



Prevention Login Brut eforce MikroTIK

**Oleh Fajar Amanullah Zaky
SMK Catur Global**

MUM Indonesia 2016

Tentang Saya

1. Salah satu Pelajar di SMK Catur Global Kota Bekasi
2. Pernah mengikuti Pesantren Networkers ID-
Networkers
3. Kenal MikroTIK sejak Kelas 1 SMK (2014)
4. MTCNA, MTCRE, MTCINE
5. Email : fajarstw8899@gmail.com
6. Contact : +62-831 4459 6878

About SMK Catur Global



About ID-Networkers



Bruteforce Attack

PASSWORD
BRUTE FORCE ATTACK

Apa itu Bruteforce ?

Brute force attack adalah sebuah metode penyerangan terhadap sebuah sistem, dengan mencoba semua kemungkinan password (kata kunci).

Brute force attack merupakan serangan yang dapat meningkatkan resource spu secara drastis, karena mencoba seluruh kemungkinan kata.

Perbedaan Dictionary attack dengan Brute force attack

Dictionary attack menyerang target dengan mencoba semua kata-kata yang didefinisikan dalam sebuah list (disebut juga dengan istilah kamus atau dictionary).

Berbeda dengan **Brute force attack** yang menggunakan semua kemungkinan kombinasi karakter yang lingkup katanya sangat luas

Brute force Attack

- Penyerangan brutal dengan menggunakan seluruh kemungkinan

Contoh : **aaaa s/d zzzz**

AAAA s/d ZZZZ

aAaA s/d zZzZ

AaAa s/d ZzZz

- Serangan ini membutuhkan waktu yang sangat lama
- Persentase keberhasilan yang cukup besar

Dictionary Attack

- Penyerangan yang mencoba kemungkinan seluruh kata yang telah disusun dalam list kamus (Dictionary)

Contoh : **admin 4dm1n**
admin123 ADMIN
admin321 4DM1N

- Persentase yang didapat kurang menentu, tergantung kita memperkirakan password yang dibuat oleh adminnya
- Dapat memakan banyak waktu jika amunisinya cukup banyak dalam menebak password

K

The screenshot shows the Windows Event Viewer window with the title bar "Log". The left pane displays "Freeze" as the selected view. The right pane shows a list of events filtered by "all". The events are listed in a table format:

Date and Time	Source	Category	Description
Sep/10/2016 20:09:47	memory	system, error, critical	login failure for user admin from 10.10.10.253 via ssh
Sep/10/2016 20:09:47	memory	system, error, critical	login failure for user admin from 10.10.10.253 via ssh
Sep/10/2016 20:09:47	memory	system, error, critical	login failure for user admin from 10.10.10.253 via ssh
Sep/10/2016 20:09:48	memory	system, error, critical	login failure for user admin from 10.10.10.253 via ssh
Sep/10/2016 20:09:48	memory	system, error, critical	login failure for user admin from 10.10.10.253 via ssh
Sep/10/2016 20:09:48	memory	system, error, critical	login failure for user admin from 10.10.10.253 via ssh
Sep/10/2016 20:09:48	memory	system, error, critical	login failure for user admin from 10.10.10.253 via ssh
Sep/10/2016 20:09:48	memory	system, error, critical	login failure for user admin from 10.10.10.253 via ssh
Sep/10/2016 20:09:49	memory	system, error, critical	login failure for user admin from 10.10.10.253 via ssh
Sep/10/2016 20:09:49	memory	system, error, critical	login failure for user admin from 10.10.10.253 via ssh
Sep/10/2016 20:09:49	memory	system, error, critical	login failure for user admin from 10.10.10.253 via ssh
Sep/10/2016 20:09:49	memory	system, error, critical	login failure for user admin from 10.10.10.253 via ssh
Sep/10/2016 20:09:49	memory	system, error, critical	login failure for user admin from 10.10.10.253 via ssh
Sep/10/2016 20:09:49	memory	system, error, critical	login failure for user admin from 10.10.10.253 via ssh
Sep/10/2016 20:09:49	memory	system, error, critical	login failure for user admin from 10.10.10.253 via ssh
Sep/10/2016 20:09:49	memory	system, error, critical	login failure for user admin from 10.10.10.253 via ssh
Sep/10/2016 20:09:49	memory	system, error, critical	login failure for user admin from 10.10.10.253 via ssh
Sep/10/2016 20:09:49	memory	system, error, critical	login failure for user admin from 10.10.10.253 via ssh
Sep/10/2016 20:09:49	memory	system, error, critical	login failure for user admin from 10.10.10.253 via ssh
Sep/10/2016 20:09:49	memory	system, error, critical	login failure for user admin from 10.10.10.253 via ssh
Sep/10/2016 20:09:49	memory	system, error, critical	login failure for user admin from 10.10.10.253 via ssh
Sep/10/2016 20:09:49	memory	system, error, critical	login failure for user admin from 10.10.10.253 via ssh
Sep/10/2016 20:09:50	memory	system, error, critical	login failure for user admin from 10.10.10.253 via ssh

Tools Bruteforce

1. Hydra

```
root@Z:/home/fajar/Documents/New Folder/exploit# hydra -l admin -P pass.txt 10.10.10.1 -t 4 ssh
Hydra v8.1 (c) 2014 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2016-06-01 09:32:43
[DATA] max 4 tasks per 1 server, overall 64 tasks, 15871 login tries (l:1/p:15871), ~62 tries per task
[DATA] attacking service ssh on port 22
[22][ssh] host: 10.10.10.1 login: admin password: 1234567890
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2016-06-01 09:32:49
```

2. Medusa

```
root@Z:/home/fajar/Documents/New Folder/exploit# medusa -h 10.10.10.1 -u admin -P pass.txt -M ssh
Medusa v2.1.1 [http://www.fooofus.net] (C) JoMo-Kun / Foofus Networks <jmk@fooofus.net>

ACCOUNT CHECK: [ssh] Host: 10.10.10.1 (1 of 1, 0 complete) User: admin (1 of 1, 0 complete) Password: 1234567890 (1 of 15870 complete)
ACCOUNT FOUND: [ssh] Host: 10.10.10.1 User: admin Password: 1234567890 [SUCCESS]
```

3. Ncrack

```
root@Z:/home/fajar/Documents/New Folder/exploit# ncrack -v --user admin -P pass.txt 10.10.10.1:22
Starting Ncrack 0.5 ( http://ncrack.org ) at 2016-06-01 09:40 WIB
Discovered credentials on ssh://10.10.10.1:22 'admin' '1234567890'
```


Penanganan Bruteforce SSH

Disable service SSH

```
[admin@MikroTik] > ip service disable ssh
```

```
root@Z:/home/fajar/Documents/New Folder/exploit# nmap 10.10.10.1
```

```
Starting Nmap 7.01 ( https://nmap.org ) at 2016-06-01 10:22 WIB
```

```
Nmap scan report for 10.10.10.1
```

```
Host is up (0.10s latency).
```

```
Not shown: 994 closed ports
```

```
PORT      STATE SERVICE
```

```
21/tcp    open  ftp
```

```
23/tcp    open  telnet
```

```
80/tcp    open  http
```

```
81/tcp    open  hosts2-ns
```

```
2000/tcp  open  cisco-sccp
```

```
8291/tcp  open  unknown
```

```
MAC Address: 4C:5E:0C:BA:B4:0D (Routerboard.com)
```

