Komunikacijski protokoli in omrežna varnost
2017/18
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) Peter sumi, da se nekdo poigrava z njegovimi paketi, ki potujejo med dvema njegovima računalnikoma. Kako naj ugotovi, če je to res – ne kako naj to prepreči, če je res. Podrobno opišite postopek preverjanja.

B) Kako ESP preprečuje napade s ponavljanjem? Utemeljite (opišite) kako vaš odgovor v resnici preprečuje napade s ponavljanjem. Lažje bo, če narišete strukturo paketa.

C) Peter Zmeda se je odločil, da bo postavil navidezno omrežje med s pomočjo OpenVPN. Spisal je takole nastavitveno datoteko, s katero se povezava vzpostavi:

```
remote 212.235.189.164
dev tap
secret static.key
```

i.) Kakšen IP naslov ima na strežnik *na vpn*? Utemeljite odgovor. ii.) Kje / kako lahko to preberemo? iii.) Kako ga lahko spremeni?

2. naloga: AAA in RADIUS.

VPRAŠANJA:

A) OTP (*One-time password*) iz RFC 2289 je podoben (odgovor utemeljite):

(a) protokoloma SRTP in CHAP,
(b) protokoloma TSL in EAP,
(c) protokoloma SRTP in EAP ali
(d) protokoloma IPsec in CHAP.

B) Protokol Radius nudi nekaj varnostnih elementov. i.) Ali nudi zakrivanje ali celovitost sporočila in kako? ii.) Opišite podrobno varovanje česa omogoča ter zakaj ostalega ne.

NAMIG: Lažje bo, če opišete (narišete) paket in smer komunikacije.

C) Peter poizkuša postaviti svoj strežnik Radius. V ta namen uporablja ukaz `radtest`. V dokumentaciji piše, da se ukaz uporablja takole:

```
radtest <username> <password> <hostname> <NAS port> <secret>
```

i.) Kakšno vrednost naj uporabi za NAS port in zakaj? Kaj ta parameter sploh pomeni? ii.) Če bo vnesel napačno geslo (*password*), kakšen odgovor lahko pričakuje? Kaj pa, če bo vnesel napačno skrivnost (*secret*)?

3. naloga: Peter Zmeda je doma v Butalah na Glavni #5 in dela na Občini Butale. Njegov e-naslov je `peter@gov.bu`. Razmislimo o naslednjih razločevalnih imenih:

1. `CN=Peter,C=Butale,STREET=Glavna #5,O=Ob. Butale,DC=gov+DC=bu`
2. `CN=Peter,C=Butale,STREET=Glavna \#5,O=Ob. Butale,DC=gov+DC=bu`
3. `CN=Peter,C=Butale,STREET=Glavna \#5,O=Ob. Butale,DC=gov,DC=bu`
4. `CN=Peter C=Butale STREET=Glavna #5 O=Ob. Butale DC=gov DC=bu`

VPRAŠANJA:

A) Katero od naštetih razločevalnih imen, določeno glede na opis v RFC 4514, je pravilno in *zakaj*. Zakaj so ostala napačna?

B) Peter se je odločil, da bo s prijatelji vzpostavil navidezno zasebno omrežje. Za avtentikacijo so se odločili, da uporabijo certifikate, ustvarjene s pomočjo `easy-rsa`, ki so ga dobili poleg OpenVPN. i.) Ali bi lahko certifikate za OpenVPN ustvarili kako drugače? Če da, kako; če ne, zakaj ne? ii.) V datoteki `vars` je vsak nastavil svoj KEY_CN. Bi lahko vsi uporabili istega? Odgovor utemeljite. iii.) Ko je Peter nastavil spremenljivke v datoteki `vars`, ukazi, kot so `build-key`, `build-req` in `sign-req`, niso delovali. Kaj je pozabil? Kako skripte, ki sestavljajo `easy-rsa` preberejo nastavitve?

C) V sistemu DNS korenski strežnik preusmerja poizvedbe, na katere ne zna odgovoriti, na DNS poizvedbe naslednjim strežnikom. i.) Kako lahko napademo ta sistem in kako se lahko branimo pred takšnim napadom? ii.) Kaj je lažje izvesti pri poizvedbah proti DNS strežnikom – varovanje celovitosti sporočil ali zakrivanje. Utemeljite odgovor.

4. naloga: IEEE 802.

VPRAŠANJA:

1. EAPOL (*EAP over LAN*) omogoča avtentikacijo uporabnika za uporabo storitve priklop na mrežo. Ali obstaja v EAPOL tudi paket, ki sporoči strežniku, da uporabnik ne potrebuje več te storitve? Izberite najboljši odgovor in ga utemeljite:

(a) Ne, saj se odklop zgodi samodejno, če v predoločenem času ni nobenega prometa.
(b) Ne, saj avtentikacija je druga storitev kot priklop na mrežo.
(c) Ne, saj ni potrebno, ker je ponudnik obeh storitev ista naprava.
(d) Da, imenuje se Logoff.

2. Pri protokolu IEEE 802.1x nastopajo tri entitete. i.) Katere in kakšna je vloga posamezne od njih? ii.) Paroma se neposredno pogovarjata po dve entiteti. Kateri in kakšen protokol se uporablja pri tem? Na kateri plasti je ta protokol? Utemeljite odgovor.

3. Peter si je doma postavil brezžično omrežje tako, da je kupil običajno brezžično dostopno točko (*wireless access point*). Sedaj bi rad do omrežja omejil dostop, pri čemer bi vsakemu uporabniku dodelil svoje ime in geslo. i.) Katero vrsto avtentikacije mora iskati v nastavitvah? ii.) Ali kaj takega sploh lahko naredi z običajno brezžično točko, namenjeno domačim uporabnikom, ne pa večjim podjetjem? Utemeljite odgovor iii.) Poleg nastavitve na brezžični dostopni točki, kaj bo moral še postaviti na omrežje – kje bodo podatki o uporabnikih?