Komunikacijski protokoli in omrežna varnost
2013/14
Pisni izpit 10. svečana 2014

Izpit morate pisati posamič. Pri reševanju je literatura dovoljena.

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:

VPRAŠANJA:

1. DHCP oziroma bootp protokol podpira tudi uporabo vmesnega strežnika (*proxy*). (i) Narišite shemo omrežja, v katerem se uporablja vmesni strežnik ter na tem primeru opišite delovanje bootp protokola z uporabo vmesnega strežnika. (ii) Katera polja v bootp paketu se uporabljajo in kako, ko imamo opravka z vmesnim strežnikom.

2. Peter zaganja svoj računalnik prek mreže. Ker je slišal, da je TFTP neučinkovit protokol, ga sploh ne bi rad uporabljal. Ali lahko to doseže? Katere kose programske opreme bo moral popraviti?

3. Ali na omrežju lahko zasledimo DHCPv6 zahtevo (*request*) odjemalca, kjer sta izvorna IPv6 naslov in številka vrat [fe80::0011:33de:fe17:55aa]:547 ter ciljna IPv6 naslov in številka vrat [ff02::1:4]:546? Utemeljite odgovor.

2. naloga: Peter je ugotovil, da mu v službi nekdo krade sendviče iz skupnega hladilnika. Da bi ugotovil, kdo je zmikavt, je pred hladilnik postavil računalnik s kamero in na njem pognal:

```
vlc --sout "#transcode{vcodec=h264,acodec=mpga,ab=128,
    channels=2,samplerate=44100}:
  rtp{dst=239.255.12.55,port=5004,mux=ts,sap,name=obodin,ttl=6}"
  --sout-keep v4l2:///dev/video0
```

Nato je na enem od računalnikov, ki je povezan v lokalno omrežje v podjetju ter ima naslova 192.168.6.12 in 212.235.189.163, pognal:

```
vlc --sout "#transcode{vcodec=mp2v,vb=800,
    acodec=mpga,ab=128,channels=2,samplerate=44100}:
  http{mux=ts,dst=:8080/}" rtp://239.255.12.55:5004
```

Doma je na računalniku, ki ima dva omrežna vmesnika, od katerih je eden na javnem IP naslovu in drugi na naslovu 192.168.1.13, pognal:

```
vlc --sout "#transcode{acodec=mpga,ab=128,
    channels=2,samplerate=44100}:
  http{mux=ts,dst=:8080/}" http://212.235.189.163:8080/
```

Na koncu je na malem, tihem računalniku pod televizorjem v dnevni sobi pognal:

```
vlc http://192.168.1.13:8080/
```

Ves sistem mu deluje, tako da sedaj sedi na kavču in budno čuva svoje sendviče.

VPRAŠANJA:

1. (i) Kako se spreminja TTL na paketih, ki se pretakajo med njegovimi računalniki? (ii) Ali bi lahko to, kar počne, izvedel na manj potraten način (z manjšo porabo časa na procesorjih in pomnilnika)? (iii) Če ve, da je edini uporabnik, kako bi lahko izboljšal kakovost slike?

2. Naj vam zaupamo, da je tat zviti Cefizelj. Da bi zakril sledove, je uprizoril napad s človekom na sredi (*man in the middle attack*). (i) Kako je Cefizelj to izvedel? (ii) Kako se naj Peter zavaruje pred takšnim napadom in pri tem naj dopusti, da lahko še kdorkoli drug opazuje hladilnik preko nameščene kamere.

3. Zakaj TCP protokol ni primeren za prenos podatkov v stvarnem času?

3. naloga: Na strežnikih A.zmeda.si in B.krofki.si imamo naslednje datoteke: Datoteka `A:/etc/freeradius/proxy.conf`:

```
# -*- text -*-
##
## proxy.conf -- proxy radius and realm configuration directives
##
##  $Id$
proxy server {
    default_fallback = no
}
home_server localhost {
    type = auth
    ipaddr = 127.0.0.1
    port = 1812
    secret = testing123
    require_message_authenticator = yes
    response_window = 20
    zombie_period = 40
    revive_interval = 120
    status_check = status-server
    check_interval = 30
    num_answers_to_alive = 3
    coa {
        irt = 2
        mrt = 16
        mrc = 5
        mrd = 30
    }
}
```

```
home_server_pool my_auth_failover {
    type = fail-over
    home_server = localhost
}
realm example.com {
    auth_pool = my_auth_failover
}
realm LOCAL {
}
home_server palacinke_hs {
    ipaddr = radius.palacinke.si
    port = 1812
    secret = stepenajajca
}
home_server_pool palacinke_pool {
    type = fail-over
    home_server = palacinke_hs
}
realm palacinke {
    auth_pool = palacinke_pool
}
```

Datoteka `A:/etc/freeradius/clients.conf`:

```
# -*- text -*-
##
## clients.conf -- client configuration directives
##
##  $Id$
#####################################################
client localhost {
    ipaddr = 127.0.0.1
    secret      = MOJEGESLO
    require_message_authenticator = no
}
client B {
    ipaddr = B.krofki.si
    secret = marmelada
}
```

