

# *Mikro***Tik** Hotspot Audit & Hardening

Presented by Michael Takeuchi

MikroTik User Meeting, 27 October 2017 – Yogyakarta (Indonesia)



# Little Things About Me



- MTCNA, MTCRE, MTCINE, MTCUME, MTCWE, MTCTCE, MTCIPv6E
- MikroTik Certified Consultant on mikrotik.com
- January 2017 – June 2017 Work as Remote Network Engineer at Middle East
- July 2017 – Now Work as Network Analyst at PT. Maxindo Mitra Solusi

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

# Objective #NoOffense #Censored

[Redacted] 4/29, 1:12am  
eh eh, ajarin jebol mikrotik dong .\_.

[Redacted] bang itu mikrotik pass nya apa?  
**Michael Takeuchi**  
Tergantung di set apa sama adminnya  
[Redacted]  
Cara dapetin nya gmn?  
**Michael Takeuchi**  
Tanya ke admin nya

[Redacted] 9/27, 10:16pm  
[Redacted] Michael bagiannya sharing exploit mikrotik xixixi

[Redacted] kell  
mikrotik bisa di bypass ga 😞

[Redacted] 4 jam · 🌐

[Redacted] tau cara bypass mikrotik ga ?  
up

salam kenal ada yg tau caranya hack admin mikrotik bang atau winbox lagi butuh nih. soalnya wifi dirumah kemahalan 5000 3 jam ... kan enak kalau bisa buat sendiri

# What We Need To Do?

1. Auditing your network
2. Hardening your network
3. Penetration Testing your network
4. Repeat

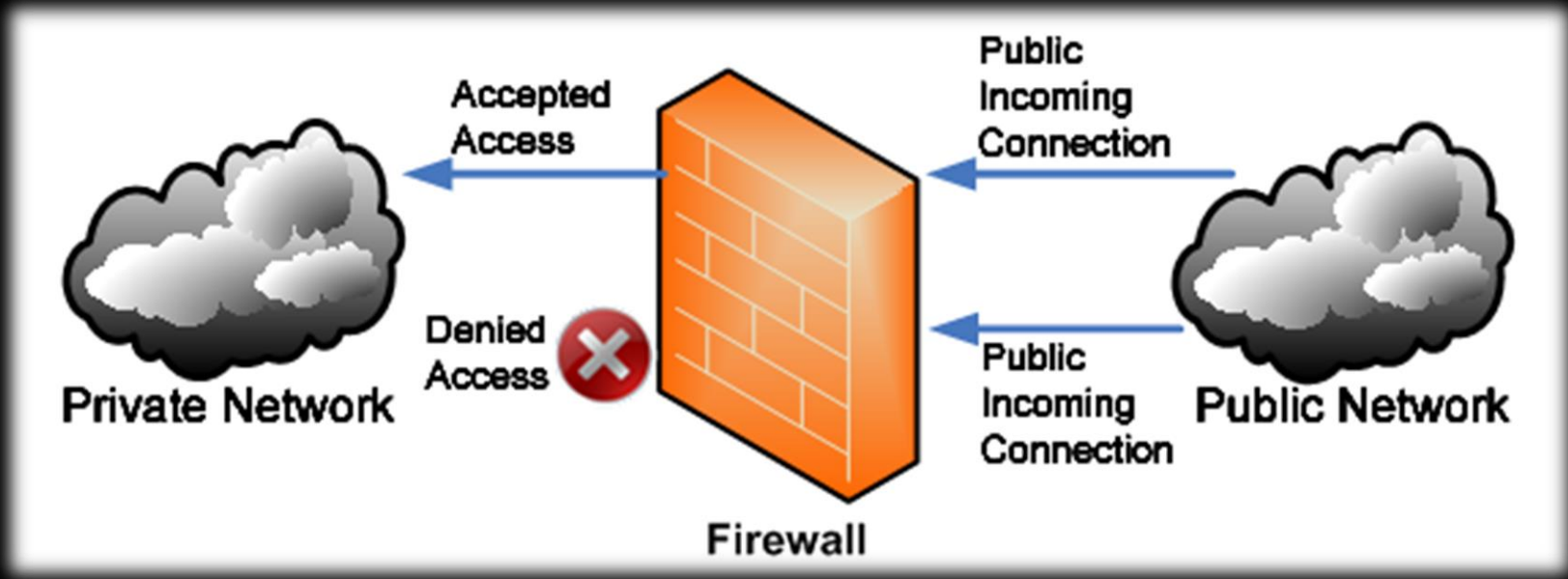
- Before we do that things, we need to know about Firewall & Network Security and how your system works

# What is Firewall?

- In computing, a firewall is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted, secure internal network and another outside network, such as the Internet, that is assumed not to be secure or trusted.

- Wikipedia, [https://en.wikipedia.org/wiki/Firewall\\_\(computing\)](https://en.wikipedia.org/wiki/Firewall_(computing))

# What is Firewall?



# What is 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. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority.
- Wikipedia, [https://en.wikipedia.org/wiki/Network\\_security](https://en.wikipedia.org/wiki/Network_security)

Before we go to hotspot, we need to audit our router  
Oopss sorry, I mean before doing a setup



# MikroTik Router Login – User

The screenshot shows the MikroTik WinBox interface. At the top, the 'User List' window is open, displaying a table of users. Below it, the 'New User' dialog is open, showing fields for Name, Group, Allowed Address, Last Logged In, Password, and Confirm Password. The 'Name' field contains 'user1' and the 'Group' dropdown is set to 'read'. The 'enabled' checkbox is checked.

