Komunikacijski protokoli irn omrežna varnost
2020/21
Prvi kolokvij

Kolokvij morate pisati posamič. Pri reševanju je literatura dovoljena. Odgovorite pazljivo na *vsa* vprašanja.

Če boste uspešno vsaj delno vse naloge, bo možno dobiti dodatne točke.

Čas pisanja kolokvija je 75 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 ter bootp in DHCP.

VPRAŠANJA:

A) Za katero vrsto aplikacijskih protokolov je na transportni plasti bolj primeren UDP protokol (predpostavimo, da želene lastnosti lahko nudi zgolj transportna plast in jih aplikacijski protokoli ne implementirajo sami)? Utemeljite odgovor.
   (a) Promet, kjer ne zahtevamo, da paketi prispejo v pravilnem vrstnem redu, zahtevamo pa, da zanesljivo prispejo.
   (b) Promet, kjer zahtevamo, da paketi prispejo v pravilnem vrstnem redu, ne zahtevamo pa, da paketi zanesljivo prispejo.
   (c) Promet, kjer ne zahtevamo vrstnega reda niti zanesljivega prispetja, zahtevamo pa hitro vzpostavitev komunikacije.
   (d) Za nobeno.

B) Peter ima doma omrežje, na katerem za dostop do Interneta skrbi usmerjevalnik z OpenWRT. (i.) Ali ima lahko na lokalni mreži DHCP strežnik, ki ni na istem računalniku kot privzeti prehod (*default gateway*)? Utemeljite odgovor. (ii.) Kako odjemalci izvedo, kam morajo pošiljati pakete, če privzeti prehod ne dodeljuje naslovov?

C) Ana in Borut vodita podjetji, med katerima se pogosto dogajajo transakcije. Vedno ena stran izvede transakcijo, o čemer obvesti drugo stran. Transakcija ni veljavna, dokler prva stran ne dobi potrditve z druge strani. Opis transakcije je dovolj majhen, da ga lahko prenesemo z enim samim IP paketom. Peter je dobil nalogo, naj začrta protokol, ki ga bosta Ana in Borut lahko uporabljala. Prvi korak je bil, da se je na prenosni plasti odločil za UDP protokol, ker se transakcije dogajajo res hitro. (i.) Katera polja naj vsebuje Petrov protokol (kako naj izgleda datagram), da bo zadoščal Aninim in Borutovim zahtevam? Kakšna je vloga polj, ki ste jih definirali. (ii.) Kako naj Peter nadgradi protokol, da bo zagotavljal celovitost (integriteto)? Utemeljite odgovor.

2. naloga: Upravljanje omrežij.

VPRAŠANJA:

A) Kako SNMPv3 preprečuje napade s ponovitvijo (*replay attack*)?

B) (i.) Kaj je to MIB in čemu služi? (ii.) Zakaj je obstoj MIB dober za gospodarstvo/industrijo? Utemeljite odgovor. (iii.) Recimo, da je Peter namestil na strežnik novo storitev, ki bere vrednost termometra. Kaj mora narediti Peter, da bo lahko upravljal s termometrom tako kot na primer z usmerjevalnikom? Utemeljite odgovor.

C) Peter je na svojem računalniku, ki ima naslov 192.168.1.10, pognal:

```
peter@marogla: $
snmpwalk -c public -v1 localhost
iso.3.6.1.2.1.1.9.1.3.1 = STRING:
  "The SNMP Management Architecture MIB."
peter@marogla: $
snmpwalk -c vaglvuglbambam -v1 192.168.1.10
  iso.3.6.1.2.1.1.9.1.3.1
Timeout: No Response from 192.168.1.10.
```

(i) Zakaj ukaz snmpwalk prvič deluje in drugič ne? Opišite vsaj dva možna razloga. (ii) Peter je pričakoval, da bo izpis daljši. Kaj običajno izpiše snmpwalk? V kateri datoteki pod GNU/Debian to nastavimo? Ali moramo datoteko popraviti na strežniku ali tam, kjer snmpwalk poženemo? (iii) Peter meni, da je s tem, da je namesto *public* uporabil res skriven niz, svoje omrežje dobro zavaroval. Je to res? Odgovor utemeljite.

