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

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 Brutef orce attack

Dictionary attack menyerang target dengan me ncoba semua kata-kata yang didefinisikan dal am sebuah list (disebut juga dengan istilah kamus atau dictionary).

Berbeda dengan **Brute force attack** yang mengg unakan 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

Pendeteksian Bruteforce MikroTIK

Log

Freeze

all

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 20:09:49	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 organizatio
ns, 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 t
ask
[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.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [ssh] Host: 10.10.10.1 (1 of 1, 0 complete) User: admin (1 of 1, 0 complete) Passwor
d: 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

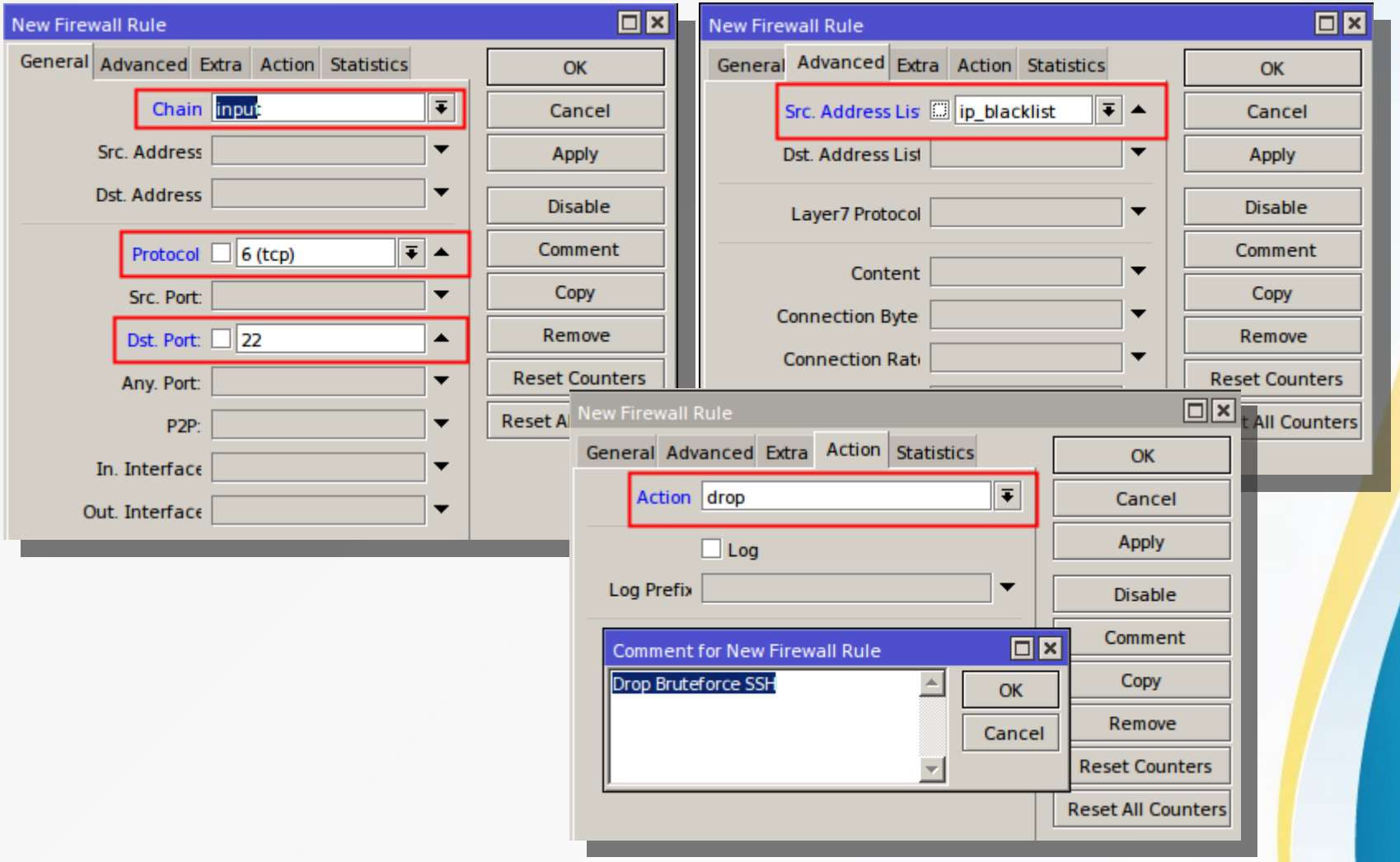
Disable service SSH

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

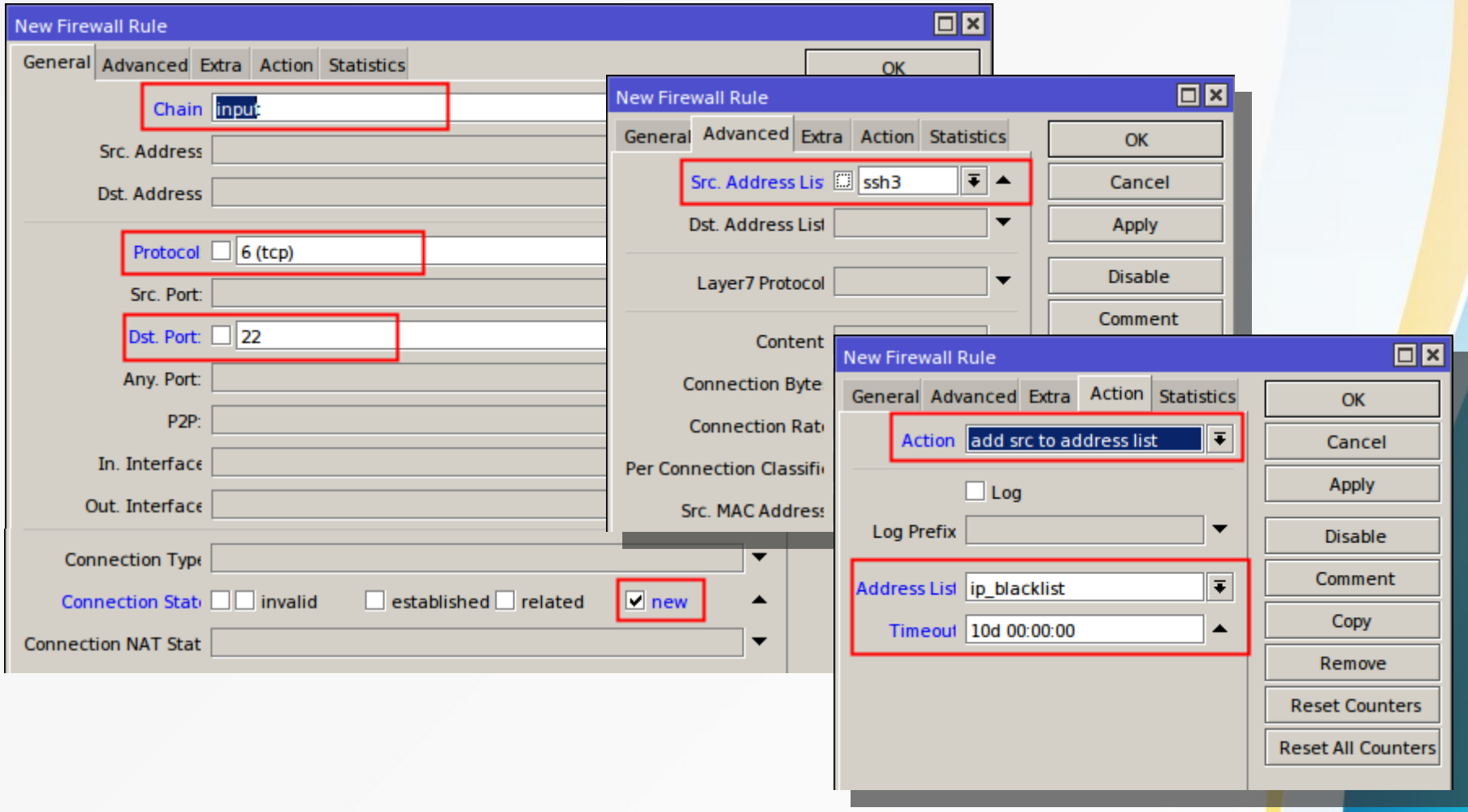
```
root@Z:/home/fajar/Documents/New Folder/exploit# nmap 10.10.10.1

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
```

