Fools your enemy with Mikrotik

BY: DIDIET KUSUMADIHARDJA

MIKROTIK USER MEETING (MUM) 2016

JAKARTA, INDONESIA

14 OCTOBER 2016

About Me

Didiet Kusumadihardja

1. IT Security Specialist
   - PT. Mitra Solusi Telematika

mitra solusi telematika

2. Trainer & IT Consultant
   - Arch Networks

Arch NETWORKS

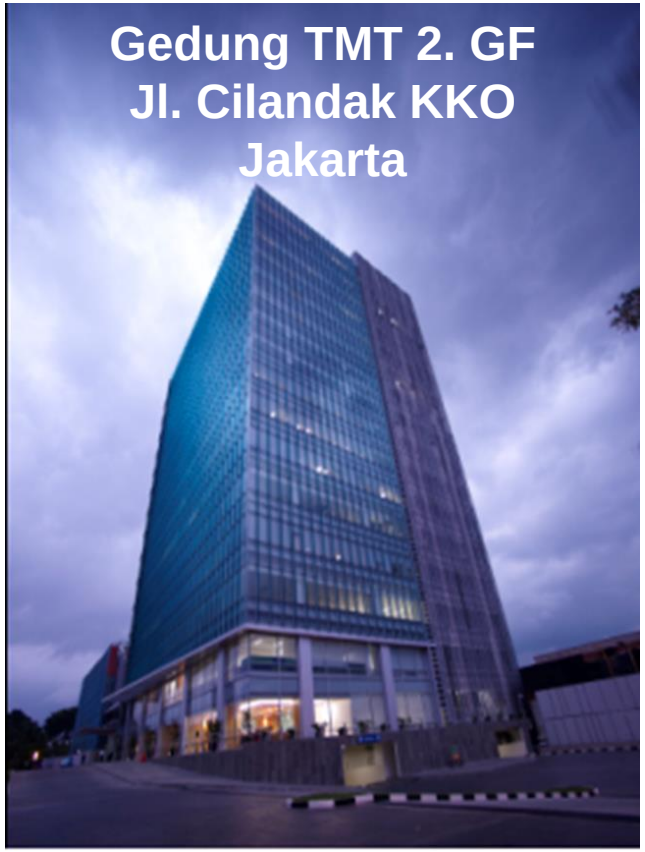
LinkedIn

MikroTik CERTIFIED

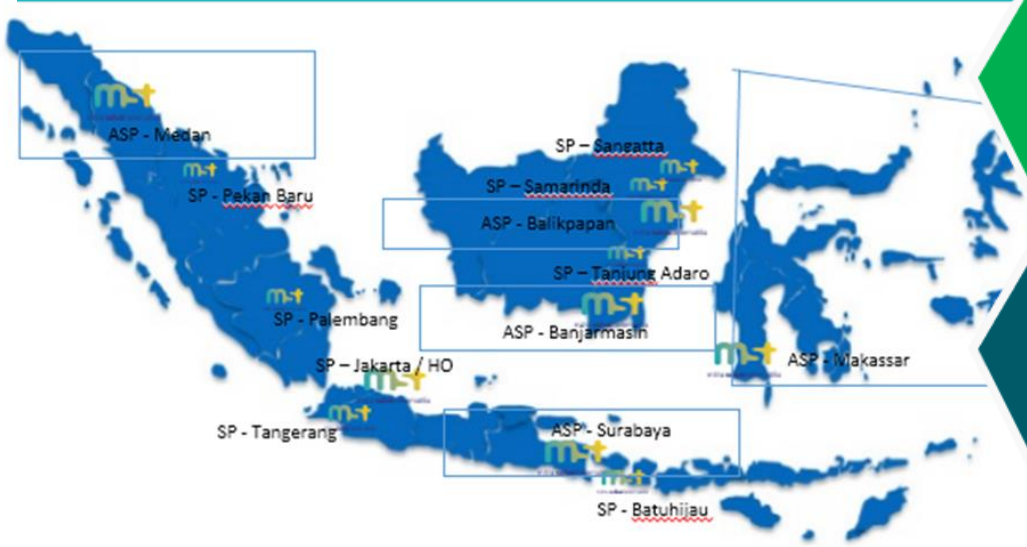
MTCNA, MTCINE, MTCWE, ~~MTCUME, MTCTCE, MTCRE~~

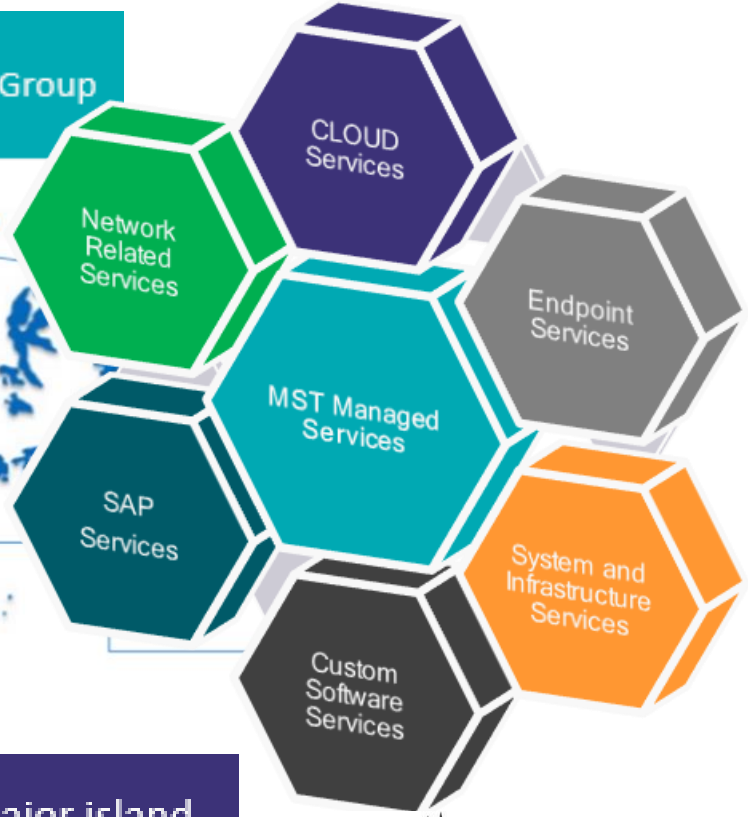
PT. Mitra Solusi Telematika

mitra solusi telematika



An ICT business unit of PT Mahadana Dasha Utama (www.mahadasha.co.id) and part of Tiara Marga Trakindo Group (www.tmt.co.id)



