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 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: Čeprav so posamezna vprašanja morda malce bolj vezana na določeno poglavje predavanj, je za reševanje vprašanja pogosto potrebno uporabiti znanje še iz drugih poglavij.

V Butalah imamo opravka s čudno druščino, ki se je odločila, da so Butale na drugem planetu kot preostanek Zemlje. Za novi planet Butale se seveda spodobi, da ima lasten Internet IPv4 z vsemi naslovi ter tudi lastno DNS storitev. Na primer, da se bo preslikal IP naslov

```
www.zmeda IN A 212.235.188.25
```

VPRAŠANJA:

1. Kaj morajo narediti, da bo njihova DNS preslikava delovala pravilno v vseh Butalah? Se pravi, da bo sistem deloval tako, da bo vsak računalnik v butalah izpisal:

   ```
   [Peter]:  nslookup
   > www.zmeda
   Non-authoritative answer:
   Name:  www.zmeda
   Address:  212.235.188.25
   > 212.235.188.25
   Non-authoritative answer:
   25.188.235.212.in-addr.arpa name = www.zmeda
   ```

2. Vendar se je kmalu izkazalo, da so si v Butalah nakopali kar nekaj težav s svojo odselitvijo v drug svet. Na primer sedaj ne morejo preprosto dostopati do Internetnih IP naslovov drugje na planetu Zemlja. Ali jim lahko predlagate, kako naj rešijo svojo zagato, da bo IP promet nekako tekel med obema svetovoma? Utemeljite svoj odgovor. Pa, seveda, da bi nazaj preštevilčili naslove svojih računalnikov ne pride v poštev, ker toliko trme je pa tudi v Butalah.

3. Peter Zmeda bi v podjetju rad poskrbel za res zanesljivo zaganjanje delovnih postaj prek omrežja. V ta namen je kupil 2 strežnika. Na oba je postavil vso potrebno programsko opremo. Večino časa delujeta oba, vendar če en odpove, naj bi drugi deloval naprej. Datotečni sistem bodo odjemalci hranili na NFS(v2) strežniku. i.) Strežnike za katere protokole bo Peter še potreboval, da bo zaganjanje delovalo? Naštejte vsaj dva in kakšno storitev nudita. ii.) Ali bodo naslovi obeh računalnikov enaki? Kaj pa podatki, ki jih nudijo zaganjajočim se delovnim postajam? Utemeljite odgovor.

2. naloga: Boris Brezdomec, najbolj znan čudak v vasi Podklanec, si je omislil sekto. Ker v vasi ni dosti prostora, so se Borisovi privrženci začeli zbirati kar prek Interneta. Ker Borisa častijo kot božanstvo, so se odločili, da bodo odslej čas merili od trenutka, ko je Boris prišel na naš svet – 11. 09. 1990. Za usklajevanje svojih ur nameravajo uporabljati kar protokol `rdate`, saj boljšega ne poznajo.

VPRAŠANJA:

1. Če hočejo obdržati nespremenjene `rdate` odjemalce na svojih računalnikih, morajo kako spremeniti programsko opremo na strežniku?

2. Peter Zmeda bi zelo rad poskrbel, da bi imeli Borisovi privrženci, ki pridejo vseeno v vas, res točne ure. Zato bi rad postavil NTP strežnik, ki bo na nivoju (stratum) 1. Na žalost ima na voljo le povsem nov pametni telefon z odklenjenim operacijskim sistemom Android (ki podpira vse, kar se le da – WiFi, Bluetooth, GSM, GPRS, GPS, UMTS, IRDA, itd.) in star računalnik. Sektašem je postavil lokalno omrežje. Edini dostop do Interneta imajo prek pametnega telefona. Ali lahko Peter s pravo programsko opremo sestavi NTP strežnik, ki bo na nivoju 1?

   NAMIG: Upoštevajte, da je seveda Peter odličen programer in da lahko povsem ukroti tako telefon kot računalnik z vsemi vhodno/izhodnimi enotami.

3. Na predavanjih smo omenili, da je protokol RTP vložen v UDP pakete. Ali bi ga lahko vložili v TCP pakete? Utemeljite odgovor.

3. naloga: Pri razpošiljanju smo omenjali usmerjevlane protokole in najpogosteje smo omenjali protokol PIM. Na prosojnici pri predavanjih opazimo, da se razlikujeta v stolpcu *vrsta drevesa*.

VPRAŠANJA:

1. O kakšnih drevesih govorimo in kakšna je vloga le teh pri razpošiljanju?

   NAMIG: Najbolje to ponazorite z opisomo paketa, ki ga razpošiljamo.

