How to Protecting your MikroTik Router From Brutes-Force Attack

By : Teddy Yuliswar

May 8, 2017

Vientiane, Laos

Indonetworkers.com

Everytime Always Learn

- **Where I Come From?**

Please visit to my hometown : Tanah Datar regency, West Sumatra

Pariangan in western Sumatra is said to be the oldest—and most culturally significant—village of the Minangkabau people and has numerous well-preserved examples of traditional Minangkabau pointed-roof architecture.
(**Most Beautiful Towns in the World by budget travel Magazine New York)**

Please visit to my hometown : Tanah Datar regency, West Sumatra

The Pacu Jawi is an age old Indonesian festival which sees fearless competitors dragged through the mud while clinging onto the tails of two charging cows The tradition has been around for hundreds of years and celebrates the end of the rice harvest season.

Please visit to my hometown : Tanah Datar regency, West Sumatra

is the istana (royal palace) of the former Pagaruyung Kingdom, located in Tanjung Emas subdistrict near Batusangkar town, Tanah Datar Regency, The palace has been destroyed by fire for several times, in 1804, 1966 and 2007. It has been rebuilt again and today function as museum and popular tourist attraction.

Please visit to my hometown : Tanah Datar regency, West Sumatra

Rendang is a spicy meat dish which originated from the Minangkabau and is now commonly served across the country.
The Most delicious Food in the World

a Norwegian singer Audun Kvitland create a song to ode to one of Indonesia's most popular dishes,
Nasi Padang (rice with various side dishes).

We also have many more.. Please visit ☺

- **Teddy Yuliswar**
- Using Mikrotik Since RouterOS 2.97 (2008)
- MTCNA, MTCRE, MTCTCE,MTCWE, MTCUME MTCINE,MTCIPv6E
- Mikrotik Certified Trainer since October 2016 (Dubai, UEA)
- https://mikrotik.com/training/centers/asia/indonesia
- Mikrotik Certified Consultant Indonesia
- https://mikrotik.com/consultants/
- Mikrotik Academy Coordinator
- https://mikrotik.com/training/academy/asia/indonesia

Security?

“Security is inversely proportional to convenience”

