FreeRADIUS
Conexión Remota mediante SSH

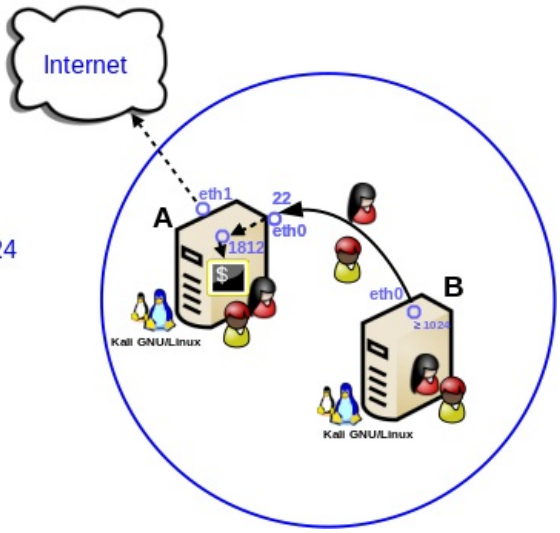
ESCENARIO

Máquinas virtuais:
RAM ≥ 2048MB CPU ≥ 2 PAE/NX habilitado
BIOS: Permite arranque dispositivo extraíble: CD/DVD, USB

Máquina virtual A:
Rede Interna: 192.168.120.0/24
eth0→IP/MS: 192.168.120.100/24
Rede: Modo NAT (10.0.2.0/24)
eth1→IP/MS: 10.0.2.15/24
Servidor RADIUS: freeradius
Servidor SSH: openssh-server
ISO: Kali Live amd64
PAM: libpam-radius-auth

Máquina virtual B:
Rede Interna: 192.168.120.0/24
eth0→IP/MS: 192.168.120.120/24

Cliente RADIUS
Cliente SSH: openssh-client (ssh)
ISO: Kali Live amd64



LIMITACIÓN DE RESPONSABILIDADE O autor do presente documento declina calquera responsabilidade asociada ao uso incorrecto e/ou malicioso que puidese realizarse coa información exposta no mesmo. Por tanto, non se fai responsable en ningún caso, nin pode ser considerado legalmente responsable en ningún caso, das consecuencias que poidan derivarse da información contida nel ou que esté enlazada dende ou hacia el, incluíndo os posibles erros e información incorrecta existentes, información difamatoria, así como das consecuencias que se poidan derivar sobre a súa aplicación en sistemas de información reais e/ou virtuais. Este documento foi xerado para uso didáctico e debe ser empregado en contornas privadas e virtuais controladas co permiso correspondente do administrador desas contornas.

NOTAS:

- Cliente ssh GNU/Linux: **comando ssh (paquete openssh-client)**

Práctica FreeRADIUS - Conexión Remota mediante SSH

Máquina A: Arrancar coa Kali Live amd64

1. Na contorna gráfica abrir un terminal e executar:
   kali@kali:~$ setxkbmap es #Cambiar o mapa de teclado ao idioma español.

2. Configurar a rede:
   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 || systemctl stop avahi-daemon #Parar o demo avahi-daemon(control resolución de nomes) para poder configurar de forma manual a configuración de rede e non ter conflicto 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 conflicto con este xestor.
   root@kali:~# ip addr show #Amosar a configuración de todas as tarxetas de rede. Nesta caso, na máquina A, as tarxetas de redes: loopback(lo), interna(eth0) e NAT(eth1).
   root@kali:~# 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@kali:~# ip addr show #Amosar a configuración de todas as tarxetas de rede. Nesta caso, na máquina A, as tarxetas de redes: loopback(lo), interna(eth0) e NAT(eth1).
   - Se a interface eth0 non está UP, é dicir, está en estado DOWN, executar:
     root@kali:~# ip link set up dev eth0 && ip addr show eth0

   root@kali:~# ping -c4 192.168.120.100 #Comprobar mediante o comando ping a conectividade coa interface de rede local eth0