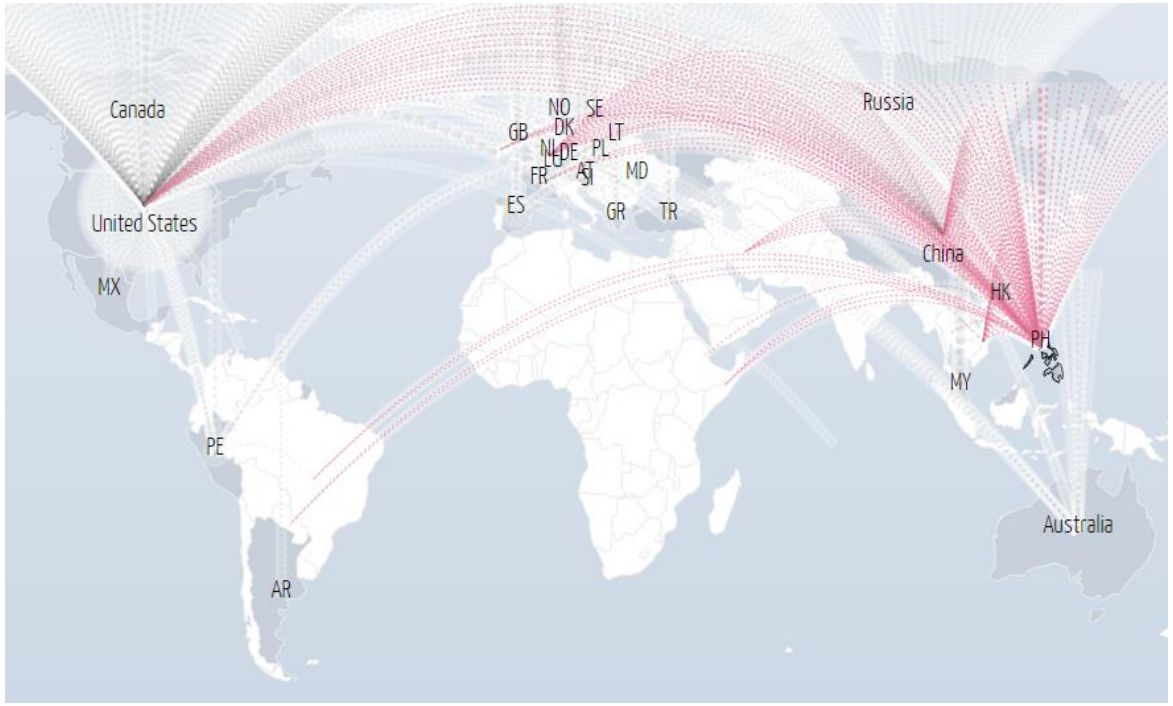


Supporting Indonesia with 12 Service points on major island

Didiet Kusumadihardja - didiet@arch.web.id

MikroTik

Global IT Security Incident



Global IT Security Incident 2014

A screen shot of an image that appeared on computers at Sony Pictures Entertainment on Nov. 24, 2014. *(Photo: Reddit)*

James Franco and Seth Rogen star in "The Interview," a movie whose full Christmas Day distribution was canceled by Sony amid hacker threats.
(Photo: Ed Araquel, AP)

Global IT Security Incident 2015

Dow Jones Alami Kebocoran Data

Indeks bursa saham AS yang terkenal yaitu Dow Jones mengakui bah
data akibat serangan *hacker*. Dow Jones, unit usaha dari News Corp
mengakui bahwa *hacker* berhasil masuk ke dalam sistemnya sejak Ag
Dow Jones sendiri mengatakan bahwa pihaknya telah menghubungi
data ini.

3 Tahun di Hack (2012 – 2015)

Dow Jones Discloses Customer Data Breach

Wall Street Journal owner says financial data from 3,500 individuals may have been accessed

DOW JONES

October 9, 2015

William Lewis
Chief Executive Officer, Dow Jones
Publisher, The Wall Street Journal

To our customers:

Protecting our customers' information is of the utmost importance to us. Out of an abundance of caution, we are notifying you that we recently determined there was unauthorized access to our systems. While we recognize that no company is immune to cyberattacks, we are committed to doing everything we can to protect our customers.

Global IT Security Incident 2016

Former Yahoo Exec Thinks Security Breach Could Have Compromised Up To 3 Billion Accounts, Not Just 500 Million

1 October 2016, 9:37 am EDT By Aaron Mamiit Tech Times

A former Yahoo executive thinks that the number of user accounts compromised by the recently revealed security breach is higher than 500 million. According to his estimate, up to 3 billion users were affected. (Justin Sullivan | Getty Images)

