ACCESS ROUTEROS USING MULTI-FACTOR AUTHENTICATION

MIKROTIK USER MEETING 2018

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

About Me

Didiet Kusumadihardja

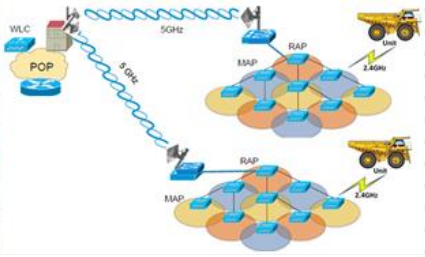
- 12 tahun pengalaman di IT

  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

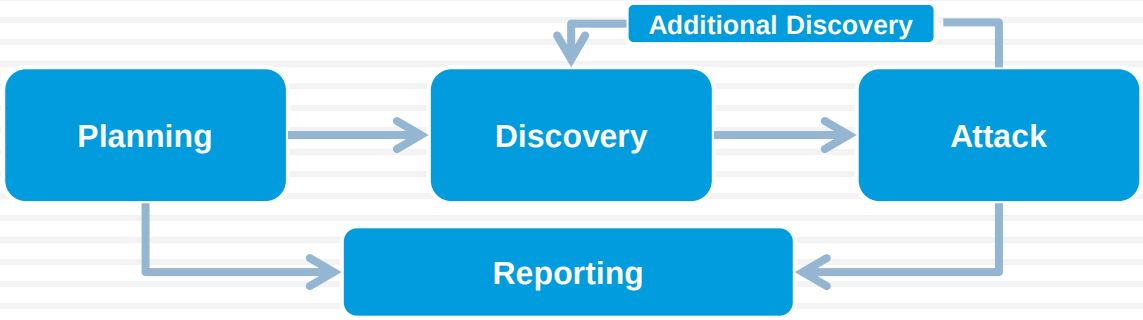
https://about.me/didiet

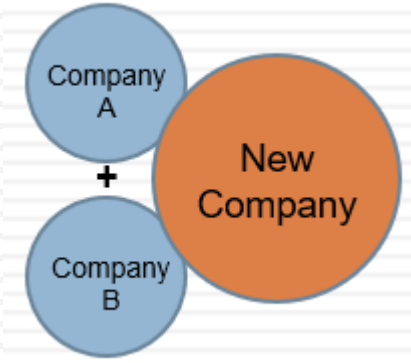
Services Offered

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

Data Breaches News 2016

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

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

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

