Komunikacijski protokoli in omrežna varnost
2015/16
Pisni izpit 28. prosinca 2016

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 in DHCP.

VPRAŠANJA:

A) Peter se je pripravljal na izpit iz KPOV. Ob poglavju o nalaganju operacijskega sistema je spoznal, da pozna protokol `bootp` vmesni strežnik (*proxy* oziroma *gateway*). (i) Podrobno opišite njegovo vlogo.

   NAMIG: Najbolje, če opišete po korakih kako potujejo sporočila med napravami.

   (ii) Poleg tega je spoznal, da se sam operacijski sistem naloži s pomočjo protokola `tftp`. Nekje je slišal, da pri slednjem ne potrebuje vmesnega strežnika. Zakaj bi ga ne potreboval?

B) Peter je s spleta pobral datoteko `delajdenar.tgz`. Datoteka naj bi vsebovala program, ki ob zagonu kar sam ustvari denar na računu osebe, ki ga je zagnala. Ko je Peter datoteko razpakiral s pomočjo ukaza `tar`, je dobil v trenutnem imeniku imenik `delajdenar`, v katerem pa še podimenika `bin` ter `data`. V podimeniku `bin` je našel datoteko `mula`, ki pa je ne more pognati, ker nima ustreznih pravic. (i) Kaj mora Peter storiti, da bo program lahko pognal? Privzemite, da program na Petrovem računalniku deluje.

   NAMIG: Napišite ukaz; če bo imel na koncu preveč pravic ali če bo kako pravico izgubil, ne boste dobili vseh točk.

   (ii) Kako naj program požene, ne da bi se premaknil iz imenika, *v katem se je nahajal na začetku, ko je razpakiral dobljeno datoteko*?

C) Pri prenašanju paketov IPv4 lahko pride do fragmentacije, kar lahko povzroči težave. Kako lahko Cefizelj uporabi fragmentiranje, da napade Petrov strežnik? Podrobnejši ko bo opis, več točk dobite.

2. naloga: Upravljanje omrežij. Peter je končno postavil celovito SNMP okolje v svojem podjetju, kar mu omogoča učinkovito upravljanje z omrežjem in napravami v njem. Toda po nekaj dneh delovanja je ugotovil, da Cefizelj uspešno prisluškuje prometu na omrežju.

VPRAŠANJA:

A) Peter se je odločil, da bo zakril SNMP promet, a ve, da ne more uporabiti SSL zaščite. (i) Zakaj je ne more uporabiti? (ii) Zaradi tega se je odločil, da bo zakrival promet z uporabo kriptiranja z veriženjem. Kaj vse bo moral spremeniti v programski opremi svojega omrežja, da bo lahko implementiral kriptiranje SNMP paketov z veriženjem? Utemeljite odgovor.

B) Peter Zmeda je zagrizen uporabnik Linuxa. Čeprav dela v podjetju, kjer uporabljajo Active Directory podjetja Microsoft, ne bi rad menjal operacijskega sistema na svojem računalniku. Toda Petrov šef zahteva, da le-ta na svojem računalniku omogoči prijavo vsem uporabnikom, ki so v imeniku. Ali Peter lahko to stori? Če ne – zakaj ne in katere kose programske opreme bi moral napisati, da bi prijavo omogočil? Če da – katere kose programske opreme mora namestiti?

C) Včasih želimo najti objekte na osnovi bolj zapletenih poizvedb. Lahko bi na primer iskali vse ljudi iz Maribora, ki jim je ime Janez ali Borut. Vprašanje je, ali poizvedbeni jezik, s katerim dobivamo podatke iz baze LDAP, kaj takega sploh podpira? Utemeljite odgovor.

3. naloga: Čas in spletne storitve.

VPRAŠANJA:

A) Varnost v RTP protokolu definira SRTP inačica protokola. Slednja uvaja varnost preko kriptitanja s tokom šifer. (i) Ali slednje zagotavlja integriteto sporočil? Utemeljite odgovor.

Ena od ključnih informacij je skupna skrivnost. (ii) Ali bi lahko uporabili IKE protokol za pridobitev le-te? Utemeljite odgovor.

NAMIG: Če menite, da se IKE da uporabiti, potem opišite korake; in, če menite, da se ne da, utemeljite, zakaj se ne da.

B) Peter je napisal program, ki naj bi bil strežnik `rdate`. Program zaganja prek `inetd`, pisan je v jeziku Pythonu, izgleda pa nekako takole:

```
import time
import struct
import sys
t = time.time() # time since the Epoch in seconds
# i -> signed integer, ! -> network byte order
sys.stdout.write(struct.pack("!i", int(t)))
```

Kaj vse je Peter storil narobe oziroma na kaj je pozabil? Utemeljite odgovor.

C) Petrovi predpostavljeni so bili zelo nezadovoljni s kakovostjo zvoka na svoji ponedeljkovi jutranji spletni konferenci. Konferenca je običajen način začetka tedna in v njej sodelujejo vodje oddelkov v Butalah, v Višnji gori in v Abderi. Peter je podrobneje pregledal sistem in ugotovil, da se kar nekaj paketov izgubi. Da bi se izognil izgubi paketov, se je odločil uporabiti TCP protokol

namesto UDP protokola. (i) Komentirajte smiselnost njegove odločitve. Utemeljite svoj komentar. (ii) Ali bi bil vaš kaj drugačen, če bi sodelovala samo vodji iz Butal in Abdere? Utemeljite svoj odgovor.

4. naloga: Povezavna in mrežna plast ter omrežna varnost.

VPRAŠANJA:

A) Pri varnosti govorimo o večih komponentah. Dve od njih sta: zakrivanje podatkov in integriteta podatkov. (i) Katera sta matematična postopka ali mehanizma, ki omogočata vsako od obeh komponent? Opišite ju. (iii) Kako lahko na tretji plasti poskrbimo za vsako od njiju? Opišite oba mehanizma. (iii) Ali VLAN na drugi plasti zagotavlja katerokoli od obeh komponent? Utemeljite odgovor.

B) Peter in Konrad sta postavila navidezno omrežje z uporabo OpenVPN. Konrad ima takšnole nastavitveno datoteko:

```
proto tcp
dev tap
remote 193.2.167.13
secret AAAA
```

(i) Kakšno nastavitveno datoteko ima Peter? (ii) Kdo med njima ima OpenVPN strežnik? Utemeljite odgovor. (iii) Je vrstica s `secret` lahko pri Petru drugačna kot pri Konradu? Utemeljite odgovor. (iv) Peter se boji, da takšna skrivnost ni varna. Konrad se s tem ne strinja. Kdo ima prav? Utemeljite odgovor. (v) Koliko bitov je dolga skrivnost? Utemeljite odgovor.

C) Cefizelj je prišel v podjetje, kjer za zaščito ožičenega omrežja uporabljajo standard IEEE 802.1x. Rad bi se priklopil na mrežo. Katerega od pristopov lahko uporabi?

- Poveže se na eno od nezasedenih ethernet vtičnic; uporabi ranljivost na strežniku RADIUS, da pridobi dostop.
- Naj raje obupa – IEEE 802.1x je varen in dobro napisan standard, tako da varnostne luknje, ki bi delovale na opremi različnih proizvajalcev, niso široko znane.
- Med enega od avtenticiranih računalnikov in omrežje vrine svoje ethernet stikalo; to stikalo potem uporabi za dostop do omrežja.
- Zajame promet enega od računalnikov na mreži, izvede napad s ponavljanjem.

Utemeljite odgovor. Pri utemeljitvi tudi zapišite zakaj ostali odgovori niso zadovoljivi.