1.1 Protokol DNS

IMUNES

Učitajte mrežu *DNS+Mail+WEB/NETWORK.imn* i analizirajte njenu topologiju. Za izradu vježbe morate na odgovarajućim računalima pokrenuti DNS poslužitelje. To ćete obaviti u sljedećim koracima:

1. Nakon što učitate mrežu, pokrenite emulaciju.
2. U konzoli (*xterm*) računala na kojem je pokrenut *IMUNES*, pozicionirajte se u direktorij *DNS+Mail+WEB*:

```
FreeBSD7# cd /root/Examples/DNS+Mail+WEB/
```

3. Pokrenite DNS poslužitelje naredbom:

```
FreeBSD7# ./start_dns
```

Naredbom `./start_dns` konfigurirat će se odgovarajući poslužitelji i klijenti u mreži.

Kako bi se osiguralo da su u alatu *Wireshark* uhvaćeni svi relevantni prometni segmenti, treba uključiti opciju `Update packets in real time` prilikom snimanja prometa. Osim toga, kako bi se jasnije vidjelo koja se vrata koriste kod prijenosa, treba isključiti opciju `Enable transport name resolution`.

Koja je uloga protokola DNS (*Domain Name System*)? Analizirajte ponašanje protokola kroz sljedeći primjer:

1. Otvorite konzolu na računalu *pc.zpm.fer.hr*.
2. Pokrenite snimanje prometa na računalu *dnsZpm.zpm.fer.hr*.
3. Pomoću naredbe *host* (za detaljnije upute kako se koristi naredba *host*, izvršite naredbu *man host* ili pogledajte primjere korištenja ispod), iz konzole na računalu *pc.zpm.fer.hr*, saznajte:
   a) IP adresu računala *mm.tel.fer.hr*. 10.0.9.4 /host mm.tel.fer.hr
   b) IP adresu računala *dnsHr.hr*. 10.0.6.2,
   c) koje računalo je nadležno za primanje pošte na domeni *zpm.fer.hr*. zpmMail.zpm.
   d) koje računalo je nadležno za primanje pošte na domeni *tel.fer.hr*. www.tel.fer.fer.hr
   e) koji su DNS poslužitelji nadležni za domenu *hr*. dns Hr. hr
   f) koji su DNS poslužitelji nadležni za domenu *fer.hr*. dns Fer. fer. hr
   g) koji su DNS poslužitelji nadležni za domenu *tel.fer.hr*. dns Tel. tel. fer. hr
   h) koji su DNS poslužitelji nadležni za vršnu domenu ("."). a Route Server
   i) ime računala s IP adresom 10.0.9.4. c Route Server
   www.tel.fer.hr b Route Server

Kakav se mrežni promet generira prilikom izvršavanja prethodnih naredbi? Obratite pozornost na računala koja izmjenjuju poruke te "smjerove" tih

DNS upiti.

dusZpm.zpm.fer.hr odmosno nadležni dus poslužitelj

poruka. Tko odgovara na DNS upite klijenta? Skicirajte tok DNS upita i DNS odgovora za zadatak 3d).

Naredba	Značenje naredbe
`host -t A mm.tel.fer.hr`	traži se IP adresa računala za koje je zadano njegovo ime
`host -t MX tel.fer.hr`	traži se računalo nadležno za primanje pošte
`host -t NS fer.hr`	traži se nadležni DNS poslužitelj
`host -t PTR 10.0.0.1`	traži se ime računala za koje je zadana njegova IP adresa

4. Što su to vršni poslužitelji i koja je njihova uloga?
5. Koji se transportni protokol koristi za slanje DNS upita i DNS odgovora? Koja se vrata pritom koriste?
6. Na temelju upita i odgovora koje razmjenjuju, ustanovite koji DNS poslužitelji rade u iterativnom načinu rada, a koji u rekurzivnom.

10.0.10.3 → 10.0.10.2 Standard query MX tel.fer.hr

10.0.10.2 → 10.0.10.3 Standard query response MX 10 www.tel.fer.hr

4. Vršni poslužitelji se nalaze na vrhu stabla DNS hijerarhije i uloga im je upravljanje vršnim domenama.

5. DNS protokol, vrata 53

6. Iterativni = dus-Tel, dus Zpm
Rekurzivni = dusCom, dusHr, dus Org, dus Fer

1.2 Protokoli elektroničke pošte

IMUNES

Prije nego što započnete s proučavanjem protokola za slanje (SMTP) odnosno primanje (POP) elektroničke pošte, morate na odgovarajućim računalima konfigurirati SMTP i POP poslužitelje. To ćete obaviti u sljedećim koracima:

1. U konzoli (*xterm*) računala na kojem je pokrenut simulator IMUNES, provjerite da li se nalazite u direktoriju *DNS+Mail+WEB*:

```
FreeBSD7# pwd
```

2. Iz direktorija *DNS+Mail+WEB* pokrenite SMTP i POP poslužitelje naredbom:

```
FreeBSD7# ./start_mail
```

Naredbom `./start_mail` konfigurirat će se odgovarajući poslužitelji i klijenti u mreži.