**User List**

Users | Groups | SSH Keys | SSH Private Keys | Active Users

+ - ✓ ✗ 📁 🔍 AAA Find

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

**New User**

Name: user1

Group: read

Allowed Address:

Last Logged In:

Password:

Confirm Password:

enabled




OK  
Cancel  
Apply  
Disable  
Comment  
Copy  
Remove

# MikroTik 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

# MikroTik Router Login – Active Users

User List □ ✕

Users Groups SSH Keys SSH Private Keys 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	

# MikroTik 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.

# MikroTik Router Config Policies

- ftp - policy that grants full rights to log in remotely via FTP and to transfer files from and to the router.
- 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, snooper and other test commands
- sensitive - to see sensitive information in the router
- sniff - to use packet sniffer tool.
- romon - accessing romon

# MikroTik Access Login Service

IP Service List				
	Name	Port	Available From	Certificate
<input checked="" type="checkbox"/>	api	8728		
<input checked="" type="checkbox"/>	api-ssl	8729		none
<input checked="" type="checkbox"/>	ftp	21		
<input checked="" type="checkbox"/>	ssh	22		
<input checked="" type="checkbox"/>	telnet	23		
<input checked="" type="checkbox"/>	winbox	8291		
<input checked="" type="checkbox"/>	www	80		
<input checked="" type="checkbox"/>	www-ssl	443		none

8 items

# Port Service Change & Whitelist

- Activate Only What You Need & Don't Use Default Port
- Port: The port particular service listens on
- Available From: List of IPv4/IPv6 prefixes from which the service is accessible.

The screenshot shows the 'IP Service List' configuration window. It contains a table with columns for Name, Port, Available From, and Certificate. The 'telnet' service is selected, and a dialog box is open to edit its configuration. The dialog shows the Name as 'telnet', the Port as '2424', and the Available From as '10.10.10.0/28'. The service is currently disabled.

	Name	Port	Available From	Certificate
X	api	8728		
X	api-ssl	8729		none
X	ftp	21		
	ssh	4444	172.16.30.60	
X	telnet	2300	10.10.10.0/26	
	winbox	8291		
X	www	80		
X	www-ssl	443		none

IP Service <telnet>

Name: telnet

Port: 2424

Available From: 10.10.10.0/28

disabled

8 items (1 selected)

# Login Comparison

Service	Encryption	Protocol	Port	OSI Layer
WinBox	YES	TCP	8291	Layer 3
WebFig (HTTP)	NO	TCP	80	Layer 3
WebFig (HTTPS)	YES	TCP	443	Layer 3
Telnet	NO	TCP	23	Layer 3
MAC-Telnet	YES	UDP	20561	Layer 2
SSH	YES	TCP	22	Layer 3
Serial Console	-	-	-	Layer 1

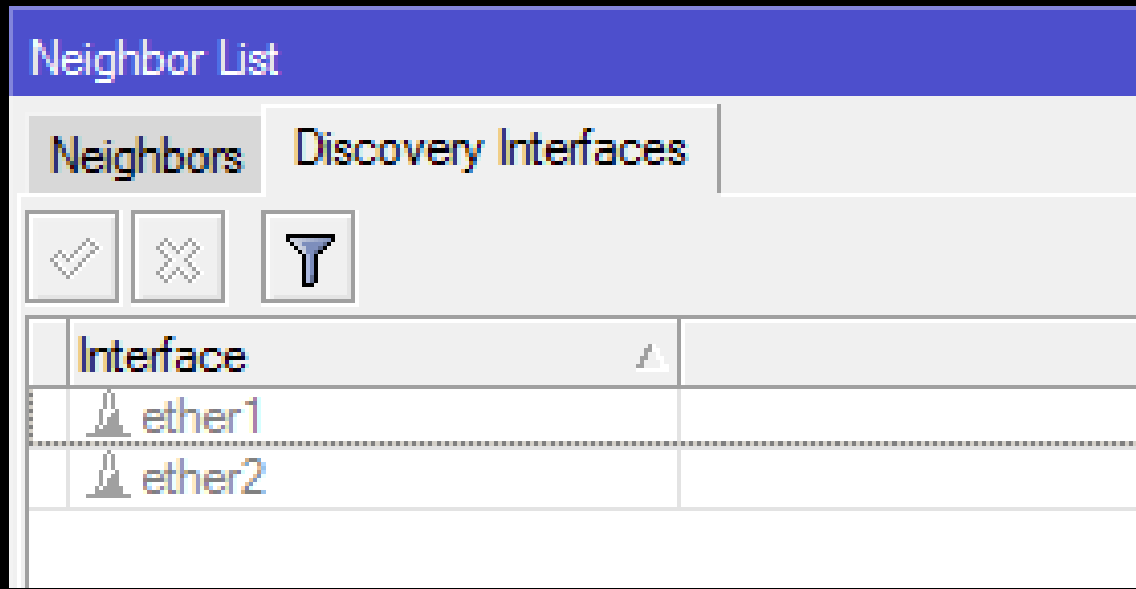
\*From Wireshark





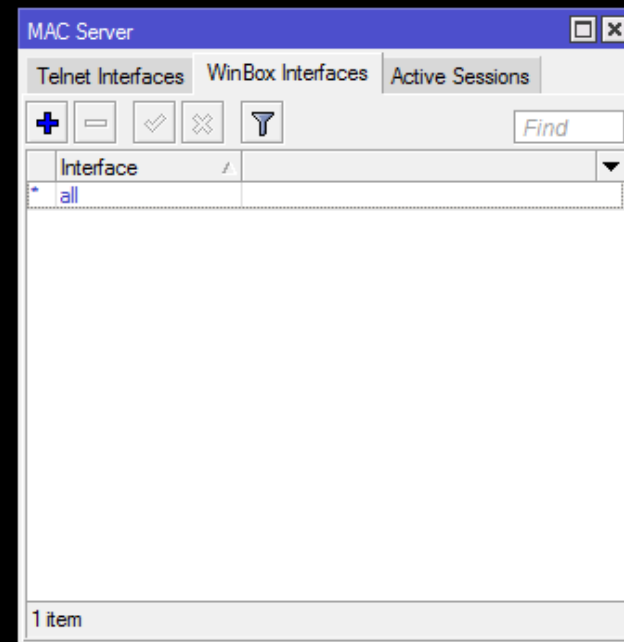
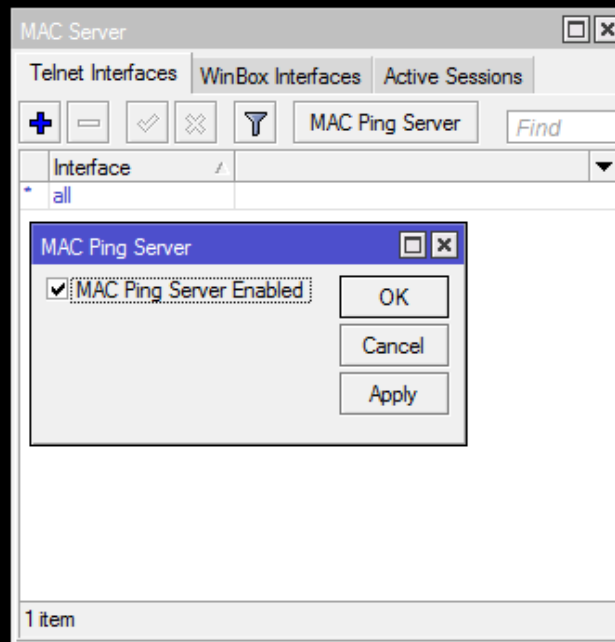
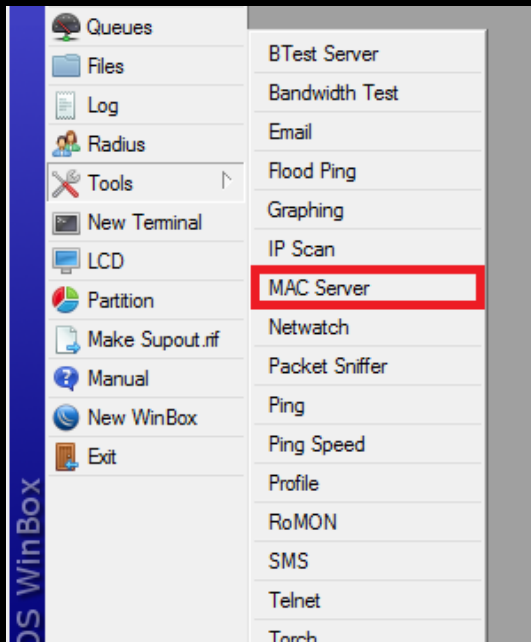
# MikroTik Neighbor Discovery

