Komunikacijski protokoli in omrežna varnost
2016/17
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) Sol je v Butlah močno cenjena dobrina in zato je Peter Zmeda za občino Butale izdelal aplikacijo za naročilo semena soli. Aplikacijo je moč uporabljati tudi preko spleta in sicer jo je Peter postavil v demilitizirano območje (*demilitarized zone*). Dostop je možen preko vrat 2017 ob uporabi TCP prenosnega protokola. Zaradi varnostnih zahtev želi Peter Cefizlju preprečiti dostop kaj šele uporabo aplikacije. S kakšnim načinom filtriranja lahko to doseže? Utemeljite odgovor.

B) Pri IPsec poznamo dva načina komunikacije: tunelski in transportni. (i.) Zapišite primer, kjer je prvi boljši od drugega, in primer, kjer je drugi primernejši od prvega. Oba primera utemeljite.

   NAMIG: Za utemeljitev razmislite kaj lahko naredimo z enim in ne moremo z drugim načinom komunikacije.

   (ii.) Pri IPsec imajo paketi lahko ESP ali AH glavo. Ali je za AH glavo tudi potreben vpis v SAD? Utemeljite odgovor.

   NAMIG: Najlaže bo, če opišete funkcionalnost, ki jo nudi AH glava ter dele IP paketa, ki ima AH glavo.

C) V Butalah so postavili navidezno lokalno IP omrežje, za kar so uporabili OpenVPN. Tip naprave so nastavili na `tap`. V Tepanjah imajo podobno omrežje, prav tako zgrajeno okrog OpenVPN. Sedaj bi v imenu boljših medsosedskih odnosov vasi radi omrežji združili, za kar bodo prav tako uporabili OpenVPN. (i.) Na kakšne težave lahko naletijo in kako jih rešiti (navedite vsaj eno)? (ii.) Kako naj nastavijo usmerjevalne tabele? (iii.) Ali omrežje lahko deluje, ne da bi imeli v usmerjevalni tabeli vsaj en prehod? Utemeljite odgovor.

2. naloga: AAA in RADIUS.

VPRAŠANJA:

A) Kako protokol CHAP preprečuje napade s ponavljanjem? Utemeljite odgovor.

B) Eden od načinov avtentikacije posameznkov je avtentikacija z biometričnmi podatki (prstni odtis, retina, ...). Peter Zmeda bi rad v svoji novi aplikaciji uporabil takšno avtentikacijo, a se ne more odločiti kako. Pri tem seveda predpostavlja, da ima uporabnik na voljo enoto, ki prebere biometrični podatek, ter ga odda kot enoličen (glede na posameznka) niz 512 bitov. Razmišljal

je o uporabi protokola CHAP. Opišite kako bi ga uporabili in implementirali celoten postopek avtentikacije.

NAMIG: Pri opisovanju rešitve posebej pazite na zaupanje posameznim elementom oziroma sestavnim delom rešitve in kako se izogniti možnosti napada. Morda bo potrebno kaj tudi narediti z napravo za branje biometričnih podatkov, da bo niz bitov, ki ga odda ter ga nato uporabimo, bolj zaupanja vreden.

C) Peter je postavil strežnik RADIUS in ustvaril nekaj uporabnikov. Nato je prišel naokrog Cefizelj, prebral `/etc/freeradius/users` in pokradel gesla vseh uporabnikov. (i.) Kako bi Peter lahko preprečil tako krajo v prihodnosti? (ii.) Kako lahko poskrbi, da gesla ne bodo shranjena na strežniku RADIUS v tekstovni obliki? Opišite vsaj 2 načina.

3. naloga: Podatki za delovanje omrežja.

VPRAŠANJA:

A) V imeniku so shranjeni predmeti. (i.) S čem je opisan posamezen predmet? Navedite primer. (ii.) Kaj je to shema in kaj določa? Navedite primer. (iii.) Kaj novega je prinesel LDAPv3 v primerjavi z LDAPv2? Naštejte vsaj tri (konkretne) dopolnitve in opišite njihovo funkcionalnost.

B) Včasih želimo najti objekte na osnovi bolj zapletenih poizvedb. Lahko bi na primer iskali vse ljudi iz Butal, ki jim je ime Francot ali Kozmijan. Vprašanje je, ali poizvedbeni jezik, s katerim dobivamo podatke iz baze LDAP, kaj takega sploh podpira? Utemeljite odgovor.

C) Peter bi rad vsem Butalcem omogočil, da bi se prijavljali na vse računalnike v vasi. Podatke o uporabnikih bo spravil v podatkovno bazo LDAP. (i.) Kaj bo moral na računalnikih nastaviti, da se bodo uporabniki lahko avtenticirali? Dovolj bo, če poveste, nastavitve katere knjižnice bo spreminjal. (ii.) Kaj bo moral nastaviti, da bo sistem ob prijavi znal prevesti uporabniška imena v številke uporabnikov? (iii.) Peter je prebral, da bo za testiranje lahko uporabil ukaz:

```
ldapsearch -H ldapi:/// \
  -D cn=peter,ou=people,dc=butale,dc=si\
  -W -b ou=people,dc=butale,dc=si
```

Kaj predstavlja niz za stikalom `-D` in kaj niz za stikalom `-b`? Kaj pa niz za stikalom `-H`?

4. naloga: IEEE 802.

VPRAŠANJA:

1. Pri protokolu IEEE 802.1X smo omenjali uporabo protokola EAPOL. (i.) Čemu je namenjen? (ii.) Prenosni protokol zanj je na Ethernet protokol na drugi plasti. Zakaj ni to IP protokol na tretji plasti? Utemeljite odgovor.

2. Peter Zmeda je slišal, da postaja internet stvari (IoT – *Internet of Things*) stvarnost. Zato se je odločil, da bo definiral svojo obliko okvirjev v protokolu IEEE802. Kaj vse mora definirati, da bodo njegovi okviri še vedno nemoteno potovali in da jih nihče drug pomotoma ne bo obdeloval? Utemeljite odgovor.

3. Peter je malce len in na vseh svojih elektronskih napravah uporablja isto geslo. Sedaj bi doma rad zavaroval svoje brezžično omrežje, obenem pa svoji sestri noče povedati svojega gesla – raje bi imel ločena uporabniška imena in gesla. Kako naj nastavi svojo brezžično dostopno točko? Kaj bo moral še postaviti / nastaviti?