Neka klijent želi saznati IP adresu *web* stranice *www.A.B.C*. Postupak je sljedeći:

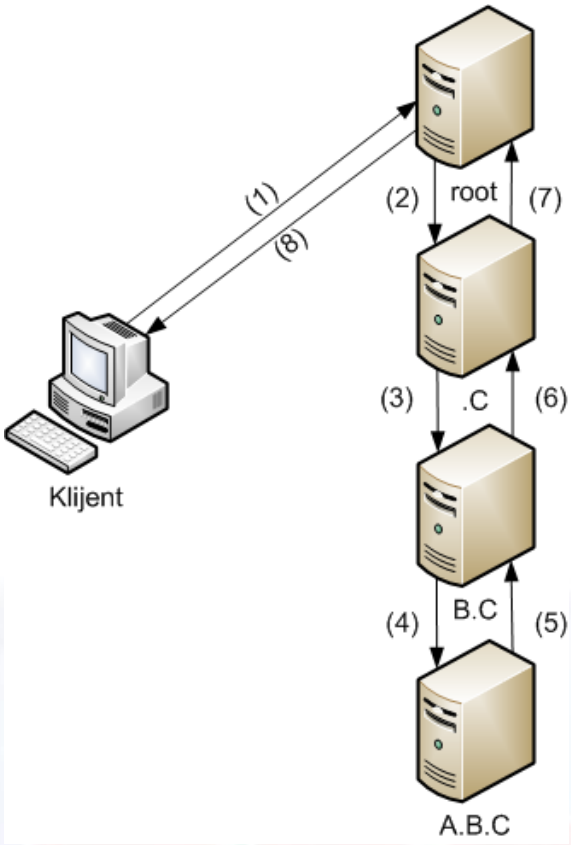
1. Klijent šalje DNS upit „Gdje je *www.A.B.C*?“ korijenskom DNS poslužitelju.
2. Korijenski DNS poslužitelj vraća IP adresu DNS poslužitelja zaduženog za domenu *.C*.
3. Klijent šalje DNS upit „Gdje je *www.A.B.C*?“ DNS poslužitelju zaduženom za domenu *.C*.
4. DNS poslužitelj na *.C* vraća IP adresu DNS poslužitelja zaduženog za domenu *B.C*.
5. Klijent šalje DNS upit „Gdje je *www.A.B.C*?“ DNS poslužitelju zaduženom za domenu *B.C*.
6. DNS poslužitelj na *B.C* vraća IP adresu DNS poslužitelja zaduženog za domenu *A.B.C*.
7. Klijent šalje DNS upit „Gdje je *www.A.B.C*?“ DNS poslužitelju zaduženom za domenu *A.B.C*.
8. DNS poslužitelj na *A.B.C* vraća klijentu IP adresu gdje može naći stranicu *www.A.B.C*.



Slika 5. Iterativni način rada

Kod rekurzivnog načina klijent šalje samo jedan DNS upit i očekuje samo jedan DNS odgovor. Ostale DNS upite i odgovore razmjenjuju DNS poslužitelji (Slika 6.). Postupak je sljedeći:

1. Klijent šalje DNS upit „Gdje je *www.A.B.C*?“ korijenskom DNS poslužitelju.
2. Korijenski DNS poslužitelj šalje DNS upit „Gdje je *www.A.B.C*?“ DNS poslužitelju zaduženom za domenu *.C*.
3. DNS poslužitelj na *.C* šalje DNS upit „Gdje je *www.A.B.C*?“ DNS poslužitelju zaduženom za domenu *B.C*.
4. DNS poslužitelj na *B.C* šalje DNS upit „Gdje je *www.A.B.C*?“ DNS poslužitelju zaduženom za domenu *A.B.C*.
5. DNS poslužitelj na *A.B.C* šalje odgovor s IP adresom za *www.A.B.C*.
6. DNS poslužitelj na *B.C* šalje odgovor s IP adresom za *www.A.B.C*.
7. DNS poslužitelj na *.C* šalje odgovor s IP adresom za *www.A.B.C*.
8. Korijenski DNS poslužitelj šalje odgovor s IP adresom za *www.A.B.C*.



Slika 6. Rekurzivni način rada

Najčešće se koristi kombinacija iterativnog i rekurzivnog načina rada: klijent rekurzivno šalje upit do DNS poslužitelja zaduženog za njegovu domenu, a DNS poslužitelj dalje iterativno pokušava doći do željene IP adrese.

Iz primjera je jasno koliko se DNS upita i odgovora razmjenjuje kako bi se došlo do željene IP adrese. Čak i uz hijerarhijsku strukturu DNS poslužitelja, zbog velikog broja DNS upita, poslužitelji bi bili preopterećeni. Zbog toga svaki klijent i DNS poslužitelj održavaju svoju DNS tablicu u priručnoj memoriji. Prije slanja DNS upita, klijent, odnosno DNS poslužitelj prvo provjerava postoji li odgovarajući zapis u njegovoj priručnoj memoriji. Ako postoji, nema potrebe slati DNS upit čime se rasterećuje ostale DNS poslužitelje. Zapisi u priručnoj memoriji imaju određeni vremenski rok trajanja koji se zove TTL (eng. *time to live*). Kada TTL istekne, zapis se briše iz priručne memorije. TTL definira administrator pojedine domene, a može iznositi par sati, par tjedana ili čak i više.

Kao i kod ARP protokola, DNS priručne memorije predstavljaju sigurnosni rizik, kao što će to biti objašnjeno u poglavlju 3.2.

3. Napadi prisluškivanjem mrežnog prometa

U uvodu je spomenuto da će u ovom dokumentu biti opisani napadi prisluškivanja mrežnog prometa koji iskorištavaju propuste u protokolima ARP i DNS. Ovi napadi još se nazivaju ARP trovanje (eng. *ARP Poisoning*) i trovanje DNS priručne memorije (eng. *DNS cache poisoning*)

ARP trovanje je objašnjeno u poglavlju 3.1, dok je trovanje DNS priručne memorije objašnjeno o poglavlju 3.2.

