

# ACCESS ROUTEROS USING MULTI-FACTOR AUTHENTICATION

MIKROTIK USER MEETING 2018



Didiet Kusumadihardja | [didiet@arch.web.id](mailto: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



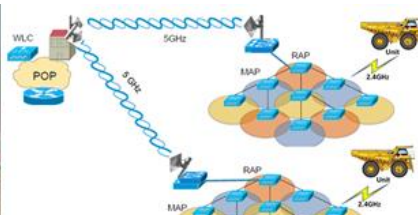
<https://about.me/didiet>



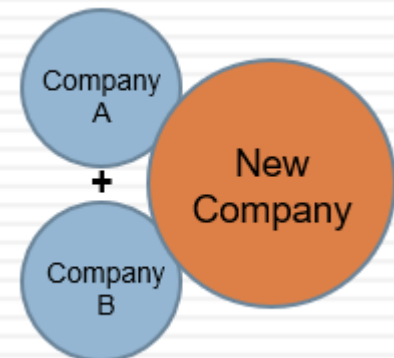
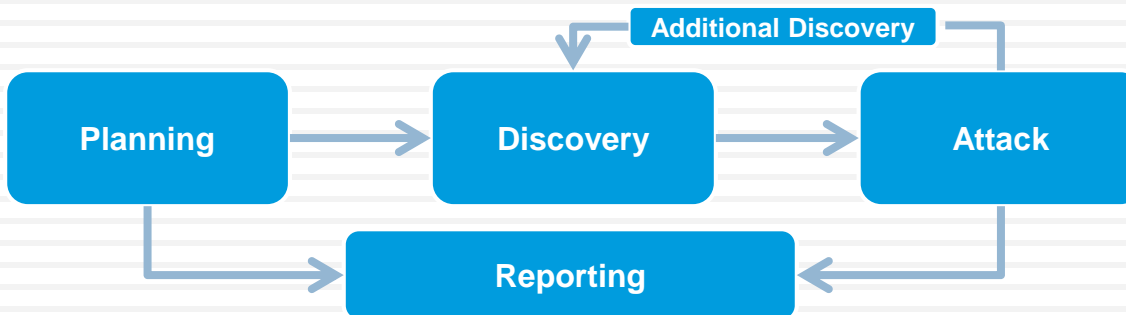
# Services Offered

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 Perloth**

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
"abcdefghijkl" 11 characters	 1 decade
"abcdefghijkl" 12 characters	 2 centuries



