



# Prevention Login Bruteforce 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](mailto:fajarstw8899@gmail.com)
6. Contact : +62-831 4459 6878

# About SMK Catur Global

**TEMPAT PENDAFTARAN**  
YAYASAN PENDIDIKAN GLOBAL  
**SMK CATUR GLOBAL**  
PROGRAM KEAHLIAN

- 01 TEKNIK PEMERIKSAAN KENDARAAN (OTOMOTIF)
- 02 TEKNIK KELOMPOK & MANAJEMEN (TKJ)
- 03 TEKNIK PENANJANG UTAMA (RPL)
- 04 AKUNTANSI

Jl. TARA BARU BUCAL KOMP. BIDAYATUL HIDAYAH, MARGAPAN JAYA, BEKASI UTARA 17224  
(021) 88952215, 80346750  
[www.smkcaturglobal.sch.id](http://www.smkcaturglobal.sch.id) [caturglobalschool@gmail.com](mailto:caturglobalschool@gmail.com)



# 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

# Pendeteksian Bruteforce MikroTI K

The screenshot shows a Mikrotik WinBox Log window with the following data:

Time	Source	Severity	Message
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 20:09:50	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.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) 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

The image displays three screenshots of the Mikrotik WinBox Firewall Rule configuration interface, illustrating the steps to create a rule for blocking SSH brute-force attacks.

**Screenshot 1: General Tab**  
Chain:   
Src. Address:   
Dst. Address:   
Protocol:  6 (tcp)  
Src. Port:   
Dst. Port:   
Any. Port:   
P2P:   
In. Interface:   
Out. Interface:

**Screenshot 2: Advanced Tab**  
Src. Address List:   
Dst. Address List:   
Layer7 Protocol:   
Content:   
Connection Byte:   
Connection Rate:

**Screenshot 3: Action Tab**  
Action:   
 Log  
Log Prefix:

**Screenshot 4: Comment for New Firewall Rule**  
Drop Bruteforce SSH

# Penanganan Bruteforce SSH dengan Firewall

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

- Top Screenshot (General Tab):** Shows the initial configuration. The **Chain** is set to `input`. The **Protocol** is set to `6 (tcp)`. The **Dst. Port** is set to `22`. The **new** checkbox under **Connection Stat** is checked.
- Middle Screenshot (Advanced Tab):** Shows the **Src. Address List** dropdown menu set to `ssh3`.
- Bottom Screenshot (Action Tab):** Shows the **Action** dropdown menu set to `add src to address list`. The **Address List** is set to `ip_blacklist` and the **Timeout** is set to `10d 00:00:00`.

# Penanganan Bruteforce SSH dengan Firewall

The image displays three screenshots of the Mikrotik Firewall Rule configuration interface, illustrating the steps to handle brute-force SSH attacks.

**Top Left Screenshot (General Tab):** Shows the initial configuration. The Chain is set to `input`. The Protocol is set to `6 (tcp)`. The Destination Port is set to `22`. The `new` connection state checkbox is checked.

**Top Right Screenshot (Advanced Tab):** Shows the configuration for the source address list. The Src. Address List is set to `ssh2`.

**Bottom Screenshot (Action Tab):** Shows the configuration for the action. The Action is set to `add src to address list`. The Log checkbox is unchecked. The Address List is set to `ssh3`. The Timeout is set to `00:01:00`.

# Penanganan Bruteforce SSH dengan Firewall

The image displays three sequential screenshots of the Mikrotik Firewall Rule configuration interface, illustrating the steps to create a rule for handling SSH brute force attacks.

**First Screenshot (New Firewall Rule - General tab):** The 'Chain' is set to 'input'. The 'Protocol' is set to '6 (tcp)'. The 'Dst. Port' is set to '22'. The 'Connection Stat' checkbox is checked, and the 'new' option is selected.

**Second Screenshot (New Firewall Rule - General tab):** The 'Src. Address List' is set to 'ssh1'. The 'Action' is set to 'add src to address list'. The 'Log' checkbox is unchecked.

**Third Screenshot (New Firewall Rule - Action tab):** The 'Address List' is set to 'ssh2'. The 'Timeout' is set to '00:01:00'.



