

### 33) DHCP / DHCP.imn

2.) #cd /root/immunes-examples/DHCP/

#./start-dhcp

4.) konzola pc3 → #dhclient eth0

- ovom naredbom se za mrežnu sučelje eth0 računala pc3 zahtjeva od DHCP-poslužitelja dodela IP-adrese

5.) ifconfig eth0

6)

src	dest	protocol	info
0.0.0.0	255.255.255.255	DHCP	DHCP Discover
10.0.0.1	10.0.0.12 (pc3)	DHCP	DHCP Offer
0.0.0.0	255.255.255.255	DHCP	DHCP Request
10.0.0.1	10.0.0.12 (pc3)	DHCP	DHCP ACK

→ MAC-adresa!

DHCP Discover: poslan od strane računala pc3 s izvišnom adresom 0.0.0.0 (jer računalo tek treba dobiti adresu) i određivanom adresom postavljenom na broadcast adresu 255.255.255.255. Računalo pc3 adresira sve uređaje jer ne zna adresu DHCP-poslužitelja.

DHCP Offer: DHCP-poslužitelj šalje ponudenu IP adresu, podatke o uadležnim DHCP-poslužiteljima, podrazumijevanom usmjerenju i mrežnoj masci.

DHCP Request: Računalo pc3 na broadcast adresu šalje zahtjev za ponudenu adresu

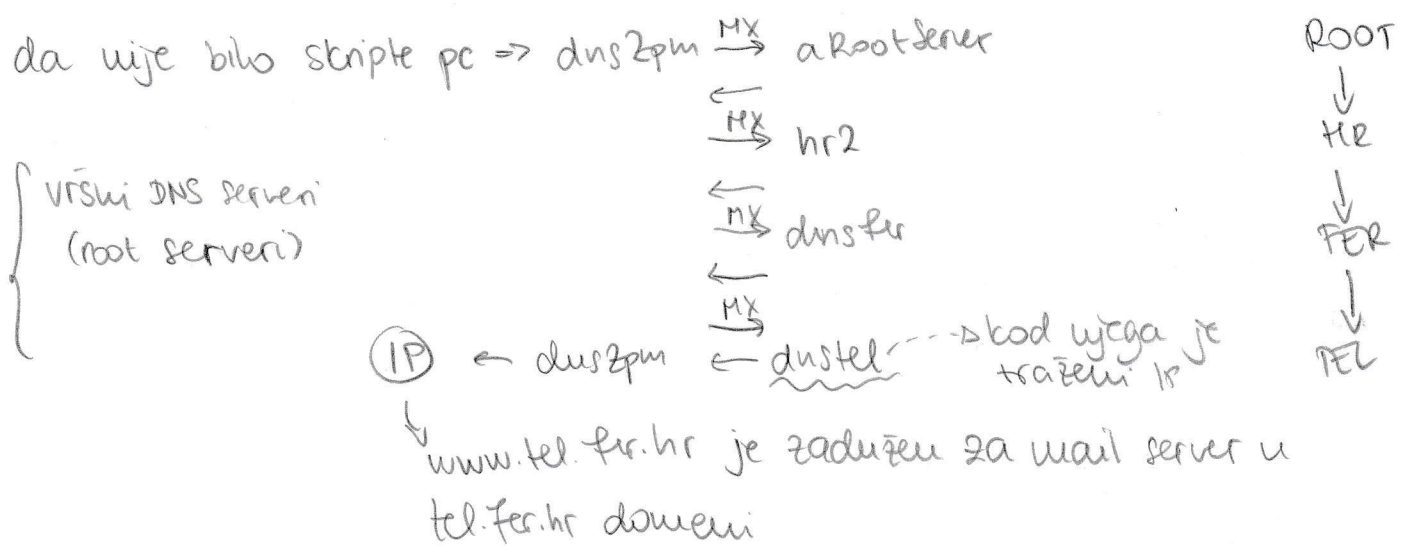
