



PORT KNOCKING

BASTIONADO DE REDES Y SISTEMAS

ERIC SERRANO MARÍN
I.E.S MARTINEZ MONTAÑES
CETI

Contenido

Instalación Knockd en servidor.....	2
Configuración del fichero knock.conf.....	2
Explicación fichero knock.conf.....	2
Configuración del fichero knockd.	3
Explicación fichero knockd.....	3
Comandos para parar, iniciar y reiniciar knockd.....	4
Activación de Firewall y estado actual.....	4
Instalación de knockd en cliente.....	4
Comprobamos el funcionamiento.....	4
Explicación del comando knock -v	5
Gif del funcionamiento	5
CONCLUSIÓN	5

Instalación Knockd en servidor.

```
root@ubuntu14:/home/usuario# apt install knockd
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  knockd
0 upgraded, 1 newly installed, 0 to remove and 64 not upgraded.
Need to get 28,9 kB of archives.
After this operation, 176 kB of additional disk space will be used.
Get:1 http://es.archive.ubuntu.com/ubuntu/ trusty/universe knockd amd64 0.5-3ubuntu1 [28,9 kB]
Fetched 28,9 kB in 0s (78,1 kB/s)
Selecting previously unselected package knockd.
```

Configuración del fichero knock.conf

```
[openWeb]
sequence      = 7777,8888,9999,12345
seq_timeout   = 30
command       = /sbin/iptables -A INPUT -s %IP% -p tcp --dport 80 -j ACCEPT
tcpflags      = syn

[closeWeb]
sequence      = 12345,9999,8888,7777
seq_timeout   = 30
command       = /sbin/iptables -D INPUT -s %IP% -p tcp --dport 80 -j ACCEPT
```

Explicación fichero knock.conf

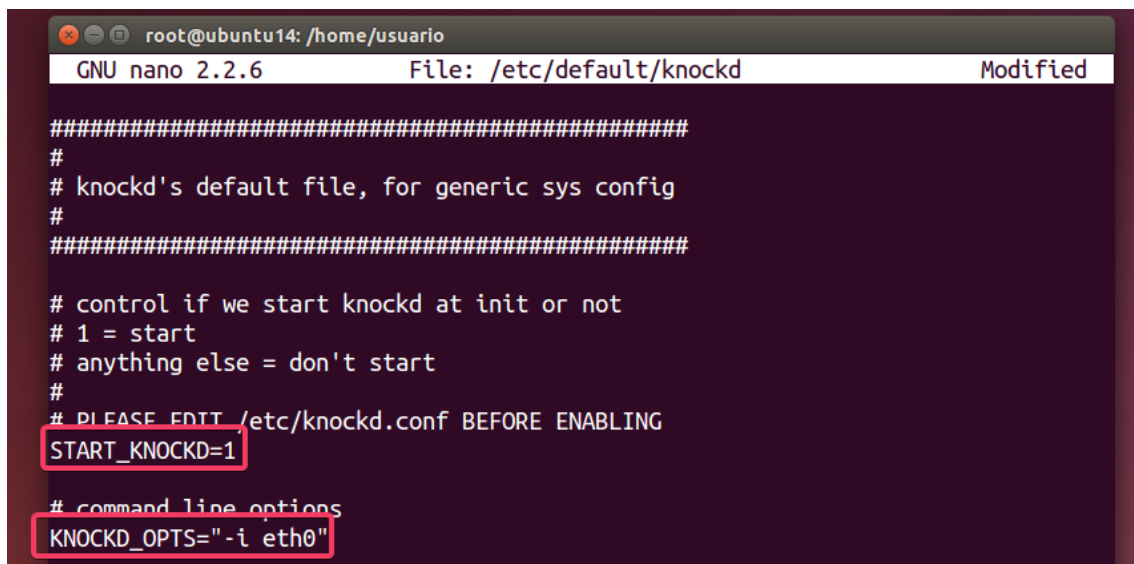
- **[openWeb]:**
 - **Secuencia de Knock:** Especificamos como una serie de puertos: 7777, 8888, 9999 y 12345.
 - **Sq_Timeout:** Define cuánto tiempo debe esperar el sistema después de recibir la secuencia antes de realizar la acción.
 - **Command:** Cuando se recibe la secuencia especificada, se ejecuta el comando. En este caso el comando agrega una regla a iptables para permitir el tráfico entrando al puerto 80 desde la dirección IP del cliente que envió la secuencia de Knock.
- **[closeWeb]:**
 - En este caso se especifica como 12345, 9999, 8888 y 7777, totalmente a la inversa.