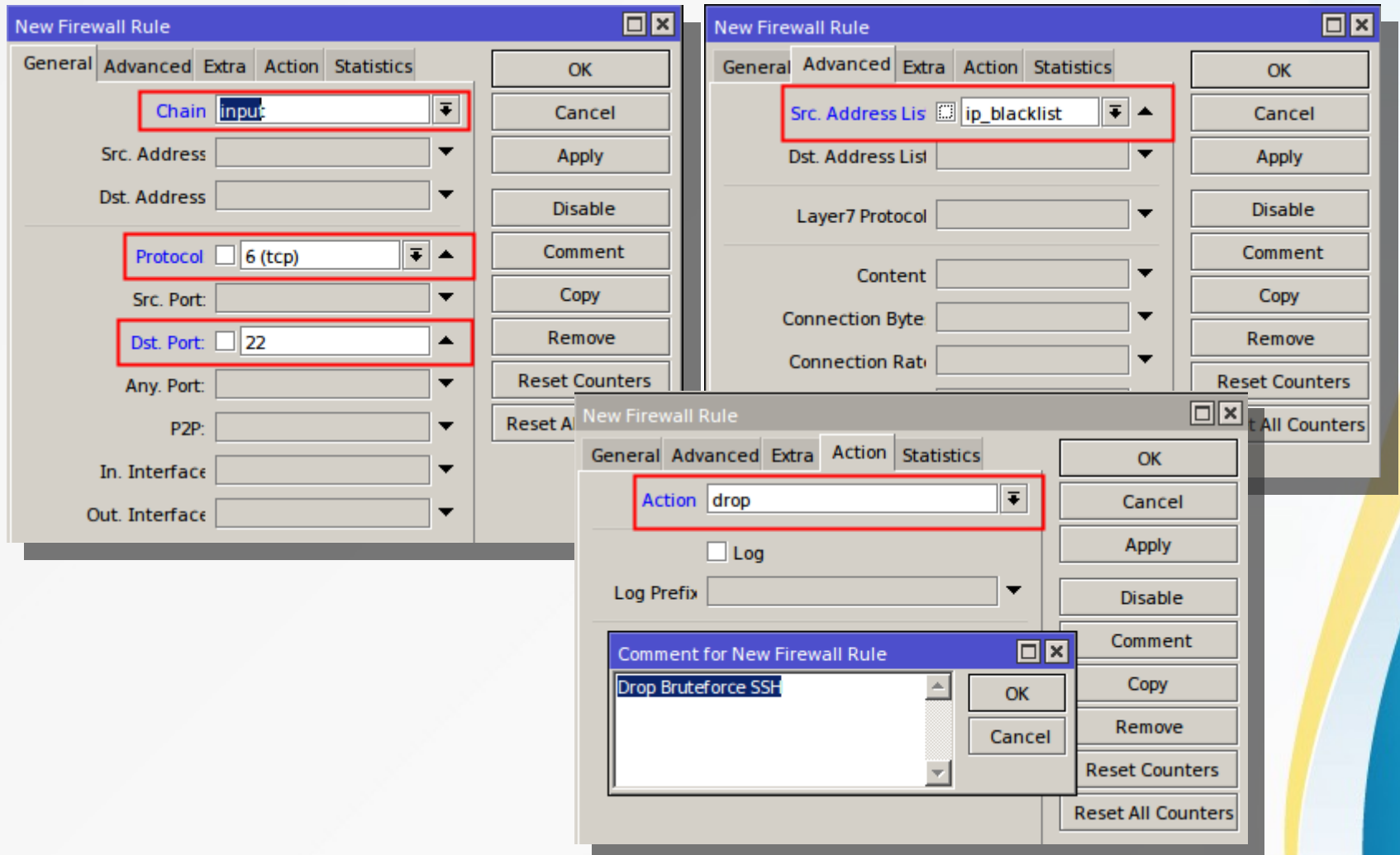
```
Nmap done: 1 IP address (1 host up) scanned in 12.33 seconds
```

```
root@Z:/home/fajar/Documents/New Folder/exploit# medusa -h 10.10.10.1 -u admin -P pass.txt -M ssh
Medusa v2.1.1 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>
```

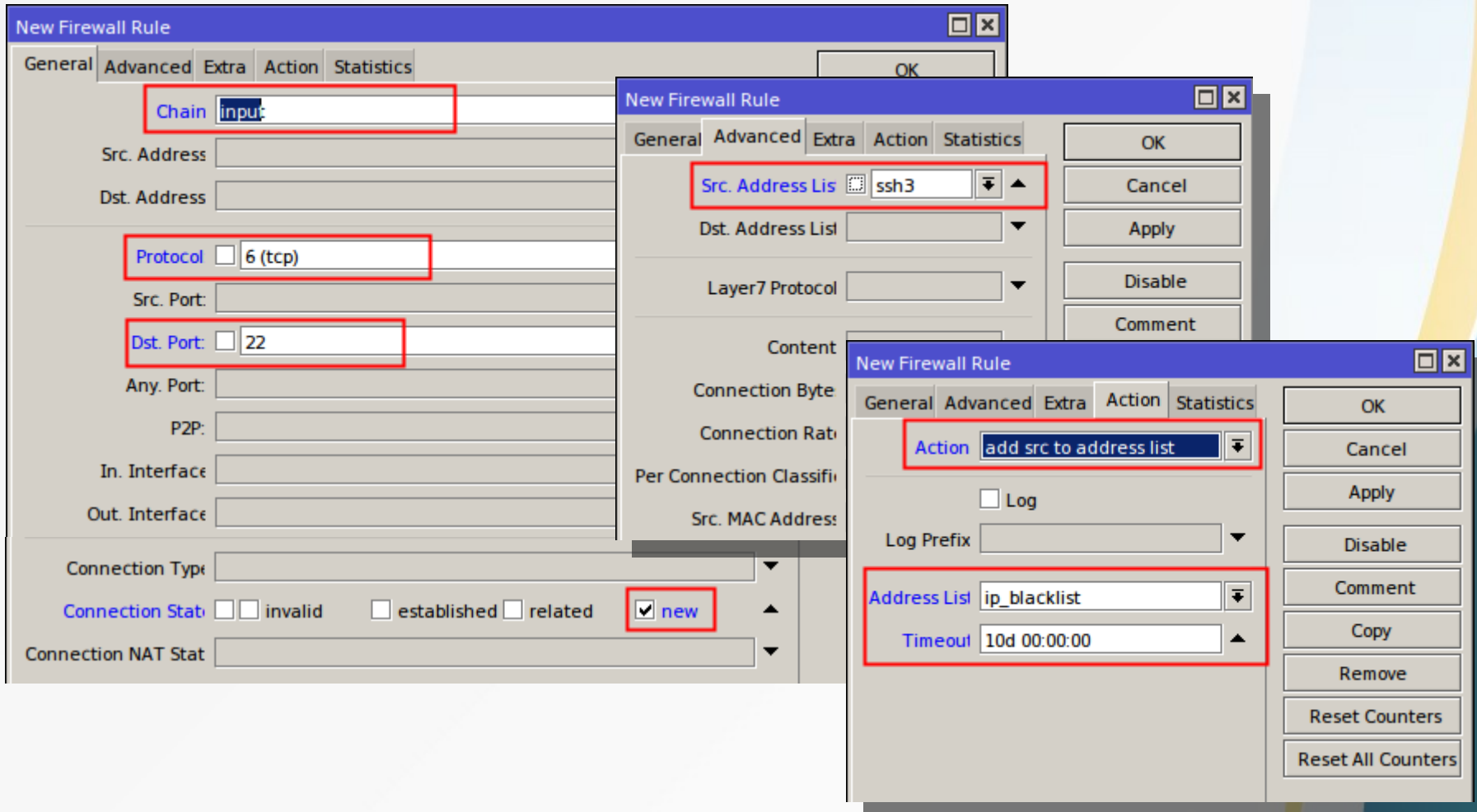
```
NOTICE: ssh.mod: failed to connect, port 22 was not open on 10.10.10.1
```

