MikroTik 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]
tau cara bypass mikrotik ga ?

up

[redacted] ▶ [redacted]
4 jam ·

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. Harderning your network
3. Penetration Testing your network
4. Repeat

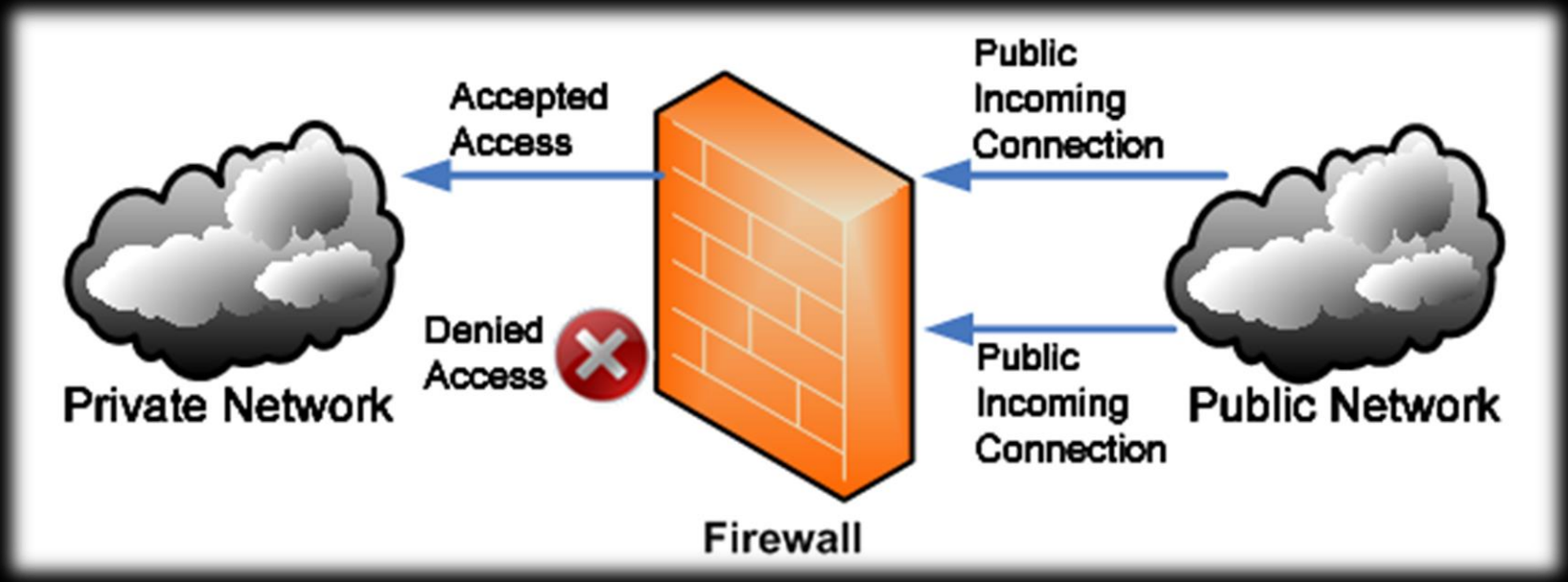
- Before we do that things, we need to know about Firewall & Network Security and how your system works

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)

What is Firewall?



What is Network Security

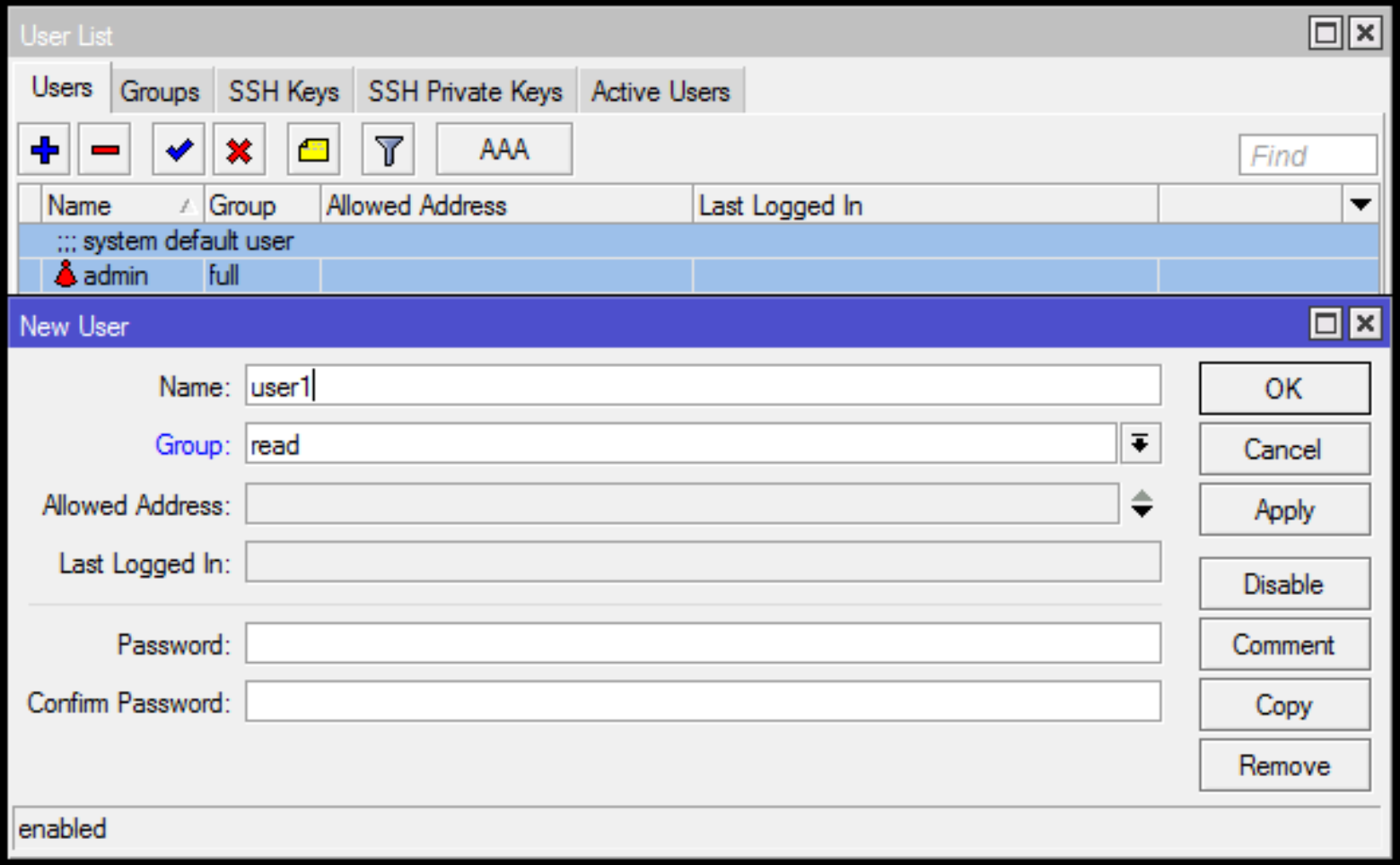
- Network security consists of the policies and practices adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the 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

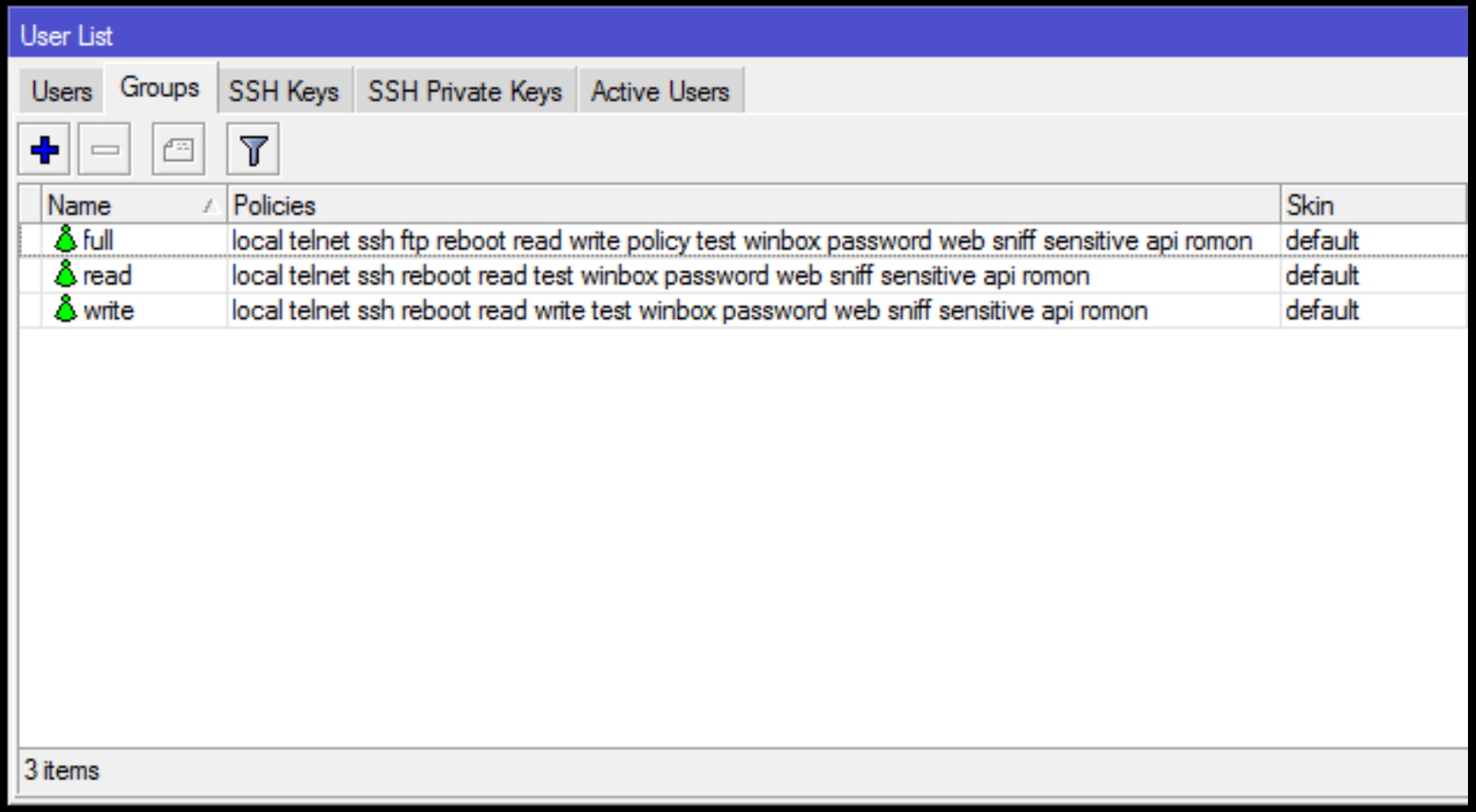
Before we go to hotspot, we need to audit our router