- Turn off neighbor discovery or your router will be discovered by your neighbor and on WinBox, it's good for being undetected 😊



# MikroTik MAC-Server

- Turn off MAC-Server for Prevent Layer 2 Communication



# Turn off Router Public Services

- Besides SSH, Telnet, WinBox, API, FTP, WWW. Router also have commonly public services like:
  - **Recursive DNS Server**
    - You must disable this services before you got DNS Amplification attack, more about DNS Amplification is available from MUM Indonesia 2014: Filtering DNS Amplification  
<https://www.youtube.com/watch?v=wd0LQcJ1j-c&t=80s>
  - **Web Proxy**
    - You must disable this services before someone use this services to use your internet connection, for the example i have IIX connection 10Gbps only and You have 1Gbps to International and 10Gbps to IIX, I can do web proxy to you (without authentication) and i can enjoy your High Speed International Connection 😊
  - **Bandwidth Test Server**
    - Bandwidth Test Server is a feature to allow anyone to test how much their throughput and generate real traffic to the server

# Turn off Router Vulnerable Public Services

DNS Settings

Servers: 192.168.88.1

Dynamic Servers:

Allow Remote Requests

Max UDP Packet Size: 4096

Query Server Timeout: 2.000 s

Query Total Timeout: 10.000 s

Max. Concurrent Queries: 100

Max. Concurrent TCP Sessions: 20

Cache Size: 2048 KB

Cache Max TTL: 7d 00:00:00

Cache Used: 70 KB

OK  
Cancel  
Apply  
Static  
Cache

BTest Server Settings

Enabled

Authenticate

Allocate UDP Ports From: 2000

Max Sessions: 100

OK  
Cancel  
Apply  
Sessions

Web Proxy Settings

General | Status | Lookups | Inserts | Refreshes

Enabled

Src. Address: 0.0.0.0

Port: 8080

Anonymous

Parent Proxy:

Parent Proxy Port:

Cache Administrator: webmaster

Max. Cache Size: none KB

Max Cache Object Size: 2048 KB

Cache On Disk

Max. Client Connections: 600

Max. Server Connections: 600

Max Fresh Time: 3d 00:00:00

Serialize Connections

Always From Cache

Cache Hit DSCP (TOS): 4

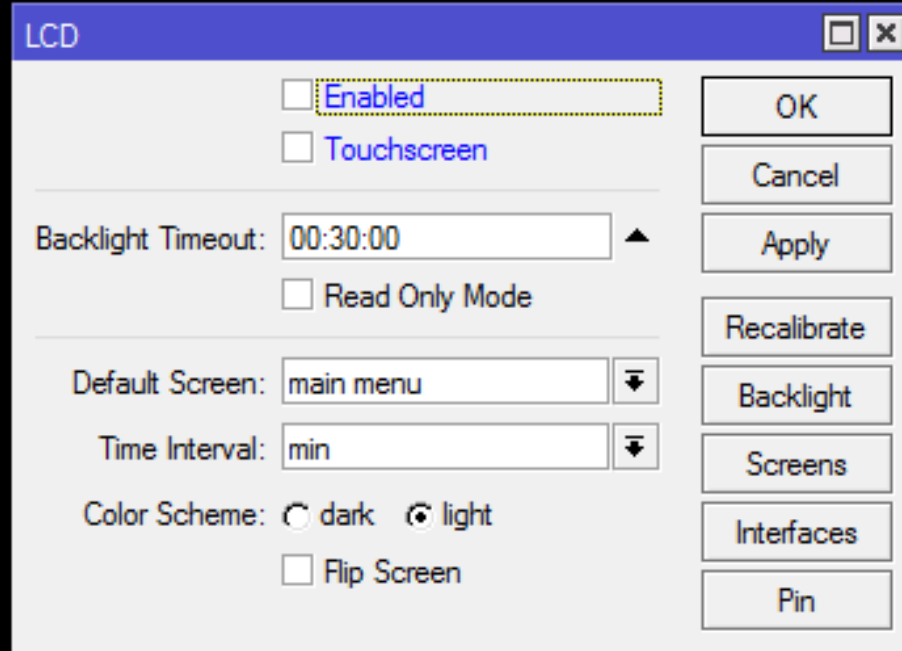
Cache Path: web-proxy

OK  
Cancel  
Apply  
Clear Cache  
Reset HTML  
Access  
Cache  
Direct  
Connections  
Cache Contents

stopped

# Protect The Physical

- Turn off the LCD



# Protect The Physical

- Protected bootloader

[https://wiki.mikrotik.com/wiki/Manual:RouterBOARD\\_setting\\_s#Protected\\_bootloader](https://wiki.mikrotik.com/wiki/Manual:RouterBOARD_setting_s#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.