# Penanganan Bruteforce SSH dengan Firewall

New Firewall Rule

General Advanced Extra Action Statistics

Chain

Src. Address

Dst. Address

Protocol  6 (tcp)

Src. Port:

Dst. Port:  22

Any. Port:

P2P:

In. Interface

Out. Interface

Connection Type:

Connection Stat:  invalid  established  related  new

Connection NAT Stat:

OK  
Cancel  
Apply  
Disable

New Firewall Rule

General Advanced Extra Action Statistics

Action

Log

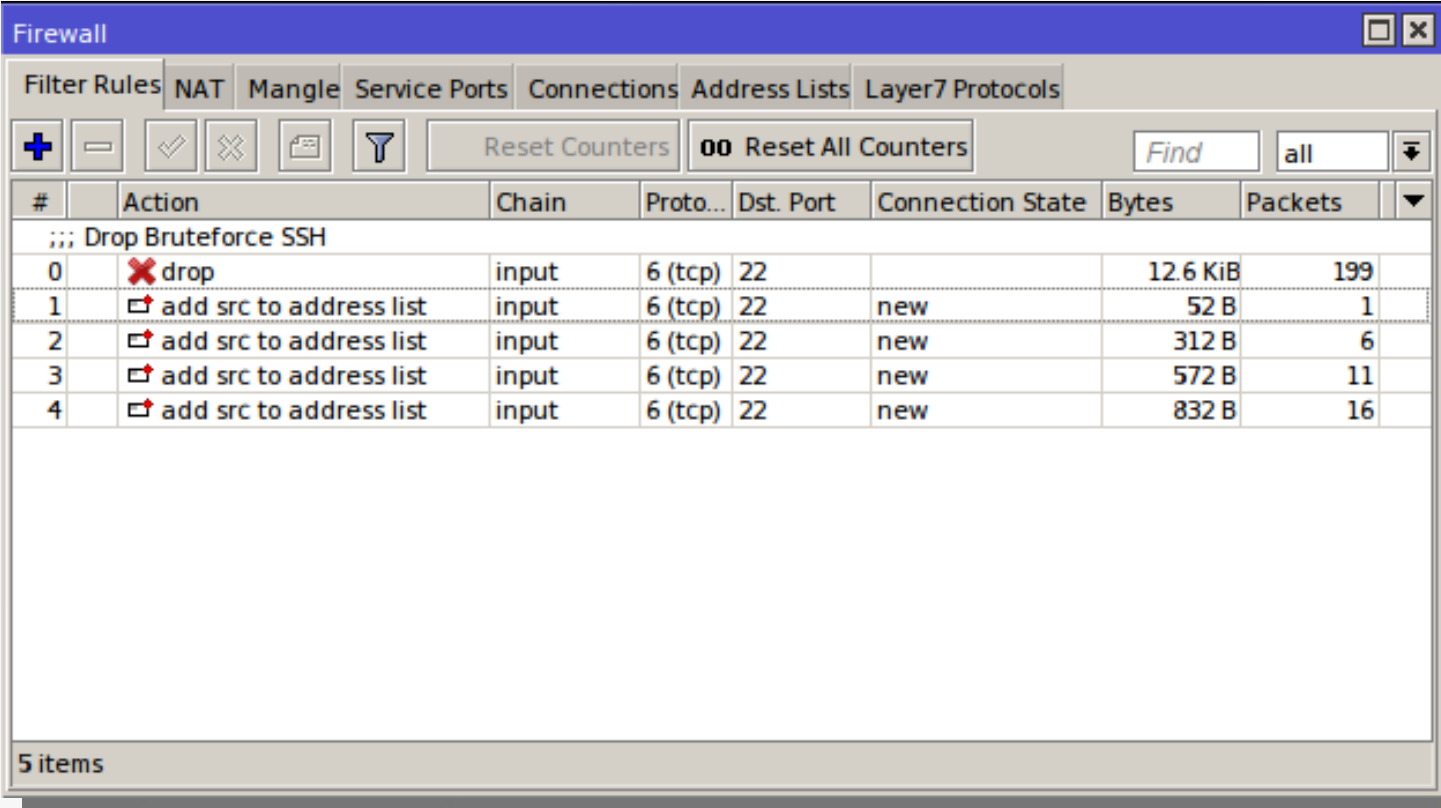
Log Prefix

Address List

Timeout

OK  
Cancel  
Apply  
Disable  
Comment  
Copy  
Remove  
Reset Counters  
Reset All Counters