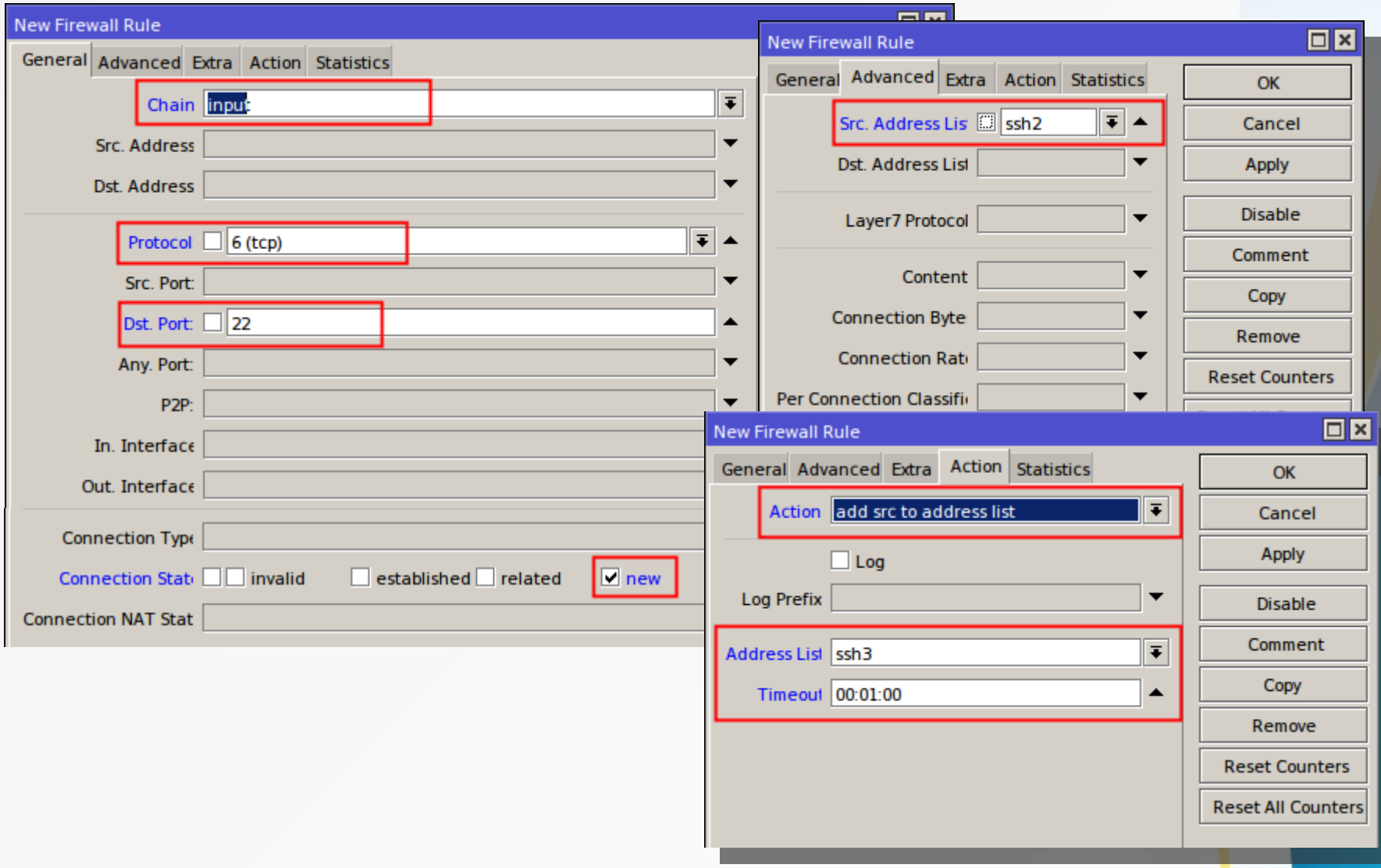
Penanganan Bruteforce SSH dengan Firewa ll



