Komunikacijski protokoli in omrežna varnost
2017/18
Pisni izpit 23. prosinca 2018

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.

VPRAŠANJA:

A) Naš prijatelj Peter Zmeda je napisal program za novo mrežno storitev `KrNeki`. Na katerih vratih naj namesti program? Utemeljite odgovor.

   NAMIG: Pri določanju vrat pazite, da nekdo drug slučajno ne bi mogel niti v preteklosti, niti v bodoče uradno povezati kakšne dobro znane storitve na ta vrata.

B) Peter na vseh domačih računalnikih poganja GNU/Linux. Tako je tudi njegovo dekle prisiljeno uporabljati ta operacijski sistem. Kadar Petrova izbranka zvečer čepi na svojem najljubšem socialnem omrežju, ji Peter včasih na daljavo odpira okna s sporočili. V ta namen uporablja ukaz `xmessage`, ki na zaslonu grafičnega vmesnika prikaže vse svoje argumente. Kako točno Peter to počne? (i) Opišite postopek oziroma (ii) napišite zaporedje ukazov, ki ji izpiše poljubno ljubezensko sporočilo. Upoštevajte, da ima Peter na vseh računalnikih v stanovanju korenski dostop in da vsakem računalniku teče strežnik `sshd`, izbranka pa ima uporabniško ime `filomena`.

C) Pri načrtovanju protokolov lahko uporabimo tehnike, ki smo jih srečali že drugje. Tokrat pripravlja Peter novo storitev, ki nudi vremenske podatke na vremenski postaji, ki vsako minuto izmeri temperaturo, vlago, smer vetra in njegavo jakost. V ta namen bo pripravil nov protokol. Zaradi omejitev, se je najprej odločil, da bo za prenos uporabil protokol UDP. Prva storitev, ki naj jo nudi vremenska postaja, je prenos vseh izmerjenih podatkov, ki jih hrani. Druga storitev pa je brisanje vseh podatkov, ki jih postaja hrani. (i) Predlagajte protkol - obliko paketov. (ii) Utemeljite svoj predlog.

2. naloga: Moje omrežje in njegovo upravljanje.

VPRAŠANJA:

A) Peter ima na svojem vedno prižganem računalniku v službi zadnjih nekaj ur težave z omrežjem. Normalno mu delujeta Facebook in Google, večina ostalih strani pa ne. Da bi preveril, ali ima dostop do Interneta, je uporabil ukaz `ping 8.8.8.8` in ni dobil nobenega odgovora. Kako menite, da bi lahko dostopal do strani podjetij Google in Facebook?

   NAMIG: vsi usmerjevalniki na omrežju so skoraj novi (stari nekaj mesecev). Če ne doseže strežnika DNS, kako lahko njegov računalnik sploh ve, na katerem naslovu je www.google.com?

B) Peter je novo zaposlen in mora urediti upravljanje omrežja. Ugotovil je, da so doslej za upravljanje uporabljali dva protokola in sicer `snmp` in `rmon`. Predvidite dve možni rešitvi, s pomočjo katerih bi združil upravljanje celotnega omrežja. (i) Za vsako od njih napišite po dve dobri strani. (ii) Utemeljite svoje odgovore.

NAMIG: V vašem odgovoru *dobro* pomeni, da jo ena rešitev ima in druga ne.

C) Kako SNMPv3 preprečuje napade s ponovitvijo (*replay attack*)?

NAMIG: Morda najlaže opišete, če narišete paket in podrobneje kateri njegov del ter kako preprečuje omenjeni napad.

3. naloga: Čas in televizija.

VPRAŠANJA:

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

B) Peter je postavil strežnik, ki v Internet oddaja video ovc na pašniku. V ta namen je uporabil ukaz:

```
vlc --sout="#transcode{vcodec=h264,vb=1000,scale=Auto, \
  acodec=mpga,ab=128,channels=2,samplerate=8000}: \
  http{mux=ts,dst=:8080/}" --sout-keep /dev/video0
```

Na žalost je sedaj ugotovil, da mu video zaseda pol pasovne širine in je zato brskanje po Internetu obupno počasno. (i) Kako naj popravi zgornji ukaz, da bo video zasedel samo pol te pasovne širine, ki jo zaseda sedaj? Napišite popravljeni ukaz. (ii) Kako naj ukaz popravi, da bosta višina in širina slike pa bosta pol manjši? (iii) Približno koliko pasovne širine bo popravljeni (manjši) video zasedel?

C) Da ne bo kakšne pomote – Butale in Tepanje sta dve vasi; in n samo, da so dve vasi, tudi dva jezika sta butalščina in tepanjščina. Peter Zmeda si je pridobil pravico oddajanja kabelske televizije v obeh vaseh. A ima velik problem, saj podnapisi v filmih nikakor ne smejo biti enaki. (i) Kaj naj naredi, oziroma kako naj oddaja filme, da bodo lahko tako Butalci kot Tepanjčani gledali filme s pravimi podnapisi? Opišite rešitev. (ii) Kaj naj naredi, da bo lahko oddajal filme tudi v Abdera, kjer imajo pa grško pisavo? Utemeljite odgovor.

NAMIG: V odgovoru morate popisati, kako naj izgleda oddajanje, kako izgleda protokol prenosa (čim podrobneje) in kako naj izgleda odjemalec, na katerem se lahko gleda film.

4. naloga: Varnost tako in drugače.

VPRAŠANJA:

A) Peter ima strežnik Radius z odjemalcema 192.168.1.4 in 192.168.1.5. Sedaj bi rad izboljšal varnost. Nastavitvena datoteka izgleda takole:

```
client mojamreza {
       ipaddr          = 192.168.1.0/24
       secret          = testing123
}
```

Ali lahko nastavi različni skrivnosti? Če ne, zakaj ne (utemeljite)? Če da, kako (napišite pravilne nastavitve)?

B) Peter je po omrežju pošiljal podatke in oblika njegovih paketov je bila naslednja:

```
<pošiljatelj><prejemnik><podatki>
```

Čez nekaj časa je ugotovil, da je Cefizelj izvedel napad s ponavljanjem. Slišal je , da se pred tem napadom braniš z dodatno informacijo ter je spremenil pakete v obliko:

```
<pošiljatelj><prejemnik><naključno število><podatki>
```

(i) Komentirajte učnkovitost njegove rešitve.

NAMIG: Pomislite na to, koliko ta zaščita preprečuje Cefizlju napad. Kako je z dodatnimi viri?

C) Peter Zmeda se je odločil zasoliti shranjena in zgoščena gesla, da bi ne bila ranljiva na mavrični napad. Žal je vrednost soli izgubil. Je to pomembno? Utemeljite zakaj je to pomemebno oziroma zakaj ne.