# 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

**ST PASSWORDS** TAKE N FROM PERFECT PASSWORD SELECTION PROTECTION, RUMORHASIT

WWE	AUSTIN	NASCAR	SEXSEX	JULIUS	WHITE	DAVE	10011	MADISON	RACING
6969	WILLIAM	JACKSON	hardcore	THX1138	TOP GUN	EAGLE1	PACKERS	987654	5555
mustang	DAVID	AMERICA	666666	PORNO	III	IIII	EINSTEIN	BRAZIL	EAGLE
letmein	GOLFER	654321	WILLIE	BABY	MOTHER	NATHAN	DOLPHINS	LAUREN	HENTAI
baseball	HEATHER	COMPUTER	WELCOME	DEBBIE	CHRIS	PANTHER	WARRIOR	JAPAN	NEWYORK
master	HAMMER	AMANDA	CHRIS	SPIDER	PANTHER	YANAHHA	WARRIOR	NAKED	LITTLE
michael	YANKEES	WILLARD	YANAHHA	SUPER	RAIDERS	STEVE	WARRIOR	SQUIRT	REDWINGS
FOOTBALL	JOSHUA	XXXXXXX	JUSTIN	GA ZWSX	MELISSA	MAGIC	FOREVER	STARS	SMITH
SHADOW	MAGGIE	PHENIX	BARBARA	BOOGER	1212	LAKERS	ANGELA	APPLE	STICKY
MONKEY	BHEME	MIKEY	DRIVER	FLYERS	RACHEL	SLAYER	IPER	875309	ALEXIS
ABC123	ENTER	BAILEY	ANGELS	FISH	SCOTT	JAKE	2XCUBUM	AAA	BONNIE
PASS	THUNDER	Knight	FISHING	PORN	MATRIX	LOVERS	POWEE	PEACHES	PRIVATE
6969	SILVER	PEOPLE	HOTERS	TEENS	ASDF	SUCKIT	GREGORY	VICTORIA	JASMINE
JORDAN	RICHARD	HORN	BUTHEAD	JASON	VIDEO	BUDDY	LOANON	ASDFGH	KEVIN
HARLEY	DAKOTA	DEANUS	WALTER	7777	WHATEVER	YOUNG	TOYOTA	TRAVIS	MATT
RANGER	ORANGE	PLAYER	BOSTON	MARLBORO	7777	WHATEVER	YOUNG	TRAVIS	ENJOY
Iwantu	MERLIN	PHASAD	CAPTAIN	BRAVES	INTERNET	LUCKY	HOTDOG	4321	DANIELLE
JENNIFER	MICHELLE	STARWARS	bigdick	YANKEE	ACTION	HELPME	ROCK	403	BEAVER
HUNTER	BIGDOG	Cowboys	Smokey	LOVER	JASPER	JACKIE	X XXX	RUNNER	PARKER
FUCK	CHEESE	EDWARD	Xavier	BARNEY	CARTER	MONSTER	MONICA	EXTREME	SWIMMING
2000	MATTHEW	GIRLS	STEVEN	VICTOR	TERESA	COLLEGE	EROTIC	DOLPHIN	TIME
TEST	1212	COFFEE	Viking	TUCKER	JEREMY	BABY	DIRTY	GORDON	SYDNEY
BATMAN	MARTIN	XXXXXX	Snoopy	PRINCESS	ILLIINI	BILL	BRIAN	ARSENAL	WOMEN
TRUSTNO	FREEDOM	bulldog	BLUE	MERCEDES	5150	DOGIE	CRYSTAL	MARK	CASPER
THOMAS	GINGER	PERMIT	JOHN	WINNER	SAMANTHA	ROBERT	NICOLE	JOHN	STUPID
TIGGER	ACCESS	SPARKY	JANNY	FLOWER	JACK	LOVE	YELLOW	GARDOLF	SHIT
1-1111	1-1111	1-1111	1-1111	1-1111	1-1111	1-1111	1-1111	1-1111	1-1111

## Password Dictionary



Dictionary Attack



Brute Force Attack



Bad Guys

## Exploits

# 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:

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

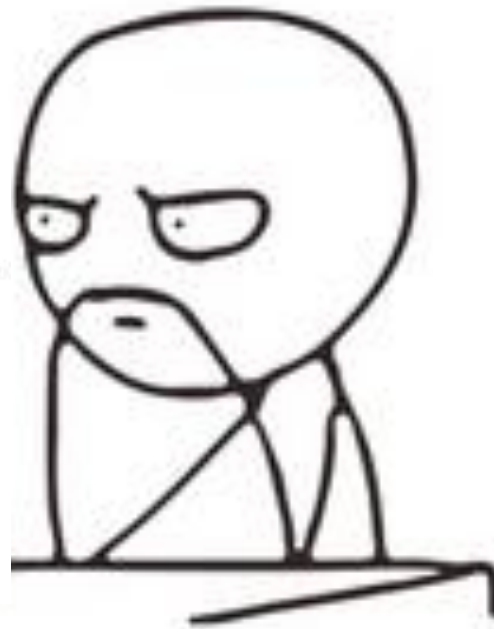
NOMOR 82 TAHUN 2012

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.