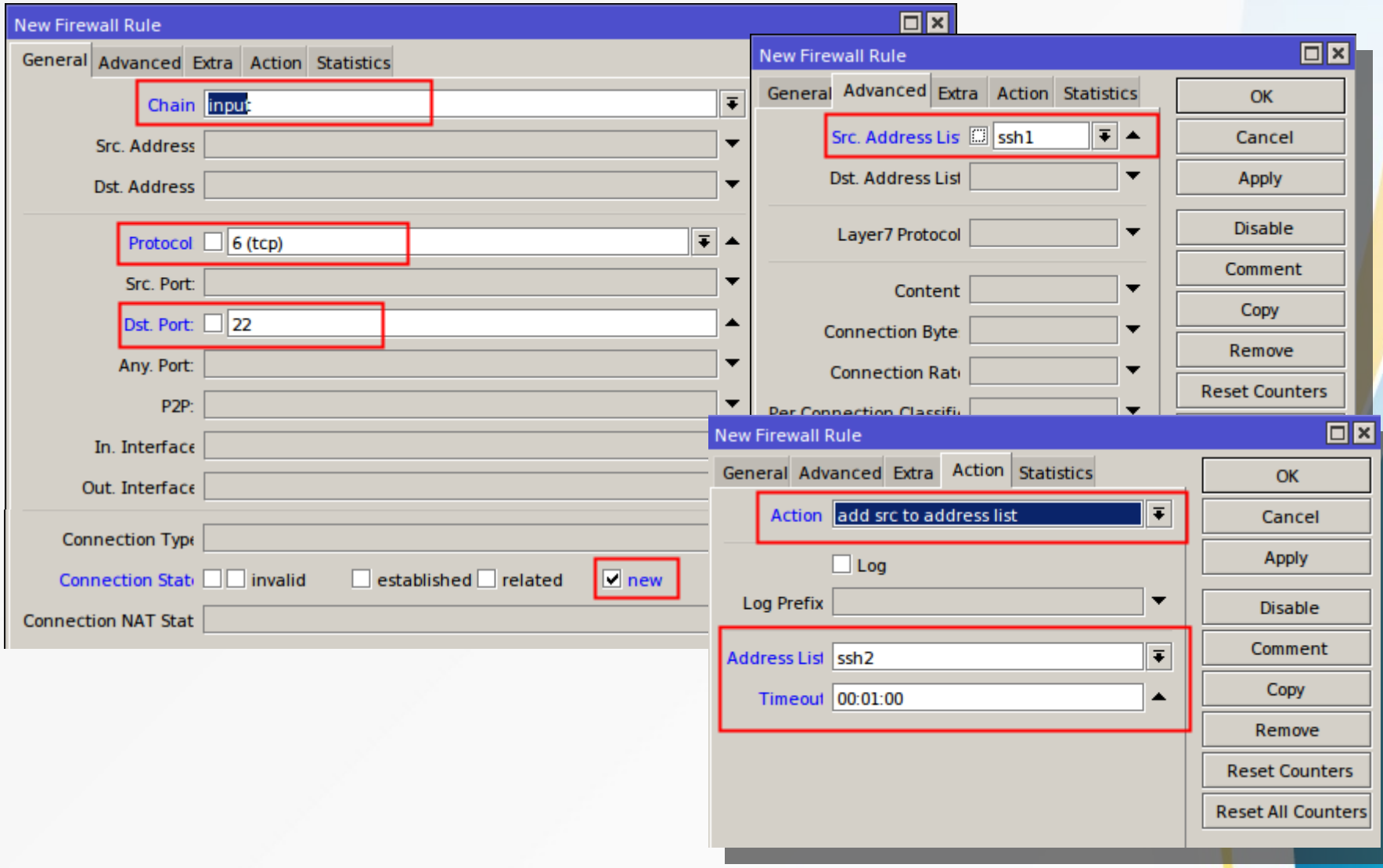
Penanganan Bruteforce SSH dengan Firewall



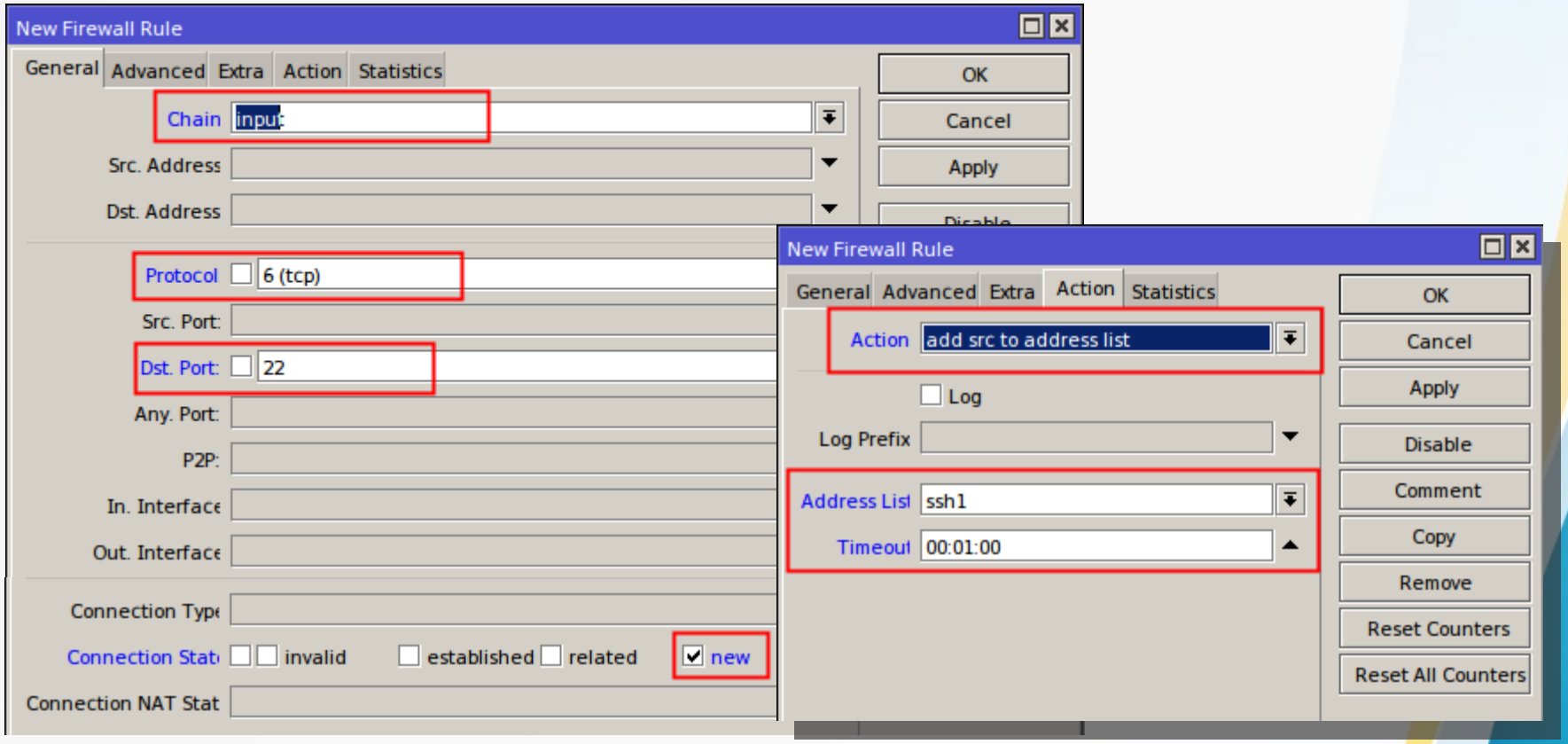
Penanganan Bruteforce SSH dengan Firewall