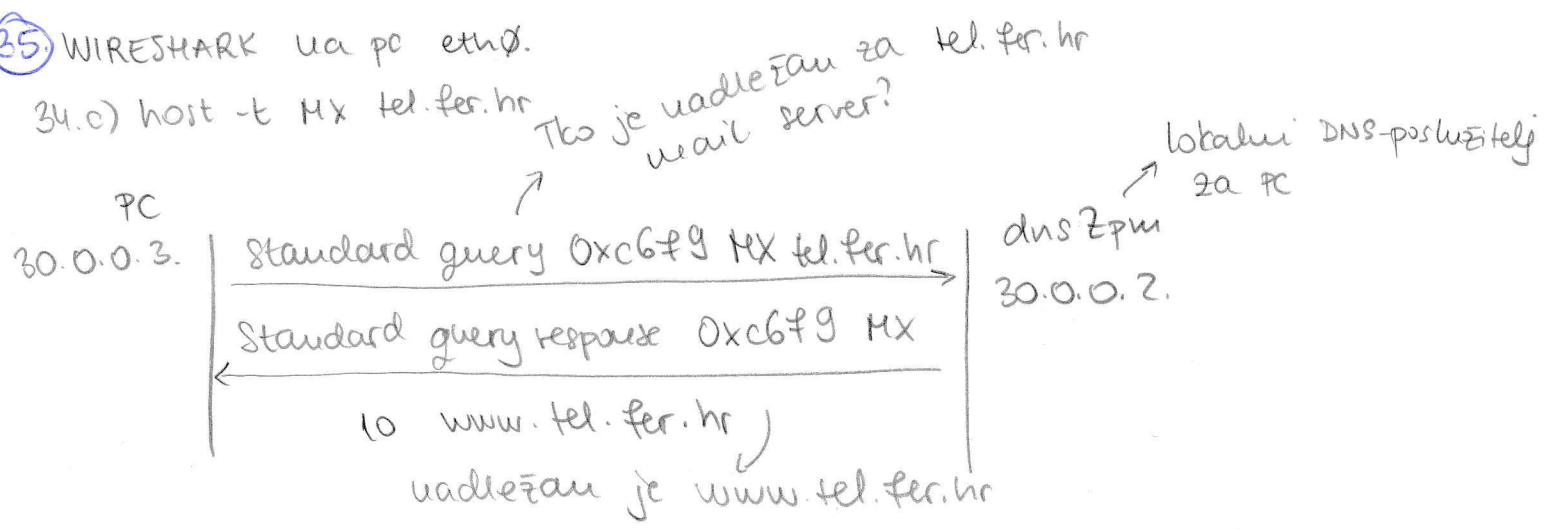
DHCP ACK: DHCP-poslužitelj odobrava zahtjev za adresu, definira vrijeme "najma" adrese, te potvrđuje podatke o podrazumijevanom usmjerenju i DNS-poslužiteljima

34) PODEŠAVANJE: 1. pokretanje simulacije  
2. Terminal (FreeBSD-a): #cd /root/Examples/DNS+Mail+WEB/  
#./start-dns

- konfiguracija odgovarajućih poslužitelja i klijenata u mreži

- a) host -t A duster.hr: 7.0.0.2.
- b) host -t MX zpm.fer.hr: zpm.fer.hr mail is handled by 10 zpmMail.zpm.fer.hr
- c) host -t MX tel.fer.hr: tel.fer.hr mail is handled by 10 www.tel.fer.hr
- d) host -t NS hr: hr name server hr2.com  
hr name server duster.hr
- e) host -t NS fer.hr: fer.hr name server dusFer.fer.hr
- f) host -t NS tel.fer.hr: tel.fer.hr name server dusTel.tel.fer.hr
- g) host -t NS.: name server cRoot Server,  
name server aRoot Server,  
name server bRoot Server.
- h) host -t PTR 20.0.0.4: 4.0.0.20. /N-ADDR.ARPA domain name pointer  
www.tel.fer.hr.

