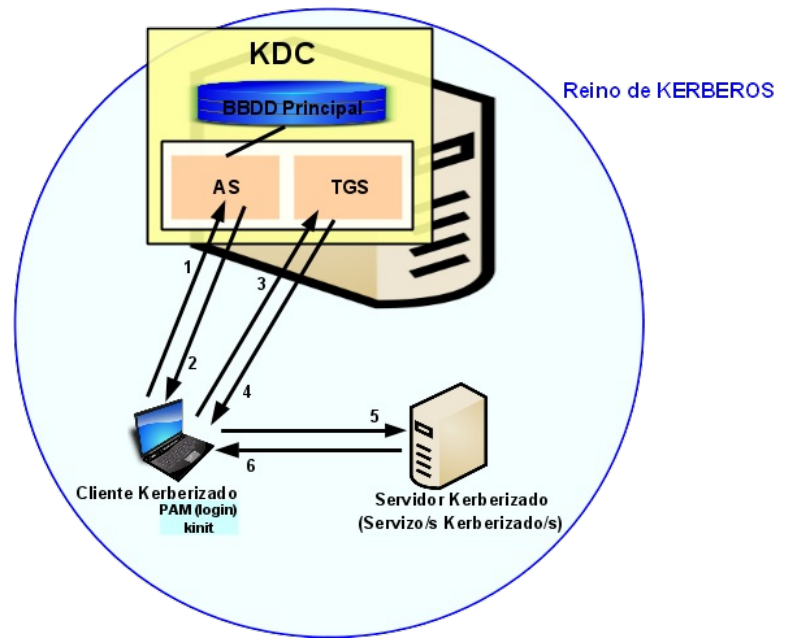


Kerberos (autenticación, SSO, cifrado simétrico, KDC)



Kerberos MIT

Kerberos Heimdal

Official documentation Ubuntu Kerberos

kadmin
Comando para administrar Kerberos de forma local ou remota

krb5-config
Comando para configuración

/etc/krb5.conf
Ficheiro de configuración

kinit
Comando que permite solicitar un ticket TGT tras verificación de autenticación do usuario que procesa a solicitude.

KDC: Key Distribution Center → Emite tickets Kerberos

Ticket: Credenciais electrónicas temporais que verifican a identidade dun cliente para un servizo particular

BBDD Principal: Base de datos de usuarios do KDC ≠ /etc/passwd

AS: Authentication Server → Emite tickets de acceso TGT para gañar acceso ao servidor TGS, é dicir, encárgase de validar ao usuario fronte ao sistema substituíndo ao login clásico

TGS: Ticket Granting Server → Emite tickets para un servizo desexado, os cales son entregados aos usuarios para que poidan acceder ao servizo

TGT: Ticket especial que permite ao cliente obter tickets sen solicitalos dende o KDC

Cliente Kerberizado (PAM(login), kinit ...)

Servidor Kerberizado (Servizo/s Kerberizado/s)

Key: Chave → Datos usados cando ciframos ou desciframos datos. Non se pode descifrar os datos cifrados sen a chave correcta

Reino de Kerberos (Realm): Rede que usa Kerberos, composto por un ou varios servidores KDCs e un número potencial de clientes. O nome do reino de Kerberos para o KDC de Microsoft é o nome do controlador de dominio en MAIÚSCULAS, por exemplo: EDUCACION.LOCAL . Un cliente en Kerberos identifícase co seu principal

Principal (nome do principal): É o nome único do usuario ou servizo que pode autenticar mediante o uso de Kerberos.

Formato: name[/instance]@REALM

→ **name** para os usuarios é o mesmo que o ID de inicio de sesión, por exemplo root

→ **instance** pode ser opcional no caso dos usuarios pero é obrigatorio para os servizos, por exemplo: alumno, alumno/admin, alumno/host1.educacion.local

→ **REALM** é o nome do reino de Kerberos, por exemplo EDUCACION.LOCAL . Todos os principais dun reino teñen a súa propia chave, sendo para os usuarios derivada do seu contrasinal e para os servizos xerada aleatoriamente.

Keytab: Para os servizos dun host é similar ao contrasinal dun usuario. Cada host que proporciona un servizo debe ter un arquivo local keytab, que contén o principal para o servizo en cuestión, o cal denomínase clave de servizo.

NOMENCLATURA KERBEROS

KERBEROS

Kerberos proporciona autenticación SSO (Single Sing-On), de xeito que un usuario soamente ten que autenticarse unha vez en cada sesión e pode facer uso de esta autenticación para tódolos servizos e equipos do reino de Kerberos.

Kerberos permite:

- Ao cliente probar a súa identidade ante un servidor
- Ao servidor probar a súa identidade fronte aos clientes
- Unha vez autenticados, cifrar a comunicación
- Que en ningún momento o contrasinal do usuario sexa enviado por rede
- Que os contrasinais dos usuarios non estén almacenados nos equipos clientes
- Que os contrasinais dos usuarios estén almacenados cifrados no KDC, na BBDD Principal
- Que os tickets soamente poden usarse durante un tempo limitado. Debido a isto é necesario a sincronización temporal do KDC, cliente e servidores kerberizados.

Microsoft Active Directory emprega Kerberos como mecanismo de seguridade predeterminado. Cando se engaden usuarios a Microsoft Active Directory, a súa identificación de Windows é equivalente a un nome principal Kerberos.

IMPORTANTE:

- **Active directory** → Non distingue entre maiúsculas e minúsculas os nomes dos servizos
- **Kerberos** → Distingue entre maiúsculas e minúsculas os nomes dos servizos
- **Convencións::**
 - Os reinos de Kerberos e os dominios de Active Directory están escritos con maiúscula.
 - Os nomes de host escríbense en minúscula.
 - As buscas de bases de datos distinguen entre maiúsculas e minúsculas.

EXPLICACIÓN PROTOCOLO KERBEROS

Autenticación en 3 fases:

Fase 1: Pasos 1 e 2. Autenticación de usuario

Fase 2: Pasos 3 e 4. Autorización de tipo de servizo

Fase 3: Pasos 5 e 6. Autorización dun servidor

A **Fase 1** soamente ten lugar unha vez, sendo a **Fase 2** e a **Fase 3** as que se repiten para acceder a múltiples servizos kerberizados.

- **Paso 1:** O usuario introduce credenciais (PAM(login, su ...) no cliente e envía o principal ao servizo AS do servidor KDC.
- **Paso 2:** O servizo AS do KDC verifica as credenciais na BBDD Principal e logo de autenticar envía ao cliente un TGT.
- **Paso 3:** O cliente quere acceder a un servizo polo que envía o TGT ao TGS do KDC.
- **Paso 4:** O TGS verifica o TGT e envía un ticket de servizo para o servizo ou aplicación destino.
- **Paso 5:** O cliente envía o ticket de servizo ao servizo kerberizado para a súa autenticación.
- **Paso 6:** Se o servizo kerberizado acepta o ticket establécese un contexto de seguridade e entón a aplicación do usuario pode intercambiar datos co servizo destino.

Finalmente, o cliente autenticouse (usuario/contrasinal) contra a BBDD Principal (Base de datos de usuarios do KDC ≠ /etc/passwd) → o cliente conta durante un período de tempo con un ticket TGT que permitira acceder a múltiples servizos kerberizados.