Penanganan Bruteforce SSH dengan Firewa

II



Penanganan Bruteforce SSH dengan Firewall



Penanganan Bruteforce SSH dengan Firewall

The image displays three overlapping screenshots of the Mikrotik WinBox 'New Firewall Rule' configuration window, illustrating the steps to create a rule for handling brute-force SSH attacks.

Top Left Screenshot (General Tab):

- Chain:** input
- Protocol:** 6 (tcp)
- Dst. Port:** 22
- Connection State:** new (checked)

Top Right Screenshot (General Tab):

- Src. Address List:** ssh2

Bottom Screenshot (Action Tab):

- Action:** add src to address list
- Log:** (unchecked)
- Log Prefix:** (empty)
- Address List:** ssh3
- Timeout:** 00:01:00

Penanganan Bruteforce SSH dengan Firewall

The image displays three overlapping screenshots of the Mikrotik WinBox interface, specifically the 'New Firewall Rule' configuration windows, illustrating the steps to create a rule for handling SSH brute force attacks.

Top Left Screenshot (General Tab):

- Chain:** input
- Protocol:** 6 (tcp)
- Dst. Port:** 22
- Connection Type:** ☒ new

Top Right Screenshot (General Tab):

- Src. Address List:** ssh1

Bottom Screenshot (Action Tab):

- Action:** add src to address list
- Log:** ☐ Log
- Address List:** ssh2
- Timeout:** 00:01:00

Penanganan Bruteforce SSH dengan Firewall

The image displays two screenshots of the Mikrotik WinBox 'New Firewall Rule' dialog box, illustrating the configuration for handling brute-force SSH attacks.

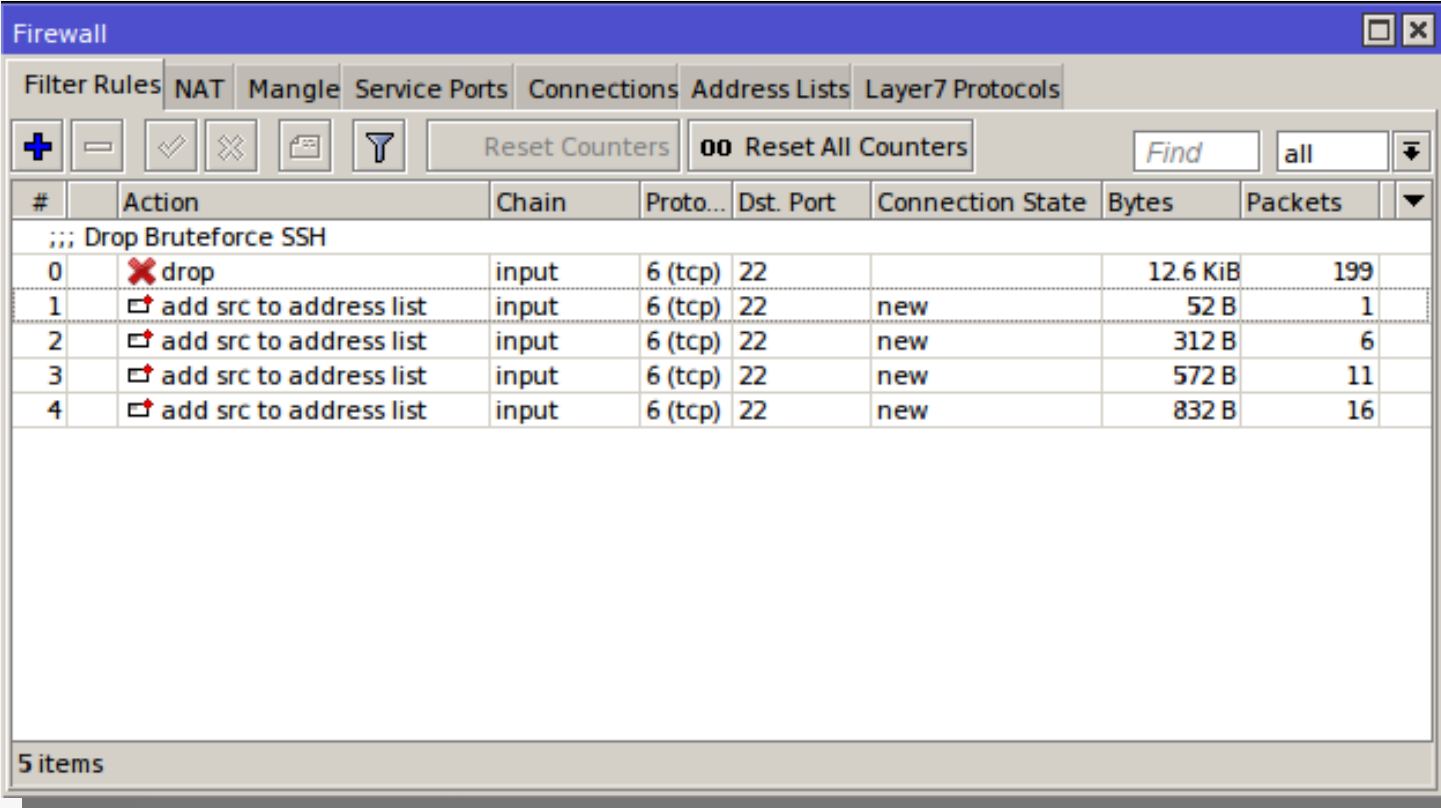
Left Screenshot (General Tab):

- Chain:** input
- Protocol:** 6 (tcp)
- Dst. Port:** 22
- Connection Type:** ☒ new

Right Screenshot (Action Tab):