35. WIRESHARK na pc etn.



Izveli se drugi put pa ga lokalni server već ima u cache-u pa ne treba od vršnih poslužitelja krenuti tražiti rekursivno.

Kako je u DNS-poslužitelju (dnsZpm) postojao zapis o uadležnom računalu za primanje pošte, dnsZpm je odmah vratio odgovor, tako da nije bilo potrebe za iznupnim ponukom sa vršnim DNS-poslužiteljem.

36) Vrata koja se koriste u 34.g) su 53

src	dst	info
30.0.0.3	30.0.0.2	Standard query 0x4660 NS <root>
30.0.0.2	30.0.0.3	Standard query response 0x4660 NS crootserver NS arootserver NS brootserver

src port → 52819

dst port → 53 → port koji koristi DNS (u okviru UDP-a, ali može i TCP-a)

37) DNS+Mail+Web/Network.imn

PODEŠAVANJE: # cd /root/Examples/DNS+Mail+WEB/

# ./start-dns

# ./start-mail

# ./start-http

2. Mail Client → Sylpheed → Create mailbox at the following default location

→ POP3 → email: root@tel.fer.hr → USER ID: root

POP3 i SMTP server: www.tel.fer.hr

3. COMPOSE → immu@zpm.fer.hr

4. a) ARP → dobivanje MAC adresa {sloj podatkovne poveznice}

TCP → prijem informacija između dva udaljena procesa {transp. sloj}

SMTP → razmjena poruka između dva udaljena računala

IMF → header i body poruke → format poruke

DNS → IP adresa računala

b) Koraci tijekom slanja e-pošte

1. mm preko ARP-a saznaje MAC-adresu dnstel DNS poslužitelja

2. uspostavlja se TCP veza

3. SMTP poruke

4. prijem poruke TCP-om i headera i formata poruke IMFom

5. prekid TCP veze

c) protokol DNS se koristi da bi mm saznao IP adresu www.tel.fer.hr  
(20.0.0.4)

uadleri poslužitelj za domenu tel.fer.hr? www.tel.fer.hr DNS

uadleri poslužitelj za domenu zpm.fer.hr? zpmMail.zpm.fer.hr DNS

Standard query i Standard response



d) 1 TCP-konekcija (port 25)

2 poruke: - između računala mm i www.tel.fer.hr

- između računala www.tel.fer.hr i zpmMail.zpm.fer.hr

Konekcije služe za pouzdan prijem paketa (pošiljke)

e) Računalo mm uspostavlja konekciju s udaljenim SMTP poslužiteljem www. Prva poruka je 220 www.tel.fer.hr ESMTP Postfix sa sadržajem "HELO mm.tel.fer.hr" čime počinje komunikacija ova dva računala.

Druga poruka je 250 www.tel.fer.hr sa sadržajem "MAIL FROM <root@tel.fer.hr>".

Treća poruka je 250 2.1.0. OK sa sadržajem RCPT TO

<imunes@zpm.fer.hr> te se u zadnjoj poruci šalje informacije i sadržaj maila.

38) DNS+Mail+WEB/Network.imm //pop

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

# ./start-dns

# ./start-mail

# ./start-http

} terminal FreeBSD-a

1 Wireshark pc(eth0)

2. Mail Client → Sylphed → Mailbox setting → Create mailbox at the following default location → OK

POP3 → FORWARD →

Display name: ime asistenta

user ID: imunes

e-mail: imunes@zpm.fer.hr

POP3 i SMTP: zpmMail.zpm.fer.hr

→ FORWARD → CLOSE

3. Get all u grafičkom sučelju. Password: imunes

4. STOP WIRESHARK.

a) TCP - pruža spojnu uslugu transporta stoji odetla → TRANSPORTNI sloj

APLIKACIJSKI sloj { POP - protokol APLIKACIJSKOG SLOJA koji služi za dohvatanje i rukovanje porukama na poslužitelju e-pošte (port 110)

