Izpit RK, VŠS, FRI, 1. letnik, Ljubljana, 21. 6. 2011

Ime: _____

Priimek: _____

Vpisna številka: _____

RKVB

*Pozorno preberite navodila! Literatura **ni** dovoljena. "Plonklistki" so literatura! Uporabljate lahko preproste kalkulatorje. Čas pisanja je **60** minut. Naloge so enakovredne.*

1. S programom Wireshark smo zajeli spodnjo sejo (za prikaz smo uporabili možnost Follow TCP Stream):

```
220 mail.example.com ESMTP Postfix
HELO lrk.si
250-mail.example.com
MAIL FROM: <kapica@lrk.si>
250 2.1.0 Ok
RCPT TO: <volk@example.com>
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
From: babica@lrk.si
To: volk@example.com
Subject: Domaca naloga RK
Date: Tue, 21 Jun 2011 07:30:06 +0200

Chuck Norris FTW!
.
250 2.0.0 Ok: queued as 9BEB98320
QUIT
221 2.0.0 Bye
```

1. Za kateri protokol aplikacijske plasti gre?
2. S katerim ukazom smo »pozdravili« strežnik? Ali bi lahko uporabili tudi kak drug ukaz?
3. Kdo je pošiljatelj e-pošte?
4. Kateri naslov bo kot pošiljatelja prikazal program za e-pošto (MUA, npr. MS Outlook)?
5. Kako označimo konec sporočila?

2. S programom Wireshark smo zajeli spodnjo zahtevo (levo) in odgovor nanjo (desno):

```
Ethernet II
  Destination: 33:33:ff:00:00:01
  Source: 6c:62:6d:60:00:a8
  Type: IPv6 (0x86dd)
Internet Protocol Version 6
  Version: 6
  Traffic class: 0x00000000
  Flowlabel: 0x00000000
  Payload length: 32
  Next header: ICMPv6 (0x3a)
  Hop limit: 255
  Source: 2001:1470:fffd::155
  Destination: ff02::1:ff00:1
Internet Control Message Protocol v6
  Type: 135 (Neighbor solicitation)
  Code: 0
  Checksum: 0x34ff [correct]
  Reserved: 0 (Should always be zero)
  Target: 2001:1470:fffd::1
ICMPv6 Option (Source link-layer address)
  Type: Source link-layer address (1)
  Length: 8
  Link-layer address: 6c:62:6d:60:00:a8
```

```
Ethernet II
  Destination: 6c:62:6d:60:00:a8
  Source: 00:12:43:3b:23:ff
  Type: IPv6 (0x86dd)
Internet Protocol Version 6
  Version: 6
  Traffic class: 0x000000e0
  Flowlabel: 0x00000000
  Payload length: 32
  Next header: ICMPv6 (0x3a)
  Hop limit: 255
  Source: 2001:1470:fffd::1
  Destination: 2001:1470:fffd::155
Internet Control Message Protocol v6
  Type: 136 (Neighbor advertisement)
  Code: 0
  Checksum: 0x8fb2 [correct]
  Flags: 0xe0000000
  Target: 2001:1470:fffd::1
ICMPv6 Option (Target link-layer address)
  Type: Target link-layer address (2)
  Length: 8
  Link-layer address: 00:12:43:3b:23:ff
```

1. Del katerega protokola sta prikazana zahteva in odgovor nanjo?
2. Napišite pošiljateljev in prejemnikov naslov MAC.
3. Napišite pošiljateljev in prejemnikov naslov IPv6.
4. Kako imenujemo naslov (tip naslova) IPv6 na katerega je bila poslana zahteva?
5. Kakšna je dolžina naslova IPv6 v bajtih?

3. Za naslov **212.235.189.134/28** napišite:

1. Naslov omrežja v desetiški obliki.
2. Naslov broadcast v desetiški obliki.
3. Najmanjši naslov naprave v omrežju v desetiški obliki.
4. Največji naslov naprave v omrežju v desetiški obliki.
5. Število naprav, ki jih lahko priklopimo v to podomrežje.

