Komunikacijski protokoli in omrežna varnost
2012/13
Pisni izpit

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 75 minut.

Veliko uspeha!

NALOGA	TOČK	OD TOČK	NALOGA	TOČK	OD TOČK
1			4		
2			5		
3					

IME IN PRIIMEK: _____

ŠTUDENTSKA ŠTEVILKA: _____

DATUM: _____

PODPIS: _____

1. naloga:

VPRAŠANJA:

1. Peter se tokrat ukvarja z bootp protokolom. No, ukvarja se tečnim šefom, ki želi svoj računalnik včasih obuti v Linux operacijski sistem in včasih v FreeBSD operacijski sistem. Peter nalaga operacijski sistem vedno preko mreže. Kako naj se loti problema, da bo šef lahko po tem, ko bo zagnal svoj računalnik, izbral želeni operacijski sistem.

   NAMIG: Podrobneje ko boste zapisali korake, več točk lahko dobite.

2. Eden najpogosteje uporabljanih protokolov je NFS. Kakšen protokol prenosa (transporta) uporablja? Čemu le-tega?

   Naštejte tri nevarnosti, ki prežijo na Petra, ko je v svojem računalniku zapisal v exports datoteko:

   ```
   /boot    -network 192.168.12.0/25
   ```

   Utemeljite svoj odgovor.

3. IP naslov in naslov podomrežja računalnika A je 192.168.12.7/25. Kateri so IP naslovi (tudi za oddajanje *broadcast*) tega omrežja?

4. Peter si je zamislil, da bo prehod iz lokalnega omrežja računalnik na IP naslovu 192.168.12.161. Ali je to sploh dovoljeno? Utemeljite svoj odgovor.

2. naloga: Ta naloga je o razpošiljanju (*multicasting*).

VPRAŠANJA:

1. Na predavanjih smo spoznali dva protokola povezana z rapošiljanjem: IGMP in PIM. Opišite vlogo vsakega od njiju pri razpošiljanju. Bodite pozorni na različna opravila pri razpošiljanju: prijava, dostava, ...

2. Peter Znmeda je na svojem računalniku vtipkal `netstat -g` in dobil naslednji izpis:

   ```
   Group                   Link-layer Address      Netif
   224.0.0.251             <none>                  lo0
   224.0.0.1               <none>                  lo0
   224.0.0.251             1:0:5e:0:0:fb           en0
   224.0.0.1               1:0:5e:0:0:1            en0
   224.0.0.251             1:0:5e:0:0:fb           en1
   224.0.0.251             1:0:5e:0:0:fb           vmnet8
   224.0.0.1               1:0:5e:0:0:1            vmnet8
   224.0.0.251             1:0:5e:0:0:fb           vmnet1
   224.0.0.1               1:0:5e:0:0:1            vmnet1
   ```

Komentirajte vnose.

3. Peter bi rad s svetom delil posnetek TV programa, na katerem zelo pogosto predvajajo baročne suite. Ker takšne glasbe razen Petra, njegove matere in njunih redkih prijateljev nihče ne mara, ga bo oddajal le v domačem omrežju. Za oddajanje bo uporabil naslednjo ukazno vrstico:

```
cvlc --"sout=#transcode{vcodec=h264,vb=200,scale=0.5}: \
  rtp{dst=233.252.0.63,port=5004,mux=ts,ttl=1}" \
  --sout-keep peter.mp4
```

   Kako bi ukazno vrstico spremenil, če bi ga naenkrat hotelo poslušati na tisoče oboževalcev tovrstne glasbe, ki bi ga hoteli gledati v visoki ločljivosti? Odgovor utemeljite.

   Kako bi ukazno vrstico spremenil, če bi si sosed omislil električni kavni mlinček iz leta 1976 z zguljenimi krtačkami, mati pa bi koncerte svojega sina občudovala samo na prenosni tablici, ki jo vedno nosi s seboj? Pri obeh podvprašanjih lahko z utemeljitvijo tudi za nenatančen odgovor dobite vse točke (od vas se ne pričakuje, da boste na pamet poznali vsa stikala, ki jih VLC podpira).

4. NEOBVEZNO. Naštejte tri stavke francoske baročne suite.

3. naloga:

VPRAŠANJA:

1. Peter se je zapletel v prepir s prijateljem Simonom in trdil da je protokol RADIUS varen protokol, saj si je zapomnil, da je del paketa tudi avtentifikator. Pojasnite vlogo avtentifikatorja v protokolu RADIUS.

2. Napišite tri scenarije napada na RADIUS protokol in kakšno škodo lahko napad povzroči.

3. Kako protokol CHAP preprečuje napade s ponavljanjem?

4. naloga:

VPRAŠANJA:

1. Varovanje prometa se lahko dogaja na različnih plasteh. Zapišite vse plasti in kako se lahko na vsaki od teh plasti izvaja varovanja prometa (navedite tudi imena protokolov za posamezno plast).

2. IPsec protokol lahko deluje v prenosnem (*transport*) ali tunelskem (*tunnel*) načinu. Opišite, kako izgleda pretvarajanje paketov v tunelskem načinu na poti od izvora do ponora, pri čemer nas zanima samo avtentikacija paketa. Bodite pasljivi pri opisu glav posameznih paketov.

3. Kaj se nahaja v DNS zapisu PTR za domeno `d.c.b.a.in-addr.arpa`?

   Eden od možnih napadov na varnost interneta je napad na korenske DNS strežnike. Komentirajte, kako škodljivo bi bilo, če bi napadalec pridobil nadzor nad enim od korenskih strežnikov.

5. naloga: IEEE 802.

VPRAŠANJA:

1. Na predavanjih smo omenjali standard IEEE 802.1x in protokol EAPOL. V kakšnem odnosu sta si? Opišite funkcijo/namen standarda in protokola.

2. Te dni so potrdili nov standard IEEE 802.11ad poznan tudi kot *WiGig*:

   > *The IEEE Standards Association has approved WiGig, a very fast, short-range networking technology that operates in the 60-GHz band. WiGig, also known as 802.11ad, has the potential to eliminate the tangled bundle of wires at the back of PCs, and could start appearing in routers as early as the second or third quarter this year. The technology would transfer data at 7 Gbits per seconds, compared to current routers using 802.11g technology that transfer data at 50 Mbits/s and 802.11n at 100 Mbits/s.*

   Ko je Peter Zmeda prebral zgornjo novico, se je zelo prestrašil, saj je razumel, da bo moral zamenjati v podjetju vsa stikala in vse mostičke. Je njegov strah utemeljen? Utemeljite svoj odgovor.

   NAMIG: Povezavna plast IEEE 802 ni monolitna.

3. Protokol IEEE 802.1d se ukvarja z MAC mostički (*bridge*) in med drugim določa protokol za izgradnjo vpetega drevesa v omrežju. Zakaj potrebujemo vpeto drevo?