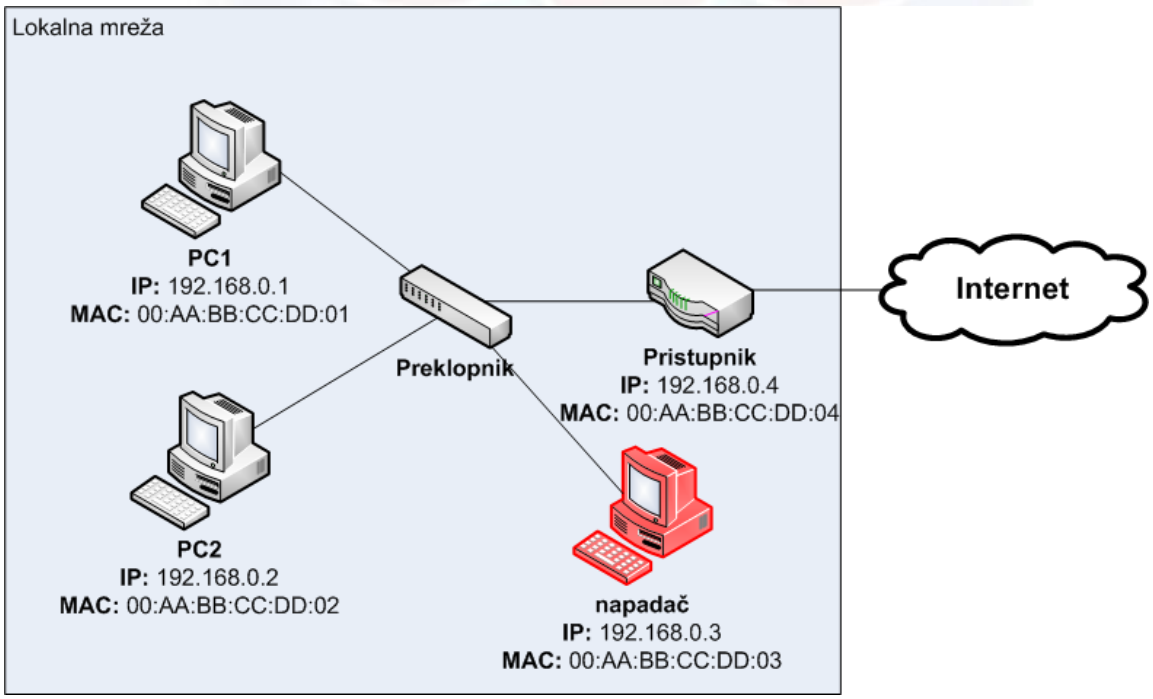
3.1. ARP trovanje

Protokol ARP je podložan napadima zbog nedovoljnih provjera primljenih ARP poruka. Naime, u protokolu nije definiran način provjere valjanosti primljenih ARP poruka što znači da napadač može poslati ARP poruku s lažnim sadržajem, a napadnuto računalo ne može provjeriti istinitost primljenog sadržaja. U nekim sustavima protokol ARP je uveden na još nesigurniji način jer uređaji obrađuju ARP odgovore čak i ako nisu prethodno poslali ARP zahtjev. Ove ranjivosti omogućuju cijeli niz MITM (eng. *man-in-the-middle*) napada.

Zbog nesigurne prirode protokola ARP, napadač može poslati ARP poruku s proizvoljnom MAC ili IP adresom koju će napadnuti uređaj prihvatiti i pohraniti u svoju ARP tablicu. Ovaj postupak se zove ARP trovanje. Najčešće napadač veže svoju MAC adresu s nekom IP adresom koju ostali uređaji u lokalnoj mreži koriste. Na taj način preusmjerava sav promet prema toj IP adresi na svoje računalo. Jednom kada paketi dođu do njega, moguće je:

- izvođenje DoS napada,
- čitanje podataka ili
- izmjena podataka.

U nastavku će biti objašnjeni napadi temeljeni na ARP trovanju. Za objašnjenje napada koristiti će se konfiguracija lokalne mreže kao na slici 7. Mreža se sastoji od dva korisnička računala (PC1 i PC2), jednog preklopnika, jednog pristupnika i napadačeva računala. Važno je naglasiti kako ovi napadi nisu uspješni ukoliko se napadač ne nalazi u istoj lokalnoj mreži kao njihova žrtva i ukoliko mreža ne koristi ARP protokol za povezivanje IP adresa s MAC adresama.



Slika 7.

3.1.1. DoS napad

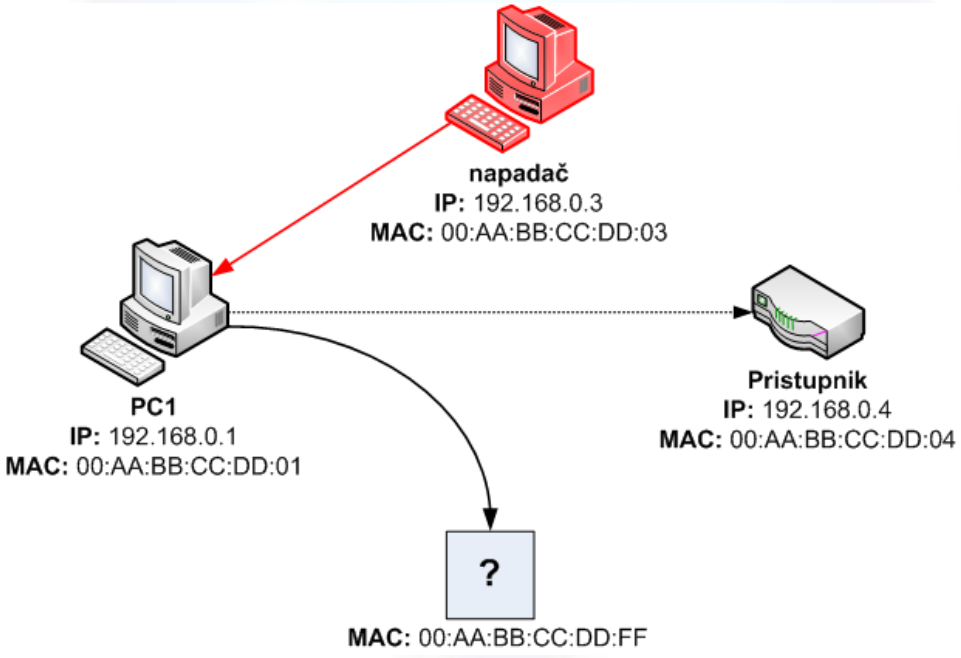
Kako bi izveo DoS napad, napadač mora spriječiti komunikaciju između korisničkih računala (PC1 i PC2) i pristupnika. Ukoliko u tome bude uspješan, lokalna mreža će biti odsječena od ostalih mreža preko kojih je bila povezana Internetom. Računala će i dalje moći komunicirati međusobno.

Napad se može izvesti slanjem ARP zahtjeva koji povezuje IP adresu pristupnika (192.168.0.4) s nepostojećom MAC adresom. Ukoliko računala PC1 i PC2 prihvate lažne ARP odgovore, njihovi paketi se neće usmjeravati prema pristupniku, nego će se odbacivati (jer ih mreža neće moći dostaviti na nepostojeću MAC adresu).

Primjer ovakvog napada je prikazan na slici 8. Napad započinje tako da napadač pošalje računalu PC1 ARP odgovor sa sadržajem: „Ja imam IP adresu 192.168.0.4. Moja MAC adresa je 00:AA:BB:CC:DD:FF“. Ova poruka je označena crvenom strelicom na slici 8. Napadač se lažno predstavio kao pristupnik i povezao svoju MAC adresu s pristupnikovom IP adresom. Računalo PC1 ne može provjeriti radi li se o lažnom predstavljanju, nego vjeruje dobivenoj poruci i zapisuje lažni par adresa u svoju ARP tablicu.

