„Puk, puk! Kto tam? Eeeee ... Spadaj!”

czyli **port-knocking** w praktyce administratora

Waldemar Chrzan

waldek@chrzan.net

Agenda

- Definicja
- Czym port-knocking jest
- Czym port-knocking nie jest
- Jak to działa
- Implementacje
- Przykład
- To naprawdę działa, ...
- Przydatne źródła
- Pytania
- Trenujemy

Co nam jest potrzebne do ćwiczeń?

- zainstalowane i skonfigurowane **iptables**;
- zainstalowany pakiet **knockd**:

```
~$ sudo apt-get install knockd
```

Definicja

Port-knocking jest metodą pozwalającą na nawiązanie zdalnego połączenia z usługami działającymi na komputerze, do którego dostęp został ograniczony np. za pomocą zapory sieciowej, umożliwiającą odróżniania prób połączeń, które powinny i nie powinny być zrealizowane.

(Źródło: Wikipedia)

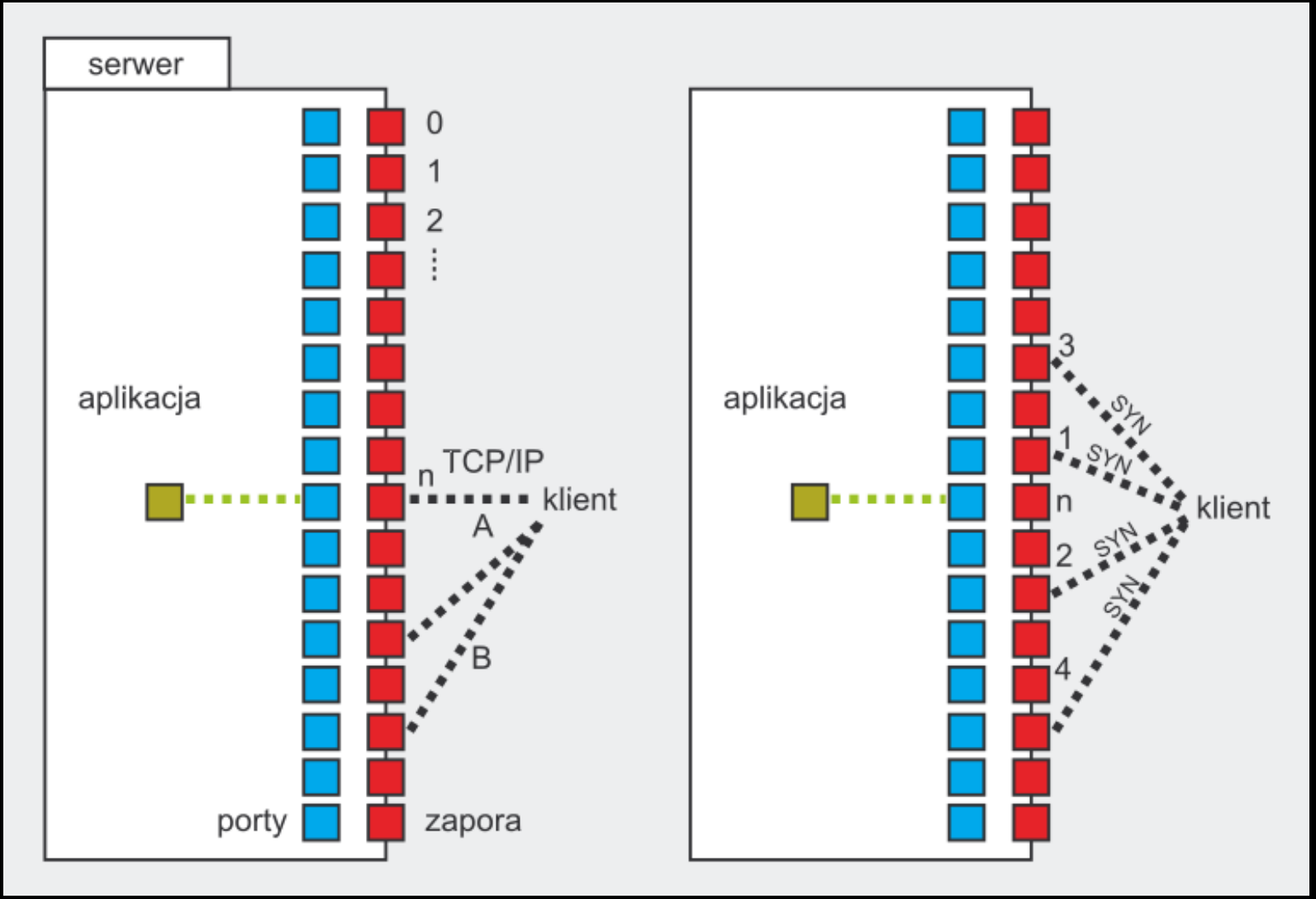
Czym port-knocking jest

- prostą metodą ukrywania usług/portów;
- sposobem na awaryjny dostęp bez niepotrzebnego kuszenia;
- metodą zdalnego wykonywania poleceń;
- prostym sposobem na zdalne zamykanie portów.