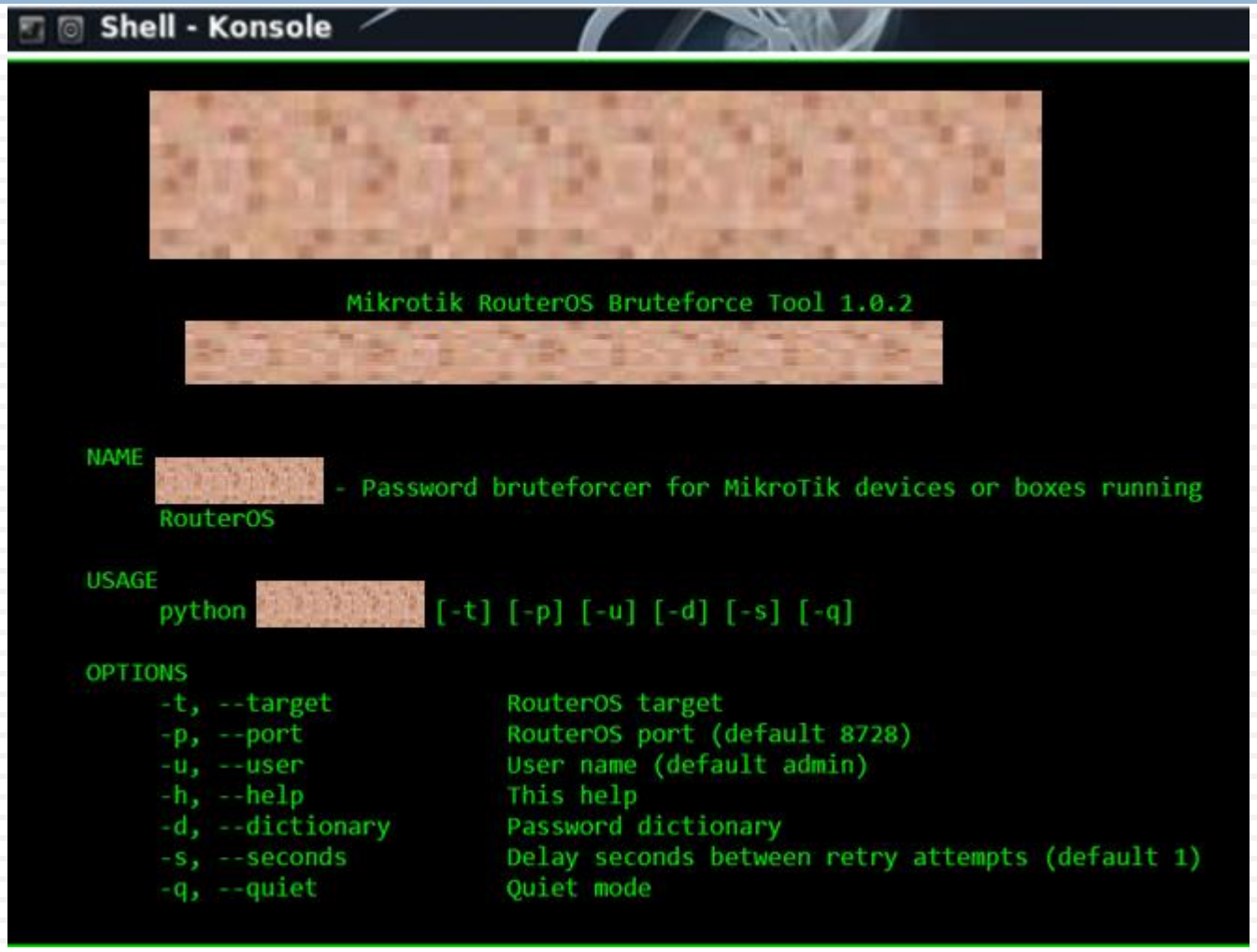
- **6.42.1 (23 April 2018)**

  winbox - fixed vulnerability that allowed to gain access to an unsecured router

- **6.42.7 (17 Agustus 2018)**

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

Exploits


Shell - Konsole
Mikrotik RouterOS Bruteforce Tool 1.0.2
NAME
- Password bruteforcer for MikroTik devices or boxes running RouterOS
USAGE
python [-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

Processing Power vs Passwords

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

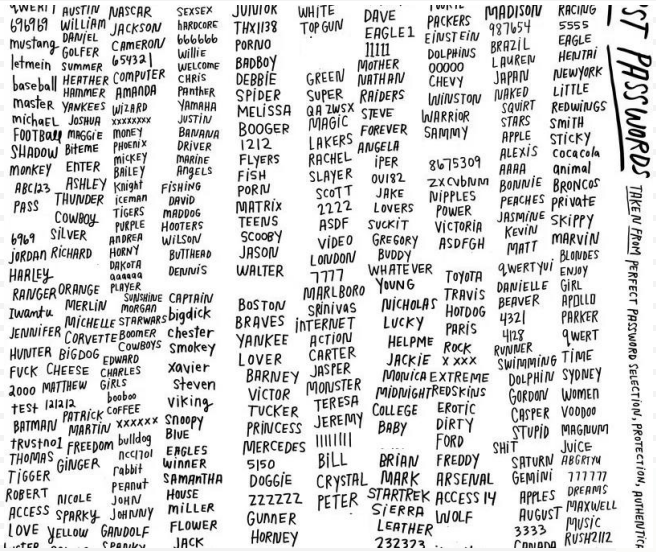
All your passwords are belong to us.

