3.Laboratorijska vježba

Boris Boronjek, JMBAG:0036531473

34. Proučite primjer DHCP/DHCP.imn (Slika 5.1). Svrha ovog primjera je pokazati kako se računalima dinamički dodjeljuje IP-adresa. Scenarij vježbe je sljedeći: 1. Započnite simulaciju. 2. Kroz konzolu (Applications Menu -> Terminal Emulator) računala na kojem je pokrenut IMUNES (dakle, konzolu operacijskog sustava FreeBSD) pozicionirajte se u direktorij /root/imunes-examples/DHCP/ te izvršite skriptu start_dhcp: # ./start_dhcp Skripta podešava odgovarajuće klijente i poslužitelje za ovaj primjer. 3. Otvorite konzolu na računalu pc3 te pokrenite alat Wireshark tako da snima mrežni promet na mrežnom sučelju računala. 4. U konzoli na računalu pc3 izvršite naredbu: # dhclient eth0 Ovom naredbom se za mrežno sučelje eth0 računala pc3 zahtijeva od DHCP-poslužitelja dodjela IP-adrese. 5. Provjerite je li računalu pc3 dodijeljena IP-adresa (naredba ifconfig eth0). 6. Zaustavite snimanje mrežnog prometa te, pomoću prikaza snimljenog u alatu Wireshark, proučite proces dobivanja IP-adrese od DHCP-poslužitelja i identificirajte pripadajuće DHCP-poruke. Skicirajte tijek razmjene DHCP-poruka, uz navođenje pripadajućih izvorišnih i odredišnih MAC-adresa i IP-adresa.

IP source	IP destination	MAC source	MAC destination	Protocol	Info
0.0.0.0	255.255.255.255	42:00:AA:00:00:02	FF:FF:FF:FF:FF:FF	DHCP	DHCP Discover
10.0.0.1	10.0.0.12	42:00:AA:00:00:03	42:00:AA:00:00:02	DHCP	DHCP Offer
0.0.0.0	255.255.255.255	42:00:AA:00:00:02	FF:FF:FF:FF:FF:FF	DHCP	DHCP Request
10.0.0.1	10.0.0.12	42:00:AA:00:00:03	42:00:AA:00:00:02	DHCP	DHCP ACK

35. Koristeći naredbu host u konzoli računala pc.zpm.fer.hr saznajte: a. IP-adresu računala dnsHr.hr, b. koje računalo je nadležno za primanje pošte u domeni zpm.fer.hr, c. koje računalo je nadležno za primanje pošte u domeni tel.fer.hr, d. koji su DNS-poslužitelji nadležni za domenu hr, e. koji su DNS-poslužitelji nadležni za domenu fer.hr, f. koji su DNS-poslužitelji nadležni za domenu tel.fer.hr, g. koji su DNS-poslužitelji nadležni za vršnu domenu („.“) i h. ime računala s IP-adresom 20.0.0.4.

a) 7.0.0.2 (host -t A dnsHr.hr)

b) 10 zpmMail.zpm.fer.hr (host -t MX zpm.fer.hr)

c) 10 www.tel.fer.hr (host -t MX tel.fer.hr)

d) dns2.com; dnsHr.hr (host -t NS hr)

e) dnsFer.fer.hr (host -t NS fer.hr)

f) dnsTel.tel.fer.hr (host -t NS tel.fer.hr)

g) cRootServer; bRootServer; aRootServer (host -t NS .)

h) mm.tel.fer.hr (host -t PTR 20.0.0.4)

36. Kakav se mrežni promet generira prilikom izvršavanja prethodnih naredbi? Skicirajte i obrazložite slijed DNS-upita i DNS-odgovora za zadatak 35.c. Izmjenjuju li se DNS-poruke s vršnim DNS-poslužiteljem? Objasnite.

Source	Destination	Protocol	Info
30.0.0.3	30.0.0.2	DNS	Standard query 0xb612 MX tel.fer.hr
30.0.0.2	30.0.0.3	DNS	Standard qeury response 0xb612 MX tel.fer.hr MX 10 www.tel.fer.hr

Kada prvi put izvedem naredbu host -t MX tel.fer.hr DNS-poruke se izmjenjuju s vršnim DNS-poslužiteljem. Kada bi istu naredbu izveo drugi puta DNS-poruke se ne bi izmjenjivale s DNS-poslužiteljem jer lokalni server već ima pohranjene te podatke.

