Komunikacijski protokoli in omrežna varnost
2021/22
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 Zmeda želi postaviti navidezno zasebno omrežje s pomočjo (izmišljenega) programa *WireSentinel*. Za razliko od *OpenVPN*, se *WireSentinel* zanaša izključno na skupne skrivnosti, pri čemer sta skrivnosti za sprejemanje in pošiljanje ločeni. (i.) Kako v takšnem primeru nastavi certifikatno agencijo? (ii.) Koliko odjemalcev ima lahko takšen sistem? Utemeljite odgovor!

B) Recimo, da bi napravi A in B želeli varno komunicirati z uporabo IPsec. (i.) Kje je zapisano, kako naj se zaščiti posamezen poslani datagram?

(1) Določa SAD.
(2) Definirano je preko IKE.
(3) V SPD.
(4) V ESP glavi.

(ii.) Utemeljite odgovor tako, da za vsakega od odgovorov opišete kaj se skriva za kratico in čemu služi mehanizem, ki ga popisuje kratica.

C) Na predavanjih smo srečali tri vrste filtriranj, ki jih lahko opravlja požarna pregrada. (i.) Katere so te vrste filtriranj? (ii.) Za vsako od njih opišite primer napada, ki ga s tem načinom filtriranja lahko branimo in kako ga branimo.

2. naloga: AAA in RADIUS.

VPRAŠANJA:

A) (i.) Kakšna je razlika med avtentikacijo in avtorizacijo?

(a) Avtentikacija nam pove dovoljenja osebe, avtorizacija pa pravila, kako se ta dovoljenja uporabijo.
(b) Avtentikacija nam pove dovoljenja osebe, avtorizacija pa identiteto osebe.
(c) Avtentikacija nam pove identiteto osebe, avtorizacija pa dovoljenja, ki jih oseba ima.
(d) Avtentikacija nam pove identiteto osebe, avtorizacija pa beleži avtorstvo izvedenih ukazov na sistemu.

(ii.) Zapišite primer avtentikacije in primer avtorizacije.

B) Peter Zmeda bi rad na vseh računalnikih vedno uporabljal isto ime in geslo. (i.) Ali lahko v ta namen uporabi strežnik *OpenLDAP*? Utemeljite odgovor. (ii.) Kaj bo moral nastaviti na vseh *GNU/Linux* in *BSD* računalnikih, da se bo lahko avtenticiral s pomočjo zunanjega strežnika? (iii.) Identifikacija mu deluje, vendar mu sistem ob prijavi vrne: `"unknown user"`. Z ukazom `getent passwd peter` prav tako ne najde ničesar. Katero knjižnico / komponento bo moral še nastaviti?

C) Pri protokolu PAP si strežnik, ki avtenticira in odjemalec, ki se želi avtenticirati, izmenjujeta sporočila. (i.) Zapišite zaporedje in pomen sporočil, ki si jih odjemalec in strežnik izmenjujeta ter utemeljite svojo izbiro. (ii.) Predlagajte in utemeljite elemente (polja), ki jih sporočilo vsebujejo. (iii.) Gesla strežnik hrani v datoteki in da oteži njihovo razšifriranje, uporablja sol. Opredelite po dve dobri in dve slabi strani, če strežnik uporablja eno samo sol za vse uporabnike in ne za vsakega uporabnika svoje soli.

3. naloga: Podatki za delovanje omrežja. Po standardu X.509 digitalno potrdilo vsebuje tudi:

(1) Version Number
(2) Serial Number
(3) Signature Algorithm ID
(4) Issuer Name
(5) Validity period: Not Before, Not After
(6) Subject name
(7) Subject Public Key (PK) Info: PK Algorithm, Subject PK
(8) Issuer Unique Identifier (opt.)
(9) Subject Unique Identifier (opt.)
(10) Extensions (opt.): ...
(11) Certificate Signature Algorithm
(12) Certificate Signature

VPRAŠANJA:

A) Podpisi so v potrdilu omenjeni v vrstici 3 in v vrsticah 11 in 12. (i.) Čemu dvakrat? Imamo naslednji konfiguraciji storitev:

$$\text{uporabnik} \iff S_1 \iff \text{AAA} \iff \text{LDAP} \quad (1)$$

$$\text{uporabnik} \iff S_2 \iff \text{LDAP} \quad (2)$$

(ii.) Za vsako od konfiguracij zapišite dva primera, ko je primernejša od druge konfiguracije. Utemeljite svoj odgovor.