ESCENARIO

Máquinas virtuais:

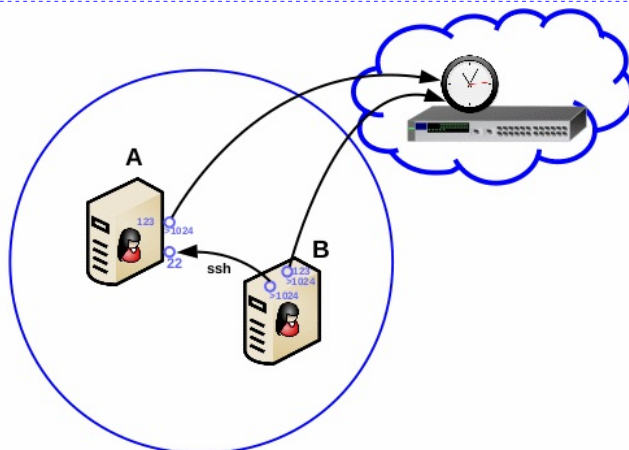
RAM ≤ 2048MB CPU ≤ 2 PAE/NX habilitado
Rede: 192.168.120.0

Máquina virtual A:

Rede Interna e NAT
Servidor Kerberos: heimdal-kdc
Servidor SSH: openssh-server
Servizo NTP: ntp
ISO: Kali Live amd64
IP/MS: 192.168.120.100/24
BIOS: Permite arranque dispositivo extraíble: CD/DVD, USB

Máquina virtual B:

Rede Interna e NAT
Cliente Kerberos: heimdal-clients
Cliente SSH: openssh-client (ssh)
Servizo NTP: ntp
ISO: Kali Live amd64
IP/MS: 192.168.120.101/24



Máquina virtual A: Kali amd64

1. Na contorna gráfica abrir un terminal e executar:

```
kali@kali:~$ setxkbmap es #Cambiar o mapa de teclado ao idioma español.  
kali@kali:~$ passwd kali #Cambiar o contrasinal do usuario kali. Por como contrasinal abc123. (Ollo que o contrasinal ten un caracter punto final).
```

2. Cambiar hostname da máquina virtual A. Por kaliA como hostname:

```
kali@kali:~$ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co comando sudo (/etc/sudoers, visudo)  
root@kali:~# echo 'kaliA' > /etc/hostname #Indicar ao sistema o valor do hostname.  
root@kali:~# echo 'kernel.hostname=kaliA' >> /etc/sysctl.conf #Indicar ao kernel o valor do hostname.  
root@kali:~# sysctl -p #Activar o cambio de hostname sen ter que pechar sesión nin reiniciar  
root@kali:~# exit #Saír da consola local sudo na que estabamos a traballar para voltar á consola local de kali.  
kali@kali:~$ exit #Pechar o terminal saíndo da consola local do usuario kali.
```

3. Configurar a rede:

Na contorna gráfica abrir un terminal e executar:

```
kali@kaliA:~$ setxkbmap es #Cambiar o mapa de teclado ao idioma español.  
kali@kaliA:~$ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co comando sudo (/etc/sudoers, visudo)  
root@kaliA:~# /etc/init.d/avahi-daemon stop #Parar o demo avahi-daemon(control resolución de nomes) para poder configurar de forma manual a configuración de rede e non ter conflito con este demo.  
root@kaliA:~# /etc/init.d/network-manager stop || pkill NetworkManager #Parar o demo network-manager(xestor de rede) ou o script NetworkManager (executado sen ser demo) para poder configurar de forma manual a configuración de rede e non ter conflito con este xestor.  
root@kaliA:~# ip addr show #Amosar a configuración de todas as tarxetas de rede. Nesta caso, na máquina A, as tarxetas de redes: loopback(lo) e interna(eth0).  
root@kaliA:~# ip addr add 192.168.120.100/24 dev eth0 #Configurar a tarxeta de rede interna eth0, coa IP: 192.168.120.100 e máscara de subrede: 255.255.255.0.  
root@kaliA:~# ip addr show #Amosar a configuración de todas as tarxetas de rede. Nesta caso, na máquina A, as tarxetas de redes: loopback(lo) e interna(eth0).  
root@kaliA:~# ping -c4 192.168.120.100 #Comprobar mediante o comando ping a conectividade coa interface de rede local eth0
```

4. Comprobar estado do Servidor SSH:

```
root@kaliA:~# /etc/init.d/ssh status #Comprobar o estado do servidor SSH, por defecto non está arrancado.  
root@kaliA:~# nc -vz localhost 22 #Mediante o comando nc(netcat) comprobar se o porto 22 do servidor ssh está en estado escoita(listen), esperando conexións. A opción -v corresponde á opción verbose, o que permite amosar información máis detallada na saída do comando. A opción -z permite devolver PROMPT do sistema e de igual xeito facer o escaneo ao/s porto/s solicitados. O número 22 é o porto TCP a escanear.  
root@kaliA:~# nc -vz 192.168.120.100 22 #Mediante o comando nc(netcat) comprobar se o porto 22 do servidor ssh está en estado escoita(listen), esperando conexións. A opción -v corresponde á opción verbose, o que permite amosar información máis detallada na saída do comando. A opción -z permite devolver PROMPT do sistema e de igual xeito facer o escaneo ao/s porto/s solicitados. O número 22 é o porto TCP a escanear.  
root@kaliA:~# netstat -natp | grep 22 #Mediante o comando netstat comprobar que o porto 22 do servidor SSH está en estado escoita(listen), esperando conexións. A opción -n permite non resolver nomes amosando así soamente as IPs e o comando ser máis rápido na execución. A opción -a equivale á opción all o que permite amosar todos os sockets (conectores) á escoita no servidor. A opción -t equivale a tcp o que permite buscar soamente información sobre o protocolo TCP. A opción -p equivale a program e amosa o PID e nome do programa ao cal pertence o socket.  
root@kaliA:~# ss -natp | grep 22 #Mediante o comando ss comprobar que o porto 22 do servidor SSH está en estado escoita(listen), esperando conexións. A opción -n permite non resolver nomes amosando así soamente as IPs e o comando ser máis rápido na execución. A opción -a equivale á opción all o que permite amosar todos os sockets (conectores) á escoita no servidor. A opción -t equivale a tcp o que permite buscar soamente información sobre o protocolo TCP. A opción -p equivale a program e amosa o PID e nome do programa ao cal pertence o socket.  
root@kaliA:~# /etc/init.d/ssh start #Arrancar o servidor SSH.  
root@kaliA:~# /etc/init.d/ssh status #Comprobar o estado do servidor SSH, agora debe estar arrancado.  
root@kaliA:~# find /etc/rc* -name "*ssh*" #Busca polas links runlevels nos cartafolios /etc/rc*  
root@kaliA:~# systemctl enable ssh #Permite que o servizo ssh sexa iniciado no arranque xerando os links nos runlevels (/etc/rcX.d)  
root@kaliA:~# find /etc/rc* -name "*ssh*" #Busca polas links runlevels nos cartafolios /etc/rc*  
root@kaliA:~# systemctl is-enabled ssh.service #Amosa se o servizo ssh está enabled ou disabled  
root@kaliA:~# nc -vz 192.168.120.100 22 #Mediante o comando nc(netcat) comprobar se o porto 22 do servidor ssh está en estado escoita(listen), esperando conexións. A opción -v corresponde á opción verbose, o que permite amosar información máis detallada na saída do comando. A opción -z permite devolver PROMPT do sistema e de igual xeito facer o escaneo ao/s porto/s solicitados. O número 22 é o porto TCP a escanear.  
root@kaliA:~# ssh -v kali@localhost #Comprobar se o servidor SSH está activo e podemos conectarnos a el dende localhost co usuario kali e o seu contrasinal. Se é a primeira vez que nos conectamos o servidor avísanos se estamos de acordo coa autenticación. Respostamos yes e pulsamos Enter. A opción -v (modo verbose) aporta información máis detallada da conexión.  
kali@kaliA:~$ exit #Saír da consola remota ssh a que acabamos de acceder, para voltar á consola local de root.  
root@kaliA:~# exit #Saír da consola local sudo na que estabamos a traballar para voltar á consola local de kali.  
kali@kaliA:~$
```

