Komunikacijski protokoli in omrežna varnost
2014/15
Pisni izpit 24. svečana 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 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. Danes je vse v oblakih in včasih je tam tudi naš prijatelj Peter Zmeda. Tako vsaj izgleda zaradi njegovega meglenega poznavanja sistemov za upravljanje in nadzor.

VPRAŠANJA:

1. Od oblakov si je Peter zapomnil tudi to, da je osrednja tehnologija, ki jih poganja, virtualizacija strojev. Naučil se je postaviti fizični strežnik ter na njem zaganjati navidezne stroje. Pri zagonu navideznega stroja bi Peter želel nastaviti tudi MAC naslov le-tega. Našel je naslednje navodilo, kako se to lahko naredi na operacijskih sistemih unix:

   ```
   ifconfig eth0 hw ether 01:02:03:04:05:06
   ```

   Poleg tega Peter pozna protokol bootp in je prišel na idejo, da bi vrednost MAC naslova dobil ob zagonu s pomočjo protokola bootp ter nato nastavil na stroju želeni MAC naslov. Komentirajte njegov pristop in utemeljite svoj komentar.

   NAMIG: Pomagalo bo, če si najprej zapišete celoten scenarij (sosledje korakov) nastavljanja ter na podlagi tega komentirate Petrov pristop.

2. Poleg tega ima Peter zoprno težavo. Ima računalnik z brezžičnim in ožičenim vmesnikom. Vseeno želi, da računalnik dobi isti IP naslov ne glede na to, s katerim vmesnikom je priklopljen na omrežje. Ali to lahko naredi? Če da, predlagajte kako in, če ne, obrazložite zakaj ne.

3. Kaj pomeni, če imata prva zloga TFTP paketa vrednosti `00 05`?

2. naloga: Upravljanje omrežij.

VPRAŠANJA:

1. Upravljanje z napravami in omrežji smo razdelili na več področij. (i) Katera so ta področja? (ii) Za vsako od področij opišite konkreten primer upravljanja in programsko opremo, ki le-to omogoča.

2. Peter je na računalniku z naslovom 192.168.1.3 pognal:

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

   Potem je pognal še:

   ```
   snmpwalk -v 2c -c public 192.168.1.3
   ```

   Prvi ukaz je deloval, pri drugem pa je dobil odgovor:

```
Timeout:  No Response from 192.168.1.3
```

(i) Kaj menite, da je s Petrovimi nastavitvami oziroma ukazom, ki ga je pognal, narobe? (ii) Nastavitve katerega programa bo moral popraviti, če uporablja privzeto namestitev Debiana, kot smo jo na vajah? (iii) Točno kateri protokol uporablja Peter?

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

   ```
   00 01 00 01 05 02 33 73 82 70 04 04
   ```

   Kaj pomeni prejeti niz? Utemeljite odgovor.

3. naloga: V tej nalogi bomo pomagali Petru postaviti spletni studio za oddajanje programa.

VPRAŠANJA:

1. Kot rečeno, se je Peter odločil, da bo postavil svojo internetno televizijo. Najprej je hotel predvajti le en video, ki ga je potegnil z naslova http://goo.gl/zPOD in ga shranil v datoteko zPOD.mp4. Zagnal je pretakanje (vse v eni vrsti):

   ```
   cvlc " --sout=#rtp{dst=239.255.1.1,port=5004,mux=ts,sap,name=zPOD}"
        --sout-keep zPOD.mp4
   ```

   Sedaj želi predvajal še video z naslova http://goo.gl/QNfNM. Pognati namerava (ponovno vse v eni vrsti)::

   ```
   cvlc " --sout=#rtp{dst=239.255.1.1,port=5004,mux=ts,sap,name=20pcnt}"
        --sout-keep QNfNM.mp4
   ```

   (i) Ali bo operacijski sistem takšen zagon VLC sploh dovolil? (ii) Bodo odjemalci lahko gledali oba videa? (iii) Če je na odjemalcih naslov oblike: rtp://IP:VRATA, ali lahko izberejo, kateri video bodo gledali? Utemeljite odgovor. (iv) Kako bi Peter še lahko spremenil zgornja ukaza, da bi bila izbira videa čim lažja? Sprememba ukazov naj bo *čim manjša*.

2. Ali je (vse v eni vrsti)

   ```
   11110000 00011100 00000000 10110111 10001001
   11011001 10010000 01101010 01011111 10101001
   00011001 01110001 11110100 10111100 01110000
   00111101
   ```

   lahko binarna predstavitev IPv6 razpošiljevalnega (multicast) naslova? Utemeljite odgovor.

3. Med Petrovimi naročniki je kar nekaj borznih navdušencev. Posredovali so mu željo, da jim ponudi kar se da sveže novice o dogajanju na borzah po svetu. Peter je našel ponudnika teh novic, vendar le-ta zahteva, da se podatki ne smejo posredovati drugače kot v kriptirani obliki. (i) Kako lahko Peter v svojem omrežju razpošilja (*multicast*) kriptirane vsebine? Opišite vsaj dva možna načina. (ii) Pri enem od načinov (izberite si ga sami) opišite korake, ki so potrebni, da lahko prične z oddajanje kriptirane vsebine.

4. naloga: Razno.

VPRAŠANJA:

1. Pri tem vprašanju se bomo pogovarjali o varnosti hrambe gesel. Eden od napadov na shranjena gesla se imenuje mavrični napad (*rainbow attack*). (i) Kaj mora pridobiti napadalec, da ga lahko izvede in kako deluje?

   Običajna zaščita pred tem napadom je soljenje gesel. (ii) Kako deluje soljenje? Pri opisu bodite natančni in opišite tudi razliko glede na delovanje pri nesoljenih geslih. (iii) Recimo, da napadalec ukrade tudi sol. Ali mu lahko to pomaga pri mavričnem napadu? Utemeljite odgovor.

2. Peter se je odločil, da postavi svoj Radius strežnik in ga uporabi tako, kot smo ga naučili na vajah. Skonfiguriral je Freeradius in Apache tako, da se pri dostopanju do ene od podstrani na svojem spletnem strežniku avtenticira z uporabniškim imenom in geslom, ki sta shranjena v datoteki /etc/freeradius/users.

   Sedaj bi Peter rad uporabnikom svojega brezžičnega omrežja omogočil, da se prijavijo na omrežje vsak s svojim uporabniškim imenom in geslom. (i) Ali lahko v ta namen uporabi isti radius strežnik, čeprav se nanj že povezuje Apache? Utemeljite odgovor.

   Petrova mama včasih nima posluha za njegove ideje in mu tako občasno izklopi strežnik, na katerem poganja Freeradius. Peter želi, da njegovo brezžično omrežje deluje tudi, če mu mati izklopi strežnik. (ii) Kaj se bo zgodilo, če Freeradius strežnik odpove, uporabnikom, ki so v tem trenutku prijavljeni na omrežje? Kateri uporabniki njegovega omrežja bodo imeli težave in kakšne? (iii) Kako bi Peter odpravil takšne težave?

3. Spet težave. Peter Zmeda je naredil napako – na omrežnem stikalu je z mrežnim kablom nehote neposredno povezal dve luknji. Mreža je prenehala delovati. Zakaj je prišlo do napake in kako jo lahko Peter odpravi? Utemeljite odgovor.