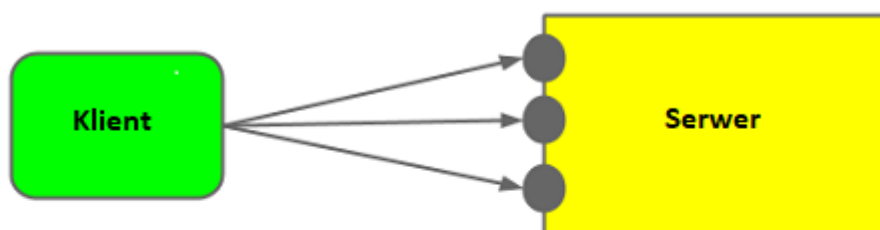


# Knocking

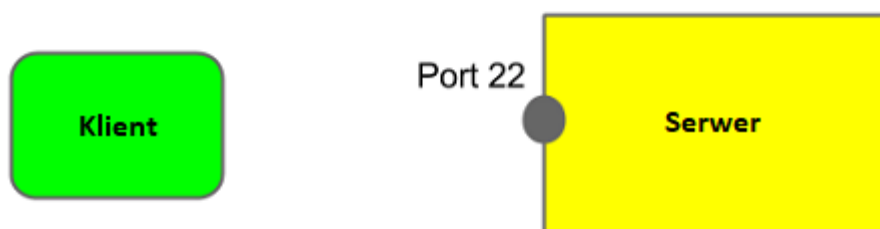
written by archi | 16 kwietnia 2021

Pukanie do portów to proces polegający na wykonaniu określonej liczby połączeń (wykonanie połączenia SYN) na różne porty, aby proces nasłuchujący knockd wykonał zdefiniowane polecenie np. otwarcie portu komunikacyjnego dla adresu wywołującego.

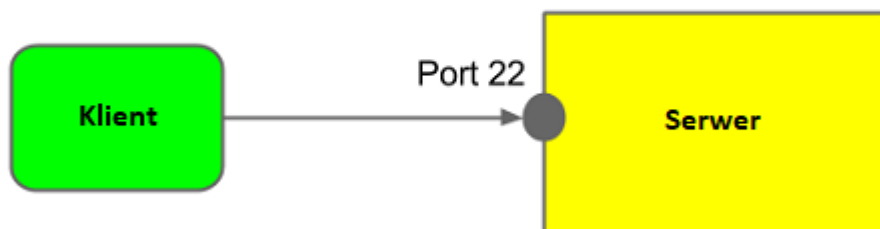
Przykład wykonania prośby otwarcia portu 22 dla wywołującego klienta:



**Krok 1: Klient wykonuje połączenia na wyznaczone porty**



**Krok 2: Serwer otwiera port 22**



**Krok 3: Możesz wykonać połączenie do portu 22**

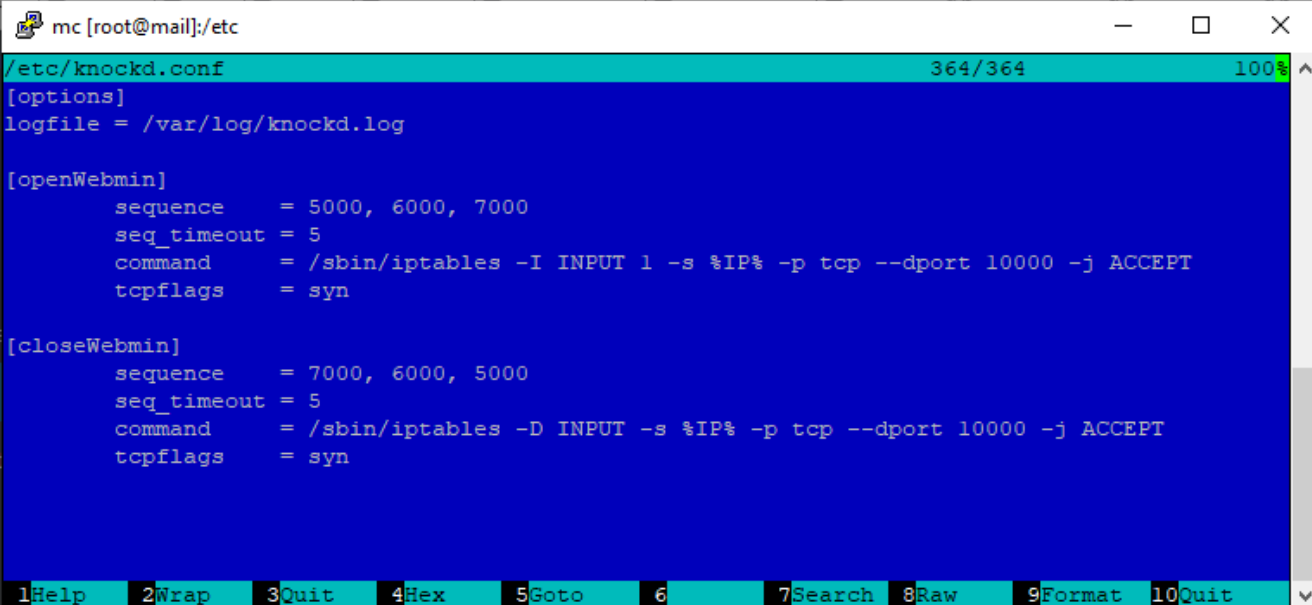
W laboratorium przygotujemy wykonanie otwarcia i zamknięcia portu 10000 (Webmin) dla wywołującego klienta po sekwencji wysłania żądania SYN na