# Protect The Physical

- Power Redundancy



- Disable idle interface(s), reserve the one that you are planning to use when doing on-site maintenance



# Other Things To Do

1. Prevent Your Router from DDoS/DOS Attack
2. Prevent Your Router from Bruteforce Attack
3. Create Port Knocking
4. Create HoneyPot

[http://mum.mikrotik.com/presentations/US17/presentation\\_4304\\_1496050983.pdf](http://mum.mikrotik.com/presentations/US17/presentation_4304_1496050983.pdf)

(DDOS Attacks and MikroTik by Dennis Burgess)

[http://mum.mikrotik.com/presentations/ID16/presentation\\_3549\\_1484646663.pdf](http://mum.mikrotik.com/presentations/ID16/presentation_3549_1484646663.pdf)

(Prevention Bruteforce MikroTik by Fajar Amanullah Zaky)

[http://mum.mikrotik.com/presentations/ID16/presentation\\_3655\\_1476604698.pdf](http://mum.mikrotik.com/presentations/ID16/presentation_3655_1476604698.pdf)

(Fools your enemy with MikroTik by Didiet Kusumadihardja)

Are we done? I don't know 😊  
hackers always have an unexpected things  
But, let's continue to hotspot

# MikroTik Hotspot

The MikroTik HotSpot Gateway provides authentication for clients before access to public networks .

- HotSpot Gateway features:

1. different authentication methods of clients using local client database on the router, or remote RADIUS server
2. users accounting in local database on the router, or on remote RADIUS server
3. walled-garden system, access to some web pages without authorization
4. login page modification, where you can put information about the company
5. automatic and transparent change any IP address of a client to a valid address

<https://wiki.mikrotik.com/wiki/Manual:IP/Hotspot>

# How MikroTik Hotspot Works?

1. User try to open browser
2. User try to open website
3. If the ip or mac not listed in cookies and ip binding or walled-garden the user will be redirected to miktotik hotspot login page
4. User doing authentication
5. If match with database on local router or RADIUS
  - Then
    - Authenticated (Logged in)
  - Else
    - Prohibited

# MikroTik Hotspot Component

1. Firewall Filter
2. Firewall NAT
3. Firewall Mangle
4. DHCP Server + IP Pool
5. Proxy Server
6. DNS Server
7. Queue

# Next to MikroTik Hotspot Security

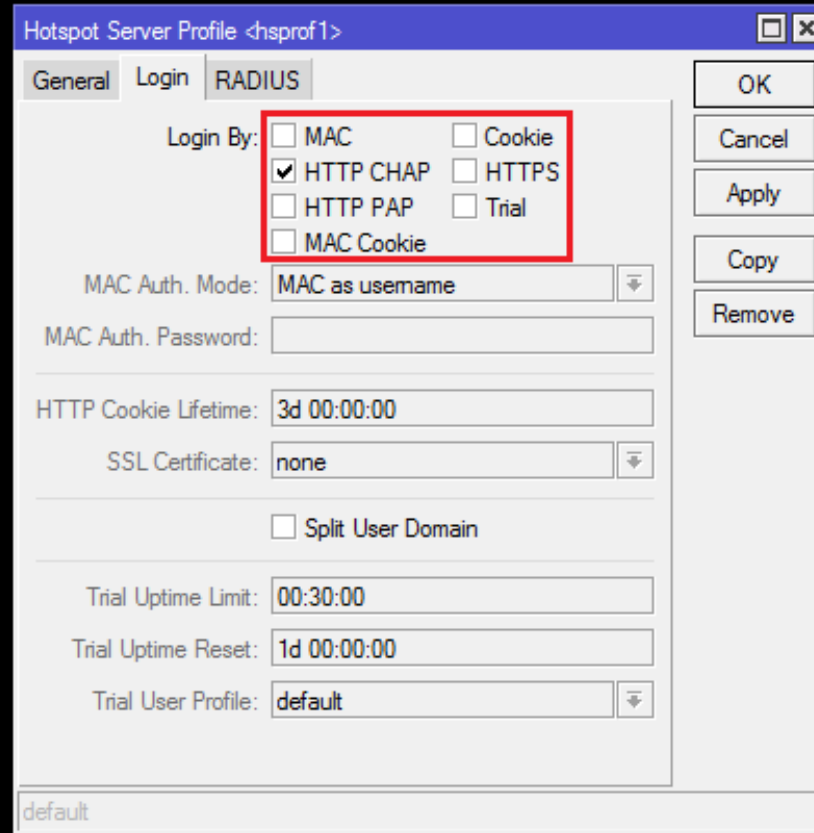
- Let's Talk About MikroTik HotSpot Login Security !
- What Do We Need To Know To Securing It?

If you know the enemy and know  
yourself you need not fear the  
results of a hundred battles

- *Sun Tzu*

# MikroTik Hotspot Authentication Method

- MAC Cookie
- HTTP CHAP
- HTTP PAP
- Cookie
- HTTPS
- MAC
- Trial



Hotspot Server Profile <hsprof1>

General Login **RADIUS**

Login By:  MAC  Cookie  
 HTTP CHAP  HTTPS  
 HTTP PAP  Trial  
 MAC Cookie

MAC Auth. Mode: MAC as username

MAC Auth. Password:

HTTP Cookie Lifetime: 3d 00:00:00

SSL Certificate: none

Split User Domain

Trial Uptime Limit: 00:30:00

Trial Uptime Reset: 1d 00:00:00

Trial User Profile: default

default

OK  
Cancel  
Apply  
Copy  
Remove



# Password Authentication Protocol (PAP)



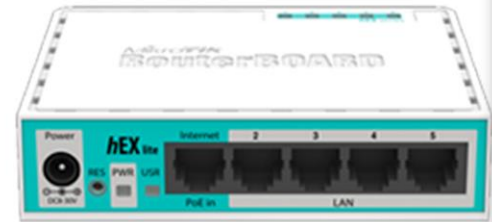
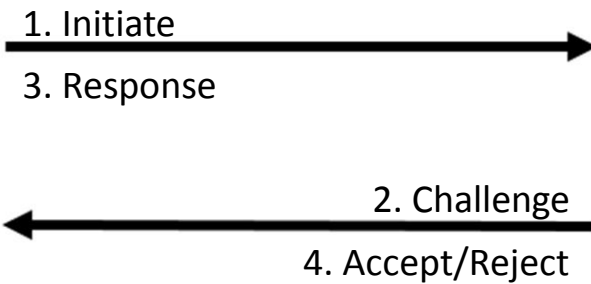
1. Username : mum\_takeuchi  
Password : mum2k17\_takeuchi



