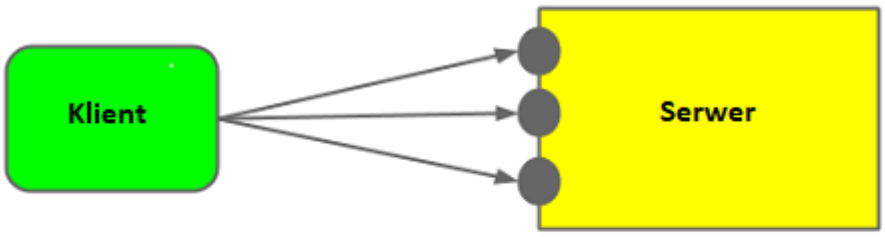
Knocking

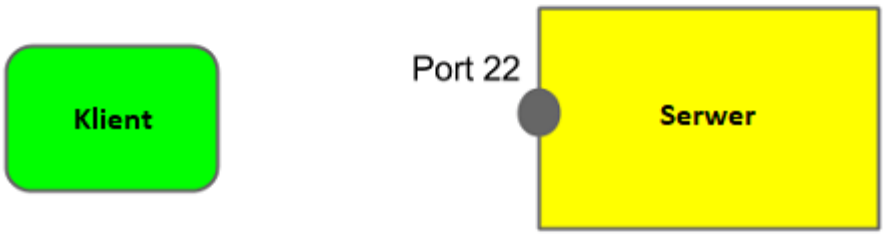
written by archi | 16 kwietnia 2021

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.

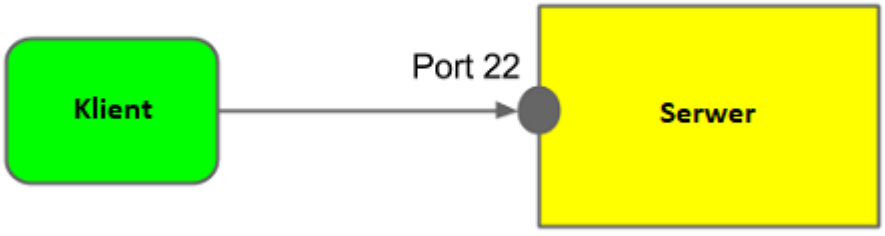
Przykład wykonania prośby otwarcia portu 22 dla wywołującego klienta:



Krok 1: Klient wykonuje połaczenia na wyznaczone porty



Krok 2: Serwer otwiera port 22



Krok 3: Możesz wykonać połaczenie do portu 22

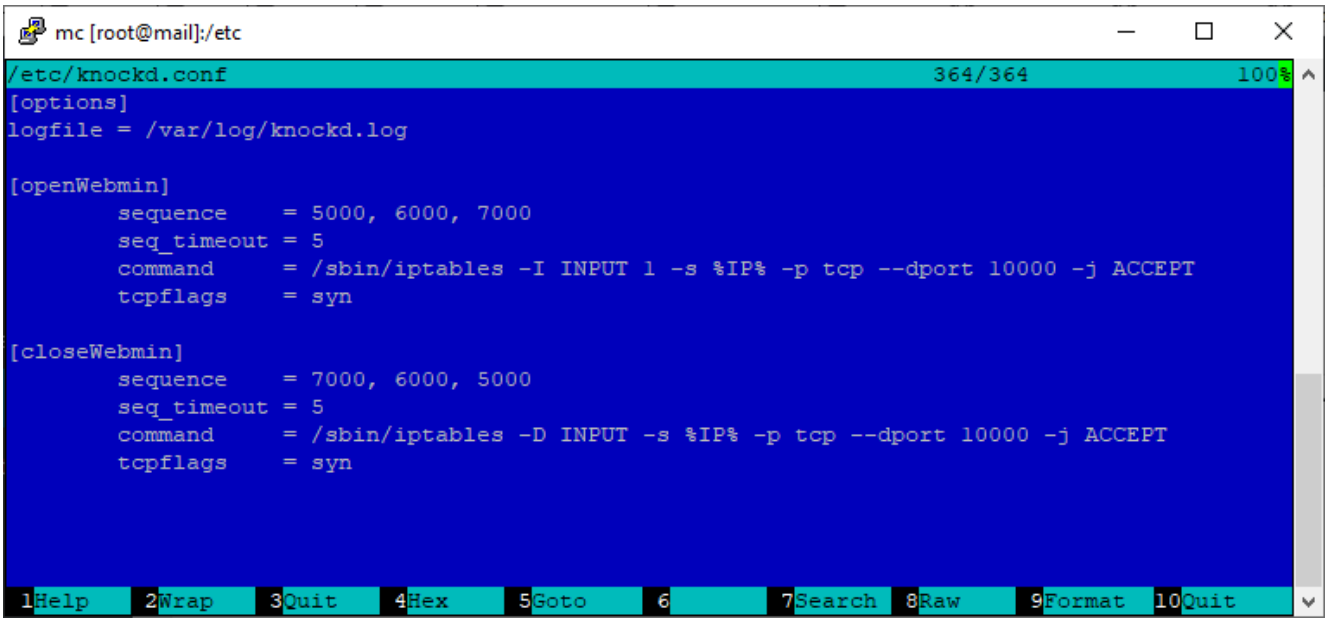
W laboratorium przygotujemy wykonanie otwarcia i zamknięcia portu 10000 (Webmin) dla wywołującego klienta po sekwecji wysłania żądania SYN na