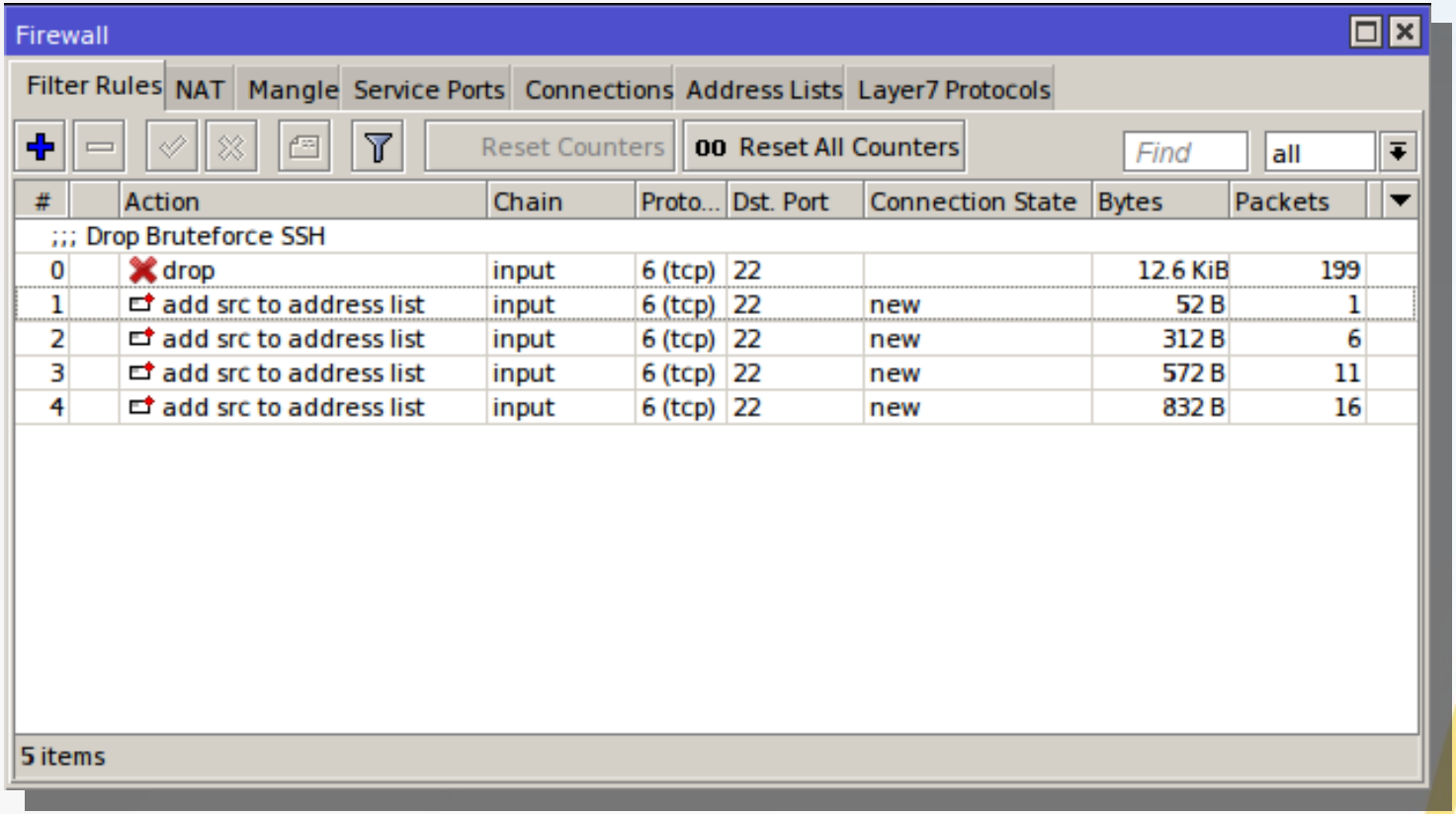
Penanganan Bruteforce SSH dengan Firewall



