باسمه تعالی

درس: امنیت شبکه

نام و نام خانوادگی: محمد هادی امینی

شماره دانشجویی: 9912762370

شماره تمرین : 03

تاریخ تحویل: 1403/02/01

موضوع تمرین: **kerbros**

احراز هویت Kerberos و سیستم های احراز هویت سنتی مبتنی بر رمز عبور هر دو رویکرد مختلفی برای اطمینان از امنیت دسترسی به سیستم هستند. چند تفاوت اصلی بین آنها عبارتند از:

1. **مبنای عملکرد:**

- **احراز هویت مبتنی بر رمز عبور :در این روش، کاربران با وارد کردن نام کاربری و رمز عبور خود احراز هویت می‌شوند.**
- **احراز هویت :Kerberos این سیستم بر اساس مدل تیکت‌بازی می‌کند. به طور خلاصه، کاربران با یک مرکز توزیع کلید (KDC) ارتباط برقرار می‌کنند و پس از احراز هویت توسطKDC ، یک تیکت امنیتی دریافت می‌کنند که به آنها اجازه دسترسی به منابع مورد نیاز را می‌دهد.**

2. **امنیت:**

- **احراز هویت مبتنی بر رمز عبور :این روش به طور عمده بر اطلاعات ورودی کاربر (نام کاربری و رمز عبور) تکیه دارد. در صورتی که این اطلاعات مورد حمله‌ی خرابکاران قرار گیرد، حساب کاربری در معرض خطر قرار می‌گیرد.**
- **احراز هویت :Kerberos این سیستم از تیکت‌های امنیتی استفاده می‌کند که بر اساس الگوریتم‌های رمزنگاری قوی ایجاد می‌شوند. حتی اگر یک تیکت در دست یک مهاجم قرار گیرد، او قادر به استفاده از آن برای دسترسی به سیستم نخواهد بود.**

3. **مدیریت کلید:**

- **احراز هویت مبتنی بر رمز عبور :مدیران سیستم باید به مداوم رمزهای عبور را مدیریت کنند، از جمله تغییر دادن آنها به فواصل زمانی منظم و مدیریت سطوح دسترسی.**

- **احراز هویت :Kerberos از آنجا که Kerberos بر اساس تبادل تیکت‌های امنیتی کار می‌کند، مدیران نیازی به مدیریت رمزهای عبور ندارند. این تیکت‌ها بر اساس کلیدهای امنیتی و معماری عمومی/خصوصی رمزنگاری شده‌اند.**

4. بهره‌وری:

- **احراز هویت مبتنی بر رمز عبور :برای کاربران ممکن است ایجاد و مدیریت رمزهای عبور مختلف برای انواع مختلف سرویس‌ها و سیستم‌ها امری زحمت‌آور باشد.**
- **احراز هویت :Kerberos کاربران می‌توانند با یکبار ورود و دریافت یک تیکت امنیتی به همه‌ی منابع مورد نیاز دسترسی پیدا کنند، بدون نیاز به ورود مجدد.**

با این تفاوت‌ها، احراز هویت Kerberos به عنوان یک سیستم مبتنی بر تیکت با قابلیت‌های امنیتی بالا و مدیریت سهل‌تر می‌تواند بهترین راه‌حل برای سازمان‌هایی با نیازهای امنیتی بالا باشد. از طرف دیگر، احراز هویت مبتنی بر رمز عبور نیز همچنان در بسیاری از محیط‌های کاربردی مورد استفاده قرار می‌گیرد، اما باید از روش‌هایی برای بهبود امنیت آن استفاده شود مانند استفاده از رمزهای عبور قوی و مکانیزم‌های دومرحله‌ای.

