

MikroTik Certified Security Engineer

MTCSE

Chapter 5: Security Router

PORT
KNOCKING

DEFAULT
PORTS FOR
THE
SERVICES



MTI-GROUP LLC / network academy

V.19-01



Port Knocking

Port knocking – это неявная форма разрешения доступа к некоему сервису, при условии прохождения предварительно заданной последовательности соединений с различными портами целевого сервера.

На стороне устройства(роутера) отслеживаются "все" входящие соединения, и если фиксируется характерная «цепочка подключений» соответствующих ранее заданному «эталонному стуку» src(источник) добавляется в некий address-list (на время)— для которого временно открывает доступ к "закрытому" порту

The port "knock" itself is similar to a secret handshake and can consist of any number of TCP, UDP, or ICMP or other protocol packets to numbered ports on the destination machine

Port Knocking

LAB

Настройка логики (правил) для Port Knocking очень похожа на предыдущую задачу с защитой от BruteForce Password

Откройте доступ до роутера по winbox - с помощью правил PortKnocking

Необходимо выполнить задачу в новой цепочке, так же должна сохраниться реализация защиты по подбору паролей

How the Port Knocking works

очень упрощенная реализация

#	Action	Chain	Protocol	Dst. Port	In. Interfac...	Out. Interf...	Src. Address List	Dst. Address List	Bytes	Packets
0	✖ drop	input	6 (tcp)	8291			!knock-final		0 B	0
1	➡ add src to address list	input	6 (tcp)	11111			knock1		0 B	0
2	➡ add src to address list	input	6 (tcp)	22222			knock2		0 B	0
3	➡ add src to address list	input	6 (tcp)	33333					0 B	0

```
/ip firewall filter
```

```
add action=drop chain=input dst-port=8291 protocol=tcp src-address-list=!knock-final
```

```
add action=add-src-to-address-list address-list=knock1 address-list-timeout=10s chain=input  
dstport=11111 protocol=tcp
```

```
add action=add-src-to-address-list address-list=knock2 address-list-timeout=10s chain=input  
dstport=22222 protocol=tcp src-address-list=knock1
```

```
add action=add-src-to-address-list address-list=knock-final address-list-timeout=1d chain=input  
dst-port=33333 protocol=tcp src-address-list=knock2
```

How the Port Knocking works

```
D:\Saya\Apps\knock>dir
Volume in drive D has no label.
Volume Serial Number is F258-BA8D

Directory of D:\Saya\Apps\knock

09/09/2018  12:40 PM    <DIR>          .
09/09/2018  12:40 PM    <DIR>          ..
07/03/2005  02:30 AM             1,295,582 cygwin.dll
08/10/2005  02:52 PM             15,238 knock.exe
               2 File(s)              1,310,820 bytes
               2 Dir(s)  127,842,557,952 bytes free

D:\Saya\Apps\knock>knock.exe
usage: knock [options] <host> <port[:proto]> [port[:proto]] ...
options:
  -u, --udp           make all ports hits use UDP (default is TCP)
  -v, --verbose       be verbose
  -V, --version       display version
  -h, --help          this help

example: knock myserver.example.com 123:tcp 456:udp 789:tcp

D:\Saya\Apps\knock>knock your.mikrotik.ip-or-domain 12345:tcp 54321:udp
```