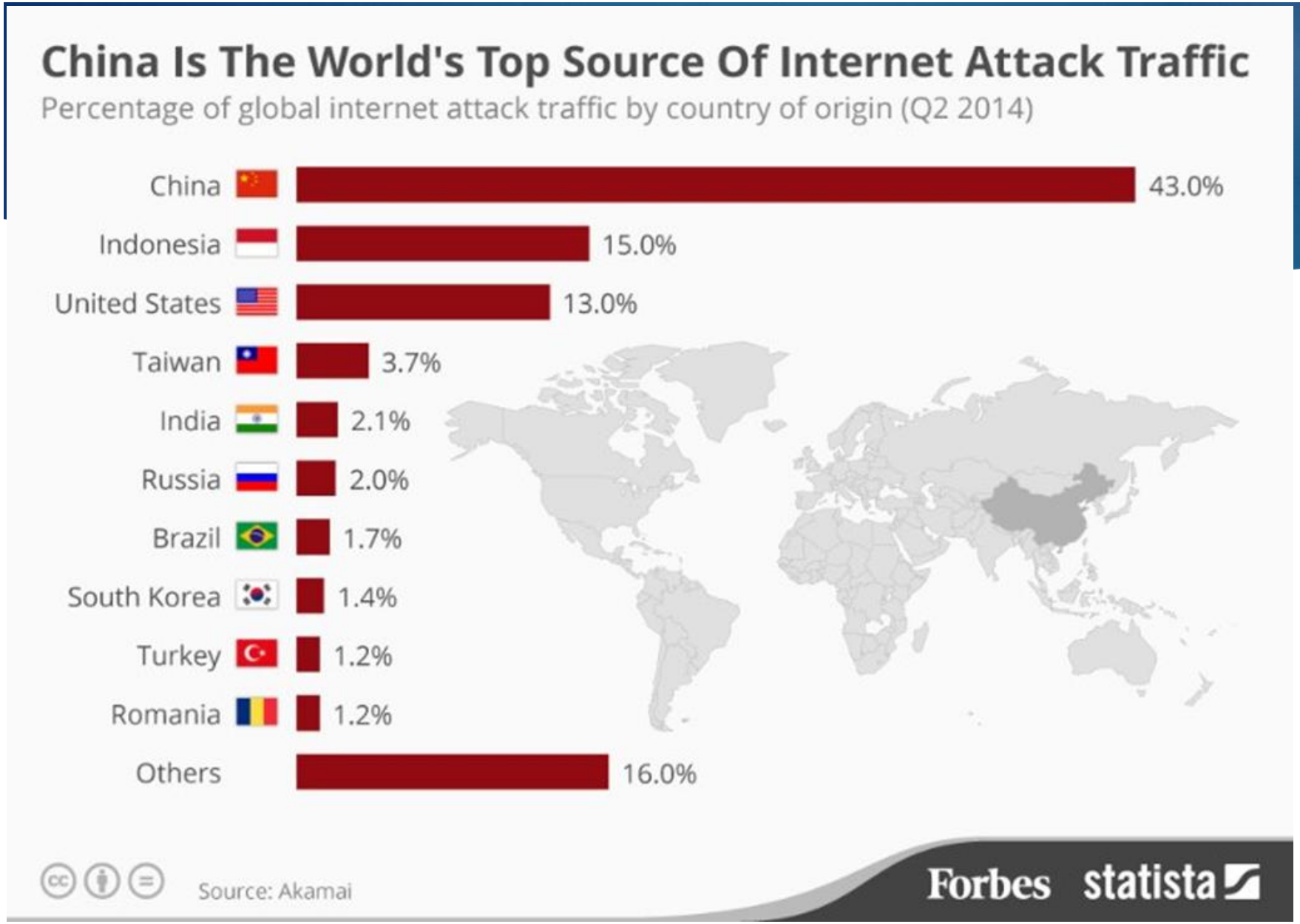
~~**500 Juta Account**~~

3 Miliar Account ???

Source: Tech Times

Indonesia IT Security Incident

Didiet Kusumadihardja - didiet@arch.web.id



INDONESIA IS SAFE?

Source: Akamai

Indonesia IT Security Incident 2013

polri.go.id
2013

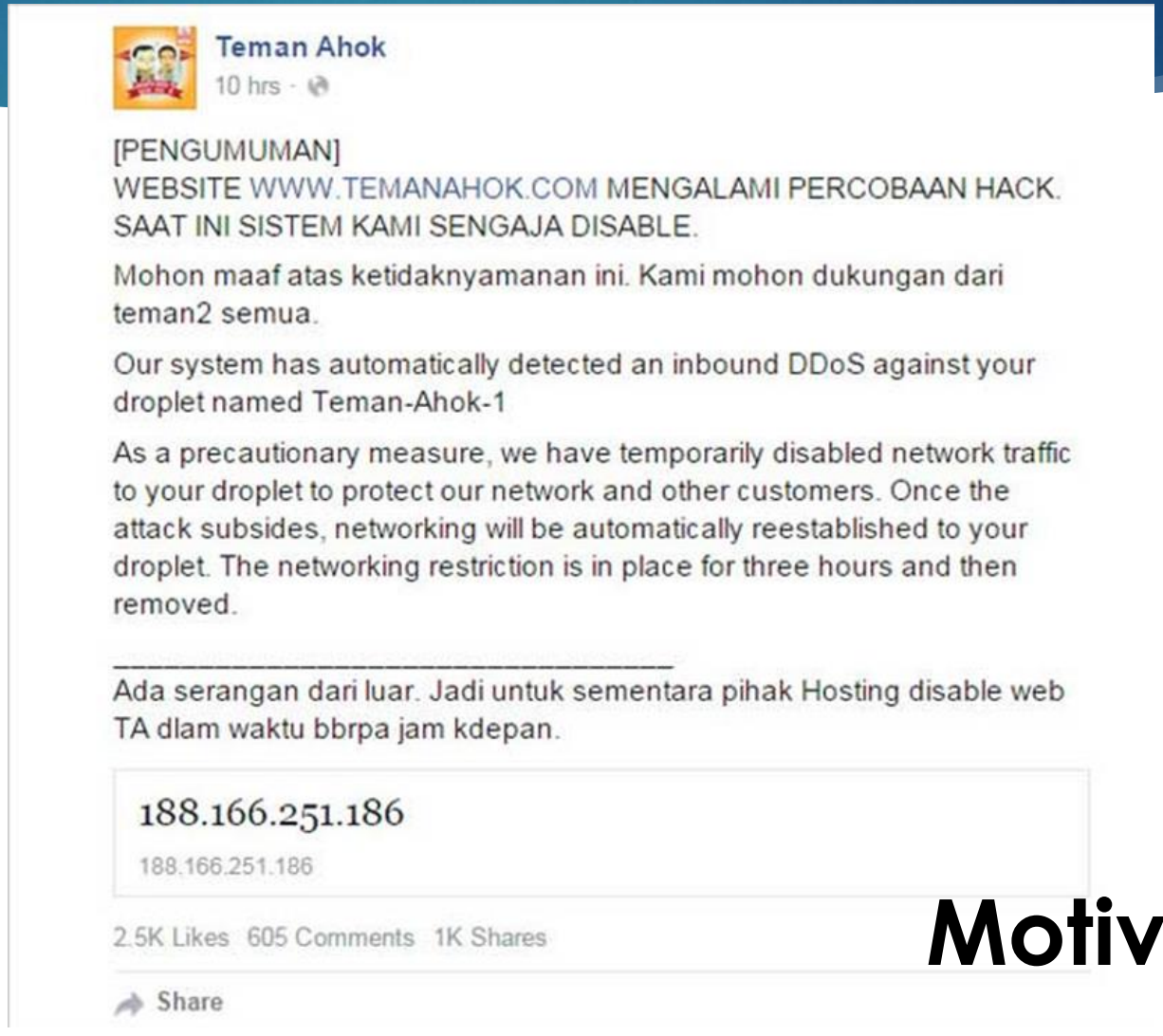
Deface

Motive: Fame?

