Komunikacijski protokoli in omrežna varnost
2019/20
Pisni izpit 11. svečana 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 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: Osnove delovanja omrežij.

VPRAŠANJA:

A) (i.) Narišite paket IPv4 in IPv6 ter uparite polja, ki služijo istemu namenu v obeh paketih. Zakaj oziroma kako služijo istemu namenu? (ii.) Mrežna plast nudi v osnovi eno samo storitev. Katera je ta? (iii.) Na kakšen način izvorni naslov uporabimo za to storitev? Utemeljite odgovor.

   NAMIG: Odgovor na to vprašanje je v posebni obliki usmerjanja, ki smo jo omenjali pri razpošiljanju.

B) Ali naprava z IP naslovom 192.168.2.10 lahko pošlje omrežni paket napravi z IP naslovom 1.2.3.4? Utemeljite odgovor.

   NAMIG: Če menite, da ne, zakaj ne. Če menite da da, kako da? Če menite, da včasih da in včasih ne – utemeljite obe možnosti.

C) Peter bi rad priklopil računalnik na Internet. Povezal se je na brezžično omrežje. Ukaz `ifconfig` pokaže, da je dobil naslov 192.168.1.110. (i.) S katerim ukazom lahko preveri, ali ima nastavljen privzeti prehod? (ii.) S katerim ukazom lahko preveri, ali lahko dostopa do strežnika na naslovu `www.arnes.si`? (iii.) Recimo, da uspešno dobi odgovor od strežnika 8.8.8.8, v spletnem brskalniku pa vedno dobiva sporočilo: „*Server not found - can't find the server at ...*“. Kaj mora še preveriti? Utemeljite odgovor.

2. naloga: Moje omrežje in njegovo upravljanje.

VPRAŠANJA:

A) Kateri protokol se uporablja za avtentikacijo uporabniškega imena in gesla pri vstopu v spletno učilnico UL FRI?

   - MIME,
   - LDAP,
   - TLS ali
   - DNS.

   Utemeljite odgovor tako, da narišete arhitekturo storitev okoli učilnice. Očitno je učilnica osrednja storitev in ostale le-ta uporablja.

B) Peter bi rad zagnal računalnik prek mreže, pri čemer bi se mu pokazal lep zagonski menu. Računalnik se bo iz menuja zagnal v operacijski sistem DOS. Na voljo ima namestitveni podatkovni nosilec USB (*Live USB* ključek) z Linux Mint. (i.) Katere datoteke s tega ključka mu bodo prišle prav? Odgovor utemeljite z opisom podatkov, ki so v vsaki od teh datotek. (ii.) Katere datoteke bo še potreboval za prikaz zagonskega menuja in kje jih lahko dobi?

C) Za napad na gesla, se pravi na to, da nepridiprav dobi gesla uporabnikov, se uporablja tudi *mavrične tabele*. Poleg tega potrebuje še zapis iz tabele z gesli (na FreeBSD je to datoteka `/etc/master.passwd`), ki izgleda takole (polje s tremi pikami je okrajšano):

```
peter:UZs...4sm:1002:1002::0:0:Peter Zmeda:/home/peter:/bin/bash
```

(i.) Kaj so to mavrične tabele – kaj vsebujejo in kako jih uporabimo za razbijanje gesel?

NAMIG: Opišite konkretno, kako lahko Cefizelj uporabi mavrične tabele, da dobi Petrovo geslo.

(ii.) Gesla lahko ščitimo dodatno s soljo. Kako to deluje? (iii.) Recimo, da se je Cefizelj dokopal ne samo do datoteke z gesli, ampak tudi do soli. Ali mu to pomaga pri napadu z mavričnimi tabelami? Utemeljite odgovor.

3. naloga: Čas in televizija. Peter Zmeda postavlja na noge Butale TV. Pri tem je naletel na naslednje zadrege, katere mu pomagajte rešiti.

VPRAŠANJA:

A) Na osrednjem strežniku Butale TV je nastavil trenutni čas z ukazom

```
Peter> rdate ntp1.arnes.si
```

(i.) Za kateri protokol gre pri tej poizvedbi? (ii.) Kako veliko napako lahko pričakuje? Od česa je to odvisno? (iii.) Kako bi še bolj (in na dolgi rok) povečal točnost svoje sistemske ure? (iv.) Opiši dve situaciji, v katerih je pomembno, da je sistemski čas pravilno nastavljen. Utemeljite svoj odgovor.

B) Petrova Butale TV uporablja za razpošiljanje programa IP protokol. Peter Zmeda je zaznal na omrežju REGISTER paket PIM-SM protokola. Kdo komu pošilja omenjeni paket?

- odjemalec, ki bi se želel priključiti skupini, odjemalcu, ki je že vključen v skupino;
- poljuben usmerjevalnik usmerjevlaniku, pri katerem je vir toka podatkov;
- usmerjevalnik, pri katerem je vir toka podatkov, drugemu usmerjevalniku;
- odjemalec, ki bi se želel priključiti skupini, svojemu usmerjevalniku.

Utemeljite odgovor tako, da razložite, kaj pravzaprav pomeni pošiljanje REGISTER paketa.

C) Kar nekaj časa je potrošil, da je ugotovil, da je ključno za gledalca, da si ustvari svojo sejo, v kateri spremlja program. (i.) Opišite kaj je seja in katere so njene tri faze. (ii.) Na predavanjih smo spoznali dva protokola za vzpostavitev seje. Katera? (iii.) Opišite na kratko vsakega od njiju. (iv.) Predlagajte, katerega naj uporabi Peter. Utemeljite svoj odgovor.

NAMIG: utemeljitev mora opisati, zakaj je eden primeren in drugi ne. Če ne bo vključevala obeh zornih kotov, dobite samo polovične točke.

4. naloga: Delovanje omrežja in varnost tako in drugače.

VPRAŠANJA:

A) Za neko stortev smo v datoteko `/etc/inetd.conf` dodali vnos

```
http stream tcp nowait root /usr/sbin/httpd
    in.httpd -r /etc/httpd.conf
```

(i.) Kateri program preko omrežja prejema zahteve in pošilja odgovore? (ii.) Kateri program ustvari odgovor za posamezno zahtevo? (iii.) Na katerih vratih je storitev dostopna? (iv.) V kateri datoteki so shranjene nastavitve, specifične za našo storitev? (v.) Kaj je (v splošnem) funkcija programa `inetd`? Kaj nam omogoča?

B) (i.) Opišite, kako ESP preprečuje napade s ponavljanjem. (ii.) In opišite, kako AH preprečuje napade s ponavljanjem. (iii.) Katero kriptografsko storitev nudi AH in katero ESP? Utemeljite odgovor.

C) Pri opisu požarnih pregrad smo omenjali tri stopnje operativne varnosti, ki jih nudijo požarne pregrade. (i.) Katere so? (ii.) Recimo, da bi radi varovali s požarno pregrado možnost, da nam nekdo ne pretihotapi v naše omrežje virusa z uporabo protokola TFTP. Katero vrsto požarne pregrade bi uporabili in zakaj ostale niso dovolj dobre?