Komunikacijski protokoli in omrežna varnost
2020/21
Pisni izpit 22. prosinca 2021

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 105 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. V Butalah so podjetni a tudi previdni ljudje. Pri časopisu *Butalske novice* so se odločili svojim bralcem ponuditi še več lokalnih novic. V ta namen nameravajo vzpostaviti storitev, na katero bi vrli Butalci pošiljali novice dolge do 1000 znakov. Pošiljatelj naj bi na določena vrata na strežniku `Butalske-novice.but` poslal sporočilo, ki mora vsebivati vsebino sporočila, čas in datum dogodka ter ime in priimek pošiljatelja. Storitev mora nato pošiljatelju potrditi prejem sporočila. Storitev naj deluje brez stanj, da strežnika ne obremenjuje po nepotrebnem. Pomagajte Butalcem vzpostaviti storitev.

VPRAŠANJA:

A) Začnimo s strojno opremo. Na strežniku storitve imajo BIOS. Kateri od spodnjih opisov najbolje opisuje iz česa sestoji BIOS kot celota? Utemeljite odgovor.
   (a) Iz programske opreme, ki pomaga pri ugašanju računalnika.
   (b) Iz strojne opreme, ki pomaga pri zagonu računalnika.
   (c) Iz strojne opreme (obstojni pomnilnik) in na njej naložene programske opreme, ki pomaga pri zagonu računalnika.
   (d) Iz programske opreme, ki pomaga pri zagonu računalnika.

B) Na strežniku bi Peter želel zagnati Linux, ampak se mu zaganjajoči računalnik ustavi s črnim zaslonom in napisom `(initrd)#`. Zaganja Ubuntu in uporablja `atftpd` in `pxelinux`. (i.) Ali `atftpd` deluje? Utemeljite odgovor. (ii.) Ali deluje `pxelinux`? Utemeljite odgovor. (iii.) Če vemo, da je narobe nastavil nekaj v `default.cfg`, kaj bi to lahko najverjetneje bilo?

C) In na koncu protokol storitve. Le-ta naj bo neposredno nad prenosno plastjo. (i.) Kateri protokol naj izberejo na prenosni plasti? Utemeljite odgovor. (ii.) Narišite čim bolj natančno polja v sporočilu (paketu, datagramu). Utemeljite zakaj je posamezno polje v sporočilu. (iii.) Butalci so slišali, da svet preplavljajo lažne novice in so se odločili, da mora biti možno preveriti, ali je prejeto novico v resnici napisala oseba, ki se izdaja za pošiljatelja. Opišite, kako naj razširijo protokol iz prejšnje točke, da bo možno narediti preverjanje.

2. naloga: Moje omrežje in njegovo upravljanje.

VPRAŠANJA:

A) Peter Zmeda je malce zmeden. Namesto v nastavitvene datoteke strežnika DNS in DHCP je namreč podatke o računalnikih - IP naslove, MAC naslove in imena v svojem omrežju vnesel v imenik, dostopen prek LDAP. Sedaj bi rad podatke uporabil za strežnike DHCP in DNS, Pri tem bi rad čim manj podatkov pretipkaval. Kateri od spodnjih nasvetov je najboljši? Utemeljite odgovor.

(a) Podatke bo moral kopirati ročno, saj sta DHCP in DNS ločena protokola od LDAP.
(b) DHCP strežnik lahko kot bazo uporabi LDAP; DNS bo moral podatke sprejemati od DHCP strežnika, saj DNS strežniki podatkov ne shranjujejo v LDAP. Alternativa je, da vsi trije strežniki - DHCP, DNS, in LDAP poberejo podatke iz skupne relacijske podatkovne baze (npr. MySQL).
(c) DHCP in DNS strežnika lahko svoje nastavitve prebereta iz baze LDAP.
(d) Za rešitev bo nujno potreboval razširitve, ki jih ponuja razširitev LDAP – *Microsoft Active Directory*.

B) Peter in Manca si delita fizični del omrežja. Vsak od njiju ima svoj seznam računalnikov in zanje bi rada dodeljevala IP naslove vsak na svojem območju. (i.) Kako bi problem rešila, če imata skupen DHCP strežnik? (ii.) Ali imata lahko tudi dva ločena DHCP strežnika? Če da, kako bi ju nastavila? Če ne, zakaj ne? (iii.) Problem BYOD. Peter in Manca občasno dobita obiskovalca, ki ima računalnik, kateri ni na nobenem od njunih seznamov. Kaj se zgodi s priključevanjem tega računalnika?

C) Protokol SNMP prenaša podatke v obliki sporočil. (i.) Katera polja ima sporočilo tipa zahteva oziroma odgovor in kakšna je vloga oziroma namen vsakega od njih? (ii.) Recimo, da sta vsebina sporočila števili `1000` in `500`. Kje se nahajata v sporočilu? (iii.) Kako sta zakodirani? Zapišite ju ustrezno zakodirani.