Indonesia IT Security Incident 2016

Teman Ahok

DDoS Attack



Motive: Politics?

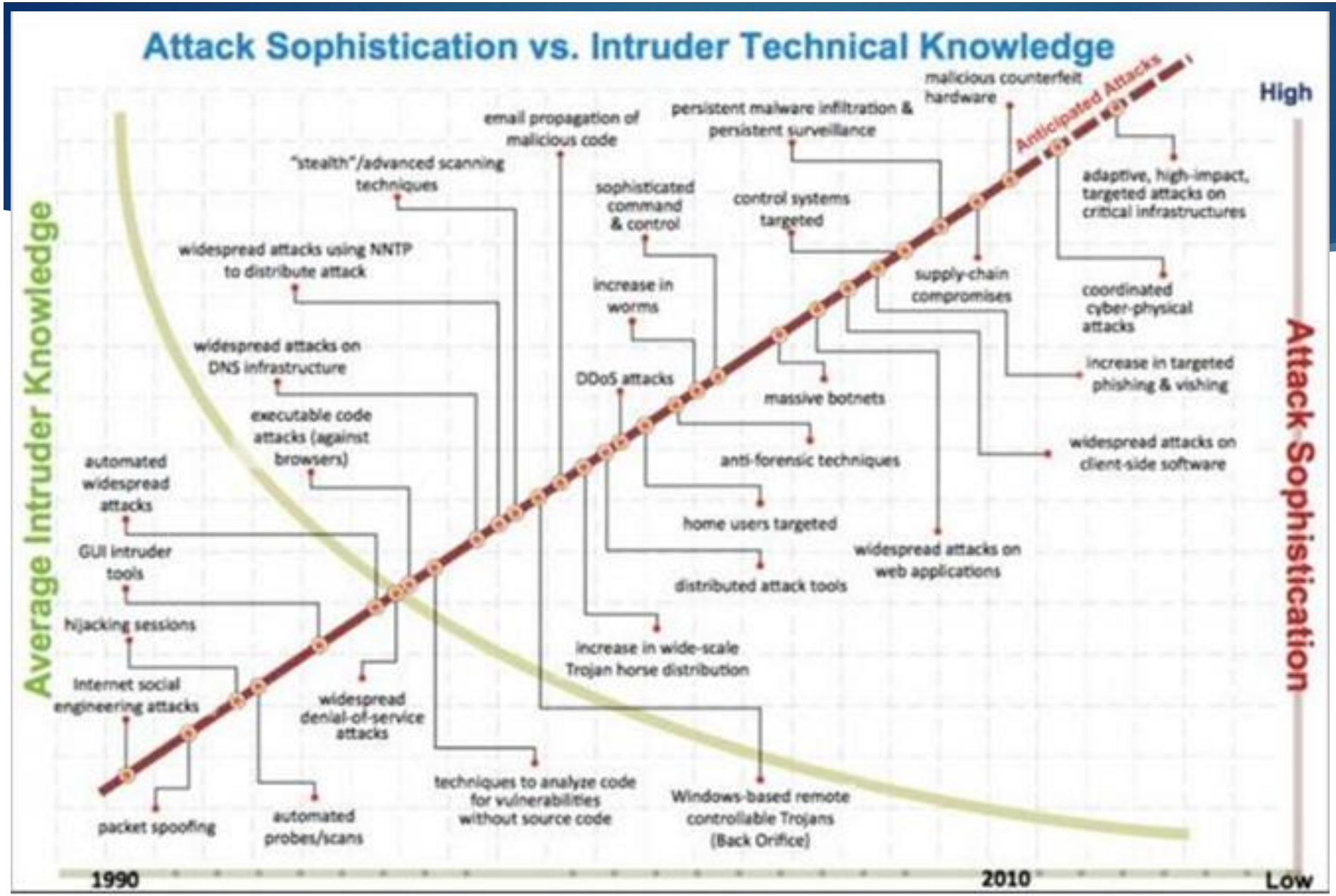
Indonesia IT Security Incident 2016

Videotron

Kebayoran Baru Jakarta Selatan

Foto: Istimewa - Ilustrator Andhika Akbarayansyah

Motive: Curiosity?



IT Security Trends

Gak Perlu Pinter Buat Hacking

Source: Carnegie Mellon University

Hacking Tools Example

WIRESHARK

AIRCRACK-NG

DROIDJACK

metasploit®

Cain & Abel

Kali Linux

Cybercrime as a Service (CaaS)

Modern Business

Source: SCMagazine

How Hackers do it?

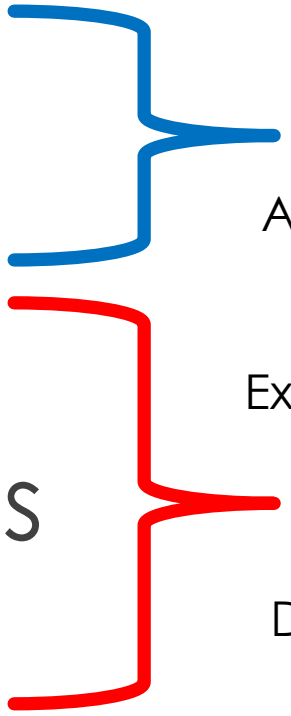
Hacking Phase

1. Reconnaissance
2. Scanning
3. Gaining Access
4. Maintaining Access
5. Clearing Tracks

Source: Ethical Hacking by EC-Council

Hacking Phase (Cont'd)