Datoteka `A:/etc/freeradius/users`:

```
#
#   Please read the documentation file
#   ../doc/processing_users_file, or 'man 5 users'
#   (after installing the server) for more information.
```

```
#
peter Cleartext-Password := "lawandorder"
    Reply-Message = "peter"
DEFAULT Framed-Protocol == PPP
    Framed-Protocol = PPP,
    Framed-Compression = Van-Jacobson-TCP-IP
DEFAULT Hint == "CSLIP"
    Framed-Protocol = SLIP,
    Framed-Compression = Van-Jacobson-TCP-IP
DEFAULT Hint == "SLIP"
    Framed-Protocol = SLIP
```

Datoteka `B:/etc/freeradius/proxy.conf`:

```
# -*- text -*-
##
## proxy.conf -- proxy radius and realm configuration directives
##
##  $Id$
proxy server {
    default_fallback = no
}
home_server localhost {
    type = auth
    ipaddr = 127.0.0.1
    port = 1812
    secret = testing234
    require_message_authenticator = yes
    response_window = 20
    zombie_period = 40
    revive_interval = 120
    status_check = status-server
    check_interval = 30
    num_answers_to_alive = 3
    coa {
        irt = 2
        mrt = 16
        mrc = 5
        mrd = 30
    }
}
home_server_pool my_auth_failover {
    type = fail-over
    home_server = localhost
```

```
}
realm example.com {
    auth_pool = my_auth_failover
}
realm LOCAL {
}
home_server palacinke_hs {
    ipaddr = radius.palacinke.si
    port = 1812
    secret = stepenajajca
}
home_server_pool palacinke_pool {
    type = fail-over
    home_server = palacinke_hs
}
realm palacinke {
    auth_pool = palacinke_pool
}
```

Datoteka `B:/etc/freeradius/clients.conf`:

```
# -*- text -*-
##
## clients.conf -- client configuration directives
##
##  $Id$
#####################################################
client localhost {
    ipaddr = 127.0.0.1
    secret      = MOJEGESLO
    require_message_authenticator = no
}
client B {
    ipaddr = B.krofki.si
    secret = marmelada
}
```

Datoteka `B:/etc/freeradius/users`:

```
#
#   Please read the documentation file
#   ../doc/processing_users_file, or 'man 5 users'
#   (after installing the server) for more information.
#
sandi Cleartext-Password := "aspdotnet"
```

VPRAŠANJA:

1. (i) Dopolnite datoteke tako, da bo strežnik A skrbel za uporabniška imena oblike `USER@zmeda.si`. Za krofki.si ni treba skrbeti, so že v redu. Uporabniki s takšnimi uporabniškimi imeni naj se prijavljajo tudi na klientih, ki se povezujejo na strežnik B. (ii) Ali obstaja način, da se na strežnika prijavi uporabnik z uporabniškim imenom `miha@zmeda.si`? Odgovor utemeljite.

2. Za varnost v protokolu RADIUS ni najbolje poskrbljeno. Sicer je v protokol vgrajen en varnostni element. (i) Kateri in kako deluje?[1] (ii) Pred kakšnimi napadi nas varuje ta mehanizem? Opišite kako delujejo in kako varuje. (iii) Pred kakšnimi napadi nas pa ne varuje? Opišite tudi delovanje le-teh in zakaj nas ne varuje.

3. Kako protokol CHAP preprečuje napade s ponavljanjem? Opišite rešitev.

4. (NEOBVEZNO) Kulturni praznik je ravno za nami. Občina Žirovnica je majhna občina na severo-zahodu Slovenije. Na njenem ozemlju so se rodili kar štirje veliki slovenski književniki. Kateri?

   NAMIG: Na pomlad, ko bodo toplejši dnevi, je pešpot kulturne dediščine v občini Žirovnica enkraten dnevni sprehod. Na koncu si privoščite še obed v gostilni, v katero naj bi zahajal literarni junak Janka Mlakarja (pa Mlakar ni eden od štirih zgoraj).

4. naloga:

VPRAŠANJA:

1. (i) Kakšna je razlika med oddajanjem (*broadcasting*) in razpošiljanjem (*multicasting*)? (ii) Na katerih plasteh vse lahko in kako deluje oddajanje?

   NAMIG: Na drugi plasti upoštevajte IEEE 802 družino, na tretji plasti IP* in na *ostalih* plasteh različne protokole.

2. Peter Zmeda je na vajah zgrožen ugotovil, da mu lahko, odkar je namestil Linux, vsakdo vdre v računalnik tako, da v menuju zagonskega nalagalnika stisne `e`, nato pa v vrstico, ki se začne z `linux` vpiše `init=/bin/bash`. Da bi se zaščitil, je predelal program `/bin/bash` tako, da ob vsakem zagonu zahteva dodatno geslo. (i) Kako napadalec lahko zaobide tovrstno

[1] Pri opisu bodite izčrpni.

zaščito? (ii) Bi takšna rešitev lahko povzročila kak problem? Utemeljite odgovor. (iii) Kako bi se pred tovrstnim napadom še lahko zaščitil?

NAMIG: Uporabnikom dostopa do tipkovnice in miške ne more preprečiti, fizični dostop do preostanka računalnika pa je že omejil.

3. Recimo, da bi želeli varno komunicirati napravi A in B s pomočjo protokola IPsec. (i) Kje in (ii) kako je zapisano, kako naj se zaščiti posamezen datagram?