2. Accept/Reject



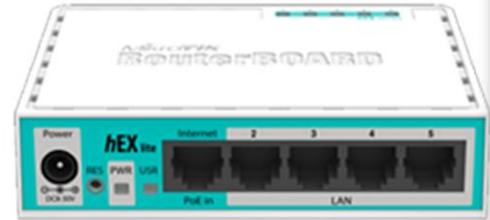
# Challenge Authentication Handshake Protocol (CHAP)



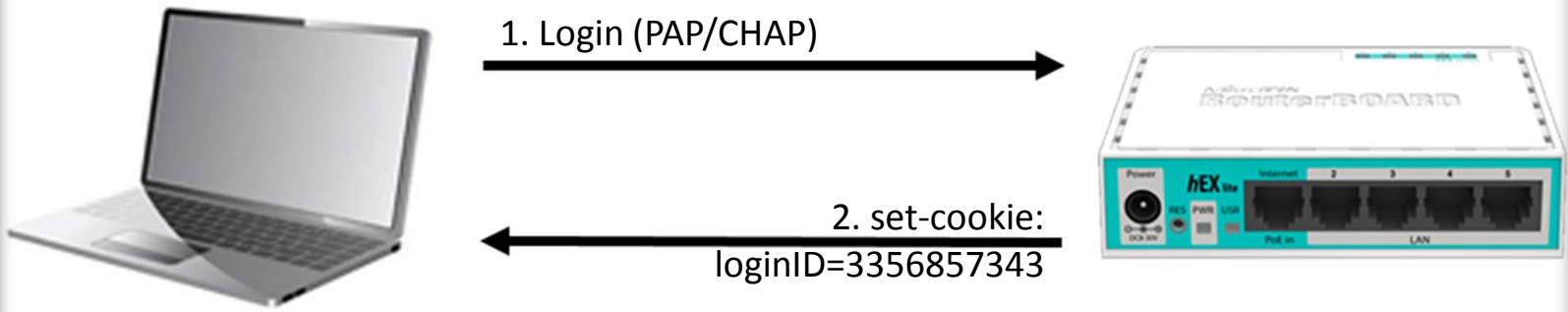
# HyperText Transfer Protocol Secure (HTTPS)



1. Start TLS Tunnel  
2. Then sending encrypted data  
3. Auth like HTTP PAP (encrypted)



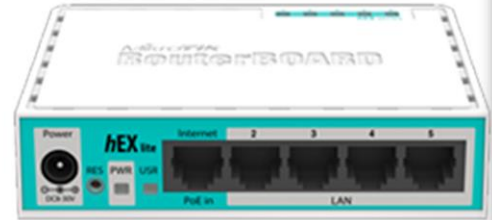
# HTTP Cookie (First Time Login)



