knockd

demonio que escucha en unos puertos determinados una secuencia determinada para realizar una serie de acciones
normalmente, se abre de manera temporal algún puerto (como de gestión remota)

instalacion

```
aptitude install -y knockd
```

configuración

arrancar el demonio:

/etc/default/knockd

```
START_KNOCKD=1
```

/etc/knockd.conf

```
[options]
        UseSyslog

[opencloseSSH]
        sequence    = 7000,8000,9000
        seq_timeout = 5
        start_command     = /sbin/iptables -A INPUT -s %IP% -p tcp --dport 22 -j ACCEPT
        stop_command     = /sbin/iptables -D INPUT -s %IP% -p tcp --dport 22 -j ACCEPT
        tcpflags    = syn
        cmd_timeout = 20
```

antes se ha tenido que aplicar un cierre de puertos y un mantener conexiones ya establecidas en IPTABLES

cliente

```
knock <servidor> 7000 8000 9000 && ssh user@servidor
```

enlaces

- http://www.zeroflux.org/projects/knock