porty 5000, 6000, 7000. Wykonanie tej samej sekwencji w odwrotnej kolejności spowoduje zamknięcie otwartego portu na firewall.

1. W celu uruchomienia procesu nasłuchującego zainstaluj:

```
knockd
```

2. Edytuj plik `/etc/knockd.conf` i zdefiniuj kombinację portów po której nastąpi odblokowanie dostępu do serwera. Ustaw kombinację portów 5000, 6000, 7000 jako odblokowanie usługi (włączenie) oraz 7000,6000,5000 jako wyłączenie usługi.



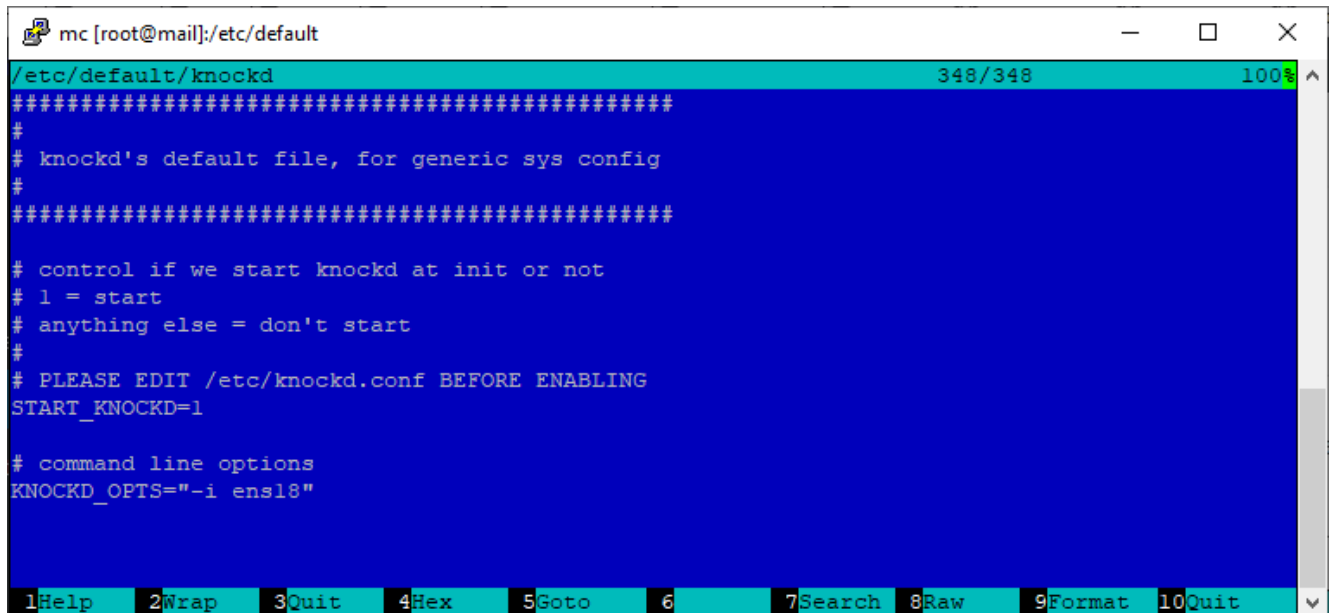
```
mc [root@mail]:/etc
/etc/knockd.conf 364/364 100%
[options]
logfile = /var/log/knockd.log

[openWebmin]
sequence = 5000, 6000, 7000
seq_timeout = 5
command = /sbin/iptables -I INPUT 1 -s %IP% -p tcp --dport 10000 -j ACCEPT
tcpflags = syn

[closeWebmin]
sequence = 7000, 6000, 5000
seq_timeout = 5
command = /sbin/iptables -D INPUT -s %IP% -p tcp --dport 10000 -j ACCEPT
tcpflags = syn

1Help 2Wrap 3Quit 4Hex 5Goto 6 7Search 8Raw 9Format 10Quit
```