Nakon toga računalo PC1 želi poslati paket nekom računalu izvan lokalne mreže. Kako bi to bilo moguće, paket treba prvo poslati pristupniku koji će se pobrinuti za daljnje prosljeđivanje paketa. Točkasta strelica pokazuje željeni put paketa. Budući da računalo PC1 ima netočnu MAC adresu, paketi će umjesto kod pristupnika završiti na nepoznatom mjestu s MAC adresom 00:AA:BB:CC:DD:FF (na slici 8. označeno upitnikom).

Paketi koje računalo PC1 šalje neće biti dostavljeni na odredište sve dok u ARP tablici postoji kriva MAC adresa pristupnika.

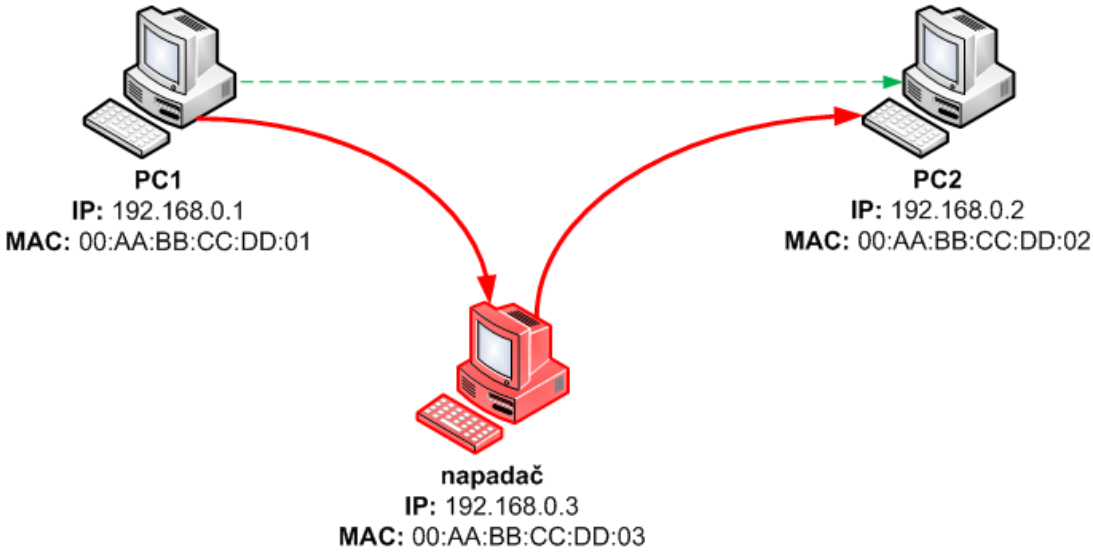


Slika 8. DoS napad

3.1.2. *Man-in-the-middle* napad

Man-in-the-middle (u nastavku MITM napad) je takav oblik napada kod kojeg napadač prisluškuje komunikaciju između dva računala bez njihovog znanja. Primjer MITM napada je prikazan na slici 9.

Napadač se priključuje na komunikacijski kanal između računala PC1 i PC2 te presreće njihove pakete, tj. prisluškuje mrežni promet. Ukradene pakete može pročitati ili izmijeniti prije nego ih pošalje prema odredištu. Računala PC1 i PC2 nisu svjesna da napadač prisluškuje njihovu komunikaciju.



Slika 9. MITM napad

Za izvođenje MITM napada moguće je iskoristiti propuste u ARP protokolu. Napad se izvodi pomoću dvije ARP poruke:

1. Napadač šalje ARP odgovor računalu PC1: „Ja imam IP adresu 192.168.0.2. Moja MAC adresa je 00:AA:BB:CC:DD:03.“
2. Napadač šalje ARP odgovor računalu PC2: „Ja imam IP adresu 192.168.0.1. Moja MAC adresa je 00:AA:BB:CC:DD:03.“

Prva ARP poruka povezuje napadačevu MAC adresu s IP adresom računala PC2. Ukoliko računalo PC1 prihvati ovu ARP poruku i pohrani ju u svoju tablicu, sav promet namijenjen računalu PC2 će zapravo dolaziti napadaču.

Druga ARP poruka povezuje napadačevu MAC adresu s IP adresom računala PC1 i namijenjena je računalu PC2. Ukoliko ju PC2 prihvati, sav promet će umjesto računalu PC1 slati napadaču.

S dvije ARP poruke, napadač je osigurao preusmjeravanje svog prometa između računala PC1 i PC2 na njegovo računalo. Ukoliko napadač želi ostati skriven, mora osigurati dostavu ukradenih paketa do njihovog odredišta. To znači da će napadač nakon što primi paket od primjerice računala PC1, morati taj paket poslati do računala PC2. Pri tome može primljeni paket i izmijeniti, a računalo PC2 neće znati da je došlo do promjene.

Opisani MITM napad se može izvesti između računala PC1 i pristupnika koji pakete prosljeđuje prema Internetu. Jedina razlika je što napadač mora poznavati IP adresu pristupnika umjesto IP adrese računala PC2.

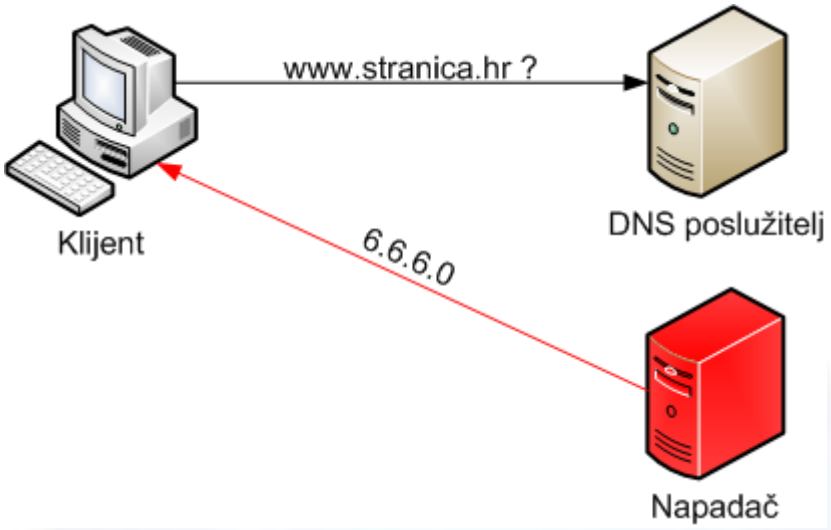
3.1.3. MAC preplavljivanje

MAC preplavljivanje je napad koji je usmjeren na mrežne preklopnike, a također se može iskoristiti za prisluškivanje mrežnog prometa. Propust koji se iskorištava je ograničeni spremnik za MAC adrese u preklopnicima. Ukoliko napadač preplavi preklopnik s velikim brojem posebno oblikovanih ARP odgovora, spremnik u preklopniku neće biti dovoljan za normalni rad preklopnika, nego će on prijeći u tzv. *hub* način rada. U tom slučaju, preklopnik više ne usmjerava pakete prema odgovarajućim računalima, nego se paketi šalju prema svim računalima u mreži (sveodredišno razašiljanje) uključujući i napadačevo računalo. Na taj način, napadač dobiva uvid u sve pakete koji se šalju u lokalnoj mreži i može prisluškivati promet.

