Komunikacijski protokoli in omrežna varnost
2013/14
Pisni izpit 25. velikega srpana 2014

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: Zagon računalnika.

VPRAŠANJA:

1. Janez Zmeda se je s svojim računalnikom priključil na službeno omrežje. Na računalniku je nastavil, da se mu dodeli IP naslov samodejno preko DHCP protokola. To se je tudi pravilno zgodilo, vendar njegov računalnik nikakor ne deluje pravilno. Nekaj časa je brskal po nastavitvah in pognal tudi programa `traceroute` in `arp`. Na koncu je ugotovil, da ima še en računalnik na mreži enak naslov kot njegov naslov. i.) Kako, menite, je uporabil omenjena programa, da je ugotovil napako? Utemeljite odgovor. ii.) Zakaj njegova povezava na internet ne deluje? Utemeljite odgovor. iii.) Opišite dva *v osnovi različna* načina, kako je lahko prišlo do te napake in odgovor utemeljite.

2. Prek katerega protokola se običajno po mreži prenaša zaganjalnik (*bootloader*)? Če hočete uporabiti drug protokol, katere dele programske opreme na zaganjajočem se računalniku bi morali zamenjati?

3. Najpomembnejša razlika med IPv4 in IPv6 je različna velikost naslovnega prostora, ki je zrasla z 32 bitov na 128 bitov. Kako ta sprememba vpliva na število domenskih imen? Utemeljite odgovor. Primer domenskega imena je `lusy.fri.uni-lj.si`.

2. naloga: Peter je bil doslej zadovoljen z Linux Mint distribucijo, sedaj pa bi rad poizkusil nekaj novega. Kupil je nov računalnik in nanj namestil SuSE Linux distribucijo. Rad bi, da bi se dogodki na novem računalniku beležili tudi na starem. Na žalost je ugotovil, da na novem računalniku ne obstaja datoteka `/etc/rsyslog.conf`, kjer bi kaj takega lahko nastavil. Računalnika sta na naslovih `mint.zmeda` (192.168.1.10) ter `suse.zmeda` (192.168.1.11).

VPRAŠANJA:

1. Peter je prebral, da SuSE namesto *rsyslog* uporablja *syslog-ng*. V nekih navodilih je še prebral, da, če želi, da se dogodki, ki jih na enem računalniku zabeleži *syslog-ng*, prenesejo še na drug računalnik s *syslog-ng*, mora v datoteko `/etc/syslog-ng/syslog-ng.conf.in` dodati:

```
# send everything to log host
destination loghost {
    udp("mint.zmeda" port(5140));
};
log {
    source(src);
    destination(loghost);
};
```

i.) Ali lahko izvaja beleženje iz *syslog-ng* na *rsyslog*? Utemeljite odgovor. ii.) Petra je strah, da bo na računalniku, kjer poganja Linux Mint, odpovedal disk. Rad bi torej beležil dogodke na dveh računalnikih. Ali to lahko počne? Če ne, zakaj ne in če da, kako? iii.) Poleg tega bi Peter rad beležil še dogodke z računalnika v službi, ki je na javnem IP naslovu. Ali to lahko stori? Kaj bo moral spremeniti v nastavitvah *rsyslog*? Kaj bo še moral nastaviti in kje?

2. Ko smo govorili o upravljanju smo omenjali štiri področja upravljanja. i.) Katera so ta štiri področja upravljanja? Za vsako zapišite konkreten primer. ii.) Za vsako od področij upravljanja zapišite kako bi konkretno uporabili *syslog* za beleženje. Bodite res konkretni!

3. Podrobno opišite kako SNMPv3 preprečuje napade s ponovitvijo (*replay attack*)?

   NAMIG: Pomagalo bo, če najprej opišete kako izgleda napad s ponovitvijo.

3. naloga:

VPRAŠANJA:

1. Omenili smo, da pri razpošiljanju uporabljamo protokola IGMP in PIM. Kakšna je natančno vloga vsakega od njiju?

2. Peter si je za avtentikacijo na domačem brezžičnem omrežju omislil strežnik radius. Da bi omrežje res vedno delovalo, si je postavil kar dva radius strežnika, brezžično dostopno točko (*wireless access point*) pa je nastavil tako, da enkrat uporablja enega in drugič drugega. Nato je na obeh strežnikih ustvaril uporabnika:

   ```
   "peter" Cleartext-Password := "urejeni"
   ```

   Čez nekaj časa je na prvem strežniku spremenil zgornjo vrstico v:

   ```
   "peter" Cleartext-Password := "zmedeni"
   ```

   Sedaj ima težavo, da mu sistem, ko se prijavlja z uporabniškim imenom `peter` in geslom `zmedeni`, včasih dovoli prijavo in včasih ne. Ali radius protokol sploh dovoljuje takšno uporabo podvojenega strežnika? Predlagajte, kako naj Peter svoj sistem predela, da bo imel lahko več radius strežnikov, gesla pa bo spreminjal na enem samem mestu.

3. Kateri protokol uporablja NTP za prenos in zakaj?

4. (NEOBVEZNO) Letos praznujemo dva tisočo obletnico ustanovitve antične Emone ali kot se je v izvirniku imenovala ÆMONA. Iz mesta so vodile pomembne ceste v druge dele rimskega imperija. Katere so bile te ceste in kam so vodile?

4. naloga:

VPRAŠANJA:

1. Povezavna plast je razdeljena na dve podplasti. i.) Kateri sta ti dve plasti in kakšna je njuna vloga? ii.) Eden od elementov mreže so mostički. Za njihovo delovanje skrbi povezavna plast. Kaj premoščajo in kako delujejo? Katera podplast je odgovorna za njihovo delovanje?

2. Katera tehnika je ena izmed ključnih pri povečanju hitrosti brezžičnega prenosa od IEEE 802.11g do IEEE 802.11n?

3. Kako lahko odjemalec ob priklopu v omrežje sploh izvede postopek 802.1x avtentikacije, če mu še ni dovoljen dostop do omrežja? Opišite postopek in kateri protokoli so uporabljeni.