Komunikacijski protokoli in omrežna varnost
2019/20
Pisni izpit 31. prosinca 2020

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 60 minut.

Veliko uspeha!

NALOGA	TOČK	OD TOČK	NALOGA	TOČK	OD TOČK
1			3		
2			4		

IME IN PRIIMEK: _____

ŠTUDENTSKA ŠTEVILKA: _____

DATUM: _____

PODPIS: _____

1. naloga: Osnove delovanja omrežij. Cefizelj je brihten poba in je naredil načrt, kako bo napadel strežnik butalskih oblasti, ki je na IP naslovu 197.44.41.204. Najprej bo pridobil omrežje botov (*botnet*) in nato bo vsak izmed botov poslal ping zahtevo na naslov 23.192.3.212, vendar tako, da bo v polje pošiljatelja dal IP naslov 197.44.41.204.[1] Za začetek je Cefizelj sam poskusil ping ukaz na omenjeni naslov in dobil naslednji rezultat

```
Cefizelj > ping 23.192.3.212 -c 8
PING 23.192.3.212 (23.192.3.212): 56 data bytes
64 bytes from 23.192.3.212: icmp_seq=0 ttl=47 time=230.110 ms
64 bytes from 23.192.3.212: icmp_seq=1 ttl=47 time=268.099 ms
64 bytes from 23.192.3.212: icmp_seq=2 ttl=47 time=307.391 ms
64 bytes from 23.192.3.212: icmp_seq=3 ttl=47 time=116.082 ms
64 bytes from 23.192.3.212: icmp_seq=4 ttl=47 time=182.987 ms
64 bytes from 23.192.3.212: icmp_seq=5 ttl=47 time=222.148 ms
64 bytes from 23.192.3.212: icmp_seq=6 ttl=47 time=266.222 ms
64 bytes from 23.192.3.212: icmp_seq=7 ttl=47 time=306.350 ms
--- 23.192.3.212 ping statistics ---
8 packets transmitted, 8 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 116.082/237.424/307.391/60.612
ms
Cefizelj >
```

VPRAŠANJA:

A) (i.) Opišite kaj je omrežje botov in kako deluje. (ii.) Odgovori na ping zahtevo naj bi po Cefizljevem načrtu leteli kam? Zakaj? Kako? (iii.) Kje in kako se lahko postavi obramba pred takšnim napadom? (iv.) Opišite dva možna razloga, zakaj so časi v Cefizljevem poskusu tako različni.

B) Kaj naj bi ščitil *SecureBoot*? Kako?

C) Peter je priklopil svoj računalnik na omrežje, vendar mu dostop do Interneta ne deluje. Spletni brskalnik mu takoj javi, da ne more najti strežnika `www.google.com`. S programom `ifconfig` je preveril, da ima naslov 192.168.1.1. Preveril je tudi, da ima v `/etc/resolv.conf` napisan naslov strežnika DNS. (i.) Kaj naj še preveri, da bo prepričan, da so nastavitve na njegovem računalniku pravilne? (ii.) Ko bo prepričan, da je računalnik nastavljen pravilno, kako naj naprej išče izvor napake?

[1] Po izpitu poskusite ugotoviti, kdo ima ta IP naslov. Opišite na forum, kako ste to ugotovili. Vsaj na dva načina.

2. naloga: Moje omrežje in njegovo upravljanje.

VPRAŠANJA:

A) (i.) Katera so področja upravljanja z omrežjem? (ii.) Za vsako od področij podajte po en primer upravljanja.

B) Peter na svojem omrežju uporablja DHCP. Zaradi težav s strojno opremo se je odločil, da zamenja strežnik. Na omrežje je postavil nov računalnik in na njem namestil ISC DHCP3. Nastavil je področje, na katerem dodeljuje naslove. Nekaj ur po menjavi strežnika je opazil, da omrežje deluje brez težav. Še več, naslovi večine računalnikov se niso niti spremenili, čeprav je bila veljavnost naslovov (lease duration) nastavljena na 30 minut. (i.) Zakaj se IP naslovi večinoma niso spremenili? Kako je strežnik dobil trenutne naslove? (ii.) Opišite vsaj en primer, ko bi se IP naslov računalnika na omrežju lahko spremenil.