Prisluškivanje prometa prestaje jednom kada se preklopnik vrati iz *hub* načina rada. Ukoliko napadač želi i dalje prisluškivati promet, mora ponovo poslati veliki broj ARP odgovora preklopniku.

3.2. Trovanje DNS priručne memorije

Napadi koji koriste DNS se temelje na sličnom nedostatku kao i ARP protokol: cilj je poslati lažnu poruku kojoj će žrtva vjerovati i uvrstiti u svoju priručnu memoriju. U ovom slučaju, napadač šalje lažne DNS odgovore pretvarajući se da je pravi DNS poslužitelj, a žrtva (klijent ili drugi DNS poslužitelj) vjeruje DNS odgovoru kojeg prvog primi (Slika 10.). Informacija u lažnom DNS odgovoru se sprema u DNS priručnu memoriju.



Slika 10. Pojednostavljeni napad korištenjem DNS-a

Ovaj oblik napada se naziva trovanje DNS priručne memorije i ima veći doseg od ARP trovanja. Naime, kod ARP trovanja, napad je bio ograničen samo na lokalnu mrežu kojoj je napadač morao imati pristup. Kod DNS trovanja, napadač ne mora biti u istoj lokalnoj mreži kao DNS poslužitelj, a jednom kada otruje poslužiteljevu priručnu memoriju, poslužitelj širi lažne podatke svim računalima koji su mu poslali DNS upit, jer ne zna da posjeduje krive podatke. Na primjer, ako napadač umetne u priručnu memoriju DNS poslužitelja krivu informaciju o IP adresi neke domene, sav promet prema toj domeni će biti preusmjeren na neko drugo računalo, najčešće na računalo koje nadzire napadač. Time napadač dobiva mogućnost izvođenja drugih napada koju uključuju:

- prisluškivanje prometa,
- izmjena prometa,
- širenje zlućudnih programa (eng. *malware*),
- krađa osjetljivih informacija,
- itd.

Za razliku od napada koji koriste ARP protokol, nije dovoljno samo poslati DNS odgovor na nepostojeći DNS upit. Lažni DNS odgovor se može poslati tek kada klijent ili drugi DNS poslužitelj pošalje DNS upit. Dodatno, lažni DNS odgovor kojeg šalje napadač mora izgledati kao da ga je poslao pravi DNS poslužitelj. Uvjeti koji moraju biti zadovoljeni kako bi žrtva prihvatila lažni DNS odgovor su:

- DNS odgovor mora doći na istu IP adresu s koje je bio poslan DNS upit,
- DNS odgovor mora doći na istu priključnicu s koje je bio poslan DNS upit,
- DNS odgovor mora sadržavati odgovor na poslani DNS upit,
- DNS odgovor mora sadržavati isti identifikacijski broj transakcije kao poslani DNS upit te
- je potrebno onemogućiti pravog DNS poslužitelja da pošalje pravi DNS odgovor ili poslati lažni DNS odgovor prije pravog DNS odgovora.

Neke od ovih stavki nije teško za ostvariti. Primjerice, napadač odmah zna koji je DNS upit poslan, jer sadrži ime domene koju napadač želi napasti. Također, IP adresu pošiljatelja DNS upita nije teško pogoditi ako se koristi rekurzivni način rada. Npr, neka napadač želi napasti

domenu *A.B.C*, a za razrješavanje se koristi rekurzivni način rada. Napadač zna da će DNS upit doći od DNS poslužitelja na domeni *B.C*.

Loše provođenje DNS-a olakšava napadačima posao. Stare inačice DNS-a su uvijek koristile istu priključnicu (priključnica 53). Neke novije inačice DNS-a koriste drugačiji broj priključnice, ali problem je što se ona ne mijenja tokom rada. Nakon što se pokazalo da statička vrijednost priključnice na koju dolaze DNS poruke olakšava napade, za vrijednost priključnice se počela uzimati slučajna vrijednost. Time, teoretski, napadač mora pogoditi pravu vrijednost priključnice između 65535 mogućih vrijednosti. U stvarnosti je broj mogućih kombinacija ipak manji jer je jedan dio priključnica unaprijed rezerviran. Ipak, slučajan odabir priključnice napadačima značajno otežava stvaranje ispravnog DNS odgovora.

Ono što je najteže za pogoditi je identifikacijski broj transakcije koji se sastoji od 16 bitova. Ponovo, loše proveden odabir identifikacijskog broja može jako olakšati napad. Primjerice, DNS klijent na Windows XP SP1 je imao jako predvidljiv odabir identifikacijskog broja:

- svaki identifikacijski broj je počinjao s 1 i
- za svaki novi DNS upit, identifikacijski broj se povećavao za 1.

Sličan propust je 1997. godine otkriven u alatu BIND, najraširenijem programskom paketu za DNS kojeg su koristili brojni DNS poslužitelji. BIND je identifikacijske brojeve izdavao sekvencijalno zbog čega su napadači vrlo lako pogađali identifikacijski broj za svoj lažni odgovor. Dovoljno je bilo prvo poslati lažni DNS upit na DNS poslužitelj s programskim paketom BIND, a zatim uvećati dobiveni identifikacijski broj i poslati lažni DNS odgovor predstavljajući se kao pravi DNS poslužitelj. Ovakvi propusti su danas rijetki, ali administratorima se preporuča provjeriti postoje li možda na njihovim DNS poslužiteljima.