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

ars TECHNICA

Jeremi Gosney

Reality



Password Dictionary

Dictionary Attack

Brute Force Attack

Exploits

Bad Guys

Humans and Password

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

Indonesia Regulation

PERATURAN PEMERINTAH REPUBLIK INDONESIA

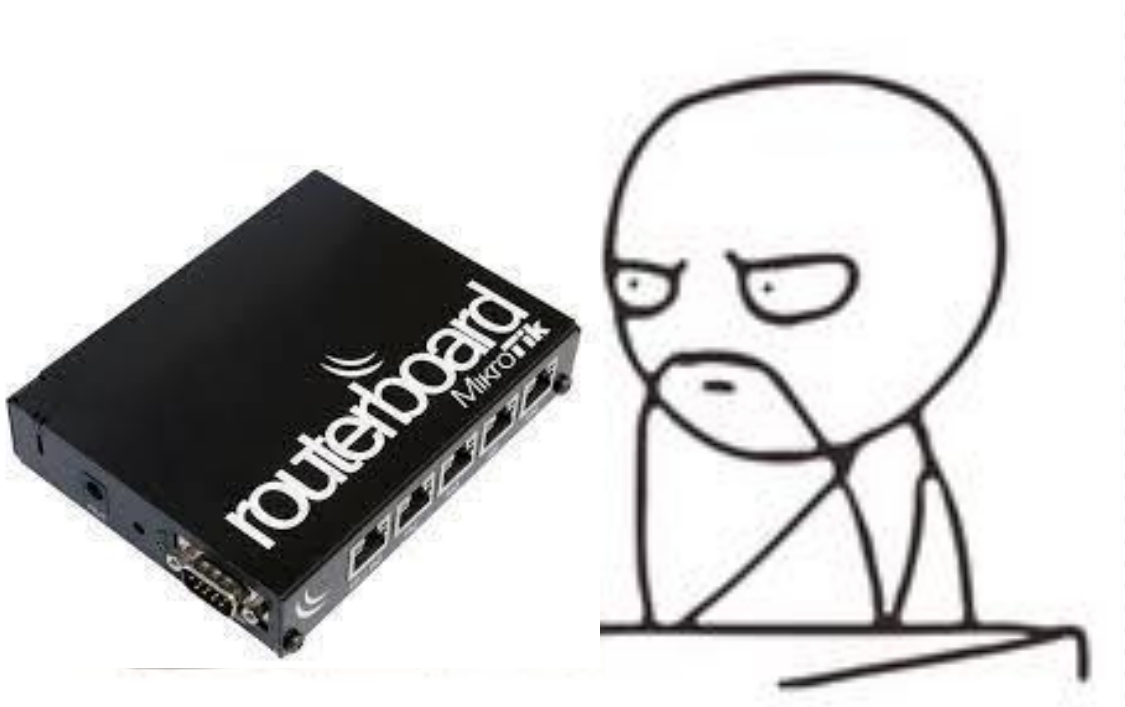
NOMOR 82 TAHUN 2012

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?

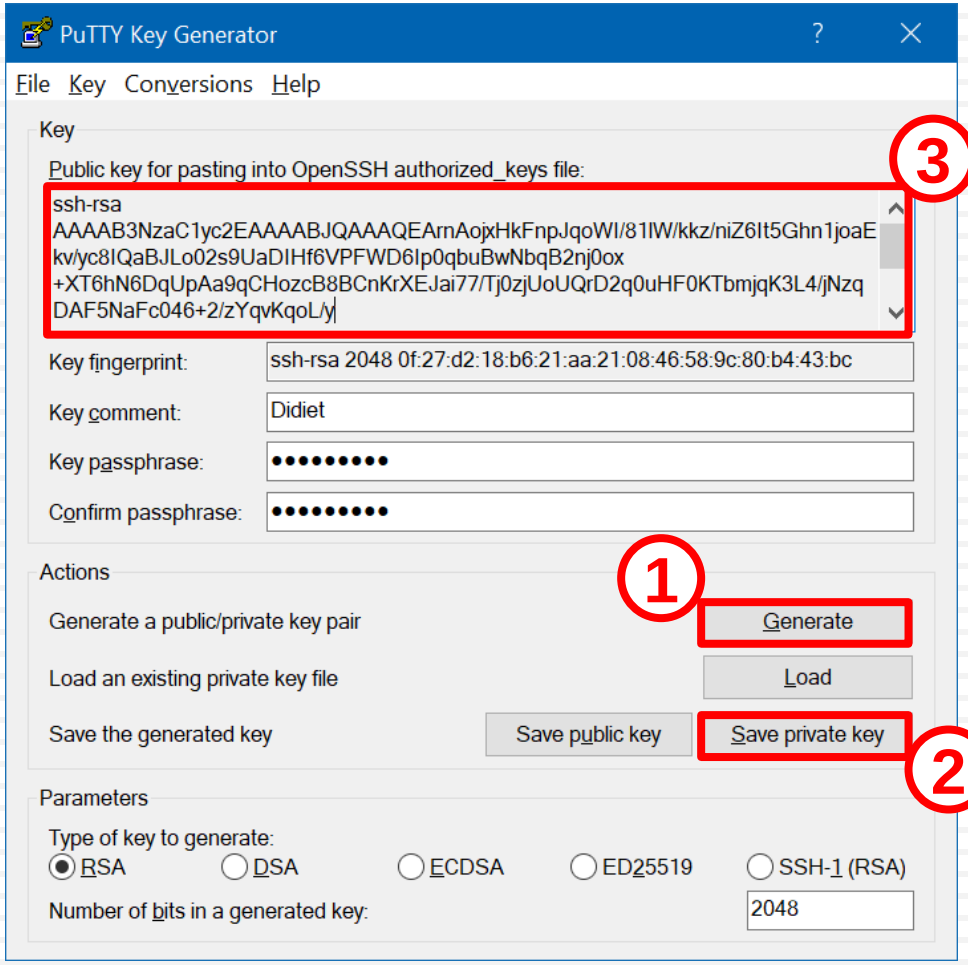


Multi-Factor Authentication on RouterOS

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

Create SSH Public & Private Key

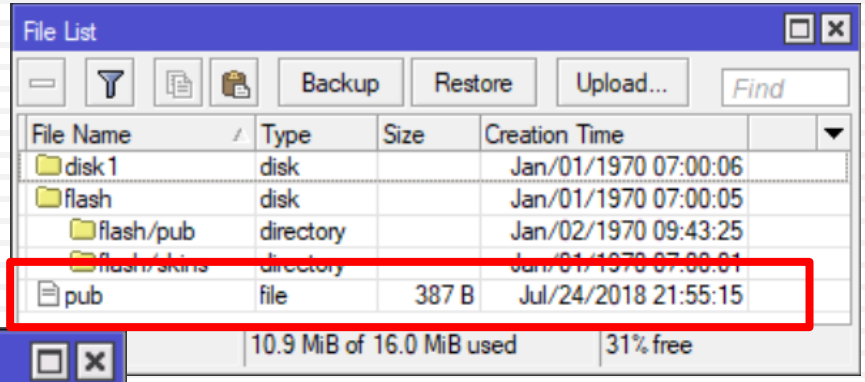
1. Generate
2. Save Private Key
3. Copy Public Key and save to file