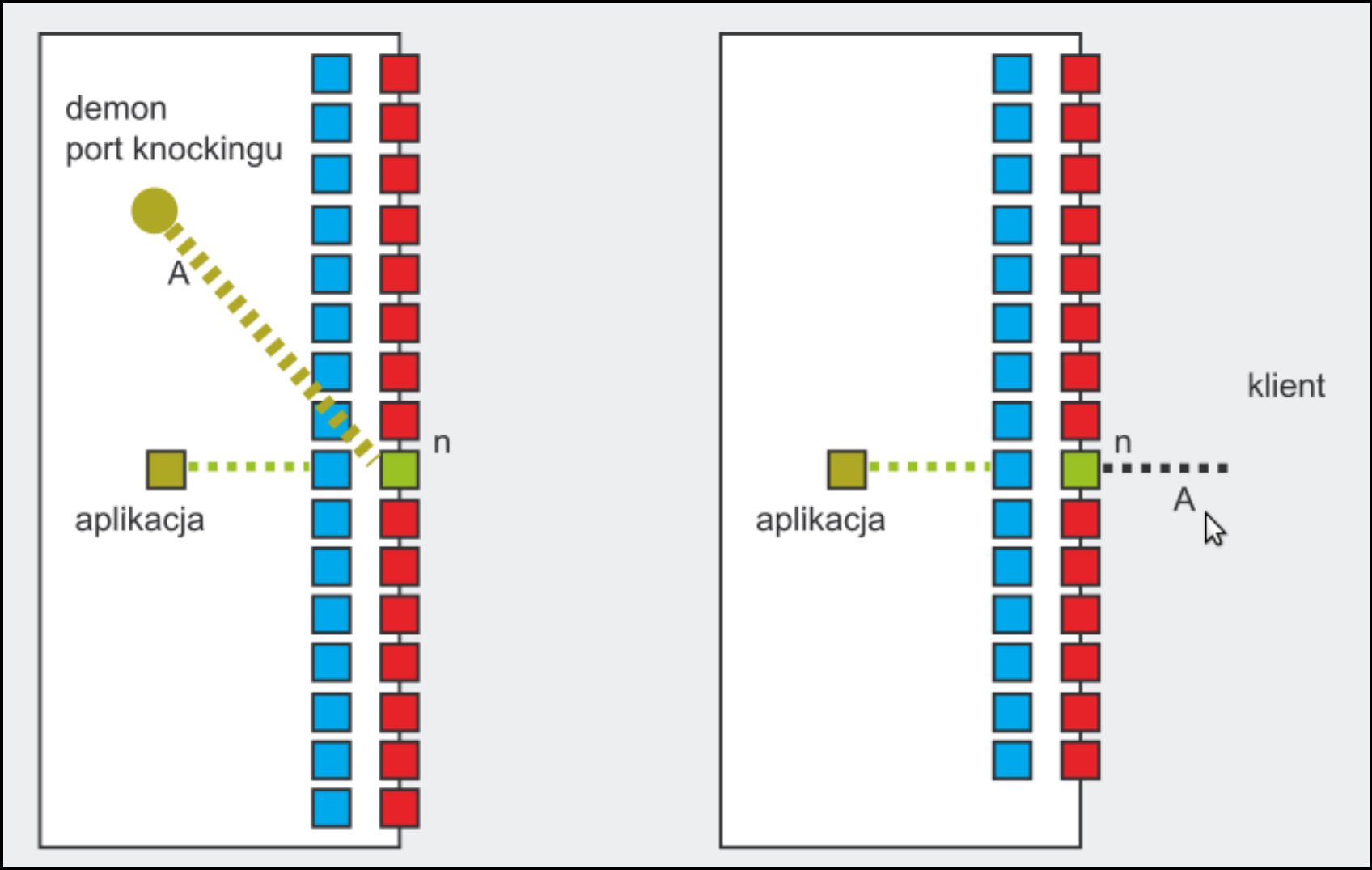
Czym port-knocking nie jest

- Nie jest „panaceum na wszelkie zło”
- Nie zastępuje innych zabezpieczeń

Jak to działa



Jak to działa, cd.