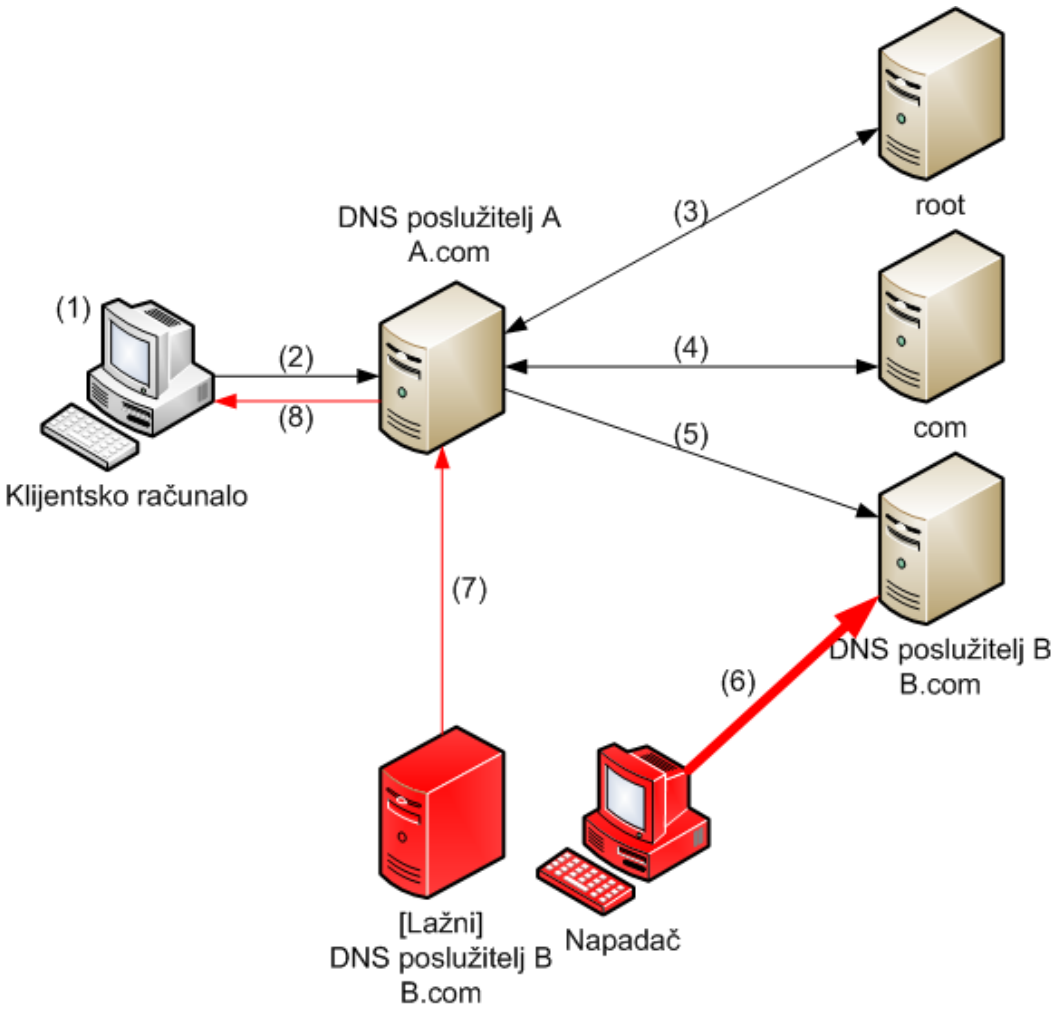
Posljednju stvar koju napadač mora osigurati je da njegov lažni DNS odgovor stigne prije pravog DNS odgovora. To je najlakše ostvariti slanjem jako velikog broja DNS upita na pravi DNS poslužitelj tako da on ne stigne obraditi klijentski DNS upit i poslati ga na vrijeme. Dok se pravi DNS poslužitelj bori s brojnim upitima, napadač slaže svoj lažni DNS odgovor i šalje ga klijentu. Dok pravi DNS poslužitelj obradi sve zahtjeve i pošalje pravi DNS odgovor, klijent će već uvrstiti lažni DNS odgovor u svoju priručnu memoriju i odbaciti pravi zahtjev misleći da je lažni.

U nastavku je primjer napada trovanjem DNS priručne memorije (Slika 11.). Klijent želi pristupiti stranici *www.B.com* koja se nalazi u domeni *B.com*. S druge strane, napadač želi korisnika preusmjeriti na drugu stranicu koju on nadgleda. Pri tome će koristiti trovanje DNS priručne memorije kako bi korisnika preusmjerio na krivu stranicu. Za razlučivanje adrese koristit će se kombinacija iterativnog i rekurzivnog načina rada: klijent šalje DNS upit u rekurzivnom načinu rada do DNS poslužitelja zaduženog za njegovu domenu (*A.com*), dok DNS poslužitelj dalje šalje DNS upit u iterativnom načinu rada. Postupak je sljedeći:

1. Klijent provjerava svoju DNS priručnu memoriju ne bi li pronašao IP adresu za stranicu *www.B.com*.
2. Budući da nema zapisanu IP adresu željene *web* stranice, šalje DNS upit DNS poslužitelju A zaduženom za njegovu domenu (*A.com*).
3. DNS poslužitelj A prvo provjerava je li zadužen za domenu *B.com*. Budući da nije (on je zadužen za domenu *A.com*), provjerava svoju DNS priručnu memoriju. Budući da ne pronalazi traženu IP adresu, počinje slati DNS upite drugim DNS poslužiteljima. Prvi na redu je korijenski DNS poslužitelj (root). Korijenski DNS poslužitelj ne zna gdje se nalazi *www.B.com*, ali zna koji je DNS poslužitelj zadužen za domenu *.com* pa kao odgovor šalje adresu DNS poslužitelja zaduženog za domenu *.com.*
4. DNS poslužitelj A šalje novi DNS upit poslužitelju za domenu *.com*. Ovaj mu vraća adresu poslužitelja B.
5. DNS poslužitelj A šalje novi DNS upit poslužitelju B. Do ovog dijela se proces razlučivanja domenskog imena ne razlikuje od standardne procedure opisane u poglavlju 2.2. Međutim, sada u postupak ulazi napadač koji je odlučio otrovati priručnu memoriju DNS poslužitelja A. Kako bi to mogao, mora saznati identifikacijski broj transakcije i priključnicu na koju se šalje odgovor. Ukoliko napadač posjeduje ove vrijednosti, onda može oponašati DNS poslužitelja B. Uz dovoljno vremena, napadač može otkriti obje vrijednosti.
6. Kako bi dobio na vremenu, a ujedno i onemogućio DNS poslužitelj B da pošalje pravi DNS odgovor, napadač izvodi DoS napad na DNS poslužitelju B. Najčešće se to izvodi slanjem jako velikog broja DNS upita koje DNS poslužitelj ne stiže obraditi. Dok se DNS

poslužitelj B muči s obradom velikog broja (lažnih) zahtjeva, napadač otkriva identifikacijski broj i priključnicu.

7. Kada napadač otkrije identifikacijski broj, šalje lažni DNS odgovor DNS poslužitelju A, pretvarajući se da je DNS poslužitelj B. U lažnom DNS odgovoru, umjesto prave IP adrese za stranicu *www.B.com*, šalje IP adresu stranice koju može nadgledati. DNS poslužitelj A prihvaća odgovor, ne sumnjajući u njegovu ispravnost i zapisuje ga su svoju DNS priručnu memoriju.
8. DNS poslužitelj A šalje DNS odgovor klijentu, ali umjesto točne IP adrese za *www.B.com*, klijentu šalje IP adresu koju je dobio od napadača. Klijent također zapisuje dobivenu IP adresu u svoju DNS priručnu memoriju.



