Лабораторна робота

Автентифікація LDAP +Kerberos

Для виконання завдань роботи потрібні такі пакети Linux:
ldapscripts, ***slapd***, ***ldap-auth-config***, *ldap-auth-client, ldap-utils,* ***krb5-kdc, krb5-admin-server****, krb5-config,* ***krb5-pkinit***, ***krb5-kdc-ldap,*** *krb5-user, krb5-locales,* ***libpam-krb5****, libldap-x.x-x, libnss-ldap, libpam-ldap, libgssapi-krb5-2, libkrb5-26-heimdal, libkrb5-3, libkrb5support*

Відсутні пакети можна встановити командою *apt-get install*

#sudo apt-get install ldapscripts

Попередньо у встановленому дистрибутиві оновити базу пакетів

#sudo apt-get update -y

* Виділені пакети потрібно встановити, інші при цьому будуть встановлені автоматично.
* Завдання роботи протестовано на дистрибутивах Ubuntu 14.04, 16.04 та 20.04.

ВАЖЛИВО: У наступних завданнях ви маєте персоналізувати ім`я домена - замість *testdomain.com* і *myhost.testdomain.com* використовуйте унікальне ім'я домена (наприклад, прізвисько) і унікальне ім'я хоста (наприклад, ваше ім'я :).

Client та Server мають бути в одній мережі (або Host-only Networking для VM).

1.1 Ознайомтесь с документацією про LDAP:

https://openldap.org/doc/
https://ubuntu.com/server/docs/service-ldap-introduction

1.2 В файлах */etc/hostname* хостів клієнта та сервера встановіть адреси *myhost.testdomain.com* та *kdc.testdomain.com*

Задайте змінну оточення *HOSTNAME.*

#export HOSTNAME=myhost.testdomain.com

та в файл */etc/environment* додайте строку

HOSTNAME=”myhost.testdomain.com”

1.3 Налаштуйте систему DNS або встановіть у файлах */etc/hosts* клієнта і сервера відповідність між IP-адресами і доменними іменами, наприклад:
192.168.29.176 kdc.testdomain.com kdc
192.168.29.177 myhost.testdomain.com myhost

1.4 На хостах клієнта і сервера встановіть однаковий час (або сінхронізуйте за протоколом NTP):
#*date* [*MMDDhhmmCCYY*]
#*date*

*Протокол Kerberos, за замовчуванням, допускає розбіжність між годинниками сторін Kerberos не більше 5 хвилин.

2. Налаштування LDAP

2.1 Налаштування LDAP-сервера:

Запустіть утиліту налаштування LDAP - сервера і дайте відповідь на питання:
#*sudo dpkg-reconfigure slapd*

Omit OpenLDAP server configuration: No
DNS domain name: testdomain.com
Organization name: testdomain
Administrator Password: P@ssw0rd
Database backend to use: HDB
Remove the database when slapd is purged: No
Move old database: Yes
Allow LDAPv2 protocol: No

Після цього сервер має запуститись.

Перевірте можливість анонімного підключення:
#*ldapwhoami -H ldap:// -x*
=>> anonymous

Щоб запустити (перезапустити) LDAP сервер:
#*service slapd* [*start*|*restart*]

* При перенесенні віртуальної машини або зміні IP адрес вам доведеться перезапустити сервіси LDAP (*slapd*) і Kerberos (*krb5-kdc*).

2.2 Налаштування LDAP-клієнта:

В файлах */etc/ldap.conf* клієнта та сервера вкажіть наступні параметри:
Файл */etc/ldap.conf*:

host 192.168.29.176
base dc=testdomain,dc=com
binddn cn=admin,dc=testdomain,dc=com
bindpw P@ssw0rd
#rootbinddn cn=manager,dc=testdomain,dc=com //закоментуйте дану строку

2.3 Структура каталога

Нехай файл *ldap_top* містить опис структури каталога в ldif-форматі:

Файл *ldap_top*:

#dn: dc=testdomain, dc=com
#objectclass: top
#objectclass: organization
#o: testdomain

dn: ou=Group, dc=testdomain, dc=com
objectclass: top
objectclass: organizationalUnit
ou: Group

dn: ou=People, dc=testdomain, dc=com
objectclass: top
objectclass: organizationalUnit
ou: People

dn: cn=users, ou=Group, dc=testdomain, dc=com
objectclass: posixGroup
objectclass: top
cn: users
gidNumber: 100

Імпортуйте дану структуру в каталог:
#ldapadd -f ./ldap_top -D "cn=admin, dc=testdomain,dc=com" -w P@ssw0rd -v -x

2.4 Щоб додати облікові записи нових користувачів до LDAP-каталога, використовуйте команду:
#ldapadd -f ./ldap_user -D "cn=admin, dc=testdomain,dc=com" -w P@ssw0rd -v -x

В файлі *ldap_user* наведен приклад облікового запису користувача:

Файл *ldap_user*:

dn: uid=bublic, ou=People, dc=testdomain, dc=com
uid: bublic
cn: Bublic The Dog
objectclass: account
objectclass: posixAccount
objectclass: top
objectclass: shadowAccount
userPassword: {crypt}1zrCksfCH$mTg61xzuAwjscKq.zVOwk1
uidNumber: 1102
gidNumber: 100
loginShell: /bin/bash
homeDirectory: /home/bublic

Додайте ще декілька облікових записів користувачів.