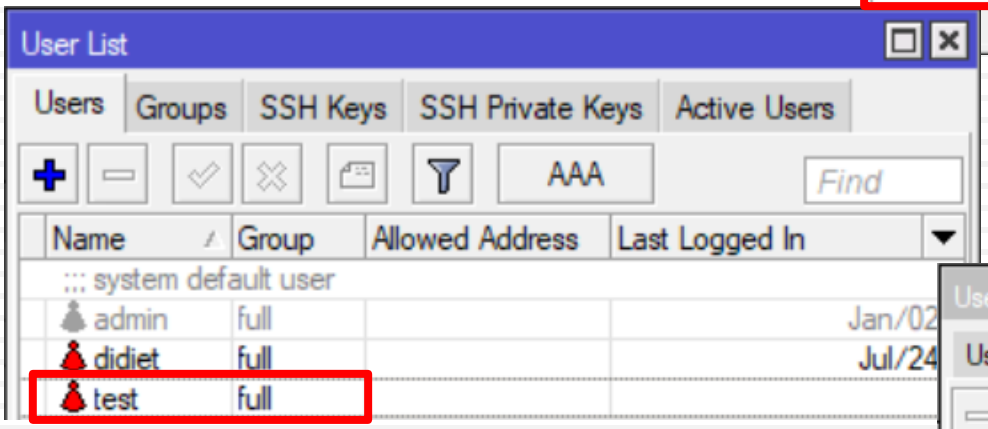
For OS X and Linux users can use '**ssh-keygen**'