1.2.1 Protokol SMTP

Protokol SMTP (*Simple Mail Transfer Protocol*) definira postupak razmjene poruka elektroničke pošte između dva udaljena računala. Svi podaci se, u toku prijenosa pošte s jednog na drugo računalo, prenose u ASCII obliku, a sastoje se od niza naredbi te samog sadržaja poruke. Analizirajte rad protokola kroz sljedeći primjer:

IMUNES

1. Otvorite konzolu na računalu *mm*. U konzoli se pozicionirajte u direktorij *DNS+Mail+WEB* (naredba: `cd /root/Examples/DNS+Mail+WEB/`).
2. Pokrenite snimanje prometa na mrežnim sučeljima računala *mm* i *www*.
3. Iz konzole računala *mm*, koristeći program *cone* (naredba *man cone* daje detaljnije informacije), pošaljite poruku korisniku na adresu *imunes@zpm.fer.hr*.

   Izvršite naredbu:

```
[root@mm ~/Examples/DNS+Mail+WEB]# cone -c cone.tel
```

   Na tipkovnici odaberite tipku *M* (koja odgovara pozivu glavnog izbornika programa), a zatim tipku *W* (koja odgovara odabiru opcije za sastavljanje nove elektroničke poruke). Nakon što popunite potrebna zaglavlja (*To* i *Subject*) te napišete poruku, istu šaljete odabirom kombinacije tipki *Ctrl* i *X*.

4. Zaustavite snimanje prometa, te pomoću prikaza snimljenog u alatu *Wireshark* odgovorite na sljedeća pitanja:
   a) Koji su se protokoli pojavili kao rezultat slanja elektroničke poruke? Koja je njihova osnovna uloga? standardna
   b) Koji su koraci prilikom slanja elektroničke poruke s računala *mm* na adresu *imunes@zpm.fer.hr*?

DNS, SMTP, TCP

DNS-ov radi' server, uspostavi' logičku vezu TCP i SMTP-om pošalji' email

c) Gdje se sve koristi protokol DNS u ovom slučaju? Za upit o imenu odredi
- Koje računalo je nadležni poslužitelj elektroničke pošte za domenu *tel.fer.hr*? Kako računalo *mm* saznaje IP adresu tog poslužitelja?
- Koje računalo je nadležni poslužitelj elektroničke pošte za domenu *zpm.fer.hr*? Kako računalo *www* saznaje IP adresu tog poslužitelja?

d) Koliko se (TCP) konekcija uspostavlja u ovom primjeru i koja se vrata pritom koriste? Odaberite opciju *Statistics* → *Conversation List* → *TCP (IPv4 & IPv6)* u izbornoj traci alata. Čemu služe te konekcije?

e) Pronađite TCP segment kojim započinje uspostava konekcije s računala *mm* prema njegovom nadležnom SMTP poslužitelju. Označite ga, zatim pritisnite desnu tipku miša te odaberite opciju *Follow TCP stream*. Kako teče komunikacija protokolom SMTP između tog računala i njegovog nadležnog poslužitelja? Pronađite segment u kojem se prenosi sadržaj elektroničke poruke.

1.2.2 Protokol POP

Protokol POP (*Post Office Protocol*) definira postupak pristupa elektroničkoj pošti koja je pohranjena u poštanskom sandučiću na POP poslužitelju. Svi podaci se prenose u ASCII obliku, a sastoje se od niza naredbi te samog sadržaja poruke. Analizirajte rad protokola kroz sljedeći primjer:

IMUNES

1. U prethodnom zadatku poslana je elektronička poruka na adresu *imunes@zpm.fer.hr*. Otvorite konzolu na računalu *pc*. U konzoli se pozicionirajte u direktorij *DNS+Mail+WEB* (naredba: `cd /root/Examples/DNS+Mail+WEB/`).
2. Pokrenite snimanje prometa na mrežnom sučelju računala *pc*.
3. Iz konzole računala *pc*, korištenjem programa *cone*, pristupite POP poslužitelju na računalu *zpmMail* kako bi pročitali pristiglu poruku.

   Izvršite naredbu:

   ```
   [root@pc ~/Examples/DNS+Mail+WEB]# cone -c cone.zpm
   ```

   Nakon izvršavanja naredbe, odaberite opciju *imunes@zpm.fer.hr:*, kojom se otvara poštanski sandučić. Koristite lozinku *imunes*. Otvorite pristiglu poruku.
4. Zaustavite snimanje prometa, te pomoću prikaza snimljenog u alatu *Wireshark* odgovorite na sljedeća pitanja:

   a) Koji su se protokoli pojavili kao rezultat pristupanja elektroničkoj pošti na POP poslužitelju računala *zpmMail*?

   b) Koliko se (TCP) konekcija uspostavlja u ovom primjeru i koja se vrata pritom koriste?