Oopss sorry, I mean before doing a setup

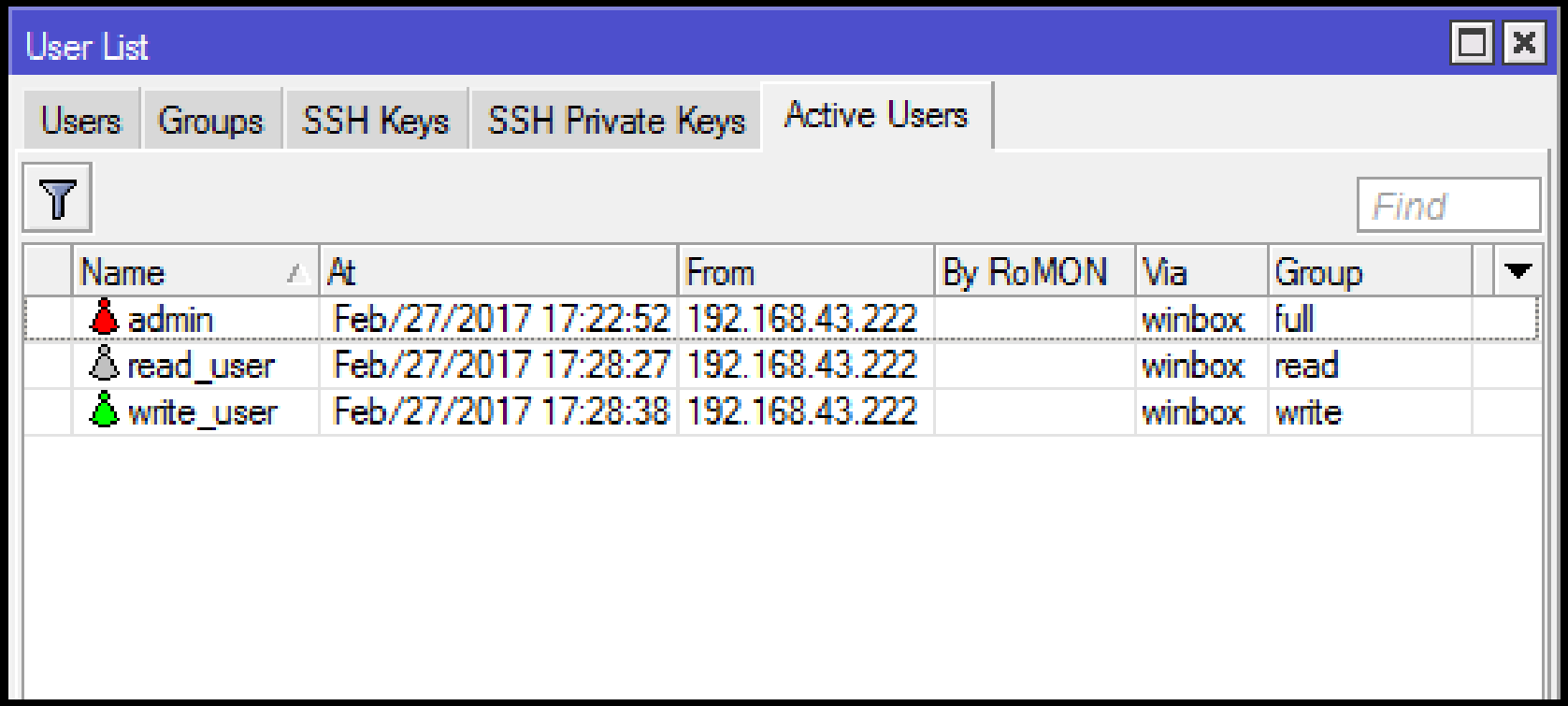
MikroTik Router Login – User



MikroTik Router Login – Groups



MikroTik Router Login – Active Users



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

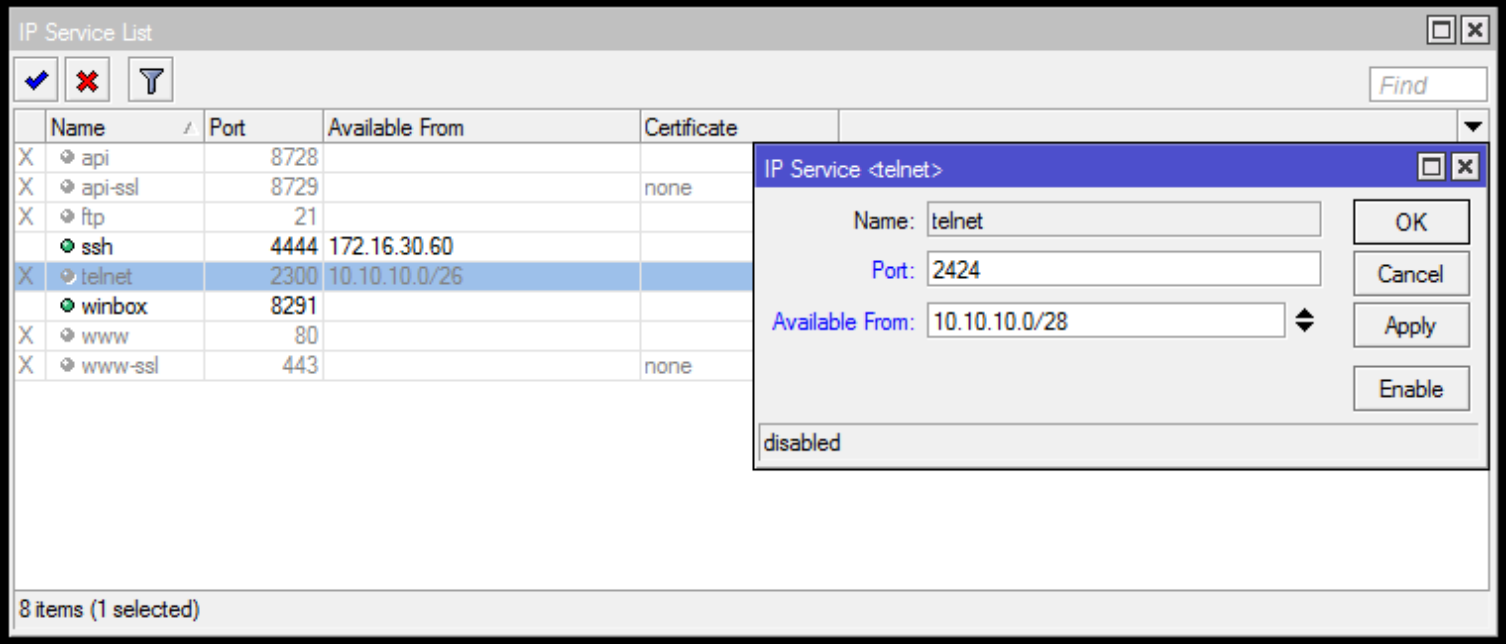
IP Service List

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

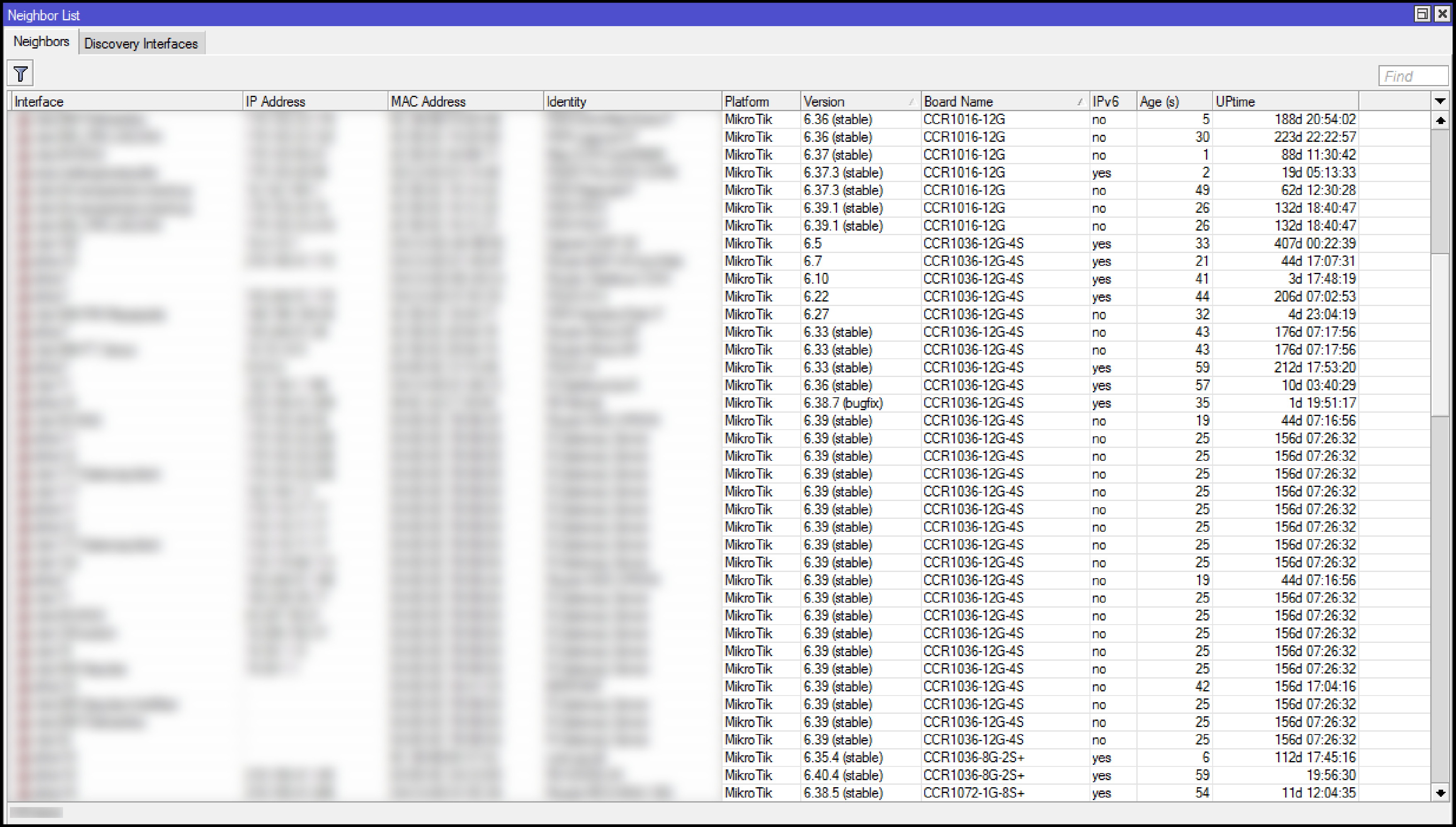


Login Comparison

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

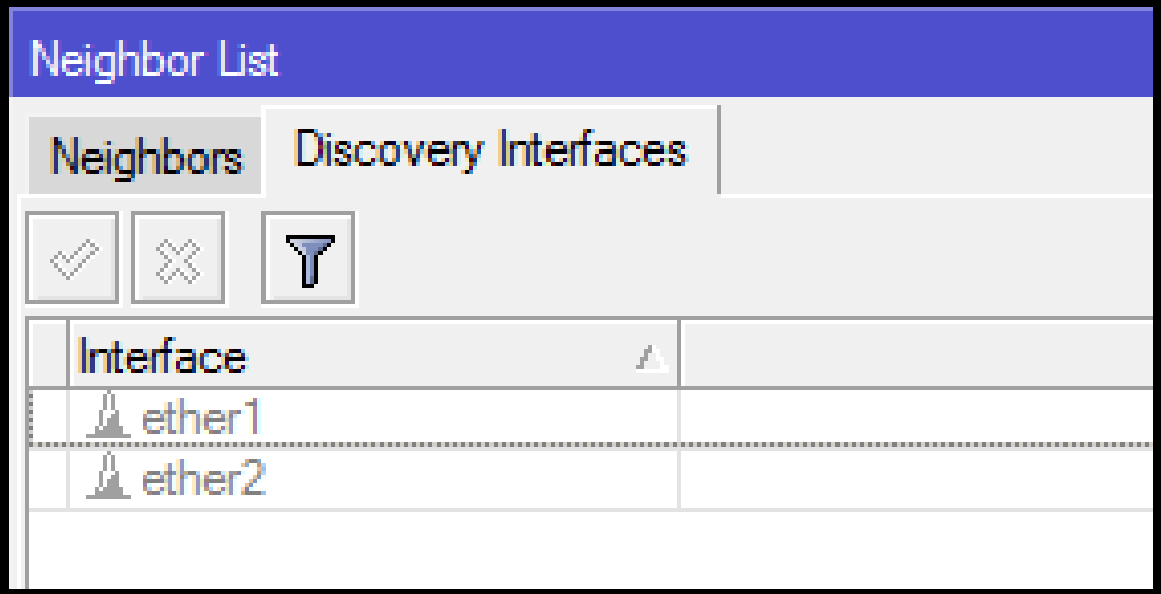
MikroTik Neighbor Discovery



Interface	IP Address	MAC Address	Identity	Platform	Version	Board Name	IPv6	Age (s)	UPtime
[redacted]	[redacted]	[redacted]	[redacted]	MikroTik	6.36 (stable)	CCR1016-12G	no	5	188d 20:54:02
[redacted]	[redacted]	[redacted]	[redacted]	MikroTik	6.36 (stable)	CCR1016-12G	no	30	223d 22:22:57
[redacted]	[redacted]	[redacted]	[redacted]	MikroTik	6.37 (stable)	CCR1016-12G	no	1	88d 11:30:42
[redacted]	[redacted]	[redacted]	[redacted]	MikroTik	6.37.3 (stable)	CCR1016-12G	yes	2	19d 05:13:33
[redacted]	[redacted]	[redacted]	[redacted]	MikroTik	6.37.3 (stable)	CCR1016-12G	no	49	62d 12:30:28
[redacted]	[redacted]	[redacted]	[redacted]	MikroTik	6.39.1 (stable)	CCR1016-12G	no	26	132d 18:40:47
[redacted]	[redacted]	[redacted]	[redacted]	MikroTik	6.39.1 (stable)	CCR1016-12G	no	26	132d 18:40:47
[redacted]	[redacted]	[redacted]	[redacted]	MikroTik	6.5	CCR1036-12G-4S	yes	33	407d 00:22:39
[redacted]	[redacted]	[redacted]	[redacted]	MikroTik	6.7	CCR1036-12G-4S	yes	21	44d 17:07:31
[redacted]	[redacted]	[redacted]	[redacted]	MikroTik	6.10	CCR1036-12G-4S	yes	41	3d 17:48:19
[redacted]	[redacted]	[redacted]	[redacted]	MikroTik	6.22	CCR1036-12G-4S	yes	44	206d 07:02:53
[redacted]	[redacted]	[redacted]	[redacted]	MikroTik	6.27	CCR1036-12G-4S	no	32	4d 23:04:19
[redacted]	[redacted]	[redacted]	[redacted]	MikroTik	6.33 (stable)	CCR1036-12G-4S	no	43	176d 07:17:56
[redacted]	[redacted]	[redacted]	[redacted]	MikroTik	6.33 (stable)	CCR1036-12G-4S	no	43	176d 07:17:56
[redacted]	[redacted]	[redacted]	[redacted]	MikroTik	6.33 (stable)	CCR1036-12G-4S	yes	59	212d 17:53:20
[redacted]	[redacted]	[redacted]	[redacted]	MikroTik	6.36 (stable)	CCR1036-12G-4S	yes	57	10d 03:40:29
[redacted]	[redacted]	[redacted]	[redacted]	MikroTik	6.38.7 (bugfix)	CCR1036-12G-4S	yes	35	1d 19:51:17
[redacted]	[redacted]	[redacted]	[redacted]	MikroTik	6.39 (stable)	CCR1036-12G-4S	no	19	44d 07:16:56
