Komunikacijski protokoli in omrežna varnost
2019/20
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) Eden od načinov za vzpostavitev VPN je uporaba protokola IPsec. (i.) Pri IPsec se morata strani vzajemno avtenticirati, za kar potrebujeta skupno skrivnost. Kje se hrani le-ta? (ii.) ESP glava vsebuje dve polji. Kateri? čemu služi in kako se uporablja vsako od njih? (iii.) IPsec datgram vsebuje tudi polnilo. Ali lahko polnilo vedno uporabimo za prenos kakšnih dodatnih podatkov med članoma entitetnega para? Utemeljite odgovor.

B) (i) Kako ESP preprečuje napade s ponavljanjem? (ii) Utemeljite odgovor?

C) Peter Zmeda želi postaviti navidezno zasebno omrežje s pomočjo `OpenVPN`. Namesto skupnega ključa želi uporabiti asimetrično kriptografijo in je zato postavil svojo certifikatno agencijo (CA). Odgovore na naslednja vprašanja tudi utemeljite. (i.) Katere certifikate bo moral spraviti na OpenVPN strežnik? Za vsakega napišite, čemu je namenjen. (ii.) Katere certifikate bo moral spraviti na vsakega OpenVPN klienta? Za vsakega napišite, čemu je namenjen.

2. naloga: AAA in RADIUS.

VPRAŠANJA:

A) Storitev `syslog` je zabeležila:

```
Jan 17 10:07:27 AndyBook timed[133]:
  settimeofday({0x5e21794f,0x436ca}) == 0
```

(i.) Kateri program je zahteval zabeležko? Utemeljite odgovor. (ii.) Kaj menite, da zabeležka pomeni.

B) (i.) Opišite kako deluje napad vmesnega napdalca (*man in the middle*). (ii.) Ali je RADIUS protokol ranljiv na napad vmesnega napadalca? Utemeljite odgovor. (iii.) Zakaj protokola CHAP ne bi mogli uporabiti ob uporabi RADIUS storitve, če bi bil protokol ranljiv na napad vmesnega napadalca? Utemeljite odgovor.

NAMIG: Razmislite kje in kako (arhitektura) se uporablja CHAP protokol pri RADIUS storitvi in kdo v tem primeru pozna skupno skrivnost ter za koga ne želimo, da jo pozna.

C) Kot rečeno, RADIUS storitev nudi Špela, ki v ta namen uporablja strežnik `freeradius`. (i.) Ali lahko Špela poskrbi, da bo RADIUS deloval tudi,

če ji nekdo ugasne računalnik? Odgovor utemeljite. (ii.) Špela želi uporabnike hraniti na način, kjer, če ji nekdo ukrade računalnik, ne bo mogoče razbrati gesel. Na predzadnjih vajah pri KPOV je slišala, da je to mogoče doseči z nekakšnimi moduli. Za kakšne module gre in kako jih uporabimo v `freeradius`?

3. naloga: Podatki za delovanje omrežja.

VPRAŠANJA:

A) Imeniška storitev je osnovana na standardu X.500. (i.) Katere operacije definira standard? (ii.) Kaj posamezna operacija naredi? (iii.) Izberite tri operacije in opišite scenarij, ko jih bi neka storitev uporabila.

B) (i) Katere načine varne komunikacije ponuja protokol LDAP? (ii) Opišite njihovo delovanje.

C) 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?

4. naloga: IEEE 802.

VPRAŠANJA:

1. (i) Katera tehnika je ena izmed ključnih pri povečanju hitrosti brezžičnega prenosa od 802.11g do 802.11n? (ii) Zakaj oziroma kako omogoča povečanje hitrosti?

2. Ethernet okvir ima določeno obliko. (i.) V primeru, da je okvir uporabljen za EAPOL protokol, se kje v okvirju nahaja ta podatek? (ii.) Kakšna je vrednost, ki se uporablja, za označeavnje EAPOL protokola? (iii.) Kako to polje vpliva na delovanje mostičkov? Utemeljite odgovor.

3. Peter ima težavo - ponudnik interneta mu je „zaklenil“ usmerjevalnik tako, da deluje samo z njegovim starim računalnikom, ki bi ga sedaj rad zamenjal. (i.) Na osnovi katerega podatka, vezanega na računalnik, lahko ponudnik to zaklepanje izvaja? Utemeljite odgovor. (ii.) Recimo, da ima Peter na računalniku prav Vaš najljubši operacijski sistem. Opišite, kateri ukaz naj izvede ali kam naj klikne, da bo prišel do tega podatka. (iii.) Poleg zaklepanja na računalnik ponudnik interneta zahteva še, da se Peter prijavi z uporabniškim imenom in geslom. Ali v ta namen ponudnik lahko uporabi isti standard (802.1x) kot za avtentikacijo na brezžična omrežja? Če ne, zakaj? Če da, katera oprema mora standard podpirati?