3. naloga: Čas in splet.

VPRAŠANJA:

A) Peter Zmeda je zaznal na omrežju REGISTER paket PIM-SM protokola. (i.) Kdo komu pošilja omenjeni paket?

(a) Poljuben usmerjevalnik usmerjevlaniku, pri katerem je vir toka podatkov.
(b) Odjemalec, ki bi se želel priključiti skupini, odjemalcu, ki je že vključen v skupino.
(c) Usmerjevlanik, pri katerem je vir toka podatkov, drugemu usmerjevalniku.
(d) Odjemalec, ki bi se želel priključiti skupini, svojemu usmerjevalniku.

(ii.) Kaj sporoča s paketom pošiljatelj prejemniku?

B) Peter Zmeda vzdržuje več sto računalnikov, ki so vsi priključeni na notranje, lokalno omrežje. Vsako jutro, ko zaposleni pridejo na delovno mesto in

prižgejo računalnike, sprožijo najprej NTP protokol, da uskladijo ure, kar povsem zasede lokalno omrežje. Peter je dobil idejo, da bi vzpostavil storitev, ki bi na notranjem omrežju vsakih deset sekund razposlala (*multicast*) trenutni čas, medtem ko bi računalniki bili v skupini prejemnikov. Razposlani paket vsebuje samo eno polje in sicer čas v nanosekundah od 1. januarja 1900. (i.) Kakšen IPv4 razpošiljevalni naslov naj uporabi za skupino in kakšnega v primeru IPv6? Utemeljite odgovor. (ii.) Peter se je odločil šifrirati (zakriti) podatek o času in namerava uporabiti enak pristop kot pri protokolu SRTP - veriženje. Ali ga lahko? Če da, kako in če ne, kaj naj naredi, da ga bo lahko?

C) Peter Zmeda postavlja *Butalsko Televizijo*. Za razpečevanje videomateriala bi rad uporabljal razpošiljanje. V ta namen namerava uporabiti naslove med 224.0.5.3 in 224.0.5.33. Strežnik je na naslovu 192.168.1.31. (i.) So ti naslovi primerni? Utemeljite odgovor. (ii.) Če ima 10 gledalcev, koliko naslovov bo porabil? (iii) Trenutno mu predvajanje ne deluje. Zaenkrat poganja:

```
vlc --sout="#transcode{acodec=mp4a,ab=128,channels=2,
  samplerate=44100,scodec=none}:rtp
  {dst=192.168.1.31,port=5004,mux=ts}"
  --no-sout-all --sout-keep Cin\ cin\ to\ sem\ jaz
  \(Kosmatko\ Ver\ by\ Butn8\).mkv
```

in na odjemalcu:

```
vlc rtp://192.168.1.31:5004
```

(iv.) Popravite ukaza, da bo predvajanje delovalo s pomočjo razpošiljanja.

4. naloga: Varnost tako in drugače.

VPRAŠANJA:

A) Peter Zmeda načrtuje spletno storitev *NekiNeki*, za uporabo katere se bodo morali uporabniki prijaviti in avtenticirati. Kaj od spodaj naštetega je najbolje, da Peter hrani v ta namen? Utemeljite odgovor.

(a) Podatkovno bazo z imeni uporabnikov in zgoščena njihova zasoljena gesla.
(b) Podatkovno bazo z imeni uporabnikov in solmi za njihova gesla.
(c) Podatkovno bazo s imeni uporabnikov in šifriranimi gesli.
(d) Podatkovno bazo s imeni uporabnikov in njihovimi gesli.

NAMIG: Utemeljitev mora sloneti na lastnosti, ki jo ima izbrana rešitev, druge pa ne.

B) (i.) Poleg požarne pregrade katero storitev še uporabljamo za varovanje notranjega omrežja? (ii.) Kako ta storitev in požarna pregrada sodelujeta? Opišite primer napada in kako ta storitev ob pomoči požarne pregrade zavaruje notranje omrežje. (iii.) Na predavnjih smo spoznali tri oblike požarne pregrade. Katere so in v čem se razlikujejo.

C) Peter Zmeda v svojem podjetju postavlja VPN s pomočjo OpenVPN. Za avtentikacijo bo uporabil certifikate. V ta namen uporablja EasyRSA. Vsakemu uporabniku ustvari vse potrebne datoteke in mu jih potem dostavi na optičnem disku, ki ga pošlje po navadni pošti. Cefizelj se ob tem krohota in meni, da je takšno početje nevarno. (i.) Kdo ima prav? Utemeljite odgovor. (ii.) Katere datoteke dobi vsak uporabnik? (iii.) Kako bi Peter dosegel, da v primeru, če nekdo pismo ukrade, podjetje ne bi bilo ogroženo? Opišite postopek, ki bi ga Peter in zaposleni uporabili.