C) Za nalaganje operacijskega sistema se običajno uporablja protokol TFTP. (i.) Narišite paket(e) protokola in opišite, kaj se nahaja v posameznem delu paketa. (ii.) Protokol TFTP je koračni protokol. Opišite kako je izvedena koračnost? Navedite primer. (iii.) Kako odjemalec ve, da se je pričel prenos datoteke in kako ve, da se je končal?

3. naloga: Čas in televizija.

VPRAŠANJA:

A) SRTP je varni RTP protokol. (i.) Koliko RTP paketa kriptiramo z njim? (ii.) Zakaj te dele in ne preostalih?

B) Peter Zmeda postavlja *Butalsko Televizijo*. Za razpečevanje videomateriala bi rad uporabljal razpošiljanje. V ta namen namerava uporabiti naslove med 172.18.0.1 in 172.19.255.254. Strežnik je na naslovu 192.168.1.31. (i.) So ti naslovi primerni? Utemeljite odgovor. (ii.) Katere naslove bi (še) lahko uporabil? Utemeljite odgovor. (iiii) Trenutno uspešno gleda film, če požene na strežniku ukaz

```
vlc --sout="#transcode{acodec=mp4a,ab=128,channels=2,
  samplerate=44100,scodec=none}:rtp
  {dst=172.18.0.2,port=5004,mux=ts}"
  --no-sout-all --sout-keep Cin\ cin\ to\ sem\ jaz
  \(Kosmatko\ Ver\ by\ Butn8\)-zy6qR1q2RvM.mkv
```

in na odjemalcu

```
vlc rtp://192.168.1.31:5004
```

(iv.) Popravite ukaza, da bo VLC uporabljal izbrane (razpošiljevalne) naslove.

C) Peter Zmeda je prišel na briljantno idejo in sicer ga je vedno motilo, da protokol RTP ne pozna seje. Zato je želel definirati protokol PRTP (Petrov RTP), ki bi omogočal vzpostavitev seje med odjemalcem in strežnikom ter njeno podiranje. (i.) Recimo, da bi vi morali implementirati ta protokol. Predlagajte obliko paketov in pomen posameznih polj v njem. (ii.) Ali je tako definiran protokol uporaben za razpošiljanje? Utemeljite odgovor.

4. naloga: Varnost tako in drugače.

VPRAŠANJA:

A) Peter in Maja se želita pogovarjati preko interneta, ampak ljubosumna Maša želi prisluškovati njunim pogovorom, zato se odločita da bosta uporabila šifriranje z javnim in zasebnim ključem. Ali morata izmenjavo ključev zaščititi pred Mašo in kako?

- da, s protokolom Diffie-Hellman;
- ne, ker poteka povezava preko SSL in je dovolj zaščitena;
- da, ključe izmenjata preko certifikatne agencije (CA);
- da, z RSA+MD5

Utemeljite odgovor.

B) Pri VPN smo omenjali pojem *tuneliranja*. (i.) Kaj je to tuneliranje in opišite primer le-tega. (ii.) Poleg tega smo omenjali možnost vpostavitve VPN v *tunelskem* in v *prenosnem* (transportnem) načinu. Opišite za vsakega od načinov po dva primera, kjer je boljši od drugega.

NAMIG: Če je en način boljši od drugega pri nečem, to pomenim, da se v drugem načinu tega ne more narediti ali pa je to zelo okorno.

C) Gregor Copatka, Peter Zmeda in Jurež Pismouk bi se radi varno pogovarjali po omrežju, v katerega je Peter Zmeda povezal butalsko planinsko kočo na Velikem hribu in tepanjsko gorsko kočo na Mali planini. Peter bi, da bo manj dela, v ta namen uporabil OpenVPN s skupno skrivnostjo. Gregor in Jurež bi raje uporabila certifikate. (i.) Čigava rešitev je boljša in zakaj? (ii.) Kako odločitev glede avtentikacije vpliva na to, ali bodo uporabili omrežno napravo tipa tap ali tun? (iii.) Če je prehod do ostalega Interneta na Velikem hribu, kje je bolje, da se postavi VPN strežnik in zakaj?