Penanganan Bruteforce SSH dengan Firewall

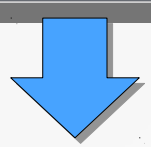


Hasil akhir Filter Rules



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
```



Firewall

Filter Rules | NAT | Mangle | Service Ports | Connections | Address Lists | Layer7 Protocols

Find | all

	Name	Address	Timeout
D	ip_blacklist	10.10.10.253	9d 23:59:46
D	ssh1	10.10.10.253	00:00:45
D	ssh2	10.10.10.253	00:00:46
D	ssh3	10.10.10.253	00:00:46

Penanganan Bruteforce FTP

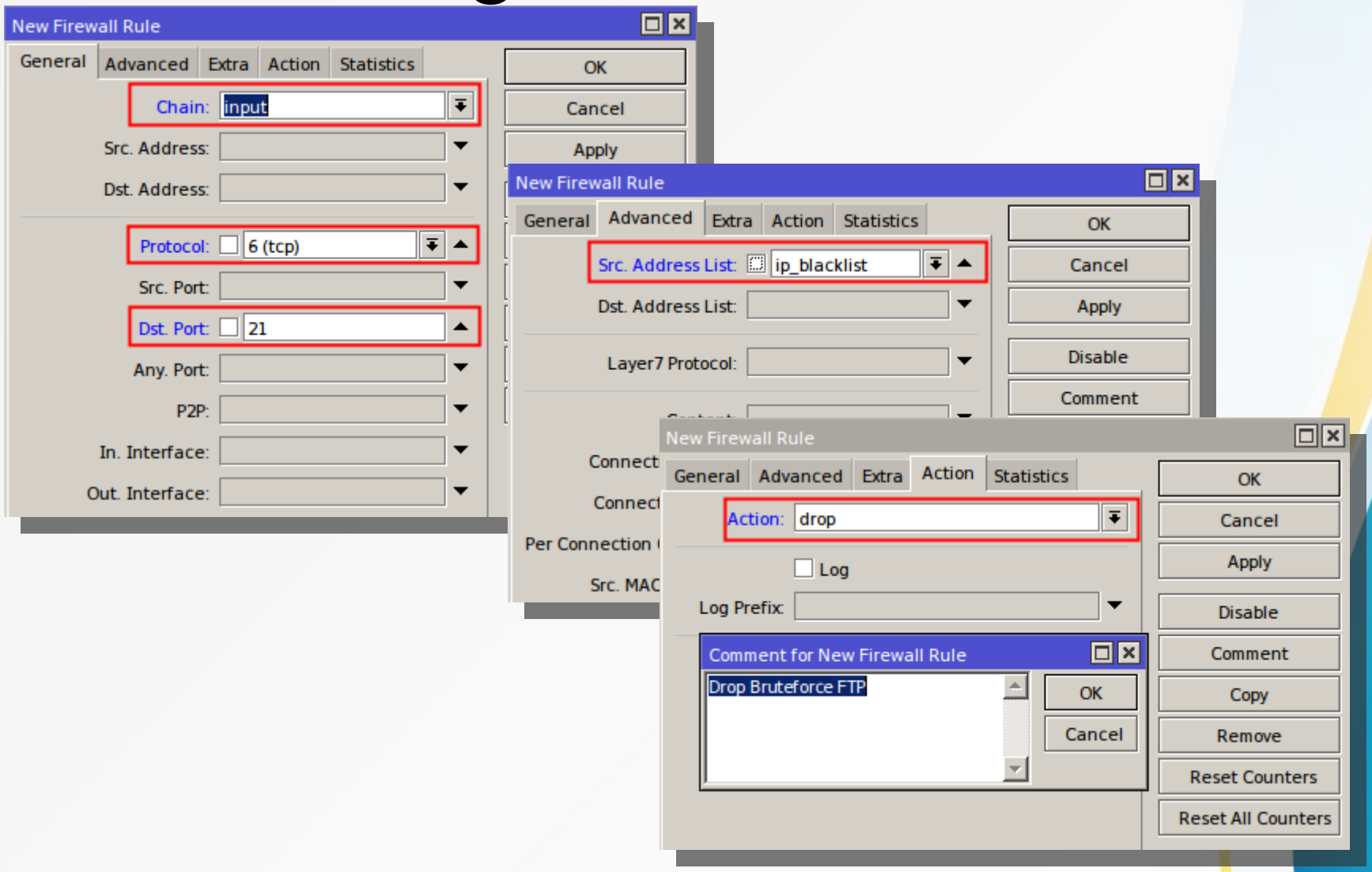
Disable service FTP

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

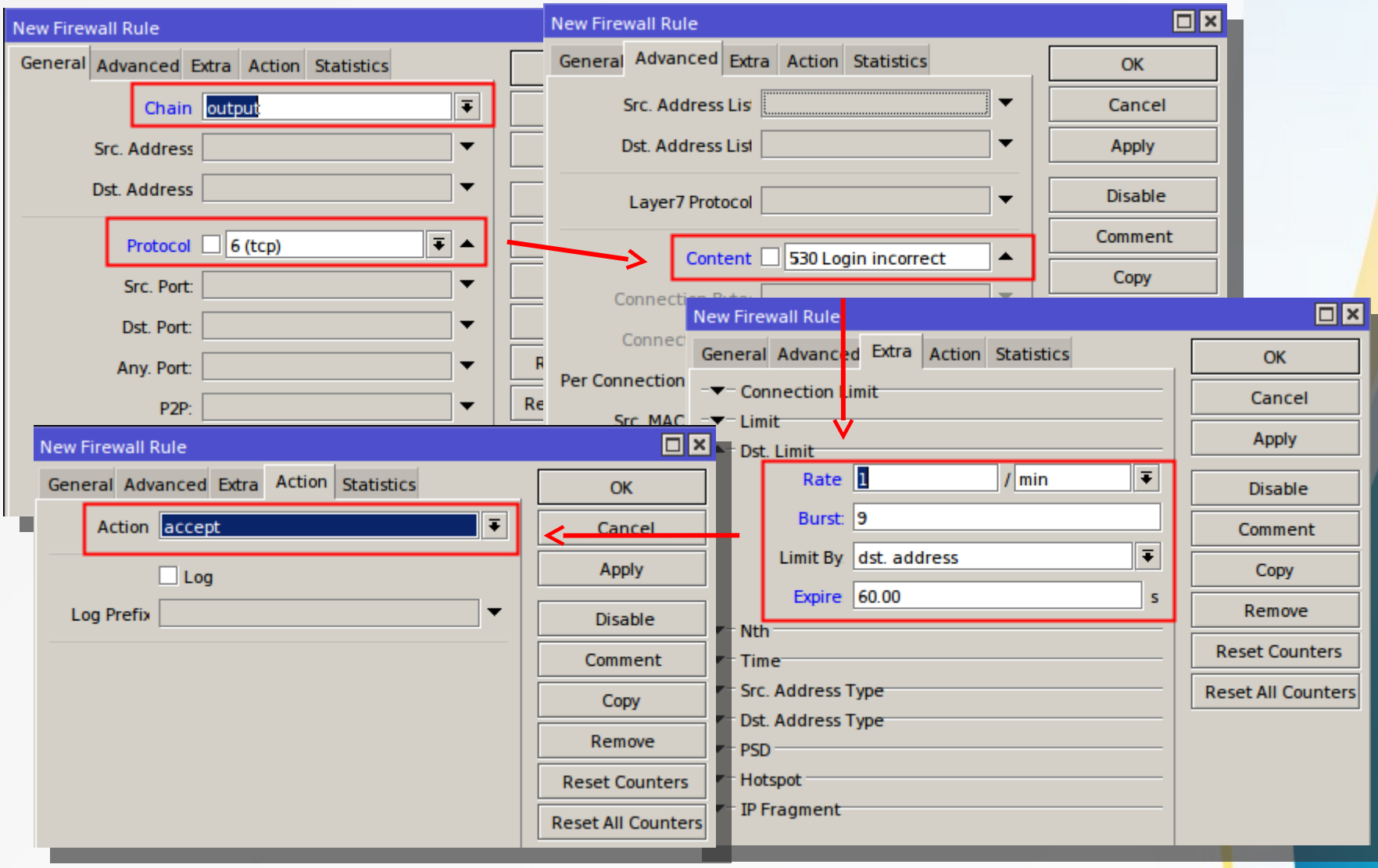
```
root@Z:/home/fajar# nmap 10.10.10.1