Indonetworkers.com

Everytime Always Learn

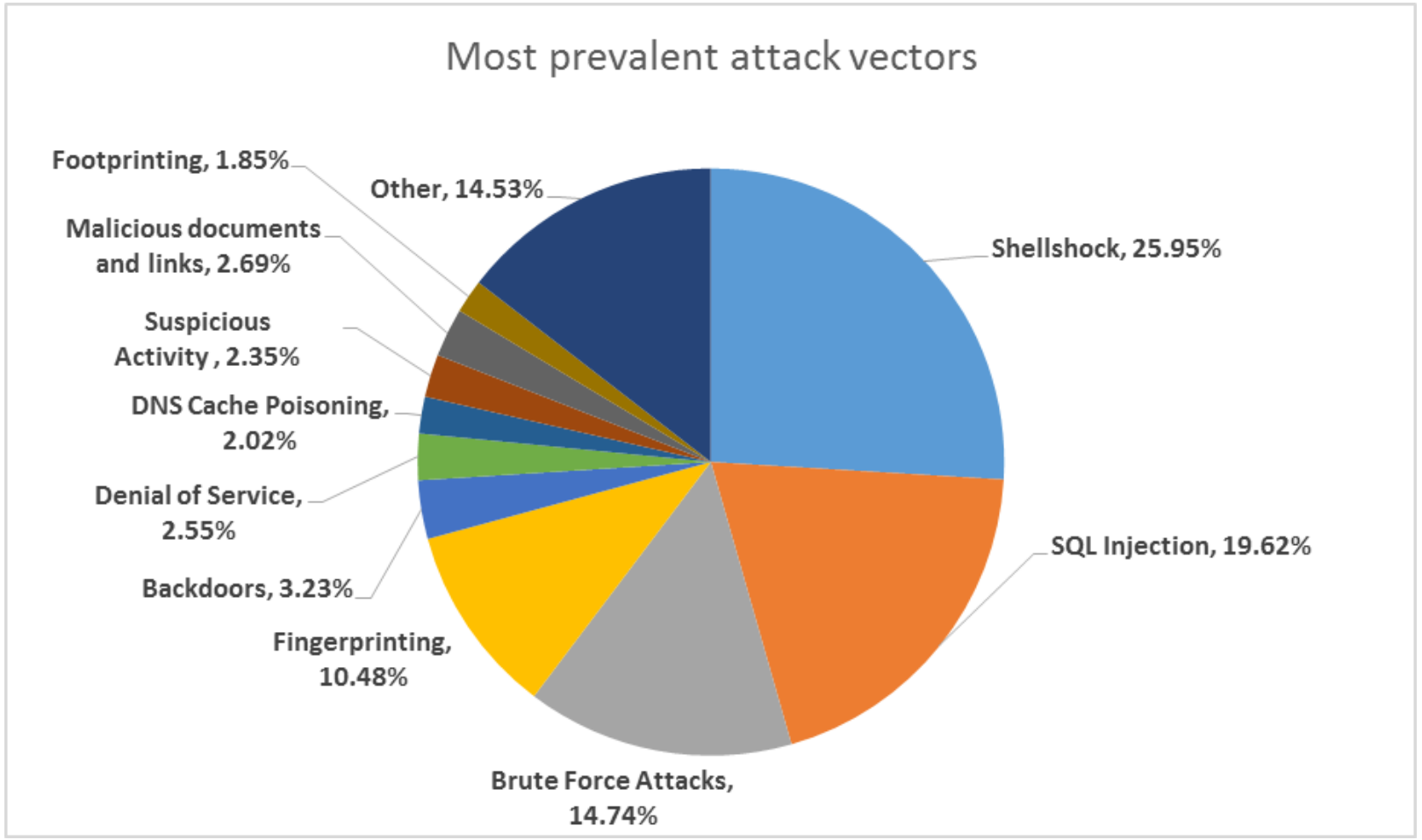
WIKIPEDIA

Network Security

Network security consists of the policies and practices adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources.

WIKIPEDIA

In computer and computer networks an **attack** is any attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset.



What is Firewall?

WIKIPEDIA

a firewall is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules.

Indonetworkers.com

Everytime Always Learn

Firewall Concepts

Exclusive	Inclusive
firewall allows all traffic through except for the traffic matching the rule set.	Firewall only allows traffic matching the rules through and blocks everything else.

MikroTik RouterOS has very powerful firewall implementation with features including:

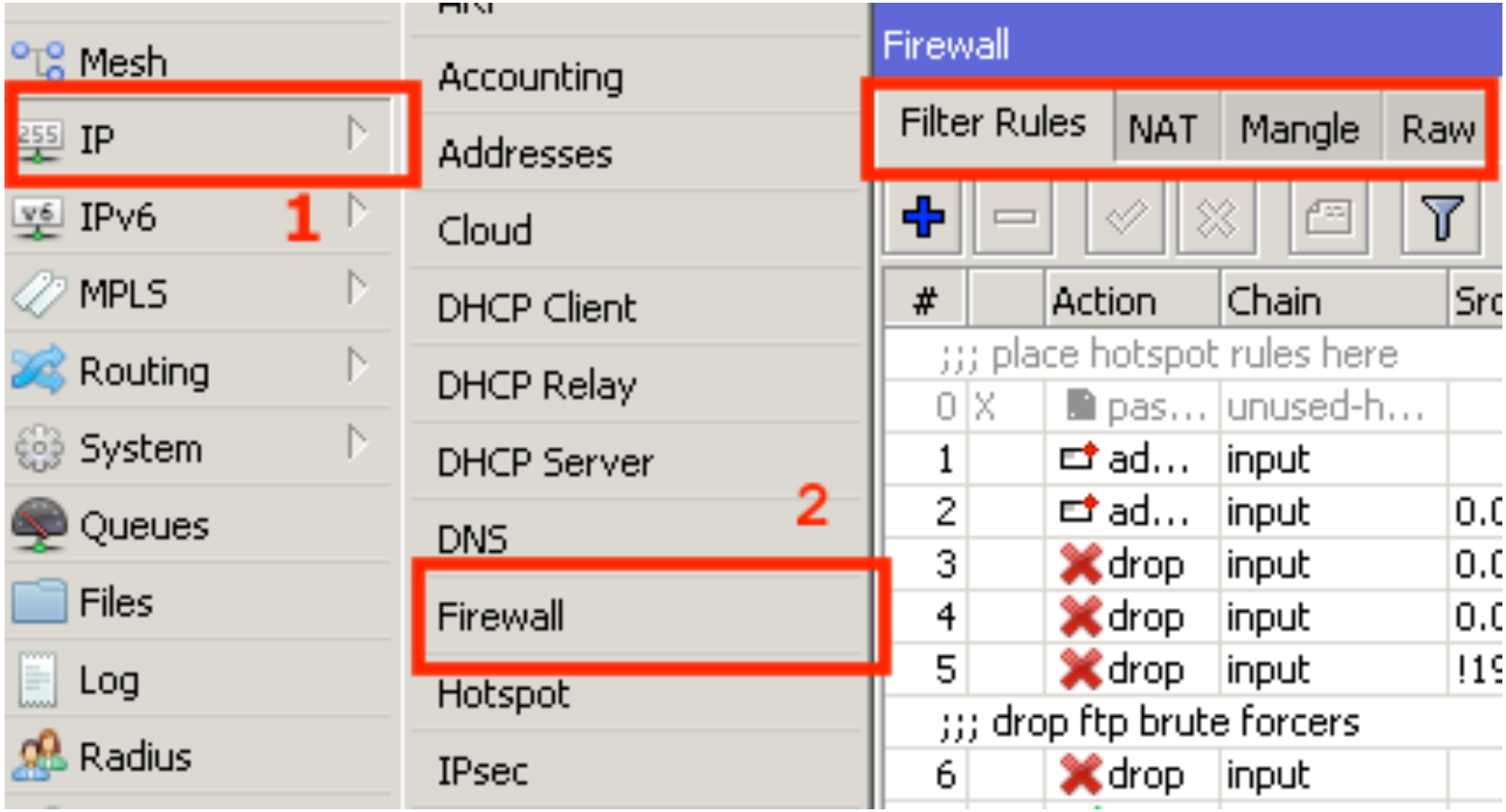
- stateful packet inspection
- Layer-7 protocol detection
- peer-to-peer protocols filtering