# Hasil akhir Filter Rules



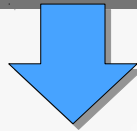
The screenshot shows the Mikrotik WinBox Firewall Filter Rules configuration window. The window title is "Firewall". The "Filter Rules" tab is selected. The interface includes a toolbar with icons for adding, deleting, enabling, disabling, and saving rules, along with a "Reset Counters" button and a "00 Reset All Counters" button. A search bar contains the text "Find" and "all". The main area displays a table of filter rules. The table has columns for #, Action, Chain, Proto..., Dst. Port, Connection State, Bytes, and Packets. The rules are grouped under "Drop Bruteforce SSH". Rule 0 is a "drop" action. Rules 1-4 are "add src to address list" actions. The status bar at the bottom indicates "5 items".

#	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
```



Firewall

Filter Rules NAT Mangle Service Ports Connections Address Lists Layer7 Protocols

+ - ✓ ✗ [Folder Icon] [Filter Icon] Find all [Dropdown Arrow]

	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

The image displays three overlapping screenshots of the Mikrotik WinBox Firewall Rule configuration interface, illustrating the steps to create a rule for blocking brute-force FTP attempts.

- First Screenshot (New Firewall Rule - General):** Shows the initial configuration. The **Chain** is set to `input`. The **Protocol** is set to `6 (tcp)`. The **Dst. Port** is set to `21`. These three fields are highlighted with red boxes.
- Second Screenshot (New Firewall Rule - General):** Shows the **Src. Address List** set to `ip_blacklist`. This field is highlighted with a red box.
- Third Screenshot (New Firewall Rule - Action):** Shows the **Action** set to `drop`. This field is highlighted with a red box.
- Fourth Screenshot (Comment for New Firewall Rule):** Shows the **Comment** field containing the text `Drop Bruteforce FTP`.

# Penanganan Bruteforce FTP dengan Firewall

The image displays three overlapping screenshots of the Mikrotik WinBox Firewall Rule configuration interface, illustrating the steps to create a rule for blocking brute force FTP attacks.

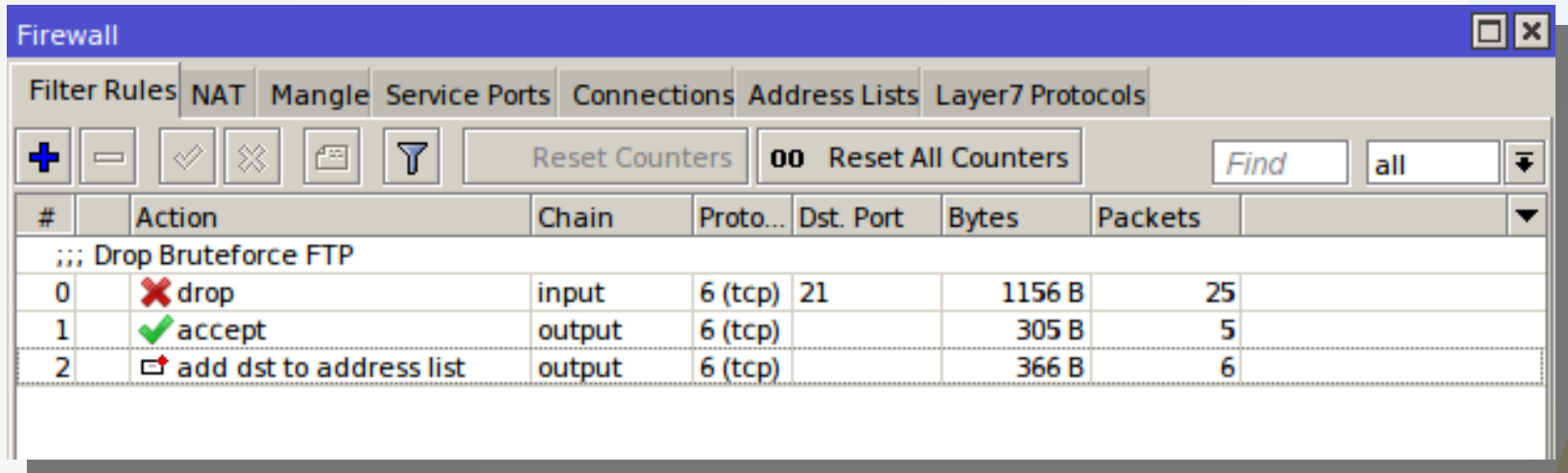
- Top Screenshot (General Tab):** Shows the 'Chain' set to 'output' and the 'Protocol' set to '6 (tcp)'. A red box highlights the 'Chain' dropdown, and another red box highlights the 'Protocol' dropdown.