1. Reconnaissance
2. Scanning
3. Gaining Access
4. Maintaining Access
5. Clearing Tracks



Information Gathering

Device Type

OS Detail

Open Port

Application

Version

Vulnerability

Exploit Vulnerability

Backdoors

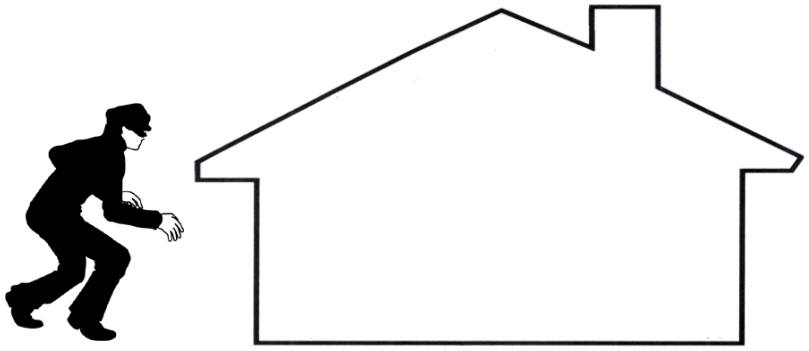
Escalate Privilege

Data harvesting

Delete/overwrite Event/Logs

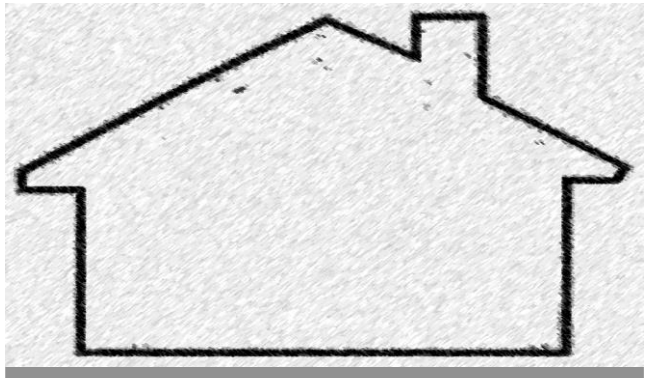
Hacking Phase Analogy

1. Reconnaissance
2. Scanning
3. Gaining Access
4. Maintaining Access
5. Clearing Tracks



When we fools them?

1. Reconnaissance
2. Scanning
3. Gaining Access
4. Maintaining Access
5. Clearing Tracks

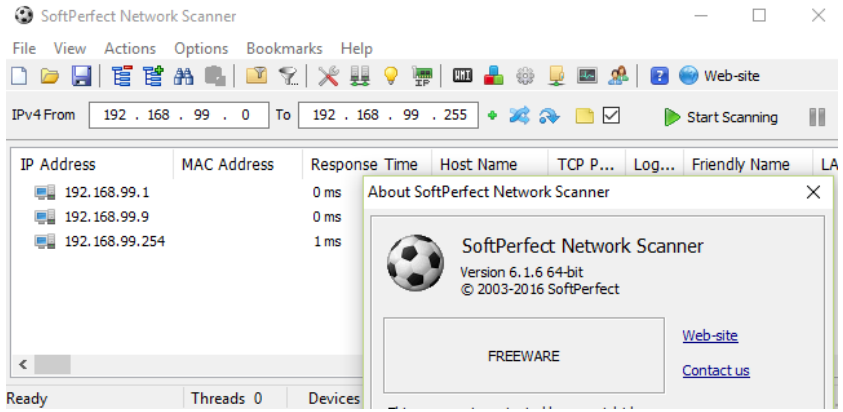


Why at Scanning Phase?