[redacted]	[redacted]	[redacted]	[redacted]	MikroTik	6.39 (stable)	CCR1036-12G-4S	no	25	156d 07:26:32
[redacted]	[redacted]	[redacted]	[redacted]	MikroTik	6.39 (stable)	CCR1036-12G-4S	no	25	156d 07:26:32
[redacted]	[redacted]	[redacted]	[redacted]	MikroTik	6.39 (stable)	CCR1036-12G-4S	no	25	156d 07:26:32
[redacted]	[redacted]	[redacted]	[redacted]	MikroTik	6.39 (stable)	CCR1036-12G-4S	no	25	156d 07:26:32
[redacted]	[redacted]	[redacted]	[redacted]	MikroTik	6.39 (stable)	CCR1036-12G-4S	no	25	156d 07:26:32
[redacted]	[redacted]	[redacted]	[redacted]	MikroTik	6.39 (stable)	CCR1036-12G-4S	no	25	156d 07:26:32
[redacted]	[redacted]	[redacted]	[redacted]	MikroTik	6.39 (stable)	CCR1036-12G-4S	no	25	156d 07:26:32
[redacted]	[redacted]	[redacted]	[redacted]	MikroTik	6.39 (stable)	CCR1036-12G-4S	no	25	156d 07:26:32
[redacted]	[redacted]	[redacted]	[redacted]	MikroTik	6.39 (stable)	CCR1036-12G-4S	no	19	44d 07:16:56
[redacted]	[redacted]	[redacted]	[redacted]	MikroTik	6.39 (stable)	CCR1036-12G-4S	no	25	156d 07:26:32
[redacted]	[redacted]	[redacted]	[redacted]	MikroTik	6.39 (stable)	CCR1036-12G-4S	no	25	156d 07:26:32
[redacted]	[redacted]	[redacted]	[redacted]	MikroTik	6.39 (stable)	CCR1036-12G-4S	no	25	156d 07:26:32
[redacted]	[redacted]	[redacted]	[redacted]	MikroTik	6.39 (stable)	CCR1036-12G-4S	no	25	156d 07:26:32
[redacted]	[redacted]	[redacted]	[redacted]	MikroTik	6.39 (stable)	CCR1036-12G-4S	no	25	156d 07:26:32
[redacted]	[redacted]	[redacted]	[redacted]	MikroTik	6.39 (stable)	CCR1036-12G-4S	no	42	156d 17:04:16
[redacted]	[redacted]	[redacted]	[redacted]	MikroTik	6.39 (stable)	CCR1036-12G-4S	no	25	156d 07:26:32
[redacted]	[redacted]	[redacted]	[redacted]	MikroTik	6.39 (stable)	CCR1036-12G-4S	no	25	156d 07:26:32
[redacted]	[redacted]	[redacted]	[redacted]	MikroTik	6.39 (stable)	CCR1036-12G-4S	no	25	156d 07:26:32
[redacted]	[redacted]	[redacted]	[redacted]	MikroTik	6.35.4 (stable)	CCR1036-8G-2S+	yes	6	112d 17:45:16
[redacted]	[redacted]	[redacted]	[redacted]	MikroTik	6.40.4 (stable)	CCR1036-8G-2S+	yes	59	19:56:30
[redacted]	[redacted]	[redacted]	[redacted]	MikroTik	6.38.5 (stable)	CCR1072-1G-8S+	yes	54	11d 12:04:35

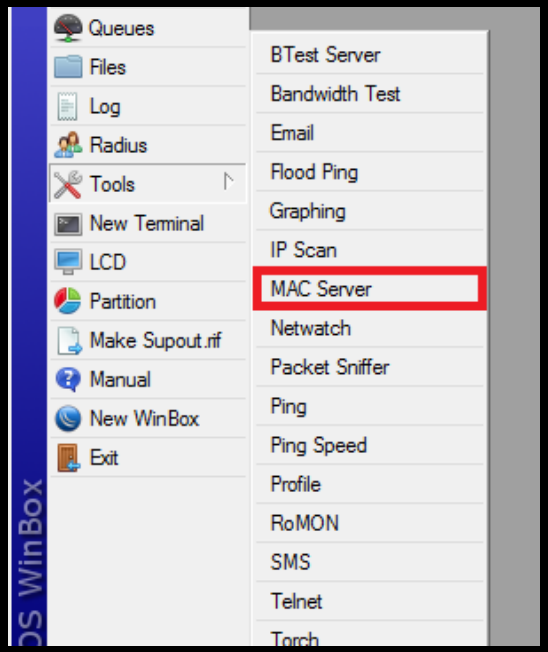
MikroTik Neighbor Discovery

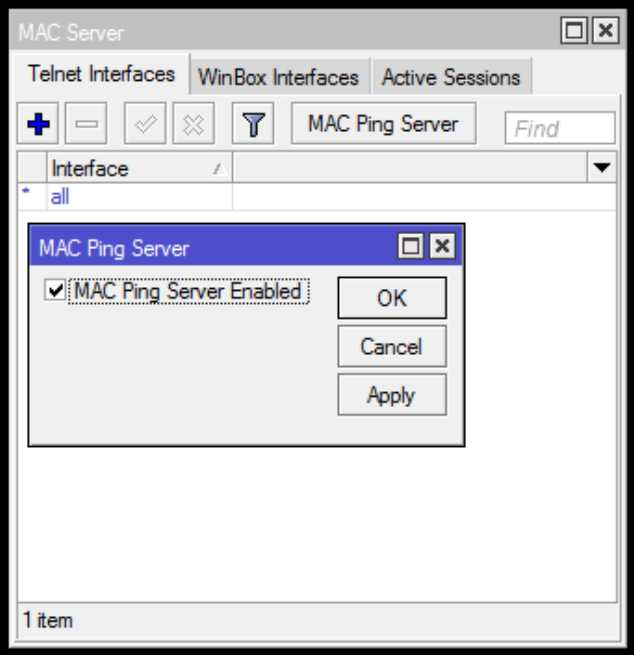
- Turn off neighbor discovery or your router will discovered by your neighbor and on winbox, it's good for being undetected ☺