- Middle Screenshot (Advanced Tab):** Shows the 'Content' field set to '530 Login incorrect'. A red box highlights this field, and a red arrow points from the 'Protocol' field in the top screenshot to this field.
- Bottom Screenshot (Action Tab):** Shows the 'Action' set to 'accept'. A red box highlights this dropdown, and a red arrow points from the 'Content' field in the middle screenshot to this field.
- Bottom Screenshot (Advanced Tab):** Shows the 'Connection Limit' configuration with 'Rate' set to 1 / min, 'Burst' set to 9, 'Limit By' set to 'dst. address', and 'Expire' set to 60.00 s. A red box highlights these fields, and a red arrow points from the 'Content' field in the middle screenshot to the 'Rate' field.

# Penanganan Bruteforce FTP dengan Firewall

The image displays three overlapping screenshots of the Mikrotik WinBox interface, illustrating the configuration of a Firewall Rule to handle brute-force FTP attempts. Red boxes highlight the key configuration elements in each step:

- First Screenshot (General tab):** Shows the rule chain set to **output** and the protocol set to **6 (tcp)**.
- Second Screenshot (Advanced tab):** Shows the **Content** field configured to **530 Login incorrect**.
- Third Screenshot (Action tab):** Shows the action set to **add dst to address list**, with the **Address List** set to **ip\_blacklist** and the **Timeout** set to **03:00:00**.

# Hasil akhir Filter Rules



The screenshot shows the Mikrotik WinBox Firewall Filter Rules configuration window. The window title is "Firewall". The "Filter Rules" tab is selected, with other tabs including NAT, Mangle, Service Ports, Connections, Address Lists, and Layer7 Protocols. The interface includes a toolbar with icons for adding (+), removing (-), enabling (checkmark), disabling (cross), and filtering (funnel), along with buttons for "Reset Counters" and "Reset All Counters". A search field labeled "Find" contains the text "all". Below the toolbar is a table with columns: #, Action, Chain, Proto..., Dst. Port, Bytes, and Packets. The table shows three rules under the heading ";;; Drop Bruteforce FTP".

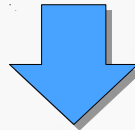
#	Action	Chain	Proto...	Dst. Port	Bytes	Packets
;;; Drop Bruteforce FTP						
0	drop	input	6 (tcp)	21	1156 B	25
1	accept	output	6 (tcp)		305 B	5
2	add dst to address list	output	6 (tcp)		366 B	6



# 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
```