MikroTik RouterOS firewall traffic classification by:

- source MAC address
- IP addresses (network or list) and address types (broadcast, local, multicast, unicast)
- port or port range
- IP protocols
- protocol options (ICMP type and code fields, TCP flags, IP options and MSS)
- interface the packet arrived from or left through
- internal flow and connection marks
- DSCP byte
- packet content
- rate at which packets arrive and sequence numbers
- packet size
- packet arrival time

and much more!

MikroTik RouterOS firewall



Chain Of Tables

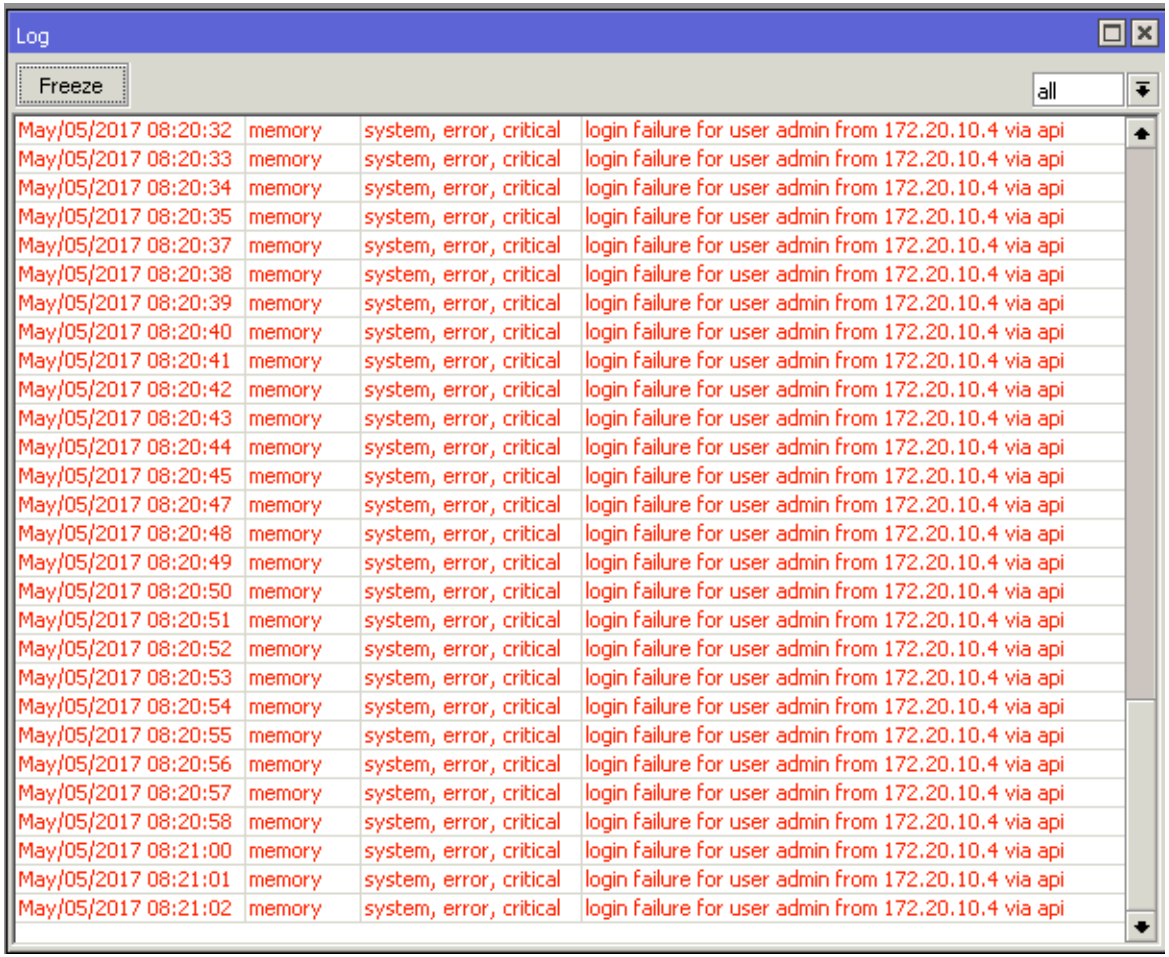
Table / Chain	Filter	Mangle	NAT	RAW
Input	✔	✔		
Output	✔	✔		✔
Forward	✔	✔		
Prerouting		✔	✔	✔
Postrouting		✔	✔	