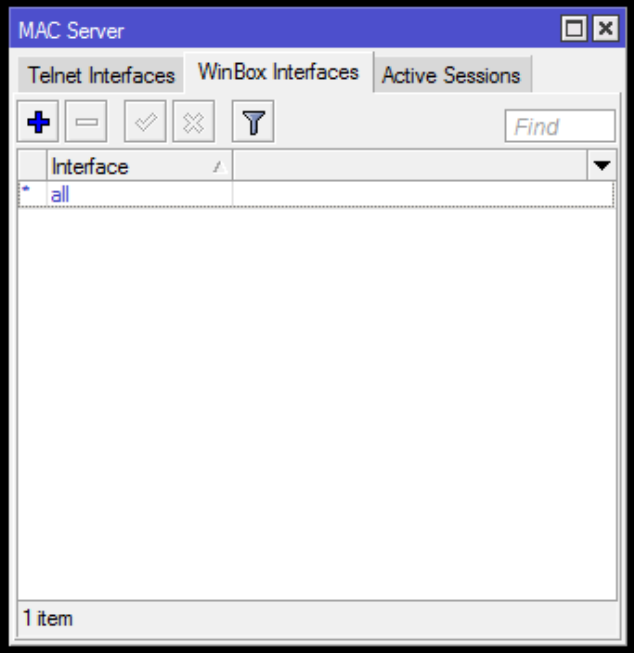


MikroTik MAC-Server

- Turn off MAC-Server for Prevent Layer 2 Communication



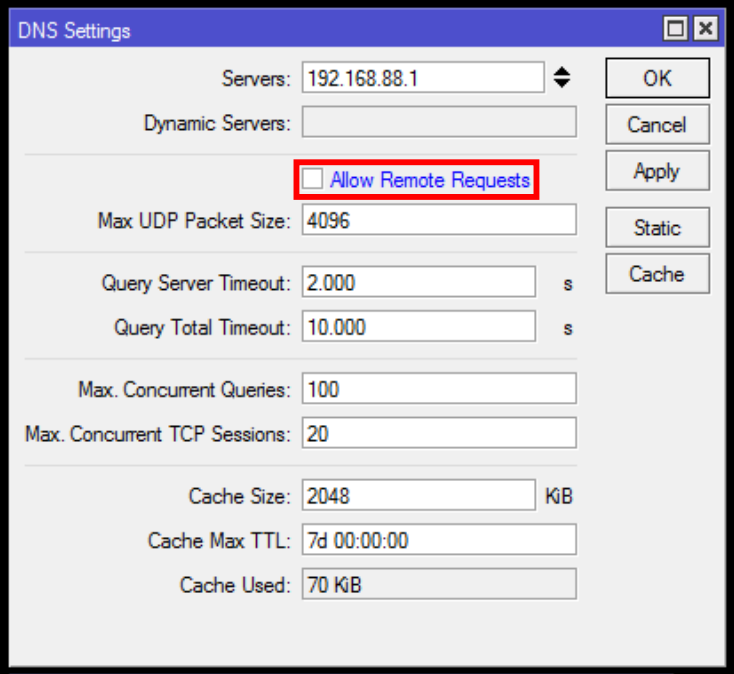


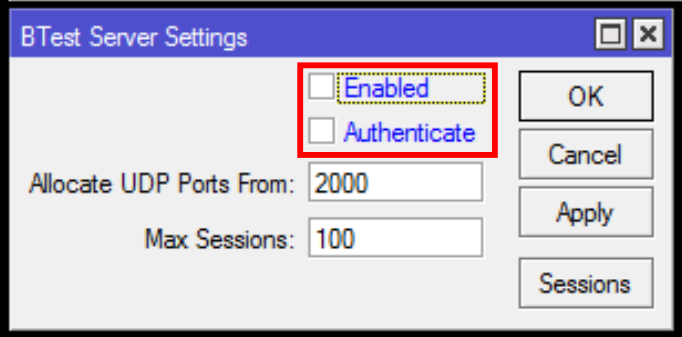


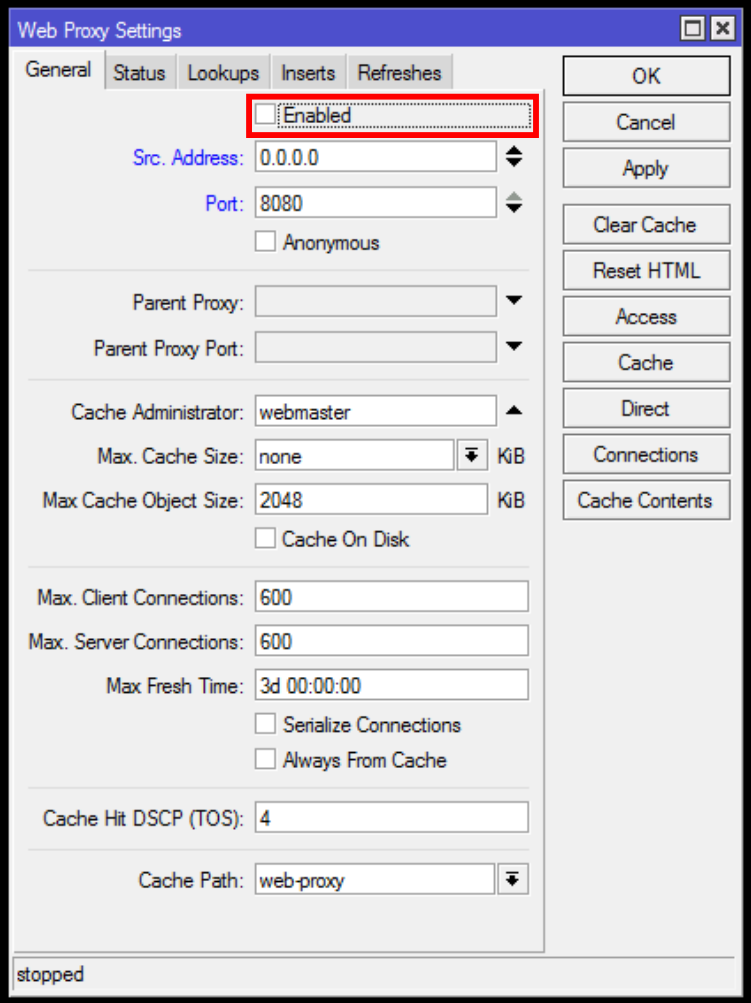
Turn off Router Public Services

- 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

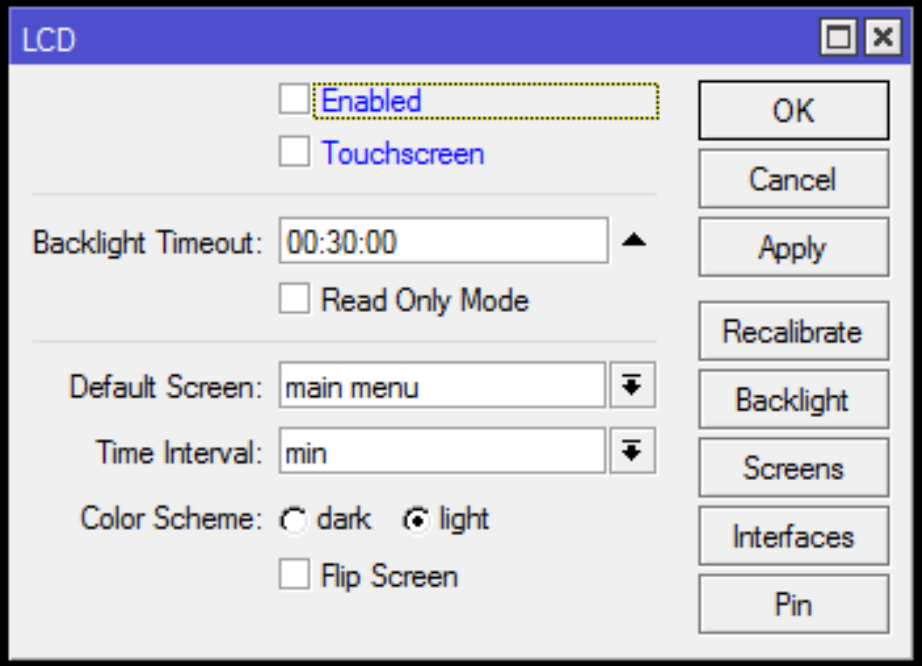






Protect The Physical

- Turn off the LCD



Protect The Physical

- 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.