3. naloga: Stvarni čas.

VPRAŠANJA:

A) Kateri protokol uporablja NTP za prenos? Zakaj ta protokol?

B) Pri obliki paketov za promet v stvarnem času smo omenjali, da vsak paket vsebuje vsaj zaporedno številko in časovno značko. (i.) Vendar, če bi na prenosni plasti namesto UDP protokola uporabljali protokol TCP, bi lahko enega od dveh podatkov izpustili. Katerega in zakaj? (ii.) Če človek takole premišlja, že časovne značke določajo zaporedje paketov. Zakaj je potrebna poleg časovne značke še zaporedna številka paketa? (iii.) Protkolu SRTP omogoča zakrivanje podatkov. V resnici bi lahko zakrili poleg podatkov tudi večino polj v glavi razen enega. Katerega in zakaj?

C) Peter je na svojem računalniku v EFI nastavil uro. Pod Microsoft Windows mu je delovala pravilno, ko pa je zagnal GNU/Linux, je ura za eno uro zaostajala. (i) Zakaj bi lahko prišlo do zgoraj opisane težave? (ii) Če je uro nastavil v EFI, ali jo lahko pravilno nastavi s pomočjo NTP? Ali bo ura ostala nastavljena po ponovnem zagonu? Odgovor utemeljite. (iii) Kaj je bolje - da sta čas v EFI in čas, ki ga prikažete uporabniku, enaka ali različna? Kdaj bi lahko prišlo do problemov, če sta, in kdaj, če nista? Kateri problemi so hujši?

NAMIG: Konec oktobra ste se vsaj en dan naspali bolje kot sicer. En dan konec marca ste se naspali slabše.

4. naloga: Razpošiljanje.

VPRAŠANJA:

A) Ali je `11110000...01` lahko binarna predstavitev IPv6 razpošiljevalnega naslova? Utemeljite odgovor!

B) Osnovni protokol za pridruževanje in zapuščanje razpošiljevalni skupini je IGMP. (i.) Kateri prenosni (*transport*) protokol uporablja? (ii.) Zapišite vrednosti polj v paketu IGMP ter naslova prejemnika in pošiljatelja v IP delu paketa, če naprava na IP naslovu 1.2.3.4 želi zapustiti skupino 224.223.222.221? (iii.) Utemeljite vaš odgovor.

C) NEOBVEZNO IN NI ZA OCENO. Letos proslavljamo 250 letnico rojstva neverjetnega skladatelja. Med drugim se je navduševal nad revolucionarnim voditeljem Napoleonom in mu je posvetil eno od svojih skladb, vendar je posvetilo kasneje preklical. (i.) Kako se je izvorno imenovala skladba iz let 1803.-1804? (ii.) V kaj jo je kasneje preimenoval, ko se je Napoleon okronal za cesarja? (iii.) Kdo je bil ta skladatelj?

D) Peter nastavlja svoj DHCP strežnik. Ker bi rad ugotovil, kako se le-ta pogovarja z računalnikom, se je odločil, da zajame nekaj prometa. Pognal je spodnji ukaz.

```
sudo /usr/sbin/tcpdump -i wlp4s0 port 67 or port 68
14:15:06.771635 IP 0.0.0.0.bootpc >
  255.255.255.255.bootps: BOOTP/DHCP,
  Request from 90:32:4b:35:2f:09 (oui Unknown),
  length 292
```

(i.) Kaj je v tem primeru 255.255.255.255 - izvorni ali ponorni naslov? Utemeljite odgovor. (ii.) Ali lahko pri prometu, ki ga razpošiljamo, sploh govorimo o vratih (angl. *port*), če se vrata uporabljajo pri TCP. TCP pa, kot vemo, ne podpira razpošiljanja? Utemeljite odgovor. (iii.) Če bi Peter rad nastavil, da njegov računalnik vedno dobi isti naslov, na osnovi katerega podatka oz. podatkov, ki jih računalnik pošlje strežniku, lahko to stori? Utemeljite odgovor.