



Michael Takeuchi, MTC(ALL)E, CEH

MikroTik Security : The Forgotten Things

21 January 2019, Phnom Penh
MikroTik User Meeting Cambodia



- MikroTik Certified Engineer (ALL)
(MTCNA, MTCRE, MTCINE, MTCWE, MTCUME, MTCTCE, MTCIPv6E)
 - MikroTik Certified Consultant (World Wide)
 - Trainer at Trainocate Indonesia
 - Network Engineer at NetData
 - Solution Architect at HIGO
-  <https://www.linkedin.com/in/michael-takeuchi>
-  <https://www.facebook.com/mict404>
-  michael@takeuchi.id

Hello, I am Michael Takeuchi

From Jakarta, Indonesia

What is Security? (in Computer)

- **Computer security, cybersecurity or information technology security (IT security)** is the protection of computer systems from theft or damage to their hardware, software or electronic data, as well as from disruption or misdirection of the services they provide.

- Wikipedia,
https://en.wikipedia.org/wiki/Computer_security

What is Security? (in Computer Network)

- **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. Network security involves the authorization of access to data in a network, which is controlled by the network administrator

- Wikipedia,
https://en.wikipedia.org/wiki/Network_security

Continuing

- After we talk about what security is, now I will explain some forgotten things about your own router security that skipped by common junior network engineer
- We will focused on the router because that so **many vulnerabilities** appears because we forgot something with our router security

Router Login – Users

The image shows a network management interface with two windows. The top window, titled 'User List', has tabs for 'Users', 'Groups', 'SSH Keys', 'SSH Private Keys', and 'Active Users'. Below the tabs is a toolbar with icons for adding (+), removing (-), enabling (checkmark), disabling (X), saving (floppy), and filtering (funnel), along with an 'AAA' button and a 'Find' search box. A table below the toolbar lists users with columns for Name, Group, Allowed Address, and Last Logged In. The table contains two entries: '::: system default user' and 'admin' (with a red key icon) in the 'full' group. The bottom window, titled 'New User', is a form for creating a new user. It has fields for Name (filled with 'user1'), Group (filled with 'read'), Allowed Address, Last Logged In, Password, and Confirm Password. On the right side of the form are buttons for OK, Cancel, Apply, Disable, Comment, Copy, and Remove. At the bottom left of the form, the text 'enabled' is displayed.

Name	Group	Allowed Address	Last Logged In
::: system default user			
admin	full		

Name:

Group:

Allowed Address:

Last Logged In:

Password:

Confirm Password:

enabled

Router Login – Groups

User List

Users Groups SSH Keys SSH Private Keys Active Users

+ - [icon] [icon]

Name	Policies	Skin
full	local telnet ssh ftp reboot read write policy test winbox password web sniff sensitive api romon	default
read	local telnet ssh reboot read test winbox password web sniff sensitive api romon	default
write	local telnet ssh reboot read write test winbox password web sniff sensitive api romon	default

