Komunikacijski protokoli in omrežna varnost
2018/19
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) Za uspešno vzpostavitev zasebnega navideznega omrežja so ključni podatki, ki jih vsebuje SA zapis. (i.) Naštejte pet elementov, ki jih SA zapis hrani ter za vsakega od njih kako (oziroma za kaj) se uporablja. (ii.) Zakaj en SA zapis vsebuje samo podatke za vzpostavitev enosmerne povezave?

B) Kateri od naslednjih opis najbolje opisuje pojem *tunneling*:

   (a) sistem za zaznavo napak v paketu pri prenosu preko omrežja;
   (b) način šifriranja paketa, tako da se šifrira podatke in glavo;
   (c) sistem za detekcijo vdorov v omrežje; ali
   (d) način šifriranja paketa, tako da se šifrira samo podatke.

   Utemeljite odgovor, oziroma opišite postopek.

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.) Ali mora biti CA postavljena na računalniku znotraj navideznega omrežja? (ii.) Na računalniku s CA se je pokvaril disk, zaradi česar so izgubljeni vsi podatki. Se lahko uporabniki še zmeraj povežejo v navidezno omrežje? (iii.) Kaj morajo narediti uporabniki, preden bodo lahko začeli uporabljati novo CA?

2. naloga: AAA in RADIUS.

VPRAŠANJA:

A) Storitev `syslog` je zabeležila:

```
Jan  1 21:38:22 svarun dhcpd: uid lease 192.168.127.137
  for client 10:9a:dd:a6:dd:38 is duplicate on 192.168.127.0/24
```

   Kateri od naslednjih programov je zahteval zabeležko: a.) `lease`; b.) `svarun`; c.) `uid`; ali č.) `dhcpd`. Utemeljite odgovor.

B) Peter želi ponuditi novo storitev in sicer tiskanje nalepk. Razumljivo, tiskanje ni dovoljeno kar vsakomur in zato želi uporabiti RADIUS storitev, ki jo ponuja Špela. (i.) Narišite sliko arhitekture Špeline in Petrove storitve ter kje je uporabnik Petrove storitve. Označite kakšen protokol je uporabljen med posameznimi elementi arhitekture. (ii.) Luka Kratkohlačnica je uporabnik, ki želi uporabiti Petrovo storitev. Čim podrobneje opišite, kako poteka avtentikacija in avtorizacija, pri čemer se naj uporabklja CHAP protokol.

NAMIG: Kakšni podaki (čistopis ali šifrirani in kako šifrirani) se prenašajo med elementi vaše arhitekture.

(iii.) Opišite, kako lahko Cefizelj izvede vmesni (MITM, *man in the middle*) napad na CHAP protocol. Za lažje odgovarjanje, vam ni potrebno upoštevati RADIUS protokola; se pravi Ana bi rad avtenticirala Braneta in Cefizelj izvaja MITM napad.

C) Kot rečeno, RADIUS storitev nudi Špela, ki v ta namen uporablja strežnik `freeradius`. (i.) Na koga oziroma kaj se nanašajo vnosi v datoteki `/etc/freeradius/3.0/clients.conf`? (ii.) Špela želi uporabnike hraniti v podatkovni bazi `mysql`. Ali naj bo strežnik `mysql` na istem računalniku kot `freeradius`? Zapišite po eno prednost za uporabo ločenega in za uporabo istega stroja za obe storitvi.

3. naloga: Podatki za delovanje omrežja.

VPRAŠANJA:

A) Peter za hranjenje podatkov uporablja storitev LDAP, ki jo nudi Simona. Ker Peter ni zahteval nobenih posebnosti, je Simona doslej ponujala LDAP.V2, sedaj pa mora nadgraditi storitev na LDAP.V3. (i.) Kaj je zahteval Peter, da Simona ni mogla tega zagotoviti s starejšo inačico storitve? (ii.) Poleg tega je Peter našel na sistemu ukaz `ldapcompare` z naslednjim opisom:

> **ldapcompare** opens a connection to an LDAP server, binds, and performs a compare using specified parameters. The DN should be a distinguished name in the directory. Attr should be a known attribute. If followed by one colon, the assertion value should be provided as a string. If followed by two colons, the base64 encoding of the value is provided. The result code of the compare is provided as the exit code and, unless ran with `-z`, the program prints TRUE, FALSE, or UNDEFINED on standard output.

Zakaj vrne opisane rezultate? Utemeljite odogovor in primer uporabe.

B) Peter Zmeda je doma v Butalah na Glavni ulici #5 in dela na Občini Butale. Njegov e-naslov je `peter.zmeda@gov.bu`. Kakšno je razločevalno ime, ki ga najbolje določa glede na opis v RFC 4514:

   (a) `CN=Peter Zmeda,C=Butale,STREET=Glavna ulica \#5,O=Ob. Butale,DC=gov,DC=bu`
   (b) `CN=Peter Zmeda,C=Butale,STREET=Glavna ulica \#5,O=Ob. Butale,DC=gov+DC=bu`

(c) `CN=Peter Zmeda,C=Butale,STREET=Glavna ulica #5,O=Ob. Butale,DC=gov+DC=bu`

(d) `CN=Peter Zmeda C=Butale STREET=Glavna ulica #5 O=Ob. Butale DC=gov DC=bu`

Utemeljite odgovor.

C) Kaj in kam moramo v sistemih Unix zapisati, da se bo za razreševanje internetnih imen uporabljal DNS strežnik z naslovom `193.2.1.66`? Utemeljite odgovor.

4. naloga: IEEE 802.

VPRAŠANJA:

1. 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. Izberite eno od kombinacij polj v okvirju, ki jih mora definirati, da bodo njegovi okviri še vedno nemoteno potovali in da jih nihče drug pomotoma ne bo obdeloval: a.) ciljni naslov in podatke; b.) izvorni naslov in podatke; c.) samo podatke; ali č.) polje `ethertype`? Utemeljite odgovor.

2. Prenosna plast, ki je implementirana z IEEE.802 protocolom je običajno razdeljena na dve podplasti. (i.) Kateri sta ti podplasti? (ii.) V kateri podplasti delujejo mostički (*bridge*)? Utemeljite odgovor. (iii.) Usmerjanjem (*routing*) in premoščanje (*bridging*) sta zelo podobni storitvi. Katera od njiju zahteva več virov za enako število ciljnih vozlišč in zakaj?

3. Peter ima slab spomin in si nikakor ne more zapomniti MAC naslova omrežnega vmesnika v svojem računalniku. Rad bi namreč poskrbel, da bi njegov računalnik ob priklopu v domače omrežje vedno dobil isti naslov. (i.) Kako lahko ugotovi kakšen je MAC naslov njegovega računalnika? (ii.) Kako lahko poskrbi, da bo njegov računalnik dobil isti naslov? Seveda, ročno nastavljanje IP naslova ne pride v poštev. (iii.) Zakaj uporaba DHCP storitve ne omogoča zaščite omrežja pred priklopom nepovabljenih gostov?

   NAMIG: Opišite napad.