*Для обчисления гешу пароля використовуйте утиліту *slappasswd*.
(щоб геш пароля був застосовний для входу в Linux, він має бути сумісний за форматом з гешами, що зберігаються у файлі */etc/shadow*).
*Для заміни пароля облікового запису ч-з LDAP використовуйте утиліту *ldappasswd.*

2.5 Перевірте наявність тестових записів в каталозі:
ldapsearch -b "dc=testdomain,dc=com" "uid=bublic" -v -x

----приклад виведення----
ldap_initialize(<DEFAULT>)
filter: uid=bublic
requesting: ALL
version: 2

#
 # filter: uid=bublic
 # requesting: ALL
#

 # bublic, People, testdomain, com
dn: uid=bublic, ou=People, o=testdomain, c=com
uid: bublic

cn: Bublic The Dog
objectClass: account
objectClass: posixAccount
objectClass: top
objectClass: shadowAccount
userPassword::
e2NyeXB0fSQxJHpyQ2tzZkNIJG1UZzYxeHp1QXdqc2NLcS56Vk93azE=
uidNumber: 1102
gidNumber: 100
loginShell: /bin/bash
homeDirectory: /home/bublic

 # search result
search: 2
result: 0 Success

 # numResponses: 2
 # numEntries: 1

2.6 Протестуйте роботу таких команд:

ldapsearch -h 192.168.29.176 -b "dc=testdomain,dc=com" "uid=" -v -x*
ldapsearch -h 192.168.29.176 -b "dc=testdomain,dc=com" "uid=user" dn cn -v -x*
ldapsearch -h 192.168.29.176 -b "dc=testdomain,dc=com" "(&(uid=user) (gidNumber=100))" dn cn -v -x*

ldappasswd -h 192.168.29.176 -D "cn=admin,dc=testdomain,dc=com" -s P@ssw0rt -v -w P@ssword -x "uid=bublic,ou=People,dc=testdomain,dc=com"
ldappasswd -h 192.168.29.176 -D "uid=bublic,ou=People,dc=testdomain,dc=com" -s userP@ss -v -w P@sswort -x

2.7 Утилітою LDAP Admin (https://www.ldapadmin.org/download/ldapadmin.html) підключіться до LDAP-сервера.
Вкажіть адресу хоста, Base "*dc=testdomain, dc=com*", "Simple authentication", Username "*cn=admin,dc=testdomain, dc=com*" та пароль облікового запису (*P@ssw0rd*).

Перевірте можливості утиліти адміністрування і опис схеми каталогу.
Послуговуючись LDAP Admin, зручно встановлювати або змінювати паролі користувачів. З форматом файлу /etc/shadow Linux у LDAP Admin сумісні функції MD5 Crypt, SHA-256 Crypt та SHA-512 Crypt.
Для додавання користувачів і зміни паролів в подальшому використовуйте LDAP Admin.

3. PAM - модулі

3.1 Ознайомтеся з документацією щодо модулів автентифікації (PAM, Pluggable Authentication Module):
https://manpages.ubuntu.com/manpages/bionic/man7/pam.7.html
https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/system-level_authentication_guide/pluggable_authentication_modules

* Слід зауважити, що якщо зовнішній сервер автентифікації не буде доступний, то користувач можливо не зможе увійти у систему. Тому, під час налаштування PAM, рекомендується залишати можливість автентифікації за допомогою локальних облікових записів хоча б з метою адміністрування у разі недоступності сервера автентифікації.

3.2 Наштування бібліотеки *nsswitch*:

В файлі */etc/nsswitch.conf* в строках *passwd, shadow* и *group* додайте "*ldap*"
Файл */etc/nsswitch.conf:*
passwd: compat ldap
group: compat ldap
shadow: compat ldap

3.3 Використовуючи створені в 2.4 облікові записи користувачів, спробуйте увійти в клієнтську систему (VM Client). Поексперементуйте з декількома обліковими записами користувача і поясніть результати.