3 items

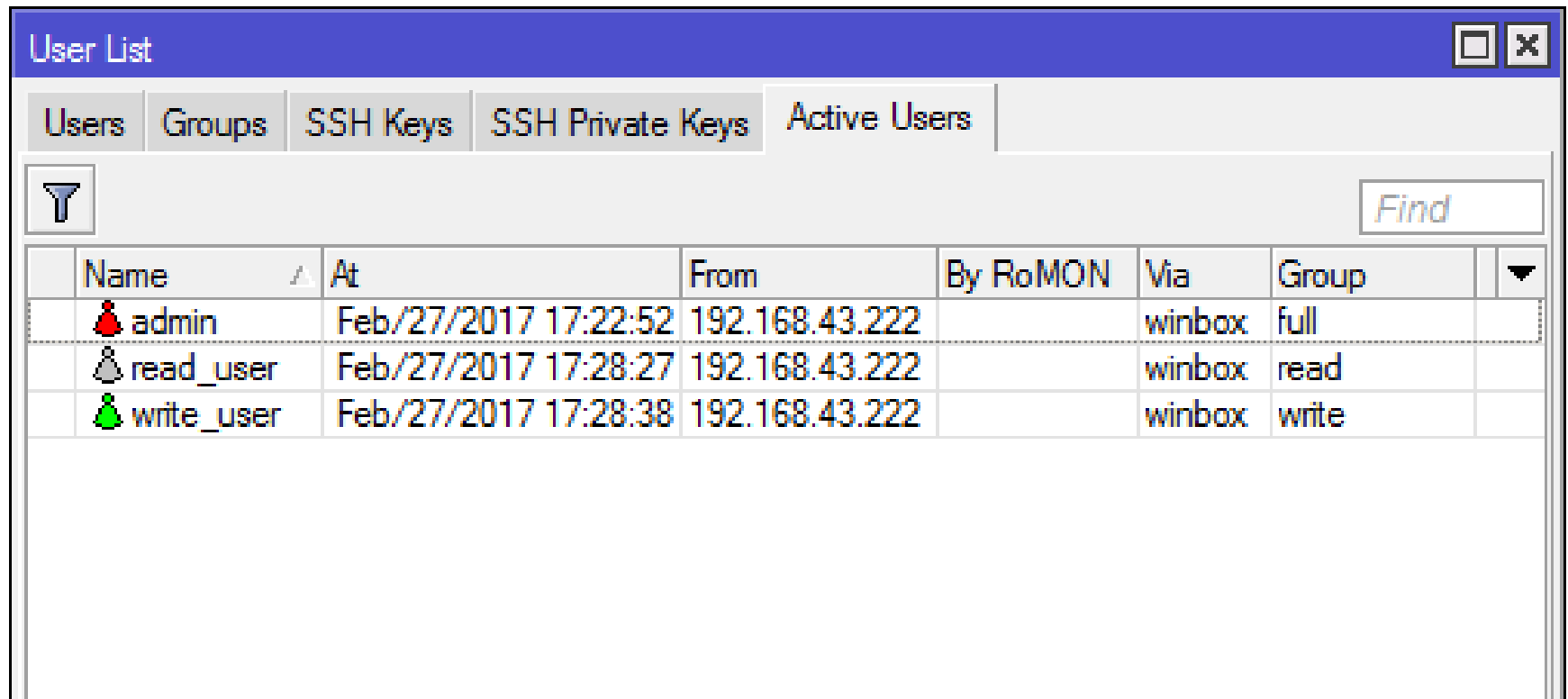
Router Login – Policies




- local - policy that grants rights to log in locally via console
- telnet - policy that grants rights to log in remotely via telnet
- ssh - policy that grants rights to log in remotely via secure shell protocol
- web - policy that grants rights to log in remotely via WebBox
- winbox - policy that grants rights to log in remotely via WinBox
- password - policy that grants rights to change the password
- api - grants rights to access router via API.
- dude - grants rights to log in to dude server.
- ftp - policy that grants full rights to log in remotely via FTP and to transfer files from and to the router.

Router Login – Policies

- reboot - policy that allows rebooting the router
- read - policy that grants read access to the router's configuration. All console commands that do not alter router's configuration are allowed. write - policy that grants write access to the router's configuration, except for user management.
- policy - grants user management rights. Should be used together with write policy.
- test - policy that grants rights to run ping, traceroute, bandwidth-test, wireless scan, sniffer, snoop and other test commands
- sensitive - to see sensitive information in the router
- sniff - to use packet sniffer tool.
- romon - accessing romon

Router Login – Active Users



Name	At	From	By RoMON	Via	Group
 admin	Feb/27/2017 17:22:52	192.168.43.222		winbox	full
 read_user	Feb/27/2017 17:28:27	192.168.43.222		winbox	read
 write_user	Feb/27/2017 17:28:38	192.168.43.222		winbox	write

Enough?

Are we enough to have strong
username & password?

BIG NO

Forgotten #1

RouterOS Vulnerabilities in 2012 – 2015

CVE #	Description
CVE-2015-2350	Cross-site request forgery (CSRF) vulnerability in MikroTik RouterOS 5.0 and earlier allows remote attackers to hijack the authentication of administrators for requests that change the administrator password via a request in the status page to /cfg.
CVE-2012-6050	The winbox service in MikroTik RouterOS 5.15 and earlier allows remote attackers to cause a denial of service (CPU consumption), read the router version, and possibly have other impacts via a request to download the router's DLLs or plugins, as demonstrated by roteros.dll.