ابتدا با دستور زیر Kerberos را روی ماشین dutنصب میکنیم:

```
sudo apt-get install krb5-kdc krb5-admin-server
```

و روی ماشین in و out دستور زیر را میزنیم:

```
sudo apt-get install krb5-user
```

در هنگام نصب ، نام قلمرو را برابر با AMINI.IR قرار میدهیم و kdc و admin_server برابر با ادرس ماشین dut است. این اطلاعات در فایل krb5.conf قابل مشاهده است.

```
  GNU nano 4.8                          /etc/krb5.conf                          Modif
[libdefaults]
        default_realm = AMINI.IR

# The following krb5.conf variables are only for MIT Kerberos.
        kdc_timesync = 1
        ccache_type = 4
        forwardable = true
        proxiable = true
        default_tkt_enctypes = aes256-cts-hmac-sha1-96 aes128-cts-hmac-sha1-96
        default_tgs_enctypes = aes256-cts-hmac-sha1-96 aes128-cts-hmac-sha1-96

# The following encryption type specification will be used by MIT Kerberos
# if uncommented.  In general, the defaults in the MIT Kerberos code are
# correct and overriding these specifications only serves to disable new
# encryption types as they are added, creating interoperability problems.
## The only time when you might need to uncomment these lines and change
# the enctypes is if you have local software that will break on ticket
# caches containing ticket encryption types it doesn't know about (such as
# old versions of Sun Java)
#       default_tgs_enctypes = des3-hmac-sha1
#       default_tkt_enctypes = des3-hmac-sha1
#       permitted_enctypes = des3-hmac-sha1

# The following libdefaults parameters are only for Heimdal Kerberos.
        fcc-mit-ticketflags = true

[realms]
        AMINI.IR = {
                kdc = 192.168.100.1
                admin_server = 192.168.100.1
        }
```

برای دسترسی به ماشین ها از طریق نام، آیپی آن ها را در فایل /etc/hosts قرار میدهیم.

```
  GNU nano 4.8                                  /etc/hosts
127.0.0.1 localhost
127.0.1.1 in
192.168.100.1 dut
192.168.101.2 out
# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

ماشین in

```
 GNU nano 4.8                                    /etc/hosts
127.0.0.1 localhost
127.0.1.1 dut
192.168.100.1 in
192.168.101.1 out
# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

ماشین dut

```
 GNU nano 4.8                                    /etc/hosts
127.0.0.1 localhost
127.0.1.1 out
192.168.100.1 in
192.168.101.2 dut
# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

ماشین out

بعد از تنظیم کانفیگ ها با دستور krb5_newrealm میتوانیم دیتابیس کربروس را راه اندازی کنیم.

سپس در ماشین dut با دستور kadmin.local وارد دستورات مربوط به ادمین میشویم.

```
kadmin:  ?
Available kadmin requests:

