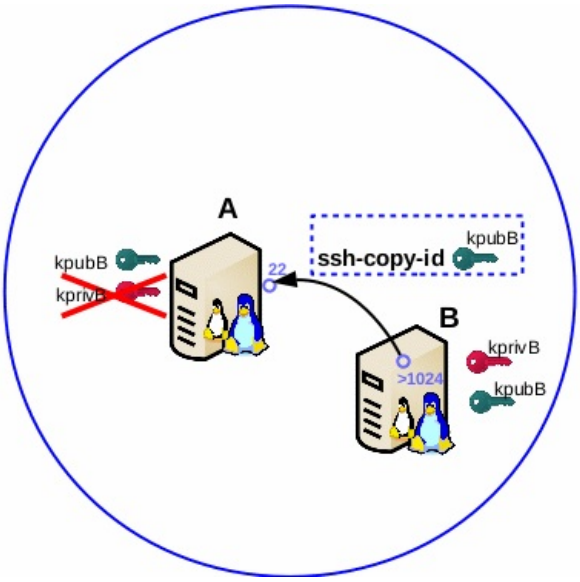
Cifrado asimétrico
Conexión Remota mediante SSH sen contrasinal

ESCENARIO

Máquinas virtuais ou físicas:
RAM ≤ 2048MB CPU ≤ 2 PAE/NX habilitado
Rede: 192.168.120.0/24
BIOS: Permite arranque dispositivo extraíble: CD/DVD, USB

Máquina A:
Servidor SSH
IP/MS: 192.168.120.100/24
SO: Kali Live amd64
Usuario: kali
Contrasinal: abc123.
id_rsa.pub=kpubB

Máquina B:
Cliente SSH
IP/MS: 192.168.120.101/24
SO: Kali Live amd64
Usuario: kali
Contrasinal: kali
id_rsa.pub = kpubB
id_rsa = kprivB



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)**
- Cliente ssh Microsoft Windows: **putty**
- Documentación sobre **putty**

Práctica Cifrado asimétrico - Conexión Remota mediante SSH sen contrasinal

Máquina A: Arrancar coa Kali Live amd64

1. Pór contrasinal ao usuario, co que arranca a live, de nome: kali
   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. 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 #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 192.168.120.100/24 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) 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 interface de rede local eth0

3. Comprobar estado do Servidor SSH:

root@kali:~# /etc/init.d/ssh status #Comprobar o estado do servidor SSH, por defecto non está arrancado.
root@kali:~# 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@kali:~# 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@kali:~# 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@kali:~# 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@kali:~# /etc/init.d/ssh start #Arrancar o servidor SSH.
root@kali:~# /etc/init.d/ssh status #Comprobar o estado do servidor SSH, agora debe estar arrancado.
root@kali:~# find /etc/rc* -name "*ssh*" #Busca polas links runlevels nos cartafoles /etc/rc*
root@kali:~# systemctl enable ssh #Permite que o servizo ssh sexa iniciado no arranque xerando os links nos runlevels (/etc/rcX.d)
root@kali:~# find /etc/rc* -name "*ssh*" #Busca polas links runlevels nos cartafoles /etc/rc*
root@kali:~# systemctl is-enabled ssh.service #Amosa se o servizo ssh está enabled ou disabled
root@kali:~# 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@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. 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.

Máquina B: Arrancar coa Kali Live amd64

4. Na contorna gráfica abrir un terminal e executar:

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

5. 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 #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 192.168.120.101/24 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**.

6. Configurar cifrado asimétrico:

kali@kali:~$ ssh-keygen -t rsa #Crear un par de chaves: pública e privada. No comando emprégase o algoritmo de cifrado rsa (Rivest, Shamir y Adleman), que por defecto a non ser que o modifiquemos co parámetro -b nº_bits é de 2048bits.