- Action:** add src to address list
- Address List:** ssh1
- Timeout:** 00:01:00

Hasil akhir Filter Rules

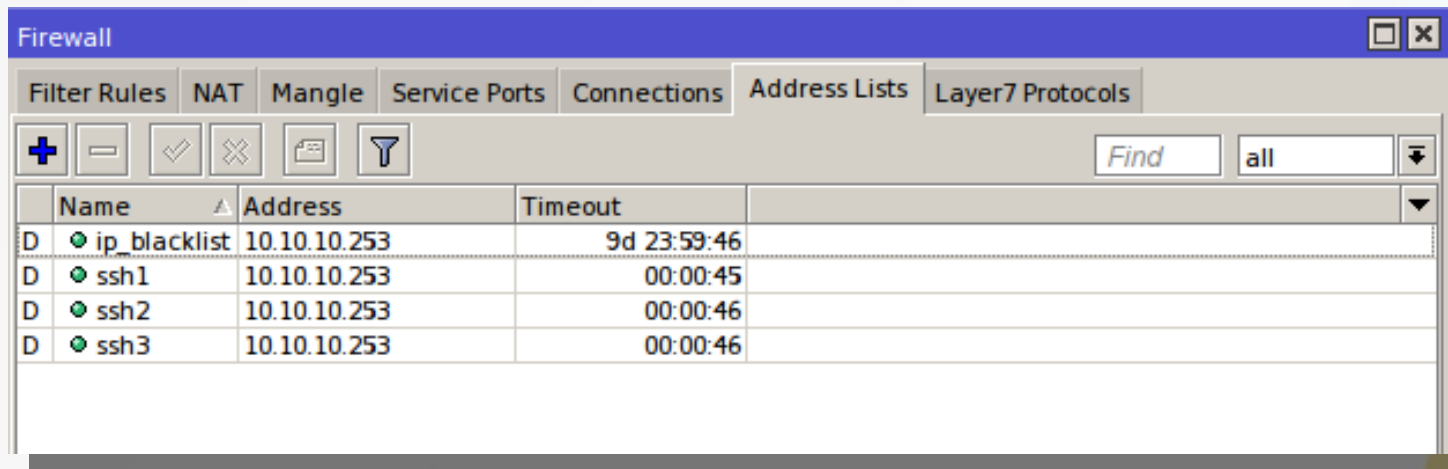
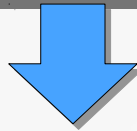


#	Action	Chain	Proto...	Dst. Port	Connection State	Bytes	Packets
... Drop Bruteforce SSH							
0	✗ drop	input	6 (tcp)	22		12.6 KiB	199
1	➡ add src to address list	input	6 (tcp)	22	new	52 B	1
2	➡ add src to address list	input	6 (tcp)	22	new	312 B	6
3	➡ add src to address list	input	6 (tcp)	22	new	572 B	11
4	➡ add src to address list	input	6 (tcp)	22	new	832 B	16

5 items

Testing Bruteforce SSH

```
root@Z:/home/fajar/Documents/New Folder/exploit# ncrack -v --user admin -P pass.txt 10.10.10.1:22  
Starting Ncrack 0.5 ( http://ncrack.org ) at 2016-06-01 11:56 WIB
```



Penanganan Bruteforce FTP

Disable service FTP

```
[admin@MikroTik] > ip service disable ftp
```

```
root@Z:/home/fajar# nmap 10.10.10.1

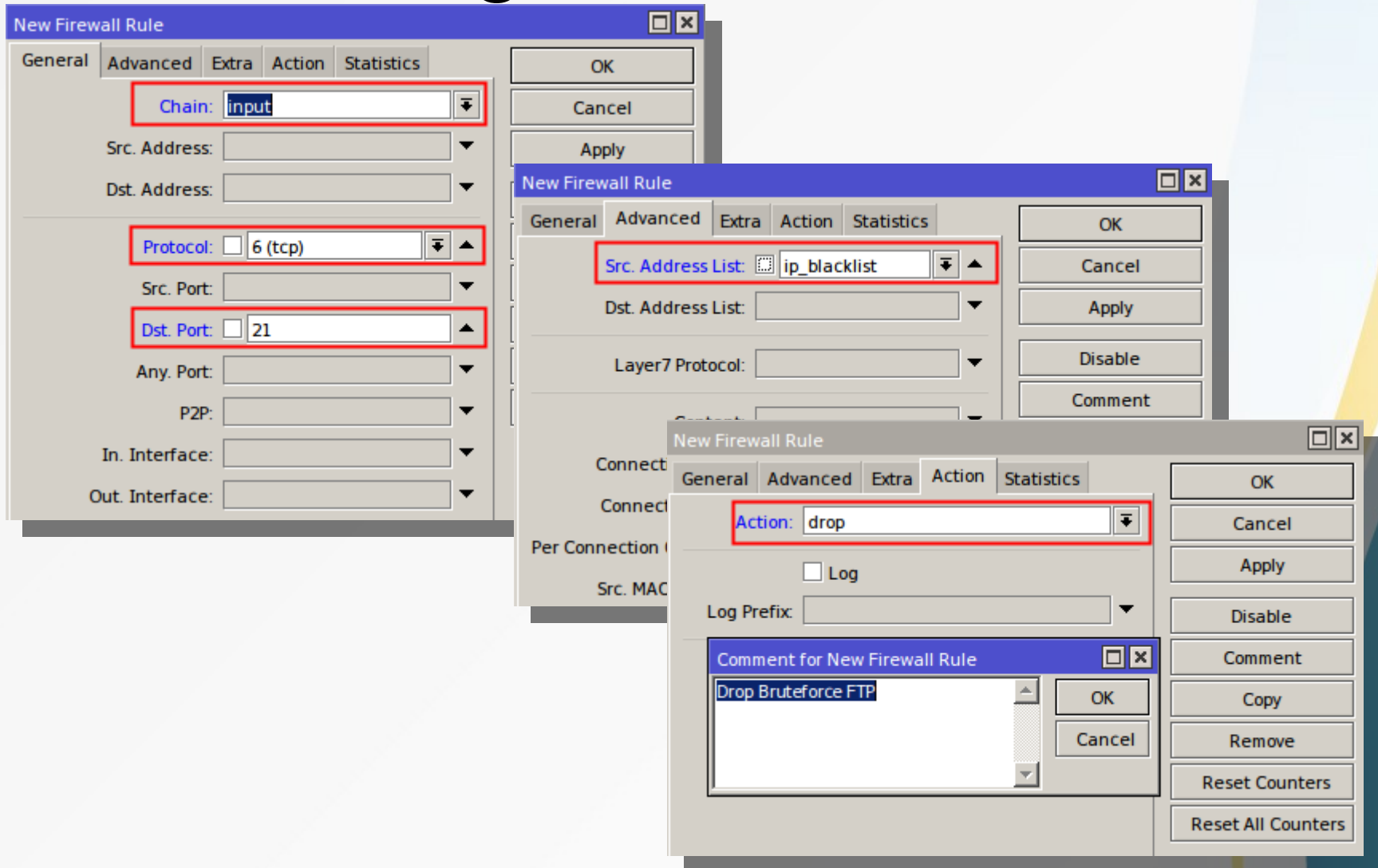
Starting Nmap 7.01 ( https://nmap.org ) at 2016-06-01 22:01 WIB
Nmap scan report for 10.10.10.1
Host is up (0.026s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
80/tcp    open  http
81/tcp    open  hosts2-ns
2000/tcp  open  cisco-sccp
8291/tcp  open  unknown
MAC Address: 4C:5E:0C:BA:B4:0D (Routerboard.com)

Nmap done: 1 IP address (1 host up) scanned in 31.99 seconds
```

