Komunikacijski protokoli in omrežna varnost
2017/18
Pisni izpit 7. svečana 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 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: Osnove.

VPRAŠANJA:

A) Kaj in kako naj bi ščitil *SecureBoot*? Opišite podrobnosti tako za kaj kot za kako.

B) Ena od zadreg pri nalaganju operacijskega sistema ob zagonu je velikost letega. (i) V katerem protokolu je omejitev velikosti naloženega operacijskega sistema? Zakaj? (ii) Koliko sme biti največ velik operacijski sistem, da ga še lahko naložimo? Utemeljite odgovor. (iii) Peter se želi izogniti omenjeni omejitvi. Predlagajte mu rešitev ter utemeljite odogvor. (iv) Kaj pa varnost pri vaši rešitvi? Utemeljite odgovor.

   NAMIG: Pri zadnjem vprašanju najprej opišite varnostno tveganje.

C) Peter ima težave s svojim GNU/Linux namizjem. Namesto upravljalnika oken (*window manager*) se mu ob prijavi odpre le črno okno terminala, v katerem ima na voljo lupino `bash`. (i) Sedaj bi Peter rad obenem zagnal upravljalnik oken `butalebox`, še en terminal `xterm` ter spletni brskalnik `firefox` – vse v enem samem ukazu. Napišite ta ukaz. (ii) Ko je opravil z delom, bi Peter rad z enim ukazom zaprl vse terminale xterm. Kako naj to stori?

2. naloga: Čas, televizija in razpošiljanje.

VPRAŠANJA:

A) Butalci in Tepanjčani so se odločili imeti skupno sejo trških svetov. Da pa bi znižali stroške, so se odločili, da sveta povežejo samo preko videokonferenčne povezave. Nalogo postavitve videokonferenčne povezave so zaupali Petru Zmedi. Peter se zaveda pomembnosti svoje naloge in je nekje slišal, da je TCP prenosni protokol zanesljivejši od UDP, ter se je zato odločil zanj pri prenosu videokonference. (i) Kako lahko Cefizej napade prenos seje, da videokonferenca ne bo kakovostno delovala? Opišite napad in utemeljite zakaj bi napad deloval. (ii) Kako naj se Peter brani in še vedno uporablja protokol TCP? Utemeljite odgovor.

B) (i) Če se odjemalec želi prijaviti v skupino `224.6.2.18`, potem uporabi kateri protokol? (ii) Kako izgleda paket, ki ga pošlje?

C) 4. Peter si je izmislil protokol za sporočanje časa, po katerem strežnik klientu odgovori z dvema številkama: 32-bitnim številom sekund od 1. 1. 1970 ob polnoči, ki je predstavljen z malim koncem (*little endian*), in 8-bitnim številom, ki predstavlja dvestotinke sekunde. Napiši funkcijo v poljubnem

programskem jeziku, ki kot argument sprejme podatke, ki jih je poslal strežnik (kot tabelo byte-ov ali niz) in ki izpiše datum in čas v človeku prijaznejši obliki.

3. naloga: Upravljanje omrežij. Protokol `syslog` je zabeležil naslednji zapis;

```
Feb  5 08:13:37 kajtimar dhcpd: uid lease 192.168.126.141
  for client 00:cb:00:00:3a:f2 is duplicate on 192.168.126.0/24
```

VPRAŠANJA:

A) (i) Kateri program je zahteval zabeležko? (ii) Kaj pravzaprav sporoča program? (iii) Ali naj sistemskega administratorja Petra Zmedo skrbi zabeležka? Utemeljite odgovor!

B) Peter ima nov računalnik, ki ima na matični plošči nekaj lučk. Sedaj bi rad prek SNMP bral in nastavljal barvo lučk. Slišal je, da lahko v ta namen razširi `snmpd`. (i) Kako konkretno lahko to stori (navedite, kaj naj popravi in v kateri datoteki)? (ii) Kako mora popraviti MIB, da bo rešitev delovala? Utemeljite odgovor.

C) Peter pripravlja novo storitev `nasinaolimp`, ki bo nudila tekoče novice, rezultate, pričakovanj in sploh vse o slovenskih športnikih na bližajočih se olimpijskih igrah v Pjongčangu. Novic ne želi nuditi kar počez, ampak samo prijateljem. V ta namen se je odločil sestaviti sistem, ki bo vključeval strežnik RADIUS. (i) Opišite in narišite celotno arhitekturo: kje je odjemalec, kje je strežnik vsebin in kje je strežnik RADIUS; kakšna je vloga posameznega gradnika in kakšen je protokol med njimi? (ii) Ena od stvari, ki ga zanima, je, kateri šport je najbolj popularen med njegovimi uporabniki. Kako naj uporabi RADIUS, da bo sestavil statistiko? Opišite pakete (navedite vrste sporočil), ki se bodo v ta namen pošiljali. (iii) Kje in kako pri storitvi RADIUS nastopa srednji `A` – avtorizacija?

NAMIG: Odgovora na vprašanji (ii) in (iii) sta dolga po nekako dve vrstici. Pri (ii) morda pomaga slikica.

4. naloga: Infrastruktura v podjetju *Naša sol*.

VPRAŠANJA:

A) Za vodenje podatkov o zaposlenih v podjetju Peter uporablja LDAP. V bazi ima zapis:

```
dn: cn=si,ou=users,dc=nasasol,dc=butale,dc=si
objectClass: inetOrgPerson
objectClass: person
cn: si
sn: Marko
gn: Jan
```

(i) Kako je človeku, ki ga zapis predstavlja, ime? Kako se piše? (ii) Iz katere države je? Utemeljite odgovor.

B) Podjetje *Naša sol* ima gojilnico, skladišče in pakirnico na različnih mestih. Poleg tega imajo v podjetju še pet agentov, ki potujejo po svetu. Peter mora med njimi vzpostaviti varno povezavo in se je odločil se je za VPN. (i) Kaj pomeni tuneliranje *(tunneling)* pri omrežjih VPN? (ii) Narišite topologijo, kjer je še posebej uporabno ter utemeljite svoj odgovor.

C) Gojenje soli je posebno pomembna zadeva in zato so si v podjetju omislili celoten sistem nadzora rasti soli v gojilnici. V ta namen so vgradili v gojilnico temperaturne senzorje in senzorje vlažnosti, katerih odčitki v sistemu sprožijo vklop ali izklop grelcev ter vklop ali izklop namakanja. Senzorji imajo silno preprosto zgradbo ter pošiljajo podatke zgolj neposredno na drugi plasti. Peter mora zato začrtati protokol, ki bo omogočal zajem podatkov iz senzorjev. (i) Kako naj izgleda okvir, ki ga pošiljajo senzorji, da se ne bo pomešal z ostalimi okvirji? Utemeljite odgovor. (ii) Peter se zaveda, da se naredi velika škoda, če je temperatura prenizka ali vlaga previsoka. Kako naj zavaruje odčitke, ki se prenašajo, da jih Cefizelj ne bi potvoril? Opišite gradnike v protokolu ter kako ščitijo prenešene podatke.

NAMIG: Omejite se na napad, kjer napadalec pokvari prenešene okvirje.