Credit: <https://www.cvedetails.com>

RouterOS Vulnerabilities in 2017

CVE #	Description
CVE-2017-8338	A vulnerability in MikroTik Version 6.38.5 could allow an unauthenticated remote attacker to exhaust all available CPU via a flood of UDP packets on port 500 (used for L2TP over IPsec), preventing the affected router from accepting new connections; all devices will be disconnected from the router and all logs removed automatically.
CVE-2017-7285	A vulnerability in the network stack of MikroTik Version 6.38.5 released 2017-03-09 could allow an unauthenticated remote attacker to exhaust all available CPU via a flood of TCP RST packets, preventing the affected router from accepting new TCP connections.
CVE-2017-6297	The L2TP Client in MikroTik RouterOS versions 6.83.3 and 6.37.4 does not enable IPsec encryption after a reboot, which allows man-in-the-middle attackers to view transmitted data unencrypted and gain access to networks on the L2TP server by monitoring the packets for the transmitted data and obtaining the L2TP secret.

Credit: <https://www.cvedetails.com>

RouterOS Vulnerabilities in 2018

CVE #	Description
CVE-2018-1156	MikroTik RouterOS before 6.42.7 and 6.40.9 is vulnerable to stack buffer overflow through the license upgrade interface. This vulnerability could theoretically allow a remote authenticated attacker execute arbitrary code on the system.
CVE-2018-1157	MikroTik RouterOS before 6.42.7 and 6.40.9 is vulnerable to a memory exhaustion vulnerability. An authenticated remote attacker can crash the HTTP server and in some circumstances reboot the system via a crafted HTTP POST request.
CVE-2018-1158	MikroTik RouterOS before 6.42.7 and 6.40.9 is vulnerable to a stack exhaustion vulnerability. An authenticated remote attacker can crash the HTTP server via recursive parsing of JSON.
CVE-2018-1159	MikroTik RouterOS before 6.42.7 and 6.40.9 is vulnerable to a memory corruption vulnerability. An authenticated remote attacker can crash the HTTP server by rapidly authenticating and disconnecting.

Credit: <https://www.cvedetails.com>

RouterOS Vulnerabilities in 2018

CVE #	Description
CVE-2018-7445	A buffer overflow was found in the MikroTik RouterOS SMB service when processing NetBIOS session request messages. Remote attackers with access to the service can exploit this vulnerability and gain code execution on the system. The overflow occurs before authentication takes place, so it is possible for an unauthenticated remote attacker to exploit it. All architectures and all devices running RouterOS before versions 6.41.3/6.42rc27 are vulnerable.
CVE-2018-14847	MikroTik RouterOS through 6.42 allows unauthenticated remote attackers to read arbitrary files and remote authenticated attackers to write arbitrary files due to a directory traversal vulnerability in the WinBox interface.

Credit: <https://www.cvedetails.com>

Good Things to Know

those vulnerabilities were possible only on the routers which didn't have default firewall configuration, or had improperly configured firewall

Forgotten #2

Good Things to Know

- MikroTik is growing rapidly and have bigger user year by year
- And because of that, many Hackers is interesting with MikroTik because so many infrastructure use MikroTik now
- And because of that, MikroTik vulnerabilities is also growing rapidly
- And because of that, DOESN'T MEAN MIKROTIK IS A BAD PRODUCT



“high winds blown on high hills”



Forgotten #3

So What?

- Upgrade to Patched Version
- Protect all services
- Layered Security

Forgotten #4

Upgrade to Patched Version

Package List

Name	Version	Build Time	Scheduled
advanced-tools	6.35	Apr/14/2016 12:55:07	
dhcp	6.35	Apr/14/2016 12:55:07	
dude	6.35	Apr/14/2016 12:55:07	
gps	6.35	Apr/14/2016 12:55:07	
hotspot	6.35	Apr/14/2016 12:55:07	
ipv6	6.35	Apr/14/2016 12:55:07	
kvm	6.35	Apr/14/2016 12:55:07	
lcd	6.35	Apr/14/2016 12:55:07	
mpls	6.35	Apr/14/2016 12:55:07	
multicast	6.35	Apr/14/2016 12:55:07	
ntp	6.35	Apr/14/2016 12:55:07	
ppp	6.35	Apr/14/2016 12:55:07	
routing	6.35	Apr/14/2016 12:55:07	
security	6.35	Apr/14/2016 12:55:07	
system	6.35	Apr/14/2016 12:55:07	
ups	6.35	Apr/14/2016 12:55:07	
user-manager	6.35	Apr/14/2016 12:55:07	
wireless-cm2	6.35	Apr/14/2016 12:55:07	
wireless-fp	6.35	Apr/14/2016 12:55:07	

Check For Updates

Channel:

Installed Version:

Latest Version:

What's new in 6.43.8 (2018-Dec-21 07:10):

MAJOR CHANGES IN v6.43.8:

!) telnet - do not allow to set "tracefile" parameter;

Changes in this release:

- *) bridge - fixed IPv6 link-local address generation when auto-mac=yes;
- *) capsman - fixed "group-key-update" parameter not using correct units;
- *) crs3xx - improved data transmission between 10G and 1G ports;
- *) console - properly remove system note after configuration reset;
- *) dhcpv4-server - fixed dynamic lease reuse after expiration;
- *) dhcpv6-server - properly handle DHCP requests that include prefix hint;
- *) ethernet - fixed VLAN1 forwarding on RB1100AHx4 and RB4011 devices;
- *) gps - added "coordinate-format" parameter;
- *) led - fixed default LED configuration for RBMetalG-52SHPacn;
- *) led - fixed PWR-LINE AP ethernet led polarity ("/system routerboard upgrade" required);
- *) lte - disallow setting LTE interface as passthrough target;
- *) lte - fixed DHCP IP acquire (introduced in v6.43.7);
- *) lte - fixed passthrough functionality when interface is removed;
- *) lte - increased reported "rsrq" precision;
- *) lte - reset USB when non-default slot is used;
- *) package - use bundled package by default if standalone packages are installed as well;

New version is available

Upgrade to Patched Version – Tips (RouterOS After 6.31)

```
[takeuchi@MikroTik] > {  
{... /system package update  
{... check-for-updates once  
{... :delay 3s;  
{... :if ( [get status] = "New version is available") do={ install }  
{... }  
  
        channel: current  
current-version: 6.35  
        status: finding out latest version...  
        channel: current  
current-version: 6.35  
latest-version: 6.43.8  
        status: Downloaded 6% (1.5MiB)  
-- [Q quit|D dump|C-z pause]
```

This script can applied for RouterOS After 6.31

Upgrade to Patched Version – Tips (RouterOS Until 6.31)

```
[takeuchi@MikroTik] > {  
{... /system package update  
{... check-for-updates  
{... :delay 3s;  
{... :if ( [get current-version] != [get latest-version]) do={ upgrade }  
{... }
```

```
[takeuchi@MikroTik] /system package update> █
```

This script can applied for RouterOS Until 6.31

Upgrade to Patched Version – Tips (Deploying)

You can deploy this script with:

- Ansible SSH (<https://github.com/mict404/ansible-mikrotik-auto-upgrade>)
- Python Paramiko
- MikroTik Scheduler
- Etc. (any other automation tools)
- ~~Manual~~ 😊

Protect All Services

To protect all services, you need to:

1. Enable the service you **only** need
2. Whitelisting
3. Securing

Protect All Services (Router Access & Discovery)

```
[takeuchi@MikroTik] > ip neighbor discovery-settings print
```

```
discover-interface-list: none
```

```
[takeuchi@MikroTik] > ip service set [find name!=winbox] disabled=yes
```

```
[takeuchi@MikroTik] > ip service set winbox port=9999
```

```
[takeuchi@MikroTik] > ip service print
```

Flags: X - disabled, I - invalid

#	NAME	PORT	ADDRESS
0	XI telnet	23	
1	XI ftp	21	
2	XI www	80	
3	XI ssh	22	
4	XI www-ssl	443	
5	XI api	8728	
6	winbox	9999	
7	XI api-ssl	8729	

```
[takeuchi@MikroTik] > tool mac-server print
```

```
allowed-interface-list: none
```

```
[takeuchi@MikroTik] > tool mac-server mac-winbox print
```

```
allowed-interface-list: none
```

```
[takeuchi@MikroTik] > tool mac-server ping print
```

```
enabled: no
```

```
[takeuchi@MikroTik] > █
```

- Neighbor Discovery
- Services
- MAC-Server
(Extra Security for Layer 2 Networks)

Protect All Services (Router Feature)

```
[takeuchi@MikroTik] > ip dns print
    servers: 1.1.1.1
    dynamic-servers:
    allow-remote-requests: no
    max-udp-packet-size: 4096
    query-server-timeout: 2s
    query-total-timeout: 10s
    max-concurrent-queries: 100
    max-concurrent-tcp-sessions: 20
    cache-size: 2048KiB
    cache-max-ttl: 1w
    cache-used: 17KiB
[takeuchi@MikroTik] > ip upnp print
    enabled: no
    allow-disable-external-interface: no
    show-dummy-rule: yes
[takeuchi@MikroTik] > ip socks print
    enabled: no
    port: 1080
    connection-idle-timeout: 2m
    max-connections: 200
[takeuchi@MikroTik] > tool bandwidth-server print
    enabled: no
    authenticate: yes
    allocate-udp-ports-from: 2000
    max-sessions: 100
[takeuchi@MikroTik] > █
```