37. Analizirajte korištena UDP-vrata za scenarij iz zadatka 35.g.

Korištena vrata iz zadatka 35.g su 53 i 12640

38. Analizirajte rad protokola SMTP kroz sljedeći scenarij: 1. Pokrenite snimanje mrežnog prometa na mrežnim sučeljima eth0 računala mm i www. 2. Na računalu mm konfigurirajte klijentsku aplikaciju elektroničke pošte. Desnim klikom miša nad računalom mm odaberite opciju Mail client, čime se automatski pokreće klijentska aplikacija Sylpheed. Potom, u dijalogu Mailbox setting odaberite opciju Create mailbox at the following default location i pritisnite tipku OK. U sljedećem koraku odaberite opciju POP3 i pritisnite tipku Forward. Nakon toga, u polje Display name upišite svoje ime, a u polje E-mail address adresu root@tel.fer.hr, te pritisnite tipku Forward. Nakon toga, u polje User ID upišite root, te u polja POP3 server i SMTP server upišite adresu pretpostavljenog mail poslužitelja (u ovom slučaju to je poslužitelj www.tel.fer.hr). Ostale postavke ostavite nepromijenjene te pritisnite tipku Forward, a potom i Close. 3. U grafičkom sučelju aplikacije Sylpheed sastavite novu poruku elektroničke pošte proizvoljnog sadržaja (opcija Compose), te poruku pošaljite na adresu imunes@zpm.fer.hr. 4. Zaustavite snimanje mrežnog 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? Navedite kojem sloju TCP/IP-modela pripada svaki od tih protokola. b. Koji su koraci prilikom slanja elektroničke poruke s računala mm na adresu imunes@zpm.fer.hr? Obratite pozornost na primjenu sustava DNS i protokola SMTP. c. Gdje se sve koristi protokol DNS u ovom slučaju? 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 → Conversations → TCP u izbornoj traci alata Wireshark. Čemu služe te konekcije? e. Pronađite TCP-segment kojim započinje uspostava konekcije s računala mm prema njegovom nadležnom SMTP-poslužitelju. Označite ga, zatim pritisnite opciju Follow Stream. Kako teče komunikacija protokolom SMTP između tog računala i njegovog nadležnog poslužitelja? Skicirajte dobiveni tijek poruka. Pronađite segment u kojem se prenosi sadržaj elektroničke poruke.

a) Pojavili se se protokoli ARP, TCP, SMTP i DNS. ARP pripada sloju podatkovne poveznice i služi za pretvaranje IP adrese u MAC adresu i obratno. TCP pripada transportnom sloju i služi za prijenos podataka. SMTP pripada aplikacijskom sloju i služi za slanje elektroničke pošte između računala. DNS pripada aplikacijskom sloju i služi za pretvaranje IP adresa u imena računala i obratno.

b) mm šalje ARP zahtjev kako bi pronašao MAC adresu svojeg nadležnog DNS poslužitelja. Nakon što sazna MAC adresu DNS poslužitelja uspostavlja se TCP veza, te se SMTP protokolom prenosi poruka. Nakon slanja poruke prekida se TCP veza.

c) DNS se koristi kako bi dobili ip adresu www.tel.fer.hr. Nadležni poslužitelj elektroničke pošte za domenu tel.fer.hr je www.tel.fer.hr, a računalo mm to saznaje DNS protokolom. Nadležni poslužitelj elektroničke pošte za domenu zpm.fer.hr je zpmMail.zpm.fer.hr, a računalo mm to također saznaje DNS protokolom.

d) uspostavljaju se dvije TCP konekcije. Između računala mm i njegovog nadležnog DNS poslužitelja računala www koriste se vrata 25 i 36659, a između DNS poslužitelja www i zpmMail se koriste vrata 25 i 56687.

e)

```
220 www.tel.fer.hr ESMTP Postfix (3.3.4)
HELO mm.tel.fer.hr
250 www.tel.fer.hr
MAIL FROM:<root@tel.fer.hr>
250 2.1.0 Ok
RCPT TO:<imunes@zpm.fer.hr>
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
Date: Wed, 24 May 2023 18:36:07 +0000
From: Boris <root@tel.fer.hr>
To: imunes@zpm.fer.hr
Subject: Hello
Message-Id: <20230524183607.128eb0ee10f1a3313ad4f5a8@tel.fer.hr>
X-Mailer: Sylpheed 3.7.0 (GTK+ 2.24.32; i386-portbld-freebsd11.2)
Mime-Version: 1.0
Content-Type: text/plain; charset=US-ASCII
Content-Transfer-Encoding: 7bit

Hello world!
.
250 2.0.0 Ok: queued as A2E00773EB
QUIT
221 2.0.0 Bye
```

