Komunikacijski protokoli in omrežna varnost
2018/19
Pisni izpit 6. svečana 2019

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.

VPRAŠANJA:

A) Peter je priklopil svoj računalnik na omrežje, vendar ne more do Interneta – spletni brskalnik javi, da ne najde strežnika www.google.com. Z `ifconfig` je preveril, da ima naslov 192.168.1.1. V `/etc/resolv.conf` ima naslov strežnika DNS. (i.) Kaj naj še preveri, da bo prepričan, da so nastavitve na njegovem računalniku pravilne? Utemeljite odgovor. (ii.) Ko bo prepričan, da je računalnik nastavljen pravilno, kako naj naprej išče izvor napake?

B) Kdaj se računalnik z BIOS lahko zažene preko omrežja? Utemeljite odgovor.

C) `tftp` uporablja `udp` protokol., ki ne pozna seje in ne zagotavlja prenosa podatkov. (i.) Kako `tftp` na aplikacijski plasti uporabi polja glave `tftp` paketa, da prenese celotno datoteko? (ii.) Peter Zmeda že ima strežnik `tftp` in bi ga rad uporabil za prenos poljubno velikih datotek. Kako naj to naredi?

2. naloga: Čas, televizija in razpošiljanje.

VPRAŠANJA:

A) Najprej poglejmo, kako program, ki po RTP sprejema glasbo in jo predvaja na zvočni kartici, ve, v kakšnem formatu je glasba zapisana? Razložite odgovor.

B) Med predvajanjem videa pesmi prek mreže smo zajeli (okrajšan) paket:

```
HTTP/1.0 200 OK
  Content-type: video/webm
  Content-Length: 7456250
  Last-Modified: Mon, 04 Feb 2019 18:09:57 GMT
  .E.....B..webm..B...C*..B@{..Lithium Flower..
  .Lavf58....V_VP9...#.."..eng..A_OPUS...c
  ..V.. c..OpusHead..8..g..E..ARTISTD..Raj Ramayya..
  .ENCODERD..Lavf58.."E..DURATIOND..00:03:18.706000000.
```

(i.) Kako dolga je pesem? Kdo je izvajalec in kakšen je naslov pesmi? (ii.) V katerem formatu je vsebina? Zapišite vsebujoči (*container*) format in kodeka za video ter avdio del posnetka. (iii.) Kateri protokol (na najvišji plasti) se uporablja za prenos podatkov? Zapišite po eno prednost in slabost uporabe tega protokola za prenos videa in utemeljite svoj odgovor.

C) Ker bomo naš program razpošiljali večim poslušalcem, si poglejmo protokol PIM, ki lahko deluje v gostem ali v redkem načinu ela. (i.) Ali sta razpošiljevalni drevesi, ki ju zgradi v enem in drugem načinu dela enaki?

Utemeljite odgovor, pri čemer se osredotočite na vprašanje *zakaj* naj bi bili ali naj bi ne bili enaki. (ii.) Na predavanjih smo srečali algoritem RPL (poizvedba o obratni poti, *reverse path lookup*). Ali ga uporablja protokol PIM? Utemeljite odgovor. (iii.) Ali sploh lahko razpošiljamo (*multicast*) video, ki ga predvajamo uporabljajoč `http` protokol? Utemeljite odgovor.

3. naloga: Upravljanje sistemov.

VPRAŠANJA:

A) 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. Ali poizvedbeni jezik, s katerim dobivamo podatke iz baze LDAP, kaj takega sploh podpira? Utemeljite odgovor.

B) Peter uporablja LDAP. V bazo je vnesel tudi podatke o sebi:

```
dn: cn=si,ou=users,dc=butale,dc=si
objectClass: inetOrgPerson
objectClass: person
cn: si
sn: Zmeda
givenName: Peter
```

(i.) Razložite, kaj pomenijo `dn`, `cn`, `ou` in `dc` v prvi vrstici. (ii.) Ker se je poročil s prelepo Rozamundo, bi sedaj rad imel dva priimka - Zmeda in Turjaški. Kako naj popravi svoj vnos v bazi?