Port Knocking for Windows

Port Knocking for Linux

apt-get install knockd or yum install knockd

knock your.mikrotik.ip-address-or-domain 12345:tcp 54321:udp

MikroTik Certified Security Engineer

MTCSE

Chapter 5: Security Router

PORT
KNOCKING

DEFAULT
PORTS FOR
THE
SERVICES



MTI-GROUP LLC / network academy

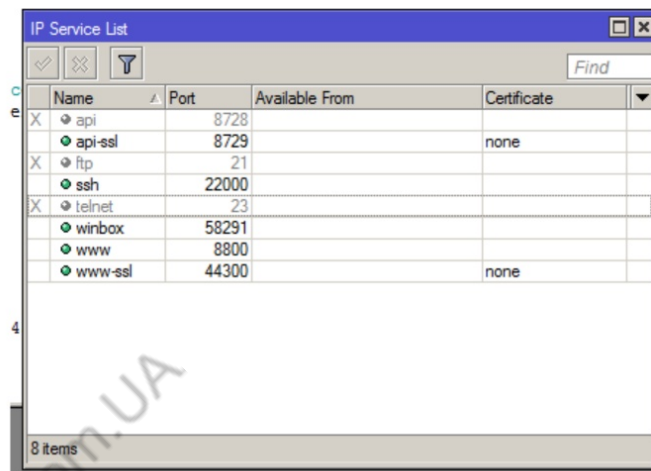
V.19-01

Default Ports for the Services

- A connection that is encrypted by one or more security protocols to ensure the security of data flowing between two In TCP/IP and UDP networks, a port is an endpoint to a logical connection and the way a client program specifies a specific server program on a computer in a network.
- The port number identifies what type of port it is, and what kind of service those port is serving
- Some ports have numbers that are assigned to them by the IANA, and these are called the "well-known ports" which are specified in RFC1700.
- Port numbers range from 0 to 65535, but only port numbers 0 to 1023 are reserved for privileged services and designated as well-known ports.or more nodes.
- When a connection is not encrypted, it can be easily listened to by anyone with the knowledge on how to do it.
- Protect the data being transferred from one computer to another

Default Ports for the Services

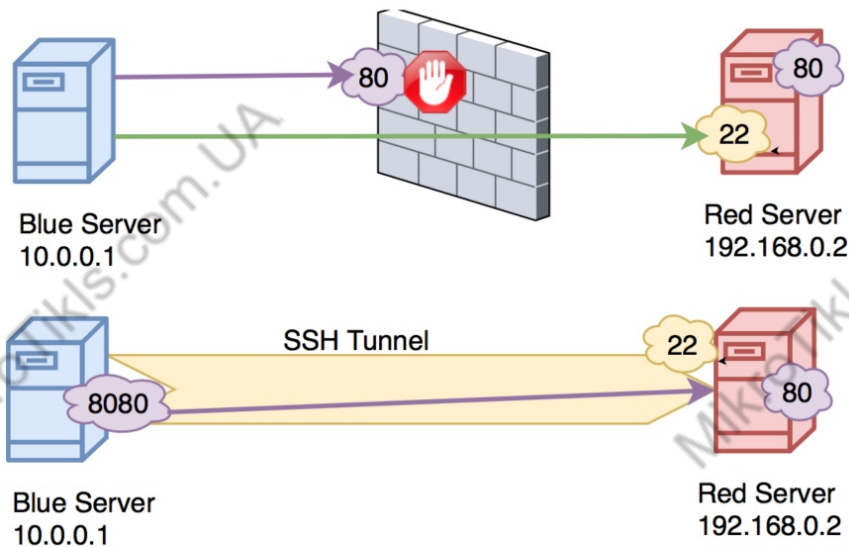
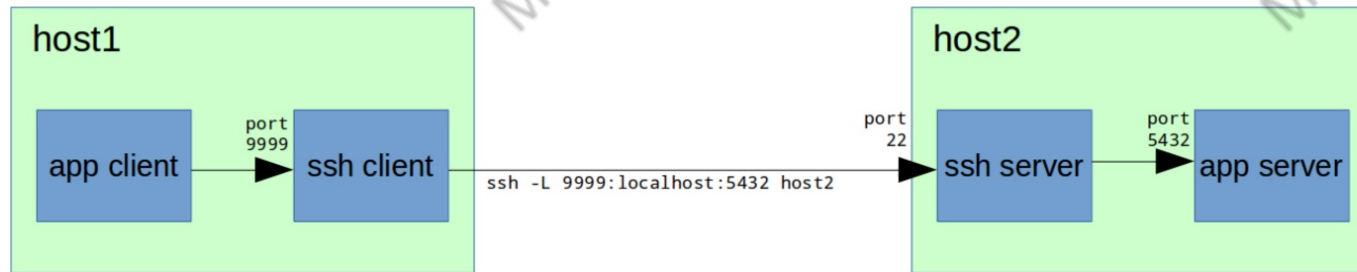
```
/ip service set telnet disabled=yes  
/ip service set ftp disabled=yes  
/ip service set www port=8800  
/ip service set ssh port=22000  
/ip service set www-ssl disabled=no port=44300  
/ip service set api disabled=yes  
/ip service set winbox port=58291
```