add_principal, addprinc, ank
                         Add principal
delete_principal, delprinc
                         Delete principal
modify_principal, modprinc
                         Modify principal
rename_principal, renprinc
                         Rename principal
change_password, cpw     Change password
get_principal, getprinc  Get principal
list_principals, listprincs, get_principals, getprincs
                         List principals
add_policy, addpol       Add policy
modify_policy, modpol    Modify policy
delete_policy, delpol    Delete policy
get_policy, getpol       Get policy
list_policies, listpols, get_policies, getpols
                         List policies
get_privs, getprivs      Get privileges
ktadd, xst               Add entry(s) to a keytab
ktremove, ktrem          Remove entry(s) from a keytab
lock                     Lock database exclusively (use with extreme caution!)
unlock                   Release exclusive database lock
purgekeys                Purge previously retained old keys from a principal
get_strings, getstrs     Show string attributes on a principal
set_string, setstr       Set a string attribute on a principal
del_string, delstr       Delete a string attribute on a principal
list_requests, lr, ?     List available requests.
quit, exit, q            Exit program.
kadmin:
```

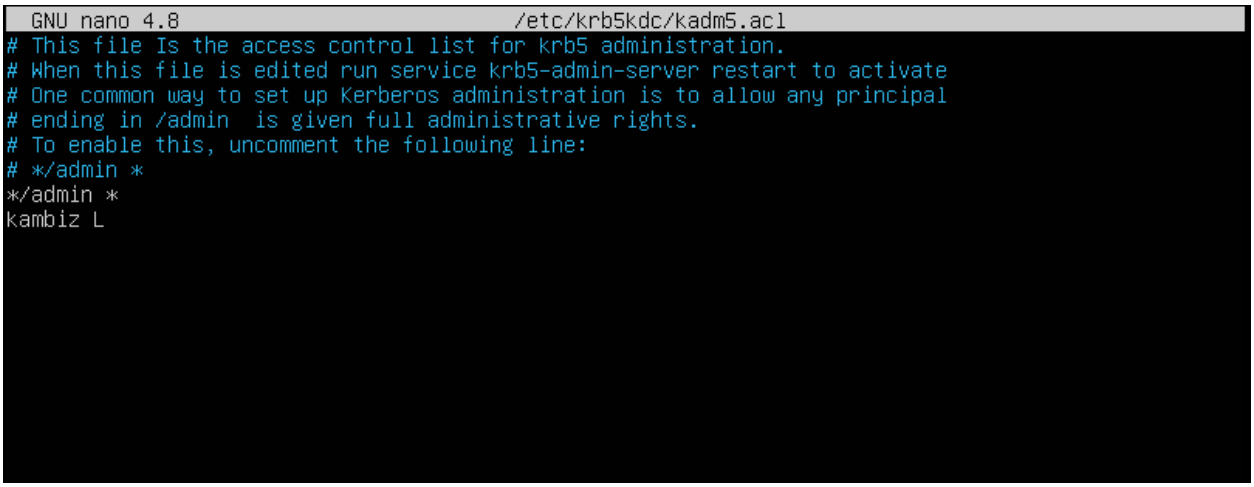
برای ساخت مدیر از دستور addprinc استفاده میکنیم.

```
kadmin.local:  addprinc hadi/admin
WARNING: no policy specified for hadi/admin@AMINI.IR; defaulting to no policy
Enter password for principal "hadi/admin@AMINI.IR":
Re-enter password for principal "hadi/admin@AMINI.IR":
Principal "hadi/admin@AMINI.IR" created.
```

دو principal با نام های kambizو hadi/admin میسازیم.

برای ایجاد سطح دسترسی متفاوت، فایل kadm5.acl را ویرایش میکنیم.

برای مدیران (با اسم admin)تمام دسترسی ها را مجاز میکنیم و برای kambiz دسترسی محدودتری درنظر میگیریم



فرمت دستورات به صورت زیر است:

principal permissions

لیست فلگ های قابل استفاده:

a	[Dis]allows the addition of principals or policies
c	[Dis]allows the changing of passwords for principals
d	[Dis]allows the deletion of principals or policies
e	[Dis]allows the extraction of principal keys
i	[Dis]allows inquiries about principals or policies
l	[Dis]allows the listing of all principals or policies
m	[Dis]allows the modification of principals or policies
p	[Dis]allows the propagation of the principal database (used in Incremental database propagation)
s	[Dis]allows the explicit setting of the key for a principal
x	Short for admcilsp. All privileges (except `e`)
*	Same as x.

با حروف کوچک دسترسی اعطا میشود و با حروف بزرگ دسترسی ممنوع میشود.

اکنون kambiz دسترسی مشاهده لیست principals را ندارد

سپس با دستورات زیر ادمین سرور و kdc را ریستارت میکنیم.

```
sudo systemctl restart krb5-admin-server.service
sudo systemctl restart krb5-kdc.service
```

حالا میتوانیم با دستور kinit در ماشین های in و outتیکت دریافت کنیم و با دستور klist آن را مشاهده کنیم.