Máquina virtual B: Kali amd64

1. Configuración da rede. Na contorna gráfica abrir un terminal e executar:

```
kali@kali:~$ setxkbmap es #Cambiar o mapa de teclado ao idioma español.
```

```
kali@kali:~$ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co comando sudo (/etc/sudoers, visudo)
root@kali:~# /etc/init.d/avahi-daemon stop #Parar o demo avahi-daemon(control resolución de nomes) para poder configurar de forma manual a configuración de rede e non ter conflito con este demo.
```

```
root@kali:~# /etc/init.d/network-manager stop || pkill NetworkManager #Parar o demo network-manager(xestor de rede) ou o script NetworkManager (executado sen ser demo) para poder configurar de forma manual a configuración de rede e non ter conflito con este xestor.
```

```
root@kali:~# ip addr show #Amosar a configuración de todas as tarxetas de rede. Nesta caso, na máquina B as tarxetas de redes: loopback(lo) e interna(eth0).
```

```
root@kali:~# ip addr add 192.168.120.101/24 dev eth0 #Configurar a tarxeta de rede interna eth0, coa IP: 192.168.120.101 e máscara de subrede: 255.255.255.0.
```

```
root@kali:~# ip addr show #Amosar a configuración de todas as tarxetas de rede. Nesta caso, na máquina B as tarxetas de redes: loopback(lo) e interna(eth0).
```

```
root@kali:~# ping -c4 192.168.120.101 #Comprobar mediante o comando ping a conectividade coa interface de rede local eth0
```

```
root@kali:~# ping -c4 192.168.120.100 #Comprobar mediante o comando ping a conectividade coa interface de rede da máquina virtual A
```

```
root@kali:~# echo '192.168.120.100 kaliA' >> /etc/hosts #Engadir no ficheiro /etc/hosts, é dicir, na táboa estática de búsqueda para nomes de host (DNS) o nome kaliA, para que atenda á IP 192.168.120.100
```

```
root@kali:~# ping -c4 kaliA #Comprobar mediante o comando ping a conectividade coa interface de rede da máquina virtual A
```

2. Cambiar hostname da máquina virtual B. Por kaliB como hostname:

```
root@kali:~# echo 'kaliB' > /etc/hostname #Indicar ao sistema o valor do hostname.
```

```
root@kali:~# echo 'kernel.hostname=kaliB' >> /etc/sysctl.conf #Indicar ao kernel o valor do hostname.
```

```
root@kali:~# sysctl -p #Activar o cambio de hostname sen ter que pechar sesión nin reiniciar
```

```
root@kali:~# exit #Saír da consola local sudo na que estabamos a traballar para voltar á consola local de kali.
```

```
kali@kali:~$ exit #Pechar o terminal saíndo da consola local do usuario kali.
```

3. ^{SSH} **B → A** Acceder mediante SSH dende a máquina virtual B á máquina virtual A. Dende agora executaremos sempre os comandos dende a máquina virtual B, a través da consola SSH:

Na contorna gráfica abrir un terminal e executar:

```
kali@kaliB:~$ setxkbmap es #Cambiar o mapa de teclado ao idioma español.
```

```
kali@kaliB:~$ nc -vz 192.168.120.100 22 #Mediante o comando nc(netcat) comprobar que o porto 22 do servidor SSH está en estado escoita(listen), esperando conexións. A opción -v corresponde á opción verbose, o que permite amosar información máis detallada na saída do comando. A opción -z permite devolver PROMPT do sistema e de igual xeito facer o escaneo ao/s porto/s solicitados. O número 22 é o porto TCP a escanear.
```

```
kali@kaliB:~$ nc -vz kaliA 22 #Mediante o comando nc(netcat) comprobar que o porto 22 do servidor SSH está en estado escoita(listen), esperando conexións. A opción -v corresponde á opción verbose, o que permite amosar información máis detallada na saída do comando. A opción -z permite devolver PROMPT do sistema e de igual xeito facer o escaneo ao/s porto/s solicitados. O número 22 é o porto TCP a escanear.
```

```
kali@kaliB:~$ ssh -v kali@192.168.120.100 #Comprobar se o servidor SSH está activo e podemos conectarnos a el. Agora accedemos como o usuario kali a través da conexión cifrada SSH.
```

```
kali@kaliA:~$
```

NTP (sincronizar hosts para validez de tickets Kerberos)



Realizar nas 2 máquinas virtuais: A e B

Opción 1: Servizo NTP (ntpd)

1. Instalar servizo NTP:

```
# apt update || apt-get update #Actualizar o listado de paquetes dos repositorios (/etc/apt/sources.list, /etc/apt/sources.list.d/)
# apt search ntp || apt-cache search ntp #Buscar calquera paquete que coincida co patrón de búsqueda ntp
# apt -y install ntp || apt-get -y install ntp #Instalar o paquete ntp, é dicir, instalar o servizo NTP. Co parámetro -y automaticamente asumimos yes a calquera pregunta que ocorra na instalación do paquete.
```

2. Configurar servizo NTP (/etc/ntp.conf):

```
# A=$(grep -n server /etc/ntp.conf | cut -d':' -f1 | xargs | awk '{print $NF}')
# sed -i -e 's/server/##server/g' -e "${A}a\server 2.es.pool.ntp.org iburst prefer\nserver 3.europe.pool.ntp.org
iburst prefer\nserver 1.europe.pool.ntp.org iburst prefer" /etc/ntp.conf #Cambiar os servidores ntp cos que sincronizar o sistema
(ver http://www.pool.ntp.org/zone/es)
# systemctl restart ntp.service #Reiniciar o servizo ntp para ter en conta o cambio dos servidores realizado
# nc -uvz localhost 123 #Mediante o comando nc(netcat) comprobar se o porto 123 do servizo NTP está activo. A opción -u indica que o porto a buscar emprega o protocolo UDP, a opción -v corresponde á opción verbose, o que permite amosar información máis detallada na saída do comando. A opción -z permite devolver PROMPT do sistema e de igual xeito facer o escaneo ao/s porto/s solicitados. O número 123 é o porto UDP a escanear.
# ntpq -p #Identificar con que servidores ntp estamos a sincronizar o sistema
```