3. Comprobar estado do Servidor SSH:
   root@kali:~# /etc/init.d/ssh status || systemctl status ssh #Comprobar o estado do servidor SSH, por defecto non está arrancado.
   root@kali:~# /etc/init.d/ssh start || systemctl start ssh #Arrancar o servidor SSH.
   root@kali:~# /etc/init.d/ssh status || systemctl status ssh #Comprobar o estado do servidor SSH, agora debe estar arrancado.
   root@kali:~# 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 (kali). Se é a primeira ver 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@kali:~$ exit #Saír da consola remota ssh a que acabamos de acceder, para voltar á consola local de **root**
   root@kali:~# ssh -v kali@192.168.120.100 #Comprobar se o servidor SSH está activo en 192.168.120.100 e podemos conectarnos a el co usuario kali e o seu contrasinal (kali). Se é a primeira ver 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@kali:~$ exit #Saír da consola remota ssh a que acabamos de acceder, para voltar á consola local de **root**

4. Configurar FreeRADIUS:

root@kali:~# apt update || apt-get update #Actualizar repositorios declarados no ficheiro */etc/apt/souces.list* e nos ficheiros existentes no directorio */etc/apt/sources.list.d*

Así, unha vez realizada a consulta dos ficheiros existentes nas rutas anteriores, descárganse uns ficheiros coas listas de paquetes posibles a instalar. Estes ficheiros son gardados en */var/lib/apt/lists*

root@kali:~# apt -y install freeradius || apt-get -y install freeradius #Instalar o paquete de nome *freeradius*. Co parámetro -y automaticamente asumimos yes a calquera pregunta que ocorra na instalación do paquete.

root@kali:~# echo 'client kali-b {
ipaddr = 192.168.120.120
secret = ccbysa
}' >> /etc/freeradius/3.0/clients.conf #Definir un novo cliente para o servidor FreeRADIUS, chamado kali-b no ficheiro onde FreeRADIUS garda a lista de clientes autorizados que poden realizar solicitudes de autenticación, onde:

- En *client kali-b* especifícase o nome do cliente, neste caso "kali-b", o cal é simplemente unha etiqueta ou alias para identificar o cliente, e pode ser calquera nome que axude a recoñecelo.
- En *ipaddr = 192.168.120.120* especifícase a dirección IP do cliente que está autorizado para conectarse ao servidor FreeRADIUS(192.168.120.100)
- En *secret = ccbysa* defínese a clave compartida, ou "shared secret", neste caso "ccbysa", que funciona como unha especie de contrasinal entre o cliente (neste caso 192.168.120.120) e o servidor FreeRADIUS(192.168.120.100). Esta clave debe coincidir entre o cliente e o servidor para que se poidan autenticar as conexións entre eles.

root@kali:~# echo 'ana Cleartext-Password := "1234"' >> /etc/freeradius/3.0/users #Engadir esta entrada permite que o usuario "ana" poida autenticarse no sistema FreeRADIUS utilizando a contrasinal *1234*. Cando un cliente envía unha solicitude de autenticación para este usuario, FreeRADIUS comprobará o nome de usuario e a contrasinal contra as entradas do ficheiro *users*. Se a contrasinal proporcionada polo cliente coincide coa que está almacenada, a autenticación será exitosa; se non, será rexeitada.

root@kali:~# echo 'brais Cleartext-Password := "abc123."' >> /etc/freeradius/3.0/users #Engadir esta entrada permite que o usuario "brais" poida autenticarse no sistema FreeRADIUS utilizando a contrasinal "*abc123.*" Cando un cliente envía unha solicitude de autenticación para este usuario, FreeRADIUS comprobará o nome de usuario e a contrasinal contra as entradas do ficheiro *users*. Se a contrasinal proporcionada polo cliente coincide coa que está almacenada, a autenticación será exitosa; se non, será rexeitada.