- Debemos elixir o cartafol onde gardar as chaves e o nome destas. Pulsamos Enter para deixar por defecto o cartafol .ssh/ e o nome id_rsa dentro do HOME do usuario: /home/kali.
- Passphrase nulo. Se aquí pomos un contrasinal, frase ou similar, cando queiramos conectarnos ao Servidor SSH en vez de pedir o contrasinal do usuario da conexión pedirá iste passphrase, mais como cando queremos conectarnos queremos facelo de forma directa sen petición de contrasinal ou passphrase, entón pulsamos 2 veces Enter para que a conexión se faga sen contrasinal.
- Chave pública e privada creadas. Fingerprint. Creáronse no cartafol anteriormente indicado a chave privada id_rsa e a chave pública id_rsa.pub. Tamén creouse o fingerprint da chave pública, e dicir, a identificación inequívoca da chave pública correspondente ao usuario kali deste equipo.

kali@kali:~$ ls -lahtr $HOME/.ssh #Executar o comando ls dentro do cartafol de traballo do usuario ($HOME=/home/kali) coas opcións -l, -a, -h, -t e -r. A opción -l permite amosar de forma extendida o atopado (tipo de ficheiro, permisos, propietarios...), a opción -h engade unha letra indicativa de tamaño, tal como M para megabytes binarios (`mebibytes'), a cada tamaño. A opción -t clasifica polo tempo de modificación (o `mtime' no inodo) en vez de alfabeticamente, cos ficheros máis recientes en primeiro lugar. A opción -r clasifica en orde inversa. Polo tanto, o comando lista ficheiros e directorios do directorio /home/kali amosando de abaixo hacia arriba os máis recentes e en formato de lectura de tamaño máis amigable para as persoas (K, M, G...)

De interese: Comprobar os **permisos** dos ficheiros: **id_rsa**, **id_rsa.pub, authorized_keys**

kali@kali:~$ ssh-copy-id -i .ssh/id_rsa.pub kali@192.168.120.100 #Copia da chave pública ao Servidor SSH. Para poder establecer a conexión sen contrasinal enviamos unha copia da chave pública ao Servidor SSH. Soamente será posible establecer unha conexión sen contrasinal se posuimos a parella desa chave pública, que non é outra que a chave privada, polo cal, nunca deberiamos desprendernos da chave privada, xa que sen ela a conexión non sería posible ou outro usuario podería suplantarnos no caso de facerse coa chave privada.

- Password usuario kali: Como aínda non temos copiada a chave pública nesta conexión pídese o contrasinal do usuario co cal queremos conectarnos ao Servidor SSH: kali. A password do usuario kali é **abc123.** (Ollo que o contrasinal ten un caracter punto final)
- Agora a conexión sen contrasinal será posible para o usuario kali, con todos os permisos deste usuario, na máquina Servidor SSH (192.168.120.100).

kali@kali:~$ ls -lahtr $HOME/.ssh #Executar o comando ls dentro do cartafol de traballo do usuario ($HOME=/home/kali) coas opcións -l, -a, -h, -t e -r. A opción -l permite amosar de forma extendida o atopado (tipo de ficheiro, permisos, propietarios...), a opción -h engade unha letra indicativa de tamaño, tal como M para megabytes binarios (`mebibytes'), a cada tamaño. A opción -t clasifica polo tempo de modificación (o `mtime' no inodo) en vez de alfabeticamente, cos ficheros máis recientes en primeiro lugar. A opción -r clasifica en orde inversa. Polo tanto, o comando lista ficheiros e directorios do directorio /home/kali amosando de abaixo hacia arriba os máis recentes e en formato de lectura de tamaño máis amigable para as persoas (K, M, G...)

De interese: Comprobar os **permisos** dos ficheiros: **id_rsa**, **id_rsa.pub, authorized_keys**

kali@kali:~$ ssh -v kali@192.168.120.100 #Comprobar se o servidor SSH está activo e podemos conectarnos a el dende a máquina B sen contrasinal, a través de cifrado asimétrico. 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 mediante cifrado asimétrico, para voltar á consola local de **kali** na máquina B.

kali@kali:~$ ssh -v -i .ssh/id_rsa kali@192.168.120.100 #Comprobar se o servidor SSH está activo e podemos conectarnos a el dende a máquina B sen contrasinal, a través de cifrado asimétrico. Agora indícase onde se pode atopar a clave privada para a autenticación mediante a opción **-i**

kali@kali:~$ exit #Saír da consola remota ssh a que acabamos de acceder mediante cifrado asimétrico, para voltar á consola local de **kali** na máquina B.

Ricardo Feijoo Costa