# HTTP Cookie (Login Again)



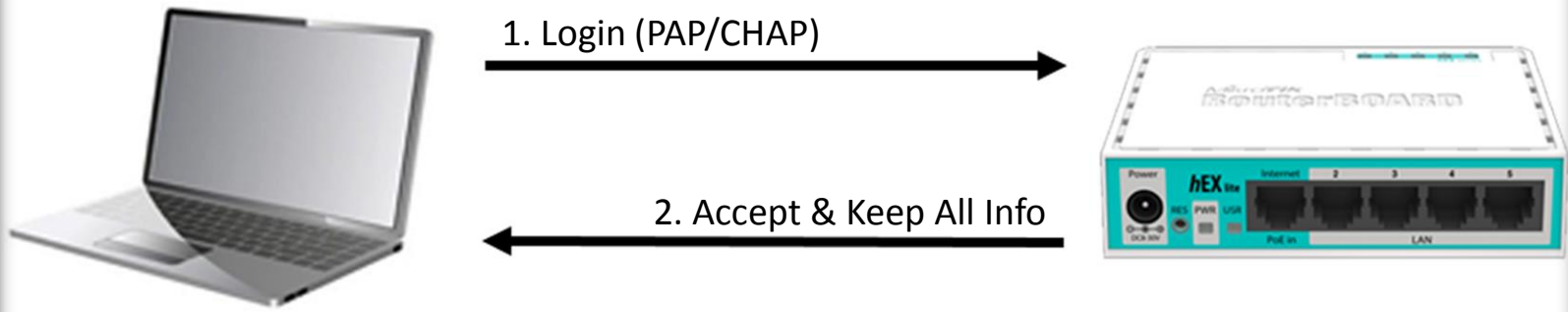
1. cookie: loginID=3356857343



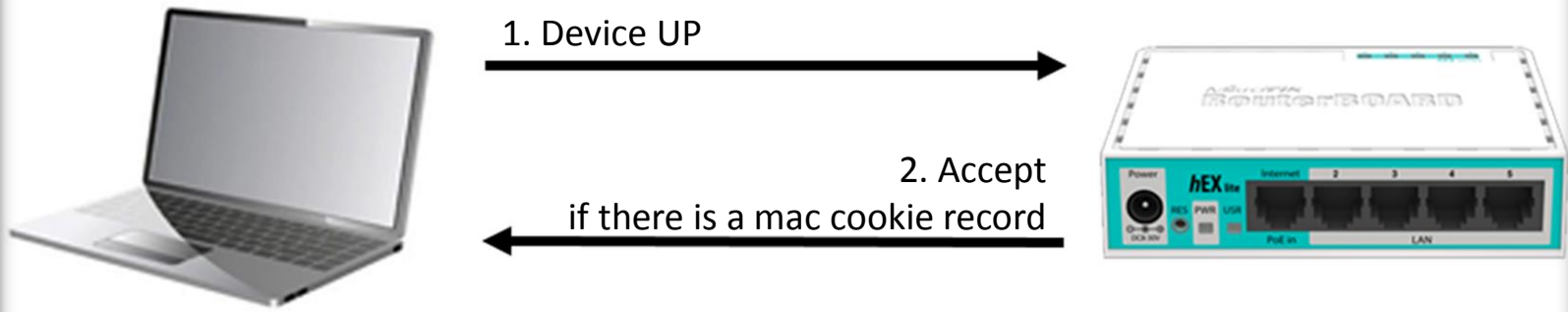
2. Accept



# MAC Cookie (First Login)



# MAC Cookie (Login Again)



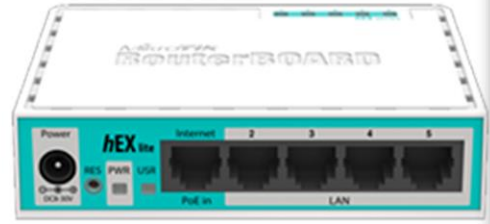
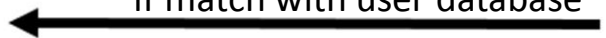
# MAC



1. Device UP



2. Accept  
if match with user database

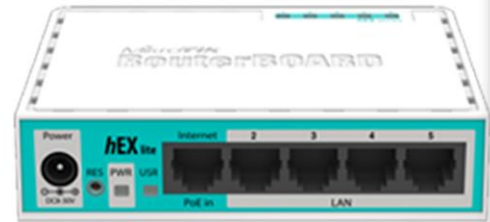
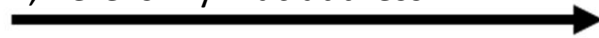




# Trial



1. Login (Trial Click)  
, here is my mac address



2. Accept



# MikroTik Router & Hotspot Audit

1. See how hard your username & password to guess
2. Always use secure protocol to login
3. Who can access your router?
4. See your router services
5. We need neighbor discovery?
6. We need MAC-Server?
7. What authentication method we need to set?

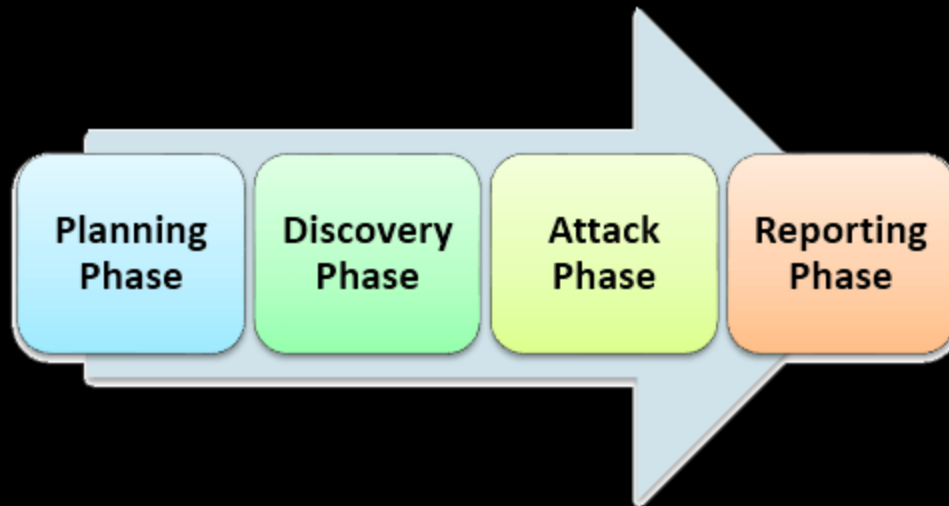
# MikroTik Router & Hotspot Hardening

1. Use Unexpected User Login Name
2. Do Not Use Default Port on Router
3. Use HTTP CHAP or HTTPS for Hotspot
4. Turn Off Neighbor Discovery for Router
5. Uncheck MAC, HTTP Cookie & Trial for Hotspot
6. Drop DDoS & Brute Force (Using Connection Limit) for Router
7. Use BGP Blackhole on Edge/Border Router for DDoS/DOS Mitigation

[http://wiki.mikrotik.com/wiki/DDoS Detection and Blocking](http://wiki.mikrotik.com/wiki/DDoS_Detection_and_Blocking)

[http://wiki.mikrotik.com/wiki/DoS attack protection](http://wiki.mikrotik.com/wiki/DoS_attack_protection)

# Common Penetration Test Step



in RouterOS can be like : on the next slide

# MikroTik Router & Hotspot Penetration Test Step

1. Information Gathering  
(neighbor discovery is also powerful 😊)
  2. Try default router login information
  3. See your neighbor
  4. Try to be your authenticated neighbor by using :
    1. Hotspot MAC Clone (can use TMAC & macchanger)
    2. Login Information Sniffing (can use wireshark)
    3. Cookie Stealing (can use wireshark)
  5. Brute Force (can use brutus)
- Don't forget to make a documentation for report 😊

# MikroTik Hotspot Auth. Packet (HTTP PAP)

The image shows a Wireshark capture of an HTTP POST request. The top pane displays a list of network packets, with the selected packet (No. 66) highlighted in blue. The packet details pane shows the structure of the POST request, including headers and the body. The body contains the authentication credentials: `dst=&popup=true&username=mum_takeuchi&password=mum2k17_takeuchi`.

No.	Time	Source	Destination	Protocol	Length	Info
11	0.246133	192.168.1.13	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
18	1.247107	192.168.1.13	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
37	6.266893	192.168.1.13	192.168.1.1	HTTP	546	GET /status HTTP/1.1
58	7.337385	192.168.1.13	192.168.1.1	HTTP	521	GET /logout? HTTP/1.1
62	7.891656	192.168.1.13	192.168.1.1	HTTP	521	GET /login? HTTP/1.1
66	7.920377	192.168.1.13	192.168.1.1	HTTP	456	GET /img/logobottom.png HTTP/1.1

```
POST /login HTTP/1.1
Host: hotspot.takeuchi.id
Connection: keep-alive
Content-Length: 63
Cache-Control: max-age=0
Origin: http://hotspot.takeuchi.id
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.90 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://hotspot.takeuchi.id/login?
Accept-Encoding: gzip, deflate
Accept-Language: id-ID,id;q=0.8,en-US;q=0.6,en;q=0.4,ms;q=0.2

dst=&popup=true&username=mum_takeuchi&password=mum2k17_takeuchiHTTP/1.1 200 OK
```

`username=mum_takeuchi&password=mum2k17_takeuchi`



# MikroTik Hotspot Auth. Packet (HTTP CHAP)

The image shows a Wireshark capture of an HTTP CHAP login packet. The packet list pane shows a POST request to /login. The packet bytes pane shows the raw data, and the packet details pane shows the HTTP request structure, including the password field.

