Pràctica Kerberos

Curs 2019-2020

Authenticació Kerberos

Pràctica1

3 hores

Imatges Docker

edtasixm11/k19:kserver servidor kerberos detach. Crea els principals pere(kpere) pau(kpau, rol: admin), jordi(kjordi), anna (kanna), marta (kmarta), marta/admin (kmarta rol:admin), julia (kjulia) i admin (kadmin rol:admin). Crear també els principals

kuser01...kuser06 amb passwd (kuser01...kuser06). Assignar-li el nom de host: *kserver.edt.org*.

edtasixm11/k19:khost host client de kerberos. Simplement amb eines kinit, klist i kdestroy (no pam). El servidor al que contacta s'ha de dir *kserver.edt.org*. Cal verificar el funcionament de kadmin.

Authenticació

edtasixm11/k19:khostp host amb PAM de kerberos. El servidor al que contacta s'ha de dir *kserver.edt.org*. Aquest host configura el *system-auth* de pam per usar el mòdul *pam_krb5.so*. Crear els usuris local01..local06 (idem nom de passwd) i kuser01..kuser06 (sense passwd). Aquest host utlitza /etc/passwd de IP Information Provider i valida usuaris locals local01... amb pam_unix.so (on /etc/passwd fa de IP i AP) i usuaris locals+principals kuser01... (on /etc/passwd fa de IP i kerberos de AP Authentication Provider).

Verificació:

En una sessió interactiva en el container khostp iniciar amb “su -” sessió com a local01, convertr-se en altre cop amb “su -” en local02 i finalment convertir-se en kuser01. Validar que kuser01 obté un ticket i que pot accedir amb kadmin a l’administració del servidor kerberos (amb independència dels permisos que tingui).

Instal·lació

Eliminar del vostre host físic les particions sda2, sda3 i sda4. Crear una partició sda2 de 8GB. Instal·lar-hi Fedora-27 amb una instal·lació **MINIMAL**.
Refer el GRUB deixant per defecte la partició matí, les etiquetes MATI, TARDA i HISX2-LAB. Cal que el grub que mani (i el fitxer grub.conf) sigui el del matí.

Engegar la màquina a la partició matí (sda5)

Fer:

- # cp /boot/grub2/grub.cfg /boot/grub2/grub.hisx2
- # grub2-mkconfig > /boot/grub2/grub.cfg
- # vim /boot/grub2/grub.cfg (veure què cal modificar)
- # grub2-install /dev/sda

Cal modificar:

- set timeout=-1
- set default=0 (o el número corresponent a l'entrada del matí, comencen per zero)
- MATI (posem aquesta etiqueta a la partició matí sda5)
- TARDA (posem aquesta etiqueta a la partició tarda sda6)
- HISX2-LAB (posem aquesta etiqueta a la partició de treball hisx2 sda2)

Pràctica2

2 hores

Host aula + Kerberos + AWS EC2

Usarem un host real de l'aula, la partició on hem instal·lat un Fedora 27 MINIMAL. Cal configurar la autenticació dels usuaris utilitzant Unix i Kerberos. El servidor kserver.edt.org estarà desplegat a AWS EC2.

Caldrà configurar una AMI a AWS EC2 amb docker i executar el kserver fent un mapping dels ports de kerberos al host de Amazon AWS EC2. També caldrà configurar el firewall. Per fer-ho crearem un *Security groups* propi anomenat *kerberos* que obri els ports del firewall per poder accedir des de l'exterior al kerberos i al ssh. Identifica els ports i de quin tipus són.

Penseu en tot el què cal configurar en el host de l'aula.

Pràctica3

Kerberos + LDAP (PAM)

Farem un nou container host client de kerberos i de ldap per verificar que sabem fer un muntatge equivalent al de l'escola. En aquest esquema usem dos containers servidors, un de kerberos i un de ldap (ja els tenim fets). Cal crear el container host client que es descriu a continuació.

edtasixm11/k19:khostpl (khost-pam-ldap) host amb PAM amb autenticació AP de kerberos i IP de ldap. El servidor kerberos al que contacta s'ha de dir *kserver.edt.org*. El servidor ldap s'anomena ldap.edt.org. Aquest host es configura amb *authconfig* (us ajudarà saber que és una configuració mimètica a la que fem en realitzar la instal·lació de les aules)..

Verificar en el host client l'autenticació d'usuaris locals i usuaris globals (ldap+kerberos).
En el host client hi ha usuaris locals (local01…) usuaris locals amb passwd al kerberos (kuser01, etc que en realitat podem eliminar o ignorar) i usuaris de ldap (pere…, user1…). Aquests usuaris cal que tinguin password al kerberos (tipus kpere, kuser01, etc).

Host Aula + Kerberos + LDAP

Configurar el host de l'aula amb Fedora-27-Minimal per tal de permetre l'autenticació d'usuaris locals amb pam_unix.so i usuaris globals kerberos+ldap. Cal utilitzar *authconfig*. Verificar l'accés d'usuaris locals local01,etc i d'usuaris globals pere, user01, etc.

nota: no confongueu els usuaris de ldap user01 amb els de ‘mentida’ que vam crear localment al lclient anomenats kuser01.

Seveis Kerberitzats

Pràctica 4

Servei SSH Kerberitzat

edtasixm11/k19:sshd Servidor SSHD *kerberitzat*. Servidor ssh que permet l'accés d'usuaris locals i usuaris locals amb autenticació kerberos. El servidor s'ha de dir *sshd.edt.org*.