root@kali:~# useradd -m -d /home/ana -s /usr/bin/zsh ana #Crear o usuario *ana* co comando *useradd*, onde:

-d /home/ana → Xera a casa do usuario, é dicir, o directorio de traballo do usuario, no cartafol /home/ana
-m → Copia na casa do usuario o que exista no cartafol /etc/skel
-s /usr/bin/zsh → Establece como shell de traballo para o usuario a shell zsh
ana → Establece como nome de autenticación de usuario o nome ana
IMPORTANTE!: Non se establece contrasinal para o usuario ana

root@kali:~# useradd -m -d /home/brais -s /usr/bin/zsh brais #Crear o usuario *brais* co comando *useradd*, onde:

-d /home/brais → Xera a casa do usuario, é dicir, o directorio de traballo do usuario, no cartafol /home/brais
-m → Copia na casa do usuario o que exista no cartafol /etc/skel
-s /usr/bin/zsh → Establece como shell de traballo para o usuario a shell zsh
brais → Establece como nome de autenticación de usuario o nome brais
IMPORTANTE!: Non se establece contrasinal para o usuario brais

root@kali:~# freeradius -CX Comprobar se a configuración de freeradius é correcta(opción -C) e diagnosticar problemas no modo depuración(opción -X)

root@kali:~# /etc/init.d/freeradius status || systemctl status freeradius #Comprobar o estado do servidor FreeRADIUS, por defecto non está arrancado.

root@kali:~# /etc/init.d/freeradius start || systemctl start freeradius #Arrancar o servizo freeradius para ter en conta o cambio dos servidores realizado

root@kali:~# /etc/init.d/freeradius status || systemctl status freeradius #Comprobar o estado do servidor FreeRADIUS, agora debe estar arrancado.

root@kali:~# apt -y install freeradius-utils || apt-get -y install freeradius-utils #Instalar o paquete de nome *freeradius*. Co parámetro -y automaticamente asumimos yes a calquera pregunta que ocorra na instalación do paquete.

root@kali:~# radtest ana 1234 127.0.0.1 0 testing123 #Probar a autenticación dun usuario contra un servidor FreeRADIUS. Este comando permite enviar unha solicitude de autenticación ao servidor RADIUS para verificar se un usuario e o seu contrasinal son correctos e están configurados adecuadamente no servidor.

```
Sent Access-Request Id 81 from 0.0.0.0:36569 to 127.0.0.1:1812 length 73
        User-Name = "ana"
        User-Password = "1234"
        NAS-IP-Address = 127.0.0.1
        NAS-Port = 0
        Message-Authenticator = 0x00
        Cleartext-Password = "1234"
Received Access-Accept Id 81 from 127.0.0.1:1812 to 127.0.0.1:36569 length 38
        Message-Authenticator = 0x517050ebfa24fcef4d26fb89be9833ac
```

Explicación en detalle de cada parte:

- radtest: Este é o comando usado para realizar unha proba de autenticación RADIUS. É unha ferramenta de liña de comandos que vén incluída con FreeRADIUS e serve para enviar solicitudes de autenticación ao servidor.
- ana: Este é o nome de usuario que se está a probar. Neste exemplo, estamos tentando autenticar ao usuario "ana".
- 1234: Esta é a contrasinal que se está a enviar xunto co nome de usuario "ana". FreeRADIUS comparará esta contrasinal coa almacenada no seu sistema (por exemplo, no ficheiro users) para verificar se coincide.
- 127.0.0.1: Esta é a dirección IP do servidor FreeRADIUS ao que se envía a solicitude de autenticación. 127.0.0.1 é a dirección de "loopback" ou "localhost", o que significa que o servidor está executándose na mesma máquina onde se executa radtest.
- 0: Este é o número de porto NAS (Network Access Server). Aínda que en moitos casos este valor non se usa de forma práctica, ten que estar presente porque forma parte da estrutura da solicitude. Aquí, simplemente se pon 0.
- testing123: Esta é a "clave compartida" ou "shared secret" que se usa para autenticar a conexión entre o cliente (neste caso, radtest) e o servidor FreeRADIUS. Esta clave debe coincidir coa configurada no servidor FreeRADIUS para que a solicitude sexa aceptada.