- DNS
- UPNP
- SOCKS
- Bandwidth Test Server

Protect All Services (Router Feature)

```
[takeuchi@MikroTik] > ip proxy print
```

```
    enabled: no
```

```
    src-address: ::
```

```
        port: 8080
```

```
    anonymous: no
```

```
    parent-proxy: ::
```

```
    parent-proxy-port: 0
```

```
    cache-administrator: webmaster
```

```
        max-cache-size: unlimited
```

```
    max-cache-object-size: 2048KiB
```

```
        cache-on-disk: no
```

```
    max-client-connections: 600
```

```
    max-server-connections: 600
```

```
        max-fresh-time: 3d
```

```
    serialize-connections: no
```

```
        always-from-cache: no
```

```
        cache-hit-dscp: 4
```

```
        cache-path: web-proxy
```

```
[takeuchi@MikroTik] > █
```

○ Proxy

Protect All Services (Whitelisting)

IP Service List

✓ ✗ ⏏

	Name	Port	Available From	Certificate
X	api	8728		
X	api-ssl	8729		
X	ftp	21		
X	ssh	22		
X	telnet	23		
	winbox	17845	192.168.1.0/26	
X	www	80		
X	www-ssl	443		

IP Service <winbox>

Name: winbox

Port: 17845

Available From: 192.168.1.0/26

OK

Cancel

Apply

Disable

enabled

Protect All Services (Securing)

- This is an example how we can protect DNS and Proxy services from WAN

```
/ip firewall raw
```

```
add action=drop chain=prerouting dst-address-  
type=local dst-port=53 in-interface=[WAN]  
protocol=udp
```

```
add action=drop chain=prerouting dst-address-  
type=local dst-port=53 in-interface=[WAN]  
protocol=tcp
```

```
add action=drop chain=prerouting dst-address-  
type=local dst-port=8080 in-interface=[WAN]  
protocol=tcp
```

Layered Security (Port Knocking)

- This is an example how we can protect our Winbox Access with Port Knocking that need to knock to port **TCP/1234** first

```
/ip firewall raw
```

```
add action=add-src-to-address-list address-  
list=allow-winbox address-list-timeout=30m  
chain=prerouting comment="Port Knocking" dst-  
port=1234 protocol=tcp dst-address-type=local
```

```
add action=accept chain=prerouting  
comment="Allow Winbox" src-address-list=allow-  
winbox dst-port=[Winbox Port] protocol=tcp  
dst-address-type=local
```

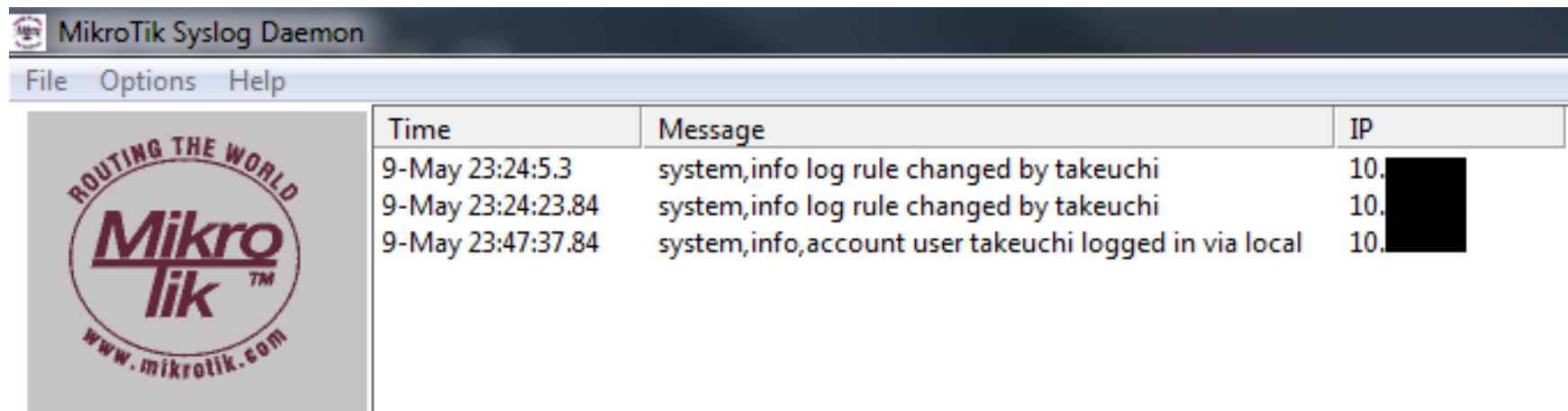
```
add action=drop chain=prerouting dst-address-  
type=local dst-port=[Winbox Port] protocol=tcp
```

