CONFIGURACIÓN PARA CREAR UN PORTKNOCKING EN SSH DEL PUERTO 22

Vamos a configurar el Port Knocking en un servidor Linux para abrir el puerto SSH (22) mediante una secuencia de golpes de puertos. Asegúrate de tener acceso root o privilegios de sudo para seguir estos pasos.

Actualizar Repositorios:

```
$ sudo apt-get update
```

Instalar Knockd e iptables-persistent:

```
$ sudo apt install knockd
```

```
$ sudo apt-get install knockd iptables-persistent
```

Configurar Firewall:
Bloquea el puerto SSH (22) y acepta conexiones establecidas y relacionadas:

```
$ sudo iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
$ sudo iptables -A INPUT -p tcp --dport 22 -j DROP
$ sudo iptables-save > /etc/iptables/rules.v4
```

Configurar Knockd:
Edita el archivo de configuración de Knockd:

```
$ sudo nano /etc/knockd.conf
```

Y modifica las secciones [openSSH] y [CloseSSH] como se muestra a continuación:

==========

```
[options]
    logfile = /var/log/knockd.log
    Interface     = enp0s3

[openSSH]
    sequence      = 8375,0386,1904
    seq_timeout   = 5
    start_command = /sbin/iptables -I INPUT -s %IP% -p tcp --dport 22 -j ACCEPT
    tcpflags      = syn

[closeSSH]
    sequence      = 1000,2000,3000
```

```
    seq_timeout   = 5
    start_command = /sbin/iptables -D INPUT -s %IP% -p tcp --dport 22
-j ACCEPT
    tcpflags      = syn
```

==========

Guarda los cambios y cierra el editor.

Para ver tu interfaz de red y así poderlo poner en los pasos anteriores, en mi caso es “enp0s3”

```
$ ip addr
```

Configurar Knockd para que arranque al iniciar:
Edita el archivo de configuración:

```
$ sudo nano /etc/default/knockd
```

Y modifica START_KNOCKD=0 a START_KNOCKD=1.

Guarda los cambios y cierra el editor.

Inicia Knockd:

```
$ sudo systemctl start knockd
```

Verificar el estado de Knockd:
Puedes verificar si Knockd está en funcionamiento ejecutando:

```
$ sudo systemctl status knockd
```

Si todo está bien, deberías ver que está en ejecución.

Una vez configurado, puedes probar el Port Knocking enviando la secuencia de puertos (8375, 0386, 1904) desde otra terminal o dispositivo. Después de enviar la secuencia correctamente, el puerto SSH (22) debería abrirse temporalmente y podrás acceder al servidor a través de SSH.

Recuerda que, debido a la seguridad adicional proporcionada por el Port Knocking, necesitarás enviar la secuencia de puertos antes de intentar acceder al servidor a través de SSH.

CONFIGURARLO PARA QUE SE QUEDE PERMANENTE LA CONFIGURACIÓN DEL PORTKNOCKING:

Para asegurarte de que la configuración de knockd persista después de reiniciar el servidor, es importante realizar algunos pasos adicionales para guardar la configuración y habilitar el servicio para que se

inicie automáticamente durante el arranque del sistema. Aquí tienes los pasos que debes seguir:

Guardar la configuración de iptables:

Después de configurar iptables para bloquear y permitir el tráfico según sea necesario para el Port Knocking, asegúrate de guardar la configuración actual para que se cargue automáticamente al reiniciar el sistema. Esto se hace típicamente con el comando:

```
$ sudo iptables-save > /etc/iptables/rules.v4
```

Esto guardará las reglas de iptables en un archivo persistente que se cargará durante el arranque del sistema.

Guardar la configuración de knockd:

Si has realizado cambios en el archivo de configuración de knockd (/etc/knockd.conf), asegúrate de guardar esos cambios. El archivo knockd.conf ya debería estar guardado en disco, pero si has realizado modificaciones, asegúrate de guardarlas antes de continuar.

Habilitar el servicio knockd para que se inicie automáticamente:

Debes habilitar el servicio knockd para que se inicie automáticamente durante el arranque del sistema. Esto se hace con el siguiente comando:

```
$ sudo systemctl enable knockd
```

Esto configurará el servicio knockd para que se inicie automáticamente cada vez que se inicie el sistema.

Con estos pasos, la configuración de knockd debería persistir después de reiniciar el servidor. Verifica que todo esté configurado correctamente después de reiniciar el sistema para asegurarte de que knockd se inicie y funcione como se espera.