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

(DDOS Attacks and MikroTik by Dennis Burgess)

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

(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

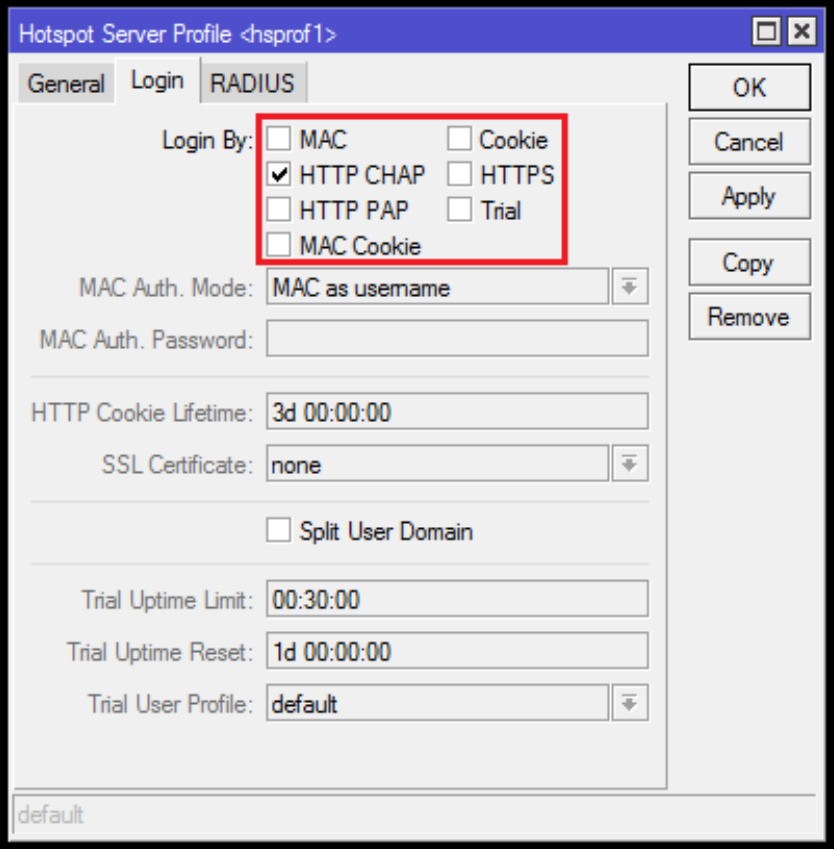
- Let’s Talk About MikroTik HotSpot Login Security !
- What Do We Need To Know To Securing It?

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

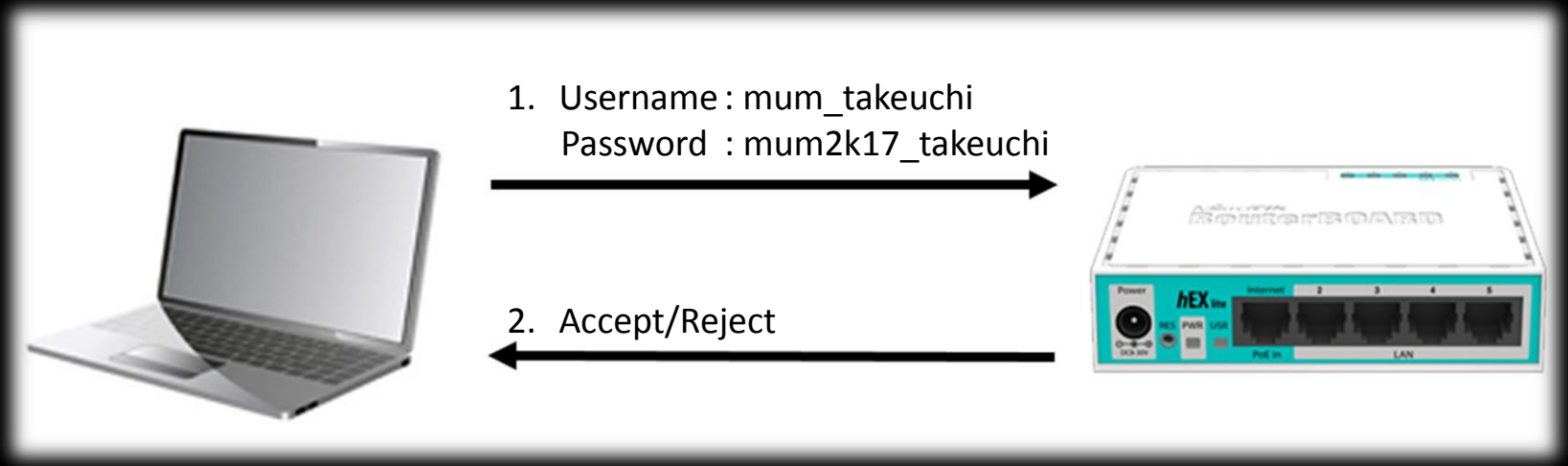
- Sun Tzu

MikroTik Hotspot Authentication Method

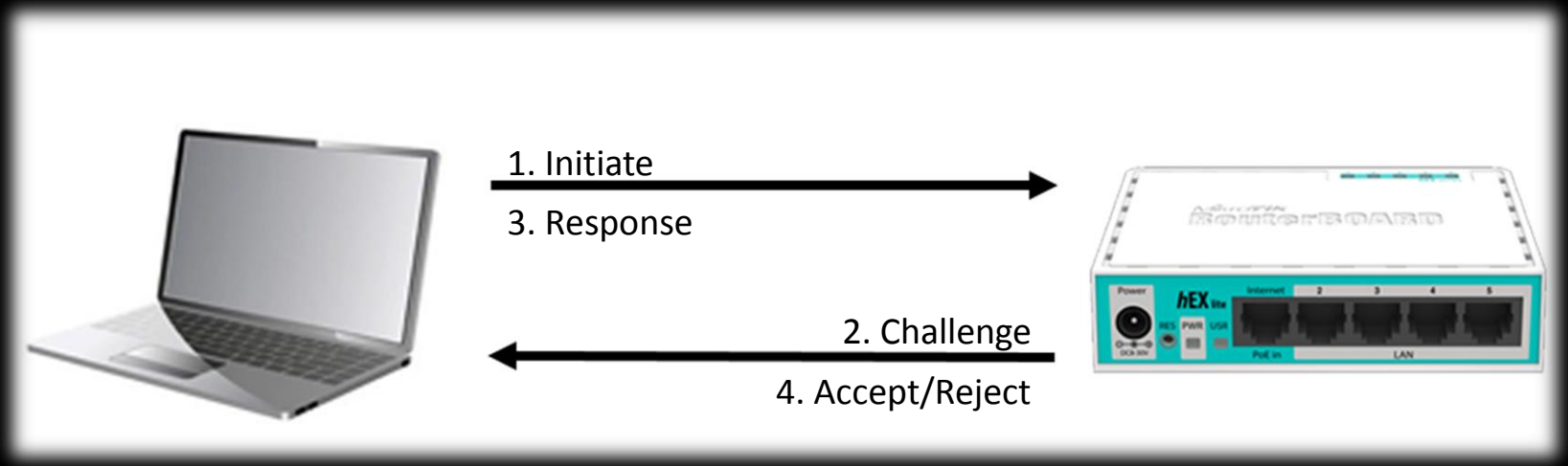
- MAC Cookie
- HTTP CHAP
- HTTP PAP
- Cookie
- HTTPS
- MAC
- Trial



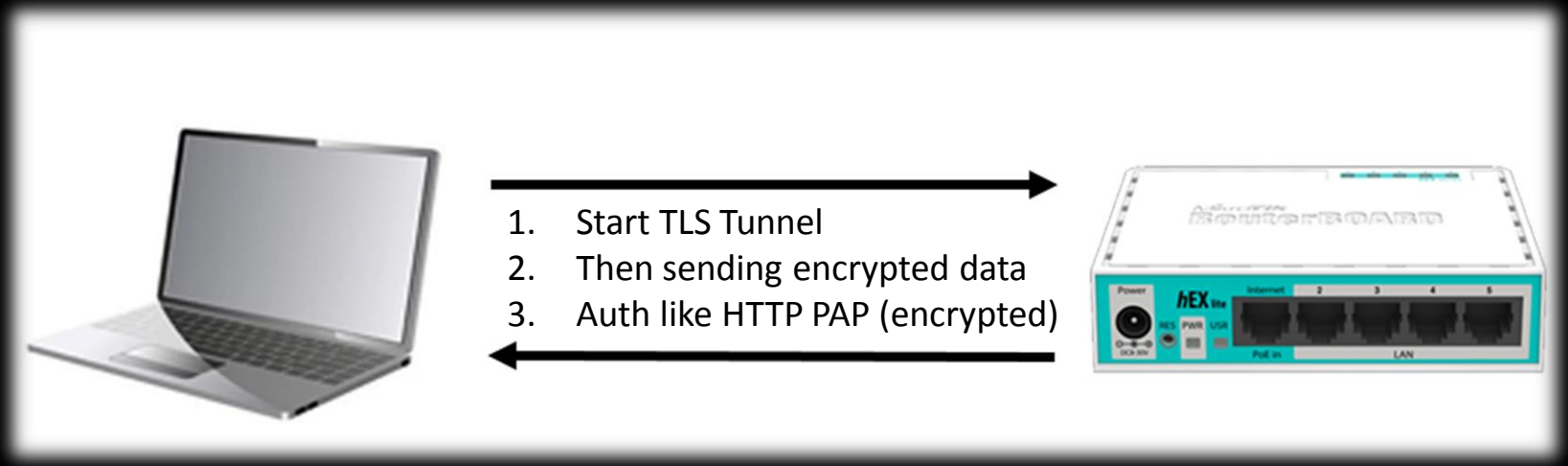
Password Authentication Protocol (PAP)



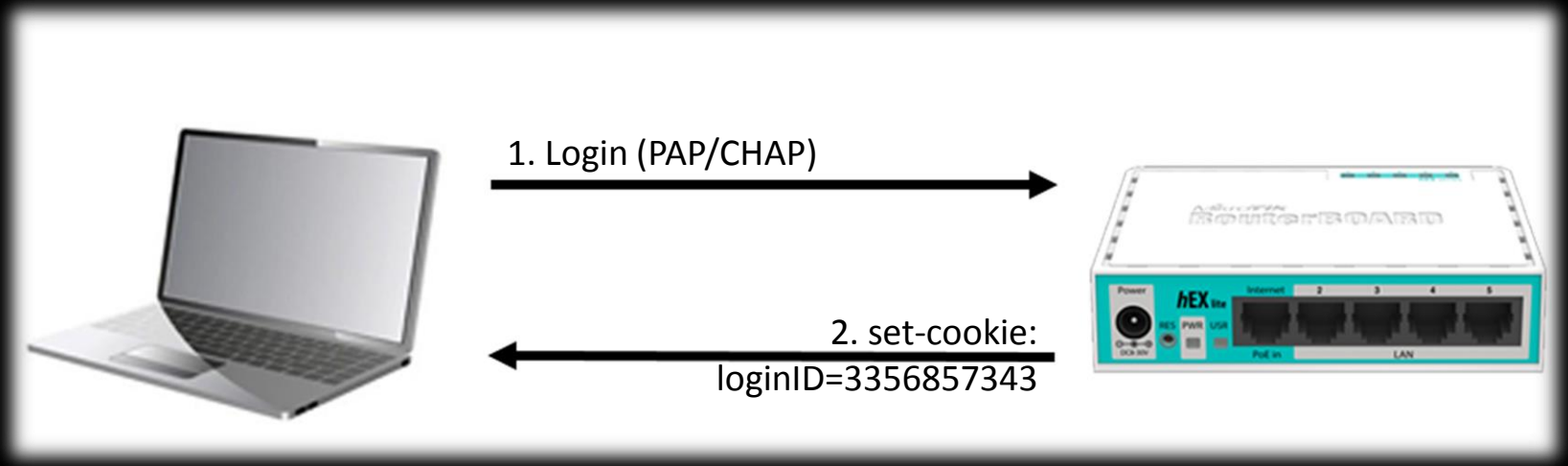
Challenge Authentication Handshake Protocol (CHAP)