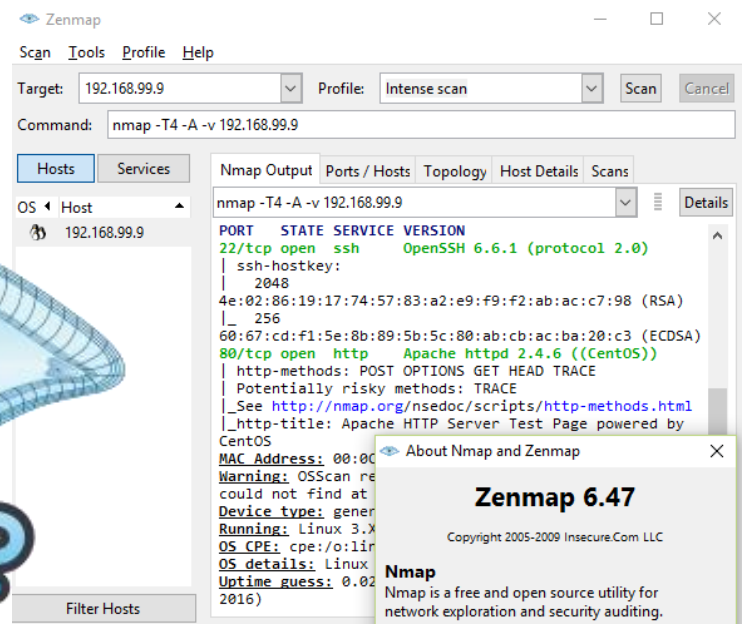
TELNET **SSH**

Scanning Tools

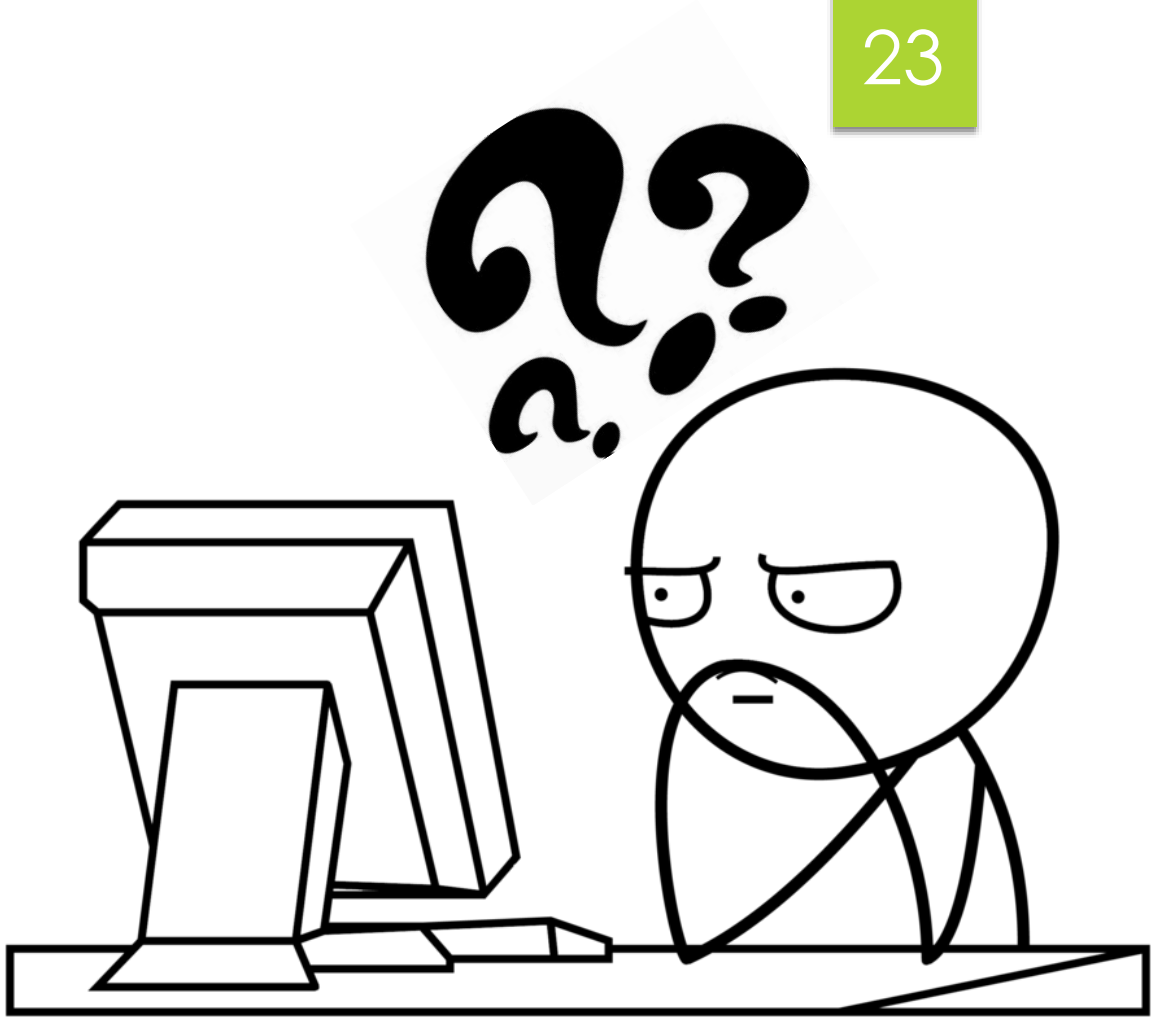
SoftPerfect Network Scanner



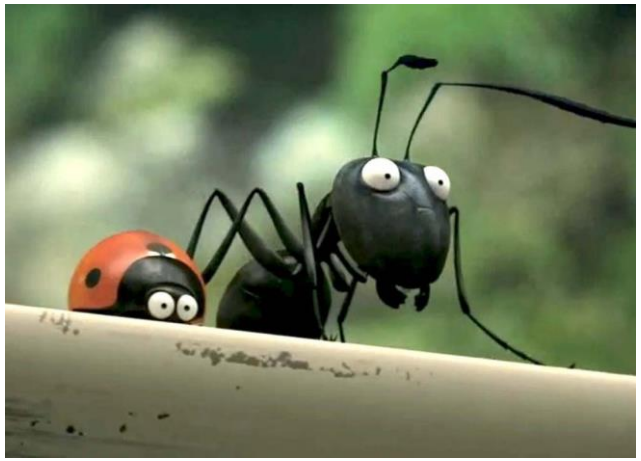
The Dude



How to fools them?