- También está establecido en 30 segundos.
- En este caso, el comando elimina la regla de iptables que permite el tráfico entrante al puerto 80 desde la dirección IP del cliente que envió la secuencia de Knock.

Resumidamente, el bloque [openWeb] abre el acceso al puerto 80 cuando se recibe la secuencia de puertos especificada (7777,8888,9999,12345), mientras que el bloque [closeWeb] cierra el acceso al puerto 80 cuando se recibe otra secuencia de puertos especificada (12345,9999,8888,7777).

Esto proporciona una capa adicional de seguridad al restringir el acceso al servidor web a través de un mecanismo de “tocar puertos” antes de permitir el acceso.

Configuración del fichero knockd.



```
root@ubuntu14: /home/usuario
GNU nano 2.2.6      File: /etc/default/knockd      Modified

#####
#
# knockd's default file, for generic sys config
#
#####

# control if we start knockd at init or not
# 1 = start
# anything else = don't start
#
# PLEASE EDIT /etc/knockd.conf BEFORE ENABLING
START_KNOCKD=1

# command line options
KNOCKD_OPTS="-i eth0"
```

Explicación fichero knockd.

START_KNOCKD = 1: para que se inicie automáticamente durante el arranque del sistema, en caso de que este configurado correctamente en knock.conf, mientras que **KNOCKD_OPTS** para decirle la interfaz de red en la que debe escuchar.

Comandos para parar, iniciar y reiniciar knockd.

```

root@ubuntu14:/home/usuario# service knockd stop
* Stopping Port-knock daemon knockd [ OK ]
root@ubuntu14:/home/usuario# service knockd start
* Starting Port-knock daemon knockd [ OK ]
root@ubuntu14:/home/usuario# service knockd restart
* Stopping Port-knock daemon knockd [ OK ]
* Starting Port-knock daemon knockd [ OK ]
root@ubuntu14:/home/usuario#

```

Activación de Firewall y estado actual.

```

root@ubuntu14:/home/usuario# sudo ufw enable
Firewall is active and enabled on system startup
root@ubuntu14:/home/usuario# ufw status numbered
Status: active
root@ubuntu14:/home/usuario#

```

Instalación de knockd en cliente.

```

(root@kali)-[/home/kali]
# apt install knockd
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer require
d:

```

Comprobamos el funcionamiento.

```

(root@kali)-[/home/kali]
# curl 192.168.1.135
^C
Podemos observar que no nos abre el puerto 80

(root@kali)-[/home/kali]
# knock -v 192.168.1.135 7777 8888 9999 12345
hitting tcp 192.168.1.135:7777
hitting tcp 192.168.1.135:8888
hitting tcp 192.168.1.135:9999
hitting tcp 192.168.1.135:12345
Hacemos el knock para abrir el puerto 80

(root@kali)-[/home/kali]
# curl 192.168.1.135
Nos abre correctamente el puerto

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
  <!--
    Modified from the Debian original for Ubuntu
    Last updated: 2014-03-19
    See: https://launchpad.net/bugs/1288690
  -->
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
    <title>Apache2 Ubuntu Default Page: It works</title>
    <style type="text/css" media="screen">

```

```

(root@kali)-[/home/kali]
# knock -v 192.168.1.135 12345 9999 8888 7777
hitting tcp 192.168.1.135:12345
hitting tcp 192.168.1.135:9999
hitting tcp 192.168.1.135:8888
hitting tcp 192.168.1.135:7777
Hacemos un knock con la secuencia inversa

(root@kali)-[/home/kali]
# curl 192.168.1.135
Observamos como se ha cerrado correctamente.

```

Explicación del comando knock -v

Este comando sirve para enviar una secuencia de “golpes” a un servidor que tiene configurado knockd. Cada “golpe” intenta conectarse a un puerto específico en el servidor en un orden particular, según la combinación establecida en nuestro archivo knockd.conf, hará una cosa u otra.

Gif del funcionamiento: <https://i.imgur.com/qMo5p1N.gif>

CONCLUSIÓN

Después de usar Knockd, he comprendido cómo mejorar la seguridad de un servidor usando Port Knocking, una técnica que requiere una cadena de conexión de puerto específica para permitir el acceso.

Esta práctica me ha enseñado la importancia de proteger los servicios y me ha ayudado a desarrollar mis habilidades en la configuración de sistemas y resolución de problemas, ya que he tenido que pelearme bastante con ella para que la práctica funcionase correctamente.