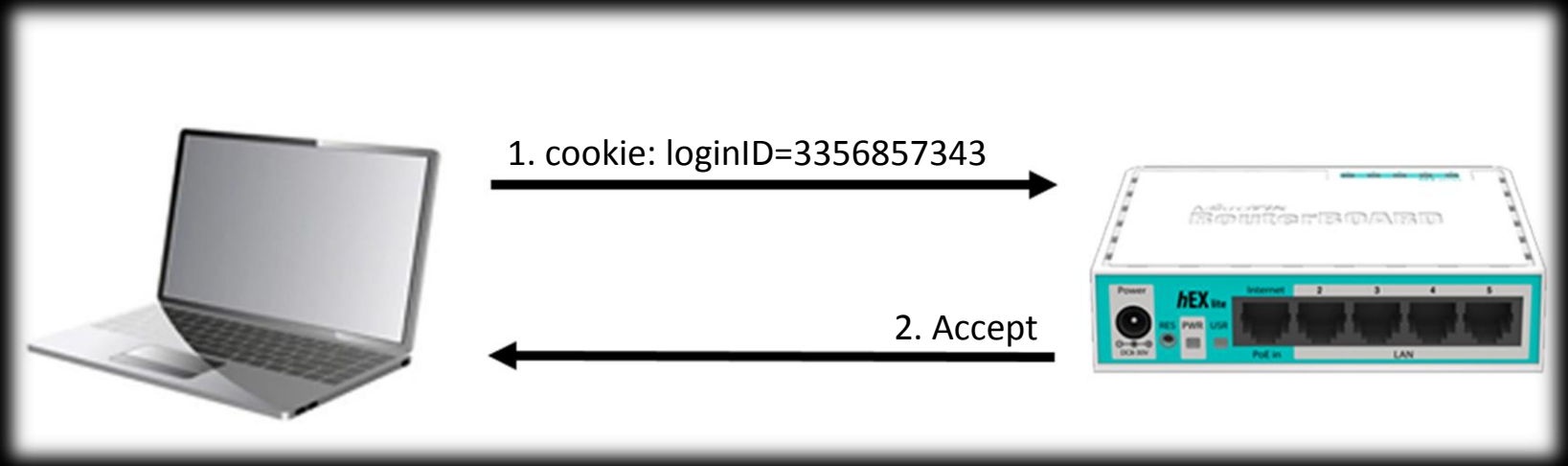
HyperText Transfer Protocol Secure (HTTPS)



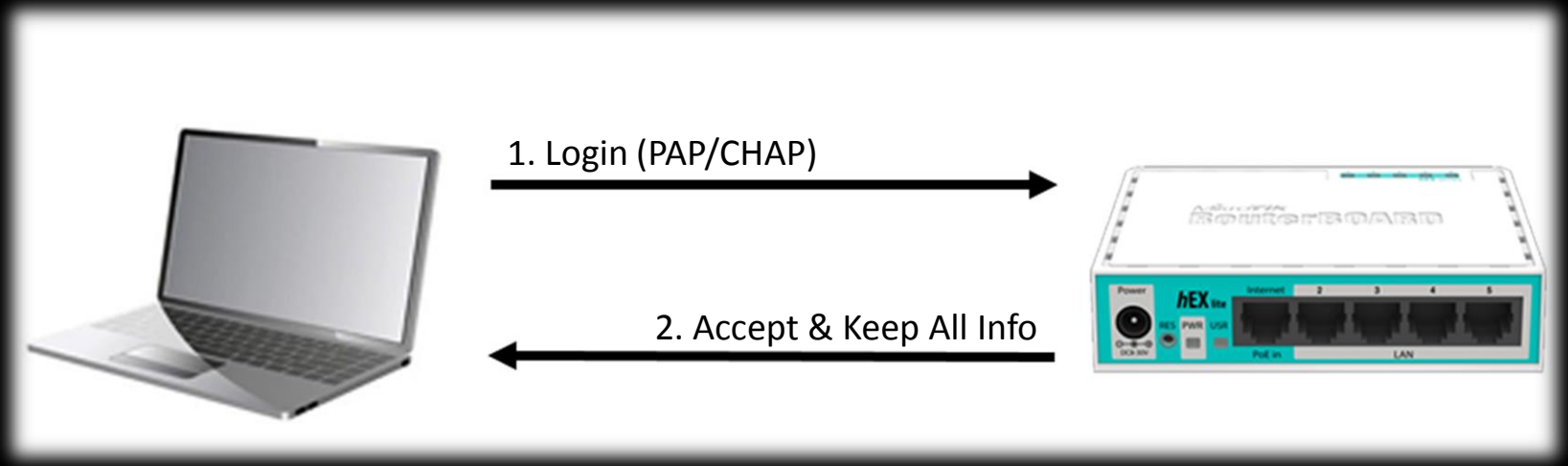
HTTP Cookie (First Time Login)



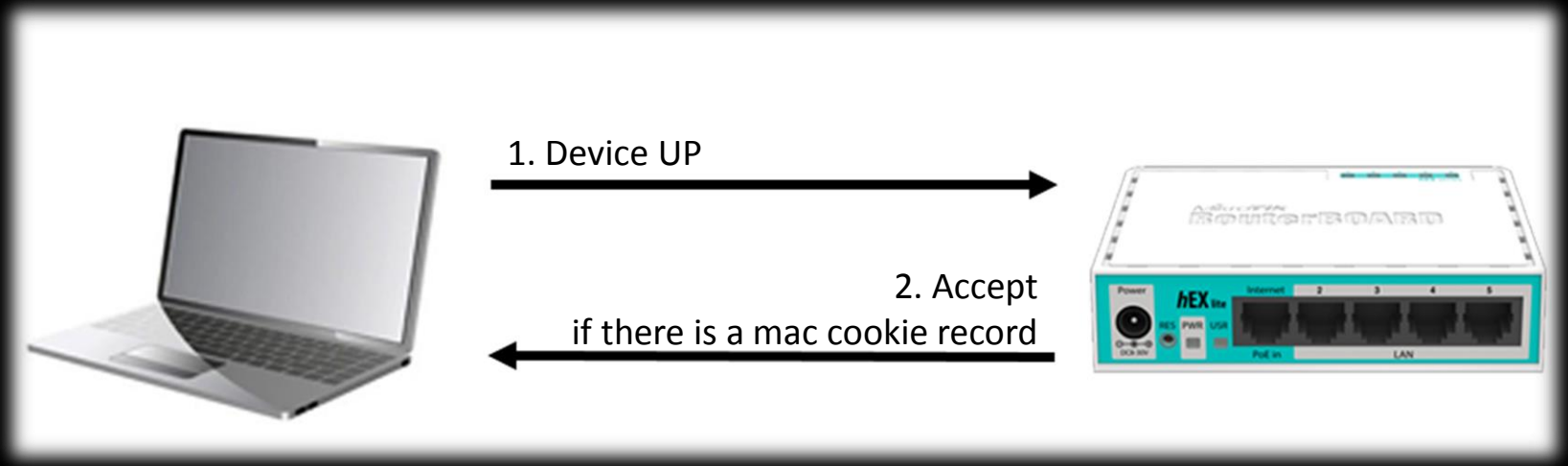
HTTP Cookie (Login Again)



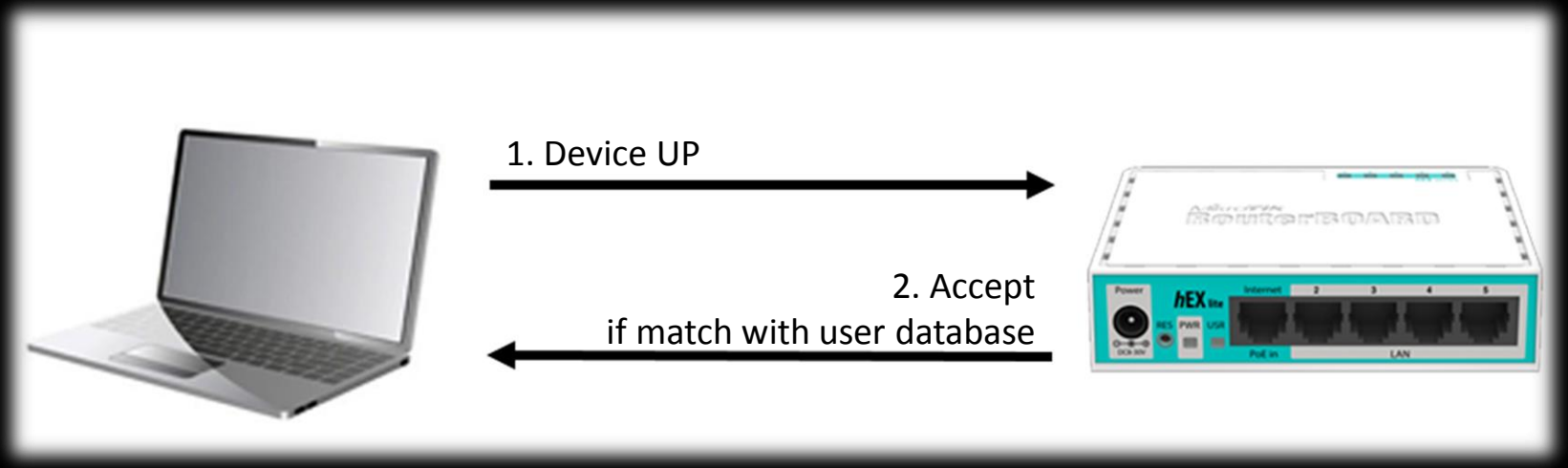
MAC Cookie (First Login)



