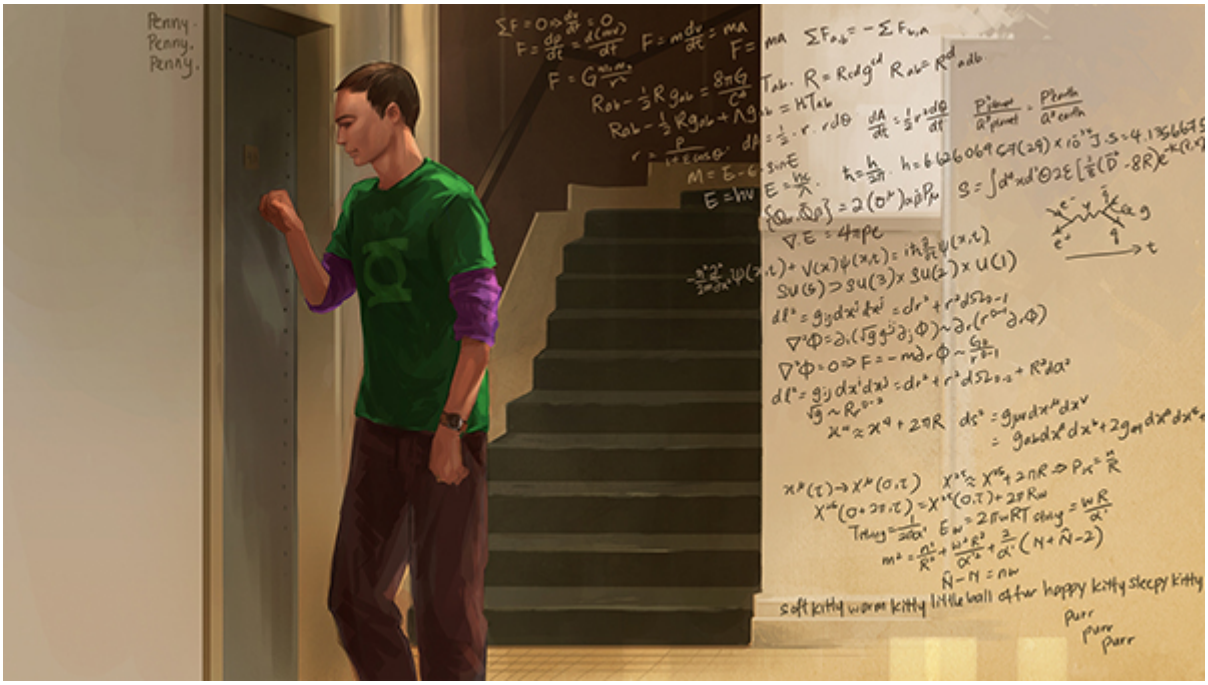
Port knocking или как обезопасить себя от брута по ssh

Информационная безопасность

Из песочницы

Речь пойдет о борьбе с надоедливыми брутфорсами и сканерами портов, которые всячески норовят получить доступ к серверу. В статье будет рассказано о технологии *Port Knocking*, позволяющей обезопасить доступ на сервер посредством скрытия портов.



Немного о самой технологии

В технологии **Port Knocking** есть интересная особенность. Она применяет несколько попыток подключения к закрытым портам. Вы спросите: «А зачем это нужно?» Давайте представим себе, что вы пришли на собеседование в какую-то организацию с пропускным режимом. Сначала вы попадаете на (1)пост охраны, где на вас выписывают пропуск, затем (2)вы попадаете в отдел кадров, где заполняете анкету и с вами беседуют, и в конечном итоге (3)вы попадаете в кабинет управляющего, который проводит завершающую беседу и принимает решение. А теперь давайте представим, что бы случилось, если бы все желающие напрямую шли к управляющему?

Технология *Port Knocking* осуществляет последовательность попыток подключения к закрытым портам. Даже не смотря на то, что все порты закрыты, вы можете отследить все попытки подключения в лог-файлах файрвола. Сервер, чаще всего, никак не отвечает на эти подключения, но он считывает и обрабатывает их. Но если же серия подключений была заранее обозначена пользователем, то выполнится определенное действие. Как пример,

подключение к SSH-сервису на порту 22. *Port Knocking* позволяет осуществлять не только данное действие. триггер позволяет выполнять и другие действия (скажем, отключение питания, перезагрузку системы и т.д.).