Actions Of Tables

Chain \ Table	Filter	NAT	RAW
Accept	✔	✔	✔
No track	✔		✔
Drop	✔		✔
Reject	✔		
Tarpit		✔	
Masquerade		✔	
Redirect		✔	
Src-Nat		✔	
Dst-Nat		✔	

Brute-force Attack

What the solution to prevent our router from this?



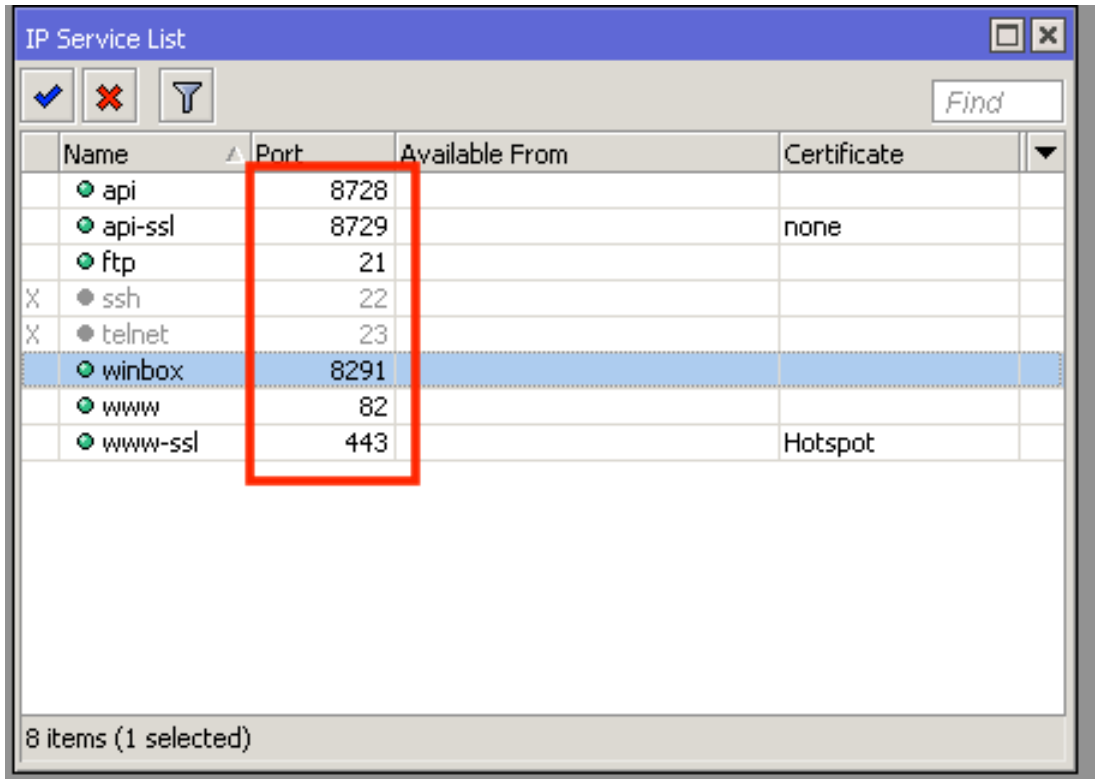
Brute-force Attack

WIKIPEDIA

an attacker trying many passwords or passphrases with the hope of eventually guessing correctly. The attacker systematically checks all possible passwords and passphrases until the correct one is found.

