2. kolokvij RKVB, VSS, FRI, 1. letnik, 25. 5. 2012

Ime: _____

Priimek: _____

Vpisna številka: _____

RKVB Sežana

*Pozorno preberite navodila! Literatura **ni** dovoljena. Odgovarjajte kratko (z eno, največ dvema povedima)! Čas pisanja je **45** minut. Naloge so enakovredne.*

1. Kaj so piškotki HTTP, s kakšnim namenom jih uporabljamo? Kako sploh deluje mehanizem piškotkov?

2. Kriptiranje.

a. Primerjajte simetrično in asimetrično kriptiranje.
b. Kako in za kaj uporabljamo simetrično in asimetrično kriptografijo v avtentikacijskih protokolih?
c. Koliko je tu pomembna hitrost enkripcije in dekripcije?

3. Na katero plast po ISO/OSI modelu sodijo naslednje storitve:

a. digitalni izvleček,
b. usmerjanje datagramov skozi omrežje,
c. nadzor pretoka,
d. DNS,
e. eMule.

4. Trenutna ocena RTT v neki TCP povezavi je 30 časovnih enot, ocena odmika pa 20 časovnih enot. Naslednja potrditev pride po preteku 85 časovnih enot od oddaje ustreznega segmenta.

a. Koliko je odmik trenutnega vzorca?
b. Kakšen je novi povprečni odmik?
c. Kolikšen bo interval časovne kontrole?

5. Kaj so naloge sejne plasti?

6. Pojasnite način delovanja protokola FTP. Zakaj potrebuje dve povezavi TCP in zakaj npr. HTTP tega ne potrebuje? Primerjajte delovanje FTP z delovanjem interneta (HTTP).

7. S programom Wireshark smo zajeli del seje TCP, ki je prikazan spodaj.

a. Kateri segmenti (napišite njihove številke predstavljajo) rušenje povezave TCP?
b. Katere segmente potrjuje segment številka **170**? Predpostavite, da so vsi segmenti pred 166 že potrjeni.
c. Katere segmente potrjuje segment številka **172**? Predpostavite, da so vsi segmenti pred 166 že potrjeni.
d. Koliko bajtov podatkov se prenese v segmentu številka **166**?
e. Koliko bajtov podatkov se prenese v segmentu številka **170**?

Št.	Čas	Pošiljatelj	Prejemnik	Protokol	Opis
166	25.682682	192.168.0.101	128.153.4.131	TCP	[ACK] Seq=2894 Ack=5406
167	25.731437	128.153.4.131	192.168.0.101	TCP	[ACK] Seq=5406 Ack=2938
168	25.908677	192.168.0.101	128.153.4.131	TCP	[ACK] Seq=2938 Ack=5450
169	25.964884	128.153.4.131	192.168.0.101	TCP	[ACK] Seq=5450 Ack=2938
170	25.967164	192.168.0.101	128.153.4.131	TCP	[ACK] Seq=2938 Ack=5634
171	25.968266	192.168.0.101	128.153.4.131	TCP	[FIN, ACK] Seq=2974 Ack=5634
172	26.024317	128.153.4.131	192.168.0.101	TCP	[ACK] Seq=5634 Ack=2975
173	26.031474	128.153.4.131	192.168.0.101	TCP	[FIN, ACK] Seq=5634 Ack=2975
174	26.031492	192.168.0.101	128.153.4.131	TCP	[ACK] Seq=2975 Ack=5635