Slika 11. DNS napad

Iz primjera je vidljivo kako se trovanje DNS priručne memorije na DNS poslužitelju propagira dalje. U ovom primjeru, sva računala iz domene A.com koja žele pristupiti stranici www.B.com, tražit će IP adresu od svog DNS poslužitelja A. Budući da je njegova DNS priručna memorija otrovana, sva računala u domeni A.com će dobiti krivu IP adresu za www.B.com te će i njihove DNS priručne memorije biti otrovane.

Ovisno o tome kako napadač oblikuje svoj lažni DNS odgovor moguće je izvesti različite napade:

- **Otkrivanje osjetljivih informacija** – napadač u lažni DNS odgovor umjesto prave IP adrese postavlja IP adresu poslužitelja kojeg on nadzire. Na tom poslužitelju postavlja *web* stranicu koja je jako slična izvornoj *web* stranici čiju IP adresu je zamijenio sa svojom. Zbog trovanja DNS priručne memorije, dio prometa prema izvornoj *web* stranici bit će preusmjeren na lažnu *web* stranicu. Na primjer, napadač može preusmjeriti sav promet s *web* stranice neke banke na svoju stranicu, a zatim prikupljati podatke o

lozinkama od korisnika koji završe na njegovoj stranici. Dobivene lozinke, napadač može iskoristiti za pristup korisničkim računima na pravoj stranici banke, te tako doći do dodatnih informacija o, primjerice, kreditnim karticama.

- **MITM napad** – kao i kod MITM napada kod ARP protokola, napadač se postavlja između dva korisnika koji žele komunicirati. Neka se korisnici zovu Alice i Bob. Napadač mora otrovati DNS priručnu memoriju kod Alice tako da poveže Bobovu IP adresu sa svojom IP adresom. Nakon toga, kada Alice šalje pakete Bobu, zapravo ih šalje napadaču. Napadač presreće pakete, mijenja ih ili samo čita, a zatim prosljeđuje prema Bobu. Pakete koje Bob šalje nazad, napadač također presreće, mijenja ili samo čita i vraća nazad do Alice. Pri tome Alice i Bob nisu svjesni napadačeve prisutnosti, a napadač može saznati osjetljive informacije ili upravljati komunikacijom mijenjajući sadržaj paketa.

4. Obrana od prisluškivanja

U sljedećim poglavljima biti će objašnjeni načini zaštite od ARP i DNS trovanja.

4.1. ARP obrana

Napadi koji iskorištavaju propust u ARP protokolu predstavljaju veliki problem jer su vrlo jednostavni za izvesti ukoliko napadač ima pristup lokalnoj mreži. Zbog toga je potrebno svaku mrežu osigurati od ovakvog oblika napada.

Jedan vrlo jednostavan način za obranu je korištenje statičkih ARP tablica. Ukoliko svako računalo zna parove IP i MAC adresa za sva računala u svojoj lokalnoj mreži neće postojati potreba za ARP porukama, pa se uređaje može podesiti da ne primaju ARP poruke. Zbog toga će se odbacivati i zlonamjerne ARP poruke koji bi inače uzrokovale DoS ili MITM napade. Međutim, ovaj pristup je moguć samo kod malih mreža jer administrator mreže mora ručno održavati ARP tablice na svakom računalu u mreži. Kod velikih mreža je to nemoguće za izvesti jer, primjerice, dodavanje jednog novog računala u mrežu ili promjena IP adrese postojećeg računala zahtijeva ažuriranje ARP tablica u svim ostalim računalima.

Za velike mreže se preporuča korištenje nekog alata za zaštitu poput ArpOn ili ARPDefender.

ArpON je prijenosni pozadinski proces (eng. *daemon*) koji štiti od ARP trovanja. ArpON ne zahtijeva izvođenje na središnjem poslužitelju ili kriptiranje, niti ne mijenja specifikacijom zadan rad ARP protokola. Kako bi uspješno obavljao svoj rad, potrebno ga je instalirati na sva računala i poslužitelje u lokalnoj mreži. ArpON podržava sljedeće operacijske sustave:

- Linux,
- Mac OS X,
- FreeBSD,
- NetBSD i
- OpenBSD.

U svom radu koristi algoritam detaljno objašnjen na *web* stranici:

http://arpon.sourceforge.net/algorithms.html

ArpON može raditi u tri načina rada:

- SARPI (eng. *Static ARP inspection*),
- DARPI (eng. *Dynamic ARP inspection*) i
- HARPI (eng. *Hybrid ARP inspection*).

SARPI način rada je prilagođen mrežama koje koriste statičke IP adrese, DARPI mrežama koje koriste dinamičku dodjelu IP adresa, a HARPI mrežama koje koriste i statičke i dinamičke IP adrese.

ArpON nadgleda ARP poruke i ovisno o vrsti ARP poruke (dolazni/odlazni upit/odgovor), obrađuje ju po određenom algoritmu. Pri obradi koriste se privremene SARPI i DARPI tablice.

ARPDefender se koristi u istu svrhu kao ArpON, ali ima drugačiji pristup. Prvotno je osmišljen za zaštitu bankovnih lokalnih mreža, ali danas se preporuča za zaštitu svih lokalnih mreža. ARPDefender je samostojeći uređaj (Slika 12) koji nadzire ARP promet tražeći sumnjive ARP poruke. Ukoliko primijeti sumnjivu aktivnost, prijavljuje ju na zadanu adresu elektroničke pošte, a moguće je prijave preusmjeriti na mobitel kako bi administrator što prije reagirao.

ARPDefender dolazi u tri inačice koje se razlikuju po broju sučelja (za administraciju i nadgledanje) i podržanoj veličini lokalne mreže koju može nadgledati (32, 128 ili 256 računala.)

Slika 12. ARPDefender uređaj
Izvor: ARPDefender

Zbog vrlo nesigurne prirode protokola ARP, planira se njegova zamjena u novoj inačici IP protokola (IPv6). U protokolu IPv6 (eng. *Internet Protocol Version 6*) ARP je zamijenjen s protokolom NDP[4] (eng. *Neighbor Discovery Protocol*) koji ne sadrži propuste ARP protokola. Jednom kada se uvede IPv6, ARP trovanje će većim dijelom postati prošlost.