# How we do it with RouterOS?





# Multi-Factor Authentication on RouterOS

17



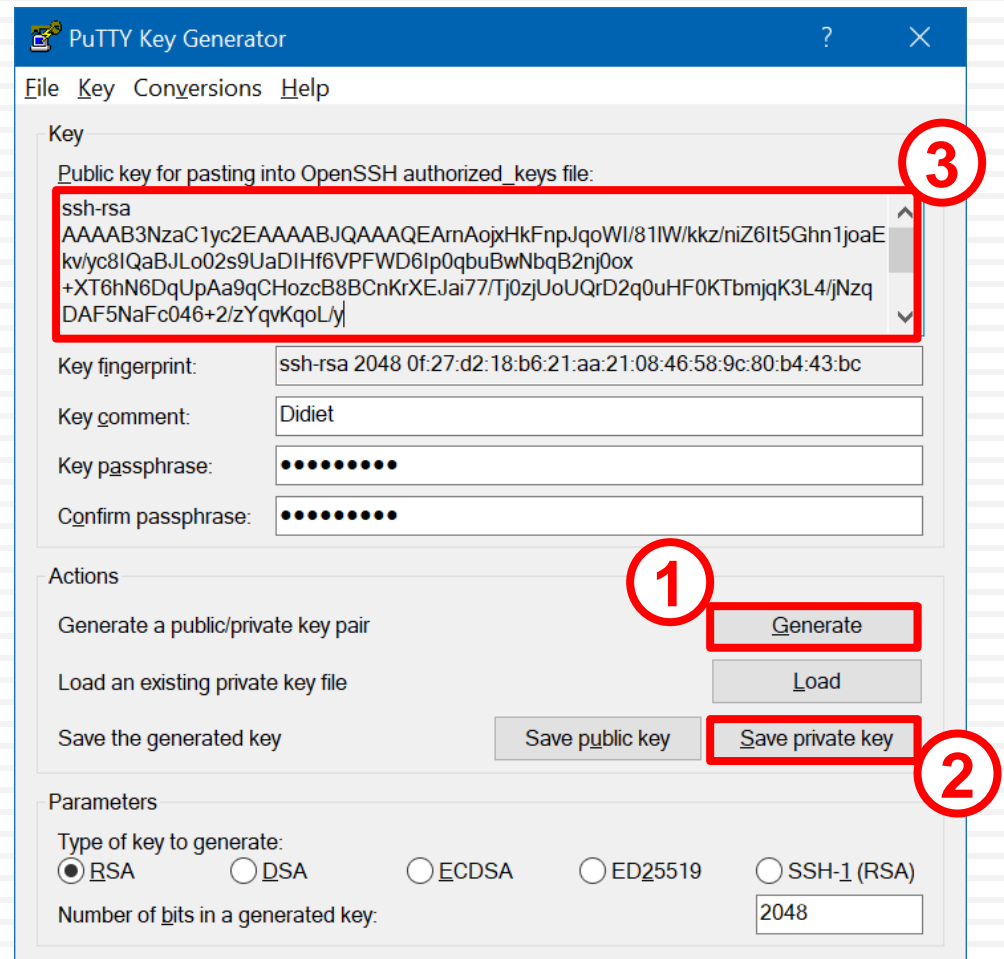
- Something you know → Password
- Something you have → SSH Keys
- Somewhere you from → IP Address