4. Preučite zajete segmente in odgovorite na spodnja vprašanja:

Št	Izvorni IP	Ponorni IP	Protokol	Opis
1	10.0.0.200	10.0.0.197	TCP	1043 > 80 [SYN] Seq=0 Win=64240
2	10.0.0.197	10.0.0.200	TCP	80 > 1043 [SYN, ACK] Seq=0 Ack=1 Win=5840
3	10.0.0.200	10.0.0.197	TCP	1043 > 80 [ACK] Seq=1 Ack=1 Win=64240
4	10.0.0.200	10.0.0.197	TCP	1043 > 80 [PSH, ACK] Seq=1 Ack=1 Win=64240
5	10.0.0.200	10.0.0.197	TCP	1043 > 80 [PSH, ACK] Seq=15 Ack=1 Win=64240
6	10.0.0.197	10.0.0.200	TCP	80 > 1043 [ACK] Seq=1 Ack=15 Win=5840
7	10.0.0.197	10.0.0.200	TCP	80 > 1043 [ACK] Seq=1 Ack=17 Win=5840
8	10.0.0.200	10.0.0.197	TCP	1043 > 80 [PSH, ACK] Seq=17 Ack=1 Win=64240
9	10.0.0.197	10.0.0.200	TCP	80 > 1043 [ACK] Seq=1 Ack=19 Win=5840
10	10.0.0.197	10.0.0.200	TCP	80 > 1043 [PSH, ACK] Seq=1 Ack=19 Win=5840
11	10.0.0.197	10.0.0.200	TCP	80 > 1043 [RST] Seq=703 Ack=19 Win=5840 Len=0

1. Kateri segmenti vsebujejo rušenje povezave TCP? *Napišite številke segmentov.*
2. Katere segmente potrjuje segment številka **9**? *Napišite številke segmentov, ki jih potrjuje, ne pozabite upoštevati predhodnih potrditev!*
3. Koliko podatkov (v bajtih) se prenese v segmentu številka **4**?
4. Kakšna je najmanjša velikost sprejemnega okna, ki ga pošilja računalnik z naslovom 10.0.0.197?

5. Na katero plast po ISO OSI modelu sodijo naslednje storitve in protokoli:

a) UDP	f) usmerjanje
b)BitTorrent	g) prenos okvirjev med adapterji
c) BlueTooth	h) razdelitev segmentov med vtiči
d) ICMP	i) prenos sporočil od odjemalca do strežnika
e) RSA	j)prenos signala

6. Aplikacijska plast:

1. Naštejte tri standardne protokole aplikacijske plasti.
2. Naštejte tri nestandardne protokole aplikacijske plasti.
3. Kakšno vlogo ima polje Received v glavi SMTP sporočila? Koliko takih polj je lahko v glavi, kdo jih oblikuje? Pojasnite dinamiko (spreminjanje) tega polja v življenjski dobi SMTP sporočila.
4. V enem stavku pojasnite glavno varnostno pomanjkljivost protokola SMTP.

7. Varnost: Kako uresničujemo spodnje varnostne zahteve? Povežite pravilne trditve in tehnologije!

A) Integriteta sporočila
B) Zaupnost dolgega sporočila
C) Zaupnost kratkega sporo-čila (npr. izvlečka ali ključa)
D) Preverjanje podpisa certifikata
E) Podpis dokumenta

P)RSA + SHA-1 + RC4
q)SHA-1 + RSA
r)AES + CBC + MD5
s)SHA-256 + RSA + AES
t)DES + 3DES + AES
u)RSA
v)RSA + 3DES
z)SHA-1 + MD5
x)DES + AES + IPsec
y)SSL + SMTP
w) SSL+ UDP

1 - Kriptiranje s prejemnikovim javnim ključem
2 - Zgoščevalna funkcija + podpis izvlečka s svojim tajnim ključem
3 - Zgoščevalna funkcija + podpis izvlečka s svojim tajnim ključem + kriptiranje s prejemnikovim javnim ključem
4 - Kriptiranje s simetričnim algoritmom, prej pa pošiljanje simetričnega ključa, kriptiranega s prejemnikovim javnim ključem
5 - Zgoščevalna funkcija + kriptiranje izvlečka s sogovornikovim javnim ključem

8. Transportna plast – TCP:

1. Opišite vzpostavljanje TCP povezave.
2. Na kateri napad je občutljiv ta mehanizem?
3. Kakšen pomen ima parameter Zamašitveno okno (CongWin) pri nadzoru zamašitev?

9. Omrežna plast: v enem stavku opišite razliko med IPv4 in IPv6

1. Glede omrežnega naslova
2. Glede zagotavljanja kakovosti storitve
3. Glede fragmentacije
4. Glede preslikovanja med omrežnimi in fizičnimi naslovi.

10. Povezavna plast: skupinski prenosni medij

1. Opišite princip delovanja protokolov, ki za dostop do skupinskega prenosnega medija uporabljajo delitev medija. Naštejte nekaj (vsaj 2) protokola.
2. Ali so v takih protokolih možne kolizije in zakaj da oziroma zakaj ne?