

**Komunikacijski protokoli in omrežna varnost**  
**2013/14**  
**Pisni izpit 24. prosinca 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 60 minut.  
Veliko uspeha!

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

IME IN PRIIMEK: \_\_\_\_\_

ŠTUDENSKA ŠTEVILKA: \_\_\_\_\_



DATUM: \_\_\_\_\_

PODPIS: \_\_\_\_\_

**1. naloga:** Peter Zmeda bi rad nekaj računalnikov pripravil do tega, da bi se zagnjali prek mreže. Postavil je strežnik DHCP na naslovu 192.168.1.1 z naslednjimi nastavitvami:

```
ddns-update-style none;
option domain-name-servers 193.2.1.66;
default-lease-time 600;
max-lease-time 7200;
allow booting;
subnet 192.168.1.0 netmask 255.255.255.128 {
    range 192.168.1.8 192.168.1.62;
    next-server 192.168.1.2;
}
```

VPRAŠANJA:

1. Vseeno se računalniki nikakor nočejo zagnati prek mreže. (i) Kaj je v njegovih nastavitvah narobe? Kaj v nastavitvah manjka? (ii) Če privzamemo, da so nastavitve pravilne, a nepopolne, kaj mora postoriti, da bo konfiguracija delovala? Ali lahko to naredi, ne da bi kupil kak dodaten računalnik? Utemeljite odgovor. 
2. Za protokola bootp in DHCP je znano, da ne skrbita kaj dosti za varnost. (i) Kako lahko uprizorimo napad s človekom na sredi (man in the middle) in kako lahko s tem napadom škodujemo odjemalcu, ki bi želel dobiti IP naslov? (ii) Glede na znanje iz celotnega predmeta opišite dva načina obrambe pred takšnim napadom ter utemeljite, zakaj naj bi obramba delovala. 
3. Peter Zmeda ponuja v Butalah dostop do interneta. Butalski veljaki so se dogovorili, da naj Lavdon Štimani pripravi spletno predstavitev o Butalah. Da bi bila spletna predstavitev vedno vidna širnemu svetu, mora Lavdonov računalnik dobiti stalen IPv4 IP naslov. Ali je to možno, glede na to, da Peter za dodeljevanje IP naslovov uporablja storitev DHCP?

**2. naloga:**

VPRAŠANJA:

1. Na prosojnicah piše, da protokol SNMPv3 „omogoča kriptografijo, zagotavlja zaupnost, integriteto, avtentikacijo.“ V ta namen uporablja več različnih mehanizmov. (i) Opišite enega od mehanizmov, (ii) pred kakšnim napadom nas ščiti in (iii) kje v paketih se pojavljajo njegovi podatki?

NAMIG: Na predavanjih smo omenjali RFC 3414.

2. Peter Zmeda se je po ekstremno divji noči zbudil v Carigradu. Vprašal se je: „Koliko je ura?“. Zagnal je ukaze:

```
peter@zmedotron: rdate -p nist1-nj.ustiming.org
Mon Jan 14 17:31:17 2013
peter@zmedotron: rdate -p ntpl.arnes.si
Mon Jan 14 23:31:28 2013
```

Koliko je dejansko ura, kjer se nahaja? Odgovor utemeljite. Carigrad se nahaja v časovnem pasu GMT+2.

3. Vir toka podatkov (SSRC) pošilja podatke sprejemniku. Kako lahko sprejemnik ugotovi kaj je pošiljatelj (kamera, mikrofonski, ...)?

