Komunikacijski protokoli in omrežna varnost
2014/15
Pisni izpit 20. svečana 2015

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: Za uspešno nalaganje operacijskega sistema mora računalnik opraviti štiri korake: a) znati poiskati strežnik, s katerega bo naložil OS; b) znati se nastaviti, kot bo svetoval/zahteval strežnik; c) prenesti OS k sebi; ter č) namestiti OS in ga zagnati.

VPRAŠANJA:

1. V sklopu nalaganja OS smo srečali več protokolov. (i) Kateri protokol poskrbi za posameznega od zgoraj naštetih korakov? (ii) Opišite kako in kakšni podatki potujejo po omrežju, če sta na voljo dva strežnika, ki pošljeta nasvet/zahtevek v koraku b).

2. Peter Zmeda bi rad spravil svoj računalnik na Internet. Pognal je

   ```
   Peter> ping -c 3 193.2.1.87
   PING 193.2.1.87 (193.2.1.87): 56 data bytes
   Request timeout for icmp_seq 0
   Request timeout for icmp_seq 1
   --- 193.2.1.87 ping statistics ---
   3 packets transmitted, 0 packets received, 100.0% packet
   loss
   ```

   Sedaj bi rad preveril, ali ima sploh nastavljen privzeti prehod. Ve, da se v imeniku `/usr/local/nettools` nahaja program `route`, ni pa se še odločil, kako bi ga pognal. (i) Kako bi lahko preveril, katere imenike ima naštete v okoljski spremenljivki `PATH`? (ii) Recimo, da ima Peter spremenljivko `PATH` nastavljeno na:

   ```
   /usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games
   ```

   Naštejte 4 zaporedja ukazov, s katerimi lahko zažene program – dve zaporedji tako, da spremeni `PATH`, dve brez spreminjanja.

3. Kako odjemalec ve pri protokolu TFTP, da je dobil zadnji paket s podatki?

2. naloga: Upravljanje omrežij.

VPRAŠANJA:

1. Polja RADIUS paketa so med drugim *Code*, *Identifier* in *Authenticator*. Za vsako od polj opišite: (i) čemu služi; in (ii) kako se uporablja v toku protokola.

2. Peter se je odločil, da bo za nadzor svojega računalnika uporabil protokol SNMP. Namestil je snmpd in pognal ukaz:

```
Peter> snmpwalk -c public localhost
snmpwalk: No securityName specified
```

(i) Zakaj je prišlo do napake / kako si razlagate napako? Nato je pognal:

```
Peter> snmpwalk -c public -v 2c localhost
```

Ukaz je tokrat deloval, vendar mu ni izpisal vseh podatkov, ki bi jih od računalnika lahko pričakoval. (ii) Kaj je naredil narobe? (iii) Kaj mora popraviti oz. nastaviti, da bo prišel do ostalih podatkov, do katerih bi lahko dostopal prek SNMP?

3. Prejeli smo naslednji niz zlogov v TLV zapisu (najprej onega povsem na desni, vrednosti so desetiške):

   ```
   33 73 82 70 22 04 00 01 00 01 04 02
   ```

   Kaj pomeni prejeti niz? Utemeljite odgovor.

3. naloga: Varnost in navihanost.

VPRAŠANJA:

1. Nekje med letom smo omenjali protokol IKE. (i) V povezavi s čim smo ga omenjali? (ii) Kaj je tista najpomembnejša zadeva, ki jo uporaba protokola IKE poenostavi? Kako in zakaj?

2. Čas počitnic je mimo in Peter Zmeda je prijatelju pripovedoval zgodbo iz hotelske sobe. V hotelski sobi našel vtičnico po standardu RJ45. S kablom se je priklopil nanjo in njegov računalnik je v nekaj sekundah dobil naslov 169.254.13.5. Vseeno mu dostop do Interneta ne deluje. (i) Zakaj? (ii) Kako menite, da je njegov računalnik pridobil naslov?

3. Ti nesrečnik Peter. Ponovno so mu vdrli v računalnik. Tokrat so mu ukradli zakriptirana gesla. Na srečo so bila zasoljena, toda na žalost so ukradli tudi soli posameznih gesel. Kako (če sploh) si lahko napadalec pomaga s plenom, da bo prišel do gesel? Utemeljite odgovor.

   NAMIG: Pri utemeljitvi upoštevajte predvsem časovno praktičnost napada.

4. naloga: Stvarni čas in okoli njega.

VPRAŠANJA:

1. Omrežni protokol, ki se uporablja za nastavljanje lokalnega časa je ntp. (i) Na kateri plasti deluje in kateri so protokoli na plasteh pod njim? (ii) Ena osnovnih težav, ki nastopi pri pridobivanju časa z drugega računalnika, je zakasnitev. Kje vse nastopi ta zakasnitev in kako jo protokol odpravlja?

2. Peter Zmeda bi rad predvajal posnetek koncerta prek Interneta in želi ponuditi tako glasbo, kot tudi sliko dirigenta. Poleg tega bi rad omogočil poslušanje koncerta tudi tistim, ki jih slika ne zanima. Napisal je naslednjo skripto (vrstice so lomljene zaradi izpisa):

   ```
   #!/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  &
   ```

   Njegova skripta žal ne deluje. (i) Kaj bi moral Peter popraviti, da bi vse skupaj delovalo? (ii) Bi mu moral pomagati še kdo in če da, kako? (iii) Kaj bi moral Peter dodati, da bi lahko koncert z manj slabe vesti poslušali tudi uporabniki mobilnih naprav, ki za vsak prenešeni kilobajte drago plačajo?

3. Ali je mogoče in zakaj je morda koristno ter zakaj nespametno prenašanje RTP prometa prek HTTP? Utemeljite odgovor.