No.	Time	Source	Destination	Protocol	Length	Info
146	4.513703	192.168.95.5	192.168.95.1	TCP	66	51758 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
147	4.514224	192.168.95.1	192.168.95.5	TCP	66	80 → 51758 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1 WS=4
148	4.514310	192.168.95.5	192.168.95.1	TCP	54	51758 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
149	4.514623	192.168.95.5	192.168.95.1	HTTP	731	POST /login HTTP/1.1 (application/x-www-form-urlencoded)
150	4.515398	192.168.95.1	192.168.95.5	TCP	60	80 → 51758 [ACK] Seq=1 Ack=678 Win=15956 Len=0
151	4.524246	192.168.95.1	192.168.95.5	HTTP	1408	HTTP/1.1 200 OK (text/html)
152	4.600859	192.168.95.5	192.168.95.1	HTTP	520	GET /status HTTP/1.1

```
username=mum_takeuchi&password=d5b8bceabcee921685cc7f1bdd335814&dst=&popup=trueHTTP/1.1 200 OK
```

POST /login HTTP/1.1  
Host: hotspot.takeuchi.id  
Connection: keep-alive  
Content-Length: 79  
Cache-Control: max-age=0  
Origin: http://hotspot.takeuchi.id  
Upgrade-Insecure-Requests: 1  
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36  
Content-Type: application/x-www-form-urlencoded  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8  
Referer: http://hotspot.takeuchi.id/login?  
Accept-Encoding: gzip, deflate  
Accept-Language: id-ID,id;q=0.8,en-US;q=0.6,en;q=0.4,ms;q=0.2

username=mum\_takeuchi&password=d5b8bceabcee921685cc7f1bdd335814&dst=&popup=trueHTTP/1.1 200 OK  
Cache-Control: no-cache  
Connection: Keep-Alive  
Content-Length: 1190  
Content-Type: text/html  
Date: Mon, 11 Sep 2017 05:47:18 GMT

**username=mum\_takeuchi&password=d5b8bceabcee921685cc7f1bdd335814**

# MikroTik Hotspot Auth. Packet (HTTP CHAP)

Decrypt!

## Results

**Md5 Hash:** d5b8bceabcee921685cc7f1bdd335814

**A decryption for this hash wasn't found in our database**

Copyright © 2005-2017 MD5decrypter.com  
All Rights Reserved.

<https://www.md5decrypter.com>



# MikroTik Hotspot Auth. Packet (HTTP CHAP)

Decrypt (search for a match):

Hash String

[Enable mass-decrypt mode](#)

Reverse decryption is failed. No match found. Try to search via "by all hash types" option. or try later. Sorry... :(

<https://md5hashing.net/hash/md5/>

# MikroTik Hotspot Auth. Packet (HTTPS)

The screenshot displays a Wireshark capture of an SSL/TLS handshake. The packet list pane shows the following sequence of packets:

No.	Time	Source	Destination	Protocol	Length	Info
46	2.278004	192.168.95.5	192.168.95.1	TLSv1.2	571	Client Hello
48	2.283635	192.168.95.1	192.168.95.5	TLSv1.2	191	Server Hello, Change Cipher Spec, Encrypted Handshake Message
49	2.284754	192.168.95.5	192.168.95.1	TLSv1.2	105	Change Cipher Spec, Hello Request, Hello Request
56	2.287971	192.168.95.5	192.168.95.1	TLSv1.2	571	Client Hello
58	2.293786	192.168.95.1	192.168.95.5	TLSv1.2	191	Server Hello, Change Cipher Spec, Encrypted Handshake Message
59	2.294012	192.168.95.5	192.168.95.1	TLSv1.2	105	Change Cipher Spec, Hello Request, Hello Request
60	2.294383	192.168.95.5	192.168.95.1	TLSv1.2	749	Application Data
62	2.306648	192.168.95.1	192.168.95.5	TLSv1.2	1437	Application Data

The packet details pane for the selected packet (No. 48) shows the following structure:

- Type: server\_name (0x0000)
- Length: 24
- Server Name Indication extension
  - Server Name list length: 22
  - Server Name Type: host\_name (0)
  - Server Name length: 19
  - Server Name: hotspot.takeuchi.id

The packet bytes pane shows the raw data for the Server Name Indication extension, which is the ASCII string "hotspot.takeuchi.id".

Summary: Server Name (ssl.handshake.extensions\_server\_name), 19 bytes | Packets: 164 · Displayed: 8 (4.9%) · Dropped: 0 (0.0%) | Profile: Default

Encrypted



# MikroTik Hotspot Auth. Packet (HTTPS)

The image shows a Wireshark capture of an HTTPS packet. The packet list pane shows a sequence of TLSv1.2 records. The selected packet (No. 62) is a TLSv1.2 Application Data record. The packet details pane shows the following structure:

- Transmission Control Protocol, Src Port: 443, Dst Port: 55014, Seq: 138, Ack: 1264, Len: 1383
- Secure Sockets Layer
  - TLSv1.2 Record Layer: Application Data Protocol: http-over-tls
    - Content Type: Application Data (23)
    - Version: TLS 1.2 (0x0303)
    - Length: 1378
    - Encrypted Application Data: e8ab96578b12165f4c78691dc304b6c1dc9ebec5b5289e9e...

