Prevent RDP logon brute force in mikrotik router via winbox

Masters,

I need help, how to config our router to block RDP brute force attacks

I would like to set our router to only allow RDP connection from a specified country (our specified IP ranges), plus i need to set up router to block (take ips to black list) and drop brute force attepmst to specified port numbers.

I try to set this with changeing the ftp port to rdp port.

http://wiki.mikrotik.com/wiki/Bruteforce_login_prevention_%28FTP_%26_SSH

Any suggestion tnx.

H

Current configuration:

I try to configure the router via Winbox.

I set some NAT rules (from dyndns to local address, rdp port)

In the filter rules tab:

2	;;; drop Rdp brute forcers					
	Action:	drop	Chain:	input	Protocol:	6 (tcp)
	Dst. Port:	3389	Src. Address List:	rdp_backlist	Bytes:	50.9 KiB
	Packets:	666	Rate:	0 bps	Packet Rate:	0
3	Action:	accept	Chain:	output	Protocol:	6 (tcp)
	Content:	530 Login incorrect	Dst. Limit/Rate:	1/min	Dst. Limit/Burst:	5
	Dst. Limit/Limit By:	dst. address	Dst. Limit/Expire:	100.00	Bytes:	0 B
	Packets:	0	Rate:	0 bps	Packet Rate:	0
4	Action:	add dst to address list	Chain:	output	Protocol:	6 (tcp)
	Content:	530 Login incorrect	Address List:	rdp_backlist	Timeout:	03:00:00
	Bytes:	0 B	Packets:	0	Rate:	0 bps
	Packet Rate:	0				

- I'm not sure this configuration should do the trick?! Is the content text "530 login incorrect" is fit for RDP connection to? Because in the tutorial used for filtering FTP connection.
- How to set router to allow RDP attempts from specified IP ranges?

Thank you

// New config

5	;;; Drop RDP Brute Forcers					
	Action:	drop	Chain:	input	Protocol:	6 (tcp)
	Dst. Port:	3389	Src. Address List:	rdp_blacklist	Bytes:	420 B
	Packets:	6	Rate:	0 bps	Packet Rate:	0
6	Action:	add src to address list	Chain:	input	Protocol:	6 (tcp)
	Dst. Port:	3389	Connection State:	new	Src. Address List:	rdp_stage3
	Address List:	rdp_blacklist	Timeout:	4d 04:39:00	Bytes:	0 B
	Packets:	0	Rate:	0 bps	Packet Rate:	0
7	Action:	add src to address list	Chain:	input	Protocol:	6 (tcp)
	Dst. Port:	3389	Connection State:	new	Src. Address List:	rdp_stage2
	Address List:	rdp_stage3	Timeout:	00:01:00	Bytes:	0 B
	Packets:	0	Rate:	0 bps	Packet Rate:	0
8	Action:	add src to address list	Chain:	input	Protocol:	6 (tcp)
	Dst. Port:	3389	Connection State:	new	Src. Address List:	rdp_stage1
	Address List:	rdp_stage2	Timeout:	00:01:00	Bytes:	0 B
	Packets:	0	Rate:	0 bps	Packet Rate:	0
9	Action:	add src to address list	Chain:	input	Protocol:	6 (tcp)
	Dst. Port:	3389	Connection State:	new	Address List:	rdp_stage1
	Timeout:	00:01:00	Bytes:	0 B	Packets:	0
	Rate:	0 bps	Packet Rate:	0		

router rdp mikrotik

edited Oct 27 '13 at 8:32

asked Oct 27 '13 at 6:58

holian

157 5 13

The linked config should accomplish what you're trying to do. Can you explain what's not working, and provide your current configuration? – Shane Madden ♦ Oct 27 '13 at 7:13

I added some modification, please check – holian Oct 27 '13 at 7:31

Added answer. You have to use the SSH version not the FTP version, since as you noticed, the 530 login incorrect is not going to match RDP sessions – Regan Oct 27 '13 at 7:34

1 Answer

The FTP config is actually looking into the FTP data to see the 530 code. You'll want to adapt the SSH config not the FTP config. Try this:

```
add chain=forward protocol=tcp dst-port=3389 src-address-list=rdp_blacklist action=drop \
comment="drop rdp brute forcers" disabled=no

add chain=forward protocol=tcp dst-port=3389 connection-state=new \
src-address-list=rdp_stage3 action=add-src-to-address-list address-list=rdp_blacklist \
address-list-timeout=10d comment="" disabled=no

add chain=forward protocol=tcp dst-port=3389 connection-state=new \
src-address-list=rdp_stage2 action=add-src-to-address-list address-list=rdp_stage3 \
address-list-timeout=1m comment="" disabled=no

add chain=forward protocol=tcp dst-port=3389 connection-state=new src-address-
list=rdp_stage1 \
action=add-src-to-address-list address-list=rdp_stage2 address-list-timeout=1m comment=""
disabled=no

add chain=forward protocol=tcp dst-port=3389 connection-state=new action=add-src-to-
address-list \
address-list=rdp_stage1 address-list-timeout=1m comment="" disabled=no
```

What this config actually does, is for each incoming attempt it adds the IP address to a list. The first time it gets added to stage1, then if the IP is still in stage1 (after a minute) and another attempt is made, it gets added to stage2, and after it does this two more times it is added to the rdp_blacklist list where it actually gets blocked for 10 days.

If you want it to be more or less aggressive you can change the list timeouts, or even add more lists if you so desire.

You can add a list of these to allow specific IP ranges only:

```
add chain=forward dst-port=3389 src-address=192.168.0.0/24 action=accept
add chain=forward dst-port=3389 src-address=10.10.0.1/32 action=accept
add chain=forward dst-port=3389 action=drop
```

Just add as many of the src-address lines you need ahead of the final drop line. If you have a LOT of ranges, you can create an address-list and reference that using this:

```
add chain=forward dst-port=3389 src-address-list=rdp_acceptlist action=accept
add chain=forward dst-port=3389 action=drop
```

And then add your addresses to the rdp_acceptlist

To add to the rdp_acceptlist use the following command:

```
/ip firewall address-list add list=rdp_acceptlist address=192.168.0.0/24
```

edited Oct 27 '13 at 9:28

answered Oct 27 '13 at 7:30

Regan
771 1 4 12

In winbox, may i have to create the rdp_blacklist or will be created automatically? – holian Oct 27 '13 at 7:42

The rdp_blacklist will get created once the first address is added to the list once an address makes it through all the stages. I added more to answer your question about having an accept list for your ranges, that list you will have to create using the command at the bottom, or using the graphical interface – Regan Oct 27 '13 at 7:46

Regan! Many many many thank you for your help! i try it now! Will back to accept your solution! – holian Oct 27 '13 at 8:08

I try to test the black list thing, but it seems not working. The stage and black list not created, but i made 10 fake login attemtpt in one minute. I edited my post with the new config. Please check – holian Oct 27 '13 at 8:32

Can you explain more on how your network is setup? More specifically, are you protecting a nat'ed server? And is the external port also 3389? Also, you are verifying from a remote host/outside firewall host, correct? Also try `/ip firewall address-list add list=rdp_blacklist address=your.test.ip.address/32` and make sure it blocks the connection, if not then something else is amiss. – Regan Oct 27 '13 at 8:41