3.4 Послуговуючись *tcpdump* запишіть різні запити до LDAP-сервера (Додавання користувача, пошук, зміна пароля, процедура автентифікації) і дослідіть їх в *wireshark*.

* У наведеній конфігурації LDAP передає дані у відкритому вигляді.
Для захисту сеансу LDAP в реальних умовах використовуйте TLS (STLS).

4. Протокол Kerberos

4.1 Ознайомтесь с документацією стосовно протоколу Kerberos:
https://kerberos.org/docs/index.html
https://web.mit.edu/kerberos/krb5-latest/doc/
https://ubuntu.com/server/docs/kerberos-introduction

* У прикладі використовується доменне ім'я хоста *myhost.testdomain.com*.
* Зверніть увагу, що Kerberos розрізняє рядкові і великі літери.

Тому, для розрізнення, ім'я домену буде позначатися рядковими літерами (*testdomain.com*), а область (realm) Kerberos - великими (*TESTDOMAIN.COM*).

4.2 Налаштування Kerberos

В файлах */etc/krb5kdc/kdc.conf* (налаштування сервера Kerberos) та */etc/krb5.conf* (налаштування клієнта Kerberos) заменіть *example.com* та *EXAMPLE.COM* на вибране ім`я домена та ім`я області Kerberos.

У файлі налаштування Kerberos KDC */etc/krb5kdc/kdc.conf* заменіть ім`я домену на *TESTDOMAIN.COM*

Файл */etc/krb5.conf* налаштування Kerberos-клієнта на VM Client та VM Server:
default_realm = TESTDOMAIN.COM
[realms]
TESTDOMAIN.COM = {
kdc = 192.168.29.176
admin_server = 192.168.29.176
}

4.3 Створіть KDC principal database (при цьому вкажіть Master Password для цієї області (realm):

#kdb5_util create -s //створення області Kerberos (realm)

4.4 Запустіть KDC:
#service krb5-kdc start

4.5 Послуговуючись утилітою *kadmin.local,* створіть декілька Kerberos principals (облікові записи Kerberos)
*Враховуйте, що для автентифікації Kerberos+LDAP для створених в Kerberos облікових записів мають існувати відповідні облікові записи в каталозі LDAP.

 # kadmin.local [-m]
kadmin.local: addpol users
kadmin.local: ank -policy users user1
kadmin.local: quit

Перевірте, які облікові записи існують в даній Kerberos-області (realm) та їх характеристики:

 # kadmin.local [-m]
kadmin.local: get_principals
kadmin.local: getprinc user1
kadmin.local: quit

4.6 Перевірте автентифікацію Kerberos (чи взмозі поточний користувач отримати TGT):

#kinit <principal>
#klist
#kdestroy
#klist

4.7 Запустіть сервіс адміністрування Kerberos:

#kadmind [-m]

та перевірте його роботу:

#kadmin
kadmin: listprincs
kadmin: quit

4.8 Налаштування PAM для Kerberos автентифікації в системі.

Якщо у вас встановлені всі пакети, що вказано в початку завдання, то, скоріш за все, налаштування модулів PAM було проведено автоматично. Перевірте, що файли *common-account*, *common-auth*, *common-password*, *common-session* та *common-session-noninteractive* в каталозі */etc/pam.d/* вже мають незакоментовані посилання на модулі *pam_ldap.so* та *pam_krb5.so*. За вибір модулів автентифікації відповідає утиліта *pam-auth-update*. Запустіть її, впевніться, що Kerberos та LDAP автентифікацію в системі активовано, та виберіть "*Create home directory on login*". Існує модуль PAM, що при автентифікації нового користувача створює для нього домашній каталог. Збережіть налаштування та перевірте, що змінилося в згаданих файлах каталогу */etc/pam.d/*.

4.9 Перевірте автентифікацію в системі по обліковим записам Kerberos і можливість зміни паролів (утиліті *passwd* та *kpasswd*).
*Для Kerberos-користувачів мають існувати записи в каталозі LDAP.

4.10 Використовуючи *tcpdump*, збережіть діалог спілкування з Kerberos сервером і перегляньте його в *wireshark*.

Kerberos, на відміну від LDAP, не вміє зберігати інформацію облікових записів, таку як *uidNumber, gidNumber, loginShell, homeDirectory,* тощо.
Тому як сховище облікових записів можуть використовуватися, наприклад, або локальні файли (*/etc/passwd*, */etc/shadow* та /*etc/group*) або сервіс LDAP.

Щоб перевірити, яку інформацію автентифікації знає система, введіть:
#*getent passwd*
#*getent shadow*
#*getent group*

У кінцевій конфігурації автентифікація здійснюється за допомогою Kerberos, а дані облікових записів беруться з локальних файлів, а при відсутності відповідних облікових записів - з LDAP каталогу.