RouterOS Configuration

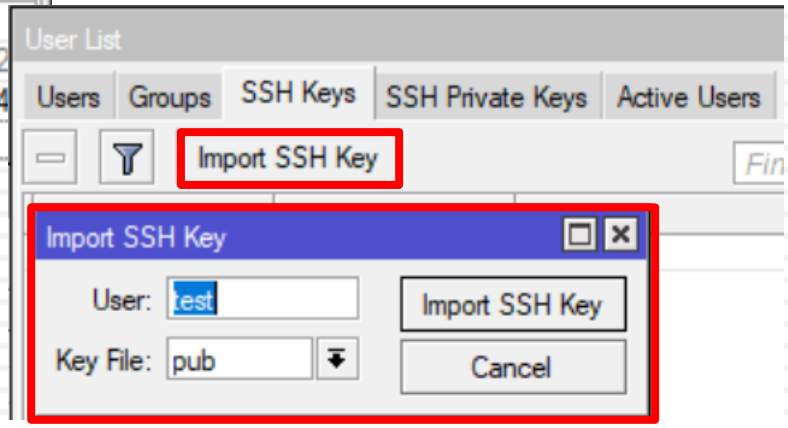
1. Upload Public Key



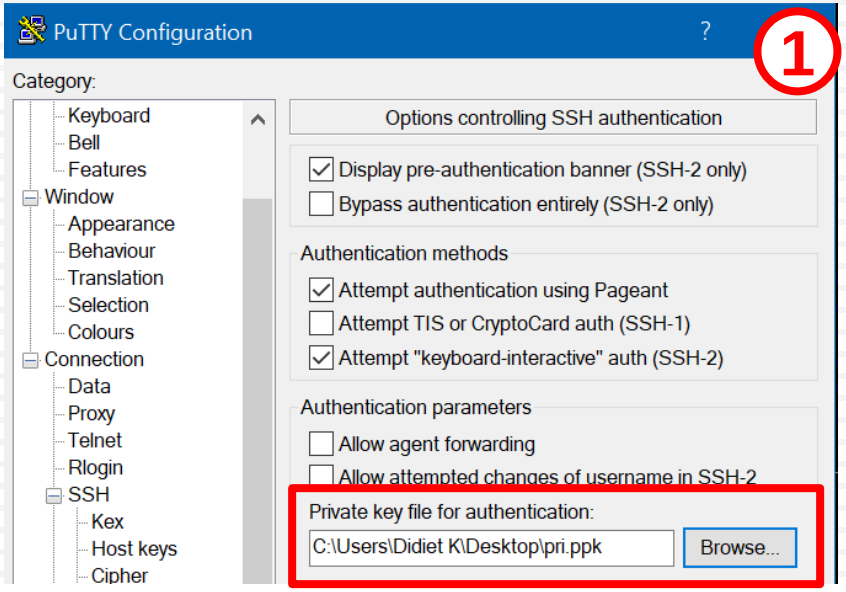
2. Create New User



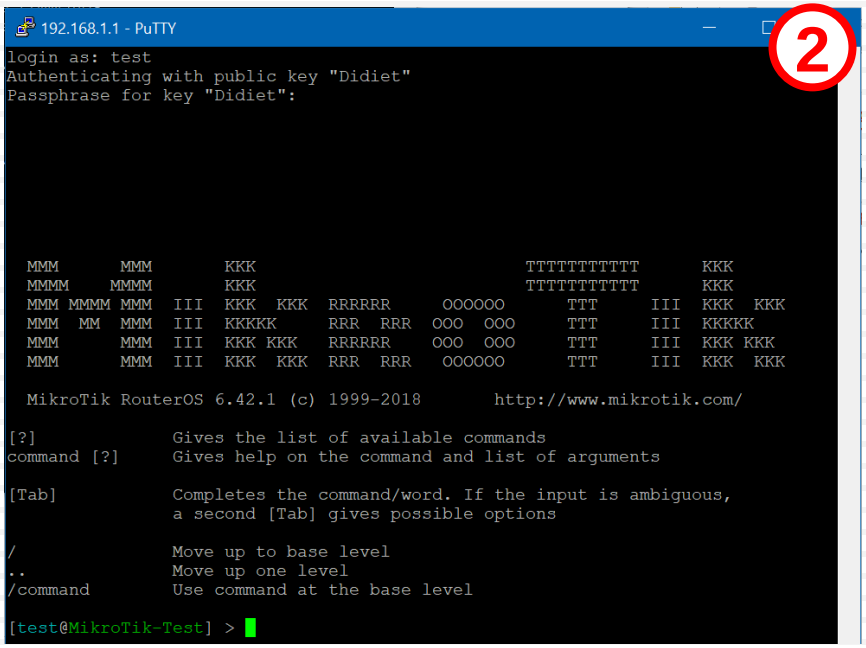
3. Import SSH Key