C) Protokol SNMP uporablja za prenos sporočil prenosni protokol `udp`. (i.) Kako je poskrbljeno v protokolu, da spraševalec ve, da je dobil odgovor na svoje vprašanje? Utemeljite odgovor z opisom komunikacije. (ii.) Za prenos podatkov uporablja TLV zapis. Opišite ga. (iii.) Kaj je vsebina naslednjega TLV zapisa (desna vrednost je prvi bajt in zapisi so šestnajstiški):

```
00x E3x 07x 02x 02x 02x 01x 02x 06x 01x 02x
```

4. naloga: Varnost. Peter Zmeda je v sistemskem dnevniku našel naslednje vrstice:

```
Dec 31 06:29:28 colin sshd[25212]: Invalid user xc from 106.12.37.232
port 58944
Dec 31 06:29:28 colin sshd[25212]: input_userauth_request: invalid
user xc [preauth]
```

```
Dec 31 06:29:28 colin sshd[25212]: pam_unix(sshd:auth): check
pass; user unknown
Dec 31 06:29:28 colin sshd[25212]: pam_unix(sshd:auth): authentication
failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=106.12.37.232
Dec 31 06:29:30 colin sshd[25212]: Failed password for invalid
user xc from 106.12.37.232 port 58944 ssh2
```

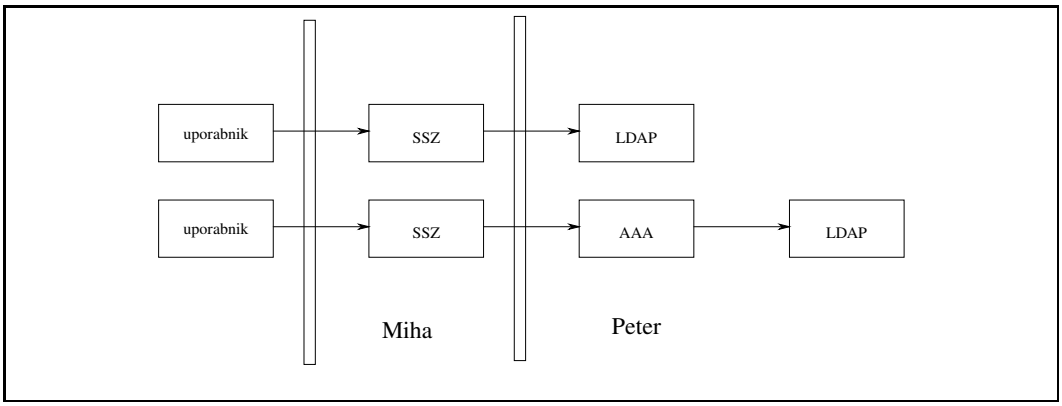
Nekaj se očitno dogaja z uporabniki na njegovem sistemu.

VPRAŠANJA:

A) Naprej se je lotil podrobnejšega razumevanja zapisa. Pomagajte mu. (i.) Kateri program je zabeležil te vrstice? (ii.) Za kakšno napako gre in kaj je neposredni vzrok te napake? (iii.) Zakaj je dobro pri avtentikaciji kljub napačnemu uporabniškemu imenu še zmeraj zahtevati geslo?

B) Naslednji korak je bila vzpostavitev VPN med njegovim sistemom in Špelinim sistemom. Med RFC-ji, ki jih je prebral je tudi tisti, ki govori o IKE. Omenjeni RFC omenja dve fazi. Čemu je namenjena druga faza? Odgovor utemeljite vključno s tem, zakaj bi potreboval funkcionalnost, ki jo ponuja druga faza.

C) Tako, sistem ima postavljen in v njem tudi storitev `ldap`. Mihatu se to zdi enkratno in bi ponujeno storitev rad uporabil za avtentikacijo v svoji storivi snemanja glasbenih zgoščenk SSZ. Peter ni čisto prepričan, ali naj dovoli Mihovi storitvi dostop do `ldap` ali ne. Odloča se med dvema možnima arhitekturama na sl. 1. (i.) Katera se vam zdi varnejša iz zornega kota kdo pozna



Slika 1: Možni topologiji za storitev SSZ.

skupno skrivnost za avtentikacijo. Odgovor utemeljite. (ii.) Kaj pomeni za Mihatovo implementacijo SSZ, če Peter namesto AAA ponudi storitev CHAP? Utemeljite odgovor.