SOLUTION

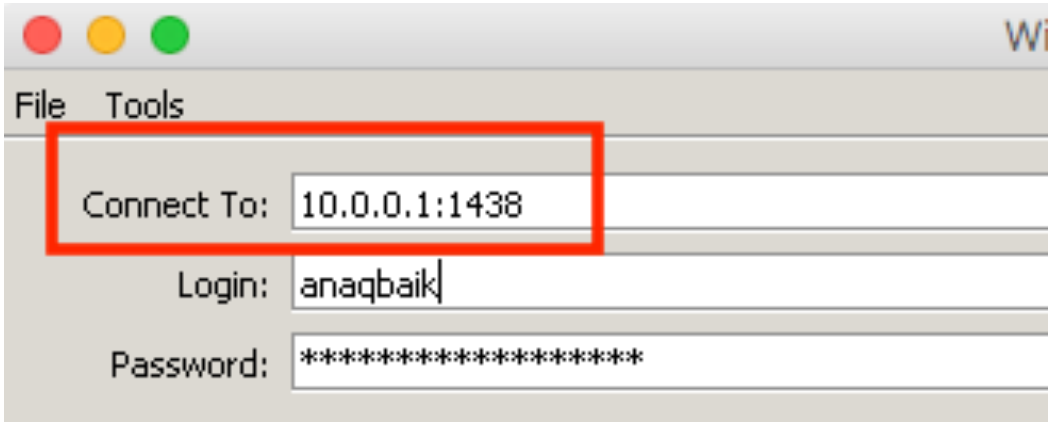
- Please change the default port from IP -> Services Especially port Telnet (default 23), SSH (default 22), FTP (default 21) Winbox 8291/TCP and API 8728/TCP or disable if you don't use that services.



SOLUTION (2)

- How to login with winbox after we change the port? We can use this format in Winbox Login

- Connect to : **IP_address:port**



SOLUTION (3)

Please set Firewall in your router like this :

```
ip firewall filter
add chain=input protocol=tcp dst-port=21,22,23,8291,8728 src-address-list=bruteforce_blacklist action=drop
\ comment="drop brute forcers" disabled=no

add chain=input protocol=tcp dst-port=21,22,23,8291,8728 connection-state=new \
src-address-list=bruteforce_stage3 action=add-src-to-address-list address-list=bruteforce_blacklist \
address-list-timeout=10d comment="" disabled=no

add chain=input protocol=tcp dst-port=21,22,23,8291,8728 connection-state=new \
src-address-list=bruteforce_stage2 action=add-src-to-address-list address-list=bruteforce_stage3 \
address-list-timeout=1m comment="" disabled=no

add chain=input protocol=tcp dst-port=21,22,23,8291,8728 connection-state=new src-address-
list=bruteforce_stage1 \
action=add-src-to-address-list address-list=bruteforce_stage2 address-list-timeout=1m comment=""
disabled=no

add chain=input protocol=tcp dst-port=21,22,23,8291,8728 connection-state=new action=add-src-to-
address-list \
address-list=bruteforce_stage1 address-list-timeout=1m comment="" disabled=no
```

SOLUTION (4)

This configuration allows only 10 FTP login incorrect answers per minute

/ip firewall filter

add chain=input protocol=tcp dst-port=21 src-address-list=ftp_blacklist action=drop comment="drop ftp brute forcers"

add chain=output action=accept protocol=tcp content="530 Login incorrect" dst-limit=1/1m,9,dst-address/1m

add chain=output action=add-dst-to-address-list protocol=tcp content="530 Login incorrect" address-list=ftp_blacklist address-list-timeout=3h