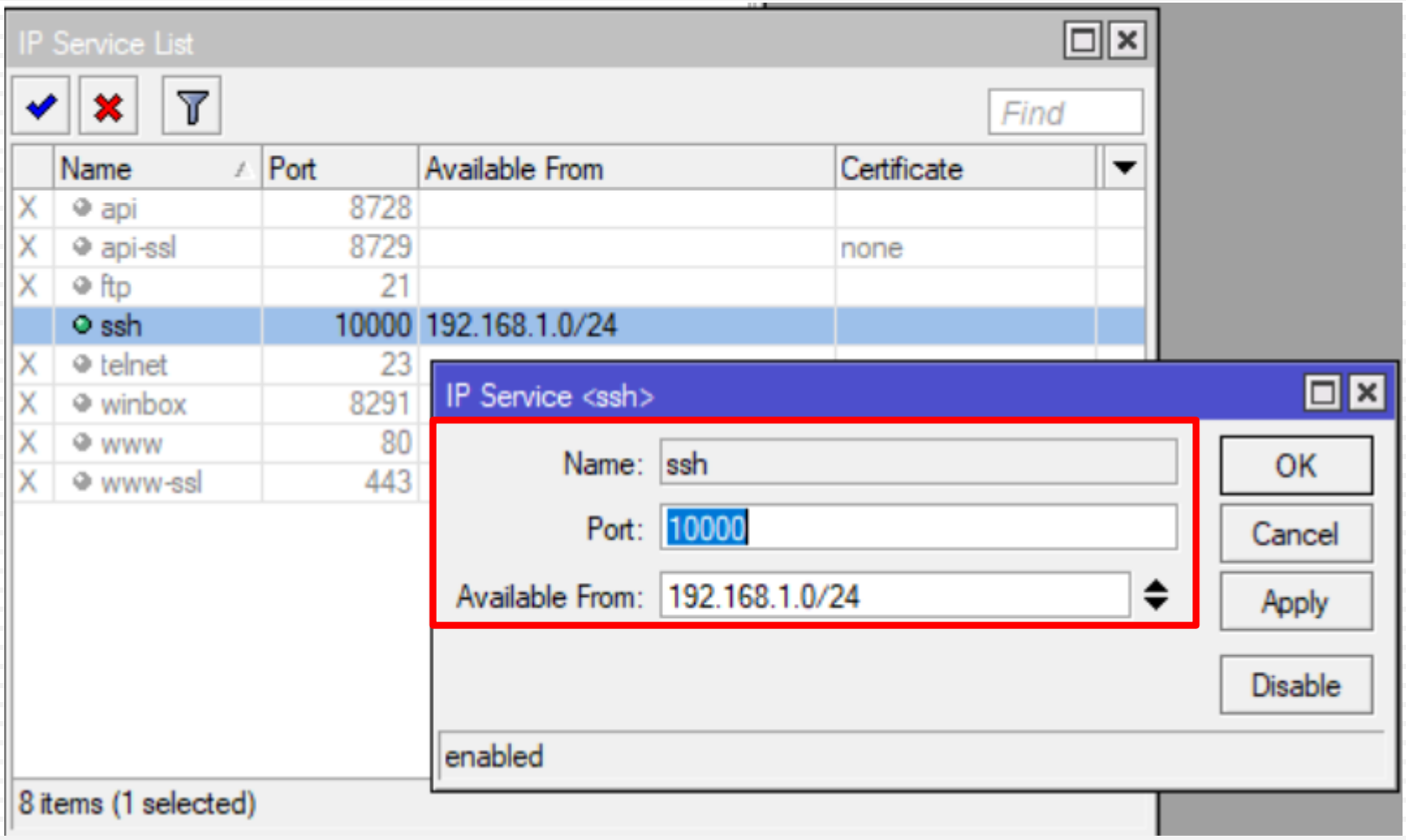
Login using SSH Keys



Connection > SSH > Auth

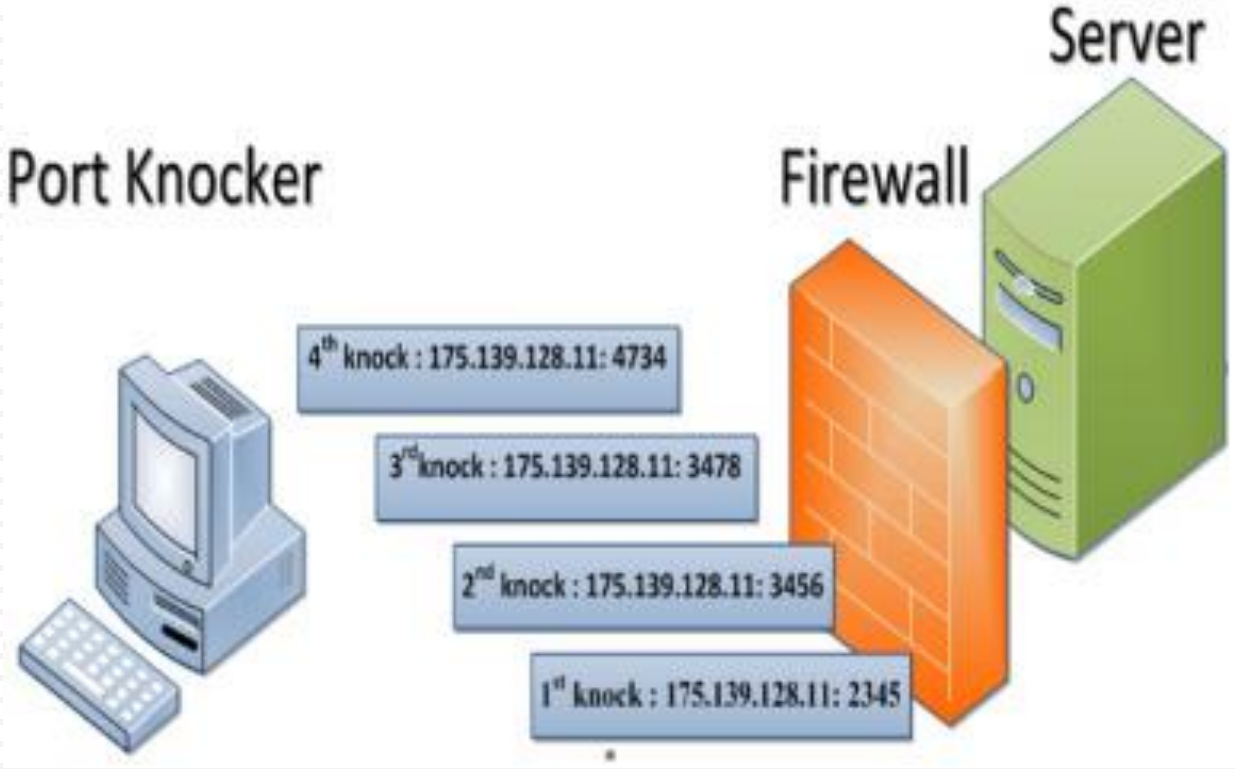


Only permit from specific IP address



Other Methods (1/3)