Opción 2: Servizo NTP (systemd-timesyncd)

3. Purgar servizo NTP (ntpd):

```
# apt update || apt-get update #Actualizar o listado de paquetes dos repositorios (/etc/apt/sources.list, /etc/apt/sources.list.d/)
# apt -y purge ntp || apt-get -y purge ntp #Eliminar o servizo NTP mediante a purga do paquete de nome ntp. Co parámetro -y automaticamente asumimos yes a calquera pregunta que ocorra na desinstalación do paquete. IMPORTANTE: Con purge SI SE ELIMINAN os ficheiros de configuración do paquete desinstalado.
# systemctl status systemd-timesyncd #Comprobar o estado do servizo systemd-timesyncd.
```

4. Configurar NTP mediante timesyncd (systemd, timedatectl):

```
# A=$(grep -n 'NTP=' /etc/systemd/timesyncd.conf | cut -d':' -f1 | xargs | awk '{print $NF}')
# sed -i -e 's/NTP=###NTP=/g' -e "${A}a\NTP=2.es.pool.ntp.org\nNTP=3.europe.pool.ntp.org\nNTP=1.europe.pool.ntp.org"
/etc/systemd/timesyncd.conf #Cambiar os servidores ntp cos que sincronizar o sistema (ver http://www.pool.ntp.org/zone/es)
# systemctl restart systemd-timesyncd #Reiniciar o servizo ntp para ter en conta o cambio dos servidores realizado
# timedatectl set-timezone Europe/Madrid #Modificar a zona temporal a Europe/Madrid
```

```
$ timedatectl #Comando que controla a hora e data do sistema. Executado Sen opcións amosa información sobre como está configurada a hora/data do sistema (sincronización NTP, zona temporal...)
$ timedatectl list-timezones #Lista as zonas temporais
```



dnsmasq (DNS + DHCP) na máquina virtual A

Convencións::

- Os reinos de Kerberos e os dominios de Active Directory están escritos con maiúscula.
- Os nomes de host escríbense en minúscula.
- As buscas de bases de datos distinguen entre maiúsculas e minúsculas.

1. Hostname. Pór kalia.ies.local como hostname:

```
root@kalia:~# echo 'kalia.ies.local' > /etc/hostname #Indicar ao sistema o valor do hostname.
root@kalia:~# sed -i 's/kaliA/kalia.ies.local/' /etc/sysctl.conf #Indicar ao kernel o valor do hostname.
root@kalia:~# sysctl -p #Activar o cambio de hostname sen ter que pechar sesión nin reiniciar
root@kalia:~# exit #Saír da consola local sudo na que estabamos a traballar para voltar á consola local de kali.
```

2. Instalar dnsmasq:

```
root@kalia:~# apt update #Actualizar o listado de paquetes dos repositorios (/etc/apt/sources.list, /etc/apt/sources.list.d/)
root@kalia:~# apt search dnsmasq #Buscar calquera paquete que coincida co patrón de búsqueda dnsmasq
root@kalia:~# apt -y install dnsmasq #Instalar o paquete dnsmasq. Co parámetro -y automaticamente asumimos yes a calquera pregunta que ocorra na instalación do paquete.
```

3. Resolución DNS. Actualizar o arquivo /etc/hosts:

```
root@kalia:~# echo '192.168.120.100 kalia.ies.local' >> /etc/hosts #Engadir no ficheiro /etc/hosts, é dicir, na táboa estática de
búsqueda para nomes de host (DNS) o nome kalia.ies.local para que atenda á IP 192.168.120.100
root@kalia:~# echo '192.168.120.101 kalib.ies.local' >> /etc/hosts #Engadir no ficheiro /etc/hosts, é dicir, na táboa estática de
búsqueda para nomes de host (DNS) o nome kalib.ies.local para que atenda á IP 192.168.120.101
root@kalia:~# hostname -f #Comprobar que se responde ao nome FQDN: kalia.ies.local
```

4. Configurar /etc/resolv.conf para apuntar a dnsmasq como servidor DNS a empregar para as resolucións de nomes/IPs:

/etc/resolv.conf: Arquivo onde se configuran os servidores DNS. Exemplo contido tipo:

```
domain example.local #Dominio a engadir na procura de hostnames. Se o host a buscar é pepito, é a procura falla, intentariase de
novo esta como pepito.example.local

search example.local #Lista de dominios a engadir na procura de hostnames.

nameserver 8.8.8.8 #Servidor DNS primario para resolución de nomes.

nameserver 8.8.4.4 #Agregar servidor DNS secundario para resolución de nomes.
```

domain e search son excluintes, a última directiva que apareza no ficheiro prevalece.

```
root@kalia:~# echo -e 'nameserver 127.0.0.1\nnameserver 192.168.120.100\nnameserver 8.8.4.4' > /etc/resolv.conf
#Agregar servidor DNS para resolución de nomes.
```

5. Habilitar servizo dnsmasq(DNS + DHCP):

```
root@kalia:~# /etc/init.d/dnsmasq status #Comprobar o estado do servidor dnsmasq
root@kalia:~# /etc/init.d/dnsmasq start #Arrancar o servidor dnsmasq.
root@kalia:~# /etc/init.d/dnsmasq status #Comprobar o estado do servidor dnsmasq
```




Servidor Kerberos Heimdal (kdc) na máquina virtual A

1. Instalar servidor Kerberos Heimdal e definir REALM:

```
root@kalia:~# apt update || apt-get update #Actualizar o listado de paquetes dos repositorios (/etc/apt/sources.list, /etc/apt/sources.list.d)
root@kalia:~# apt search heimdal-kdc || apt-cache search heimdal-kdc #Buscar calquera paquete que coincida co patrón de
búsqueda heimdal-kdc
root@kalia:~# apt -y install heimdal-kdc || apt-get -y install heimdal-kdc #Instalar o paquete heimdal-kdc, é dicir, instalar o
servidor Kerberos. Co parámetro -y automaticamente asumimos yes a calquera pregunta que ocorra na instalación do paquete.
```

```
Default Kerberos version 5 realm:
IES.LOCAL #Indicar reino Kerberos (MAIÚSCULAS)
Kerberos servers for your realm:
kalia.ies.local #Indicar servidor Kerberos (minúsculas)
Administrative server for your Kerberos realm:
kalia.ies.local #Indicar servidor administrador do reino Kerberos (minúsculas)
```

```
root@kalia:~# dpkg-reconfigure kbr5-config #Reconfigurar kerberos
root@kalia:~# apt -y install heimdal-docs #Instalar paquete documentación Heimdal Kerberos
root@kalia:~# dpkg -L heimdal-docs #Listar ficheiros pertencentes ao paquete heimdal-docs
```