Primera versió simple (podem usar de base k19:khost) d'un host amb usuaris locals (local01…) i usuaris locals amb passwd al kerberos (kuser01…). A aquest host li afegim el servei ssh per convertir-se en un servidor SSH Kerberitzat. Ha de permetre l'accés tant a usuaris locals (local01) com a usuaris kerberos (kuser01).

El model de funcionament és disposar de un host client de kerberos, per exemple k19:khost i aquest servidor sshd kerberitzat. En el client un usuari 'qualsevol' es pot connectar i iniciar sessió al servidor SSH com a usuari destí local (local01).

En el client un usuari que disposi de ticket kerberos (per exemple kuser01) pot iniciar sessió remota al servidor ssh com a usuari kuser01 automàticament, ja que disposa de les credencials kerberos (similar a iniciar sessió desatesa amb claus pública/privada).

Pràctica 5

edtasixm11/k19:sshdpl (sshd-pam-kerberos-ldap) Servidor SSH amb PAM amb autenticació AP de kerberos i IP de ldap. El servidor kerberos al que contacta s'ha de dir *kserver.edt.org*. El servidor ldap s'anomena ldap.edt.org. Aquest host es configura amb authconfig . S'ha generat partint del host edtasixm11/k19:khostpl i se li ha afegit la part del servidor sshd. Conté els fitxers per poder activar el mount del home samba, però no s'ha configurat.

edtasixm11/k19:sshdpls (sshd-pam-kerberos-ldap-home-samba) Servidor SSH amb PAM (kerberos+ldap) que munta els homes dels usuaris (dins del home) via samba.

Volumes / Entrypoint / Scripts

Pràctica 6

Volumes
Desar la base de dades en un volum anomenat *krb5-data* de manera que les dades de kerberos siguin perdurables. Practiqueu amb kadmin des del client i amb un compte d'administració crear, modificar, esborrar i llistar principals (manteniu els per defecte).

Practiqueu a assignar permisos diferents als usuaris, en especial el de poder llistar els principals.

Entrypoint
Modificar l'script startup.sh per actuar com a entrypoint amb els següents arguments possibles:

- *res*: engegar el servei kerberos usant la base de dades existent actualment (el volum).
- *Initdb*: inicialitza la base de dades.¡ i engega el servei.
- *initdbedt*: inicialitza la base de dades de kerberos amb els principals per defecte i engega el servei.
- *kadmin*: executa kadmin-local passanli la resta de parametres.

Volumnes
La base de dades ldap es desa en un volum anomenat *ldap-data*.

Entrypoint ldap
Modificar la imatge ldapserver:latest (*ldapserver:entrypoint*) de manera que tingui un script startup.sh de entrypoint que permety inicialitzar la base de dades ldap i engegar-la (*initdb*), initiclitzar amb dades i engegar-la (*initdbedt*) o simplement engegar el servei ldap (res). Qualsevol altre acció que es passi s'executarà usant eval.

Entrypoint kserver
Ampliar l'script d'administració startup.sh del keserver de manera que contingui les opcions:

- *useradd*: rep les dades necessaries per crear un principal i una entrada d'usuari ldap.
- *userdel*: rep les dades necessaries per eliminar un usuari (principal i entrada ldap).
- *list*: llista els principals.

Samba
edtasixm11/k19:khostpls (khost-pam-ldap-samba) Conté els fitxers per activar el mount del home samba, que munta els homes dels usuaris (dins del home) via samba. Caldrà

crear un volum amb els homes dels usuaris. Primer el farem manualment hardcoded i després amb un script de creació.

Teoria

Autenticaction Provider AP

Kerberos proporciona el servei de proveïdor d'autenticació. No emmagatzema informació dels comptes d'usuari com el uid, git, shell, etc. Simplement emmagatzema i gestiona els passwords dels usuaris, en entrades anomenades *principals* en la seva base de dades.

Coneixem els següents AP:

- */etc/passwd* que conté els password (AP) i també la informació dels comptes d'usuari (IP).
- *ldap* el servei de directori ldap conté informació dels comptes d'usuari (IP) i també els seus passwords (AP).
- *kerberos* que únicament actua de AP i no de IP.

Information Provider IP

Els serveis que emmagatzemen la informació dels comptes d'usuari s'anomenen Information providers. Aquests serveis proporcionen el uid, gid, shell, gecos, etc. Els clàssics són /etc/passwd i ldap.

Model de pràctiques

El model que mantindrem a tot el mòdul ASIX M11-SAD és el següent:

- **ldap** al servidor ldap tenim els usuaris habituals pere, marta, anna, julia, pau, jordi. El seu password és el seu propi nom.

- **/etc/passwd** en els containers hi ha els usuaris locals local01, local02 i local03 que tenen assignat com a password el seu mateix nom.

- **kerberos + IP** els usuaris kuser01, kuser02 i kuser03 són principals de kerberos amb passwords tipus kuser01, kuser02 i kuser03. La informació del seu compte d'usuari és local al */etc/passwd* on **no** tenen password assignat.

- **kerberos + ldap** Al servidor kerberos hi ha també principals per als usuaris usuals ldap pere, marta, anna, julia, jordi i pau. Els seus passwords són del tipus kpere, kmarta, kanna, kjulia, kjordi i kpau.

Es resum, podem verificar l'accés/autenticació d'usuaris locals usant el prototipus *local01*, podem fer test de la connectivitat kerberos amb comptes locals amb usuaris tipus *kuser01*. I

finalment podem verificar l'autenticació d'usuaris kerberos amb ldap (fent de IP) amb els clàssics pere (kpere).