39. Analizirajte rad protokola POP kroz sljedeći scenarij: 1. Pokrenite snimanje mrežnog prometa na mrežnom sučelju eth0 računala pc. 2. Na računalu pc konfigurirajte klijentsku aplikaciju elektroničke pošte. Desnim klikom miša nad računalom pc odaberite opciju Mail client, čime se automatski pokreće klijentska aplikacija Sylpheed. Potom, u dijalogu Mailbox setting odaberite opciju Create mailbox at the following default location i pritisnite tipku OK. U sljedećem koraku odaberite opciju POP3 i pritisnite tipku Forward. Nakon toga, u polje Display V. Podobnik, O. Dobrijević, T. Grgić, K. Ivešić: Internetski protokoli u primjeni (inačica udžbenika v1.4) 94 V. Podobnik, O. Dobrijević, T. Grgić, K. Ivešić: Internetski protokoli u primjeni (inačica udžbenika v1.4) name upišite ime svog asistenta, a u polje E-mail address adresu imunes@zpm.fer.hr, te pritisnite tipku Forward. Nakon toga, u polje User ID upišite imunes, te u polja POP3 server i SMTP server upišite adresu pretpostavljenog mail poslužitelja (u ovom slučaju to je poslužitelj zpmMail.zpm.fer.hr). Ostale postavke ostavite nepromijenjene te pritisnite tipku Forward, a potom i Close. 3. U grafičkom sučelju aplikacije Sylpheed pristupite POP-poslužitelju na računalu zpmMail kako bi pročitali pristiglu poruku. To napravite tako da pritisnete opciju Get all u grafičkom sučelju, u ponuđenom izborniku upišete lozinku imunes, te pritisnete tipku OK. Otvorite pristiglu poruku. 4. Zaustavite snimanje mrežnog 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? Navedite kojem sloju TCP/IP-modela pripada svaki od tih protokola. 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 i odaberite opciju Follow Stream. Kako teče razmjena POP-poruka između računala pc i njegovog nadležnog poslužitelja? Skicirajte dobiveni tijek poruka. Čemu služe POP-poruke LIST i RETR? Analizirajte njihove odgovore. e. Pogledajte sadržaj elektroničke poruke i analizirajte polja Received. Kojim „putem“ je poruka stigla na poslužitelj zpmMail? f. Je li komunikacija između ovih računala šifrirana? Analizirajte slanje segmenata koji se odnose na prijenos lozinke.

a) Pojavili su se protokoli DNS, ARP, TCP i POP. ARP pripada sloju podatkovne poveznice. TCP pripada transportnom sloju. POP i DNS pripadaju aplikacijskom sloju

b) Uspostavlja se jedna TCP-konekcija. Koriste se vrata 33856 i 110.

c) DNS se koristi kako bi pc saznao ip adresu servera zpmMail.zpm.fer.hr

d)

```
+OK
USER imunes
+OK
PASS imunes
+OK
STAT
+OK 1 863
UIDL
+OK
1 f1ac223b1cb13c8a8025a9ffccb174bb
.
LIST
+OK
1 863
.
RETR 1
+OK
From root@tel.fer.hr  Wed May 24 18:36:09 2023
Return-Path: <root@tel.fer.hr>
X-Original-To: imunes@zpm.fer.hr
Delivered-To: imunes@zpm.fer.hr
Received: from www.tel.fer.hr (www.tel.fer.hr [20.0.0.3])
          by zpmMail.zpm.fer.hr (Postfix) with ESMTP id 7B92B7759B
          for <imunes@zpm.fer.hr>; Wed, 24 May 2023 18:36:09 +0000 (UTC)
Received: from mm.tel.fer.hr (mm.tel.fer.hr [20.0.0.4])
          by www.tel.fer.hr (Postfix) with SMTP id A2E00773EB
          for <imunes@zpm.fer.hr>; Wed, 24 May 2023 18:36:07 +0000 (UTC)
Date: Wed, 24 May 2023 18:36:07 +0000
From: Boris <root@tel.fer.hr>
To: imunes@zpm.fer.hr
Subject: Hello
Message-Id: <20230524183607.128eb0ee10f1a3313ad4f5a8@tel.fer.hr>
X-Mailer: Sylpheed 3.7.0 (GTK+ 2.24.32; i386-portbld-freebsd11.2)
Mime-Version: 1.0
Content-Type: text/plain; charset=US-ASCII
Content-Transfer-Encoding: 7bit

Hello world!


.
QUIT
+OK
```

