

ACCESS ROUTEROS USING MULTI-FACTOR AUTHENTICATION

MIKROTIK USER MEETING 2018



Didiet Kusumadihardja | didiet@arch.web.id
Yogyakarta, Indonesia | 20 Oktober 2018

About Me

2

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



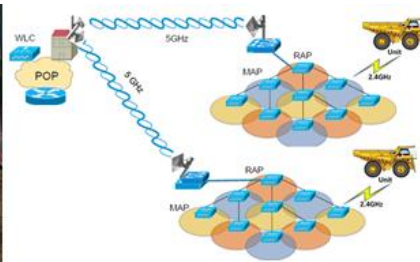
<https://about.me/didiet>



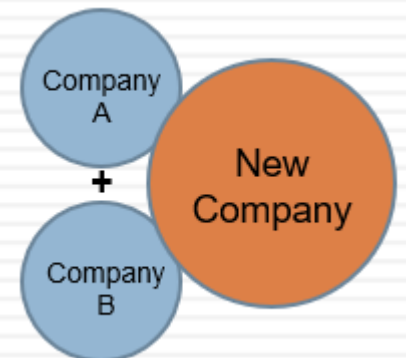
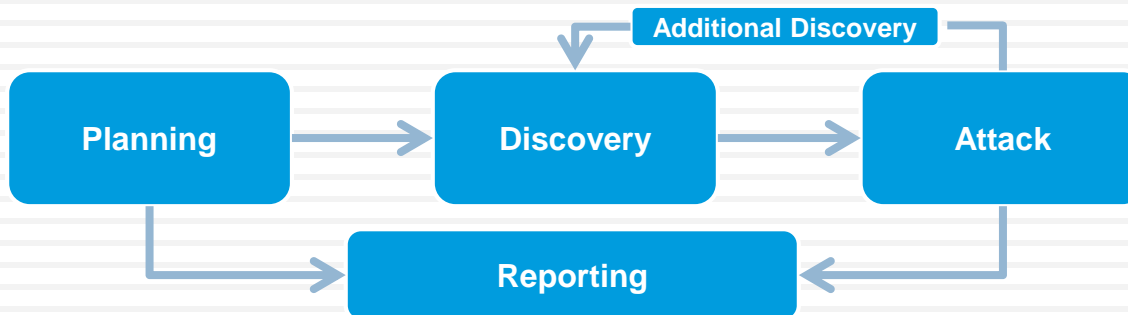
Services Offered

3

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



4

Background



Data Breaches News 2016

5

The New York Times

By Vindu Goel and Nicole Perlroth

Dec. 14, 2016

Yahoo Says 1 Billion User Accounts Were Hacked

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.

Data Breaches News 2017

6



REUTERS

OCTOBER 4, 2017 / 3:57 AM / A YEAR AGO

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](#)).

Data Breaches News 2018

7

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

8

- **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)**
security - fixed vulnerabilities CVE-2018-1156, CVE-2018-1157, CVE-2018-1158, CVE-2018-1159