4.2. DNS obrana

Neki načini obrane od trovanja DNS priručne memorije su spomenuti u poglavlju 3.2. Korištenje statičke priključnice i predvidljivog stvaranja identifikatora znatno olakšava napad. Zbog toga se savjetuje slučajan odabir identifikatora i priključnice. Identifikator se sastoji od 16 bitova, što daje relativno mali broj mogućih vrijednosti (2^{16} = 65 536). Uz slučajan odabir priključnica, broj mogućih vrijednosti se značajno povećava. Broj priključnice se također sastoji od 16 bitova što također daje 65 536 mogućih vrijednosti, ali dio priključnica je unaprijed rezerviran za druge potrebe. Zbog toga je broj mogućih vrijednosti priključnica za DNS mnogo manji i iznosi oko 2000 vrijednosti (ovisno o inačici). Kombiniranjem mogućih vrijednosti za identifikacijski broj i priključnicu dolazi se do sljedećeg izraza za broj mogućih kombinacija:

(broj ID-eva) * (broj priključnica) = $2^{16} * 2^{11} = 2^{27}$ > 134 milijuna kombinacija

Dakle, slučajnim odabirom identifikacijskog broja i priključnice, napadač mora pogoditi jednu od 134 milijuna mogućih kombinacija.

Rekurzivni način rada također olakšava prikupljanje informacija potrebnih za napad jer napadač može lakše saznati odakle je došao DNS zahtjev, kao što je objašnjeno u poglavlju 3.2. Zbog toga se administratorima savjetuje korištenje iterativnog umjesto rekurzivnog načina rada.

Naravno, uvijek se preporuča korištenje najnovijeg programskog paketa za DNS razlučivanje (BIND inačice 9.x ili više, ili Microsoft Windows Server 2008).

Kako bi se povećala sigurnost DNS-a, predlaže se korištenje DNSSEC-a (eng. *Domain Name System Security Extensions*). DNSSEC je povratno kompatibilan s DNS-om, a za povećanje

[4] Više informacija o NDP-u može se pronaći u leksikonu pojmova na kraju dokumenta

sigurnosti DNS-a koristi digitalne potpise kako bi dokazao autentičnost DNS upita i odgovora. Pri tome se koristi infrastruktura javnog ključa ili PKI (eng. *Public key infrastructure*). Svaki element u DNS hijerarhiji dobiva vlastiti par javni/privatni ključ kojim potpisuje svoje DNS odgovore ili upite.

DNSSEC jamči:

- **Autentičnost izvora DNS poruka** – primatelj može biti siguran da je poruku poslao pravi DNS poslužitelj, a ne netko drugi (npr. napadač).
- **Integritet podataka** – primatelj može provjeriti je li poruka mijenjana.
- **Nepostojanje podataka** – ukoliko ne postoji tražena domena, klijent može biti siguran da ona zbilja ne postoji jer odgovarajući DNS poslužitelj jamči za nepostojanje podataka (ne može se dogoditi da napadač javi klijentu da tražena domena ne postoji, a zapravo postoji).

DNSSEC ne jamči:

- **Povjerljivost podataka** – podaci u DNS porukama se ne šifriraju, pa stoga napadač može čitati DNS poruke ukoliko ih presretne.

DNSSEC osigurava klijenta od napada trovanjem DNS priručne memorije, a time štiti korisnike i od jednog od oblika napada prisluškivanjem mrežnog prometa. Smatra se da će se povećanjem sigurnosti DNS-a ujedno povećati sigurnost cijelog Interneta budući da Internet korisnici jako ovise o DNS-u pri svom radu. Ipak, DNSSEC još uvijek nije u potpunosti uveden zbog brojnih problema, kao što su:

- složenost protokola koji se još uvijek nadograđuje dodatnim zahtjevima.
- DNSSEC mora biti uveden na sve DNS poslužitelje i DNS klijente na korisničkim računalima.
- Postoje neslaganja među proizvođačima tko bi trebao imati ovlast nad ključevima korijenske domene.
- DNSSEC mora biti povratno kompatibilan s DNS-om.
- DNSSEC se mora nositi sa sve većim povećanjem Interneta.
- DNSSEC poruke su zahtjevnije za obradu od DNS poruka zbog čega neki DNS poslužitelji imaju smanjene performanse.

5. Zaključak

Prisluškivanje mrežnog prometa jedan je od oblika napada kojim zlonamjerni korisnici mogu prikupiti osjetljive informacije (poput korisničkih imena i lozinki, informacija o sustavu itd.) potrebne za kasnije napade. Prisluškivanje mrežnog prometa može biti samo uvod u ozbiljnije napade koji rezultiraju DoS napadom ili preuzimanjem potpunog nadzora nad sustavom. Dodatno, ako napadač ima pristup mrežnom prometu, onda također ima i mogućnost sadržaja podatkovnih paketa. Na taj način može utjecati na komunikaciju između dvije strane, bez da te strane znaju da je njihova veza kompromitirana (MITM napad).

Zbog toga je potrebno posvetiti pažnju osiguranju sustava od ovakvog oblika napada. Najbolji način za zaštitu je poznavanje načina kako se napadi odvijaju. U dokumentu su opisani protokol ARP i DNS koji se često iskorištavaju za napad prisluškivanjem mrežnog prometa. ARP i DNS su ranjivi zbog istog razloga - nemaju mogućnost provjere autentičnosti pošiljatelja ARP odnosno DNS poruke. Zbog toga vjeruju prvoj informaciji koju prime i na njoj temelje daljnji rad. Ovo uzrokuje brojne probleme ako se zlonamjerno iskoristi, kao što je opisano u ovom dokumentu.

Propusti u ARP protokolu mogu se ublažiti korištenjem alata kao što su ArpON i ARPDefender, koji nadgledaju mrežni promet i javljaju sumnjive aktivnosti. U budućnosti, ARP protokol će biti zamijenjen NDP protokolom što će napadačima otežati prisluškivanje prometa u lokalnoj mreži.

Kao zaštita od napada koji iskorištavaju propuste u DNS-u, preporuča se redovita primjena nadogradnje za DNS klijente na korisničkim računalima, odnosno programske pakete koji obavljaju rad DNS poslužitelja. Postoje neke smjernice koje su korisne za otežavanje napada (omogućiti slučajan odabir priključnica i identifikacijskog broja te onemogućavanje rekurzivnog načina rada), ali veća sigurnost će se ostvariti tek širim uvođenje DNSSEC-a.

