Komunikacijski protokoli in omrežna varnost
2018/19
Prvi kolokvij

Kolokvij morate pisati posamič. Pri reševanju je literatura dovoljena. Odgovorite pazljivo na *vsa* vprašanja.

Če boste uspešno vsaj delno vse naloge, bo možno dobiti dodatne točke.

Čas pisanja kolokvija je 60 minut.

Veliko uspeha!

NALOGA	TOČK	OD TOČK	NALOGA	TOČK	OD TOČK
1			3		
2			4		

IME IN PRIIMEK: _____

ŠTUDENTSKA ŠTEVILKA: _____

DATUM: _____

PODPIS: _____

1. naloga: Osnove.

VPRAŠANJA:

A) Imamo napravi z IP naslovoma 192.168.2.10 in 192.168.3.15. Kdaj si lahko neposredno pošiljata promet in kdaj potrebujeta posrednika? Utemeljite odgovor.

B) Peter ima dve mreži - 192.168.1.64/26 in 192.168.1.128/26. (i) Najmanj koliko DNS strežnikov potrebuje, da bo njegovim uporabnikom normalno deloval svetovni splet? (ii) Kaj in kako bo moral nastaviti (poleg samih strežnikov), če bo hotel, da bo uporabnikom ponudil pravi DNS čim bolj preprosto?

C) (i) Kot rečeno ima Peter dve mreži in koliko strežnikov z operacijskim sistemom potrebuje, da bodo nudili tftp storitev? Utemeljite odgovor. (ii) Storitvi bootp in tftp smo spoznali v povezavi z zagonom stroja. Ali ju lahko uporabimo tudi, ko je operacijski sistem že delujoč na stroju? Utemeljite odgovor.

   NAMIG: Če menite da da, razložite zakaj in kako ter, če menite, da ne, utemeljite zakaj ne.

2. naloga: Peter je slišal, da lahko preveri, koliko prostora ima na disku, če izvede:

```
snmpget -v1 -c studentje localhost .1.3.6.1.4.1.2021.9.1.9.1.
```

VPRAŠANJA:

A) Sedaj ga zanima, katere ostale podatke o disku lahko dobi. (i) S katerim ukazom si lahko pomaga? Napišite celoten ukaz z vsemi argumenti. (ii) Kaj je v zgornjem ukazu `studentje`? (iii) Ali so ukazi, ki jih uporablja, varni? Utemeljite odgovor.

B) Pri SNMP protokolu imamo tri vrste komunikacije: vprašanje/odgovor med upravljalcem in upravljancem, sporočilo upravljanca upravljalcu in sporočila med upravljalci. Poleg tega imamo več tipov sporočil (*PDU Type*, *Protocol Data Unit Type*). (i) Katere tipe sporočil poznate in pri kateri vrsti komunikacije se uporabljajo? Dodajte primer, ko se uporabljajo. (ii) Protokol SNMP ni nič kaj varen protokol. Kako se branimo pred napadi s ponavljanjem? Kakšne vire na napravah in na katerih zahteva ta obramba?

C) Ali lahko stanje omrežnega (IEEE 802.3) stikala nadziramo brez SNMP? Utemeljite odgovor.

3. naloga: Stvarni čas.

VPRAŠANJA:

A) Ali za zakrivanje RTP prometa lahko uporabimo protokol SSL/TLS? Utemeljite odgovor.

B) Protokol RTP zagotavlja dve osnovni funkcionalnosti. (i) Kateri in kako? (ii) Recimo, da bi se dogovorili, da za prenosni protokol uporabimo namesto UDP protokola protokol TCP. Kateri del glave paketa RTP bi postal nepotreben in zakaj? (iii) Peter je v svojem podjetju vzpostavil videofonski sistem z uporabo protokola RTP. Za vzpostavitev povezave je uporabil storitev SIP. Kako naj zagotovi celovitost (integriteto) toka podatkov? Opišite predlog svoje rešitve čim bolj natančno.

C) Protokol TIME (oziroma `rdate`) lahko na prenosni plasti uporablja tako TCP kot UDP. V katerem primeru bi izbrali enega oziroma drugega? Utemeljite odgovor.

4. naloga: Razpošiljanje.

VPRAŠANJA:

A) Ali DHCP protokol uporablja razpošiljevalne naslove? Utemeljite odgovor.

NAMIG: Upoštevajte, kateri protokol je na mrežni plasti.

B) Imamo napravo z naslovom 1.4.6.7, ki se prijavlja na razpošiljevalno skupino 224.0.24.32. (i) Zapišite naslovnikov in pošijateljev naslov v IP glavi ter vsebino IGMPv2 paketa. Utemeljite zakaj so vrednosti takšne, kot ste jih zapisali? (ii) Na predavanjih smo zapisali, da je vrednost TTL polja 1. Kdaj je smiselno, da je večja kot 1? Opišite primer. (iii) Ali IGMP protokol vsebuje zaščito, ki zagotavlja celovitost (integriteto) sporočila? Odgovor utemeljite.

NAMIG: Če menite, da jo vsebuje, opišite kako deluje in če ne, opišite kako lahko napadalec spremeni sporočil ne da bi prejemnik vedel za spremembo.

C) NEOBVEZNO IN NI ZA OCENO. Letos proslavljamo 100 letnico konca prve svetovne vojne. (i) Naštejte tri države, ki so se bojevale na strani centralnih sil in tri države, ki so se bojevale na strani ANTANTE. (ii) Zakaj Rusija ni bila med podpisniki miru pred 100 leti?

D) V Butalah je spet rdeči alarm. Nekaj gre hudo narobe in Peter Zmeda sumi, da je v ozadju ponovno Cefizelj. Zato se je lotil problema tako, da je zajel omrežni promet in dobil je naslednji zapis:

```
Frame 1543: 62 bytes on wire (496 bits),
  62 bytes captured (496 bits) on interface 0
Ethernet II, Src: 00:6c:bb:2f:30:00 (00:6c:bb:2f:30:00),
  Dst: IPv4mcast_16 (01:00:5e:00:00:16)
Internet Protocol Version 4, Src: 10.0.0.2, Dst: 224.0.0.22
Internet Group Management Protocol
    [IGMP Version: 3]
    ...
    Num Group Records: 1
    Group Record : 224.1.1.1  Mode Is Include
        Record Type: Mode Is Include (1)
        Aux Data Len: 0
        Num Src: 2
        Multicast Address: 224.1.1.1
        Source Address: 192.168.1.2
        Source Address: 8.8.8.8
```

(i) Na katerem IP naslovu sumi Peter, da je Cefizelj? Utemeljite odgovor. (ii) Kaj pravzprav želi početi Cefizelj? Natančneje kot opišete, več točk boste dobili.

NAMIG: Preglejte natančno vsebino paketa na vseh plasteh in iz vsebine sklepajte, za katere vrste paket gre ter čemu je namenjen.