Komunikacijski protokoli in omrežna varnost
2011/12
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 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: 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. V paketu `bootp` sta polji `xid` in `secs`. Kaj zagotavljata omenjeni polji na ravni protokola?

2. V protokolu TFTP imamo eno od operacij `ACK` (= 4). Kaj točno pomeni, če odjemalec pošlje paket z vrednostjo (zapisano desetiško po dva zloga/bajta): `4` | `210`.

3. Kako veliko datoteko lahko prenesemo s protokolom TFTP. Utemeljite odgovor.

2. naloga: Peter Zmeda je res prava zmeda. Njegova prijateljica Simona se ukvarja z vrtnarstvom. V rastlinjakih prideluje vrtnine, ki zahtevajo posebno dobro nadzorovano temperaturo. Tako je kupila novo napravo, ki ima vgrajen termometer in grelec. Prvi po potrebi vključuje in izključuje drugega. Poleg tega ima naprava še možnost uporabniške programske nadgradnje. Slednje pomeni, da lahko uporabnik pripravi lastno programje ter ga vgradi v napravo.

VPRAŠANJA:

1. Simona ima tudi domači strežnik ter je prosila Petra, da bi ji napisal potrebno programje, da bo lahko s strežnika upravljala in nadzorovala novo napravo. Peter se je odločil, da bo za upravljanje uporabil protokol SNMP. Katere kose programske opreme mora namestiti in kje?

2. Protokol SNMP definira več tipov sporočil. Katere? Za vsakega napišite primer uporabe v primeru Simoninega rastlinjaka.

3. Protokol SNMP uporablja za prenos protokol UDP, ki smo ga po drugi strani omenjali pri razpošiljanju. Simona ima načrt povečati število rastlinjakov ter posledično število naprav. Da bi zmanjšal količino prometa v omrežju, je Peter prišel na prekrasno idejo, da bo uporabil princip razpošiljanja (*multicasting*) za hkratno rokovanje z vsemi napravami. Komentirajte njegovo idejo.

4. Eno od sporočil, ki smo jih prestregli na omrežju govori o trenutni temperaturi (najprej) in pritisku v rastlinjaku. Obe vrednosti sta zapisani v TLV zapisu, pri čemer je temperatura v ^{o}C in pritisk v kPa. Vrednost sporočila je (po bajtih):

12	1	2	23	0	2	2	$\rightarrow$

Kakšna je temperatura in kakšna relativna vlaga?

3. naloga: Razpošiljanje.

VPRAŠANJA:

1. Na predavanjih smo omenjali delitev usmerjevalnih protokolov na tiste za razpršeni in na tiste za gosti način dela (*dense and sparse mode*). V čem je razlika med obema načinoma dela? Zakaj se enemu načinu dela reče razpršeni in drugemu gosti?

2. Razpošiljanje se uporablja tudi za dostavo televizijskega programa. Seveda dostop do določenega televizijskega programa imajo lahko samo določeni uporabniki, ki morajo biti avtorizirani za to. Predpostavimo, da se program v resnici dostavlja preko razpošiljevalnih mehanizmov. Čim podrobneje opišite, kako sta povezana AAA in razpošiljanje.

   NAMIG: Razmislite kdo dejansko dostavi program uporabniku in da je to strežnik programa.

3. Peter Zmeda se je odločil, da bo v svojem omrežju ponudil novo cenovno shemo za gledanje plačljivih vsebin. Imenoval jo je PPP - plaćaj po porabi. Njegovi odjemalci se prijavijo na razpošiljane vsebine pri najbližjem usmerjevalniku z uporabo IGMP protokola. Kaj mora Peter zabeležiti in ob prejemu katerih IGMP paketov v usmerjevlaniku?

4. naloga: Varnostni elementi omrežij in AAA..

VPRAŠANJA:

1. Protokol RADIUS uporablja za prenos protokol UDP. Zato ne moremo zagotavljati varnosti prenešenih podatkov. Vseeno protokol predvideva določeno mero varnosti s podpisovanjem. (i.) Kako točno deluje podpisovanje paketov protokola RADIUS pri avtentikaciji in avtorizaciji? Opišite posamezne korake in vsebino poslanih paketov. (ii.) Kako bi izvedli napad na takšen način varovanja?

2. Peter Zmeda je v svojem podjetju namestil brezžično omrežje, ki je od njegovega preostalega omrežja ločeno s požarno pregrado. Ali slednja nadomesti uporabo protokola IEEE 802.1x? Utemeljite odgovor.

3. Protokol SSL predvideva razbitje na zapise. Zakaj bi želeli ali celo morali razbijati podatke na zapise?

4. Eden od načinov napada je kraja TCP seje. Cefizelj se je naučil Petru ugrabiti takšno sejo. Zato je Peter vrh TCP plasti namestil SSL zaščito. Če bi Cefizelj rad ugrabil tako vzpostavljeno sejo, mora ukrasti Petru še nekaj vrednosti. Katere?