# Create SSH Public & Private Key

18

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

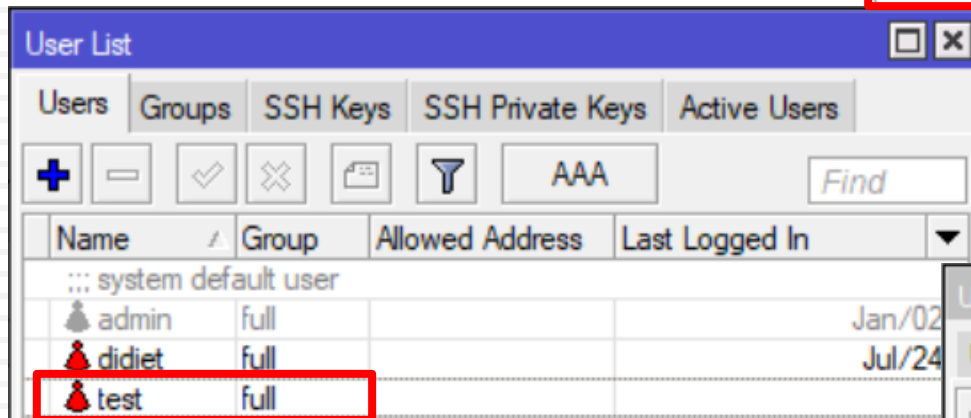
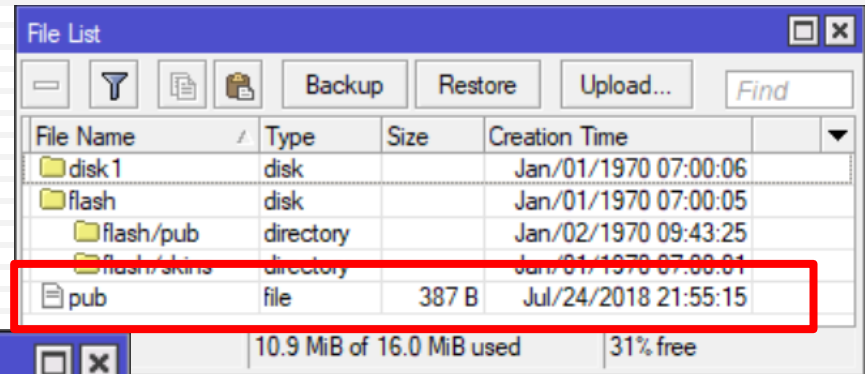
For OS X and Linux users can use  
'ssh-keygen'