IMF - format poruke

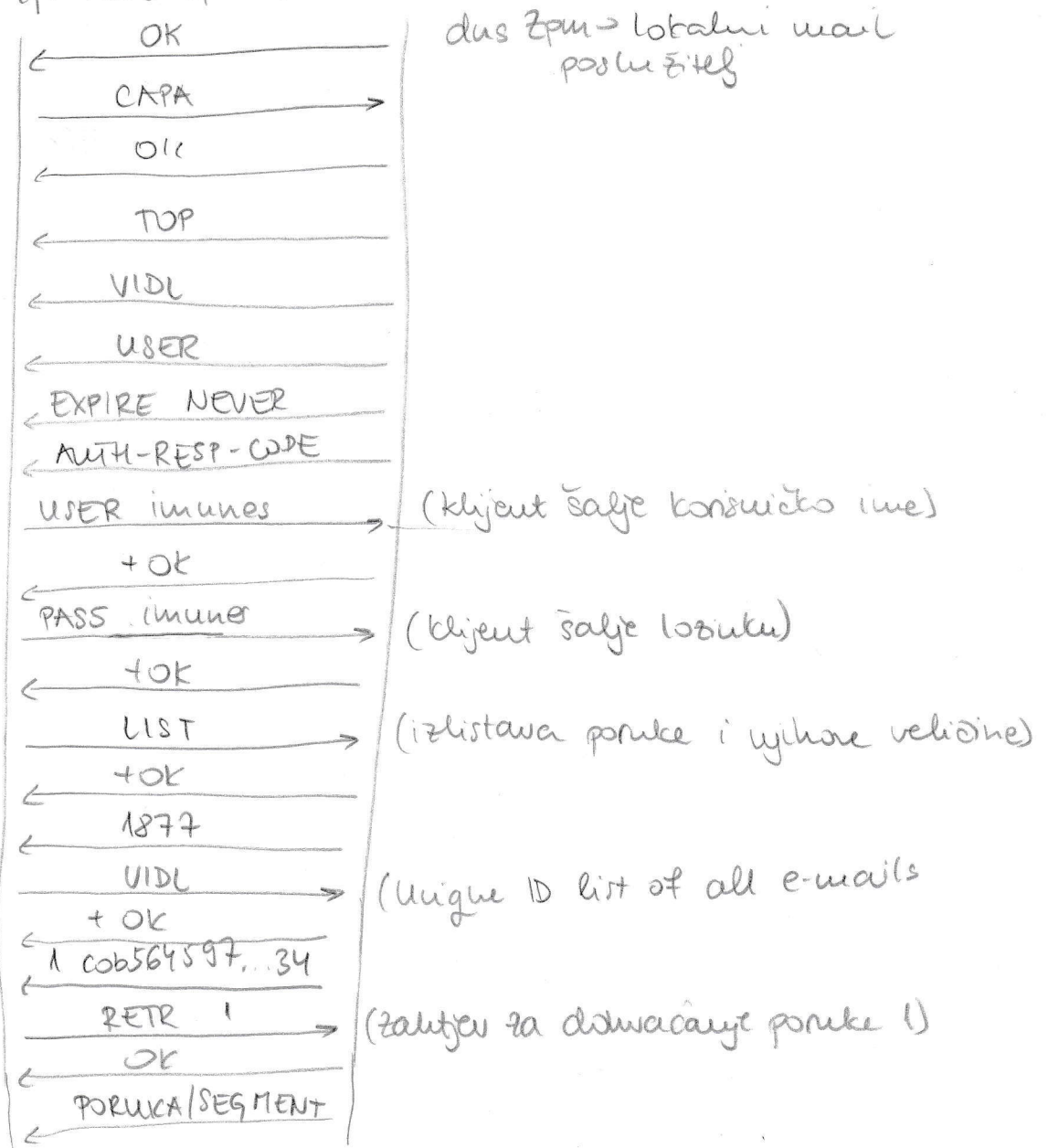
DNS - IP adresa računala

ARP - dohvatanje MAC adresa → SLOJ PODATKOVNE POVEZNICE

b) Uspostavlja se 3 TCP veze između računala s adresama 30.0.0.3 i 30.0.0.4 (110)