LIST se koristi za dobivanje popisa poruka dostupnih na poslužitelju

RETR preuzima poruku s poslužitelja na lokalni uređaj

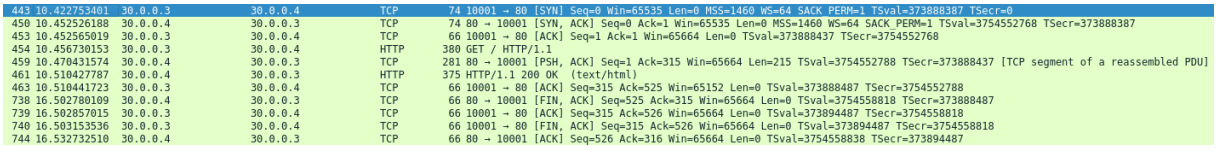
e) mm -> www -> zpmMail -> pc

f) Poruka nije šifrirana jer se u poruci vidi da je lozinka poslana u izvornom obliku

40. Otvorite početnu stranicu web poslužitelja www.zpm.fer.hr (zpmMail) korištenjem URI-a http://www.zpm.fer.hr. Koliko se HTTP-konekcija uspostavi u ovom primjeru? Čemu služe te konekcije? Odredite transportne adrese za svaku od tih konekcija.

Uspostavilo se 3 HTTP konekcije. Transportne adrese su 30.0.0.3(pc) i 30.0.0.4(www.zpm.fer.hr). Prva konekcija šalje zahtjev za početnu stranicu www.zpm.fer.hr. Druga konekcija šalje zahtjev za sliku powerlogo.gif. Treća konekcija šalje zahtjev za sliku favicon.ico, ali ta slika nije pronađena.

41. Proizvoljno odaberite jedan HTTPzahtjev i jedan HTTP-odgovor, skicirajte ih te utvrdite njihove karakteristične dijelove.

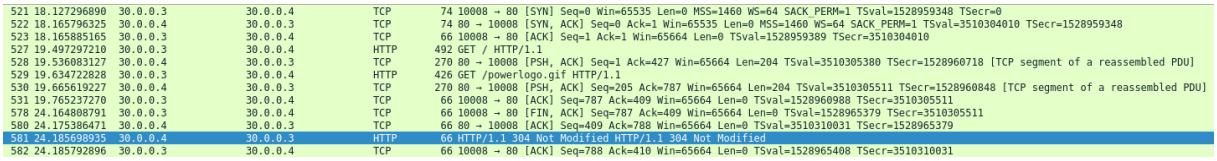


Paketi 443, 450 i 453 govore o uspostavi veze

Paketi 454, 459, 461 i 463 govore o dohvaćanju početne stranice www.zpm.fer.hr

Paketi 738, 739, 740 i 744 govore o prekidu veze.

42. U programu Firefox pokrenutom na računalu pc pristupite URI-ju http://www.tel.fer.hr te odaberite poveznicu „Link on ZPM“. Kada se učita nova stranica, odaberite poveznicu „Link on ZZT“ čime ćete se vratiti na stranicu Zavoda za telekomunikacije (http://www.tel.fer.hr). Proučite poruke protokola HTTP koje će se pojaviti u alatu Wireshark nakon odabira poveznice „Link on ZZT“, te skicirajte njihov tijek. Koja je uloga parametra If-Modified-Since u zaglavlju prvog HTTP-zahtjeva koji se pojavio nakon odabira poveznice „Link on ZZT“? Zašto je tijelo poruke prvog HTTP-odgovora koji se pojavio nakon odabira iste poveznice prazno?



Parametar If-Modified-Since prepoznaje ako se dogodila promjena na zadanoj stranici od posljednjeg posjeta. Tijelo poruke prvog HTTP odgovora je prazno jer se ništa nije promjenilo na stranici http://www.tel.fer.hr od zadnjeg posjeta te stranice.