Exploits

9

```
Shell - Konsole

Mikrotik RouterOS Bruteforce Tool 1.0.2

NAME [redacted] - Password bruteforcer for MikroTik devices or boxes running RouterOS

USAGE
python [redacted] [-t] [-p] [-u] [-d] [-s] [-q]

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

10

"abcdefg" 7 characters	 .29 milliseconds
"abcdefgh" 8 characters	 5 hours
"abcdefghi" 9 characters	 5 days
"abcdefghij" 10 characters	 4 months
"abcdefghijk" 11 characters	 1 decade
"abcdefghijkl" 12 characters	 2 centuries

 Better Buys

Processing Power vs Passwords

11

25-GPU cluster cracks every standard Windows password in <6 hours

All your passwords are belong to us.

DAN GOODIN - 12/10/2012, 7:00 AM



Jeremi Gosney

Reality

12

1ST PASSWORDS
TAKEN FROM PERFECT PASSWORD SELECTING PROTECTION AUTHENTICITY

WWE	AUSTIN	NASCAR	SEXSEX	JULIUS	WHITE	DAVE	MADISON	RACING
6969	WILLIAM	JACKSON	BARBARE	THX1138	TOP GUN	EAGLE1	987654	5555
MUSTANG	DANIEL	CAMERON	666666	PORNO	1111	00000	BRAZIL	EAGLE
letmein	GOLFER	654321	WELCOME	BADBOY	MOTHER	DOLPHIN	LAUREN	HENTAI
baseball	HEATHER	COMPUTER	CHRIS	DEBBIE	NATHAN	CHEVY	JAPAN	NEWYORK
master	HAMMER	AMANDA	PANTHER	SPIDER	SUPER	WINSTON	NAKED	LITTLE
Michael	YANKEES	WILLARD	YAMAHA	MELISSA	GAZWSX	STEVE	SQUIRT	REDWINGS