c) DNS se u ovom slučaju koristi za dobivanje IP adrese mail servera zpmMail.zpm.tel.hr

d) PC



e) Received from mm (unknown [30.0.0.4]) by www.tel.tel.hr (postfix) with ESMTP

for <immuner@zpm.tel.hr>

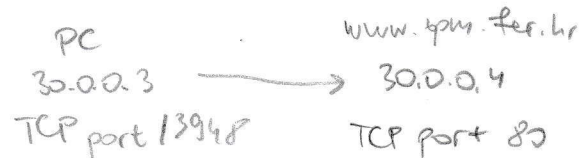
f) Nije šifrirana.

lozinka je običan niz znakova ("immuner").

39. pc konzola -> elinks

Uspostane se 3 HTTP konekcije:

1. Zahtjev za početnom stranicom servera www.zpm.tel.hr uz verziju protokola HTTP 1.1.



2. Zahtjev za slikom powerlogo.gif

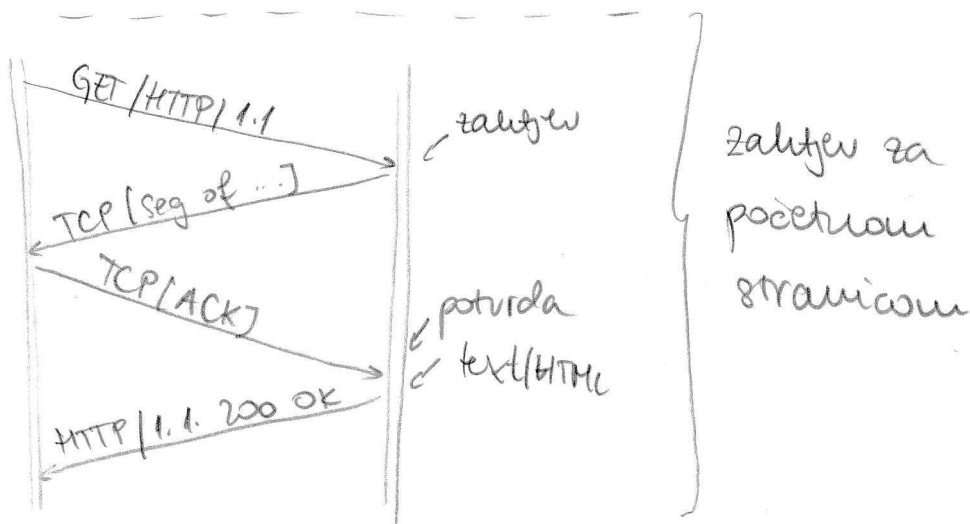
PC  
30.0.0.3 → 30.0.0.4  
TCP port 13948 TCP port 80

3. Zahtjev za slikom favicon.ico  
⇒ NEUSPJEŠNO?

(40) PC zpmMail  
30.0.0.3 30.0.0.4

TCP [SYN] →  
← TCP [SYN, ACK]  
TCP [ACK] →

} uspostava  
veze



zahtjev za powerlogo.gif  
zahtjev za favicon.ico  
zahtjev za favicon.ico

TCP [ACK] →  
TCP [FIN, ACK] →  
← TCP [ACK]

} prekid  
veze

(41) Klikom na Link on ZET uistinu se sklonile nove karteke jer browser čuva "kopiju" stranice u cacheu.

1. uspostava veze

TCP [SYN] →  
← TCP [SYN, ACK]  
TCP [ACK] →  
TCP [SYN] →  
TCP [SYN] →

← TCP [SYN, ACK]  
TCP [ACK] →  
← TCP [SYN, ACK]  
← TCP [ACK]

Nije trebao biti pokrenut protokol DNS jer je zpmMail već znao <sup>je</sup> adresu od www IP