Use a bait



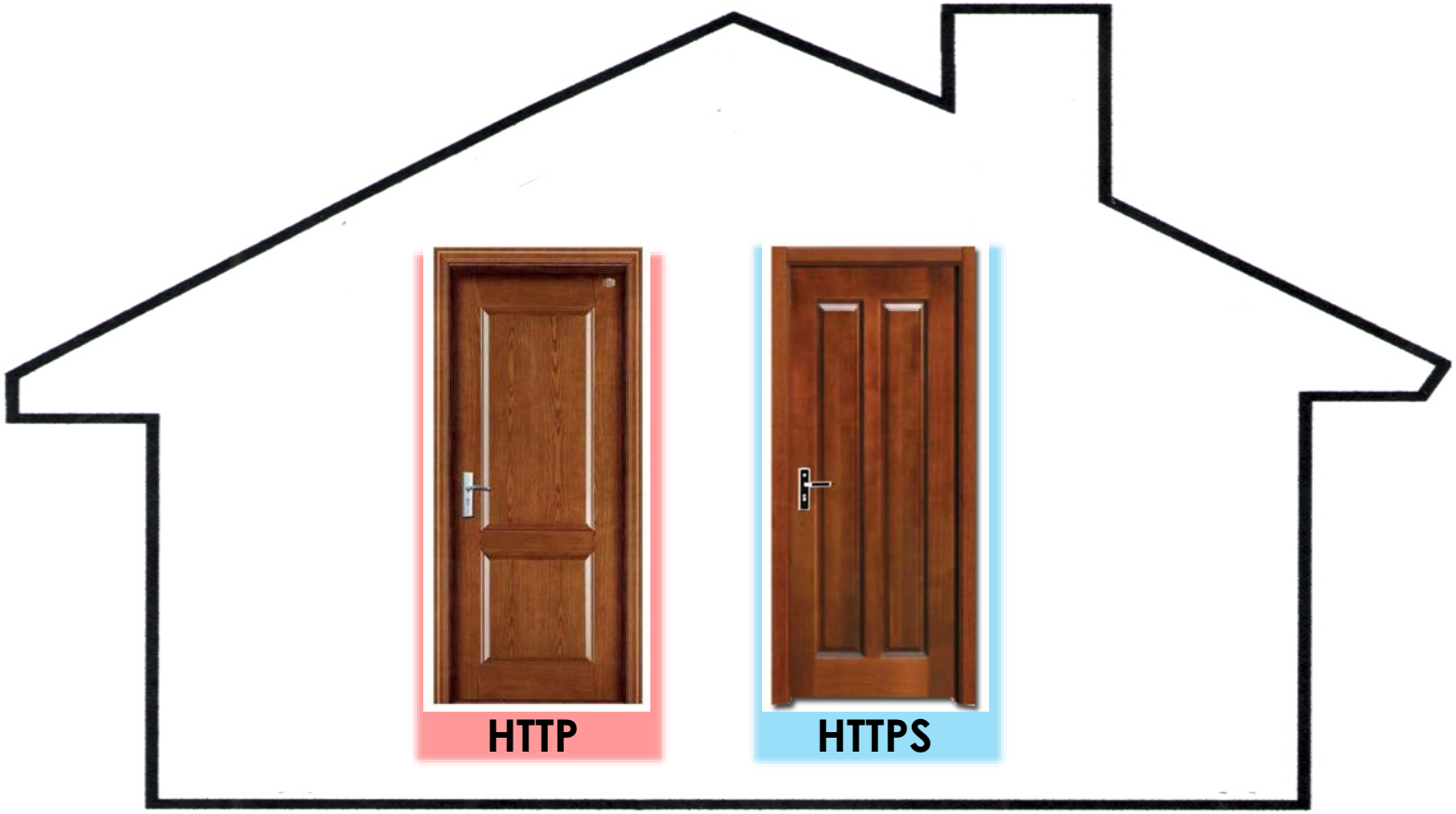
Hacker

Honey Pot

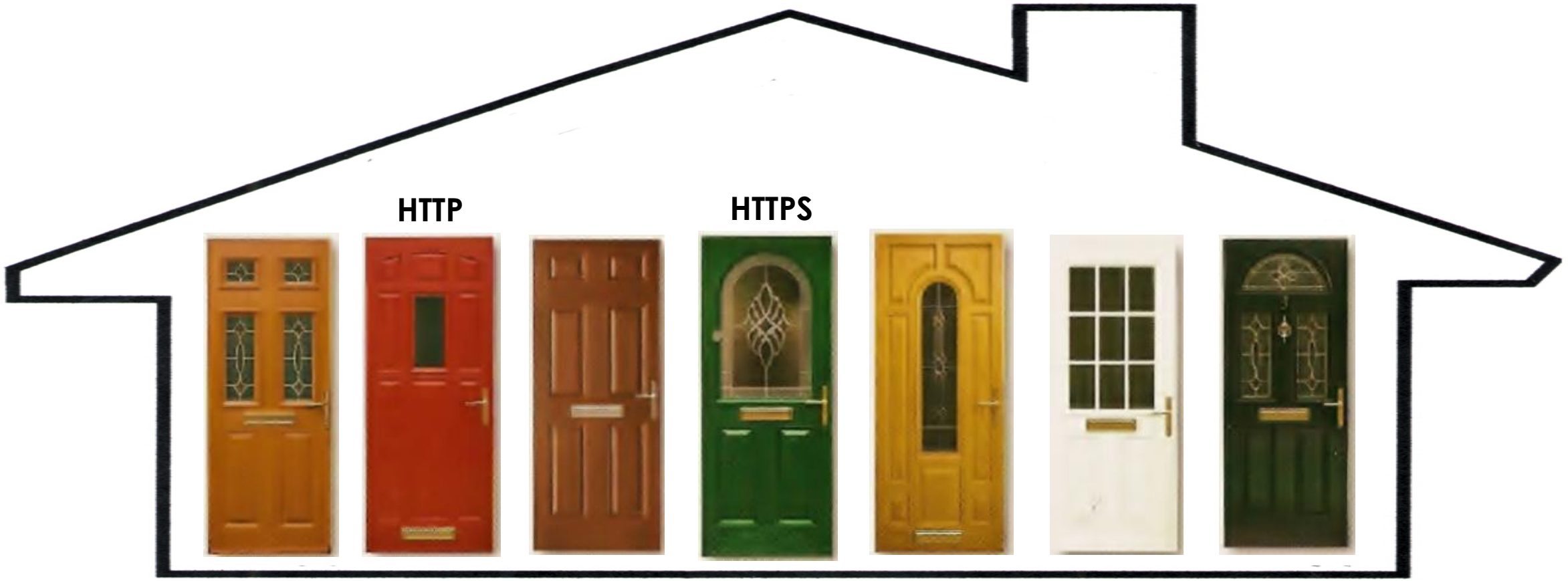
Web Server Example

Web Server

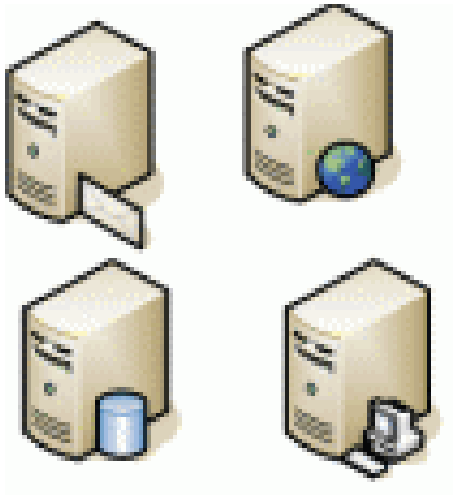
=



Confuse your enemy



Server Farm Network Example

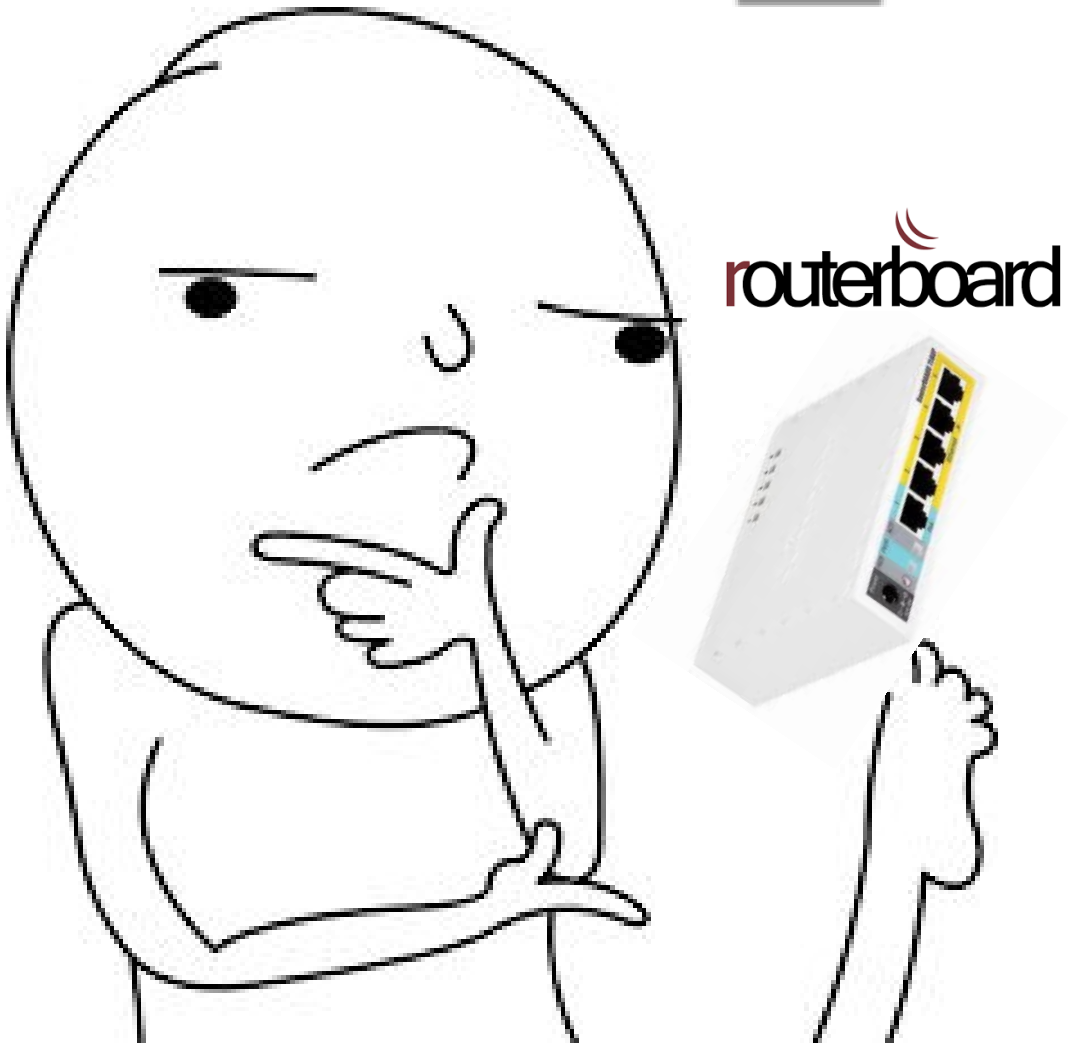


192.168.1.2 → DNS Server
192.168.1.5 → Web Server
192.168.1.10 → DB Server
192.168.1.15 → Mail Server

Confuse your enemy

192.168.1.1 → Fake Server 1
192.168.1.2 → DNS Server
192.168.1.3 → Fake Server 2
192.168.1.4 → Fake Server 3
192.168.1.5 → Web Server
192.168.1.6 → Fake Server 4