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
```

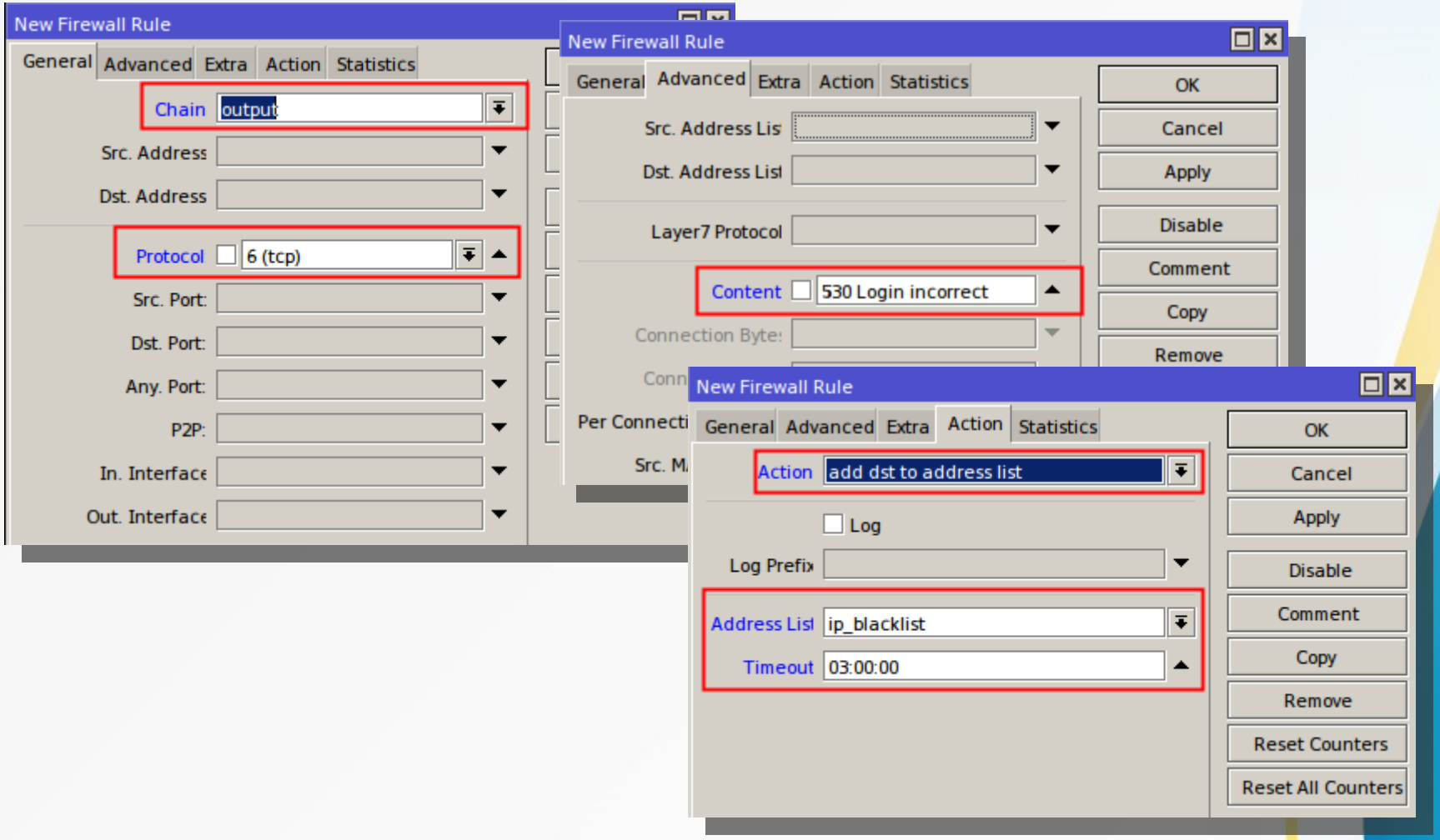
Penanganan Bruteforce FTP dengan Firewall



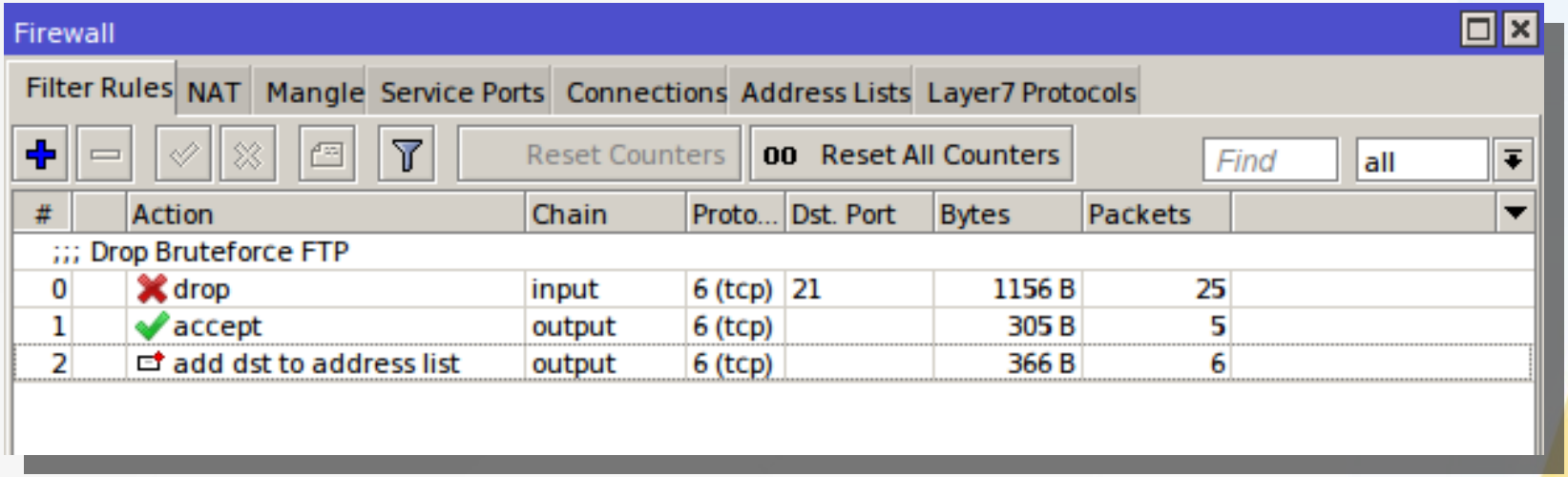
Penanganan Bruteforce FTP dengan Firewall



Penanganan Bruteforce FTP dengan Firewall

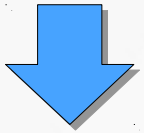


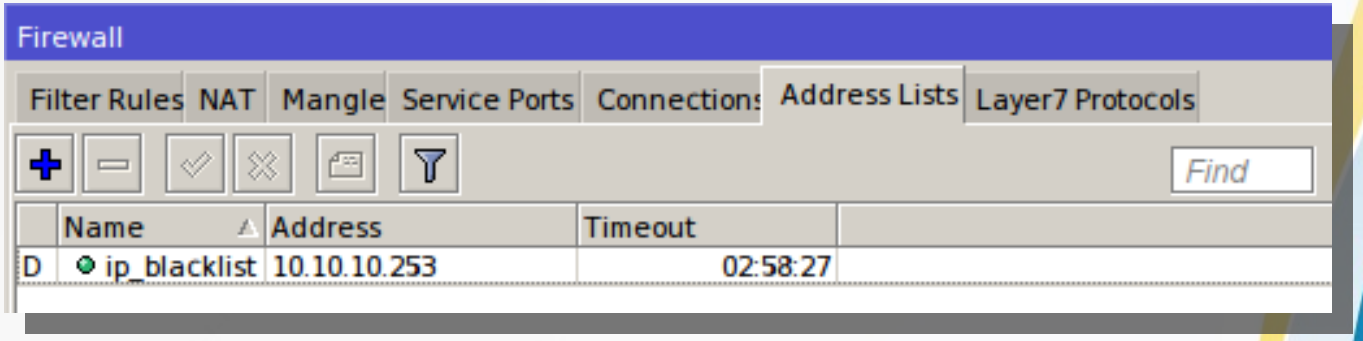
Hasil akhir Filter Rules



