xUNIVERSIDAD TECNOLÓGICA DE PANAMÁ

FACULTAD DE INGENIERÍA DE SISTEMAS COMPUTACIONALES

DEPARTAMENTO DE PROGRAMACIÓN DE COMPUTADORAS

LICENCIATURA EN CIBERSEGURIDAD

CRIPTOGRAFÍA

LABORATORIO#2

PERTENECE A:

POLANCO, OMAR 8-1014-120

PROFESOR:

MORENO, JOSE

GRUPO:

1S3121

II SEMESTRE

2024

Índice

Introducción

En la actualidad, la conexión remota segura a servidores y dispositivos es una necesidad fundamental en cualquier entorno de TI. El protocolo SSH (Secure Shell) se ha consolidado como una de las principales herramientas para este fin, garantizando una comunicación cifrada y segura. Sin embargo, el uso de contraseñas puede ser tedioso y, en algunos casos, poco seguro si no se gestionan adecuadamente.

En este laboratorio, aprenderemos cómo configurar conexiones SSH sin necesidad de contraseñas, utilizando autenticación basada en llaves públicas y privadas. A lo largo de este proceso, se seguirán tres pasos sencillos que nos permitirán establecer conexiones seguras y automatizadas entre sistemas, mejorando la eficiencia y seguridad de las operaciones remotas.

Paso#1

A continuación, aprenderemos cómo configurar una conexión desde PC#1 hacia PC#2 sin necesidad de ingresar una contraseña, utilizando solo tres pasos:

La situación es la siguiente:

- **PC#1:** Es la máquina que desea conectarse a PC#2 sin tener que ingresar una contraseña en cada intento de conexión.
- **PC#2:** Esta máquina tiene instalado un servidor SSH y será el destino de la conexión desde PC#1. En PC#2, existe un usuario llamado root.

En la **PC#1**, escribiremos lo siguiente:

```
ssh-keygen -b 4096 -t rsa
```

Esto generara nuestra llave pública.

Paso#2

Al haber hecho el paso#1, nos aparecera algo asi:

```
Generating public/private rsa key pair.
Enter file in which to save the key (/Users/omars/.ssh/id_rsa):
```

Simplemente presionaremos 3 veces [Enter], sin escribir absolutamente nada, tal que así:

```
Generating public/private rsa key pair.
Enter file in which to save the key (/Users/omars/.ssh/id_rsa):
/Users/omars/.ssh/id_rsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /Users/omars/.ssh/id_rsa
Your public key has been saved in /Users/omars/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:snqlHcix9ne9tLnGtnzMkB5n3/nIHbkU5KcimfnS0f4 omars@MacBook-Pro-3.local
The key's randomart image is:
+---[RSA 4096]----+
|                 |
|                 |
|               . |
|      .       o  |
|     ..+S    . +.|
|      =oo  +. =.*|
|     ..= .=..*o@+|
|     .o o ooo=O*O|
|    ..   . o.oXBE|
+----[SHA256]-----+
```

Y listo, tendremos nuestra llave pública.

Ahora debemos enviarle esta llave a la persona que queramos para poder acceder al servidor sin contraseña, en este caso, al profesor.

Paso#3

Luego de haberle enviado la llave pública, debemos tener el acceso al servidor con el siguiente comando:

```
ssh root@65.20.82.223
```

¡Y listo!

Tenemos acceso al servidor sin contraseña.

```
*** System restart required ***
Last login: Tue Aug 27 14:08:46 2024 from 34.138.227.128
root@poc:~#
```

Conclusión

Implementar conexiones SSH sin contraseña es un método eficaz para mejorar la seguridad y comodidad en la gestión remota de servidores. A través de los tres sencillos pasos descritos, hemos configurado con éxito la autenticación basada en llaves, eliminando la necesidad de ingresar contraseñas repetidamente. Esto no solo simplifica el proceso de conexión, sino que también reduce el riesgo asociado al uso de contraseñas, fortaleciendo la protección de nuestras infraestructuras. Con esta configuración, hemos dado un paso importante hacia la automatización y seguridad en la administración de sistemas remotos.