Name	Port	Available From	Certificate
X api	8728		
api-ssl	8729		none
X ftp	21		
ssh	22000		
X telnet	23		
winbox	58291		
www	8800		
www-ssl	44300		none

Вам также следует использовать
правила брандмауэра

TUNNELING THROUGH SSH



- Туннель SSH состоит из зашифрованного туннеля, созданного используя соединение по протоколу SSH
- Туннель SSH может использоваться для инкапсуляции незашифрованный трафик и передача его через зашифрованный канал.

TUNNELING THROUGH SSH



Host connects to RouterOS using ssh
with local-port forwarding parameter

RouterOS accepted ssh connections from host



Host trying to open unencrypted port (80)
from ssh tunnel via local-port forwarding ip

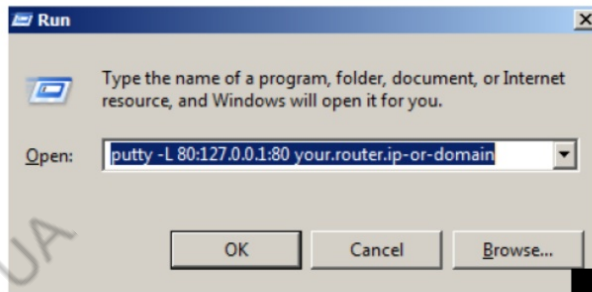


RouterOS sending http request from host
via ssh tunnel



TUNNELING THROUGH SSH

MikroTik : [admin@MB-MR5w] > ip ssh set forwarding-enabled=both



SSH Local-Forwarding for Windows

SSH Local-Forwarding for Linux

ssh -L 80:127.0.0.1:80 your.router.ip-or-domain

```
MMMM  MMM  KKK  TTTTTTTTTT  KKK
MMM  MMM  III  KKK KKK  RRRRRR  000000  TTT  III  KKK KKK
MMM  MM  III  KKKKK  RRR  RRR  000 000  TTT  III  KKKKK
MMM  MMM  III  KKK KKK  RRRRRR  000 000  TTT  III  KKK KKK
MMM  MMM  III  KKK KKK  RRR  RRR  000000  TTT  III  KKK KKK

MikroTik RouterOS 6.42.5 (c) 1999-2018      http://www.mikrotik.com/

[?]          Gives the list of available commands
command [?]  Gives help on the command and list of arguments

[Tab]        Completes the command/word. If the input is ambiguous,
              a second [Tab] gives possible options

/            Move up to base level
..          Move up one level
/command     Use command at the base level

[admin@01_Jose-Manuel] > [ ]
```

TUNNELING THROUGH SSH

127.0.0.1:2000



RouterOS v6.44.5

You have connected to a router. Administrative access only. If this device is not in your possession, please contact your local network administrator.

WebFig Login:

Login:

Password:

 Winbox

 Telnet

 Graphs

 License

 Help

© mikrotik

MikroTik Certified Security Engineer

MTCSE

Chapter 5: Security Router

PORT
KNOCKING

DEFAULT
PORTS FOR
THE
SERVICES



MTI-GROUP LLC / network academy

V.19-01