FOOTBALL	JOSHUA	xxxxxxx	JUSTIN	BOOGIE	MAGIC	FOREVER	STARS	SMITH
SHADOW	MAGGIE	ROSEY	BABY	1212	LAKERS	ANGELA	APPLE	STICKY
MONKEY	BIGDADDY	PACER	DRIVER	FLYERS	RACHEL	IPER	ALEXIS	COCACOLA
ABC123	ENTER	BAILEY	ANGELS	FISH	SLAYER	OUIS2	AAAA	animal
PASS	THUNDER	Knight	FISHING	PORN	SCOTT	JAKE	2XCVBNM	BRONCOS
COWBOY	TIGERS	DAVID	MADDOG	MATRIX	2222	LOVERS	NIPPLES	PRIVATE
6969	SILVER	PURPLE	HOTTERS	TEENS	ASDF	SUCKIT	PEACHES	SKIPPY
JORDAN	RICHARD	WILSON	SCOOBY	VIDEO	GREGORY	VICTORIA	JASMINE	MARVIN
HARLEY	DAKOTA	HORN	BUTTER	JASON	BUDDY	ASDFGH	KEVIN	BLONDES
RANGER	ORANGE	DEANUS	PLAYER	WALTER	7777	WHATEVER	MATT	ENJOY
Iwantu	MERLIN	CAPTAIN	SUBARU	BOSTON	MARLBORO	YOUNG	QWERTYUI	GIRL
JENNIFER	MICHELLE	STARWARS	bigdick	BRVES	INTERNET	NICHOLAS	DANIELLE	APOLLO
HUNTER	CORVETTE	BOONER	Chester	YANKEE	ACTION	LUCKY	BEAVER	PARKER
FUCK	BIGDOG	COWBOYS	Smokey	LOVER	CARTER	HELPME	4321	QWERT
2000	CHEESE	EDWARD	Xavier	BARNEY	JASTER	JACKIE	403	SWIMMING
TEST	MATTHEW	GIRLS	STEVEN	VICTOR	MONSTER	MIDNIGHT	RUNNER	TIME
BATMAN	PATRICK	COFFEE	VIKING	TUCKER	TERESA </td <td>EROTIC</td> <td>SWIMMING</td> <td>SYDNEY</td>	EROTIC	SWIMMING	SYDNEY
THOMAS	FREEDOM	building	BLUE	PRINCESS	TEREY	COLLEGE	DOLPHIN	WOMEN
TIGGER	GINGER	NECITOT	EAGLES	MERCEDES	111111	BABY	GORDON	VOODOO
