Komunikacijski protokoli in omrežna varnost
2020/21
Pisni izpit 3. svečana 2021

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 105 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. Na butalskem omrežju so se dogajale čudne stvari in v iskanju izvora težav Peter Zmeda je na omrežju posnel promet na sl. 1.

```
> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
> Ethernet II, Src: ba:ba:fa:fa:de:ca (ba:ba:fa:fa:de:ca), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
v Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: ba:ba:fa:fa:de:ca (ba:ba:fa:fa:de:ca)
    Sender IP address: 10.0.11.71
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 10.0.11.1
```

Slika 1: Posneta sled prometa.

VPRAŠANJA:

A) (i.) Kateri protokoli nastopajo v sledi na sl. 1 in nakaterih plasteh so? (ii.) Kdo je pošiljatelj in komu je poslan okvir ter kaj želi pošiljatelj?

B) Peter je v podjetju računalnike nastavil tako, da se zaganjajo prek mreže. Vse podatke, potrebne za zagon, jim postreže z računalnika, na katerem so vsi za to potrebni programi. Na žalost mu je na tem računalniku začelo primanjkovati prostora. (i.) Kateri kos programske opreme predlagate, da preseli drugam, da bo osvobodil čim več prostora na disku? Utemeljite odgovor. (ii.) Če mu bo še vedno primanjkovalo diska, kateri je drugi kos programske opreme, ki bi ga preselil? Utemeljite odgovor.

   NAMIG: Zapišite, katere podatke nudi prvi in kateri drugi kos programske opreme.

C) Pri opisovanju storitev in protokola smo omenjali *entitetne pare*. (i.) Kot primer storitve vzemimo storitev TCP. Kaj nudi storitev TCP? (ii.) Kako zagotavlja ponudeno storitev entiteni par?

   NAMIG: Na začetku opišete primer, ko spodnje plasti preprečujejo nudenje storitve storitvi TCP in se mora nato član entitetnega para ustrezno odzvati.

   (iii.) Recimo, da na prenosni plasti uporabimo storitev UDP in en član entitetnega para na aplikacijski plasti zastavi drugemu članu vprašanje. Da bo slednji lahko odgovoril na vprašanje, morata tako vprašanje kot odgovor vsebovati kaj? Utemeljite odgovor.

2. naloga: Čas in slika. Peter Zmeda želi vzpostaviti na svojem omrežju videokonferenčni sistem.

VPRAŠANJA:

A) Slišal je, da je pravi način za prenos zvoka in slike med sodelujočimi uporaba razpošiljanja. (i.) V katerem primeru to bi ne bilo smiselno? Utemeljite odgovor. (ii.) V videokonferenčni sistem je vgradil še možnost uporabe anket (*poll*). Naj tudi podatke za to prenaša s pomočjo razpošiljanja? Utemeljite odgovor? (iii.) Kaj pa klepet (*chat*)? Utemeljite odgovor. (iv.) Kako je z zakrivanjem vsebine pri vsaki od točk (i.) do (iii.)? Utemeljite odgovor.

B) Poleg tega je slišal, da pri razpošiljanju obstaja osrednje vozlišče (*rendezvous point*). (i.) Kakšna je njegova vloga?

   (a) Strežnik, kjer dobimo informacije o skupinah razpošiljanja.
   (b) Usmerjevalnik, ki je del dveh podomrežij in posreduje multicast promet.
   (c) Usmerjevalnik, ki ima vlogo korenskega vozlišča v drevesu razpošiljanja.
   (d) Vozlišče, ki je del večih skupin razpošiljanja.

   (ii.) Opišite primer uporabe osrednjega vozlišča.

C) Peter je postavil svoj strežnik DHCP. Uporabil je paket isc-dhcp-server distribucije Debian GNU/Linux. V /etc/dhcp/dhcpd.conf je dodal:

```
host pxelinux.0
    hardware ethernet ba:dc:0d:e5:d0:0d;
    filename "peter.si";
```

   (i.) Kakšno je tu ime računalnika? Utemeljite odgovor. (ii.) Kateri zagonski nalagalnik uporablja? Utemeljite odgovor. (iii.) Poleg strežnika DHCP, kaj še potrebuje, da se bo zagonski nalagalnik naložil? Podajte primer konkretnega programa (paketa), ki to nudi.