B) Peter je pognal naslednji ukaz:

```
ldapsearch -H ldap://ldap.zmeda.si
  -D "CN=peter,OU=peter;DC=ldap;DC=zmeda;DC=si"
  -b "O=butale,DC=zmeda,DC=si" "(CN=peter)"
```

(i.) Kaj je v tem ukazu niz za `-b`? (ii.) Kaj v angleščini predstavlja kratica `OU`? Kaj pa `DC`? (iii.) Kako bi ukaz predelali, da bi vrnil vnose, kjer je ime `peter` in priimek `zmeda`? Kratica za priimek je `SN` ali `surName`, za ime pa `GN` ali `GivenName`.

C) Peter Zmeda je malce zmeden. Namesto v nastavitvene datoteke strežnika DNS in DHCP je namreč podatke o računalnikih - IP naslove, MAC naslove

in imena v svojem omrežju vnesel v imenik, dostopen prek LDAP. Sedaj bi rad podatke uporabil za strežnike DHCP in DNS, pri tem bi rad čim manj podatkov pretipkaval. Kateri od spodnjih odgovorov daje najboljši nasvet? Utemeljite odgovor.

(a) Za rešitev bo nujno potreboval razširitve, ki jih ponuja razširitev LDAP - Microsoft Active Directory.
(b) DHCP strežnik lahko kot bazo uporabi LDAP; DNS bo moral podatke sprejemati od DHCP strežnika, saj DNS strežniki podatkov ne shranjujejo v LDAP. Alternativa je, da vsi trije strežniki - DHCP, DNS, in LDAP poberejo podatke iz skupne relacijske podatkovne baze (npr. MySQL).
(c) DHCP in DNS strežnika lahko svoje nastavitve prebereta iz baze LDAP.
(d) Podatke bo moral kopirati ročno, saj sta DHCP in DNS ločena protokola od LDAP.

4. naloga: IEEE 802.

VPRAŠANJA:

A) Protokol IEEE 802.1D se ukvarja z MAC mostički (angl. *bridge*) in med drugim določa protokol za izgradnjo vpetega drevesa v omrežju. Zakaj potrebujemo vpeto drevo?

(a) Da preprečimo razpošiljanje okvirjev.
(b) Da lahko okvir v logaritemskem času prispe do cilja.
(c) Za izračun najkrajših poti.
(d) Da imamo unikatno pot (brez ciklov) med poljubnima vozliščema.

(ii.) Utemeljite zakaj želimo imeti to lastnost?

B) Peter Zmeda je zavarovaval priklop v svoje omrežje z IEEE 802.1x storitvijo, pri čemer je uporabil Špelino RADIUS storitev. (i.) Narišite arhitekturo celotnega sistema, ki vključuje strežnik priklopa v mrežo, AAA strežnik in seveda odjemalca. (ii.) Za avtentikacijo se je odločil uporabiti CHAP protokol. Narišite format okvirja, ki potuje od odjemalca. Ker je Špela nezaupljiva, je spremenila avtentikacijo tako, da so sporočila tunelirana preko TLS tunela. Sedaj mora odjemalec najprej vzpostaviti TLS tunel z AAA strežnikom. (iii.) Kaj morata izmenjati, da se tunel lahko vzpostavi? Utemeljite, zakaj morata izmenjati prav te podatke?

C) Peter se je odločil, da bo poskrbel za varnost na svojem brezžičnem omrežju. Namesto 802.1x bo uporabil OpenVPN. (i.) Kakšne prednosti bo imela njegova rešitev? Naštejte vsaj dve. (ii.) Kakšne slabosti bo imela njegova rešitev? Naštejte vsaj dve. (iii.) Ali lahko OpenVPN poganja na brezžičnem usmerjevalniku? Utemeljite odgovor.