ROBERT	NICOLE	PERNUT	WINNER	5150	BILL	BRIAN	CASPER	JUICE
ACCESS	SPARKY	JOHN	HOUSE	DOGGIE	CRYSTAL	MARK	STUPID	MAGNUM
LOVE	YELLOW	GARDOLF	FLOWER	222222	PETER	STARTRK	DIRTY	777777
1-2-3-4-5	6-7-8-9-0	1-2-3-4-5	6-7-8-9-0	GUNNER	SIERRA	ACCESS	WOLF	DREAMS
				HORNEY	LEATHER	3333	APPLES	MAXWELL
					232323	...	AUGUST	RUSH2112
							AMANDA	

Password Dictionary



Exploits



Bad Guys

Humans and Password

13

The Daily Dot

Why humans are terrible at picking their own passwords

Gillian Branstetter — Jan 23, 2015 at 8:30PM | Last updated Dec 11 at 12:09PM

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

14

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.



Password: **sunwalkraindrive**

3

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



Indonesia Regulation

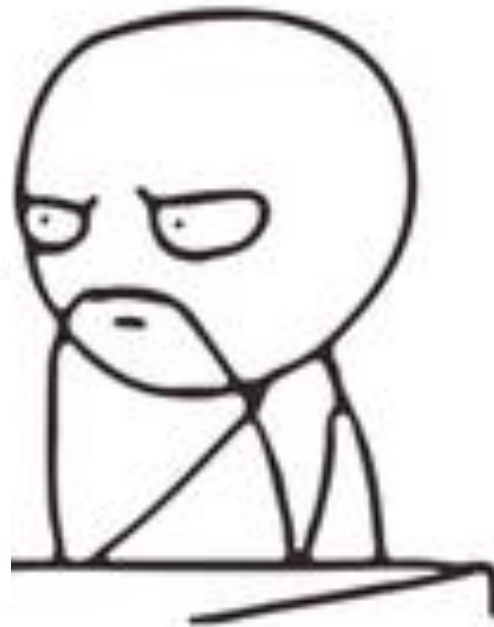
15

PERATURAN PEMERINTAH REPUBLIK INDONESIA
NOMOR 82 TAHUN 2012
TENTANG
PENYELENGGARAAN SISTEM DAN TRANSAKSI ELEKTRONIK

- (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.

16

How we do it with RouterOS?



Multi-Factor Authentication on RouterOS

17



- Something you know → Password
- Something you have → SSH Keys
- Somewhere you from → IP Address

Create SSH Public & Private Key

18

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