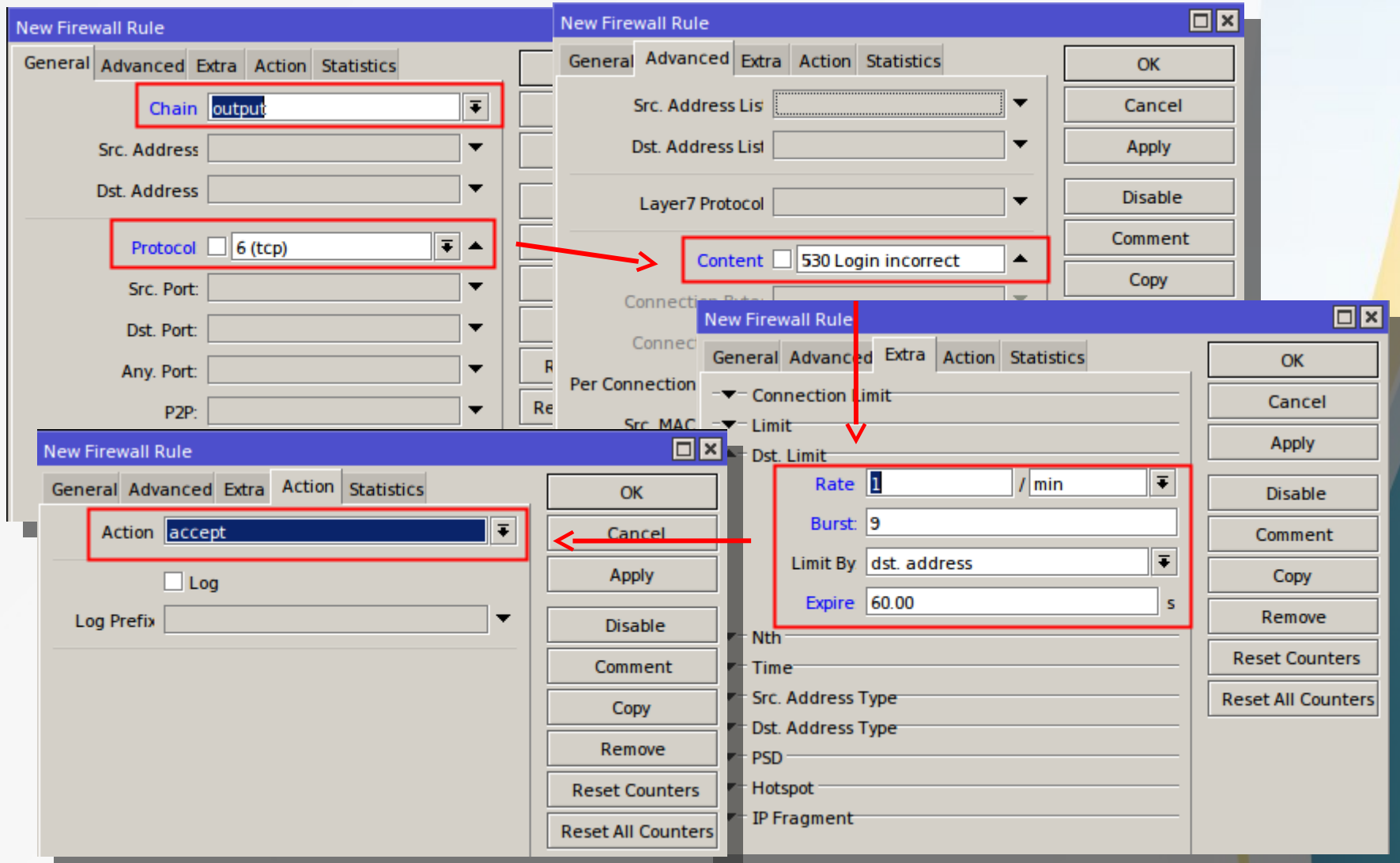
```
root@Z:/home/fajar/Documents/New Folder/exploit# medusa -h 10.10.10.1 -u admin -P pass.txt -M ftp
Medusa v2.1.1 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

NOTICE: ftp.mod: failed to connect, port 21 was not open on 10.10.10.1
```