root@kali:~# radtest ana 1234 192.168.120.100 0 ccbysa Similar ao comando anterior, pero agora non temos resposta afirmativa do servidor FreeRADIUS debido a que a "clave compartida" (ccbysa) está configurada para o cliente "kali-b" coa IP 192.168.120.120, e a petición estamos a realizala dende a IP 192.168.120.100

```
Sent Access-Request Id 19 from 0.0.0.0:51661 to 192.168.120.100:1812 length 73
        User-Name = "ana"
        User-Password = "1234"
        NAS-IP-Address = 127.0.0.1
        NAS-Port = 0
        Message-Authenticator = 0x00
        Cleartext-Password = "1234"
...
(0) No reply from server for ID 19 socket 3
```

root@kali:~# radtest brais abc123. 127.0.0.1 0 testing123 #Probar a autenticación dun usuario contra un servidor FreeRADIUS. Este comando permite enviar unha solicitude de autenticación ao servidor RADIUS para verificar se un usuario e o seu contrasinal son correctos e están configurados adecuadamente no servidor.

```
Sent Access-Request Id 163 from 0.0.0.0:47049 to 127.0.0.1:1812 length 75
        User-Name = "brais"
        User-Password = "abc123."
        NAS-IP-Address = 127.0.0.1
        NAS-Port = 0
        Message-Authenticator = 0x00
        Cleartext-Password = "abc123."
Received Access-Accept Id 163 from 127.0.0.1:1812 to 127.0.0.1:47049 length 38
        Message-Authenticator = 0x7787b9f3cb4b1329b42fb4bcf6b3dc7d
```

root@kali:~# radtest brais abc123. 192.168.120.100 0 ccbysa Similar ao comando anterior, pero agora non temos resposta afirmativa do servidor FreeRADIUS debido a que a "clave compartida" (ccbysa) está configurada para o cliente "kali-b" coa IP 192.168.120.120, e a petición estamos a realizala dende a IP 192.168.120.100

```
Sent Access-Request Id 247 from 0.0.0.0:47188 to 192.168.120.100:1812 length 75
        User-Name = "brais"
        User-Password = "abc123."
        NAS-IP-Address = 127.0.0.1
        NAS-Port = 0
        Message-Authenticator = 0x00
        Cleartext-Password = "abc123."
...
(0) No reply from server for ID 247 socket 3
```

5. Configurar SSH para autenticación mediante FreeRADIUS:

root@kali:~# apt -y install libpam-radius-auth || apt-get -y install libpam-radius-auth #Instalar o paquete de nome *libpam-radius-auth*. Co parámetro -y automaticamente asumimos yes a calquera pregunta que ocorra na instalación do paquete.

root@kali:~# echo '127.0.0.1 testing123 3
192.168.120.100 ccbysa 3' > /etc/pam_radius_auth.conf

#Esta configuración indica ao módulo pam_radius_auth que pode conectarse a dous servidores RADIUS diferentes (o servidor local en 127.0.0.1 e o servidor en 192.168.120.100) para autenticar usuarios. A clave compartida e o tempo de espera están definidos para cada servidor. Se o módulo PAM require autenticación RADIUS, intentará primeiro conectar ao servidor na primeira liña. Se non recibe resposta dentro dos 3 segundos, tentará conectar ao segundo servidor, segundo a configuración.