2. Comprobar estado do Servidor Kerberos:

```
root@kalia:~# /etc/init.d/heimdal-kdc status #Comprobar o estado do servidor Kerberos, por defecto (logo de instalar o paquete) está
arrancado.
root@kalia:~# nc -vz localhost 88 #Mediante o comando nc(netcat) comprobar se o porto 88 do servidor Kerberos está en estado
escoita(listen), esperando conexións. A opción -v corresponde á opción verbose, o que permite amosar información máis detallada na saída do comando.
A opción -z permite devolver PROMPT do sistema e de igual xeito facer o escaneo ao/s porto/s solicitados. O número 88 é o porto TCP a escanear.
root@kalia:~# nc -vz 192.168.120.100 88 #Mediante o comando nc(netcat) comprobar se o porto 88 do servidor Kerberos está en estado
escoita(listen), esperando conexións. A opción -v corresponde á opción verbose, o que permite amosar información máis detallada na saída do comando.
A opción -z permite devolver PROMPT do sistema e de igual xeito facer o escaneo ao/s porto/s solicitados. O número 88 é o porto TCP a escanear.
root@kalia:~# nc -vz kalia.ies.local 88 #Mediante o comando nc(netcat) comprobar se o porto 88 do servidor Kerberos está en estado
escoita(listen), esperando conexións. A opción -v corresponde á opción verbose, o que permite amosar información máis detallada na saída do comando.
A opción -z permite devolver PROMPT do sistema e de igual xeito facer o escaneo ao/s porto/s solicitados. O número 88 é o porto TCP a escanear.
root@kalia:~# netstat -natp | grep 88 #Mediante o comando netstat comprobar que o porto 88 do servidor Kerberos está en estado
escoita(listen), esperando conexións. A opción -n permite non resolver nomes amosando así soamente as IPs e o comando ser máis rápido na execución.
A opción -a equivale á opción all o que permite amosar todos os sockets (conectores) á escoita no servidor. A opción -t equivale a tcp o que permite
buscar soamente información sobre o protocolo TCP. A opción -p equivale a program e amosa o PID e nome do programa ao cal pertence o socket.
root@kalia:~# ss -natp | grep 88 #Mediante o comando ss comprobar que o porto 88 do servidor Kerberos está en estado escoita(listen),
esperando conexións. A opción -n permite non resolver nomes amosando así soamente as IPs e o comando ser máis rápido na execución. A opción -a
equivale á opción all o que permite amosar todos os sockets (conectores) á escoita no servidor. A opción -t equivale a tcp o que permite buscar
soamente información sobre o protocolo TCP. A opción -p equivale a program e amosa o PID e nome do programa ao cal pertence o socket.
```

3. Usuario e ticket. Autenticar como usuario en Kerberos, conseguir un ticket e ver a súa validez:

```
root@kalia:~# kadmin -l #Administrar de forma local kerberos
```

```
root@kalia:~# kadmin -l
kadmin> add user1 #Crear usuario user1 na bddd principal kerberos (base de datos de usuarios do KDC)
Max ticket life [1 day]:
Max renewable life [1 week]:
Principal expiration time [never]:
Password expiration time [never]:
Attributes []:
Policy [default]:
user1@IES.LOCAL's Password: #Introducir o contrasinal que queremos que posúa o usuario user1. Por exemplo abc123. (Olla
que o contrasinal ten un caracter punto final)
Verify password - user1@IES.LOCAL's Password: #Introducir de novo o contrasinal anterior (abc123.)
kadmin> quit
root@kalia:~#
```

Dentro de kadmin coa comando **list *** listamos todos os principais.

```
root@kalia:~# kinit user1 #Autenticar como usuario user1 e contrasinal abc123, conseguindo un ticket TGT
user1@IES.LOCAL's Password:
root@kalia:~# klist -l #Listar a validez do ticket TGT. Este ticket é válido para acceder a calquera servizo de rede que empregue Kerberos para
autenticación.
```

Apuntar ao DNS (dnsmasq en kaliA)



1. Hostname. Pór kalib.ies.local como hostname:

```
root@kaliB:~# echo 'kalib.ies.local' > /etc/hostname #Indicar ao sistema o valor do hostname.  
root@kaliB:~# sed -i 's/kaliB/kalib.ies.local/' /etc/sysctl.conf #Indicar ao kernel o valor do hostname.  
root@kaliB:~# sysctl -p #Activar o cambio de hostname sen ter que pechar sesión nin reiniciar  
root@kaliB:~# exit #Saír da consola local sudo na que estabamos a traballar para voltar á consola local de kali.
```

2. Resolución DNS. Actualizar o arquivo /etc/hosts:

```
root@kalib:~# echo '192.168.120.101 kalib.ies.local' >> /etc/hosts #Engadir no ficheiro /etc/hosts, é dicir, na táboa estática de  
búsqueda para nomes de host (DNS) o nome kalib.ies.local para que atenda á IP 192.168.120.101  
root@kalib:~# hostname -f #Comprobar que se responde ao nome FQDN: kalib.ies.local  
root@kalib:~# sed -i 's/kaliA/kalia.ies.local/' /etc/hosts #Modificar a entrada de kaliA no ficheiro /etc/hosts, é dicir, na táboa estática de  
búsqueda para nomes de host (DNS) para que o nome kalia.ies.local atenda á IP 192.168.120.100
```

3. Configurar /etc/resolv.conf para apuntar a dnsmasq como servidor DNS a empregar para as resolucións de nomes/IPs:

/etc/resolv.conf: Arquivo onde se configuran os servidores DNS. Exemplo contido tipo:

```
domain example.local #Dominio a engadir na procura de hostnames. Se o host a buscar é pepito, é a procura falla, intentariase de  
novo esta como pepito.example.local  
  
search example.local #Lista de dominios a engadir na procura de hostnames.  
  
nameserver 8.8.8.8 #Servidor DNS primario para resolución de nomes.  
  
nameserver 8.8.4.4 #Agregar servidor DNS secundario para resolución de nomes.
```

domain e search son excluintes, a última directiva que apareza no ficheiro prevalece.

```
root@kalib:~# echo -e 'nameserver 192.168.120.100\nnameserver 8.8.4.4' > /etc/resolv.conf #Agregar servidor DNS para  
resolución de nomes.
```



Ciente Kerberos Heimdal na máquina virtual B


1. Instalar cliente Kerberos Heimdal e reino REALM:
root@kalib:~# apt update || apt-get update #Actualizar o listado de paquetes dos repositorios (/etc/apt/sources.list, /etc/apt/sources.list.d/)
root@kalib:~# apt search heimdal-clients || apt-cache search heimdal-clients #Buscar calquera paquete que coincida co patrón de búsqueda heimdal-clients
root@kalib:~# apt -y install heimdal-clients || apt-get -y install heimdal-clients #Instalar o paquete heimdal-clients, é dicir, instalar o cliente Kerberos. Co parámetro -y automaticamente asumimos yes a calquera pregunta que ocorra na instalación do paquete.
- Default Kerberos version 5 realm:
IES.LOCAL #Indicar reino Kerberos (MAIÚSCULAS)
Kerberos servers for your realm:
kalia.ies.local #Indicar servidor Kerberos (minúsculas)
Administrative server for your Kerberos realm:
kalia.ies.local #Indicar servidor administrador do reino Kerberos (minúsculas)
- root@kalib:~# dpkg-reconfigure kbr5-config #Reconfigurar kerberos
2. Usuario e ticket. Autenticar como usuario en Kerberos, conseguir un ticket e ver a súa validez:
root@kalib:~# kinit user1 #Autenticar como usuario user1 e contrasinal abc123. conseguindo un ticket TGT. Ter en conta que o usuario user1 xa existe na bbdd principal de kerberos e foi xerado de forma local en kalia mediante o comando kadmin -l
user1@IES.LOCAL's Password:
root@kalib:~# klist -l #Listar a validez do ticket TGT. Este ticket é válido para acceder a calquera servizo de rede que empregue Kerberos para autenticación.