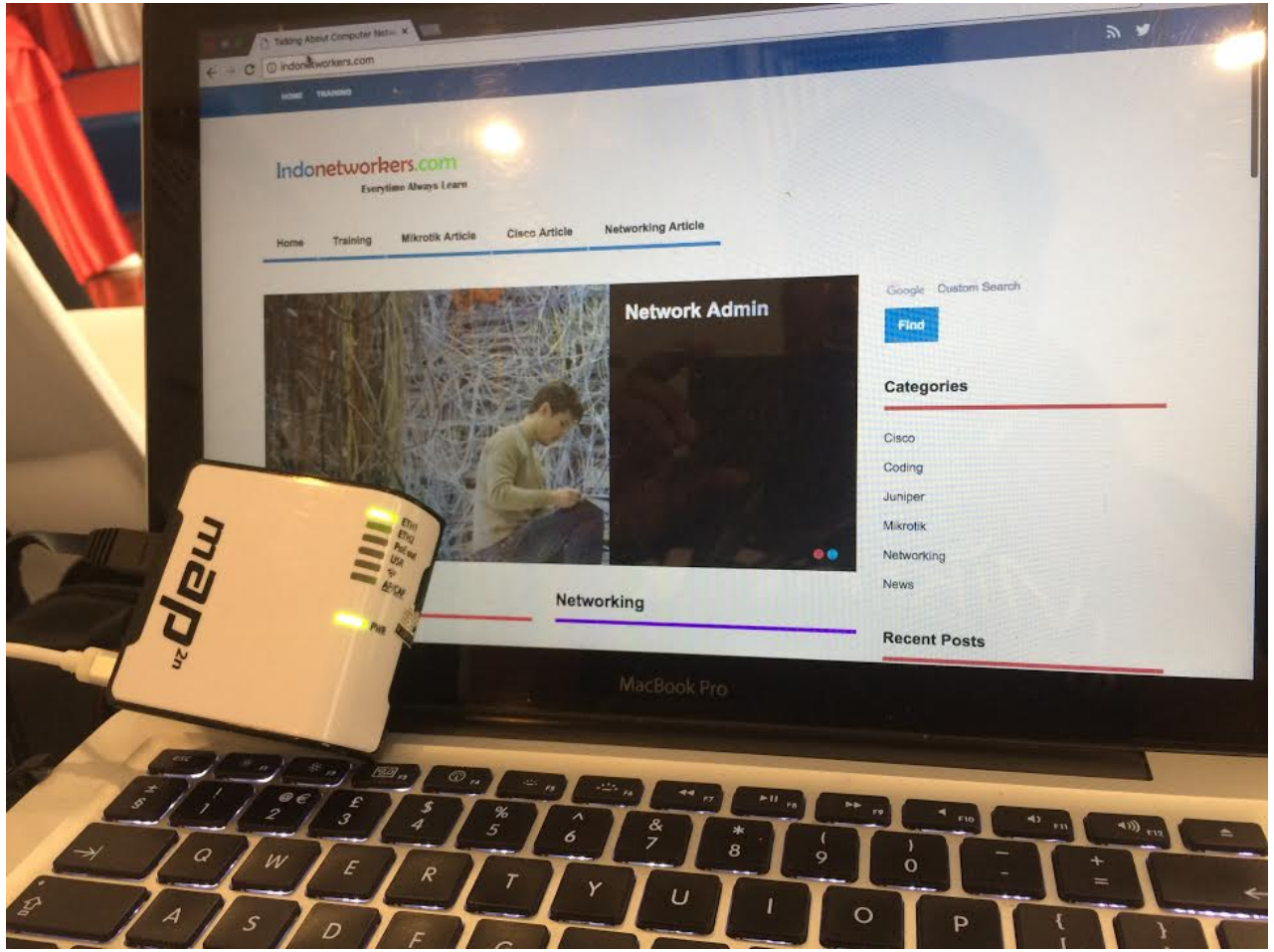
Basic Hardening MikroTIK RouterOS

1. Disable www in ip -> services if you never use webfig and other services that you never used.
2. Change port for winbox and to login please use "ipaddress:port"
3. Remove user admin and make a new user for full privilege access user
4. Disable discovery on the interface to which your network users are connected : /ip > neighbor > discovery or block the default MT discovery protocol port (5678) on your router - if this is convenient and if you haven't changed this default

CONCLUSION

MikroTik RouterOS has very powerful firewall implementation but the network administrator must make configuration alone because **MikroTik RouterOS** just give the facilities of that so never stop learn ☺

DEMO



Any Question?

email : teddy.yuliswar@gmail.com
Whatsapp : +62853 1477 1774

ขอบใจ