Implementacje

cd00r, SAd00r, COK,

Doorman, **knockd**, pasmal,

tumbler, **fwknop**, *pknock*

Przykład – konfiguracja iptables

```
# Ustalenie polityki domyślnej.
iptables -P FORWARD ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P INPUT DROP

# Akceptacja połączeń lokalnych.
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT

# Akceptacja zestawionych sesji.
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Przykład – test konfiguracji

```
~$ nmap -PN serwer.test.pl

Starting Nmap 5.21 ( http://nmap.org ) at 2011-01-16 02:37 CET
Nmap scan report for serwer.test.pl (10.10.10.10)
Host is up.
All 1000 scanned ports on serwer.test.pl (10.10.10.10) are filtered

Nmap done: 1 IP address (1 host up) scanned in 202.04 seconds
```

Przykład – domyślna konfiguracja knockd (/etc/knockd.conf)

```
[options]
    UseSyslog

[openSSH]
    sequence    = 7000,8000,9000
    seq_timeout = 5
    command     = /sbin/iptables -A INPUT -s %IP% -p tcp --dport 22 -j ACCEPT
    tcpflags    = syn

[closeSSH]
    sequence    = 9000,8000,7000
    seq_timeout = 5
    command     = /sbin/iptables -D INPUT -s %IP% -p tcp --dport 22 -j ACCEPT
    tcpflags    = syn
```

Przykład – „przerobiona” konfiguracja knockd

```
[options]
      UseSyslog

[opencloseSSH0]
  sequence      = 2000:tcp,4043:tcp,8000:tcp,1090:tcp,4425:tcp
  seq_timeout   = 8
  start_command = /sbin/iptables -I INPUT -s %IP% -p tcp --dport 22 -j ACCEPT
  cmd_timeout   = 60
  stop_command  = /sbin/iptables -D INPUT -s %IP% -p tcp --dport 22 -j ACCEPT
```

Przykład – domyślna konfiguracja knockd (/etc/default/knockd)

```
##################################################
#
# 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"
```

Przykład – jak pukać

- netcat;
- knock

```
~$ knock serwer.test.pl 2000:tcp 4043:tcp 8000:tcp 1090:tcp \
4425:tcp
```

Przykład – ułatwiamy sobie życie

- ~/.knock/serwer.test.pl

```
#!/bin/bash
HOST=`basename $0`
echo "Knocking to \"$HOST\" host."
knock $HOST 2000:tcp 4043:tcp 8000:tcp 1090:tcp 4425:tcp
exit 0
```

- alias

```
alias c_test='bash ~/.knock/serwer.test.pl && sleep 1s && ssh
waldek@serwer.test.pl'
```

Przykład – łączymy się do serwera

```
~$ c_test
Knocking to "serwer.test.pl" host.
Linux serwer 2.6.35-22-server #35-Ubuntu SMP Sat Oct 16 22:02:33
UTC 2010 x86_64 GNU/Linux
Ubuntu 10.10

Welcome to the Ubuntu Server!
 * Documentation:  http://www.ubuntu.com/server/doc
Last login: Sun Jan 16 01:57:55 2011 from ajd35.neoplus.adsl.tpnet.pl
waldek@serwer:~$
```

Przykład – test portów

```
~$ nmap -PN serwer.test.pl

Starting Nmap 5.21 ( http://nmap.org ) at 2011-01-16 02:47 CET
Nmap scan report for serwer.test.pl (10.10.10.10)
Host is up (0.089s latency).
Not shown: 999 filtered ports
PORT    STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 15.44 seconds
```

To naprawdę działa, ale...

- czasem potrzebne jest kilka prób pukania aby otworzyć port;
- czasem nie wpuszcza i dopiero po jakiejś przerwie zaczyna działać;
- dużo zależy od parametrów czasowych zdefiniowanych w konfiguracji oraz od doboru portów;
- czasem się zacina i wtedy nie działa:
  - restart interfejsu powoduje zatrzymanie daemona;

Przydatne źródła

- http://en.wikipedia.org/wiki/Port_knocking;
- Hakin9 nr 5/2005;
- http://portknocko.berlios.de/

Pytania?

Trenujemy

Co nam jest potrzebne?

- zainstalowane i skonfigurowane iptables;
- zainstalowany pakiet knockd:

```
~$ sudo apt-get install knockd
```

Dziękuję za uwagę