Komunikacijski protokoli in omrežna varnost
2015/16
Drugi kolokvij

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

Če boste uspešno vsaj delno odgovorili na vsa vprašanja, bo možno dobiti dodatne točke.

Čas pisanja izpita je 60 minut.

Veliko uspeha!

NALOGA	TOČK	OD TOČK	NALOGA	TOČK	OD TOČK
1			3		
2			4		

IME IN PRIIMEK: _____

ŠTUDENTSKA ŠTEVILKA: _____

DATUM: _____

PODPIS: _____

1. naloga: Varnostni elementi.

VPRAŠANJA:

A) Na govorilni uri je nekdo postavil vprašanje, ali se pri IPsec v paketu vidi izvorna in ponorna vrata? Kaj menite, se vidijo? Utemeljite odgovor.

B) Peter bi rad s svojim prijateljem Konradom igral prastaro igrico – *Warcraft II*. Igrica za igranje preko omrežja uporablja protokol IPX. Peter in Konrad živita na različnih koncih mesta in uporabljata takšnole konfiguracijo za *OpenVPN*:

Peter	Konrad
`proto tcp`	`proto tcp`
`remote vpn.prijateljkonrad.net`	`dev tun`
`dev tun`	`secret skrivnost.txt`
`secret skrivnost.txt`	

(i) Kdo bo za igrico postavil strežnik – Peter ali Konrad? Utemeljite odgovor.
(ii) Veselo sta odigrala nekaj partij *openra* (*Open Red Alert*) prek svojega navideznega omrežja. *Warcraft II* vseeno ne deluje. Kaj menite, da je razlog? Kako naj težavo odpravita?

C) Peter Zmeda se je odločil zasoliti shranjena in zgoščena gesla, da bi ne bila ranljiva na mavrični napad. Žal je vrednost soli izgubil. Je to pomembno? Utemeljite odgovor.

2. naloga: AAA in RADIUS.

VPRAŠANJA:

A) Eden od protokolov za avtentikacijo se imenuje CHAP. (i) Opišite, kako deluje. (ii) Posebna lastnost protokola CHAP je, da preprečuje napad s ponavljanjem. Kako?

B) Zgoraj smo zapisali, da je CHAP protokol za avtenkacijo. (i) Ali omogoča vzajemno avtentikacijo? (ii) Če da, kako; in če ne, kako bi ga nadgradili, da bi jo omogočal?

NAMIG: Če menite, da CHAP ne omogoča vzajemne avtentikacije, lahko definirate svojo novo inačico CHAP protokola.

C) Peter Zmeda je našel v sistemski zabeležki naslednjo vrstico:

```
Jan 18 06:30:45 svarun saslauthd[52023]:
  do_auth: auth failure: [user=pzmeda] [service=smtp]
  [realm=] [mech=pam] [reason=PAM auth error]
```

(i) Kateri program je zahteval zabeležko? (ii) Kaj pravzaprav pravi zabeležka in ali bi Peter moral biti zaskrbljen? Utemeljite odgovor.

3. naloga: Podatki za delovanje omrežja.

VPRAŠANJA:

A) Osnovni protokol za nudenje podatkov za delovanje, ki smo ga spoznali, je LDAP. Opišite *tri bistveno različne načine* kako lahko promet protokola LDAP zakrijemo. Za vsakega od njih opišite, kdaj bi ga izbrali namesto drugih dveh. Utemeljite odgovor.

   NAMIG: Vaš odgovor mora za vsakega od načinov vsebovati *situacijo* (in *utemeljitev*), ko je ta način primerjnejši od drugih dveh.

B) Peter Zmeda za shranjevanje uporabnikov uporablja LDAP. Njegova domena je `butale.si`. Vsi njegovi uporabniki so del organizacije `trg`. Sedaj je po sili razmer prisiljen ustvariti uporabnika `cefizelj`, ki bo v organizacijski enoti `lopovi`. Kakšno bo razpoznavno ime (*distinguished name*) objekta v imeniku LDAP, ki opisuje Cefizlja? Utemeljite odgovor.

C) Pri SSL/TLS rokovanju odjemalec pošlje strežniku seznam podprtih šifrirnih algoritmov. Kako lahko SSL/TLS prepreči izbris močnejših algoritmov s seznama podprtih? Utemeljite odgovor.

4. naloga: IEEE 802.

VPRAŠANJA:

1. (i) Na kateri plasti govori odjemalec s ponudnikom priklopa na lokalno mrežo? (ii) Peter je slišal da protokol IEEE 802.1x uporablja RADIUS. Glede na odgovor na prvi del vprašanja, ali bo Petru uspelo spraviti RADIUS promet do odjemalca, ki bi se rad priključil na lokalno mrežo z uporabo protokola IEEE 802.1x? Utemeljite odgovor.

2. Peter je postavil strežnik *Freeradius*. Sedaj bi ga rad uporabil za avtentikacijo na več dostopnih točkah. (i) Ali lahko na vseh uporabi isto skrivnost?

   Recimo, da imam Peter nastavitveno datoteko z naslednjo vsebino:

```
client dostopna
    secret = secret
    shortname = localhost
    nastype = other
    ipaddr = 192.168.1.1
    require_message_authenticator = no
```

(ii) Pomagajte mu jo dopolnite tako, da bosta strežnik lahko uporabljali še dve dostopni točki na isti mreži kot že nastavljena. Privzamete lahko, da gre za sodobno dostopno točko, ki deluje v skladu z RFC5080.

3. Kateri izmed naslednjih izrazov je najbolj primeren za izračun naključne VLAN ID vrednosti (rand() vrne naključno celo število):

   - $(\text{rand}() \bmod 4095) + 1$
   - $\text{rand}() \bmod 4096$
   - $\text{rand}() \bmod 4094$
   - $(\text{rand}() \bmod 4094) + 1$

   Utemeljite odgovor.

   NAMIG: Upoštevajte, vendar ne uporabite, rezervirane vrednosti za VLAN ID (IEEE 802.1Q).