ACCESS ROUTEROS USING MULTI-FACTOR AUTHENTICATION

MIKROTIK USER MEETING 2018
About Me

Didiet Kusumadihardja

- 12 tahun pengalaman di IT
  RT/RW Net, Startup (e-commerce), Manage Service, IT Consulting, IT Auditor, Penetration Tester & Training Service
- Penguji UKK TKJ
- Mikrotik Certified Trainer
- Mikrotik Certified Consultant

https://about.me/didiet
Services Offered

1. Network Assessment/Design Service
2. IT General Control Audit Service
3. Vulnerability Assessment & Penetration Testing Service
4. IT Due Diligence Service
5. Training Service

- UU ITE No 11 Tahun 2008
- POJK 38/POJK.03/2016
- SEOJK 21/SEOJK.03/2017
- PBI 16/8/PBI/2014
- PCI DSS
- ISO 27001
Background
The newly disclosed 2013 attack involved sensitive user information, including names, telephone numbers, dates of birth, encrypted passwords and unencrypted security questions that could be used to reset a password. Yahoo said it is forcing all of the affected users to change their passwords and it is invalidating unencrypted security questions — steps that it declined to take in September.
Yahoo says all three billion accounts hacked in 2013 data theft

Jonathan Stempel, Jim Finkle

(Reuters) - Yahoo on Tuesday said that all 3 billion of its accounts were hacked in a 2013 data theft, tripling its earlier estimate of the size of the largest breach in history, in a disclosure that attorneys said sharply increased the legal exposure of its new owner, Verizon Communications Inc (VZ.N).
The Hacker News

Hackers Infect Over 200,000 MikroTik Routers With Crypto Mining Malware

📅 August 02, 2018  ⌚ Mohit Kumar

In all, the malware campaigns have compromised more than 210,000 routers from Latvian network hardware provider Mikrotik across the world, with the number still increasing as of writing.
MikroTik Security Fixed

- **6.38.5 (9 Maret 2017)**
  www - fixed http server vulnerability

- **6.41.3 (8 Maret 2018)**
  smb - fixed buffer overflow vulnerability, everyone using this feature is urged to upgrade

- **6.42.1 (23 April 2018)**
  winbox - fixed vulnerability that allowed to gain access to an unsecured router

- **6.42.7 (17 Agustus 2018)**
Exploits

Mikrotik RouterOS Bruteforce Tool 1.0.2

NAME
RouterOS - Password bruteforce for MikroTik devices or boxes running RouterOS

USAGE

OPTIONS
-t, --target RouterOS target
-p, --port RouterOS port (default 8728)
-u, --user User name (default admin)
-h, --help This help
-d, --dictionary Password dictionary
-s, --seconds Delay seconds between retry attempts (default 1)
-q, --quiet Quiet mode
Amount of Time to Crack Passwords

- "abcdefg" 7 characters: 0.29 milliseconds
- "abcdefgh" 8 characters: 5 hours
- "abcdefghi" 9 characters: 5 days
- "abcdefghij" 10 characters: 4 months
- "abcdefghijkl" 11 characters: 1 decade
- "abcdefghijklm" 12 characters: 2 centuries
25-GPU cluster cracks every standard Windows password in <6 hours

All your passwords are belong to us.

DAN GOODMAN - 12/10/2012, 7:00 AM
Dictionary Attack
Brute Force Attack
Exploits
Password Dictionary
Bad Guys
Humans and Password

Why humans are terrible at picking their own passwords

Memory was never the strongest suit of our species, so we too often make the password too obvious or simply pick one password we use across all platforms.
Password Tips

Password Tips

1. Don’t rely on passwords alone to protect anything you value. **Turn on multi-factor authentication wherever possible.**

2. Use a phrase with multiple words that you can picture in your head, so it’s difficult to guess but easy to remember.

3. Protect your most important accounts, like banking and primary email, by giving each a **unique passphrase**. A password manager can help.

Password: `sunwalkraindrive`

Password: `**********`
(2) Mekanisme yang digunakan oleh Penyelenggara Tanda Tangan Elektronik untuk pembuktian identitas Penanda Tangan secara elektronik wajib menerapkan kombinasi paling sedikit 2 (dua) faktor autentikasi.
How we do it with RouterOS?
Multi-Factor Authentication on RouterOS

- Something you know → Password
- Something you have → SSH Keys
- Somewhere you from → IP Address
Create SSH Public & Private Key

1. Generate
2. Save Private Key
3. Copy Public Key and save to file

For OS X and Linux users can use ‘ssh-keygen’
RouterOS Configuration

1. Upload Public Key

2. Create New User

3. Import SSH Key
Login using SSH Keys

1. Connection > SSH > Auth

2. PuTTY Configuration:
   - Private key file for authentication: C:\Users\Didiet KDesktop\id_rsa
   - Input passphrase for key "Didiet".

PuTTY session:
- login as: test
- Authenticating with public key "Didiet"
- Input passphrase for key "Didiet".

MikroTik RouterOS 6.42.1 (c) 1999-2018 http://www.mikrotik.com/
- command [?] Gives the list of available commands
- command [Tab] Completes the command/word. If the input is ambiguous, a second [Tab] gives possible options
- command Move up to base level
- command Use command at the base level

Didiet Kusumadihardja | didiet@arch.web.id
Only permit from specific IP address
Other Methods (1/3)

Port Knocking

https://wiki.mikrotik.com/wiki/Port_Knocking
Other Methods (2/3)

VPN then remote access

1. VPN (PPTP/SSTP/OpenVPN)

2. Remote Access (Winbox/SSH)
Other Methods (3/3)

Out of Band Network

Management Network
UNDANG-UNDANG REPUBLIK INDONESIA
NOMOR 11 TAHUN 2008
TENTANG
INFORMASI DAN TRANSAKSI ELEKTRONIK

BAB III
INFORMASI, DOKUMEN, DAN TANDA TANGAN ELEKTRONIK

Pasal 5

(1) Informasi Elektronik dan/atau Dokumen Elektronik
dan/atau hasil cetaknya merupakan alat bukti hukum yang
sah.
Audit Trail / Log using The Dude
A network administrator plays a vital role in an organization’s cybersecurity as they are the first line of defense against a cyber-attack.

Defense in Depth Layers
1. Policies, Procedure, and Awareness
2. Physical
3. Perimeter
4. Internal Network
5. Host
6. Application
7. Data
Reference


Dijinkan menggunakan sebagian atau seluruh materi pada modul ini, baik berupa ide, foto, tulisan, konfigurasi dan diagram selama untuk kepentingan pengajaran, dan memberikan kredit kepada penulis serta link ke www.arch.web.id

Didiet Kusumadihardja
Mobile: +62 813 1115 0054
e-mail: didiet@arch.web.id