For OS X and Linux users can use
'ssh-keygen'

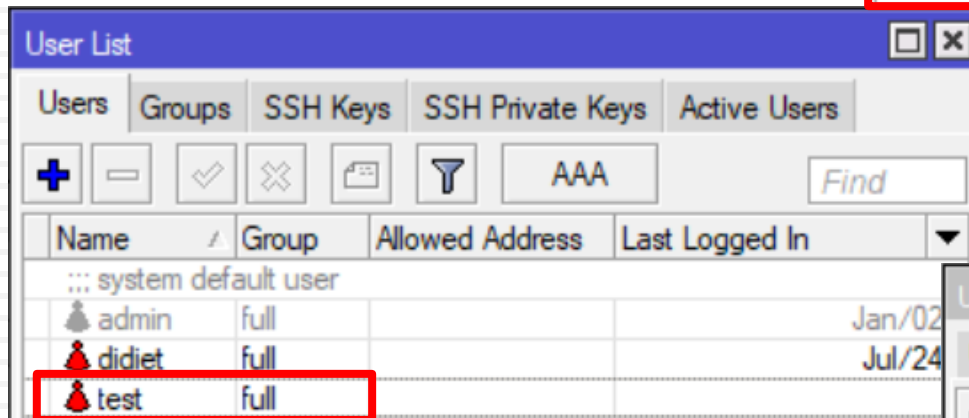
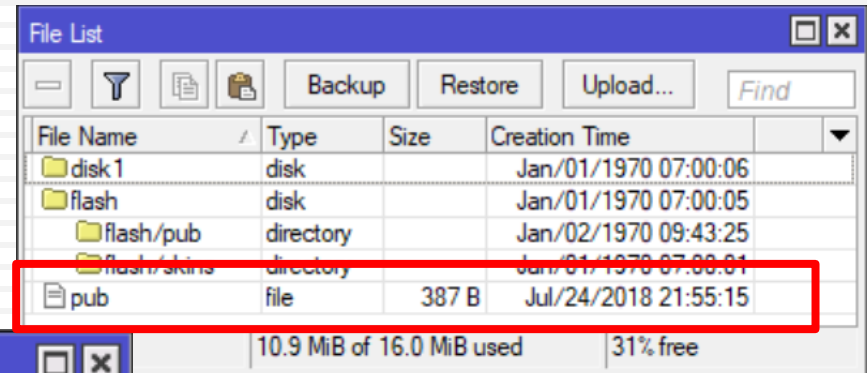
The screenshot shows the PuTTY Key Generator window with the following elements:

- Key section:** A text box containing the public key, highlighted with a red box and a circled '3'. The text is: `ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEA...`
- Key fingerprint:** A text box showing the fingerprint: `ssh-rsa 2048 0f:27:d2:18:b6:21:aa:21:08:46:58:9c:80:b4:43:bc`
- Key comment:** A text box containing the comment: `Didiet`
- Key passphrase:** A text box with masked characters (dots).
- Confirm passphrase:** A text box with masked characters (dots).
- Actions section:** Three buttons: **Generate** (circled with a red '1'), **Load**, and **Save private key** (circled with a red '2').
- Parameters section:** Radio buttons for **Type of key to generate:** ☒ RSA, ☐ DSA, ☐ ECDSA, ☐ ED25519, ☐ SSH-1 (RSA). A text box for **Number of bits in a generated key:** with the value `2048`.

RouterOS Configuration

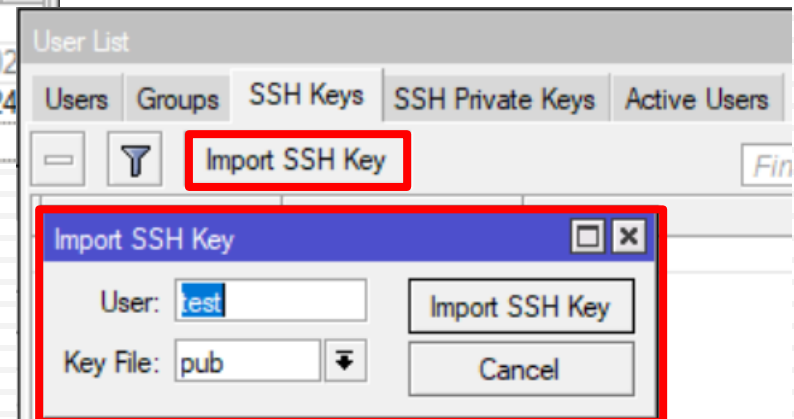
19

1. Upload Public Key



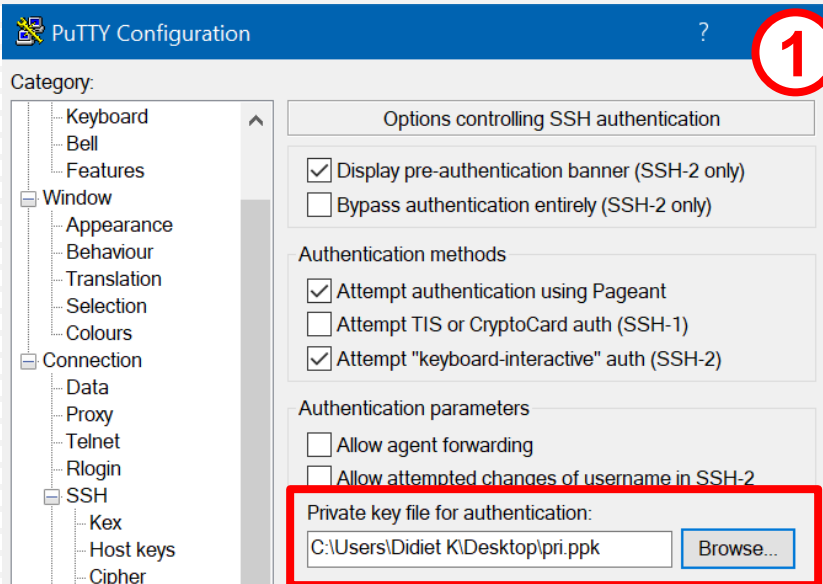
2. Create New User

3. Import SSH Key

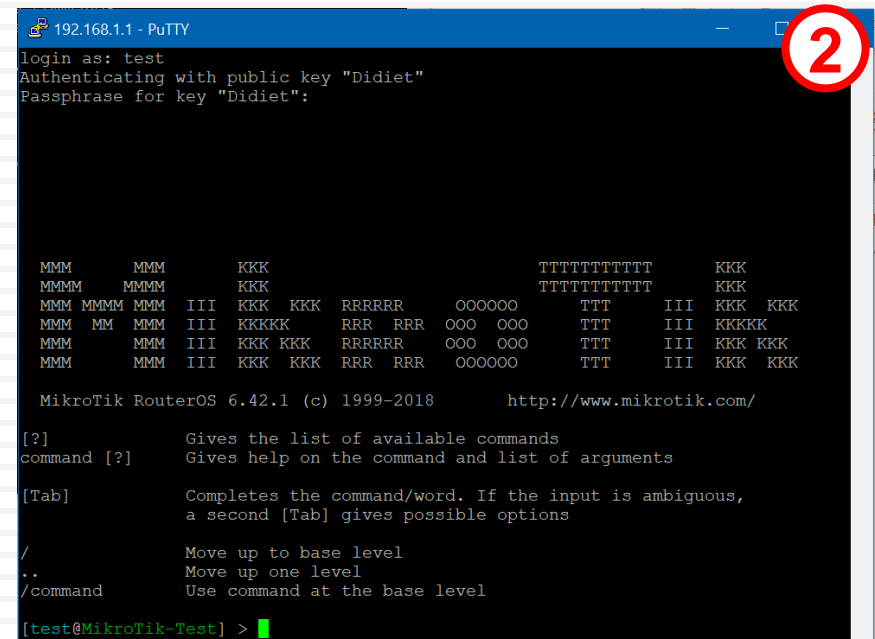