   c) Za što se koristi protokol DNS u ovom slučaju?

   d) Pronađite TCP segment kojim započinje uspostava konekcije s računala *pc* prema njegovom nadležnom POP poslužitelju. Označite ga, zatim

Autorizira se user pa se šalje poruka

root@mm.tel.fer.hr
www.tel.fer.hr
ZpmMail.zpm.fer.hr
imunes@zpm.fer.hr

pritisnite desnu tipku miša te odaberite opciju *Follow TCP stream*. Kako teče razmjena POP poruka između računala *pc* i njegovog nadležnog poslužitelja? Čemu služe POP poruke LIST i RETR? Analizirajte njihove odgovore.

e) Pogledajte sadržaj elektroničke poruke i analizirajte polja *Received*. Kojim "putem" je poruka došla na poslužitelj *zpmMail*?

f) Je li komunikacija između ovih računala šifrirana? Analizirajte slanje segmenata koji se odnose na prijenos lozinke.

Nije šifrirana!

preuzima ih

prebrojava poruke i veličin u oktetima

1.3 Protokol HTTP

HTTP (*HyperText Transfer Protocol*) je aplikacijski protokol koji definira uslugu prijenosa Web sadržaja između računala. Izvorno je HTTP bio namijenjen za prijenos tzv. hiperteksta, ali danas ima gotovo univerzalnu primjenu - koristi se za prijenos datoteka (umjesto protokola FTP), kod usluga prilagođenih Webu (npr. Web-mail) i slično.

IMUNES

Kako bi ubrzali rad, prekinite emulaciju iz prethodnih zadataka, pa ju ponovno pokrenite. Nakon što pokrenete emulaciju, naredbom `./start_dns` učitajte DNS konfiguraciju mreže. HTTP (Web) poslužitelje nije potrebno pokretati iz konzole, jer je mreža *DNS+Mail+WEB/NETWORK.imn* tako konfigurirana da se HTTP poslužitelji pokreću tijekom inicijalizacije same emulacije:

1. U konzoli (*xterm*) računala na kojem je pokrenut IMUNES, provjerite da li se nalazite u direktoriju *DNS+Mail+WEB*:

   ```
   FreeBSD7# pwd
   ```

2. Pokrenite DNS poslužitelje naredbom:

   ```
   FreeBSD7# ./start_dns
   ```

Analizirajte rad protokola HTTP kroz sljedeći primjer:

1. Pokrenite snimanje prometa na mrežnom sučelju računala *pc*.
2. Odaberite računalo *pc*, desnom tipkom miša otvorite izbornik, te pokrenite web preglednik *Opera* (*Opera Browser*). Odaberite opciju *Tools → Delete private data...* u izbornoj traci preglednika kako bi obrisali njegovo priručno spremište.

   Otvorite početnu stranicu web sjedišta na poslužitelju *www.tel.fer.hr* (Zavod za telekomunikacije) upisivanjem URI-a *http://www.tel.fer.hr*. Otvorite početnu stranicu web poslužitelja *www.zpm.fer.hr* (*zpmMail*) korištenjem poveznice/hiperveze Link on ZPM. Nakon toga, vratite se na početnu web stranicu Zavoda za telekomunikacije (poveznica Link on ZZT).
3. Zaustavite snimanje prometa, te pomoću prikaza snimljenog u alatu *Wireshark* odgovorite na sljedeća pitanja:

   a) Koji su se sve protokoli pojavili kao rezultat akcija iz prethodnog koraka? HTTP, TCP, ARP, DNS
   b) Koja je uloga protokola DNS u ovom slučaju? provlačak pojedinih stranic
   c) Koji se transportni protokol koristi za HTTP? TCP — mjerenih IP adresa
   d) Koliko se HTTP konekcija uspostavi u ovom primjeru? Odaberite opciju *Statistics → Conversation List → TCP (IPv4 & IPv6)* u izbornoj traci

   broj konekcija služe za spajanje sa serverima u kojima se nalaze stranice

alata. Čemu služe te konekcije? Odredite transportne adrese u svakoj od njih.

e) Pronađite segment koji pripada jednoj HTTP konekciji. Označite ga, zatim pritisnite desnu tipku miša te odaberite opciju *Follow TCP stream.* Kako izgledaju poruke koje su razmijenjene prilikom dohvaćanja sadržaja s ovih web poslužitelja? Čemu služe HTTP poruke GET, 200 OK i 404 Not Found?

f) Zašto se, prilikom odabira poveznice Link on ZZT, nije stvorila (nova) HTTP konekcija, koja bi dohvatila početnu web stranicu poslužitelja *www.tel.fer.hr*?

GET - podaci tražene stranice

200 OK
- prolaz uspješnog odgovora sa servera, sa traženim podacima

404 NOT FOUND
- server nemože naći tražene informacije

f) prilikom prolaska na zpm.~~fer~~.tel.fer.hr odobrava se "Connection: keepAlive, TE" koja je održala TCP konekciju na tel.fer.hr