Komunikacijski protokoli in omrežna varnost
2017/18
Pisni izpit 4. kimavca 2018

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. V podjetju *Naša Sol*, d.d. so zaposlili novega sistemskega administratorja Mihcastega Kimpeža. Kot prvo nalogo si je zastavil poenostaviti nadgrajevanje operacijskih sistemov vseh računalnikov v podjetju tako, da se jim bo nalagal operacijski sistem preko omrežja. Podjetje *Naša Sol* ima tri podružnice, katere vsaka je zaščitena s požarno pregrado. Za dostop do Interneta je nato uporabljen NAT prehod. V vsaki podružnici je Kimpež postavil svoj bootp strežnik in poleg tega na Internetu postavil na naslovu `1.2.3.4` še tftp strežnik.

VPRAŠANJA:

A) Ali se računalnik z BIOS sploh lahko zažene preko omrežja? Če da, kje se nahaja program, ki prevzame program s strežnika? Če ne, zakaj ne?

B) Peter ima selektivno slab spomin – nikakor si ne more zapomniti MAC naslova omrežnega vmesnika v svojem računalniku. Vseeno bi rad poskrbel, da bi njegov računalnik ob priklopu na omrežje vedno dobil isti naslov. Kako lahko to stori? Kako lahko poskrbi, da bo njegov računalnik dobil isti naslov tudi, če zamenja omrežni vmesnik? Ročno nastavljanje IP na računalniku ne pride v poštev.

C) Ko je naš prijatelj Peter Zmeda preučil Kimpeževo arhitekturo, je bil prepričan, da ne more delovati, saj bi moral biti tftp strežnik prav tako na lokalni mreži kot bootp strežnik. (i) Ali ima Peter prav? Utemeljite svoj odgovor. (ii) Ne glede na prejšnji odgovor, kaj pa bootp strežnik? Bi lahko imel Kimpež enega samega za vse podružnice? Utemeljite odgovor. (ii) In, spet ne glede na prejšnje odgovore, kako bi lahko Cefizelj izvedel napad na podjetje ter ukradel neprecenljivi recept za proizvodnjo soli?

2. naloga: Čas, televizija in razpošiljanje.

VPRAŠANJA:

A) Peter Zmeda postavlja Butalsko Televizijo. Za razpečevanje videogradiva bi rad uporabljal razpošiljanje. V ta namen namerava uporabiti naslove 172.18.0.1 do 172.19.255.254. Strežnik je na naslovu 192.168.1.31. (i) So ti naslovi primerni? (ii) Katere naslove bi (še) lahko uporabil? (iii) Trenutno uspešno gleda film, če požene na strežniku:

```
vlc --sout="#transcode{acodec=mp4a,ab=128,channels=2,\
  samplerate=44100,scodec=none}\
  :rtp{dst=172.18.0.2,port=5004,mux=ts}"\
  --no-sout-all \
  --sout-keep zveriniceizrezije.mkv
```

in na odjemalcu:

```
vlc rtp://0.0.0.0:5004
```

Popravite ukaza, da bo VLC uporabljal izbrane (razpošiljevalne) naslove.

B) Za prenos programa uporablja Peter protokol RTP. (i) Na kateri plasti je ta protokol in zakaj? (ii) Eno od polj v glavi protokola je časovna značka (*time stamp*). Ali je možno, da imata dva paketa isto časovno značko? Utemeljite odgovor. (iii) Kako je možno, da sprejemnik dobi paket z zgodnejšo časovno značko kasneje kot s kasnejšo? Kaj naj naredi v takšnem primeru?

NAMIG: Pri vprašanju (iii) običajno ni samo ena možnost.

C) Nova Petrova ideja. Televizijski program deluje kot bi moral in sedaj želi vzpostaviti novo storitev, s pomočjo katere bi uporabniki prenesli s strežnika posamezne datoteke. Da bi optimiral izrabo omrežnih kapacitet, si je zamislil, da bo vsem, ki hkrati zahtevajo določeno datoteko, le-to poslal s pomočjo razpošiljanja (*multicasting*). Ali bo to delovalo? Če ne, zakaj? Če da, s kakšnim protokolom?

3. naloga: Upravljanje omrežij.

VPRAŠANJA:

A) Peter Zmeda je slišal, da lahko preveri, koliko prostora ima na disku, če izvede:

```
snmpget -v1 -c studentje localhost .1.3.6.1.4.1.2021.9.1.9.1.
```

Sedaj ga zanima, katere ostale podatke o disku lahko dobi. (i) S katerim ukazom si lahko pomaga? Napišite celoten ukaz z vsemi argumenti. (ii) Kaj je v zgornjem ukazu `studentje`? (iii) Ali so ukazi, ki jih uporablja, varni? Utemeljite odgovor.

B) Pravice za upravljanje z omrežji so odvisne od uspešne avtentikacije posameznika. Eden od protokolov za avtentikacijo je CHAP. Le-ta sloni na skupni skrivnosti, vendar po drugi strani pravimo, da pri strežniku naj bi ne hranili gesla. (i) Kako potem skupaj sestavimo vse skupaj – kaj hranimo?

(ii) Petra strašansko jezi, če se mu nehote vključijo zaklenjene velike črke (*caps lock*) in potem narobe vtipka geslo. Še huje je, če se mu preklopi tipkovnica in namesto `qwertz` postane `qwerty`. Ker tega ne opazi tudi več kot petkrat poskusi vtipkati napačno geslo, za katerega sicer misli, da je pravilno. Za nameček po petih napačnih poskusih ne more poskusiti naslednjih

10 minut. Tako je prišel na idejo, da bi sistem ob vpisanem geslu poskusil biti pameten in bi poskusil vse kombinacije malih in velikih črk, ko preverja geslo uporabnika. Komentirajte Petrovo idejo.

C) Peter je na računalnikih v službi poskrbel za avtentikacijo na računalnikih z uporabo protokola RADIUS. Njegov paranoični sodelavec sedaj vsako jutro vdira v lastni računalnik, saj je prepričan, da mu zaradi Petrove rešitve nekdo lahko ukrade geslo. Je njegov strah utemeljen? Utemeljite odgovor.

4. naloga: Infrastruktura v podjetju *Naša sol* in posebej njeni varnostni vidiki.

VPRAŠANJA:

A) Pri varnosti smo omenjali več vidikov in dva med njimi sta *integriteta podatkov* in *zaupnost podatkov*. (i) Kaj pravzaprav pomenita oba izraza? (ii) Kako lahko vsakega od njiju zagotovimo pri protokolu IPsec? (iii) Kako vsakega od njiju zagotovimo pri protokolu IEEE 802.1x?

NAMIG: Pri obeh protokolih opišite način zagotavljanje samo enega vidika od omenjenih. Pri obeh protokolih je vidika morda potrebno zagotavljati s storitvami, ki ju protokola prenašata/uporabljata.

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
gn: 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) Kako ESP preprečuje napade s ponavljanjem? Utemeljite odgovor!

NAMIG: Lahko opišete strukturo paketa.