3. Edytuj plik `/etc/default/knockd` i włącz startowanie nasłuchiwanie knockd „`START_KNOCKD=1`” oraz ustaw interfejs na którym ma nasłuchiwać np. `KNOCKD_OPTS="-i ens18"`. Sprawdź nazwę interfejsu poleceniem `ifconfig` lub `ip a` i zobacz jego nazwę. Interfejs, który posiada właściwy adres IP twojej maszyny wirtualnej.



```
mc [root@mail]:/etc/default
/etc/default/knockd 348/348 100%
#####
#
# 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 ens18"
1Help 2Wrap 3Quit 4Hex 5Goto 6 7Search 8Raw 9Format 10Quit
```

4. Wykonaj restart usługi: `service knockd restart`

## Testowanie

1. Pobierz oprogramowanie do wykonywania połączeń typu knock. To oprogramowanie nie jest niezbędne. Można dokonać takich połączeń z wykorzystaniem programów np.: telnet, pytty, itp. wykonując kolejne połączenia na określone porty.

Program [PortKnock.zip](#)

2. Rozpakuj i uruchom program `portknock.exe` i zdefiniuj akcje włączającą i wyłączającą.

The screenshot shows a web browser window titled "GregSowell.com Port Knock". The interface includes a large text area labeled "Description" at the top. Below it, there are input fields for "IP" and "Desc". Underneath these, there is a table with four rows, each with a "Type" dropdown menu (all set to "None"), a "Port" input field, and a "Text" input field. At the bottom of the interface, there are three buttons: "Knock", "Add/Update", and "Delete".

	Type	Port	Text
1	None		
2	None		
3	None		
4	None		

- podaj adres IP maszyny wirtualnej
- zdefiniuj nazwę akcji (DESC)
- podaj kolejne porty do odblokowania

Następnie zdefiniuj akcję blokującą

3. Przetestuj działanie. Odblokowanie powinno wpisać twój adres IP na początku listy firewall (iptables), a blokowanie powinno usunąć ten wpis.

```
root@mail: ~  
Chain INPUT (policy ACCEPT)  
target      prot opt source                destination  
ACCEPT      tcp  --  1.1.1.1                0.0.0.0/0          tcp dpt:10000  
f2b-sasl    tcp  --  0.0.0.0/0              0.0.0.0/0  
f2b-Zimbra-recipient tcp --  0.0.0.0/0              0.0.0.0/0  
f2b-Zimbra-audit tcp --  0.0.0.0/0              0.0.0.0/0  
f2b-Zimbra-account tcp --  0.0.0.0/0              0.0.0.0/0  
f2b-Postfix tcp --  0.0.0.0/0              0.0.0.0/0          multiport dports 25  
f2b-webmin-auth tcp --  0.0.0.0/0              0.0.0.0/0          multiport dports 10000  
f2b-sshd    tcp  --  0.0.0.0/0              0.0.0.0/0          multiport dports 22  
ACCEPT      all  --  0.0.0.0/0              0.0.0.0/0  
ACCEPT      all  --  91.217.41.222           0.0.0.0/0  
ACCEPT      all  --  91.217.40.83            0.0.0.0/0  
ACCEPT      all  --  82.145.72.241           0.0.0.0/0  
ACCEPT      all  --  91.217.40.250           0.0.0.0/0  
ACCEPT      all  --  91.217.41.250           0.0.0.0/0  
ACCEPT      all  --  195.248.88.150          0.0.0.0/0  
ACCEPT      all  --  194.88.225.43           0.0.0.0/0  
ACCEPT      all  --  217.153.136.116         0.0.0.0/0  
:  
█
```