Komunikacijski protokoli in omrežna varnost
2018/19
Pisni izpit 23. prosinca 2019

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: Osnove delovanja omrežij.

VPRAŠANJA:

A) Kakšen je vrstni red (od manjšega proti večjemu) IPv4, IPv6 in MAC naslovov ter številk vrat glede na število možnih vrednosti? Utemeljite odgovor.

B) Peter ne mara angleščine, zato se je odločil, da posloveni svoj sistem. Začel je z ukazi za delo z mrežo – `ifconfig`, `route` in `ping`, ki jih bo preimenoval v `mvnastavi`, `potpaketov` in `namiznitenis`. Najprej mora ugotoviti, kje se ti programi nahajajo. (i.) Kako lahko ugotovi, kje se nahaja poljuben ukaz? (ii.) Napišite ukaze, s katerimi bo lahko programe preimenoval ne glede na to, v katerem imeniku se trenutno nahaja.

   Ker njegov strežnik pogosto uporabljajo drugi uporabniki, se je odločil poleg slovenskih ohraniti še angleška imena programov. Poleg tega bi rad, da se ob posodobitvi originalnega programa posodobi tudi slovenska različica, ne da bi moral za to kaj storiti. (iii.) Kakšno rešitev mu predlagate?

C) Pri razpošiljanju (*multicasting*) ima paket GMR (*Group Membership Request*) ima TTL nastavljen na 1. (i.) Kaj pomeni TTL in zakaj ima nastavljeno vrednost 1?

   Za protokol PIM pravimo, da usmerja razpošiljevalni promet. (i.) Kako PIM doseže na nekem usmerjevalniku, da se razpošiljevalni paketi pošiljajo na prave naslove (kako vpliva na delovanje usmerjevalnika)?

   NAMIG: V pomoč vam bo, če skicirate primer topologije, ga opremite s podatki (naslov itd.) ter nato razložite na skici kaj se dogaja.

2. naloga: Moje omrežje in njegovo upravljanje.

VPRAŠANJA:

A) Ali DHCP protokol uporablja razpošiljevalne naslove?

   (a) da, ampak le na IPv6;
   (b) da, vedno;
   (c) da, ampak samo med prepošiljevalniki (*DHCP relays*);
   (d) ne, DHCP uporablja naslov 255.255.255.255 za razpršeno oddajanje (*broadcast*).

   Utemeljite odgovor.

B) Peter je na domačem računalniku postavil spletni strežnik. Ko obišče spletno stran `www.whatismyip.com`, mu stran pokaže naslov 172.14.188.25. Ko se poizkusi povezati na ta naslov s prenosnega računalnika, se povezava ne vzpostavi. Če na domačem računalniku požene ukaz `route` vidi, da je njegov privzeti prehod na naslovu 172.19.1.1. Kaj bo moral nastaviti in kje, da bo njegov spletni strežnik dostopen z Interneta?

C) Protokol SNMP uporablja za prenos sporočil prenosni protokol `udp`. (i.) Kateri del glave paketa SNMP bi ne bil potreben, če bi uporabljal TCP in zakaj? (ii.) Za prenos podatkov uporablja TLV zapis. Opišite ga. (iii.) Kaj je vsebina naslednjega TLV zapisa (desna vrednost je prvi bajt in zapisi so šestnajstiški):

```
E3x 07x 02x 02x 01x 01x 02x 17x 01x 02x
```

3. naloga: Čas in televizija.

VPRAŠANJA:

A) Najprej DNS. Če kot strežnik DNS uporabite `dnsmasq`, lahko le-ta skrbi, da odjemalci, ki pridobijo naslov prek DHCP, dobijo tudi vnose v DNS. Ali je to mogoče tudi, če sta DHCP in DNS strežnik ločena programa?

   (a) Da, to je mogoče, če uporabljamo programsko opremo enega proizvajalca (npr. Microsoft).
   (b) Za popravke v DNS morajo poskrbeti odjemalci sami. Storitev se v angleščini imenuje *dynamic DNS*.
   (c) Avtomatizirano popravljanje vnosov v DNS je opisano v več RFC-jih.
   (d) Da, to je mogoče, a le, če uporabimo prave različice programske opreme (npr. Bind 9 in ISC DHCP server v3, Microsoft AD in Microsoft DHCP strežnik, i.t.d.)

   Utemeljite odgovor.

B) Nato tok VLC. Peter Zmeda želi predvajati video čez omrežje z uporabo VLC. (i.) Kateri naslov IP lahko uporabi, če želi video prenašati z uporabo razpošiljanja (*multicast*) IPv4? utemeljite odgovor. (ii.) Peter v svojem omrežju zaznava precej izgubljenih paketov. Kateri prenosni protokol naj uporabi? Zakaj? (iii.) V parameter `--sout` je dodal vrednost

```
#transcode{vcodec=h264,acodec=mpga}
```

   Kaj je s tem dosegel?

C) Peter razmišlja, da bi tok prenašal s pomočjo protokola RTP. Ročno se je lotil programiranja in konfiguriranja, a nikakor ne najde v dokumentaciji, kako se tok podatkov v protokolu RTP začne oziroma vzpostavi. (i.) Pomagajte mu pri njegovem problemu ter utemeljite svoj odgovor. (ii.) Naročniki njegovih oddaj so raznovrstni kot tudi oddaje. Kako naj hkrati ponudi tako točenje oddaj v slovenskem jeziku in tudi z angleškimi oziroma nemškimi podnapisi? Opišite čim podrobneje izvedbo. Seveda, kdor razume slovensko, ne želi videti podnapisov, medtem ko ostali želijo podnapise v samo enem jeziku.

4. naloga: Varnost tako in drugače.

VPRAŠANJA:

A) Kako ESP preprečuje napade s ponavljanjem? Opišite rešitev in utemeljite, zakaj deluje.

B) SA zapis vsebuje naslov izvora in naslov ponora ter potemtakem definira enosmerno povezavo. (i.) Zakaj je tako in ne definira dvosmerne povezave?

   Pri IPSEC protokolu imamo pri tunelski uporabi ESP protokola polje `Seq#`. (ii.) Čemu je namenjeno in kako izpolnjuje ta svoj namen?

   NAMIG: Kaj bi se lahko zgodilo, če bi ne imeli tega polja?

C) Gregor Copatka, Peter Zmeda in Jurež Pismouk bi se radi varno pogovarjali po omrežju, v katerega je Peter Zmeda povezal vsako butalsko in tepanjsko kočo. Seveda se vsi trije boje prisluškovanja, zato si bodo postavili navidezno omrežje s pomočjo OPENVPN. Za avtentikacijo bodo uporabili certifikate. (i.) Kdo naj ustvari zasebne ključe? Kdo javne? Kdo naj kaj podpiše? (ii.) Katere datoteke za avtentikacijo naj ima na koncu vsak od njih? (iii.) Če uporabljajo *easy-rsa*, kako naj podpišejo certifikat strežnika? Napišite natančni ukaz za podpis (brez pripravljanja okolja).