# Komunikacijski protokoli in omrežna varnost
# 2020/21
# Pisni izpit 31. prosinca 2022

Izpit morate pisati posamič. Pri reševanju je literatura dovoljena.

Če boste uspešno vsaj delno odgovorili na vsa vprašanja, bo možno dobiti dodatne točke.

Čas pisanja izpita je 105 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. Peter Zmeda je poslal sporočilo, da je zajel PPP okvir:

| | |
|---|---|
| Address: 0xff | Length: 22 |
| Control: 0x03 | Peer-ID-Length: 8 |
| Protocol: (0xc023) | Peer-ID: PeterZme |
| Code: Authenticate-Request (1) | Password-Length: 8 |
| Identifier: 13 | Password: krneki |

VPRAŠANJA:

A) (i.) Kateri protokol je tuneliran skozi PPP okvir in kako to veste? (ii.) Za vsak podatek okvirja razložite namen in pomen ter vrrednost. (iii.) Ali je Peter res zajel ta okvir? Utemeljite odgovor.

B) Za katero vrsto aplikacijskih protokolov je na transportni plasti bolj primeren UDP protokol (predpostavimo, da želene lastnosti lahko nudi zgolj transportna plast in jih aplikacijski protokoli ne implementirajo sami) (en odgovor)? Utemeljite odgovor tako, da za napačne odgovore razložite, zakaj so napačni.

   (a) Promet, kjer zahtevamo, da paketi prispejo v pravilnem vrstnem redu, ne zahtevamo pa, da paketi zanesljivo prispejo.
   (b) Za nobeno.
   (c) Promet, kjer ne zahtevamo, da paketi prispejo v pravilnem vrstnem redu, zahtevamo pa, da zanesljivo prispejo.
   (d) Promet, kjer ne zahtevamo vrstnega reda niti zanesljivega prispetja, zahtevamo pa hitro vzpostavitev komunikacije.

C) Peter Zmeda je na svoj računalnik namestil Debian GNU/Linux. (i.) S katerima ukazoma lahko ročno nastavimo naslove IP? Zapišite ukaz, ki nastavi naslov `192.168.0.123` v omrežju `192.168.0.0/24` mrežni kartici `eth0`. (ii.) S katerima ukazoma lahko ročno nastavimo usmerjanje paketov (*routes*)? Zapišite ukaz, ki vse pakete usmeri na naslov `192.168.0.1`. (iii.) V kateri datoteki pa so shranjene trajne nastavitve mrežnih vmesnikov na vašem najljubšem (ali drugem poljubnem) operacijskem sistemu?

**2. naloga:** Varnost in zasebnost. Peter je priključen na internet preko svojega lokalnega ponudnika v Butalah in Maja preko ponudnika v Tepanjah (sl. 1). Lokalni


**Slika 1:** Lokalni omrežji v Butalah in v Tepanjah.

omrežji sta povezani preko Interneta, kjer sta javna IP naslova požarne pregrade `B 1.2.3.4` in požarne pregrade `T 2.3.4.5`. V Butalah uporabljajo lokalne naslove v mreži `10.0.0.0/16` in v Tepanjah v mreži `10.1.0.0./24`.

VPRAŠANJA:

A) Maja in Peter se želita pogovarjati, ampak ljubosumna Maša želi prisluškovati njunim pogovorom, zato se odločita da bosta uporabila šifriranje z javnim in zasebnim ključem. Ali morata izmenjavo ključev zaščititi pred Mašo in kako? Utemeljite odgovor in pojasnite, zakaj ostale izbire niso pravilne.

   (a) Da, ključe izmenjata preko certifikatne agencije (CA).
   (b) Ne, ker poteka povezava preko SSL in je dovolj zaščitena.
   (c) Da, s protokolom Diffie-Hellman.
   (d) Da, z RSA+MD5.

B) Lokalni omrežji v Tepanjah in Butalah želimo povezati v navidezno zasebno omrežje. Pri odgovorih bodite natančni pri opisu zapisov in opišite tudi pomen in namen posameznih podatkov v zapisih. (i.) Kje se nahajajo SAD in kakšni vnosi so v njih. (ii.) Kje se nahajajo SPD in kakšni vnosi so v njih. (iii.) Promet med Butalami in Tepanjami se tunelira. Zapišite dve dobri posledici te odločitve, v primerjavi s transportnim načinom varovanja.