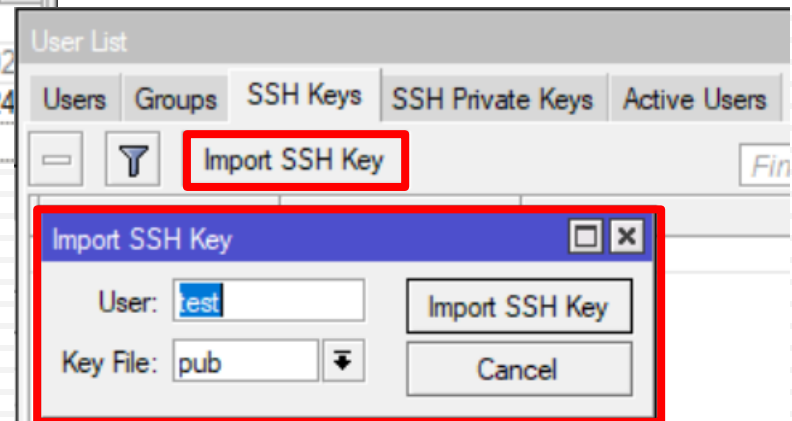
# RouterOS Configuration

19

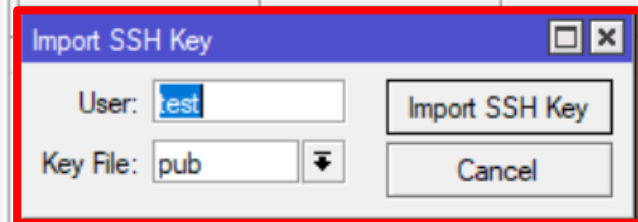
## 1. Upload Public Key



## 2. Create New User

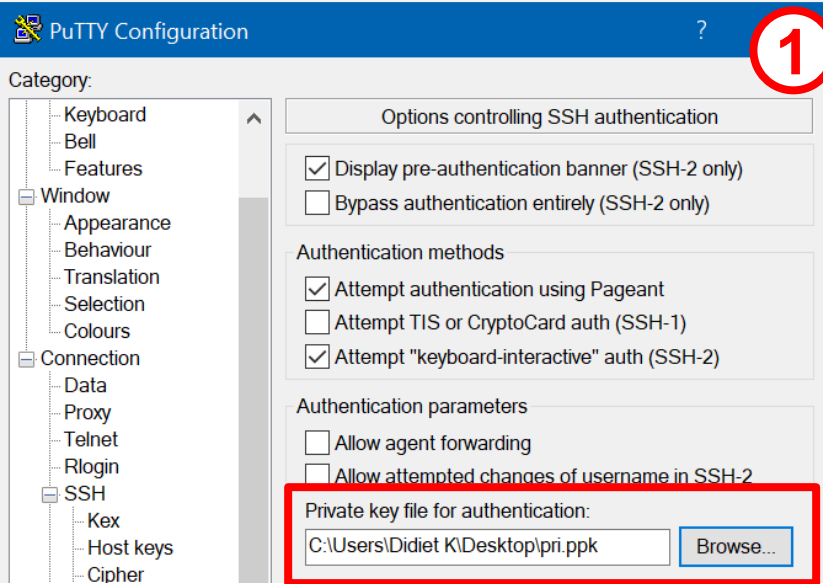


## 3. Import SSH Key

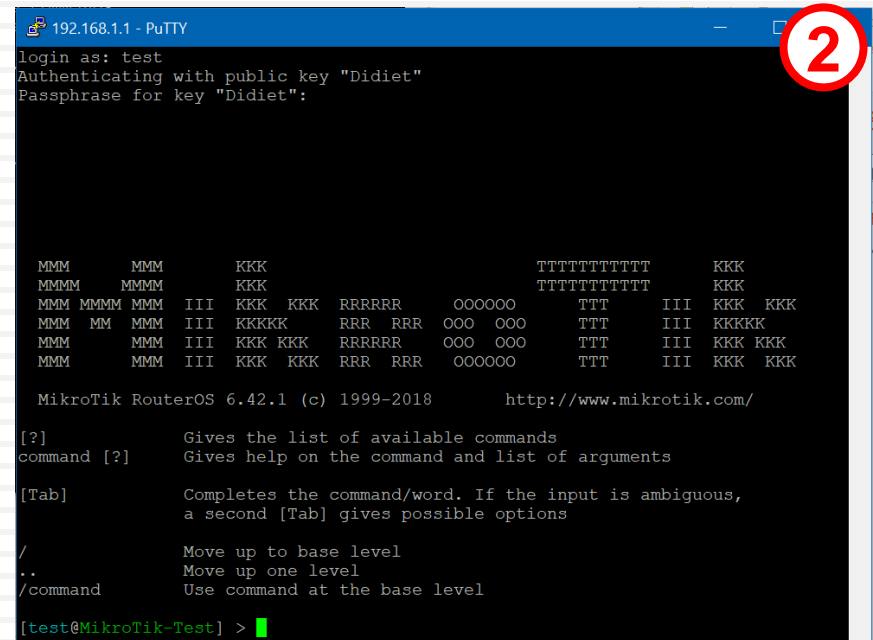


# Login using SSH Keys

20



Connection > SSH > Auth



# Only permit from specific IP address

21

The screenshot shows a configuration window titled "IP Service List" with a table of services. The "ssh" service is selected, and a sub-window titled "IP Service <ssh>" is open, showing its configuration. The sub-window has a red border around the "Name", "Port", and "Available From" fields, which are set to "ssh", "10000", and "192.168.1.0/24" respectively. The "Available From" field is a dropdown menu. The sub-window also has "OK", "Cancel", "Apply", and "Disable" buttons, and a status indicator at the bottom that says "enabled".