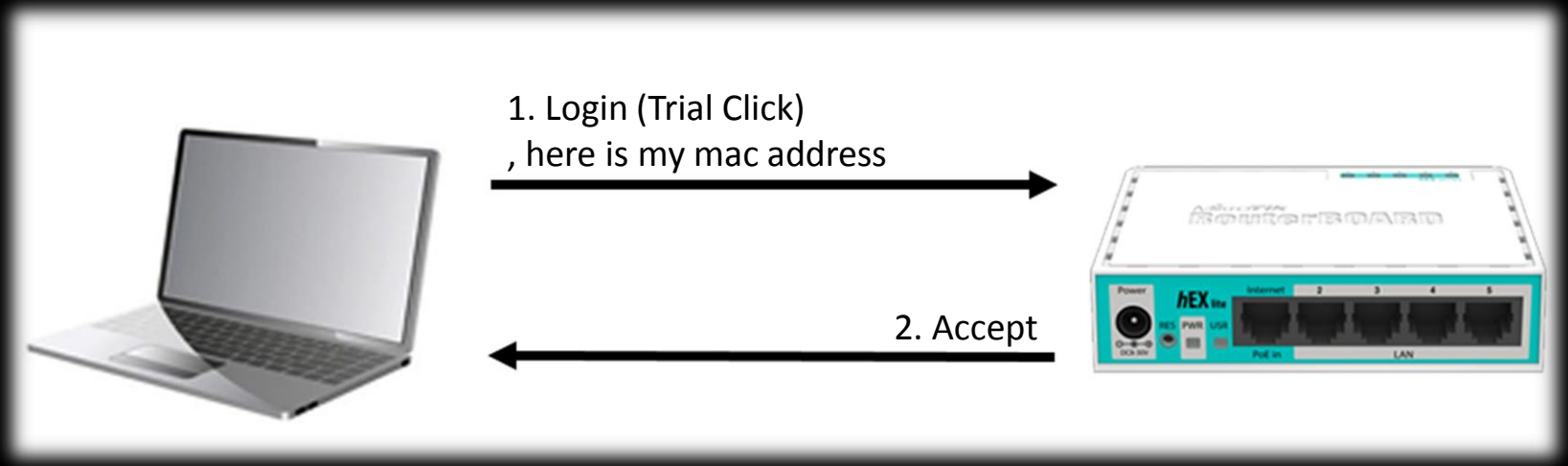
MAC Cookie (Login Again)



MAC



Trial



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?

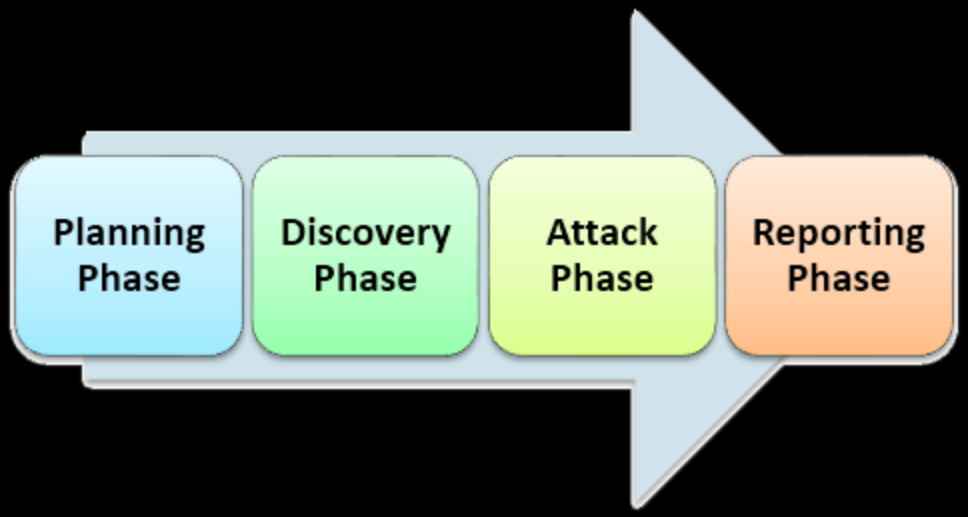
MikroTik Router & Hotspot Hardening

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/DoS_attack_protection

Common Penetration Test Step



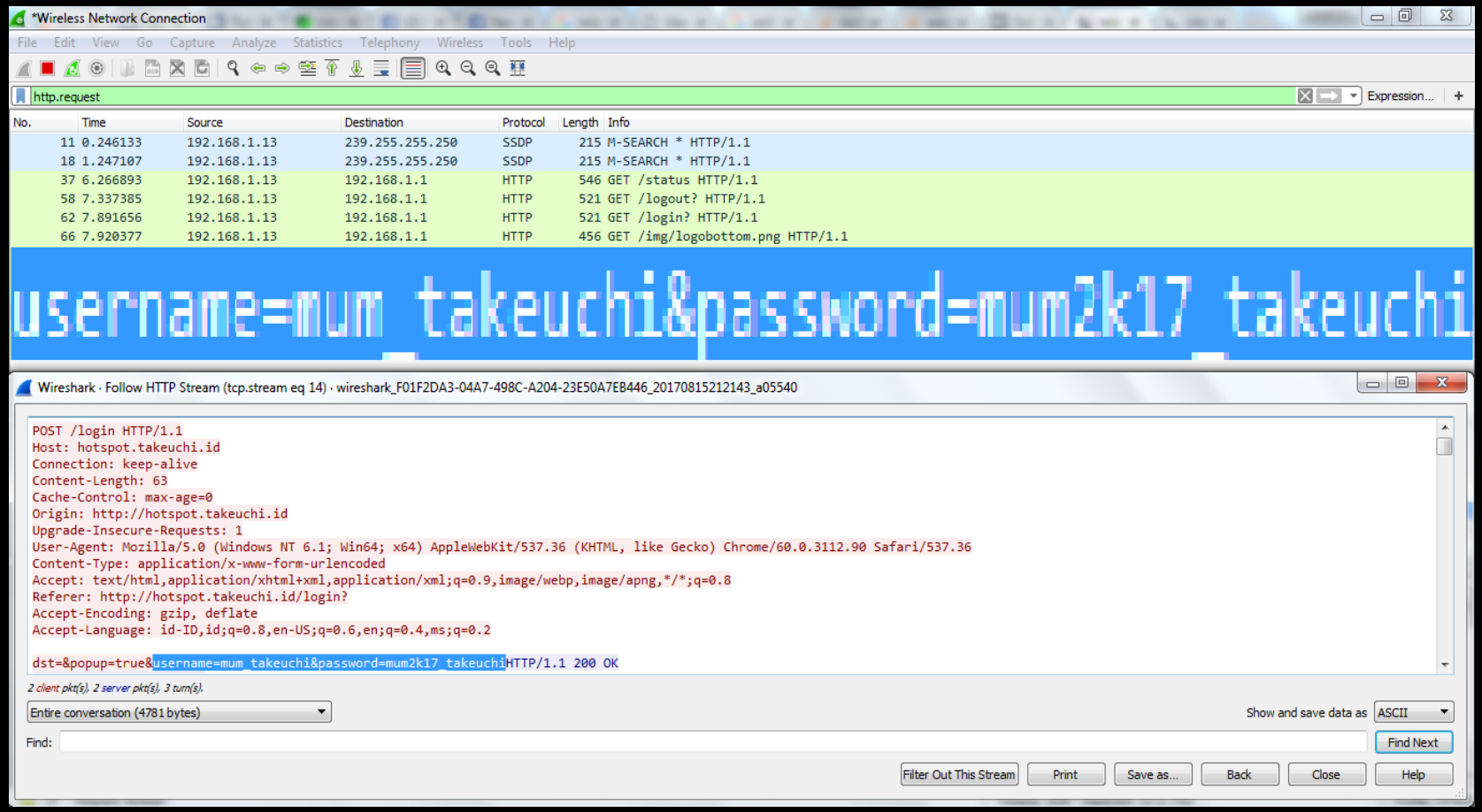
in RouterOS can be like : on the next slide

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)

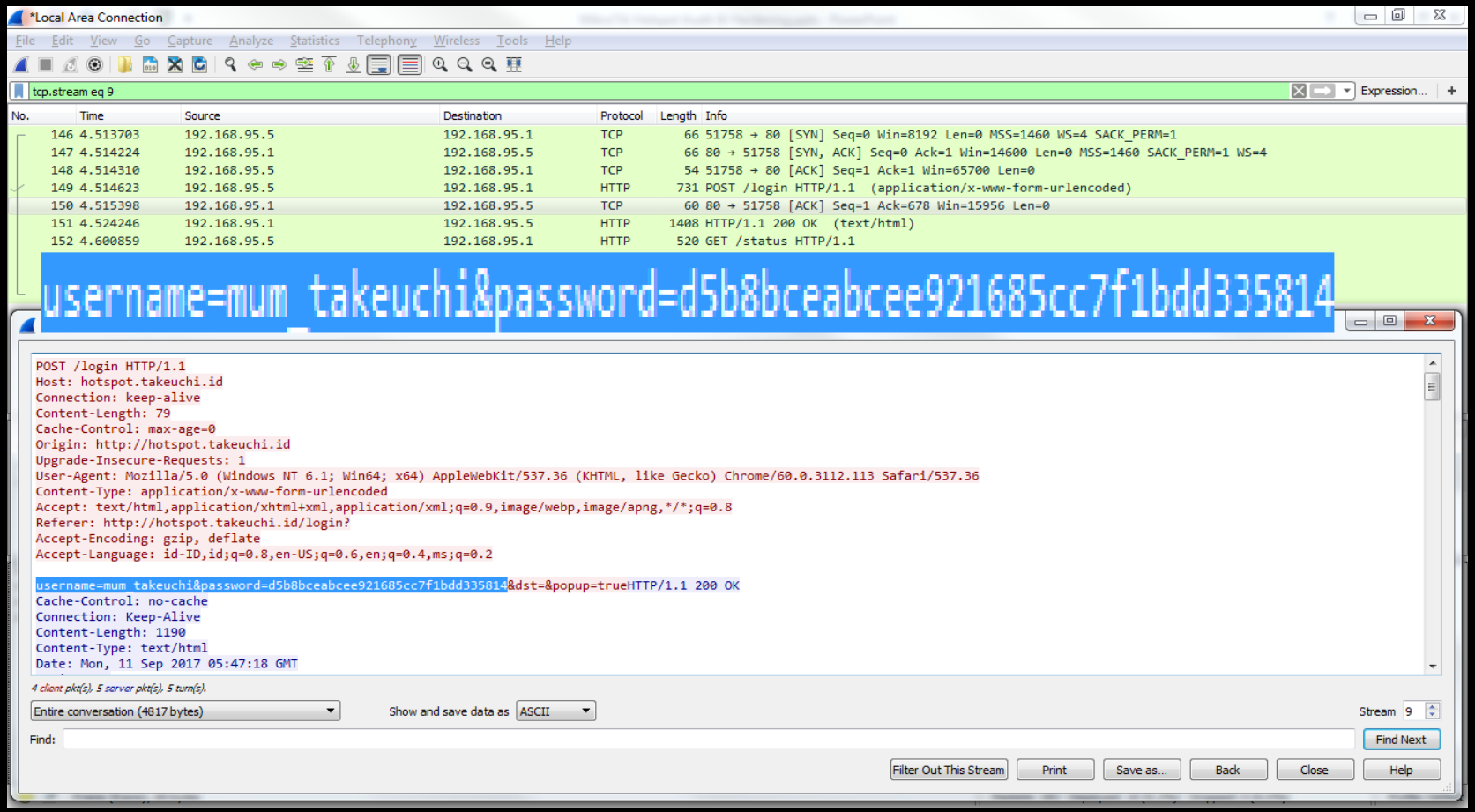
Don’t forget to make a documentation for report ☺

MikroTik Hotspot Auth. Packet (HTTP PAP)



username=**mum_takeuchi**&password=**mum2k17_takeuchi**

MikroTik Hotspot Auth. Packet (HTTP CHAP)



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

https://www.md5decrypter.com

MikroTik Hotspot Auth. Packet (HTTP CHAP)

Decrypt (search for a match):

Hash String d5b8bceabcee921685cc7f1bdd335814

Enable mass-decrypt mode

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

Decode!