Explicación en detalle de cada parte:

- 127.0.0.1 testing123 3
  127.0.0.1: Especifica a IP do servidor RADIUS ao que se quere conectar. Aquí é 127.0.0.1, a dirección de "loopback" ou "localhost", o que significa que o servidor RADIUS está executándose na mesma máquina.
  testing123: Esta é a "shared secret" ou clave compartida entre o cliente (neste caso, o módulo PAM) e o servidor RADIUS. Esta clave debe coincidir coa configurada no servidor para que a conexión funcione.
  3: Este número representa o tempo de espera (timeout) en segundos. Indica canto tempo debe esperar o módulo PAM por unha resposta do servidor antes de dar erro ou intentar unha nova conexión.
- 192.168.120.100 ccbysa 3
  192.168.120.100: Esta é outra IP dun servidor RADIUS ao que o módulo pam_radius_auth pode conectarse. Aquí sería unha IP de rede local.
  cccbysa: Esta é a clave compartida para este segundo servidor, que debe coincidir coa que se configurou en FreeRADIUS para este cliente.
  3: Igual que no caso anterior, representa o tempo de espera en segundos.

root@kali:~# sed -i '2i auth sufficient pam_radius_auth.so' /etc/pam.d/sshd Modificar o ficheiro /etc/pam.d/sshd insertando na segunda liña *auth sufficient pam_radius_auth.so*. Este ficheiro controla a configuración de autenticación do servizo SSH usando PAM (Pluggable Authentication Modules):

- auth sufficient: Este é o control que indica a PAM que, se a autenticación con pam_radius_auth.so é exitosa, non precisará máis métodos de autenticación (a menos que haxa outros requisitos).
- pam_radius_auth.so: É o módulo que permite a autenticación a través de RADIUS. Esta liña engade o módulo pam_radius_auth.so á configuración de SSH, permitindo que o sistema use autenticación RADIUS para iniciar sesión por SSH.

Tras modificar PAM → NON é necesario recargar/reiniciar o servizo SSH

Máquina B: Arrancar coa Kali Live amd64

6. Na contorna gráfica abrir un terminal e executar:
   kali@kali:~$ setxkbmap es #Cambiar o mapa de teclado ao idioma español.

7. Configurar a rede:
   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 || systemctl stop avahi-daemon #Parar o demo avahi-daemon(control resolución de nomes) para poder configurar de forma manual a configuración de rede e non ter conflicto 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 conflicto con este xestor.
   root@kali:~# 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@kali:~# ip addr add 192.168.120.120/24 dev eth0 #Configurar a tarxeta de rede interna eth0, coa IP: 192.168.120.100 e máscara de subrede: 255.255.255.0.
   root@kali:~# 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).
   - Se a interface eth0 non está UP, é dicir, está en estado DOWN, executar:
     root@kali:~# ip link set up dev eth0 && ip addr show eth0
   root@kali:~# ping -c4 192.168.120.100 #Comprobar mediante o comando ping a conectividade coa máquina A
   root@kali:~# exit #Saír da consola local sudo na que estabamos a traballar para voltar á consola local de **kali**.

8. Acceso ao servidor SSH mediante autenticación FreeRADIUS:
   kali@kali:~$ ssh -v ana@192.168.120.100 #Comprobar se o servidor SSH está activo e podemos conectarnos a el dende a máquina B co contrasinal para ana configurado en FreeRADIUS: 1234. Se é a primeira ver 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.
   ana@kali:~$ exit #Saír da consola remota ssh a que acabamos de acceder mediante autenticación FreeRAIDUS, para voltar á consola local de **kali** na máquina B.
   kali@kali:~$ ssh -v brais@192.168.120.100 #Comprobar se o servidor SSH está activo e podemos conectarnos a el dende a máquina B co contrasinal para brais configurado en FreeRADIUS: "abc123." Se é a primeira ver 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.
   brais@kali:~$ exit #Saír da consola remota ssh a que acabamos de acceder mediante autenticación FreeRAIDUS, para voltar á consola local de **kali** na máquina B.

Ricardo Feijoo Costa