C) Peter Zmeda bi rad postavil VPN. Namesto OPENVPN bo uporabil OPENCONNECT, ki je skladen z ANYCONNECT podjetja Cisco. Kot pri OPENVPN, lahko pri OPENCONNECT uporabljamo certifikate za identifikacijo uporabnikov. (i.) Ali za izdelavo certifikatov lahko uporabimo EASYRSA, čeprav je le-ta del OPENVPN in ni podprt s strani Cisco ali razvijalcev OPENCONNECT? Če da, zakaj? Če ne, zakaj? (ii.) Kaj običajno vsebuje datoteka `ca.crt`? (iii.) Peter je po nesreči enemu od uporabnikov poslal `ca.key`. Koga je s tem ogrozil? Kaj mora storiti, da napako popravi?

**3. naloga:** Upravljanje omrežij in razpošiljanje.

VPRAŠANJA:

A) Ali stikalo lahko pridobi informacije o skupinah razpošiljanja in se tako izogne razpošiljanju paketov vsem članom podomrežja? Utemeljite, če da, kako in če ne, zakaj ne.

   (a) Da, če vsi člani skupin razpošiljanja svoje članstvo registrirajo stikalu preko posebnega protokola.
   (b) Da, vendar le v primeru IPv6.
   (c) Ne.

(d) Da, s pomočjo IGMP vohljanja.

B) V Butalah in Tepanjah (sl. 1) imajo vsak svoj lokalni tevelizijski kanal, ki se oba razpošiljata preko skupine `239.0.1.2`. (i.) Ali je to, da sta lokalni omrežji povezani v navidezno zasebno omrežje, problem? Utemeljite odgovor. (ii.) Prebivalcem Butal in Tepanj želimo omogočiti, da gledajo oba **lokalna** kanala. Predlagajte dve bistveno različni tehnični rešitvi za izvedbo. Kje in kaj ter kako je potrebno poseči v nastvitve? Utemeljite odgovor.

C) Peter Zmeda postavlja *Butalsko Televizijo*. Za razpečevanje videomateriala bi rad uporabljal razpošiljanje. V ta namen bo uporabil VLC.

Zaenkrat poganja:

```
vlc --sout="#transcode{acodec=mp4a,ab=128,channels=2,
  samplerate=44100,scodec=none}:http
  {dst=224.0.0.4,mux=ts}"
  --no-sout-all --sout-keep jaz_sem_kosmatko.mkv
```

(i.) Ali z danim ukazom uporablja razpošiljanje? Če da, zakaj? Če ne, kaj bi moral popraviti? (ii.) Kakšen URL bo uporabil na odjemalcu, da si bo lahko ogledal ta televizijski program? (iii) Kaj v ukazu pomeni `ab=128`? Kaj pomeni `samplerate=44100`?

**4. naloga:** Omrežje in skrb zanj.

VPRAŠANJA:

A) Kaj se nahaja v DNS zapisu PTR za domeno `d.c.b.a.in-addr.arpa`? Zakaj so napačni odgovori napačni?

(a) Kazalec na CNAME za IP naslov `d.c.b.a` (obratni DNS).
(b) Kazalec na CNAME za IP naslov `a.b.c.d` (obratni DNS).
(c) Nič.
(d) Kazalec na DNS strežnik za poddomene `in-addr.arpa`.

B) Peter Zmeda je na svojem strežniku ustvaril storitev TEMPERATURA, ki meri zunanjo temperaturo. (i.) Predlagajte protokol (vključno z opisom polj v paketu in njihovo rabo) za branje temperature. (ii.) Druga možnost je, da storitev vsako minuto pošlje zabeležko SYSLOG strežniku. Definirajte polja sporočila in zapišite primer. (iii.) Recimo, da za branje temoerature uporabljamo SNMP. Definirajte potrebni gradnik, ki omogoča branje.

C) Peter Zmeda bi rad poskrbel za enotno prijavo v podjetju. Postavil je strežnik LDAP in vanj spravil podatke o vseh uporabnikih. Najprej ga želi uporabiti za prijavo na omrežje in računalnike. (i.) Strežnik za katero storitev bo moral postaviti za prijavo na omrežje? Navedite primer programa, ki ga implementira. (ii.) Pri nekaterih spletnih storitvah, ki jih poganja na svojih strežnikih, mora nastaviti nek niz - `Bind DN`. Kaj je ta niz? (iii.) Peter izjemno hitro pozablja imena. Ve, da je sodelavcu ime Bo... nekaj. Kakšen iskalni niz mora uporabiti, da mu bo strežnik LDAP vrnil vse vnose, kjer je ime (*GivenName* ali *GN*) `Boris` ali `Bojan`?