Login using SSH Keys

20

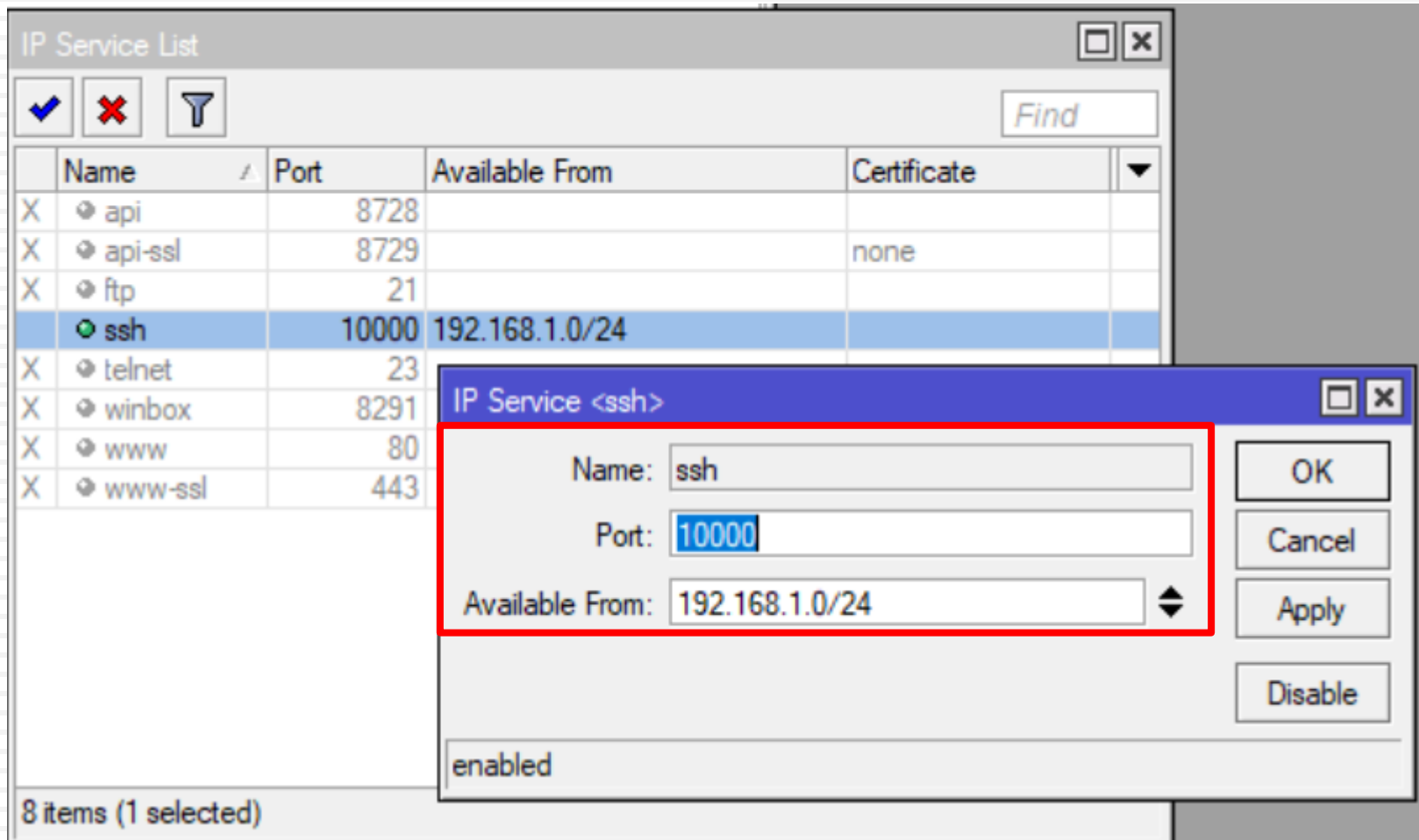


Connection > SSH > Auth



Only permit from specific IP address

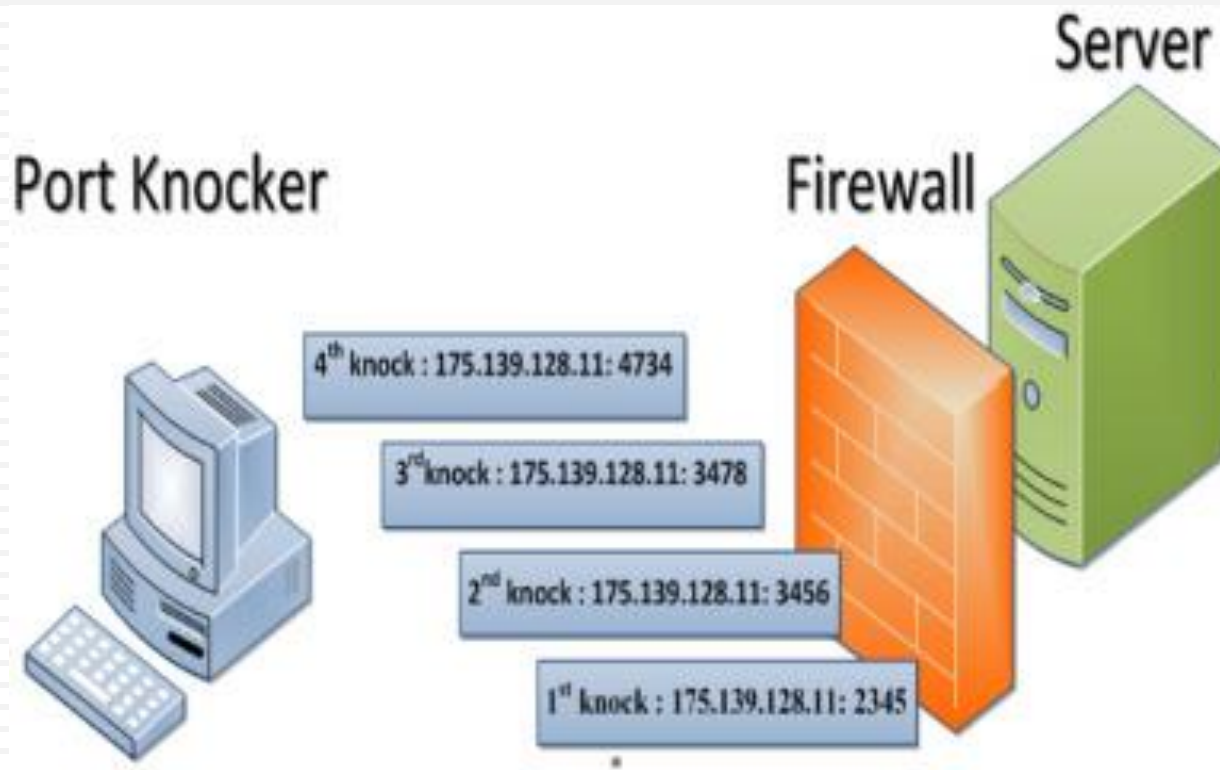
21



Other Methods (1/3)

22

Port Knocking



https://wiki.mikrotik.com/wiki/Port_Knocking

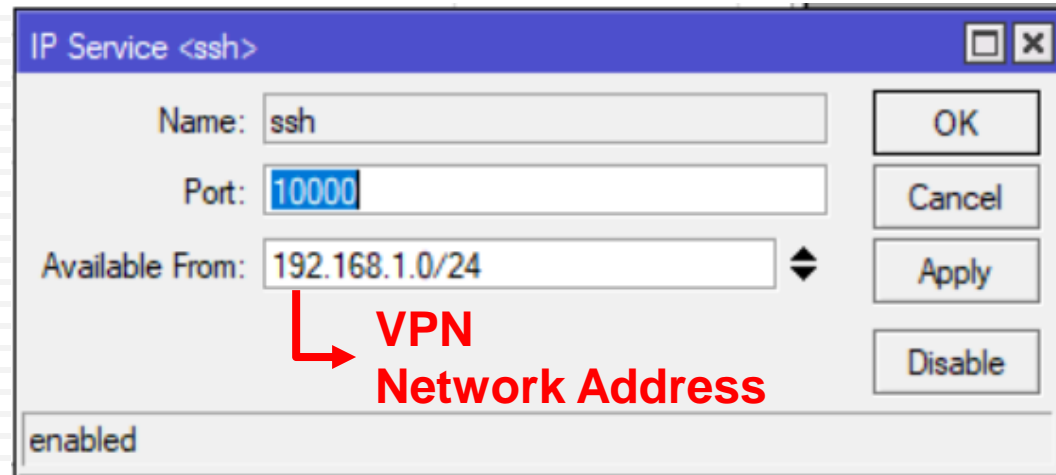
Other Methods (2/3)

23

VPN then remote access

1. VPN (~~PPTP~~/SSTP/OpenVPN)

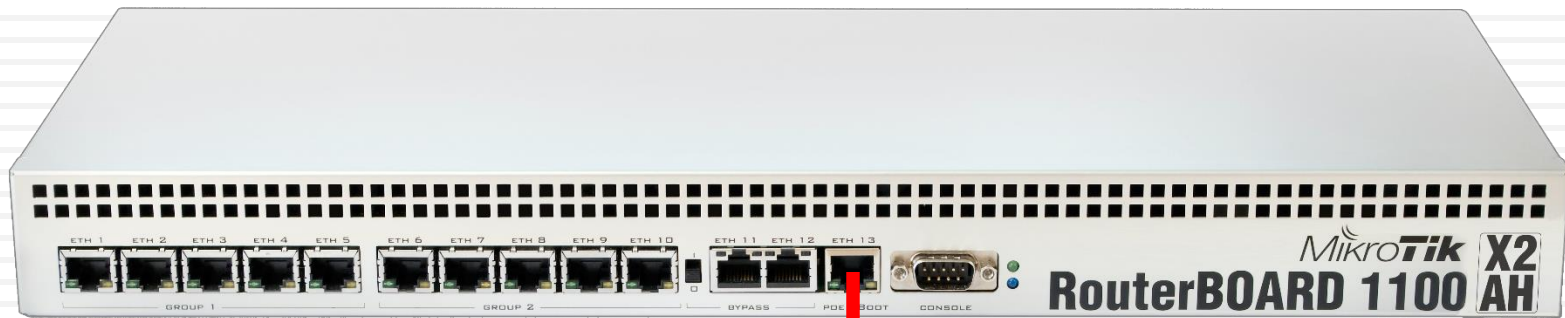
2. Remote Access (Winbox/SSH)



Other Methods (3/3)

24

Out of Band Network



Management Network

Audit Trail / Log as Evidence

25

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

26

The screenshot displays the The Dude 6.34rc15 interface. The left sidebar shows a tree view of the application's contents, with 'Logs' selected. The main window shows a table of Syslog events. A 'Syslog - Log Settings' dialog box is open, showing the 'Files' tab with settings for 'Name', 'Start New File', 'Files To Keep', and 'Buffered Entries'.

admin@172.16.0.254 - The Dude 6.34rc15

Preferences Help

Settings

Contents

- Address Lists
 - blacklist
- Admins
- Agents
- Charts
 - Gateway-resourc...
 - WAN-activity Chart
 - Wan-activity Chart
- Devices
- Files
- Functions
- History Actions
- Links
- Logs**
