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.

VPRAŠANJA:

1. Ko nalagamo na računalnik operacijski sistem z omrežja, to naredimo v štirih korakih. Kateri so ti koraki in kateri protokol uporabljamo pri posameznem koraku?

2. Pri upravljanju z omrežji smo omenjali SNMP protokol in entiteti *agent* ter *upravljalec*. Kje se nahaja upravljalec in kje agent? Recimo, da želimo izvedeti koliko papirja je še v tiskalniku. Kdo od njiju pošlje sporočilo komu in kakšno je sporočilo?

3. Kako RFC 2131 ureja obstoj večih DHCP strežnikov?

2. naloga: Peter Zmeda na svojem računalniku, ki ima naslov 15.2.20.13, posluša radijsko postajo *Puccini*, na kateri predvajajo samo Puccinijeve opere. Poslušalci radijske postaje so člani razpošiljevalne (*multicast*) skupine 224.77.66.55.

VPRAŠANJA:

1. Peter želi nehati poslušati radio in zato mora njegov računalnik zapustiti razpošiljevalno skupino, za kar uporabi IGMPv2 protokol. Narišite poslani IP paket ter IGMP sporočilo s čim več polji ter njihovo vsebino. Komentirajte, kako varno je takšno sporočilo.

   NAMIG: Prvi del vprašanja je s predavanj, pri drugem delu (varnost) pa razmislite, kako lahko kdo škodi Petru pri rabi takšnih in podobnih sporočil. Naštejte vsaj tri scenarije.

2. Na predavanjih smo omenili, da se pri razpošiljanju uporablja usmerjanje po povratni poti (*Reverse path lookup*). Kje se to uporablja in zakaj?

3. Kaj je osrednja točka (*rendezvous point* – RP)?

3. naloga: Abdul, Bob, Cefizelj in Damjan M. postavljajo skrivnostno omrežje za izmenjavo podatkov o „pogrešanih“ slikah. Za izmenjavo podatkov so se odločili, da bodo uporabljali OpenVPN. Trenutno njihove konfiguracijske datoteke izgledajo takole:

```
  abdul.cfg:
remote 10.0.0.15
dev tap0
proto tcp-client
secret vnpkey1.key
  bob1.cfg:
dev tap0
proto tcp-server
secret vpnkey1.key
  bob2.cfg:
dev tap1
secret vpnkey2.key
  cefizelj1.cfg:
remote 212.235.189.164
dev tap3
secret vpnkey2.key
  cefizelj2.cfg:
dev tun
proto tcp-server
secret vpnkey3.key
  slavcek.cfg:
remote 193.2.76.40
proto tcp-client
dev tun
secret vpnkey3.key
```

VPRAŠANJA:

1. Pri delovanju VPN smo govorili o bazi SAD. Kaj hrani baza SAD? Katere elemente/lastnosti/atribute vsebuje posamezen zapis v bazi SAD ter kakšen je pomen oziroma uporaba posameznega atributa?

2. Narišite primer omrežja, kjer bi zgornja konfiguracija lahko delovala (znotraj katerega bi lahko postavili delujoč VPN s takšnimi konfiguracijskimi datotekami). Označite vse IP naslove vsakega računalnika. Na povezavah označite naslov in omrežno masko omrežja.

3. Kaj morajo vsi štirje storiti, da bodo lahko prek IP naslovov na svojem navideznem omrežju dostopali drug do drugega? Privzemite, da so si datoteke s ključi že izmenjali.

4. NEOBVEZNO. Pred kratkim je v Sloveniji izginile tri slike nekega znanega slovenskega slikarja sicer doma iz Škofje Loke. Čigave slike so postale „pogrešane“.

NAMIG: Naslovi pogrešanih slik so *Mileva Zakrajšek*, *Petermanova Francka* in *Deklica*

4. naloga:

VPRAŠANJA:

1. Pri imeniški storitvi obstajata dva načina porazdeljevanja. Katera načina sta to in kdaj bi uporabili kakšnega od njiju?

2. Peter Zmeda je vzpostavil svojo novo spletno storitev PDR – *pomoč drugemu rulz*. Pred uporabo storitve se mora uporabnik avtenticirati z geslom, katero je shranjeno v LDAP imeniku, ki ga upravlja Špela. Peter uporablja za preverjanje gesla ukaz `search`. Zakaj Peter nikakor ne more spraviti svoje storitve v delovanje? Razložite in utemeljite odgovor.

3. Kaj pomeni zapis

   ```
   root:$6$zf422XNk$AAK/eSb7lV2AqVYok676...
   ```

   v datoteki `/etc/shadow`?