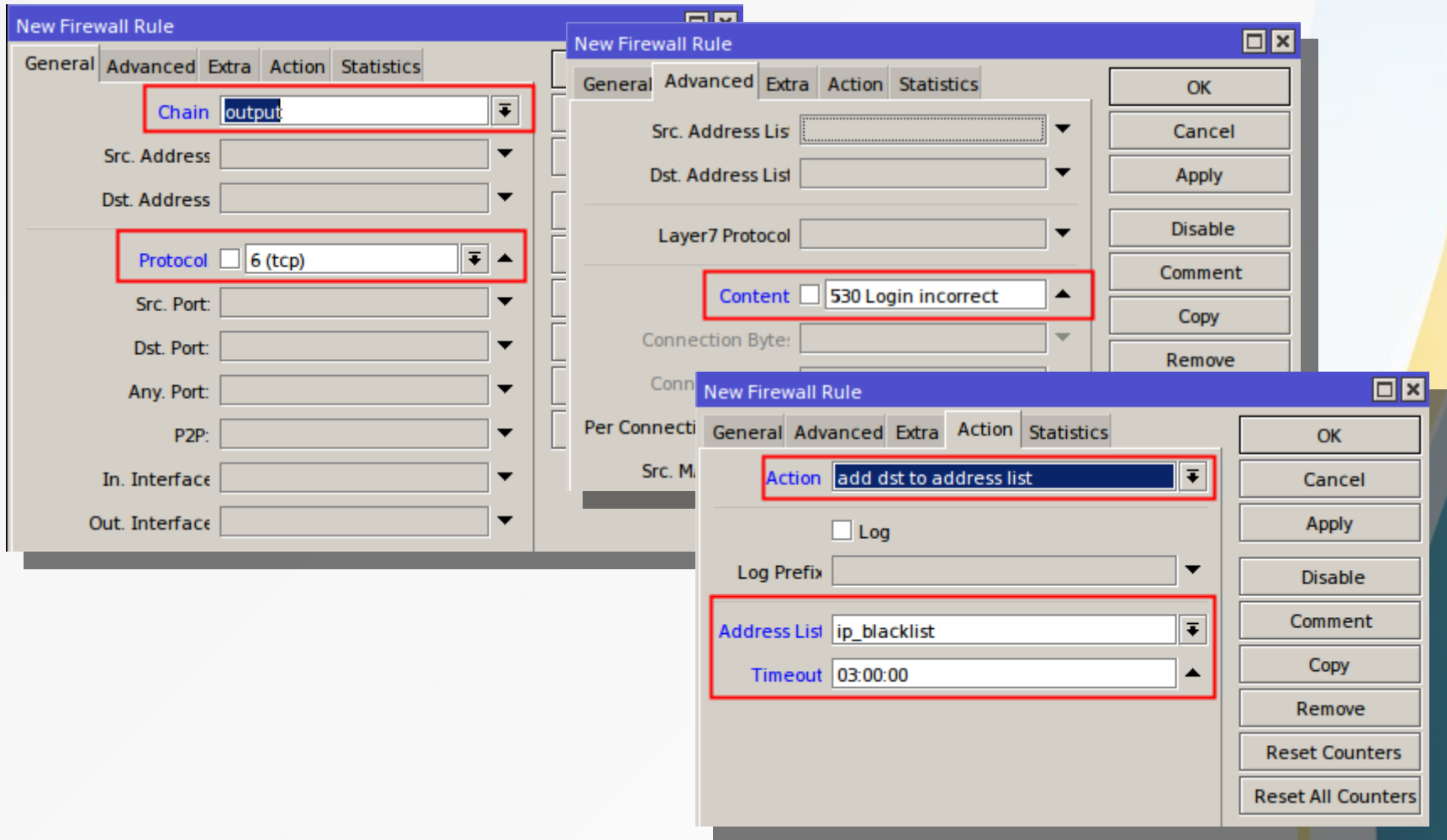

Penanganan Bruteforce FTP dengan Firewall



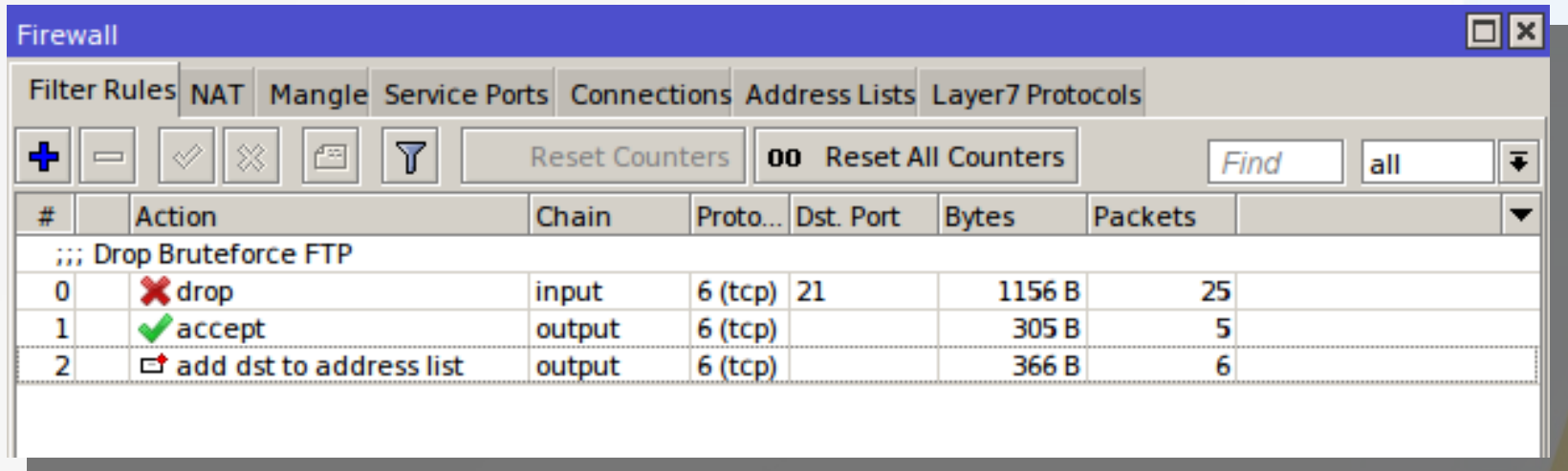
Penanganan Bruteforce FTP dengan Firewall



Penanganan Bruteforce FTP dengan Firewall



Hasil akhir Filter Rules



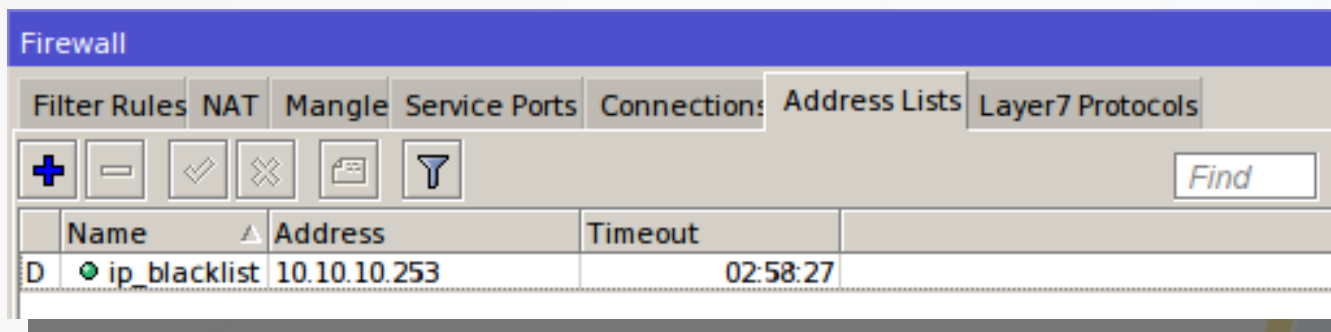
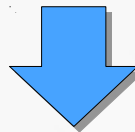
The screenshot shows the Mikrotik WinBox Firewall Filter Rules configuration window. The 'Filter Rules' tab is selected. The table below lists the configured rules for the 'Drop Brute force FTP' filter.

#	Action	Chain	Proto...	Dst. Port	Bytes	Packets
;;; Drop Brute force FTP						
0	drop	input	6 (tcp)	21	1156 B	25
1	accept	output	6 (tcp)		305 B	5
2	add dst to address list	output	6 (tcp)		366 B	6

