The sys admin's daily grind: Knockd

KNOCK-KNOCK

Horror stories are full of scary characters knocking on doors at night. On Linux, we just call this port knocking, and it can actually be quite useful.

BY CHARLY KÜHNAST

If you prefer not to have an obvious administrative port for your iptables firewall – but do need a secret one – port knocking is an interesting option that can put off script-based attacks. For the ambitious but secretive admin, the tool of choice is Knockd [1].

The package includes two components: Knock is the client that sends knocking signals, which the Knockd daemon receives.

Listing 1: /etc/knockd.conf

```
01 [options]
02    logfile = /var/log/knockd.
   log
03 [openSSH]
04    sequence    =
   7000,8000,9000
05    seq_timeout = 5
06    command     = /sbin/
   iptables -A INPUT -s %IP% -p
   tcp --dport 22 -j ACCEPT
07    tcpflags    = syn
08 [closeSSH]
09    sequence    =
   9000,8000,7000
10    seq_timeout = 5
11    command     = /sbin/
   iptables -D INPUT -s %IP% -p
   tcp --dport 22 -j ACCEPT
12    tcpflags    = syn
```


Knocking

To monitor the process, Knock, the knocking client, only needs the port number on which to knock and a *-v* option.

For example:

```
knock -v 10.0.0.42 ➥
7000 8000 9000
```

The tool responds immediately with the command-line output shown in Figure 1.

The */etc/knockd.conf* configuration file lets the system administrator specify the action the daemon performs when it receives a valid hit.

See Listing 1 for an example.

In a production environment, choose a more unusual port number, of course.

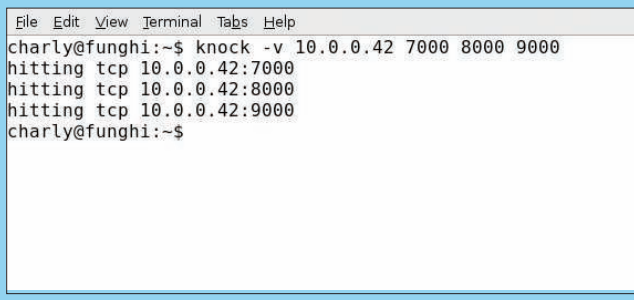

Figure 1: If it recognizes the knock signal, the tool responds.

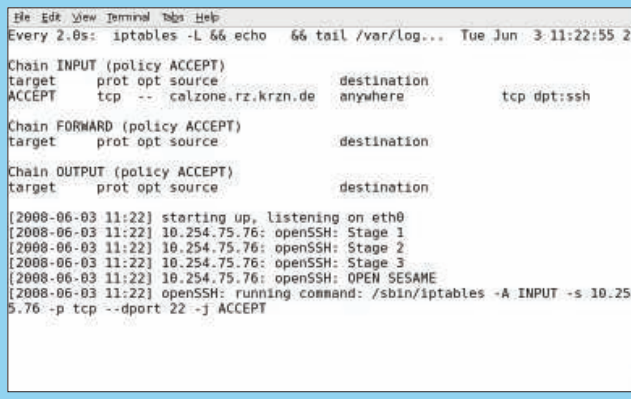

Figure 2: The Knockd daemon uses iptables to open up port 22 for the requesting IP, but only if it recognizes the knock signal.

Morse Code for Fun and Profit

If it recognizes the signal, Knockd opens up port 22 for the requesting IP, which passes in its own IP (see Figure 2).

If you knock on the ports in the wrong order, the daemon will shut down SSH access. Scatterbrained admins (like me) have another option – *knockd.conf*, which looks like this:

```
start_command = ➥
/usr/sbin/iptables ➥
-A INPUTU
 -s %IP% -p tcp --syn ➥
 --dport 22 -j ACCEPT
cmd_timeout   = 10
stop_command  ➥
= /usr/sbin/iptables -D INPUTU
 -s %IP% -p tcp --syn ➥
 --dport 22 -j ACCEPT
```

After knocking, the daemon launches *start_command*, then waits the number of minutes specified in *cmd_timeout* before executing *stop_command*.

Conclusion

Really paranoid system administrators will relish the option of configuring a file with a sequence of ports. Each sequence expires after use. ■

THE AUTHOR

Charly Kühnast is a Unix operating system administrator at the Data Center in Moers, Germany. His tasks include firewall and DMZ security and availability. He divides his leisure time into hot, wet, and eastern sectors, where he enjoys cooking, fresh water aquariums, and learning Japanese, respectively.

INFO

[1] Knockd: *http://www.zeroflux.org/cgi-bin/cvstrac.cgi/knock/wiki*