 - Action
 - Debug
 - Event
 - Syslog
- Mib Nodes
- Network Maps
 - Local
 - Networks
 - Notifications
- Panels
 - OneForTest
 - Panel
 - admin 172.16.0.20
 - krisjanis 172.16.0...
- Probes
- Services
- Tools

Syslog

Time	Address	Event
21:06:25	172.16.0.254	Service ssh on 172.16.0.254 is now down (timeout)
21:24:46	172.16.0.18	Service ping on TV is now down (failed)

Syslog - Log Settings

General Files

Name: Syslog

Start New File: never

Files To Keep: 10

Buffered Entries: 1000

Ok Cancel Apply Notes Copy Remove

Summary

27



EC-COUNCIL @ECCOUNCIL · Aug 30

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

28

- ArsTechnica. 2012. 25-GPU cluster cracks every standard Windows password in <6 hours. <https://arstechnica.com/information-technology/2012/12/25-gpu-cluster-cracks-every-standard-windows-password-in-6-hours/>.
- BetterBuys. Estimating Password-Cracking Times. <https://www.betterbuys.com/estimating-password-cracking-times/>.
- C# Corner. 2015. Passphrase vs Password For Security. <https://www.c-sharpcorner.com/UploadFile/66489a/passphrase-vs-password-for-the-security/>.
- Information is beautiful. 2018. World's Biggest Data Breaches. <http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>.