### 3. naloga:

#### VPRAŠANJA:

1. Namen storitve IGMP je, da se odjemalci včlanijo v neko skupino, iz nje izpišejo in podobno. Cefizelj je natančno preučil, kako deluje protokol in je izvedel napad z pretvarjanjem. Rezultat je bil, da je nedolžni Butalec Kozmijan Buta pričel prejemati na svojem računalniku program klasične glasbe, kljub temu, da je zapriseženi ljubitelj rock glasbe. (i) Kaj točno je naredil Cefizelj? (ii) Podajte dva predloga, kako naj Peter nadgradi omrežje, da se to ne bo več dogajalo glede na vaš odgovor iz prvega dela vprašanja.
2. Peter je med čakanjem na gledališko predstavo opazil, da iz stene visi kabel s konektorjem RJ45. Nanj je priklopljen svoj računalnik. Ker ni takoj dobil naslova prek DHCP, je uporabil ukaz `ifconfig eth0 169.254.192.168 up`. Nenadoma je iz okna, kjer prodajajo karte, zaslišal tolčenje po tipkovnici. Računalniku, na katerem je blagajna, je nehala delovati mreža. (i) Če privzamemo, da je res kriv Peter – kolikšna je verjetnost, da je z zgornjim ukazom res nastavljen isti naslov, kot ga ima računalnik na blagajni? Na blagajni tečejo Microsoft Windows brez posebnih nastavitev, na omrežju pa ni DHCP strežnika. Odgovor utemeljite z računom. (ii) Ali je računalnik, na katerem teče blagajna, priklopljen na Internet? Utemeljite odgovor. (iii) Ali lahko računalnik pride do Interneta, če na omrežju ne deluje DHCP strežnik? Utemeljite svoj odgovor.
3. Peter Zmeda je zaznal na omrežju REGISTER paket PIM-SM protokola. Kdo komu pošilja omenjeni paket in s kakšnim namenom?
4. (NEOBVEZNO) Izraz „rock glasba“ (*rock music*) ima svojo etimologijo. Kakšno in zakaj?

**4. naloga:** Tepanjci in Butalci se običajno ne razumejo najbolje, vendar morajo pogosto izmenjevati podatke. Zato so se domislili, da bodo za zaščito komunikacije uporabili protokol IPsec. Pred vzpostavitvijo povezave so uporabili protokol IKE za izmenjavo ključev. Ker pa so imeli težave s podpisovanjem certifikatov, so se odločili, da prvo fazo protokola opuste. Ni minilo dolgo in Cefizelj se je prikopiral do zaupnih podatkov o navadah bolhe Šrinca Marogle, ki so si jih izmenjevali Tepanjci in Butalci. Ti podatki so zelo občutljivi, saj lahko dajejo prednost enemu ali drugemu kandidatu pri naslednjih županskih volitvah v Butalah.

VPRAŠANJA:

1. Butalci so na pomoč poklicali Petra Zmedo, ki je hitro ugotovil, da je Cefizelj v resnici glavni krivec in da je izvedel napad s pretvarjanjem (*spoofing*). (i) Opišite, kako je izvedel napad.

Ker imajo Butalci in Tepanjci tako velike težave s protokolom IKE, morajo za zagotovitev pravilnosti delovanja protokola IPsec nekako drugače rokovati s ključi. (ii) Predlagajte kako in zakaj.

2. Peter bi rad postavil svojo TV postajo. V ta namen si je postavil spletni strežnik Apache, na katerega je postavil nekaj video vsebin. Nato je ugotovil, da bi rad prenašal tudi vsebine v živo. Pobrskal je po Internetu in nekje našel naslednji ukaz (vse v eni vrstici):

```
vlc -vvv /dev/video0
  --sout '#transcode{vcodec=h264,vb=0,scale=0,
  acodec=mpga,ab=128,channels=2,samplerate=44100}:
  http{mux=ffmpeg{mux=flv},dst=0.0.0.0:80/}'
```

Ukaz seveda ni deloval. (i) Zakaj? (ii) Kako naj ga popravi, da bo deloval?

Peter bi rad povečal svoje občinstvo, ne bi pa plačeval za širšo povezavo v Internet, zato je svoj ukaz spremenil (ponovno vse v eni vrstici):

```
vlc -vvv /dev/video0
  --sout '#transcode{vcodec=h264,vb=0,scale=0,
  acodec=mpga,ab=128,channels=2,samplerate=44100}:
  rtp{mux=ts,dst=224.0.0.116,sdp=sap,name=PeterTV}'
```

(iii) Ali bo ta ukaz deloval? Zakaj bi se Petru lahko zdelo, da deluje, njegovi gledalci pa ne bi videli ničesar? (iv) Kako naj ukaz popravi, da bo deloval za več ljudi?

3. Za uporabo aplikacije NekiNeki se mora uporabnik prijaviti z imenom in priimkom. Aplikacije predvideva rabo protokola TCP. Peter je strežnik aplikacije postavil na intranet. Peter želi Cefizlju preprečiti uporabo aplikacije. S kakšnim načinom filtriranja to doseže?