Testing Bruteforce FTP

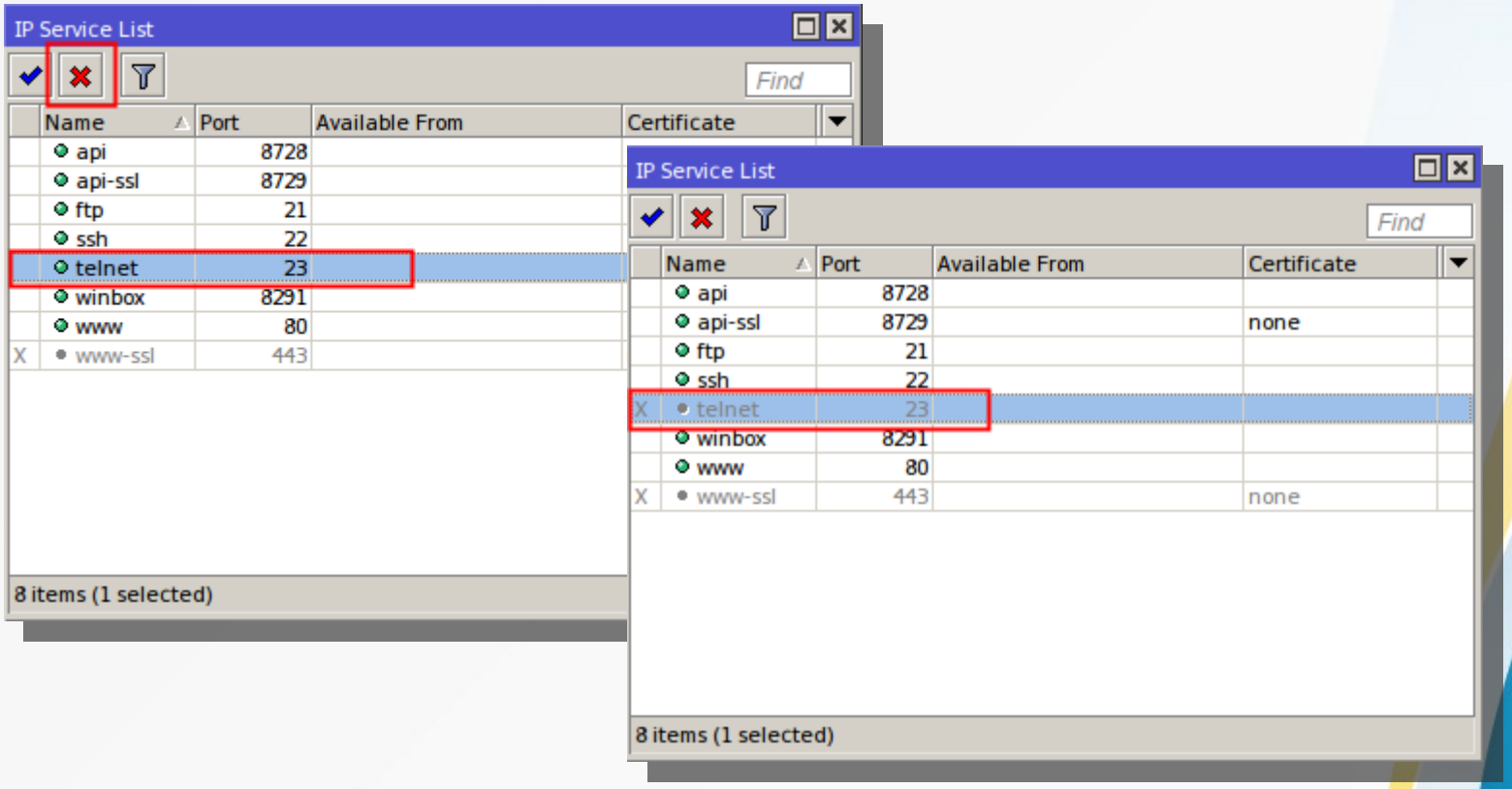
```
root@Z:/home/fajar/Documents/New Folder/exploit# medusa -h 10.10.10.1 -u admin -P pass.txt -M ftp
Medusa v2.1.1 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [ftp] Host: 10.10.10.1 (1 of 1, 0 complete) User: admin (1 of 1, 0 complete) Passwor
d: 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) Passwor