2. Tako je v tem stolpcu zapisano, da ima razpršeni način delovanja *skupno* in gosti način delovanja *posamezno* drevo. Zakaj?

3. Peter Zmeda bi rad predvajal posnetek koncerta prek Interneta. Rad bi ponudil tako glasbo, kot tudi sliko dirigenta. Poleg tega bi rad omogočil poslušanje koncerta tudi tistim, ki jih slika ne zanima. Napisal je naslednjo skripto:

```
#!/bin/sh

cvlc --sout="#transcode{vcodec=h264,vb=200,scale=0.5, \
  acodec=mp3,ab=128,channels=2,samplerate=44100}: \
  http{mux=ts,dst=:8080/}" --sout-keep  &
cvlc --sout="#transcode{vcodec=none,acodec=mp3,ab=128, \
  channels=2,samplerate=44100}: \
  http{mux=ts,dst=:8080/}" --sout-keep  &
cvlc --sout="#transcode{vcodec=none,acodec=mp3,ab=128, \
  channels=2,samplerate=44100}:rtp{dst=233.252.0.63, \
  port=5004,mux=ts,ttl=1}" --sout-keep  &
```

i.) Ker njegova skripta ne deluje napišite popravljeno različico. ii.) Na kateri naslov bi se morali povezati njegovi poslušalci, da bi bil strežnik čim manj obremenjen, ne glede na to, da je poslušalcev tisoče? iii.) Zakaj bi ta naslov utegnil ne delovati?

4. NEOBVEZNO. Katero opero je v lanskem letu zelo uspešno uprizorila Univerza v Ljubljani?

4. naloga: Peter se je lotil postavljanja zasebnega omrežja. Uporabniki na tem omrežju se bodo avtenticirali s certifikati. Za izdelavo certifikatov Peter uporablja skripte EasyRSA. Za izdelavo certifikata za vsakega uporabnika požene naslednje ukaze:

```
peter@zmeda.si:openvpn> ./build-key USERNAME
Generating a 1024 bit RSA private key
.....................................++++++
........++++++
writing new private key to 'USERNAME.key'
-----
You are about to be asked to enter information that will be
incorporated into your certificate request.
What you are about to enter is what is called a Distinguished
Name or a DN. There are quite a few fields but you can leave
some blank For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [SI]:SI
State or Province Name (full name) [LJ]:BT
Locality Name (eg, city) [Laibach]:Butale
Organization Name (eg, company) [FRI]:Brihte
```

```
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server’s hostname) [USERNAME]:USERNAME
Name []:Uporabnik
Email Address [anonymous@zmeda.si]: nekdo@bposta.com
Please enter the following ’extra’ attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from /home/polz/openvpn/openssl.cnf
Check that the request matches the signature
Signature ok
The Subject’s Distinguished Name is as follows
countryName           :PRINTABLE:’SI’
stateOrProvinceName   :PRINTABLE:’BT’
localityName          :PRINTABLE:’Butale’
organizationName      :PRINTABLE:’Brihte’
commonName            :PRINTABLE:’USERNAME’
name                  :PRINTABLE:’Uporabnik’
emailAddress          :IA5STRING:’nekdo@bposta.com’
Certificate is to be certified until Jan 12 23:44:46 2023 GMT
(3650 days)
Sign the certificate? [y/n]:y
1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

Nato uporabniku pošlje datoteko `UPORABNIK.crt`, kjer je UPORABNIK uporabniško ime uporabnika.

VPRAŠANJA:

1. Kaj vse bi moral uporabnikom še poslati? Komentirajte njegovo početje s stališča varnosti.

2. Za enega od uporabnikov, Ceneta, je pripravil naslednjo OpenVPN konfiguracijsko datoteko:

   ```
   remote openvpn.zmeda.si
   # dev tap0
   dev tun
   proto tcp-client
   tls-client
   dh dh1024.pem
   ca ca.crt
   cert dejan.crt
   key dejan.key
   ```

Ali lahko povsem enako datoteko za vzpostavitev povezave uporabi tudi uporabnik Dejan? Če da, kaj mora storiti, če ne, zakaj ne?

3. V poglavju o varnosti smo omenjali certifikate pri protokolu SSL in pri protocolu IPSec. Gre za isti certifikat? Katere podatke točno vsebuje certifikat in razložite vlogo posameznih podatkov.

4. Na predavanji smo prosojnicah zapisali:

   > Tudi, če MAC pošljemo po zaključku celega prenosa (vseh zlogov), nimamo vmesnega preverjanja integritete!

   in nato dopisali, da zato razbijemo celoten tok podatkov v zapise. Obrazložite, kakšna nevarnost oziroma škoda bi lahko nastala, če bi MAC poslali samo na koncu. Morda si lahko pomagate s primerom.