	Name	Port	Available From	Certificate
X	api	8728		
X	api-ssl	8729		none
X	ftp	21		
	ssh	10000	192.168.1.0/24	
X	telnet	23		
X	winbox	8291		
X	www	80		
X	www-ssl	443		

IP Service <ssh>

Name: ssh

Port: 10000

Available From: 192.168.1.0/24

OK

Cancel

Apply

Disable

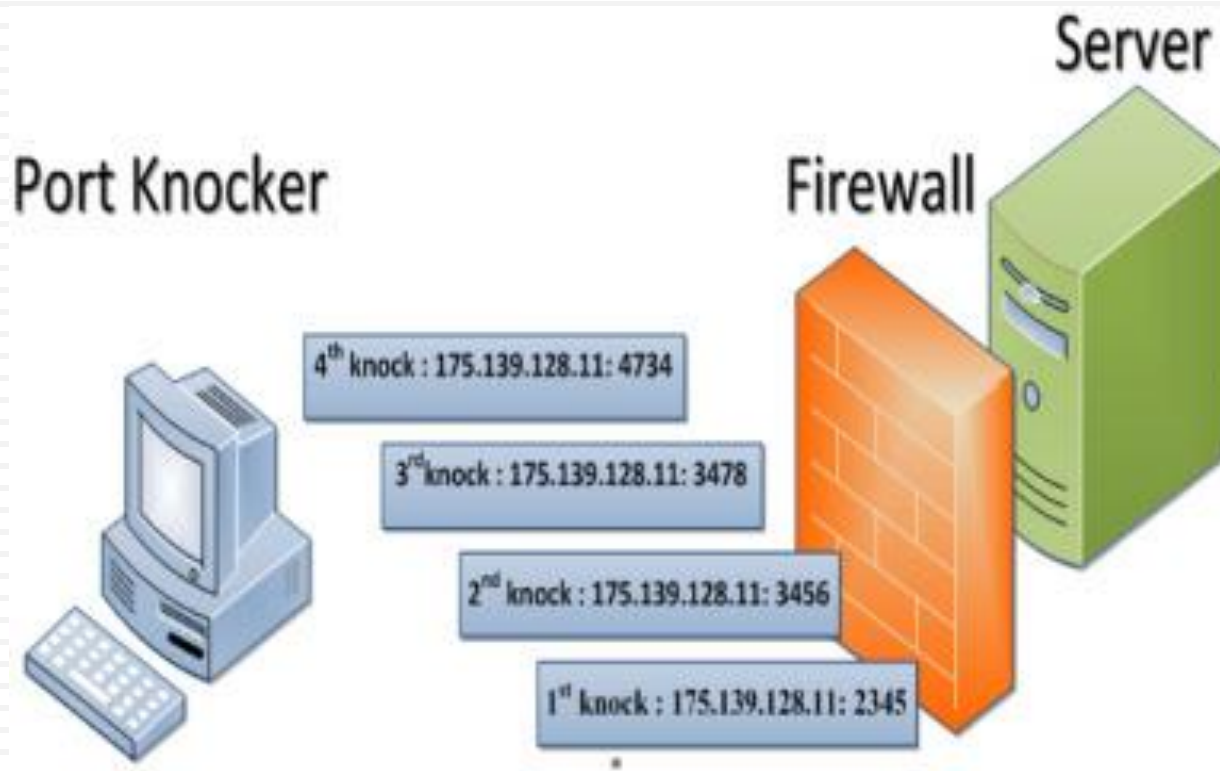
enabled

8 items (1 selected)

# Other Methods (1/3)

22

## Port Knocking



[https://wiki.mikrotik.com/wiki/Port\\_Knocking](https://wiki.mikrotik.com/wiki/Port_Knocking)