Testing Bruteforce FTP

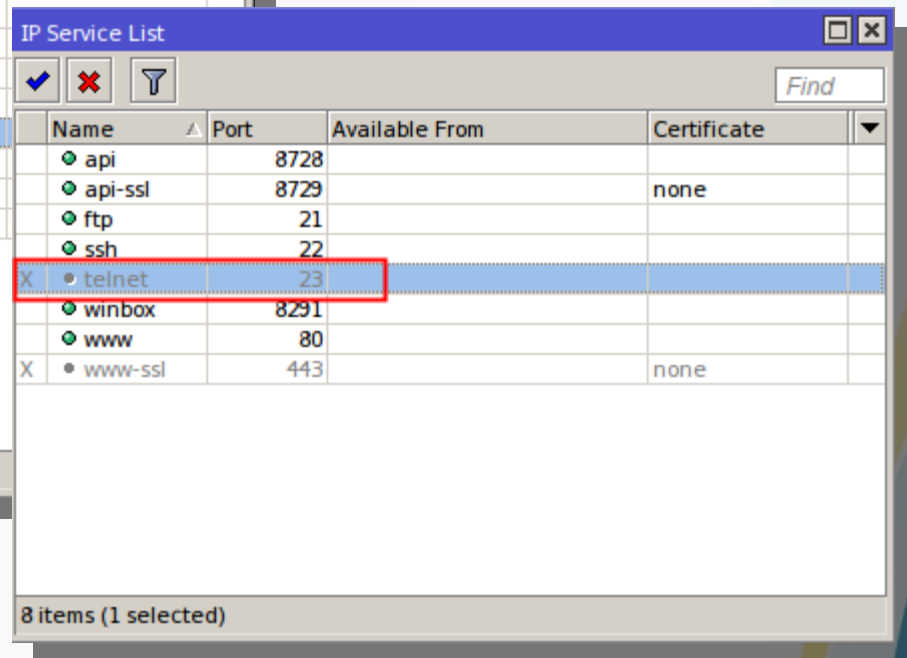
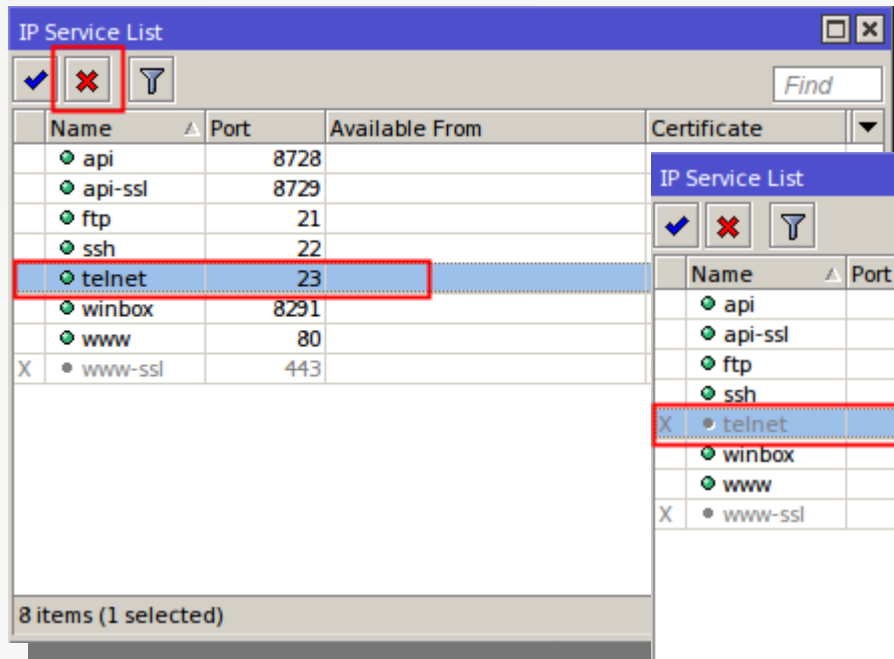
```
root@Z:/home/fajar/Documents/New Folder/exploit# medusa -h 10.10.10.1 -u admin -P pass.txt -M ftp
Medusa v2.1.1 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [ftp] Host: 10.10.10.1 (1 of 1, 0 complete) User: admin (1 of 1, 0 complete) Password: 4manah4dmin (1 of 15870 complete)
ACCOUNT CHECK: [ftp] Host: 10.10.10.1 (1 of 1, 0 complete) User: admin (1 of 1, 0 complete) Password: house69 (2 of 15870 complete)
ERROR: Thread B69FFB40: Host: 10.10.10.1 Cannot connect [unreachable], retrying (1 of 3 retries)
ERROR: Thread B69FFB40: Host: 10.10.10.1 Cannot connect [unreachable], retrying (2 of 3 retries)
ERROR: Thread B69FFB40: Host: 10.10.10.1 Cannot connect [unreachable], retrying (3 of 3 retries)
NOTICE: ftp.mod: failed to connect, port 21 was not open on 10.10.10.1
```