Port Knocking



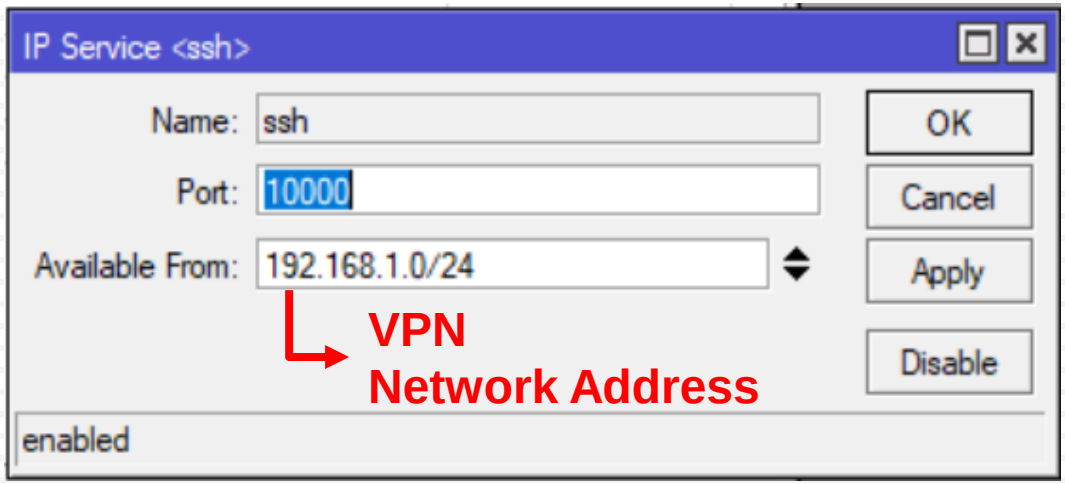
https://wiki.mikrotik.com/wiki/Port_Knocking

Other Methods (2/3)

VPN then remote access

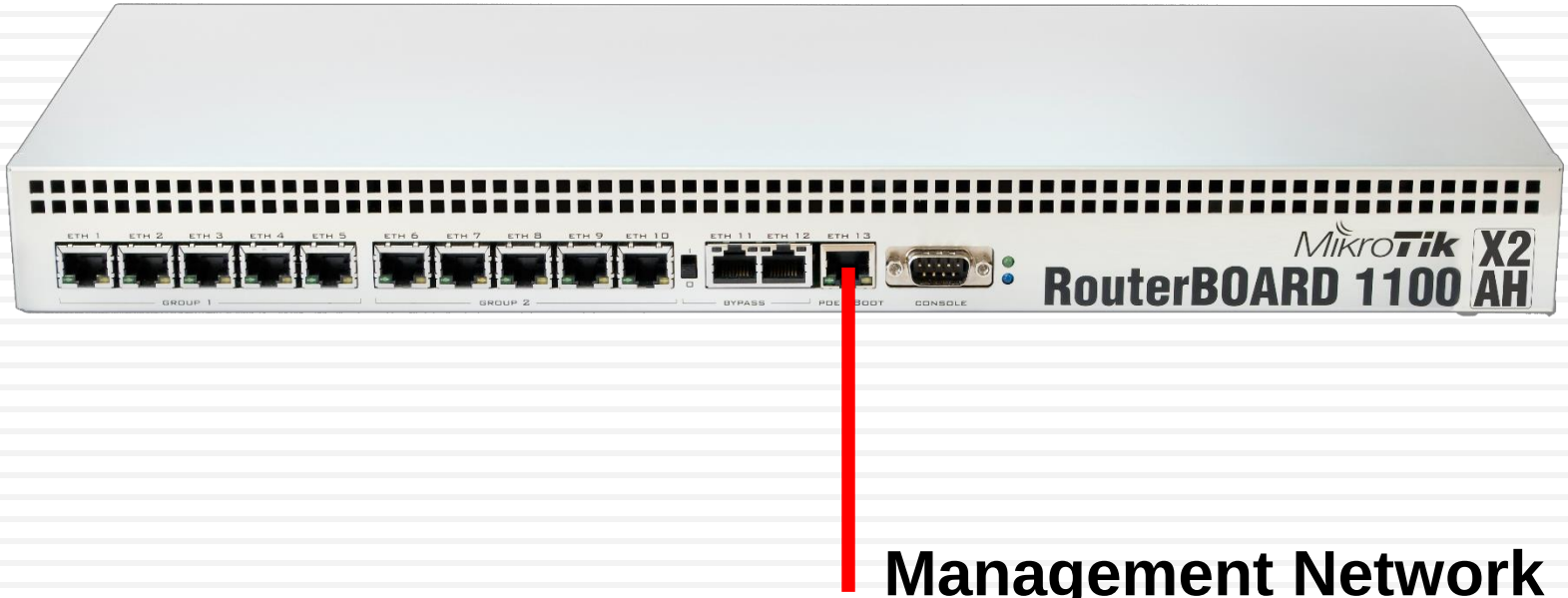
1. **VPN (~~PPTP~~/SSTP/OpenVPN)**

2. **Remote Access (Winbox/SSH)**



Other Methods (3/3)

