Izpit RKVB, VSS, FRI, 1. letnik, 18. 6. 2012

Ime: _____

Priimek: _____

RKVB Ljubljana

Vpisna številka: _____

*Pozorno preberite navodila! Literatura **ni** dovoljena. Odgovarjajte kratko (z eno, največ dvema povedima)! Čas pisanja je **60** minut. Naloge so enakovredne.*

1) Kakšna je razlika med usmerjevalnikom in stikalom in v čem sta si podobna? Na kateri plasti deluje kateri od njiju?

2) Na katero plast po omrežnem modelu ISO OSI sodijo naslednje storitve, protokoli in podatki?

a) IEEE 802.11	f)piškotki
b)nadzor zamašitev	g)MIME
c) TDM in FDM	h)ICMP
d) številka vrat	i) usmerjanje
e) naslov IPv6	j) optična povezava

3) Protokol DNS:
   a. Opišite zgradbo zapisa v podatkovni bazi DNS – pomen posameznih polj.
   b. Kaj nam pove zapis tipa CNAME?
   c. Kateri protokol se uporablja na transportni plasti in zakaj?
   d. Kako se razlikujejo iterativne in rekurzivne poizvedbe?

4) Fragmentacija: Usmerjevalnik sprejme datagram, dolg 1700 bajtov, ki ga usmeri na povezavo z MTU = 1500 bajtov.
   a. Kako se fragmentira datagram? Napišite vrednosti tistih polj v glavi, ki se nanašajo na fragmentacijo.
   b. Največ kolikšen bi moral biti MTU na izhodni povezavi, da bi se moral datagram fragmentirati na tri kose?

5) Opišite, kaj je in kako deluje nadzor pretoka pri protokolu TCP.

6) Protokol Needham - Schroeder: katere od spodnjih trditev so pravilne? Pri napačnih pojasnite, zakaj so napačne.
   a. Je namenjen za enkriptcijo – zagotavljanje varnosti sporočil.
   b. Uporablja simetrično kriptografijo.
   c. Uporablja zgoščevalne funkcije.
   d. Omogoča vzajemno avtentikacijo sogovornikov.
   e. Uporablja izzive in odgovore.
   f. Osrednja avtoriteta (center, notar) ni potreben.
   g. Uporablja ge tudi Kerberos.
   h. Uporablja ga tudi Radius.
   i. Uporabnik dobi vstopnico za dostop do vira.
   j. Uporabnik mora za vsak dostop kontaktirati osrednji strežnik.

7) SSL
   a. a) Odjemalec prejme znotraj protokola SSL Handshake strežnikov certifikat. Opiši kaj mora narediti odjemalec, da se prepriča, da je res povezan na pravi strežnik?

b. b) Opiši (lahko tudi narišeš), kaj se dogaja v protokolu SSL Record z uporabniškimi podatki, preden se predajo transportni plasti.
c. c) V seji SSL smo uporabili naslednji ciphersuite: TSSL_RSA_WITH_DES_CBC_SHA. Opiši, kateri kriptografski algoritmi in protokoli se v takšni seji uporabljajo. Na kratko (max. ena do dve povedi) opiši tudi, kakšno vlogo ima posamezen algoritem.

8) Skrbnik omrežja je vašemu računalniku dodelil IPv4 naslov 212.235.189.151 in masko podomrežja 255.255.255.224. Izračunajte (odgovori naj bodo v decimalni a.b.c.d obliki s prefiksno masko):
   a. Naslov podomrežja.
   b. Naslov broadcast.
   c. Največji naslov naprave.
   d. Najmanjši naslov naprave.
   e. Število naprav, ki jih lahko priključimo v to podomrežje.

9) Iz usmerjevalnika smo prebrali spodnjo usmerjevalno tabelo. Na kateri vmesnik (če je podan, napišite tudi prehod) bo usmerjevalnik usmeril pakete s spodnjimi ciljnimi naslovi

Omrežje	Prehod	Vmesnik
9.2.0.0/24		A
9.2.3.0/22		B
192.168.12.0/24		C
10.2.2.0/24		D
0.0.0.0/0	1.2.3.4	A

   a. 10.2.3.4,
   b. 10.2.2.3,
   c. 9.2.0.222,
   d. 9.2.3.34,
   e. 9.2.3.72,
   f. 9.3.2.3,
   g. 192.168.12.70,
   h. 192.168.12.240,
   i. 192.168.1.1,
   j. 193.2.1.66

10) S programom Wireshark smo zajeli del seje TCP, ki je prikazan spodaj.
   a. Kateri segmenti (napišite njihove številke) predstavljajo vzpostavitev povezave TCP?
   b. Za vsak segment, ki ga pošilja računalnik z naslovom 212.235.189.158 napišite katere segemnte potrjuje (napišite številke segmentov).
   c. Koliko bajtov se prenese v segmentu številka 104?

Št.	Pošiljatelj	Prejemnik	Protokol	Opis
100	212.235.189.155	212.235.189.158	TCP	[SYN] Seq=0 Win=8192
101	212.235.189.158	212.235.189.155	TCP	[SYN, ACK] Seq=0 Ack=1 Win=5840
102	212.235.189.155	212.235.189.158	TCP	[ACK] Seq=1 Ack=1
103	212.235.189.158	212.235.189.155	TCP	[PSH, ACK] Seq=1 Ack=1
104	212.235.189.155	212.235.189.158	TCP	[PSH, ACK] Seq=1 Ack=21
105	212.235.189.158	212.235.189.155	TCP	[ACK] Seq=21 Ack=31
106	212.235.189.155	212.235.189.158	TCP	[PSH, ACK] Seq=31 Ack=21
107	212.235.189.158	212.235.189.155	TCP	[ACK] Seq=21 Ack=543
108	212.235.189.155	212.235.189.158	TCP	[PSH, ACK] Seq=543 Ack=21