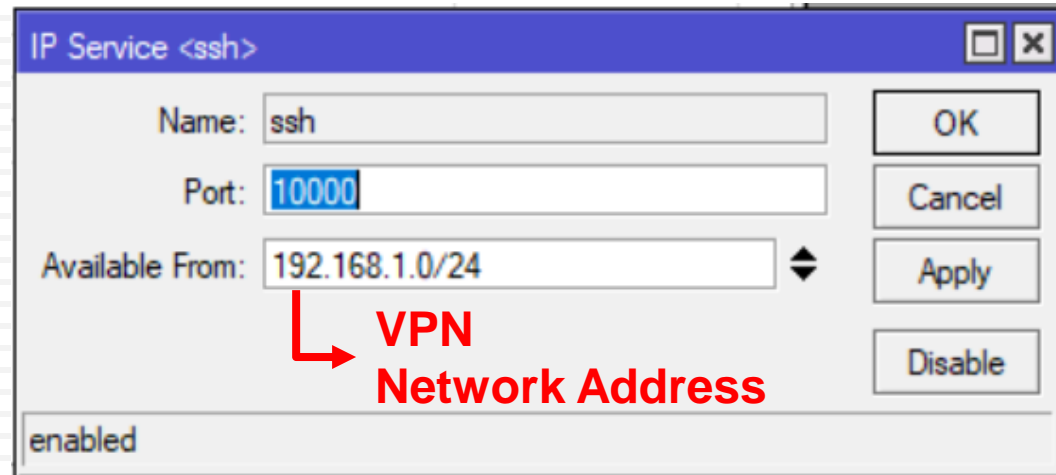
# Other Methods (2/3)

23

## VPN then remote access

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

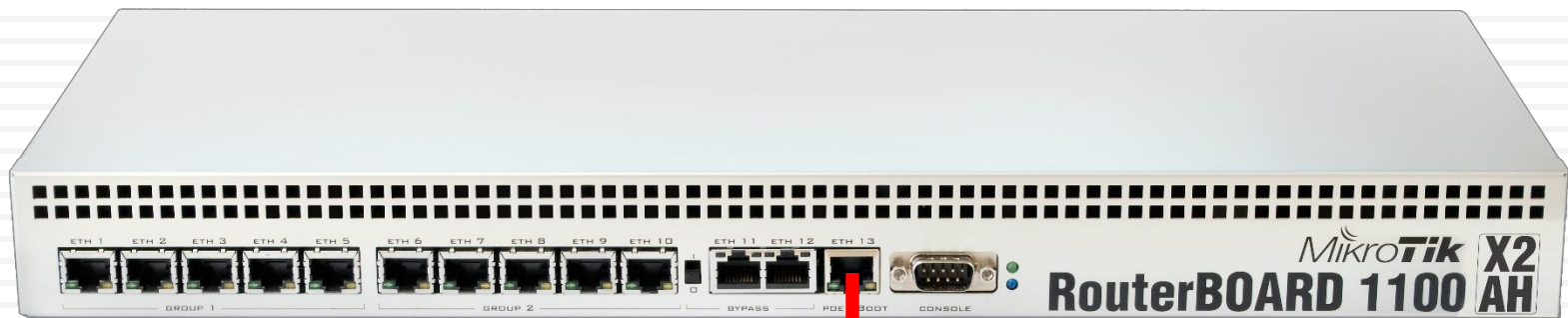
2. Remote Access (Winbox/SSH)



# 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 main window shows a Syslog log table with the following data:

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)

The 'Logs' section in the left sidebar is expanded, showing 'Syslog' selected. A 'Syslog - Log Settings' dialog box is open, showing the 'Files' tab with the following settings:

- Name: Syslog
- Start New File: never
- Files To Keep: 10
- Buffered Entries: 1000

The dialog box also includes buttons for 'Ok', 'Cancel', 'Apply', 'Notes', 'Copy', and '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

- 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](https://wiki.mikrotik.com/wiki/Port_Knocking).
- MikroTik. 2016. Manual: The Dude v6/Syslog. [https://wiki.mikrotik.com/wiki/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](mailto:didiet@arch.web.id)

29

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](http://www.arch.web.id)