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

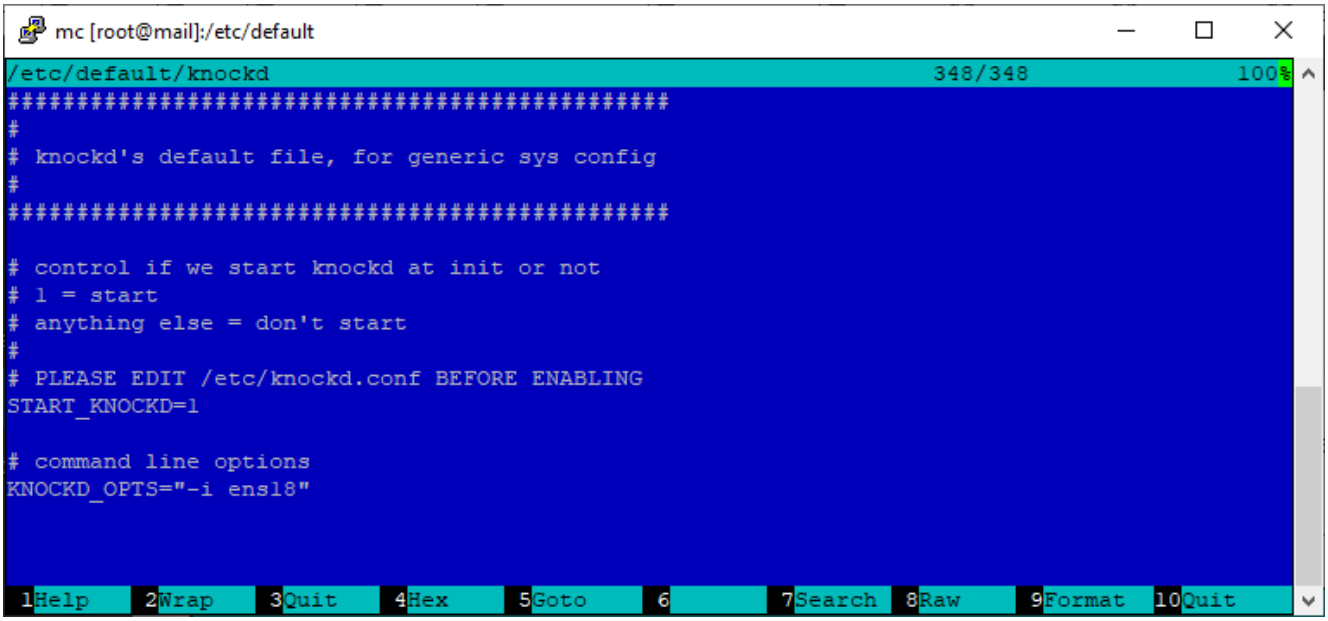
1. W celu uruchomienia procesu nasłuchującego zainstaluj:

```
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.



3. Edytuj plik `/etc/default/knockd` i włącz startowanie nasłuchiwania 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.