Exemplo1. Máquina Virtual A: Kerberizar a Autenticación Local (pam-krb5)


i. Instalar módulo libpam-krb5:


```
root@kalia:~# apt update || apt-get update #Actualizar o listado de paquetes dos repositorios (/etc/apt/sources.list, /etc/apt/sources.list.d/)
root@kalia:~# apt search libpam-krb5 || apt-cache search libpam-krb5 #Buscar calquera paquete que coincida co patrón de búsqueda libpam-krb5
root@kalia:~# apt -y install libpam-krb5 || apt-get -y install libpam-krb5 #Instalar o paquete libpam-krb5, é dicir, instalar o módulo PAM que permite aos usuarios locais autenticarse mediante o contrasinal de kerberos (e non a través de /etc/passwd) . Co parámetro -y automaticamente asumimos yes a calquera pregunta que ocorra na instalación do paquete.
```


PAM y NSS

Archivos de configuración utilizados por PAM y NSS

Bases de datos de usuarios y grupos

Módulos PAM (páxs 26,27)

YENDO MÁS ALLÁ NSS y bases de datos de sistema (getent)

Práctica Seguridad Informática - PAM

ii. Configurar PAM con Kerberos:

Xa está feito! Unha vez instalado o paquete libpam-krb5 xa podemos autenticar mediante kerberos coas contas locais. Para iso, imos crear un usuario no sistema para validar con PAM auth (/etc/passwd) e imos crear un usuario co mesmo nome na bbdd principal de Kerberos con outro contrasinal. Veremos que podemos acceder co contrasinal de Kerberos á conta local.

```
root@kalia:~# pam-auth-update #Con esta comando podemos modificar/verificar os módulos de autenticación PAM activados.
root@kalia:~# apropos krb5 #Buscar en que páxinas do man e descripciones existen referencias ao nome dado: krb5
root@kalia:~# man pam_krb5 #Ver as páxinas do manual para pma_krb5
```

```
root@kalia:~# groupadd -g 1050 testing #Crear o grupo de nome testing co GID de valor 1050.
root@kalia:~# useradd -m -u 1050 -g 1050 -d /home/testuser -p $(mkpasswd -m sha-512 abc123.) -s /bin/bash testuser
#Crear o usuario testuser co comando useradd, onde:
-m → Copia na casa do usuario o que exista no cartafol /etc/skel
-u → Establece o valor do UID, neste caso 1050
-g → Establece o grupo principal, neste caso o valor GID 1050 que corresponde ao grupo testing
-d /home/testuser → Xera a casa do usuario, é dicir, o directorio de traballo do usuario, no cartafol /home/testuser
-p $(mkpasswd -m sha-512 abc123.) → Pon abc123. como contrasinal cifrado (sha-512) para o login do usuario testing
-s /bin/bash → Establece como shell de traballo para o usuario a shell bash
testuser → Establece como nome de autenticación de usuario o nome testuser
```

```
root@kalia:~# getent passwd #Conseguir entradas de Name Service Switch libraries, neste caso conseguir os usuarios de passwd
root@kalia:~# getent passwd | grep testuser #Filtrar o comando anterior co patrón testuser, é dicir, amosa información de autenticación do usuario testuser
root@kalia:~# kadmin -l #Administrar de forma local kerberos
```

```
root@kalia:~# kadmin -l
kadmin> add testuser #Crear usuario testuser na bbdd principal kerberos (base de datos de usuarios do KDC)
Max ticket life [1 day]:
Max renewable life [1 week]:
Principal expiration time [never]:
Password expiration time [never]:
Attributes [:
Policy [default]:
testuser@IES.LOCAL's Password: #Introducir o contrasinal que queremos que posúa na bbdd principal de Kerberos o usuario testuser. Por exemplo 123456
Verify password - testuser@IES.LOCAL's Password: #Introducir de novo o contrasinal anterior (123456)
kadmin> quit
root@kalia:~#
```


```
root@kalia:~# exit #Saír da consola local sudo na que estabamos a traballar para voltar á consola local de kali.
kali@kalia:~$ su - testuser #Acceder como usuario testuser pero escribir o contrasinal kerberos de testuser: 123456
testuser@kalia:~$ klist -l #Listar a validez do ticket TGT do usuario testuser. Este ticket é válido para acceder a calquera servizo de rede que empregue Kerberos para autenticación.
```


Name	Cache name	Expires
* testuser@IES.LOCAL	FILE:/tmp/krb5cc_1050_EbG96i	Dec 15 23:29:05 2020


Exemplo2. Máquina Virtual B: Kerberizar a Autenticación Local (pam-krb5)


i. Instalar módulo **libpam-krb5**:


```
root@kalib:~# apt update || apt-get update #Actualizar o listado de paquetes dos repositorios (/etc/apt/sources.list, /etc/apt/sources.list.d/)
root@kalib:~# apt search libpam-krb5 || apt-cache search libpam-krb5 #Buscar calquera paquete que coincida co patrón de búsqueda libpam-krb5
root@kalib:~# apt -y install libpam-krb5 || apt-get -y install libpam-krb5 #Instalar o paquete libpam-krb5, é dicir, instalar o módulo PAM que permite aos usuarios locais autenticarse mediante o contrasinal de kerberos (e non a través de /etc/passwd) . Co parámetro -y automaticamente asumimos yes a calquera pregunta que ocorra na instalación do paquete.
```


 **PAM y NSS**

 **Archivos de configuración utilizados por PAM y NSS**

 **Bases de datos de usuarios y grupos**

 **Módulos PAM (páxs 26,27)**

YENDO MÁS ALLÁ NSS y bases de datos de sistema (getent) 

 **Práctica Seguridad Informática - PAM**

ii. Configurar PAM con Kerberos:

Xa está feito! Unha vez instalado o paquete libpam-krb5 xa podemos autenticar mediante kerberos coas contas locais. Para iso, imos crear un usuario no sistema para validar con PAM auth (/etc/passwd) e imos crear un usuario co mesmo nome na bbdd principal de Kerberos con outro contrasinal. Veremos que podemos acceder co contrasinal de Kerberos á conta local.

```
root@kalib:~# pam-auth-update #Con esta comando podemos modificar/verificar os módulos de autenticación PAM activados.
```

```
root@kalib:~# apropos krb5 #Buscar en que páxinas do man e descripciones existen referencias ao nome dado: krb5
root@kalib:~# man pam_krb5 #Ver as páxinas do manual para pma krb5
```

```
root@kalib:~# groupadd -g 4000 untesting #Crear o grupo de nome untesting co GID de valor 4000.
root@kalib:~# useradd -m -u 4000 -g 4000 -d /home/testuser -p $(mkpasswd -m sha-512 abc123.) -s /bin/bash testuser
#Crear o usuario testuser co comando useradd, onde:
-m → Copia na casa do usuario o que exista no cartafol /etc/skel
-u → Establece o valor do UID, neste caso 4000
-g → Establece o grupo principal, neste caso o valor GID 4000 que corresponde ao grupo untesting
-d /home/testuser → Xera a casa do usuario, é dicir, o directorio de traballo do usuario, no cartafol /home/testuser
-p $(mkpasswd -m sha-512 abc123.) → Pon abc123. como contrasinal cifrado (sha-512) para o login do usuario testing
-s /bin/bash → Establece como shell de traballo para o usuario a shell bash
testuser → Establece como nome de autenticación de usuario o nome testuser
```

```
root@kalib:~# getent passwd #Conseguir entradas de Name Service Switch libraries, neste caso conseguir os usuarios de passwd
root@kalib:~# getent passwd | grep testuser #Filtrar o comando anterior co patrón testuser, é dicir, amosa información de autenticación do usuario testuser
```

IMPORTANTE:

- Notar que o usuario debe existir localmente para que a autenticación poida realizarse, é dicir, o usuario existe e autentica pero neste caso na bbdd principal de Kerberos.
- Notar tamén que este usuario é local de kalib, polo que pode posuír outro uid, gid, grupos secundarios, contrasinal, casa de usuario... totalmente distintos ao usuario local de kalia.

```
root@kalib:~# exit #Saír da consola local sudo na que estabamos a traballar para voltar á consola local de kali.
```

```
kali@kalib:~$ su - testuser #Acceder como usuario testuser pero escribir o contrasinal kerberos de testuser: 123456
■ klist -l #Listar a validez do ticket TGT do usuario testuser. Este ticket é válido para acceder a calquera servizo de rede que empregue Kerberos para autenticación.
```

Name	Cache name	Expires
* testuser@IES.LOCAL	FILE:/tmp/krb5cc_4000_a57zUd	Dec 16 14:34:02 2020

Exemplo3. Acceso SSH: Autenticación Kerberos. Contas de usuario locais kerberizadas e Servizo SSH non Kerberizado

Xa está feito! Unha vez instalado o paquete libpam-krb5 xa podemos autenticar mediante kerberos coas contas locais de forma local ou remota mediante conexións SSH. Para iso, imos comprobar que o usuario *testuser* pode autenticar con PAM auth (/etc/passwd) e tamén con Kerberos.

Dende a máquina virtual A. Servidor SSH:

i. Comprobar estado do Servidor SSH:

```
root@kalia:~# /etc/init.d/ssh status #Comprobar o estado do servidor SSH, por defecto non está arrancado.
root@kalia:~# nc -vz kalia.ies.local 22 #Mediante o comando nc(netcat) comprobar se o porto 22 do servidor ssh está en estado escoita(listen),
esperando conexións. A opción -v corresponde á opción verbose, o que permite amosar información máis detallada na saída do comando. A opción -z
permite devolver PROMPT do sistema e de igual xeito facer o escaneo ao/s porto/s solicitados. O número 22 é o porto TCP a escanear.
root@kalia:~# /etc/init.d/ssh start #Arrancar o servidor SSH.
root@kalia:~# /etc/init.d/ssh status #Comprobar o estado do servidor SSH, agora debe estar arrancado.
```

ii. Autenticación Kerberos sen servidor Kerberizado:

```
root@kalia:~# ssh -v testuser@kalia.ies.local #Comprobar se o servidor SSH está activo e podemos conectarnos a el co usuario testuser e o
seu contrasinal PAM (/etc/passwd). Se é a primeira vez que nos conectamos o servidor avísanos se estamos de acordo coa autenticación. Respostamos yes
e pulsamos Enter. A opción -v (modo verbose) aporta información máis detallada da conexión.
root@kalia:~# ssh -v testuser@kalia.ies.local #Comprobar se o servidor SSH está activo e podemos conectarnos a el co usuario testuser e o
seu contrasinal Kerberos. Agora vemos que SI é posible a autenticación mediante Kerberos. Non fai falla configurar o servidor SSH para que o
usuario testuser poida autenticar co seu contrasinal Kerberos.
```

Dende a máquina virtual B. Cliente SSH:

i. Autenticación Kerberos sen servidor Kerberizado:

```
root@kalia:~# ssh -v testuser@kalia.ies.local #Comprobar se o servidor SSH está activo e podemos conectarnos a el co usuario testuser e o
seu contrasinal PAM (/etc/passwd). Se é a primeira vez que nos conectamos o servidor avísanos se estamos de acordo coa autenticación. Respostamos yes
e pulsamos Enter. A opción -v (modo verbose) aporta información máis detallada da conexión.
root@kalia:~# ssh -v testuser@kalia.ies.local #Comprobar se o servidor SSH está activo e podemos conectarnos a el co usuario testuser e o
seu contrasinal Kerberos. Agora vemos que SI é posible a autenticación mediante Kerberos. Non fai falla configurar o servidor SSH para que o
usuario testuser poida autenticar co seu contrasinal Kerberos.
```



Exemplo4. Kerberizar a Autenticación en Servizos (keytab)

Dende a máquina virtual A. Servidor Kerberos kalia.ies.local:

i. Crear keytab para kalia.ies.local:

(1) Crear principal host/kalia.ies.local

```
root@kalia:~# kadmin -l #Administrar de forma local kerberos
```

```
root@kalia:~# kadmin -l
kadmin> add -r host/kalia.ies.local@IES.LOCAL #Crear principal para o host kalia na bddd kerberos (KDC)
Max ticket life [1 day]:
Max renewable life [1 week]:
Principal expiration time [never]:
Password expiration time [never]:
Attributes []:
Policy [default]:
kadmin> quit
root@kalia:~#
```



(2) Exportar keytab do principal host/kalia.ies.local

```
root@kalia:~# kadmin -l #Administrar de forma local kerberos
```

```
root@kalia:~# kadmin -l
kadmin> ext host/kalia.ies.local@IES.LOCAL #Exportar a clave ao ficheiro /etc/krb5.keytab
kadmin> quit
root@kalia:~#
```

```
root@kalia:~# ls -l /etc/krb5.keytab #Listar de forma extendida o ficheiro /etc/krb5.keytab, o cal é o ficheiro por defecto onde se gardan as
claves extraídas
```

```
root@kalia:~# ktutil -k /etc/krb5.keytab list #Listar o contido do ficheiro /etc/krb5.keytab
```

O arquivo de claves keytab pode ser xerado en calquera computadora que sexa cliente Kerberos e non ten porque vincularse a esta computadora onde foi xerado. Estes arquivos poden xerarse nunha computadora e copiarse para que poidan ser empregados por outras computadoras.

ii. Crear keytab para kalib.ies.local:

(1) Crear principal host/kalib.ies.local

```
root@kalia:~# kadmin -l #Administrar de forma local kerberos en kalia
```

```
root@kalia:~# kadmin -l
kadmin> add -r host/kalib.ies.local@IES.LOCAL #Crear principal para o host kalib na bddd principal kerberos (KDC)
Max ticket life [1 day]:
Max renewable life [1 week]:
Principal expiration time [never]:
Password expiration time [never]:
Attributes []:
Policy [default]:
kadmin> quit
root@kalia:~#
```