- MikroTik. 2015. Port Knocking. https://wiki.mikrotik.com/wiki/Port_Knocking.
- MikroTik. 2016. Manual: The Dude v6/Syslog. https://wiki.mikrotik.com/wiki/Manual:The_Dude_v6/Syslog.
- NIST. 2017. Easy Ways to Build a Better P@\$5w0rd. <https://www.nist.gov/blogs/taking-measure/easy-ways-build-better-p5w0rd>.
- Records Management Center. 2017. Identity Theft – Is It All Digital. <https://rmcmaine.com/identity-theft-report/>.
- Reuters. 2017. Yahoo says all three billion accounts hacked in 2013 data theft. <https://www.reuters.com/article/us-yahoo-cyber/yahoo-says-all-three-billion-accounts-hacked-in-2013-data-theft-idUSKCN1C82O1>.
- ScienceDirect. 2017. Towards port-knocking authentication methods for mobile cloud computing. <https://www.sciencedirect.com/science/article/pii/S1084804517302813> (Accessed 2018-09-04).
- The Hacker News. 2018. Hackers Infect Over 200,000 MikroTik Routers With Crypto Mining Malware. <https://thehackernews.com/2018/08/mikrotik-router-hacking.html>.
- The New York Times. 2016. Yahoo Says 1 Billion User Accounts Were Hacked. <https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html>.



Didiet Kusumadihardja

Mobile: +62 813 1115 0054

e-mail: didiet@arch.web.id

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