The packet bytes pane shows the raw data of the encrypted application data, which is a sequence of hexadecimal bytes. The status bar at the bottom indicates: Payload is encrypted application data (ssl.app\_data), 1378 bytes. Packets: 164 · Displayed: 8 (4.9%) · Dropped: 0 (0.0%) Profile: Default

Encrypted



# MikroTik Hotspot Auth. Packet (HTTP Cookie)

The image shows a Wireshark packet capture of an HTTP login session. The main packet list shows a GET request for /login? and a corresponding 200 OK response. The response details pane shows the following headers:

```
GET /login? HTTP/1.1
Host: hotspot.takeuchi.id
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://hotspot.takeuchi.id/logout?
Accept-Encoding: gzip, deflate
Accept-Language: id-ID,id;q=0.8,en-US;q=0.6,en;q=0.4,ms;q=0.2
Cookie: loginID=3356857343

HTTP/1.1 200 OK
Cache-Control: no-cache
Connection: Keep-Alive
```

The cookie value `loginID=3356857343` is highlighted in yellow in the original image.

Cookie: loginID=3356857343



# MikroTik Hotspot Auth. Packet (Trial)

The image shows a Wireshark packet capture window titled "Local Area Connection". The main pane displays a list of captured packets, with packet 57 selected. The packet list table is as follows:

No.	Time	Source	Destination	Protocol	Length	Info
56	1.863806	192.168.90.3	192.168.90.1	HTTP	564	GET /login?dst=&username=T-02%3AE2%3AFD%3ADE%3ADA%3A67 HTTP/1.1
57	1.873535	192.168.90.1	192.168.90.3	HTTP	1408	HTTP/1.1 200 OK (text/html)
58	1.942667	192.168.90.3	192.168.90.1	HTTP	564	GET /status HTTP/1.1
60	1.951745	192.168.90.1	192.168.90.3	HTTP	928	HTTP/1.1 200 OK (text/html)

The packet details pane for packet 57 shows the following structure:

- Frame 56: 564 bytes on wire (4512 bits), 564 bytes captured (4512 bits) on interface 0
- Ethernet II, Src: 02:e2:fd:de:da:67 (02:e2:fd:de:da:67), Dst: Routerbo\_e7:37:b1 (6c:3b:6b:e7:37:b1)
- Internet Protocol Version 4, Src Port: 51101, Dst Port: 80, Seq: 1, Ack: 1, Len: 510
- Transmission Control Protocol, Src Port: 51101, Dst Port: 80, Seq: 1, Ack: 1, Len: 510
- Hypertext Transfer Protocol
  - GET /login?dst=&username=T-02%3AE2%3AFD%3ADE%3ADA%3A67 HTTP/1.1\r\n
    - [Expert Info (Chat/Sequence): GET /login?dst=&username=T-02%3AE2%3AFD%3ADE%3ADA%3A67 HTTP/1.1\r\n]
    - Request Method: GET
    - Request URI: /login?dst=&username=T-02%3AE2%3AFD%3ADE%3ADA%3A67
    - Request URI Path: /login
      - Request URI Query: dst=&username=T-02%3AE2%3AFD%3ADE%3ADA%3A67
      - Request URI Query Parameter: dst=
      - Request URI Query Parameter: username=T-02%3AE2%3AFD%3ADE%3ADA%3A67
    - Request Version: HTTP/1.1
    - Host: hotspot.takeuchi.id\r\n
    - Connection: keep-alive\r\n
    - Upgrade-Insecure-Requests: 1\r\n
    - User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Safari/537.36\r\n
    - Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8\r\n
    - Referer: http://hotspot.takeuchi.id/login?\r\n
    - Accept-Encoding: gzip, deflate\r\n
    - Accept-Language: id-ID,id;q=0.8,en-US;q=0.6,en;q=0.4,ms;q=0.2\r\n
    - \r\n
    - [Full request URI: http://hotspot.takeuchi.id/login?dst=&username=T-02%3AE2%3AFD%3ADE%3ADA%3A67]
    - [HTTP request 1/2]
    - [Response in frame: 57]

The raw packet bytes pane shows the following hex and ASCII data:

```
0030 40 29 b6 97 00 00 47 45 54 20 2f 6c 6f 67 69 6e @)...GET /login
0040 3f 64 73 74 3d 26 75 73 65 72 6e 61 6d 65 3d 54 ?dst=&username=T
0050 2d 30 32 25 33 41 45 32 25 33 41 46 44 25 33 41 -02%3AE2%3AFD%3A
0060 44 45 25 33 41 44 41 25 33 41 36 37 20 48 54 44 DE%3ADA%3A67 HT
0070 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 68 6f 74 P/1.1..Host: hot
0080 73 70 6f 74 2e 74 61 6b 65 75 63 68 69 2e 69 64 spot.tak euchi.id
```

login?dst=&username=T-02%3AE2%3AFD%3ADE%3ADA%3A67



# MikroTik Hotspot Auth. Packet (MAC/MAC Cookie)

- MAC Authentication will be done automatically when the device was up and this process is done by Router (not user)

Summary

# Secure $\neq$ Easy

# Book Reference – MikroTik Hotspot Server



**Title** : MikroTik Hotspot Server  
**Author** : Rendra Towidjojo  
**Publisher** : IlmuJaringan(dot)Com  
**Issue Date** : 19 July 2017  
**Paper** : HVS 80gsm  
**Thickness** : 326 pages  
**Size** : 210 x 145 x 200 mm  
**ISBN** : 978-602-74937-2-8  
**Language** : Bahasa Indonesia



# Link Reference

- [https://wiki.mikrotik.com/wiki/Manual:Hotspot\\_Introduction](https://wiki.mikrotik.com/wiki/Manual:Hotspot_Introduction)
- <https://wiki.mikrotik.com/wiki/Manual:IP/Hotspot>
- [http://mikrotik.co.id/artikel\\_lihat.php?id=125](http://mikrotik.co.id/artikel_lihat.php?id=125)
- <https://mum.mikrotik.com/archive>
- [https://en.wikipedia.org/wiki/Password\\_Authentication\\_Protocol](https://en.wikipedia.org/wiki/Password_Authentication_Protocol)
- [https://en.wikipedia.org/wiki/Challenge-Handshake\\_Authentication\\_Protocol](https://en.wikipedia.org/wiki/Challenge-Handshake_Authentication_Protocol)
- [https://en.wikipedia.org/wiki/HTTP\\_cookie](https://en.wikipedia.org/wiki/HTTP_cookie)
- <http://www.ilmuhacking.com/cryptography/understanding-https/>

Feel So Hard To Securing, Auditing, Hardening Your Network?

Let Me Help You !

[michael@takeuchi.id](mailto:michael@takeuchi.id)

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

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

Any Questions?





Thank  
you