Out of Band Network



Audit Trail / Log as Evidence

UNDANG-UNDANG REPUBLIK INDONESIA

NOMOR 11 TAHUN 2008

TENTANG

INFORMASI DAN TRANSAKSI ELEKTRONIK

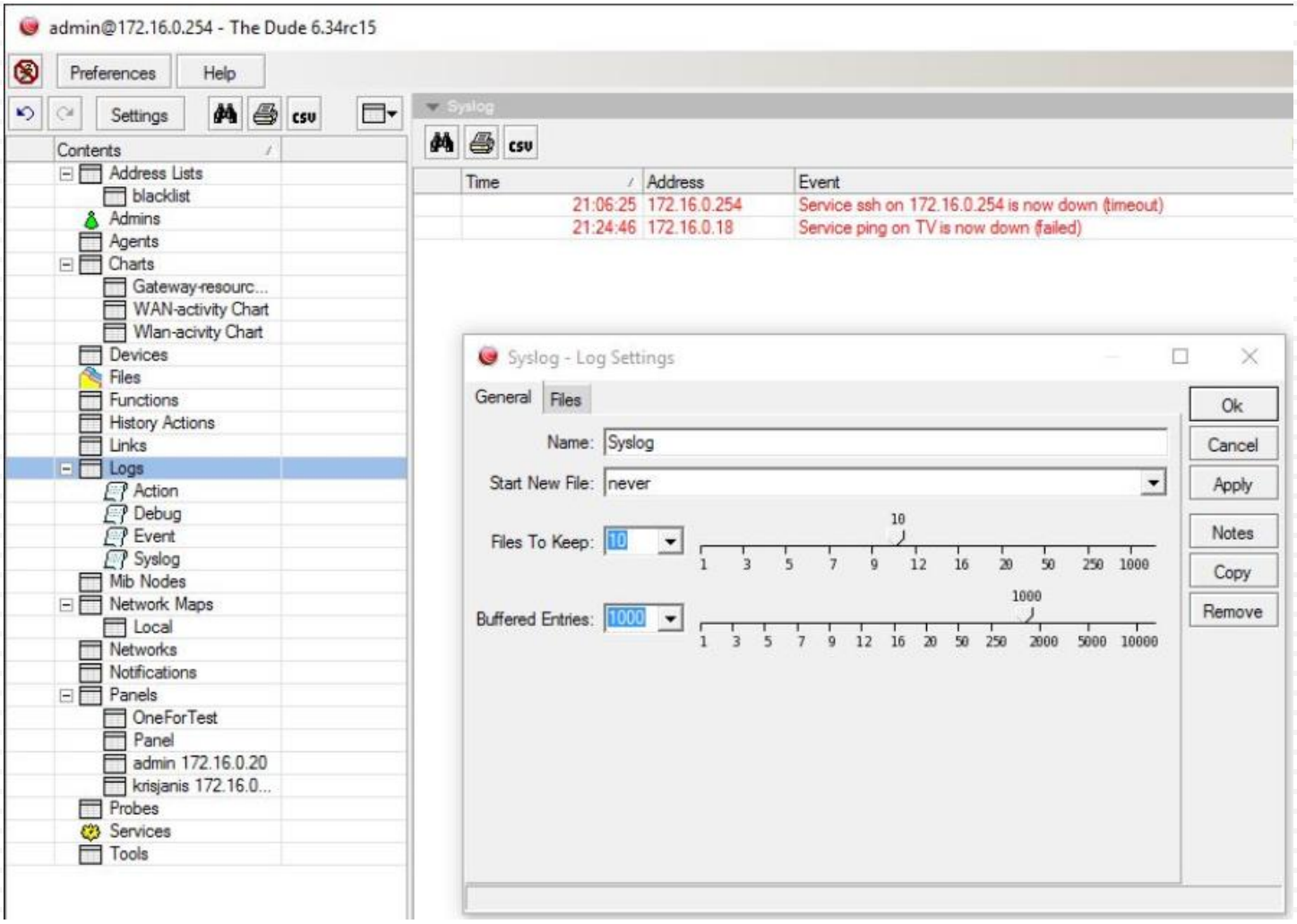
BAB III

INFORMASI, DOKUMEN, DAN TANDA TANGAN ELEKTRONIK

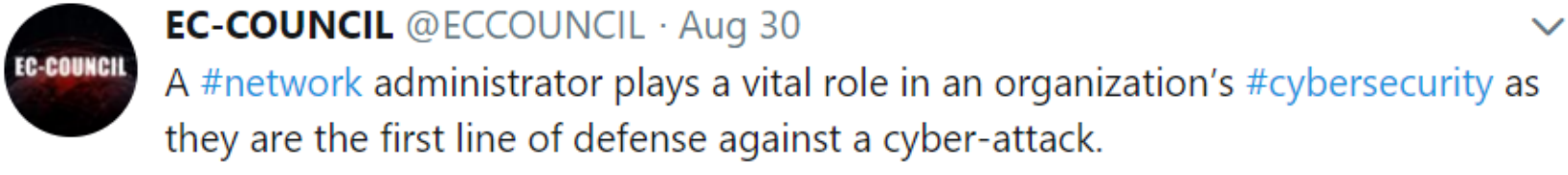
Pasal 5

(1) Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah.

Audit Trail / Log using The Dude



Summary



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.
- 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