6. Leksikon pojmova

DOS napad (Napad uskraćivanjem usluge)

Napad na sigurnost na način da se određeni resurs opterećuje onemogućujući mu normalan rad.

http://searchsoftwarequality.techtarget.com/definition/denial-of-service

DNS (*Domain Name System*)

Domain Name System (DNS) je hijerarhijski sustav imenovanja izgrađen na distribuiranim bazama podataka za računala, usluge ili bilo koji resurs spojen na Internet ili privatnu mrežu.

http://www.kb.iu.edu/data/adns.html

E-mail (Elektronička pošta)

Predstavlja način prijenosa tekstualnih poruka putem komunikacijskih mreža, najčešće Interneta. Usluga omogućuje umetanje dodatnih datoteka kao privitke (eng. *attachment*), a ovisno o poslužitelju usluge može postojati ograničenje na količinu, veličinu i tip datoteka. Elektronička pošta je postala standard za poslovnu komunikaciju, te je zamijenilo standardne dopise (dopisi se i dalje šalju ali putem elektroničke pošte). Nedugo nakon popularizacije elektronička pošta je postala medij za prijenos raznih zlonamjernih, štetnih programa kao što su crvi i virusi. Uporabom raznih heurističkih metoda prepoznavanja ovo se većinom spriječilo, no i dalje se dnevno razmjenjuju razne (bezopasne) spam ili junk poruke kojima je cilj reklamirati neki proizvod ili uslugu.

http://www.webopedia.com/TERM/E/e_mail.html

IP protokol (*Internet Protocol*)

IP je jedan od glavnih protokola u Internetu, a koristi se za usmjeravanja paketa kroz Internet. U tu namjenu, dodjeljuje IP adrese izvora paketa i njegovog odredišta na temelju kojih će se paketi usmjeravati kroz nekoliko računalnih mreža.

http://compnetworking.about.com/od/networkprotocolsip/g/ip_protocol.htm

IPv6 (*Internet Protocol version 6*)

IPv6 je nova inačica IP protokola. Trenutna inačica (IPv4) koristi 32 bita za IP adrese, dok IPv6 koristi IP adrese od 128 bita. Time se uvelike povećao adresni prostor što je jedan od glavnih problema IPv4 inačice. IPv6 također unosi bolju podršku za mobilnost i višeodredišne adrese, kao i neke dodatne mogućnosti koje nisu dostupne u trenutnoj inačici.

http://www.networkworld.com/news/2011/082911-ipv6-250196.html

Koncentrator (Uređaj koji povezuje uređaje u lokalnu mreže bez odvajanja prometa)

Koncentrator je uređaj za povezivanje više uvijenih parica ili svjetlovodnih niti zajedno na način da oni djeluju kao jedinstveni mrežni odsječak. Za razliku od preklopnika, koji dijeli mrežni promet i šalje ga samo na određeno odredište, koncentrator šalje pakete svim uređajima u mreži.

http://www.phy.hr/~dandroic/nastava/rm/hub_vs_switch.pdf

MAC protokol (Komunikacijski protokol za pristup mediju)

Media Access Control (MAC) je protokol za komunikaciju podacima, također poznat kao protokol upravljanja pristupom mediju. On omogućuje mehanizme adresiranja i kontrole pristupa kanalima koji služe za komunikaciju terminala, odnosno čvorišta, s mrežom koja ima više pristupnih točaka.

http://ahyco.ffri.hr/ritehmreze/teme/mac.htm

MITM napad (Napad ubacivanjem posrednika)

Napad na sigurnost pri kojem se zlonamjerni napadač umiješa u komunikaciju na način da se postavi između sugovornika te čita i izmjenjuje poruke.

http://en.wikipedia.org/wiki/Man-in-the-middle_attack

NDP (*Neighbor Discovery Protocol*)

NDP je jedan od protokola koji se koriste u novoj inačici protokola IP (IPv6). NDP zamjenjuje ARP protokol na razini podatkovne poveznice, a odgovoran je za otkrivanje mrežnih čvorova i njihovih adresa, pronalaženje odgovarajućih usmjeritelja i DNS poslužitelja itd.

http://www.ngnet.it/e/ipv6proto/ipv6-proto-6.php

PKI (Infrastruktura javnih ključeva)

PKI je sustav poslužitelja koji služi kao središnji autoritet koji povezuje javne ključeve s njihovim vlasnicima.

http://searchsecurity.techtarget.com/definition/PKI

Preklopnik (Mrežni uređaj)

Preklopnik je uređaj koji upravlja protokom podataka između dijelova lokalne računalne mreže. Za razliku od usmjeritelja, preklopnik dijeli mrežni promet te ga šalje na određena odredišta, dok usmjeritelj šalje podatke na sve uređaje koji su u mreži.

http://en.wikipedia.org/wiki/Network_switch

Priključnica (Krajnje točke u komunikaciji transportnih protokola)

Brojčane vrijednosti temeljem kojih računalo po prihvatu podataka zna koju uslužnu programsku potporu (servise) mora aktivirati te na koji način razmjenjivati podatke na transportnom sloju.

http://searchnetworking.techtarget.com/definition/port-number

Pristupnik (Mrežni element)

Pristupnik je složeni mrežni element koji stoji na rubu jedne mreže i povezuje ju s drugom mrežom. Pristupnik često ujedno obavlja funkcije posredničkog poslužitelja, vatrozida, DNS poslužitelja i sl.

http://compnetworking.about.com/od/networkdesign/g/network-gateway.htm

URL (*Uniform Resource Locator*)

URL predstavlja adresu određenog resursa na Internetu. Resurs na koji pokazuje URL adresa može biti HTML dokument, slika, datoteka ili bilo koja datoteka koja se nalazi na određenom *web* poslužitelju.

http://searchnetworking.techtarget.com/definition/URL

TTL (Time to live)

U IP protokolu TTL označava koliko još usmjeritelja podatkovni paket smije proći prije nego dođe do odredišta. Neki drugi protokoli TTL-om označavaju koliko dugo neka informacija smije postojati prije nego se odbaci jer je zastarjela

http://searchnetworking.techtarget.com/definition/time-to-live

WWW (*World Wide Web*)

WWW (eng. *World Wide Web*) je jedna od najkorištenijih usluga Interneta koja omogućuje dohvaćanje dokumenata. Dokumenti mogu sadržavati tekst, slike i multimedijalne sadržaje, a međusobno su povezani poveznicama (eng. *hiperlink*).

http://www.webopedia.com/TERM/W/World_Wide_Web.html

7. Reference

[1] Corey Nachreiner: Anatomy of an ARP Poisoning Attack, listopad 2011.

[2] Wikipedia: Address Resolution Protocol, http://en.wikipedia.org/wiki/Address_Resolution_Protocol, listopad 2011.

[3] Wikipedia: ARP spoofing, http://en.wikipedia.org/wiki/ARP_poisoning, listopad 2011.

[4] Tom Olzak: DNS Cache Poisoning: Definition and Prevention, ožujak 2006.

[5] Ian Green: DNS Spoofing by The Man In The Middle, siječanj 2005.

[6] Kim Davies: DNS Cache Poisoning Vulnerability, listopad 2008.

[7] Steve Friedl: An Illustrated Guide to the Kaminsky DNS Vulnerability, http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html, kolovoz 2008.

[8] Wikipedia: DNS cache poisoning, http://en.wikipedia.org/wiki/DNS_cache_poisoning, listopad 2011.

[9] DELL SecureWorks: DNS Cache Poisoning - The Next Generation, http://www.secureworks.com/research/articles/other_articles/dns-cache-poisoning/, kolovoz 2007.

[10] Bob Halley: How DNS cache poisoning works, http://www.networkworld.com/news/tech/2008/102008-tech-update.html, listopad 2008