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

MikroTik Hotspot Auth. Packet (HTTPS)

*Local Area Connection

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ssl

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

```
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
```

Server Name: hotspot.takeuchi.id

```
00b0  18 00 16 00 00 13 68 6f  74 73 70 6f 74 2e 74 61   ......ho tspot.ta
00c0  6b 65 75 63 68 69 2e 69  64 00 17 00 00 00 23 00   keuchi.i d.....#.
00d0  b0 a1 18 e5 39 91 7e 7a  b2 3b 40 9e 91 a4 44 64   ....9.~z .;@...Dd
00e0  44 d0 d1 bb ad 44 ea 28  36 90 fb 13 54 8e 64 47   D....D.( 6...T.dG
00f0  6f c9 c4 01 96 a2 70 da  71 f6 bf 23 05 5c 20 73   o.....p. q..#.\ s
0100  53 ec 4c 9a 7b ef e3 3a  c3 f4 b3 11 79 e3 7a 9f   S.L.{..: ....y.z.
0110  90 43 a2 04 55 9e 76 c7  cf 87 40 1b b9 12 2c cc   .C..U.v. ..@...,.
0120  9f 07 f7 c5 88 d3 e0 a0  d9 b5 5e 98 ec 02 ab 5f   ........ ..^...._
0130  19 be 0c 9b af 7f fc 6a  ad fd 27 45 d4 01 e6 fe   .......j ..'E....
0140  b6 ae e7 5f 73 52 a8 30  2b 48 ec ce 59 cb 66 86   ..._sR.0 +H..Y.f.
0150  23 6a 8a 6e 96 b5 81 c8  e3 d6 af d6 78 79 85 2c   #j.n.... ....xy.,
0160  0e 18 3f 86 70 06 fc 86  dd ce 60 a5 04 11 38 b9   ..?.p... ..`...8.
0170  9b c6 c3 1c 54 d6 36 7d  bf 1e f3 68 13 77 88 8d   ....T.6} ...h.w..
0180  87 00 0d 00 14 00 12 04  03 08 04 04 01 05 03 08   ........ ........
0190  05 05 01 08 06 06 01 02  01 00 05 00 05 01 00 00   ........ ........
01a0  00 00 00 12 00 00 00 10  00 0e 00 0c 02 68 32 08   ........ .....h2.
01b0  68 74 74 70 2f 31 2e 31  75 50 00 00 00 0b 00 02   http/1.1 uP......
01c0  01 00 00 0a 00 0a 00 08  8a 8a 00 1d 00 17 00 18   ........ ........
01d0  ca ca 00 01 00 00 15 00  62 00 00 00 00 00 00 00   ........ b.......
01e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
01f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0200  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0210  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
```

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)

*Local Area Connection

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ssl

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

```
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...
```

Encrypted Application Data:

```
0030  10 aa 6c 87 00 00 17 03  03 05 62 e8 ab 96 57 8b   ..l..... ..b...W.
0040  12 16 5f 4c 78 69 1d c3  04 b6 c1 dc 9e be c5 b5   .._Lxi.. ........
0050  28 9e 9e da ff 19 d4 9b  ef 99 53 81 84 4c 20 b9   (....... ..S..L .
0060  6b 83 9a 8a bd a6 b1 0b  cf 28 7c 2a 55 d1 33 5e   k....... .(|*U.3^
0070  cb 02 c5 4a 8a 71 03 37  70 e1 cd 0e c8 28 94 19   ...J.q.7 p....(..
0080  ab 65 95 92 75 85 22 18  7d 12 9f 8e a4 23 77 18   .e..u.". }....#w.
0090  90 b1 52 91 6c 0d 2e cf  b8 9e a6 7a 8f 6d 08 3e   ..R.l... ...z.m.>
00a0  44 ae 09 7b 91 67 0c 3f  15 25 ae 6d 67 3b 19 b6   D..{.g.? .%.mg;..
00b0  29 ad c7 2a 77 c6 37 17  fb c4 86 9c 9e 28 77 ec   )..*w.7. .....(w.
00c0  a2 a0 ac 23 c2 2c d0 42  22 fe 78 2f c4 14 28 85   ...#.,.B ".x/..(.
00d0  db d7 e4 ee ac c6 48 17  b6 8e 5d ec 05 5c e2 0d   ......H. ..]..\..
00e0  40 25 6f 1b 7a 30 e4 6f  28 f1 4c e7 a8 0f dc 6a   @%o.z0.o (.L....j
00f0  b4 a7 bf 26 fc 1d aa 93  f6 c5 8b c4 cc aa 7c dc   ...&.... ......|.
0100  4c 7e bf 75 08 6e 6a f4  ae b4 ce ee 4a 5d 46 59   L~.u.nj. ....J]FY
0110  cd d7 62 35 5d af 26 34  9f 9d 8f 0a fd 67 10 fc   ..b5].&4 .....g..
0120  fc 74 40 cf ee d9 69 6f  8b cc 37 f7 be 33 f1 30   .t@...io ..7..3.0
0130  8e 11 f6 9f a9 e7 5f da  2c c1 5f 4f 2e f3 13 ff   ......_. ,._O....
0140  7c 5a e1 b9 20 6b 91 e6  b8 ca d8 44 2c 8e 05 38   |Z.. k.. ...D,..8
0150  80 41 47 9f 1f fd c9 14  45 af 74 b6 7b c7 b9 a1   .AG..... E.t.{...
0160  1a fc d3 d8 af f5 e0 3b  69 eb 9f fd 95 be b4 2d   .......; i......-
0170  05 76 0a 24 25 7e 59 ff  a5 0f 46 2f c5 d4 35 14   .v.$%~Y. ..F/..5.
0180  54 0d 5f 12 18 19 9f 00  f1 7f 83 18 25 f7 0c 74   T._..... ....%..t
0190  7b 8c 57 15 a3 cb 95 1e  1d 71 10 cc 9e 38 93 bc   {.W..... .q...8..
```

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)

*Local Area Connection

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 10 Expression... +

No.	Time	Source	Destination	Protocol	Length	Info
89	9.711212	192.168.90.1	192.168.90.6	TCP	66	80 → 2364 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1 WS=4
90	9.711292	192.168.90.6	192.168.90.1	TCP	54	2364 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
91	9.712469	192.168.90.6	192.168.90.1	HTTP	522	GET /logout? HTTP/1.1
92	9.713128	192.168.90.1	192.168.90.6	TCP	60	80 → 2364 [ACK] Seq=1 Ack=469 Win=15672 Len=0
93	9.722414	192.168.90.1	192.168.90.6	TCP	1514	[TCP segment of a reassembled PDU]
94	9.724212	192.168.90.1	192.168.90.6	HTTP	503	HTTP/1.1 200 OK (text/html)
95	9.724284	192.168.90.6	192.168.90.1	TCP	54	2364 → 80 [ACK] Seq=469 Ack=1910 Win=65700 Len=0
114	11.974920	192.168.90.6	192.168.90.1	HTTP	550	GET /login? HTTP/1.1
115	11.987166	192.168.90.1	192.168.90.6	HTTP	1492	HTTP/1.1 200 OK (text/html)

```
Frame 114: 550 bytes on wire (4400 bits), 550 bytes captured (4400 bits) on interface 0
Ethernet II, Src: AsustekC_36:f3:f0 (2c:56:dc:36:f3:f0), Dst: Routerbo_e7:37:b1 (6c:3b:6b:e7:37:b1)
Internet Protocol Version 4, Src: 192.168.90.6, Dst: 192.168.90.1
Transmission Control Protocol, Src Port: 2364, Dst Port: 80, Seq: 469, Ack: 1910, Len: 496
Hypertext Transfer Protocol
```

Wireshark · Follow HTTP Stream (tcp.stream eq 10) · wireshark_40D0D99B-B38D-49F7-98A1-B9EB03DF2AB9_20171010215206_a02188

```
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
```

3 client pkt(s), 3 server pkt(s), 5 turn(s).

Entire conversation (7090 bytes) Show and save data as ASCII

Find: Find Next

Filter Out This Stream Print Save as... Back Close Help

Cookie: loginID=**3356857343**

MikroTik Hotspot Auth. Packet (Trial)

*Local Area Connection

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

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)

```
▷ 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: 192.168.90.3, Dst: 192.168.90.1
▷ 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]
```

```
0030  40 29 b6 97 00 00 47 45  54 20 2f 6c 6f 67 69 6e   @)....GE T /login
0040  3f 64 73 74 3d 26 75 73  65 72 6e 61 6d 65 3d 54   ?dst=&us ername=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 54   DE%3ADA% 3A67 HTT
0070  50 2f 31 2e 31 0d 0a 48  6f 73 74 3a 20 68 6f 74   P/1.1..H ost: hot
0080  73 70 6f 74 2e 74 61 6b  65 75 63 68 69 2e 69 64   spot.tak euchi.id
```

Expert Info (_ws.expert) | Packets: 173 · Displayed: 4 (2.3%) | Profile: Default

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 ≠ 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:IP/Hotspot
- 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/Challenge-Handshake_Authentication_Protocol
- 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

http://www.facebook.com/mict404

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

Any Questions?