8. Odgovorite na spodnja vprašanja povezana s protokolom SMTP. Pomagate si lahko s spodnjo sejo SMTP.

a. Katera dva ukaza lahko uporabimo na začetku seje SMTP?
b. Kateri ukaz označuje začetek sporočila v protokolu SMTP?
c. Kako sta pri pošiljanju e-pošte ločena glava sporočila in vsebina (jedro) sporočila?
d. Kako strežniku SMTP povemo, da je našega sporočila (e-pošte) konec?
e. Kako bi lahko k spodnjemu sporočilu dodali priponko v obliki datoteke ZIP? *Napišite kateri standard oz. algoritem bi uporabili za dodajanje priponke.*

```
220 ns.fri.uni-lj.si ESMTP Postfix (Debian/GNU)
HELO fri.uni-lj.si
250-ns.fri.uni-lj.si
MAIL FROM:<ubogi.student@gmail.com>
250 2.1.0 Ok
RCPT TO:<andrej.krevl@fri.uni-lj.si>
250 2.1.5 Ok
```

```
DATA
354 End data with <CR><LF>.<CR><LF>
From: ubogi.student@gmail.com
To: andrej.krevl@fri.uni-lj.si
Subject: Domaca naloga RK
Date: Sun, 22 May 2011 23:30:06 +0200

Ker spletna ucilnica ne deluje, vam nalogo posiljam po e-posti.

Lp,
  student.
.
250 2.0.0 Ok: queued as 9BEB98320
QUIT
221 2.0.0 Bye
```

9. S programom Wireshark smo zajeli spodnji zahtevi HTTP, ki jih prikazujeta izpis 1 in izpis 2.

a. Kakšen je tip zahteve HTTP v izpisu 1? Kakšen je tip zahteve HTTP v izpisu 2?
b. Kakšna je glavna razlika med prikazanima tipoma zahtev HTTP?
c. Kakšne je vrednost polja priimek v obeh primerih?
d. Za katero različico protokola HTTP gre v obeh primerih?
e. Kateri program (spletni brskalnik) smo uporabili za pošiljanje zahteve? *Odgovorite kar se da natančno.*

Izpis 1:
```
GET /form.php?ime=Rdeca&priimek=Kapica&poslji=Do+it%21 HTTP/1.1
Accept: image/gif, image/jpeg, image/pjpeg, image/pjpeg, application/x-shockwave-flash, */*
Accept-Language: sl
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0)
Accept-Encoding: gzip, deflate
Host: ubuntu
Connection: Keep-Alive
```

Izpis 2:
```
POST /form.php HTTP/1.1
Accept: image/gif, image/jpeg, image/pjpeg, image/pjpeg, application/x-shockwave-flash, */*
Accept-Language: sl
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0)
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Host: ubuntu
Content-Length: 40
Connection: Keep-Alive
Cache-Control: no-cache

ime=Rdeca&priimek=Kapica&poslji=Do+it%21
```

10. S programom Wireshark smo prestregli spodnji odgovor na poizvedbo DNS, odgovorite na spodnja vprašanja:

a. Po katerem tipu zapisa DNS je spraševala poizvedba?
b. Kaj pomeni/predstavlja za tip zapisa?
c. Kateri strežnik moramo vprašati, če želimo izvedeti IPv4 naslov strežnika www.google.com? Odgovorite glede na prikazan odgovor.
d. Kakšen je IPv4 naslov strežnika ns3.google.com?
e. Kaj vsebuje del odgovora, ki je poimenovan Additional records? Zakaj je ta del odgovora pomemben?

```
Domain Name System (response)
Transaction ID: 0x0002
Flags: 0x8180 (Standard query response, No error)
Questions: 1
Answer RRs: 4
Authority RRs: 0
Additional RRs: 4
Queries
  google.com: type NS, class IN
Answers
  google.com: type NS, class IN, ns ns2.google.com
  google.com: type NS, class IN, ns ns3.google.com
  google.com: type NS, class IN, ns ns4.google.com
  google.com: type NS, class IN, ns ns1.google.com
Additional records
  ns4.google.com: type A, class IN, addr 216.239.38.10
  ns3.google.com: type A, class IN, addr 216.239.36.10
  ns2.google.com: type A, class IN, addr 216.239.34.10
  ns1.google.com: type A, class IN, addr 216.239.32.10
```