Komunikacijski protokoli in omrežna varnost
2019/20
Pisni izpit 25. velikega srpana 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: Zagon in priklop naprave.

VPRAŠANJA:

A) Protokola BOOTP in DHCP sta dejansko pri IPv4 enak protokol, pri čemer je drugi razširitev prvega. (i.) Navedite (ali narišite) katera polja so v paketu protokola BOOTP. (ii.) Recimo, da odjemalec pošilja poizvedbo po operacijskem sistemu, ki bi ga želel naložiti. Za tri od polj, ki ste jih navedli zgoraj, navedite vrednosti, ki so v paketu poslanem s strani odjemalca. Utemeljite, zakaj so takšne vrednosti v poljih, kot ste jih navedli. (iii.) Pri IPv6 imamo prav tako inačico protkola DHCP, ki pa je povsem različna od protokola za IPv4. Zakaj, menite, so se odločili za nov protokol? Utemeljite svoj odgovor.

B) (i.) Kateri od spodnjih odgovorov najbolje popisuje iz česa sestoji BIOS kot celota ?

   1. Iz programske opreme, ki pomaga pri ugašanju računalnika.
   2. Iz strojne opreme, ki pomaga pri zagonu računalnika.
   3. Iz strojne opreme (obstojni pomnilnik) in na njej naložene programske opreme, ki pomaga pri zagonu računalnika.
   4. Iz programske opreme, ki pomaga pri zagonu računalnika.

   (ii.) Utemeljite odgovor.

C) Peter je postavil svoj DHCP strežnik. (i.) Ali lahko dodeljuje naslove na omrežju, na katerem server nima IPja? (ii.) Če ne, zakaj ne? Če da, kako?

2. naloga: Moje omrežje in njegovo upravljanje.

VPRAŠANJA:

A) Peter je podjeten mož in je v Butalah nagradil omrežje tako, da si lahko naročniki ogledajo posnetke sestankov Butalskega sveta. Seveda, posnetek sestanka posreduje tokovni strežnik uporabljajoč RTP protokol. Gledanje enega sestanka predstavlja eno sejo (*session*), ki ima svoj začetek in konec. (i.) Ali protokol RTP pozna pojem seje? (ii.) Če ga, opišite, kako deluje in če ne, kako lahko Peter potem ustvari posamezne seje? (iii.) Kako je z zakrivanjem prometa? Kako ga lahko izvede? Opišite zakrivanje prometa in kako ustvariti sejo z zakritim prometom.

B) Eden od možnih prenosnih protokolov za avtentikacijo je tudi PPP protokol. Recimo, da prejmemo PPP paket, ki prenaša podatke za avtentikacijo. (i.) Kakšna je vrednost prvih dveh zlogov?

   1. c1h 23h

2. c0h 23h
3. 00h 01h
4. c2h 23h

(ii.) Utemeljite odgovor.

C) Peter bi rad upravljal podatke o svojih uporabnikih preko storitve LDAP, zato je popravil `/etc/nsswitch.conf` takole:

```
passwd:         ldap, compat
group:          ldap, compat
shadow:         ldap, compat
```

V sistem se z uporabniškim imenom `peter`, ki ga ima na sistemu, sicer sedaj lahko prijavi, le gesla, ki je v LDAP, sistem ne sprejme. (i.) Zakaj? (ii.) Kaj bi moral še spremeniti oziroma nastaviti, da bi geslo v LDAP delovalo? Poleg tega mu sistem ne dovoli več pisati po `/home/peter`. Če pa spremeni `/etc/nsswitch.conf` na staro različico, lahko po domačem imeniku spet piše. (iii.) Zakaj bi lahko do tega prišlo?

3. naloga: Razpošiljanje. Pri razpošiljanju paketov omenjamo protokole kot je na primer PIM.

NAMIG: Razmislite kakšna je povezava med protokolom PIM in neposrednim usmerjevalnikovim razpošiljanjem paketov sosedom (usmerjanje razpošiljanih paketov).

VPRAŠANJA:

A) (i.) Kako točno je protokol PIM udeležen pri samem razpošiljanju paketov? Utemeljite odgovor. (ii.) Eden od osnovnih načinov razpošiljanja je oddajanje paketa vsem sosedom – *broadcasting*. Pri tem se uporablja postopek vpogleda za povratno pot (*reverse path lookup*). Kam pogleda usmerjevalnik ob prišlem paketu, da se lahko odloči, ali naj paket obravnava ali ne? Na podlagi česa se odloči, da naj paket obravnava? (iii.) V tem primeru lahko poplavimo celoten Internet, vendar ima IP paket zaščito pred tem. Kakšno in kako deluje?

B) Na istem podomrežju imamo napravi A in B. A je prijavljena na razpošiljevalnem naslovu 111011010X, B pa na naslovu 111011011X, kjer je X neko zaporedje 23 bitov. (i.) Kaj to pomeni za dostavo paketov na drugi (povezavni) plasti? (ii.) Utemeljite odgovor.

C) Peter Zmeda hoče na več informacijskih panojih, razpostavljenih po Butalah, predvajati isti film. Na strežniku je pognal:

```
cvlc spincamarogla_skace.mp4
  --sout '#rtp{dst=172.31.44.6,port=5004,mux=ts}'
```

Potem je na dveh panojih pognal:

```
vlc -vvv --network-caching 200 rtp://172.31.44.6:5004/
```

in slika se je prikazala samo na enem. Ko je naslov 172.31.44.6 zamenjal z naslovom 225.112.213.23, se je slika prikazala na obeh panojih. (i) Zakaj z enim naslovom rešitev deluje, z drugim pa ne? Zakaj je na začetku en pano deloval? (ii) Ali je naslov 225.112.213.23 izbran pravilno? V katerem primeru da, v katerem ne in kako bi to preverili? (iii) S katerimi naslovi bi zgornja rešitev še delovala? Navedite področje/a.

4. naloga: Varnost na različnih plasteh.

VPRAŠANJA:

A) Kako lahko odjemalec ob priklopu v omrežje sploh izvede postopek 802.1X avtentikacije, če mu še ni dovoljen dostop do omrežja?

B) Pri protokolu HTTPS, ki je varna inačica protokola HTTP, imamo odjemalca in strežnik. (i.) Kaj zagotavlja uporaba certifikata pri vzpostavitvi povezave iz zornega kota odjemalca? (ii.) Kaj zagotavlja uporaba certifikata pri vzpostavitvi povezave iz zornega kota strežnika? (iii.) Kateri del certifikata je še posebej uporaben pri vzpostavitvi šifrirane seje in zakaj?

C) 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
```

(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?