Установка на FreeBSD

На удаленной машине мы имеем FreeBSD 9.1
Port Knocking состоит из двух программ:
— сервер (knockd)
— клиент (knock)

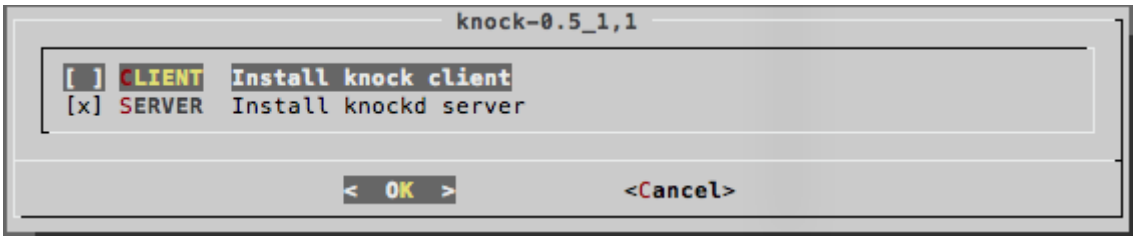
Я приведу пример настройки серверной части.

```
# cd /usr/ports/
# make search key=knocking
Port:   doorman-0.81_1
Path:   /usr/ports/security/doorman
Info:   Port knocking implementation, both daemon and client
Maint:  lupe@lupe-christoph.de
B-deps: lsof-4.88.d,8
R-deps: lsof-4.88.d,8
WWW:    http://doorman.sourceforge.net/

Port:   knock-0.5_1,1
Path:   /usr/ports/security/knock
Info:   Flexible port-knocking server and client
Maint:  sbz@FreeBSD.org
B-deps:
R-deps:
WWW:    http://www.zeroflux.org/projects/knock
```

Переходим в директорию с портом и конфигурируем.

```
cd /usr/ports/security/knock
make config
```



Ставим маркер на серверной части, а затем собираем и устанавливаем пакет.

Конфигурация

Теперь давайте займемся непосредственно настройкой.
Для начала скопируем конфиг.

```
# cd /usr/local/etc/
# cp knockd.conf.sample knockd.conf
```

В сети много вариаций настройки конфига, я приведу свой.
knockd.conf

```
[options]
        logfile = /var/log/knockd.log
        interface = em0

[openccloseSSH]
        sequence      = 7000:udp,7007:tcp,7777:udp
        seq_timeout   = 5
        tcpflags      = syn
        start_command = /sbin/pfctl -t good_hosts -T add %IP%
        cmd_timeout   = 10
        stop_command  = /sbin/pfctl -t good_hosts -T delete %IP%


[open22]
        sequence    = 7134:tcp,7675:tcp,7253:udp
        seq_timeout = 5
        tcpflags    = syn

        command     = /sbin/pfctl -t good_hosts -T add %IP%

[close22]
        sequence    = 7253:udp,7675:tcp,7134:tcp
        seq_timeout = 5
        tcpflags    = syn
        command     = /sbin/pfctl -t good_hosts -T delete %IP%
```

Сохраняем конфиг, добавляем в автозапуск и стартуем сервис.

```
# cd /usr/local/etc/rc.d/
# echo knockd_enable=\"YES\" >> /etc/rc.conf
# service knockd start
```

Настройка Firewall

Для начала включим поддержку Firewall, если она у вас отключена (как было в моем случае)

```
echo pf=\"YES\" >> /etc/rc.conf
```

Не советую делать данную процедуру удаленно, так как блокируются все подключения и доступа по ssh мы не получим.
Примечание: Если же вы не послушались и сделали данное действие удаленно, то проблему можно решить посредством включения root-логина в sshhd-config.

/etc/pf.conf

```
ext_if="rl0"

table <good_hosts> persist

block in on $ext_if all
pass in on $ext_if inet proto tcp from <good_hosts> \
 to $ext_if port 22 keep state
```

Вносим правила в настройки Firewall`a

```
/sbin/ipfw add 100 allow tcp from %IP% to me 22 keep-state
/sbin/ipfw delete 100
```

Перезагружаемся.

Стучимся

Для подключения я пользовался сторонним клиентом под MacOS — hping.

```
# knock -v *e*m*o*c*.ru 7000:udp,7007:tcp,7777:udp
hitting udp *1.*0*.*3*.*0:7000
hitting tcp *1.*0*.*3*.*0:7007
hitting udp *1.*0*.*3*.*0:7777
# ssh *e*m*o*c*.ru -l root
Password:
Last login: Thu May  9 11:30:40 2013 from *****
```

```
FreeBSD 9.1-RELEASE-p3 (GENERIC) #0: Mon Apr 29 18:11:52 UTC 2013
root@*e*m*o*c*:/root #
```