3. naloga: Moje omrežje in njegovo upravljanje. Upravljanje z omrežjem vključuje upravljanje s strojno in programsko opremo ter tudi z uporabniki.

VPRAŠANJA:

A) Za upravljanje z IP naslovi v omrežju je Peter postavil DHCP strežnik. Določil je območje, s katerega naj dodeljuje naslove. Ko je priklopil nekaj deset računalnikov, so se začele težave - nekateri računalniki niso več dobili naslova. Peter sumi, da je na strežniku zmanjkalo naslovov, zato bo dodal še en DHCP strežnik. Odgovore na naslednja vprašanja utemeljite. (i.) Je njegov

pristop pravilen? (ii.) Kako mora skonfigurirati novi strežink? (iii.) Kako bi še lahko rešil svojo težavo?

B) Pri beleženju dogodkov v omrežju je sporočilo v protokol `syslog` vsebovalo zapis:

```
Jan 31 09:21:19 kajtimar dhcpd[61626]:
  uid lease 192.168.126.164 for client ac:cc:8e:bb:17:bd
  is duplicate on internaMreza
```

(i.) Kateri program je zahteval zabeležko?

(a) `dhcpd`
(b) `kajtimar`
(c) `uid`
(d) `lease`

(ii.) Kaj sporoča zapis? Opišite do česa je prišlo.

C) Pri upravljanju z omrežji smo omenjali upravljanje: z napakami, s konfiguracijami, z varnostjo in z beleženjem dostopa. Med tremi dejavniki, s katerimi upravljamo, so tudi uporabniki. (i.) Za vsako od štirih omenjenih upravljanj opišite primer upravljanja z uporabniki. (ii.) Za vsakega od napisanih primerov upravljanj navedite programsko opremo ali protokol, ki omogoča zapisano upravljanje.

NAMIG: Pri opisovanju primera upravljanja bodite konkretni – opišite konkretno situacijo in kako v njej upravljamo z uporabniki.

4. naloga: Varnost tako in drugače.

VPRAŠANJA:

A) Recimo, da pri avtorizaciji uporabljamo podatkovno bazo LDAP. 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?

(a) Takšne poizvedbe so mogoče; za veriženje pogojev uporabljamo infiksno notacijo.
(b) LDAP je preprost protokol in takšnih zapletenih poizvedb ne podpira. Podatke je potrebno filtrirati ročno.
(c) Takšne poizvedbe so mogoče; za veriženje pogojev uporabljamo prefiksno notacijo.

(d) Takšne poizvedbe so mogoče; za veriženje pogojev uporabljamo reverzno poljsko notacijo.

B) Za zavarovanje prometa po internetu lahko uporabimo protokol TLS/SSL. Pri njem poznamo tri faze delovanja: vzpostavitev, prenos podatkov in podiranje seje. (i.) Kateri podatki v paketu IP (vse plasti) določajo eno sejo?

NAMIG: To vprašanje bi lahko bilo v nalogi o osnovah, saj je seja definirana izven samega TLS protokola.

(ii.) Opišite, kako je pri protokolu TLS zagotovljena celovitost prenašanih podatkov? (iii.) Kakšen napad bi lahko uprizoril Cefizelj, če protokol TLS ne bi vključeval posebnega paketa za podiranje seje? Opišite primer.

C) Peter Zmeda bi se rad priklopil na VPN svojega podjetja. V podjetju uporabljajo OpenVPN. S pomočjo Easy-RSA je ustvaril datoteki peter.csr in peter.key ter obe poslal administratorki.

(i.) Katere datoteke, ustvarjene na osnovi poslanih, pričakuje nazaj? (ii.) Katere dodatne datoteke bo potreboval, da se lahko poveže na VPN? (iii.) Je vse naredil pravilno? Je morda kaj pozabil? Utemeljite odgovor.