(2) Exportar keytab do principal host/kalib.ies.local

```
root@kalia:~# kadmin -l #Administrar de forma local kerberos
```

```
root@kalia:~# kadmin -l
kadmin> ext --keytab=/etc/krb5.keytab2 host/kalib.ies.local@IES.LOCAL #Exportar a clave ao ficheiro /etc/krb5.keytab2
kadmin> quit
root@kalia:~#
```

```
root@kalia:~# ls -l /etc/krb5.keytab2 #Listar de forma extendida o ficheiro /etc/krb5.keytab2, o cal é o ficheiro onde eliximos gardar a clave
extraída do principal hostB/kaliB.ies.local@IES.LOCAL
```

```
root@kalia:~# ktutil -k /etc/krb5.keytab2 list #Listar o contido do ficheiro /etc/krb5.keytab2
```

```
root@kalia:~# cp -v /etc/krb5.keytab2 /home/kali/ #Copiar (modo verbose) o ficheiro /etc/krb5.keytab2 dentro do directorio /home/kali
```

```
root@kalia:~# chown kali /home/kali/krb5.keytab2 #Cambiar o usuario propietario do ficheiro /home/kali/krb5.keytab2 ao usuario kali
```

Agora debemos facer copia deste arquivo keytab de claves a kaliB para configurar os servizos que queiramos autenticar con Kerberos, no servidor Kerberos kalia.ies.local



Exemplo5. Kerberizar a Autenticación Remota SSH (/etc/ssh/sshd_config + keytab)

Dende a máquina virtual A. Servidor SSH:

i. Autenticación Kerberos sen servidor Kerberizado:

root@kalia:~# ssh -v testuser@kalia.ies.local #Comprobar se o servidor SSH está activo e podemos conectarnos a el co usuario testuser e o seu contrasinal PAM (/etc/passwd). Se é a primeira vez que nos conectamos o servidor avísanos se estamos de acordo coa autenticación. Respostamos yes e pulsamos Enter. A opción -v (modo verbose) aporta información máis detallada da conexión.

root@kalia:~# ssh -v testuser@kalia.ies.local #Comprobar se o servidor SSH está activo e podemos conectarnos a el co usuario testuser e o seu contrasinal Kerberos. Agora vemos que SI é posible a autenticación mediante Kerberos. Non fai falla configurar o servidor SSH para que o usuario testuser poida autenticar co seu contrasinal Kerberos.

ii. Kerberizar Servidor SSH kalia.ies.local:

(1) Modificar permisos keytab (/etc/krb5.keytab) do principal host/kalia.ies.local

root@kalia:~# chown sshd.ssh /etc/krb5.keytab #Cambiar usuario propietario sshd e grupo propietario ssh ao ficheiro /etc/krb5.keytab

root@kalia:~# chmod 640 /etc/krb5.keytab #Cambiar os permisos **ugo** do ficheiro krb5.keyta situado en /etc para establecer os permisos rw-r----- (lectura e escritura para o usuario propietario, soamente lectuar para o grupo propietario e ningún permiso para o resto do mundo)

(2) Modificar configuración Servidor SSH (/etc/ssh/sshd_config)

root@kalia:~# A=\$(grep -n 'GSSAPIAuthentication' /etc/ssh/sshd_config | cut -d':' -f1 | xargs | awk '{print \$NF}')

root@kalia:~# sed -i -e 's/GSSAPIAuthentication/##GSSAPIAuthentication/g' -e "\${A}aGSSAPIAuthentication yes" /etc/ssh/sshd_config #Cambiar a directiva a yes. Esta directiva permítenos realizar a autenticación mediante Kerberos

root@kalia:~# /etc/init.d/ssh reload #Recargar o ficheiro de configuración do servidor SSH para que se activen os cambios realizados

(3) Conseguir ticket TGT para o usuario testuser

root@kalia:~# kinit testuser #Autenticar en Kerberos como usuario **testuser** e contrasinal **123456** conseguindo un ticket TGT

root@kalia:~# klist -l #Listar a validez do ticket TGT. Este ticket é válido para acceder a calquera servizo de rede que empregue Kerberos para autenticación.

Dende a máquina virtual B. Cliente SSH:

i. Copia a keytab /etc/krb5.keytab2 correspondente ao principal host/kalib.ies.local:

root@kalib:~# scp kali@kalia.ies.local:krb5.keytab2 . #Contrasinal de acceso **abc123**. (Autenticación PAM).Estando situado no HostB, copiar de A a B (do servidor ao cliente) o arquivo /home/kali/krb5.keytab2, é dicir, copiar en B o ficheiro /home/kali/krb5.keytab2 existente no HostA, e copialo na ruta onde lanza o comando o usuario cliente que é o que simboliza o caracter '.'. Neste caso a copia realizarase no \$HOME(~) do usuario root (/root)

root@kalib:~# cp -v krb5.keytab2 /etc/krb5.keytab #Copiar (modo verbose) o ficheiro krb5.keytab2 dentro do directorio /etc co nome krb5.keytab

ii. Modificar permisos keytab /etc/krb5.keytab:

(1) Modificar permisos keytab (/etc/krb5.keytab) do principal host/kalib.ies.local

root@kalib:~# chown sshd.ssh /etc/krb5.keytab #Cambiar usuario propietario sshd e grupo propietario ssh ao ficheiro /etc/krb5.keytab

root@kalib:~# chmod 640 /etc/krb5.keytab #Cambiar os permisos **ugo** do ficheiro krb5.keyta situado en /etc para establecer os permisos rw-r----- (lectura e escritura para o usuario propietario, soamente lectuar para o grupo propietario e ningún permiso para o resto do mundo)

(2) Modificar configuración Cliente SSH (/etc/ssh/ssh_config)

root@kalib:~# A=\$(grep -n 'GSSAPIAuthentication' /etc/ssh/sshd_config | cut -d':' -f1 | xargs | awk '{print \$NF}')

root@kalib:~# sed -i -e 's/GSSAPIAuthentication/##GSSAPIAuthentication/g' -e "\${A}aGSSAPIAuthentication yes" /etc/ssh/sshd_config #Cambiar a directiva a yes. Esta directiva permítenos realizar a autenticación mediante Kerberos

root@kalib:~# A=\$(grep -n 'GSSAPIDelegateCredentials' /etc/ssh/ssh_config | cut -d':' -f1 | xargs | awk '{print \$NF}')

root@kalib:~# sed -i -e 's/GSSAPIDelegateCredentials/##GSSAPIDelegateCredentials/g' -e "\${A}aGSSAPIDelegateCredentials yes" /etc/ssh/ssh_config #Cambiar a directiva a yes. Esta directiva permítenos realizar a autenticación mediante Kerberos

(3) Conseguir ticket TGT para o usuario testuser

root@kalib:~# kinit testuser #Autenticar en Kerberos como usuario **testuser** e contrasinal **123456** conseguindo un ticket TGT

root@kalib:~# klist -l #Listar a validez do ticket TGT. Este ticket é válido para acceder a calquera servizo de rede que empregue Kerberos para autenticación.

iii. Conexión mediante Autenticación Kerberos + Servizo SSH Kerberizado

root@kalib:~# ssh -K -v testuser@kalia.ies.local #Acceso sen contrasinal mediante autenticación servidor kerberizado, é dicir, o usuario testuser accede directamente sen escribir ningún contrasinal. A opción -K permite a autenticación Kerberos (basada en GSSAPI) e o reenvío de credenciais ao servidor.

testuser@kalia:~\$