Firewall

Filter Rules NAT Mangle Service Ports Connections Address Lists Layer7 Protocols

+ - ✓ ✗ [icon] [icon] Find

	Name	Address	Timeout
D	ip_blacklist	10.10.10.253	02:58:27

# Penanganan Bruteforce Telnet

Disable service Telnet

The image shows two screenshots of the 'IP Service List' window in a network management application. The top screenshot shows the 'telnet' service (port 23) selected in a list of services. The bottom screenshot shows the same list, but with a red 'X' icon in the left margin next to the 'telnet' entry, indicating that the service has been disabled.

**IP Service List (Top Screenshot)**

Name	Port	Available From	Certificate
api	8728		
api-ssl	8729		
ftp	21		
ssh	22		
telnet	23		
winbox	8291		
www	80		
X • www-ssl	443		

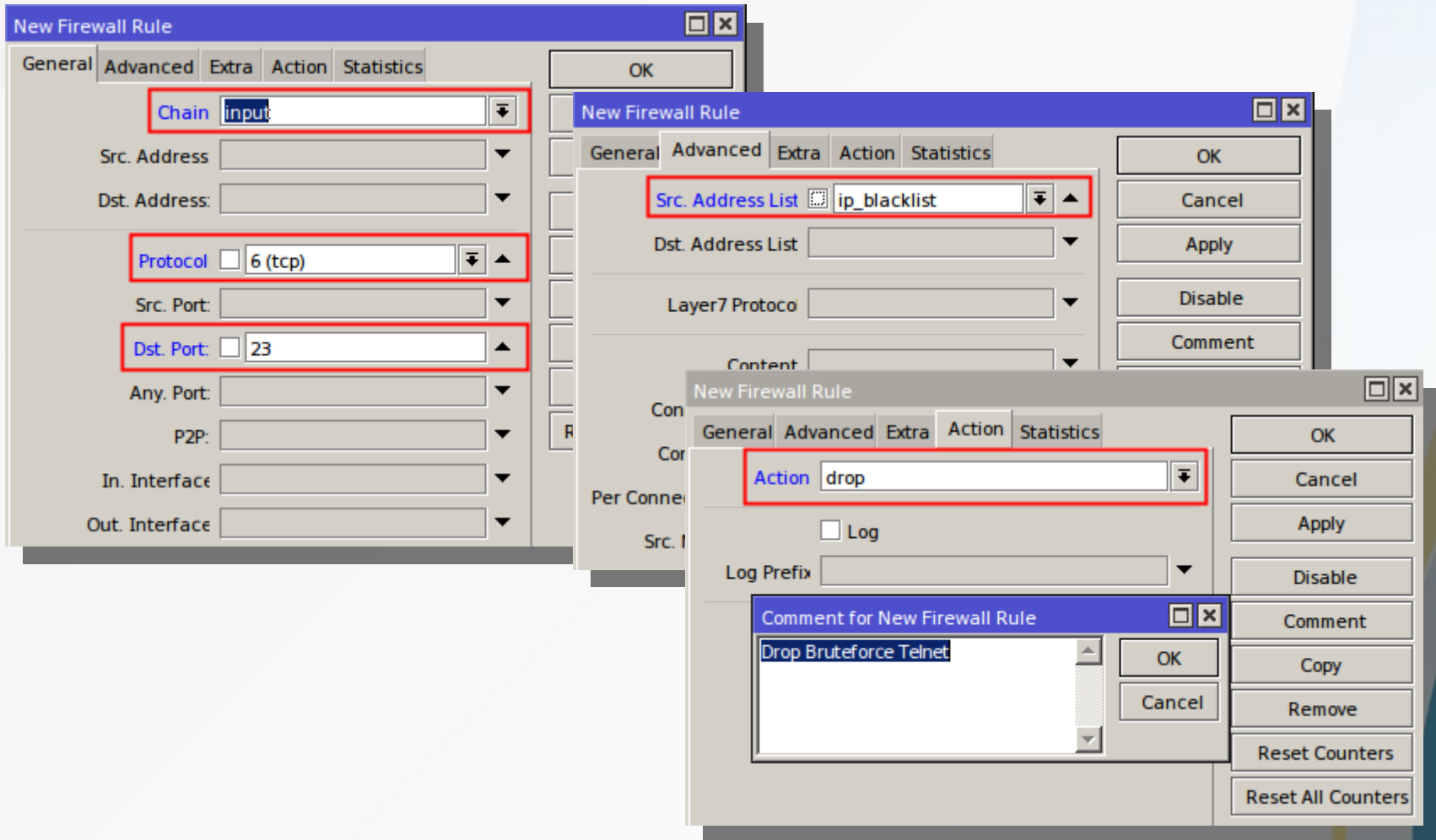
8 items (1 selected)

**IP Service List (Bottom Screenshot)**

Name	Port	Available From	Certificate
api	8728		
api-ssl	8729		none
ftp	21		
ssh	22		
X • telnet	23		
winbox	8291		
www	80		
X • www-ssl	443		none

8 items (1 selected)

