Komunikacijski protokoli in omrežna varnost
2012/13
Pisni izpit

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 90 minut.

Veliko uspeha!

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

IME IN PRIIMEK: _____

ŠTUDENTSKA ŠTEVILKA: _____

DATUM: _____

PODPIS: _____

1. naloga: Čeprav so posamezna vprašanja morda malce bolj vezana na določeno poglavje predavanj, je za reševanje vprašanja pogosto potrebno uporabiti znanje še iz drugih poglavij.

VPRAŠANJA:

1. Ko smo govorili o protokolu smo omenjali entitetni par. Kaj je to? Opišite primer entitenega para in protokol, pri katerem nastopa.

2. Peter Zmeda je kupil povsem nov računalnik in dobil ga je presenetljivo poceni. V službi ga je želel priključil na omrežje in z njim prebrati pošto s strežnika posta.butale.si. Operacijski sistem se je sicer postavil pokonci in računalnik je pričel delovati povsem v redu vendar se mu nikakor ni uspelo povezati na omenjeni naslov. (i) Navedite pet različnih razlogov, zaradi katerih se mu morda ni uspelo povezati, (ii) kako bi vsakega od njih preverili in (iii) kako bi vsakega od njih lahko odpravil. Upoštevajte, da je na Petrovem računalniku operacijski sistem Linux.

3. IP naslov in omrežna maska računalnika sta 10.0.36.0/20. Kateri IP naslovi so dovoljeni na tem omrežju, in kakšen je oddajni (*broadcast*) naslov?

2. naloga: Razpošiljanje.

VPRAŠANJA:

1. Pri razpošiljanju (*multicast*) smo srečali protokola IGMP in MLD. (i) Med katerima vozliščema poteka IGMP oziroma MLD protokol in (ii) opišite dva scenarija rabe MLD protokola (za res vse točke navedite vsebino paketov, ki potujejo med vozliščema).

2. V razpošiljevalnem drevesu vsako vozlišče ve, kdo so njegovi sosedje in sosedom mora poslati vsak paket. V resnici ne sme razposlati vseh prejetih pajketov, ampak samo nekatere. (i) Katere? Utemeljite odgovor. (ii) V katerem delu operacijskega sistema najdemo podatek o sosedih v razpošiljevalnem drevesu in kako jih lahko ugotovimo iz ukazne vrstice?

3. Ali se **oddajani (*broadcast*)** paketi usmerjajo? Utemeljite odgovor.

3. naloga:

VPRAŠANJA:

1. Peter Zmeda bi želel v službi postaviti ntp strežnik. Kako naj to naredi? Utemeljite odgovor.

2. Petrov najljubši skladatelj je Ludwig van Beethoven, ki se je rodil leta 1770 v Bonnu in umrl 1827 na Dunaju. Beethovna je na zadnjo pot, za razliko od Mozarta, pospremilo okoli 20.000 Dunajčanov. Genij velikega umetnika brez dvoma dokazuje tudi dejstvo, da je zadnja dela napisal povsem gluh. In Petru so še posebej ljuba ta zadnja dela, oziroma njegova Deveta sinfonija, kjer je prvič v zgodovini ob orkestru uporabil še pevske soliste in zbor.

   Peter si je doma postavil strežnik, na katerem si predvaja glasbo, ki jo potem s pomočjo RTP protokola prenaša do svojega računalnika v službi, kjer jo posluša. Paketi v paketnem omrežju lahko potujejo od izvora do ponora po različnih poteh in različno dolgo. Ena od lastnosti aplikacij v stvarnem času je, da ima uporabnik pri ponoru občutek, kot da bi se dogodki pred njim odvijali enako hitro, kot so se odvijali pri izvoru. Kako protokol RTP omogoča to lastnost. Natančnejši ko bo vaš odgovor, več točk boste dobili.

3. Katere načine varne komunikacije ponuja protokol LDAP?

4. NEOBVEZNO. Zadnji stavek Beethovnove Devete sinfonije ima poseben naslov. Kakšen? Kje še srečamo ta stavek?

4. naloga:

VPRAŠANJA:

1. Eden od načinov napada je kraja TCP seje. Cefizelj se je naučil Petru ugrabiti takšno sejo. Kaj vse bi moral narediti in pridobiti Cefizelj, da bi lahko ugrabil TCP sejo, ki uporablja SSL plast?

   NAMIG: Da vam bo lažje odgovoriti, najprej upoštevajte, da Cefizelj že zna ugrabiti TCP sejo - ima funkcijo, ki to naredi. Poleg tega si zamislite, da ima Cefizelj možnost slediti poteku seje (prisluškuje povezavi) in v določenem trenutku želi ugrabiti sejo. Kaj vse mora vedeti/imeti v tistem trenutku in kaj ste moral imeti/vedeti že prej, da bi lahko sledili seji. Bodite podrobni in utemeljujte svoje izjave.

2. Peter bi rad v dnevni sobi gledal filme. V ta namen si je omislil računalnik, ki bo povsem tih in ki bo priklopljen na ogromen televizor.

   Da bi računalnik ostal tih, bo Peter računalnik zaganjal prek mreže, vse podatke pa bo hranil na strežniku v kleti.

   Na kakšne načine lahko doseže, da se bo prek mreže zagnal le tihi računalnik, ne pa tudi ostali? Navedite vsaj dva in ju opišite.

   Ali se bo s spodnjo konfiguracijo `PXELINUX` njegov računalnik lahko uspešno zagnal? Utemeljite odgovor.

```
menu.c32
LABEL boot_net
MENU LABEL initrd=kernels/initrd.lz netboot=nfs ro \\
     nfsroot=10.0.0.1:/cdrom \\
     file=/cdrom/pressed/ubuntu.seed boot=casper
COM32 chain.c32
APPEND hd0
```

3. Kakšna je razlika med avtentikacijo in avtorizacijo?