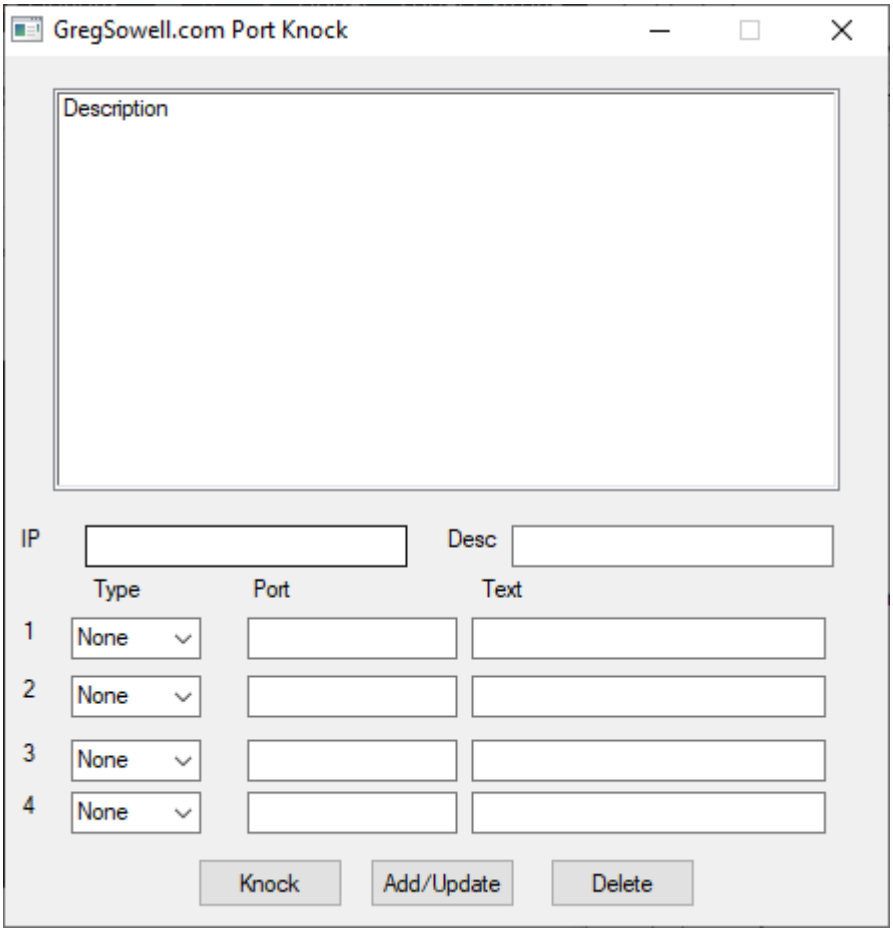
4. Wykonaj restart usługi: `service knockd restart`

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.



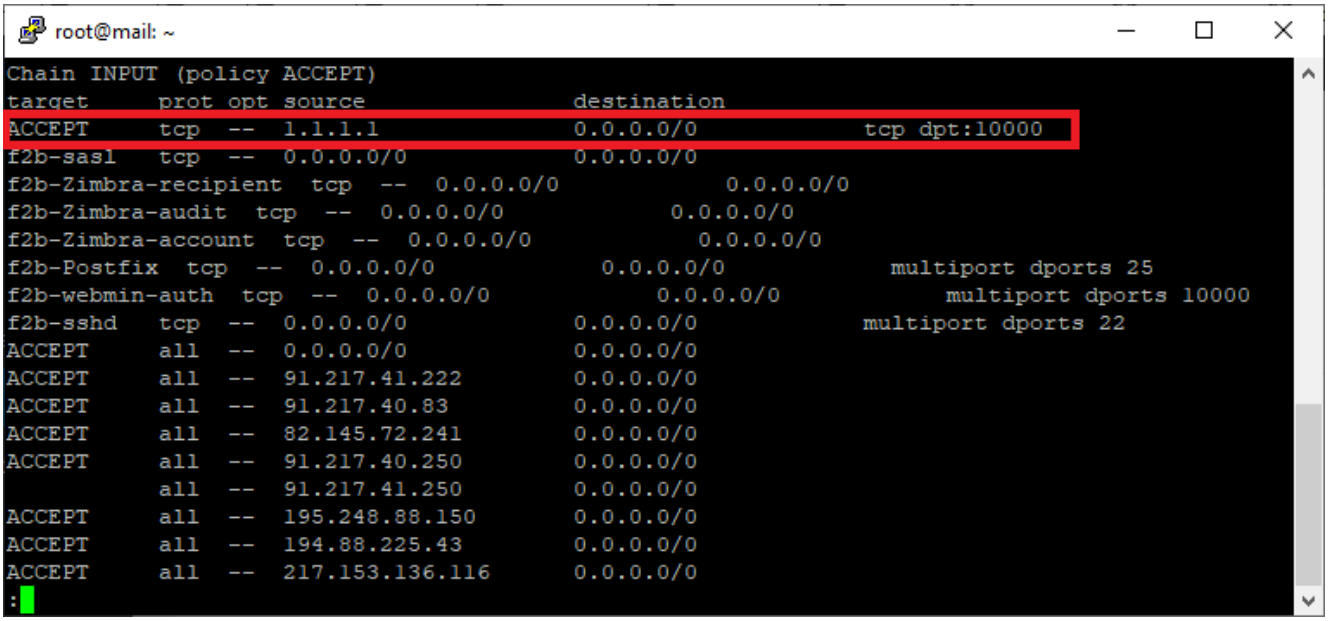
– podaj adres IP maszyny wirtualnej

– 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
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
: