Knocking on Heaven's Door, 2. dio

 U prošlom članku smo opisalo što je "knocking" sustav, no što nam je za njegovu implementaciju sustava potrebno? Osim, naravno, iptables vatrozida, potreban je **knockd**, Port knocking daemon, te ponešto konfiguracije. Prvo instalirajmo knockd na standardan način:

```
# apt-get install knockd
```

U /etc/default/knockd promijenite varijablu START_KNOCKD=0 u START_KNOCKD=1.

```
# vim /etc/default/knockd
...
```

Glavna konfiguracijska datoteka je /etc/knockd.conf. Prvo što trebamo promijeniti je sekvenca koja otvara port:

```
[openSSH]
  sequence    = 7777,1234,8888,9876
  seq_timeout = 5
  command     = <iptables naredba>
```

Jasno je da ne smijete rabiti niti default portove koji dolaze uz paket, kao ni portove iz ovog članka. Ne trebamo objašnjavati zašto?

Uzmite 3 ili 4 različita porta, ne manje. Nemojte ni pretjerivati. Također, potrudite se izabrati niz koji će koliko-toliko biti pamtljiv, a opet nepredvidljiv napadačima. Nije preporučljivo uzeti niže portove, jer su to obično Well-known [1] portovi, pa će napadači tražiti slabosti u tim servisima (iako samog servisa nema).

U datoteci knockd.conf pod sekcijom [closeSSH] upišite isti niz, obrnuti ili pak nešto treće. Ovaj će niz zatvoriti port 22.

```
[closeSSH]
  sequence    = 9876,8888,1234,7777
  seq_timeout = 5
  command     = <iptables naredba>
```

Direktiva "**seq_timeout**" označava koliko će dugo knockd čekati da se cijeli niz izvrši i može biti u bilo kojoj sekciji. Kad to vrijeme istekne, niz morate ponoviti od početka.

Direktiva "**command**" je ona koja obavlja "pravi" posao, ali ju je potrebno izmijeniti u ovisnosti o konfiguraciji vašeg vatrozida. Osnovna je:

```
/sbin/iptables -I INPUT -s %IP% -p tcp --dport 22 -j ACCEPT
```

za otvaranje porta, odnosno

```
/sbin/iptables -D INPUT -s %IP% -p tcp --dport 22 -j ACCEPT
```

za zatvaranje porta.

U dokumentaciji knockda se spominje "-A" ("append") umjesto "-I" ("insert"), no to ovisi o vašoj konfiguraciji vatrozida. Pravilo iz knockda mora doći prije završnog DENY pravila, pa je možda sigurnije ubaciti to pravilo na
početak svih pravila, pogotovo ako nemate vrlo složen vatrozid.

Pogledajte dokumentaciju iptablesa ukoliko vam je potrebno više informacija.

Ako ste možda pomislili da bi bilo zgodno da se port sam zatvori nakon što ste završili rad na poslužitelju, knock i to podržava. Umjesto "[openSSH]" i "[closeSSH]", upotrijebite "[opencloseSSH]":

```
[opencloseSSH]
        sequence      = 7777,1234,8888,9876
        seq_timeout   = 5
        tcpflags      = syn,ack
        start_command = /sbin/iptables -I INPUT -s %IP% -p tcp --syn -j ACCEPT
        cmd_timeout   = 15
        stop_command  = /sbin/iptables -D INPUT -s %IP% -p tcp --syn -j ACCEPT
```

Direktiva "**cmd_command**" određuje koliko imate vremena spojiti se na port 22. Nakon 15 sekundi (ili koliko odredite), pravilo se briše.

Bitna napomena, kako bi ovaj način radio, vaš vatrozid mora biti konfiguriran uporabom ESTABLISHED konekcija, u suprotnom će vam novouspostavljenu konekciju knockd jednostavno - prekinuti. Evo kako to primjerice može izgledati:

```
ACCEPT     tcp  --  161.53.XXX.0/26      0.0.0.0/0           tcp dpt:22
ACCEPT     tcp  --  193.198.YYY.128/25      0.0.0.0/0           tcp dpt:22
ACCEPT     tcp  --  127.0.0.0/24         0.0.0.0/0           tcp dpt:22
DROP       tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:22 state INVALID
,NEW,RELATED,UNTRACKED
```

Dodavanje zadnje direktive radite ovako:

```
# iptables -A INPUT -s <RANGE> -p tcp --dport 22 -m state \! --state ESTABLISHED -j D
ROP
```

Na kraju, ukoliko daemon nije već startan, pokrenite ga:

```
# /etc/init.d/knockd start
Starting Port-knock daemon: knockd.
```

Kako bi testirali, odnosno mogli rabiti cijeli sustav, s paketom osim daemon dolazi i klijent, "knock". Njegova sintaksa je jednostavna, otkucajte na sustavu s kojeg se želite spojiti:

```
$ knock -v knockd_posluzitelj 7777 1234 8888 9876
```

Nakon toga se možete spojiti uobičajeno:

```
$ ssh korisnik@knocd_posluzitelj
```

Imajte na umu da u direktivu "command" možete upisati i bilo koju drugu naredbu, pa tako možete s određenim nizom ugasiti poslužitelj, rebootati ga,poslati predefinirani mail, upaliti ili ugasiti druge servise i slično.

Za Windows operativni sustav, postoje mnogi klijenti, a jedan je "knock.exe" http://www.zeroflux.org/proj/knock/files/knock-win32.zip [2]. Njih možete staviti u batch ili cmd skriptu koju ćete napisati i pokretati svoj SSH klijent nakon toga.

Umjesto knock.exe, možete rabiti bilo koji drugi program (netcat, nmap, pa čak i obični "telnet" program). Svi su oni dostupni i na linuxu i na Windowsu.

Više informacije možete naći na http://www.portknocking.org.

- Logirajte [3] se za dodavanje komentara

sri, 2010-01-20 12:23 - Željko Borš**Kuharice:** Linux [4]
Kategorije: Servisi [5]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/699

Links
[1] http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers
[2] http://www.zeroflux.org/proj/knock/files/knock-win32.zip
[3] https://sysportal.carnet.hr/sysportallogin
[4] https://sysportal.carnet.hr/taxonomy/term/17
[5] https://sysportal.carnet.hr/taxonomy/term/28