Layered Security (Logging)

- Log with note everything router do, mostly hacker with clear log after they do something with our router, so I will recommend to use **syslog server** to save your log

```
/system logging action set [find name=remote]  
remote=[syslog_server]
```

```
/system logging add topics=info action=remote
```



Time	Message	IP
9-May 23:24:5.3	system,info log rule changed by takeuchi	10. [REDACTED]
9-May 23:24:23.84	system,info log rule changed by takeuchi	10. [REDACTED]
9-May 23:47:37.84	system,info,account user takeuchi logged in via local	10. [REDACTED]

Layered Security (Physical – LCD)

- Don't forget that somebody can do something to our router with LCD Screen only

The image shows a screenshot of a web-based configuration window titled "LCD". The window has a blue header bar with the title "LCD" and standard window control buttons (minimize, maximize, close). The main content area is light gray and contains several configuration options:

- Enabled (highlighted with a yellow dashed border)
- Touchscreen
- Backlight Timeout: 00:30:00 (with an up arrow icon)
- Read Only Mode
- Default Screen: main menu (with a down arrow icon)
- Time Interval: min (with a down arrow icon)
- Color Scheme: dark light
- Flip Screen

On the right side of the window, there is a vertical stack of buttons: OK, Cancel, Apply, Recalibrate, Backlight, Screens, Interfaces, and Pin.

Layered Security (Physical – Bootloader)

- Protected bootloader

https://wiki.mikrotik.com/wiki/Manual:RouterBOARD_settings#Protected_bootloader

- **EXTREMELY DANGEROUS**, will disabled reset button & netinstall. If you forget the RouterOS password, the only option is to perform a complete **reformat** of both NAND and RAM with the following method, but you have to know the reset button hold time in seconds.

Layered Security (Physical – Power)

- Use 2 Different Source Power to Reach High Availability



Layered Security (Physical – Interfaces)

	Name	Type
R	ether1_Internet-IN	Ethernet
R	vlan103	VLAN
R	vlan105	VLAN
X	ether2	Ethernet
X	ether3	Ethernet
X	ether4	Ethernet
X	ether5	Ethernet
R	ether6_toSwitch	Ethernet
R	vlan620	VLAN
X	ether7	Ethernet
X	ether8	Ethernet
X	ether9	Ethernet
X	ether10	Ethernet
X	ether11	Ethernet
X	ether12	Ethernet
	ether13_Management	Ethernet

- Disable all unused interfaces to minimize unauthorized access to router

Layered Security (Backup)

- Backup is important when your router got hacked or you just forgot your password
- Make sure your backup file is save and can be accessible anytime
- **DON'T EVER TO SAVE YOUR BACKUP FILE IN ROUTER ONLY**

Forgotten #5

Layered Security (Backup Types)

1. Full Backup (`/system backup`)

- Saved in Binary (Not Editable)
- We Can Set a Password
- Full Backup (Including User Login)

2. Partial Backup (`/export`)

- Saved in Plain Text (Editable)
- Partial Backup (e.g. “/ip firewall” only)
- Not Including User Login

```
[takeuchi@MikroTik] > export file=Backup21Jan2019
[takeuchi@MikroTik] > system backup save name=Backup21Jan2019 dont-encrypt=yes
Saving system configuration
Configuration backup saved
[takeuchi@MikroTik] > █
```

Conclusion

Secure \neq Easy

Forgotten #6

Feel so hard to securing your infrastructure?
Let me help you!

michael@takeuchi.id

<https://www.facebook.com/mict404>

<https://www.linkedin.com/in/michael-takeuchi/>

Question & Answer



Slide is available in my GitHub repository

<https://github.com/mict404/slide/>

*Thank
you*