# Penanganan Bruteforce Telnet dengan Firewall

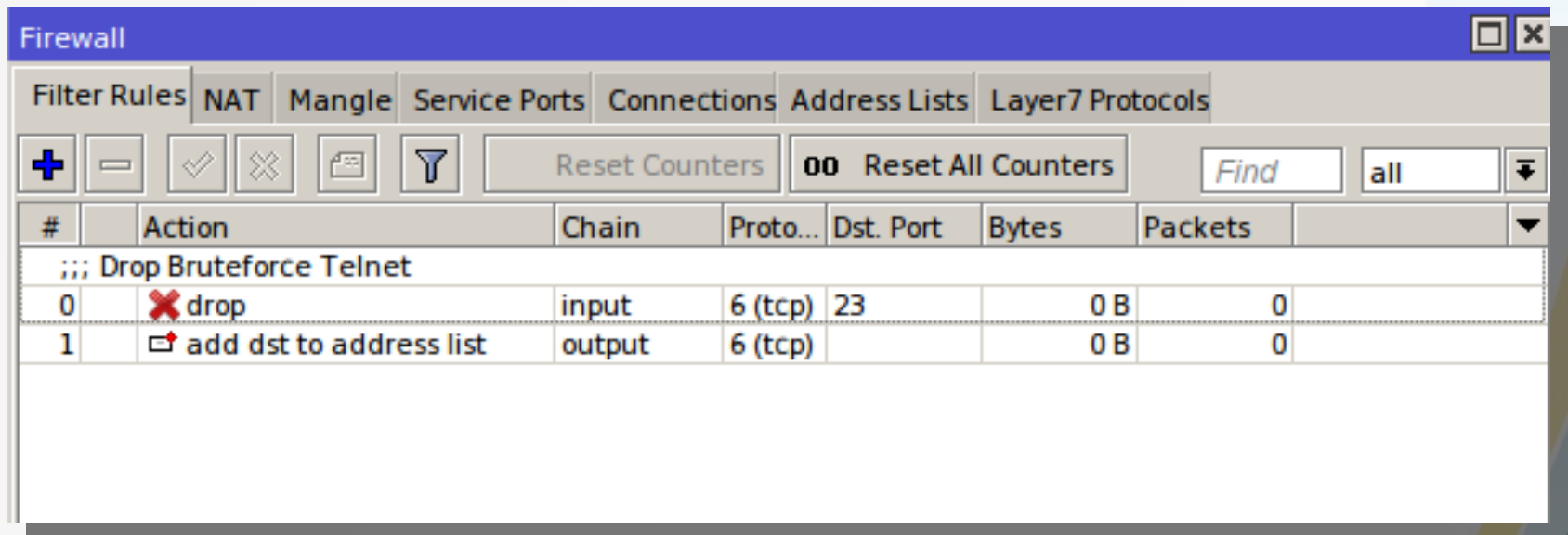


# Penanganan Bruteforce Telnet dengan Firewall



The image displays three overlapping screenshots of the Mikrotik WinBox 'New Firewall Rule' configuration dialog, illustrating the steps to create a rule for handling Telnet brute-force attacks. Red boxes highlight the specific configuration elements in each step:

- Top Screenshot (General tab):** Shows the 'Chain' dropdown menu set to 'output' and the 'Protocol' dropdown menu set to '6 (tcp)'. The 'Src. Address' and 'Dst. Address' fields are empty.
- Middle Screenshot (Advanced tab):** Shows the 'Content' field with the text 'Login failed, incorrect username or password' entered. The 'Src. Address List' and 'Dst. Address List' fields are empty.
- Bottom Screenshot (Action tab):** Shows the 'Action' dropdown menu set to 'add dst to address list'. The 'Log' checkbox is unchecked. The 'Address List' dropdown menu is set to 'ip\_blacklist' and the 'Timeout' field is set to '10:00:00'.

# Hasil akhir Filter Rules



The screenshot shows the Mikrotik WinBox Firewall Filter Rules configuration window. The window title is "Firewall". The "Filter Rules" tab is selected, with other tabs including "NAT", "Mangle", "Service Ports", "Connections", "Address Lists", and "Layer7 Protocols". The interface includes a toolbar with icons for adding (+), deleting (-), enabling (checkmark), disabling (X), and applying (funnel), along with buttons for "Reset Counters" and "00 Reset All Counters". A search field contains "Find" and "all". The main area displays a table of filter rules under the heading ";;; Drop Bruteforce Telnet".

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

# Terima Kasih

---