```
hadi@in:~$ kinit kambiz
Password for kambiz@AMINI.IR:
hadi@in:~$ klist
Ticket cache: FILE:/tmp/krb5cc_1000
Default principal: kambiz@AMINI.IR

Valid starting       Expires              Service principal
04/23/2024 17:32:54  04/24/2024 03:32:54  krbtgt/AMINI.IR@AMINI.IR
        renew until 04/24/2024 17:32:47
```

دریافت تیکت در ماشین in

میتوانیم در سرویس ssh از Kerberos برای احرازهویت استفاده کنیم.

برای این منظور نیازمند یک principal به نام host/out برای سرور هستیم. بعد از ساخت ، به وسیله دستورات زیر در ماشین out فایل keytab آن را ذخیره میکنیم.

- sudo ktutil
- addent -password -p host/out -k 1 -e aes256-cts-hmac-sha1-96
- wkt /etc/krb5.keytab

سپس فایل موجود در آدرس /etc/ssh/sshd_config را ویرایش کرده و خطوط زیر را اضافه میکنیم:

```
# Kerberos options
KerberosAuthentication yes
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes
#KerberosGetAFSToken no

# GSSAPI options
GSSAPIAuthentication yes
GSSAPIStrictAcceptorCheck yes
GSSAPIKeyExchange yes
```

با دستور زیر، سرور ssh را روی پورت 48اجرا میکنیم:

KRB5_TRACE=/tmp/ssh-krb5trace /sbin/sshd -D -d -p 48

```
hadi@out:~$ sudo KRB5_TRACE=/tmp/ssh-krb5trace /sbin/sshd -D -d -p 48
debug1: sshd version OpenSSH_8.2, OpenSSL 1.1.1f  31 Mar 2020
debug1: private host key #0: ssh-rsa SHA256:gKgcV8yLVq5YS54hI4L4gC+ucRPgHSm9nw5vJtAEqmo
debug1: private host key #1: ecdsa-sha2-nistp256 SHA256:QkgoEFCEHMy7ZOZPrpMU7IJZWkiAU6/erpcnAR7CEP0
debug1: private host key #2: ssh-ed25519 SHA256:+kOFxM4T5OckeBJBerS69mTORJkQtu+Og7JxdzTl1i8
debug1: rexec_argv[0]='/sbin/sshd'
debug1: rexec_argv[1]='-D'
debug1: rexec_argv[2]='-d'
debug1: rexec_argv[3]='-p'
debug1: rexec_argv[4]='48'
debug1: Set /proc/self/oom_score_adj from 0 to -1000
debug1: Bind to port 48 on 0.0.0.0.
Server listening on 0.0.0.0 port 48.
debug1: Bind to port 48 on ::.
Server listening on :: port 48.
```

سپس در ماشین in ، با بلیط دریافت میکنیم:

```
root@in:/home/hadi# kinit kambiz@AMINI.IR
Password for kambiz@AMINI.IR:
root@in:/home/hadi# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: kambiz@AMINI.IR

Valid starting       Expires              Service principal
04/23/2024 18:03:50  04/24/2024 04:03:50  krbtgt/AMINI.IR@AMINI.IR
        renew until 04/24/2024 18:03:47
```

با دستور زیر به ماشین out درخواست میدهیم:

ssh kambiz@out -p 48

```
Starting session: shell on pts/0 for kambiz from 192.168.100.2 port 54434 id 0
debug1: Setting controlling tty using TIOCSCTTY.
```

با توجه به دارا بودن بلیط، احراز هویت موفق است و نیازی به ورود پسورد نیست.

```
 * Introducing Expanded Security Maintenance for Applications.
   Receive updates to over 25,000 software packages with your
   Ubuntu Pro subscription. Free for personal use.

     https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection
or proxy settings


Last login: Tue Apr 23 18:00:57 2024 from 192.168.100.2
Environment:
  LANG=en_US.UTF-8
  USER=kambiz
  LOGNAME=kambiz
  HOME=/home/kambiz
  PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/sna
p/bin
  SHELL=/bin/bash
  TERM=linux
  MOTD_SHOWN=pam
  SSH_CLIENT=192.168.100.2 49480 48
  SSH_CONNECTION=192.168.100.2 49480 192.168.101.2 48
  SSH_TTY=/dev/pts/0
kambiz@out:~$
```