Komunikacijski protokoli in omrežna varnost
2014/15
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: AAA in RADIUS.

VPRAŠANJA:

1. Peter se je odpravil tokrat v skladko-grenke posle. Prodajati je pričel kavo in čokoladne tablice preko avtomatov. Menite, da bi lahko pri tem uporabil RADIUS protokol? Utemeljite odgovor.

   NAMIG: Slika s shemo sistema bi pomagala.

2. Peter je postavil strežnik RADIUS in ustvaril nekaj uporabnikov. Sedaj se boji, da Cefizlju ne bi uspelo prikrasti na njegov strežnik ter ukrasti (prebrati) datoteke /etc/freeradius/users z gesli vseh uporabnikov. Kako naj Peter prepreči škodo ob morebitni takšni kraji? Kako lahko poskrbi, da gesla ne bodo shranjena na strežniku RADIUS v tekstovni obliki? Opišite vsaj 2 načina.

3. Ali imamo lahko FTP strežnik `abc.primer` na IP naslovu X, medtem ko bi imeli poštni strežnik za naslove `...@abc.primer` pa na naslovu Y? Utemeljite odgovor.

2. naloga: Imeniške strukture in LDAP.

VPRAŠANJA:

1. Pri protokolu LDAP lahko za varnost prenesenih podatkov poskrbimo na več različnih načinov. Eden je tako, da poženemo LDAP strežnik na posebnih vratih, ki že vsebujejo SSL (ldaps). (i) Kaj pa, če tega ne naredimo? Kako lahko zaščitimo komuniciranje? (ii) Pri protokolih imamo pogosto možnost sistematično dodati nove ukaze. Ali ta možnost obstaja tudi pri LDAP? Utemeljite odgovor.

2. Peter ima obsežen telefonski imenik prijateljev, ki ga hrani v relacijski podatkovni bazi MySQL. Za vsakega prijatelja hrani ime, priimek in telefonsko številko. Peter želi prijateljem ustvariti uporabniška imena in nastaviti gesla za dostop do svoje spletne strani. Poleg tega bi ta uporabniška imena rad uporabljal še za prijavo na računalnike. (i) Predlagajte dva protokola, ki ju lahko uporabi za prijavo? (ii) Kaj bi moral nastaviti, da bi se uporabniki na računalnikih avtenticirali neposredno z uporabo MySQL?

3. Naštejte vsaj dve pomembni razliki med LDAP v2 in LDAP v3?

3. naloga: Varnostni elementi.

VPRAŠANJA:

1. Peter Zmeda je med svojo pisarno v Zgornjih Butalah in županovo pisarno v Spodnjih Butalah vzpostavil VPN. Pri tem je uporabil sistem OpenVPN. Za konec tedna je deževalo in je bil večino časa doma ter je prebral prosojnice predmeta KPOV ter spoznal, da obstaja tudi IPsec. (i) Ali lahko vzpostavi OpenVPN preko IPsec ali obratno? Utemeljite odgovor. (ii) Ali je katerakoli od dveh možnosti smiselna? Utemeljite odgovor.

2. Peter in Konrad sta z uporabo OpenVPN vzpostavila navidezno lokalno omrežje. Uporabila sta spodnji konfiguraciji: Peter:

   ```
   proto tcp
   remote vpn.pavel.net
   dev tap
   secret skrivnost.key
   ```

   in Konrad:

   ```
   proto tcp
   dev tap
   secret skrivnost.key
   ```

   Sedaj bi na svojo mrežo rada priklopila še Polono. (i) Kako bi to lahko storila in ali lahko za priklop Polone uporabijo isto skrivnost?

   (ii) Narišite skico omrežja, če Peter in Konrad obdržita trenutne nastavitve in priklopita še Polono. (iii) Potem narišite še skico omrežja, če se bo poleg Polone na omrežje priklopilo še njenih 7 prijateljic. (iv) Kaj vse bodo Polona in prijateljice potrebovale na svojih računalnikih, da se bodo lahko prijavile na omrežje?

3. Koliko mora biti najkrajša dolžina gesel, če jih sestavljamo zgolj iz malih črk angleške abecede (26 črk) in števk 0-5, če želimo, da je varnost enakovredna (ali večja) kot pri ključih dolžine 192 bitov?

4. naloga: Razno.

VPRAŠANJA:

1. Pri standardu IEEE 802.1x nastopajo tri naprave. (i) Narišite shemo, vpišite vanjo naprave, opišite kakšne so lahko povezave med njimi in opišite vlogo posamezne naprave.

   Peter Zmeda je dobil čudnega odjemalca, ki zna govoriti pri avtentikaciji za potrebe dostopa do omrežja samo PAP. (ii) Kje in kaj lahko Cefizelj napade? Razmislite, kakšno škodo lahko povzroči? (iii) Imate kakšen predlog za zaščito?

2. Peter je v prostem času ovčjerejec in rad gleda filme ovac,[1] ki se pasejo na travnikih. Zaenkrat jih predvaja s strežnika, na katerem ima VLC predvajalnik. VLC v neskončnost predvaja zaporedje videov o ovčkah.

   Petra malce moti dejstvo, da, če se prijavi na strežnik, skoraj nikdar ne ujame začetka videa. Poleg tega bi rad postavil storitev Video-na-zahtevo. (i) Kateri kos programske opreme lahko v ta namen uporabi? (ii) Ali lahko na istem strežniku nudi obe storitvi (video v živo in na zahtevo)? (iii) Kaj pa na istem naslovu? Utemeljite odgovore!

3. Kako protokol CHAP preprečuje napade s ponavljanjem? Opišite korake, ki jih izvede in kako z njimi preprečuje napade.

[1] Glede na ovce pri sosednji fakulteti, morda končno le v živo spoznamo našega Petra Zmedo.