d: 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
```



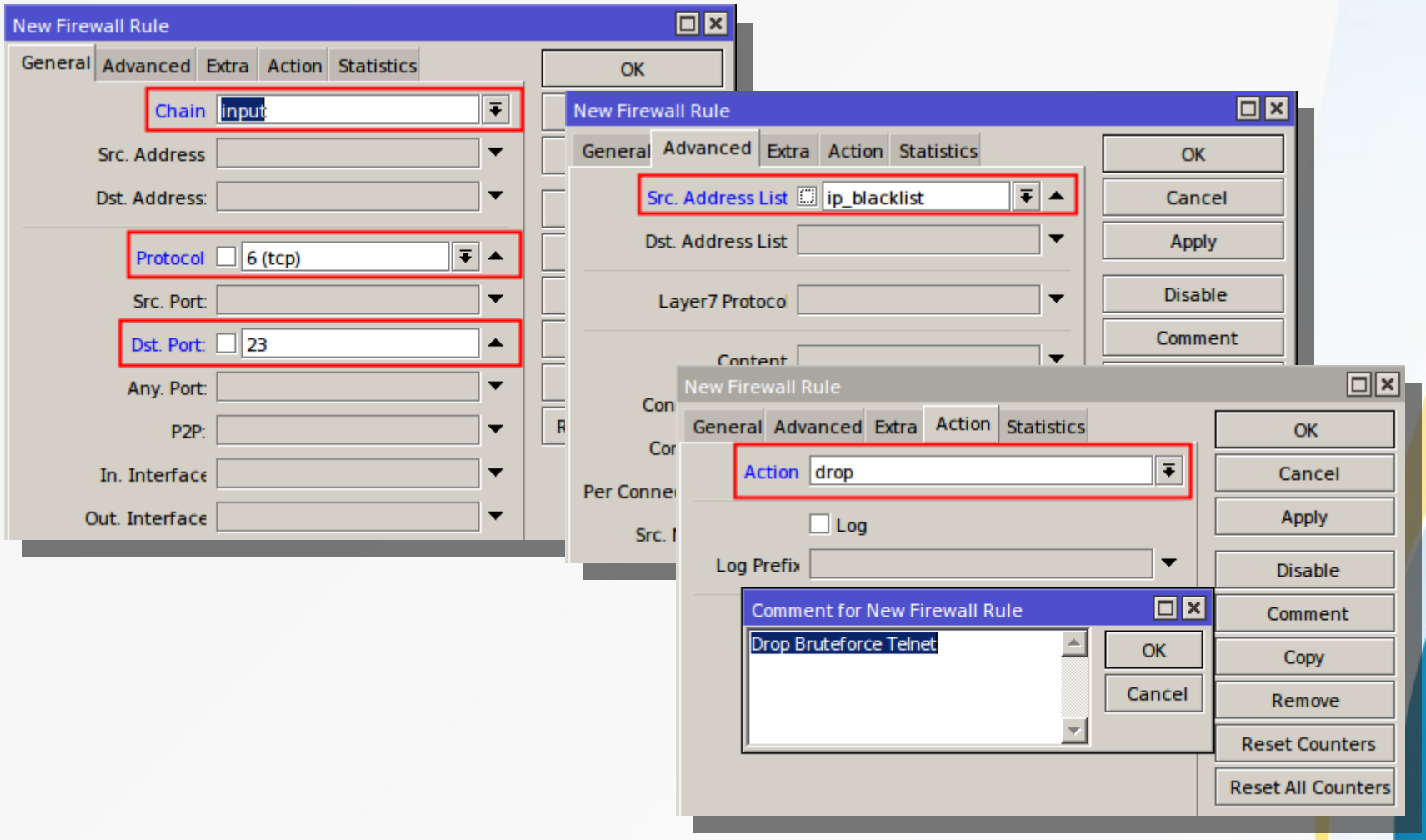


Penanganan Bruteforce Telnet

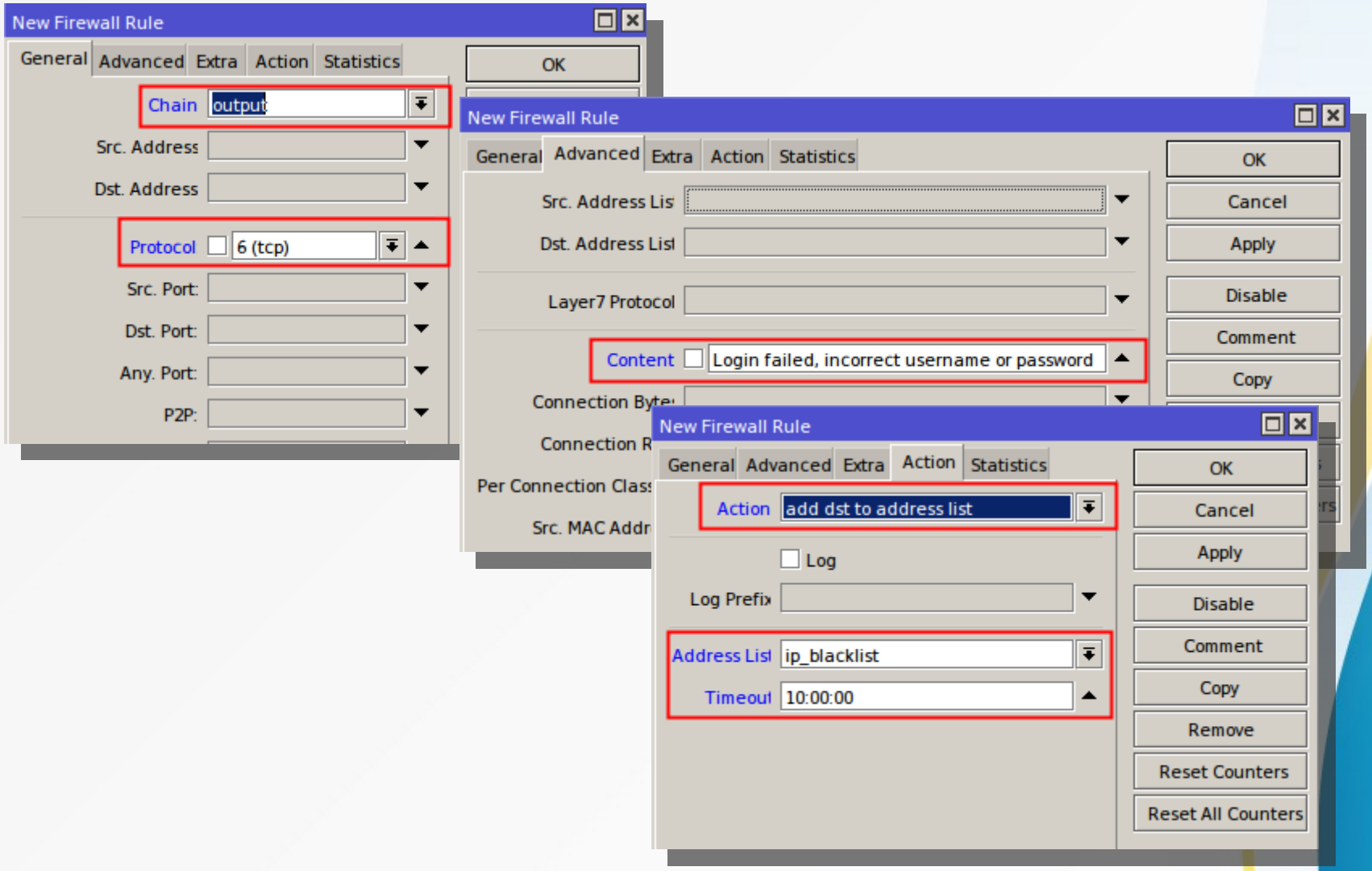
Disable service Telnet



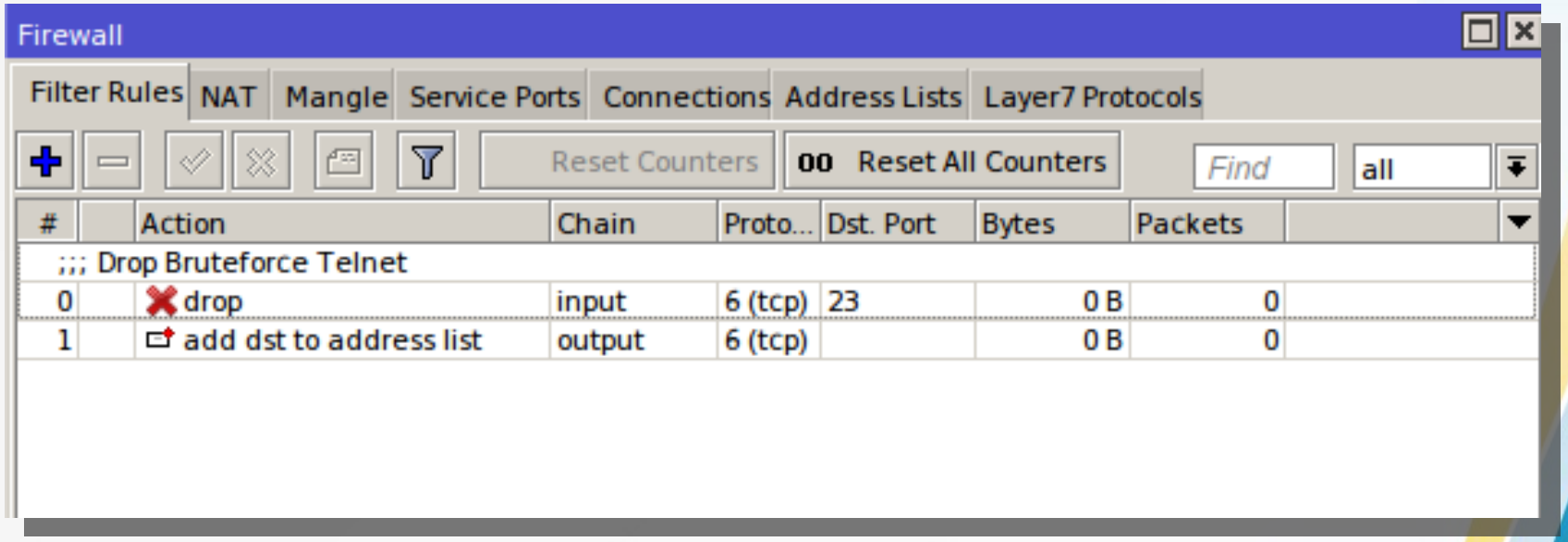
Penanganan Bruteforce Telnet dengan Firewall



Penanganan Bruteforce Telnet dengan Firewall



Hasil akhir Filter Rules



Terima Kasih

^_^