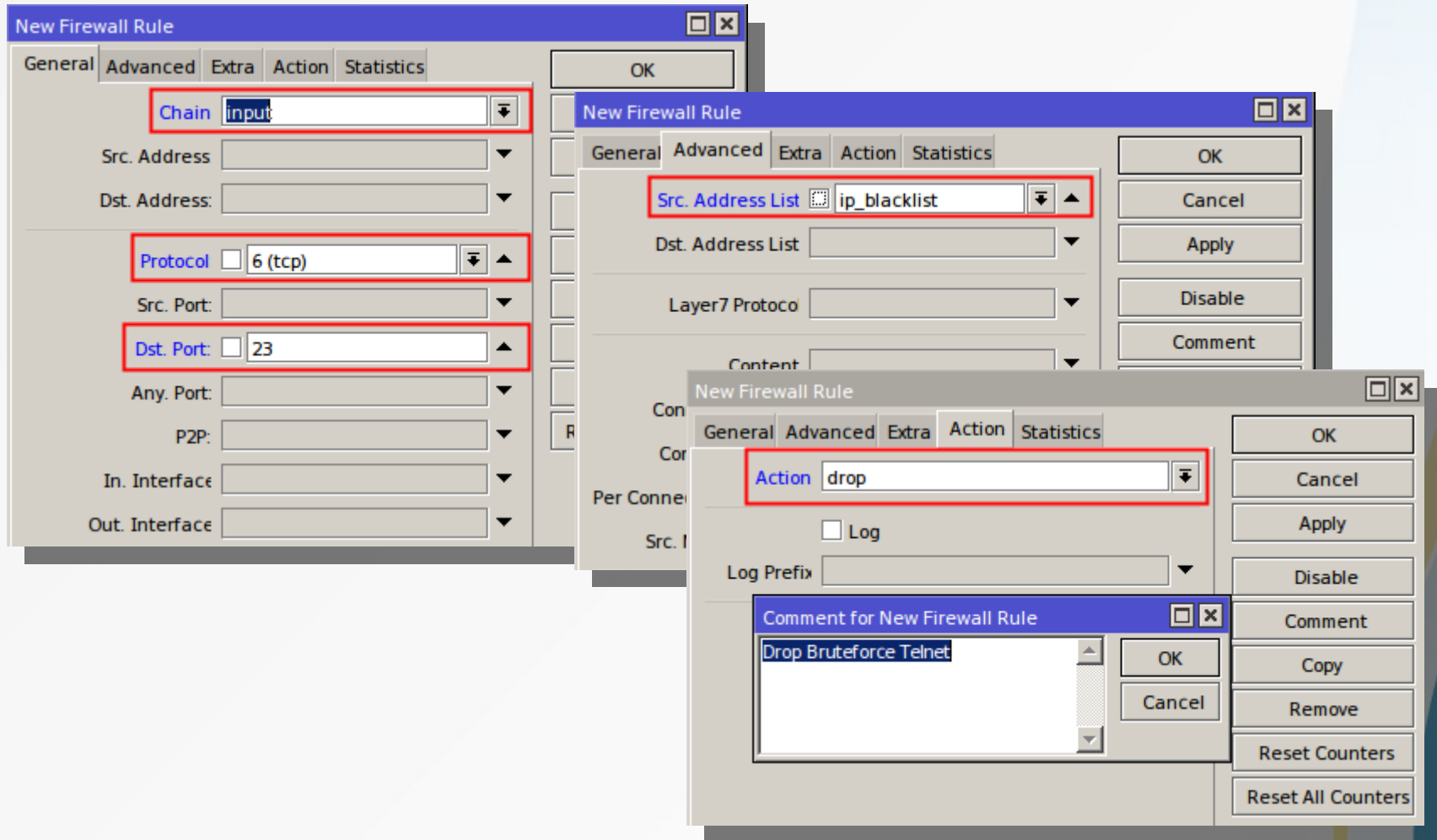


Penanganan Bruteforce Telnet

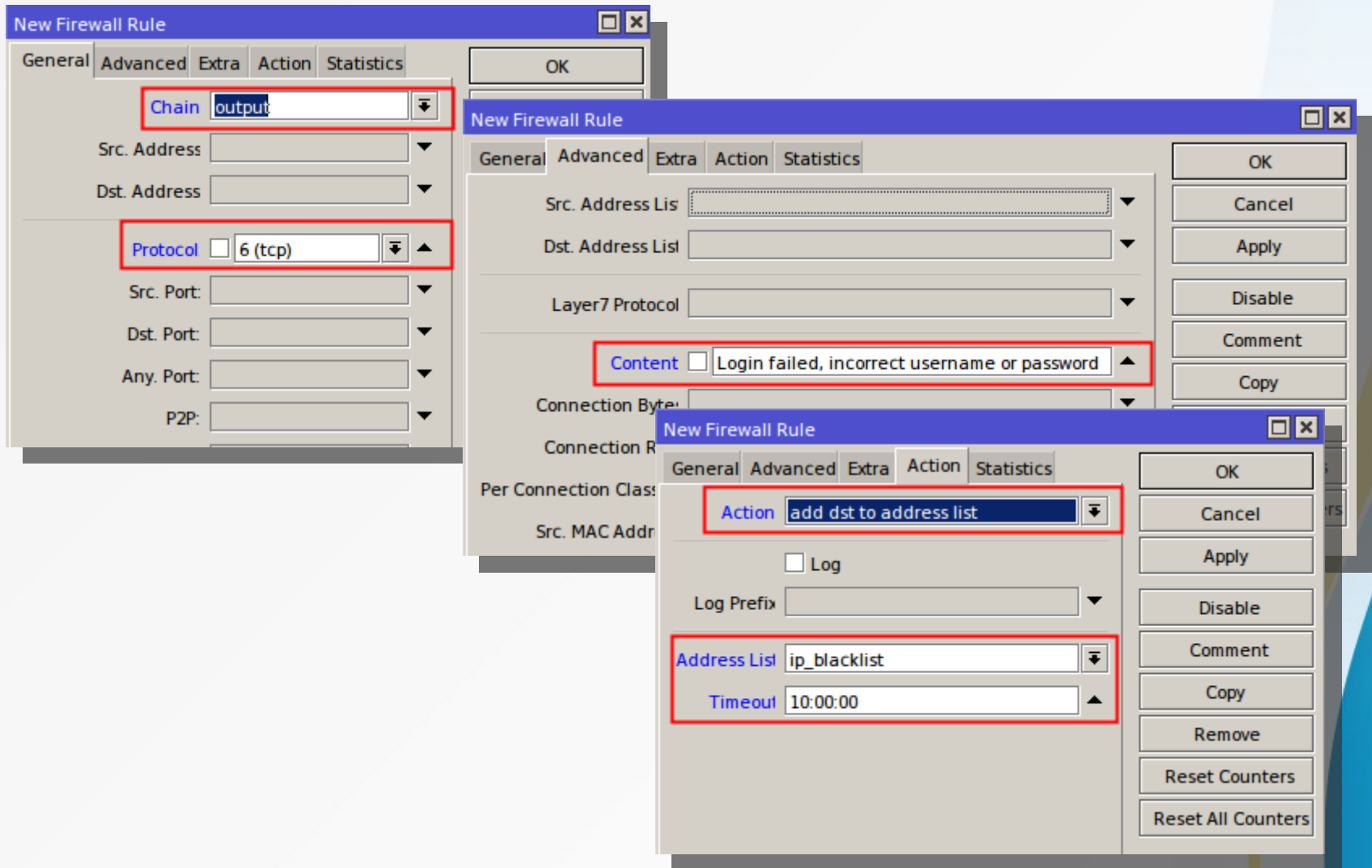
Disable service Telnet



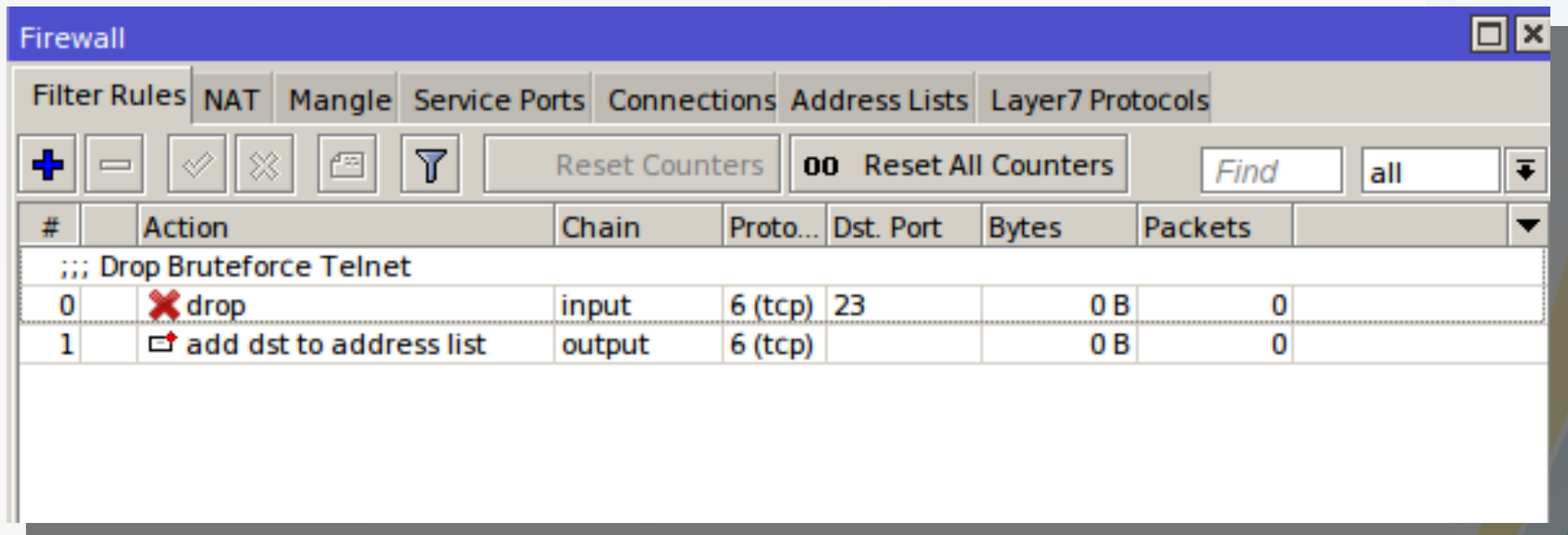
Penanganan Bruteforce Telnet dengan Firewall



Penanganan Bruteforce Telnet dengan Firewall



Hasil akhir Filter Rules



The screenshot shows the Mikrotik WinBox Firewall Filter Rules configuration window. The 'Filter Rules' tab is selected. The table below lists the configured rules for the 'Drop Brute force Telnet' filter.

#	Action	Chain	Proto...	Dst. Port	Bytes	Packets
;;; Drop Brute force Telnet						
0	 drop	input	6 (tcp)	23	0 B	0
1	 add dst to address list	output	6 (tcp)		0 B	0

Terima Kasih