192.168.1.7 → Fake Server 5
192.168.1.8 → Fake Server 6
192.168.1.9 → Fake Server 7
192.168.1.10 → DB Server
192.168.1.11 → Fake Server 8
192.168.1.12 → Fake Server 9
192.168.1.13 → Fake Server 10
192.168.1.14 → Fake Server 11
192.168.1.15 → Mail Server

How we do it with Mikrotik?



NAT
(Network Address Translation)

Fake NAT

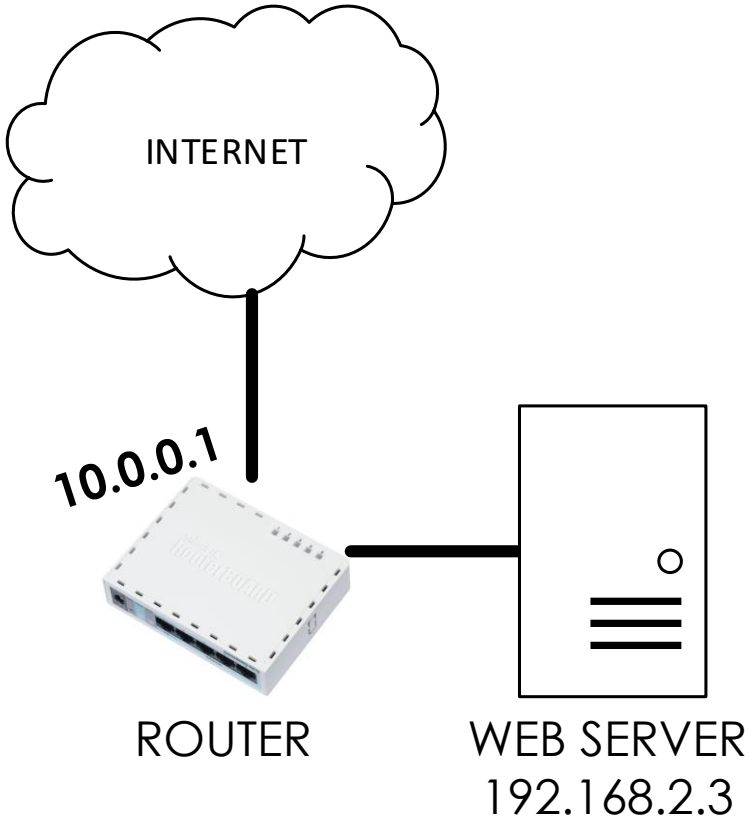
Fake Ports at your Web Server

HTTP & HTTPS to Legitimate Server

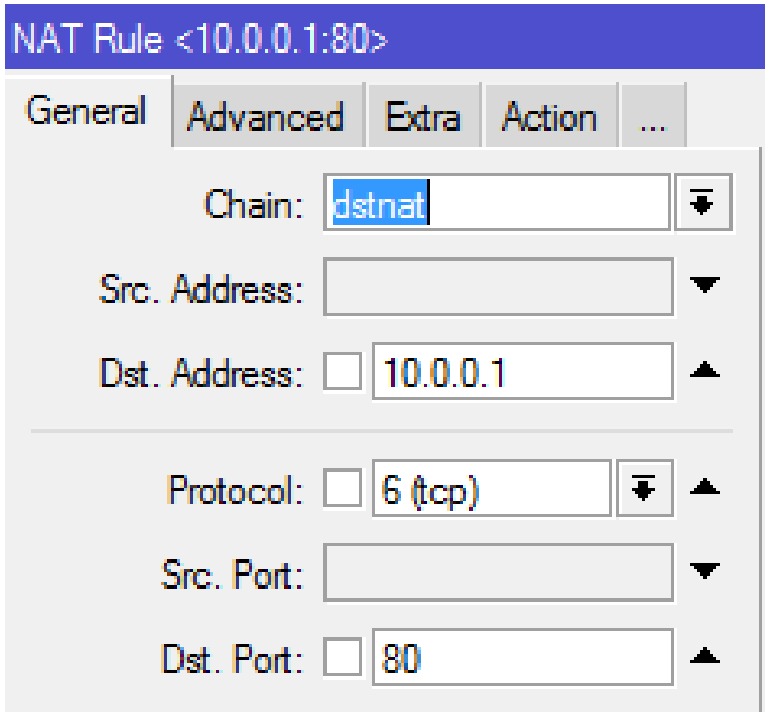
Other Ports to Fake Server

Didiet Kusumadihardja - didiet@arch.web.id

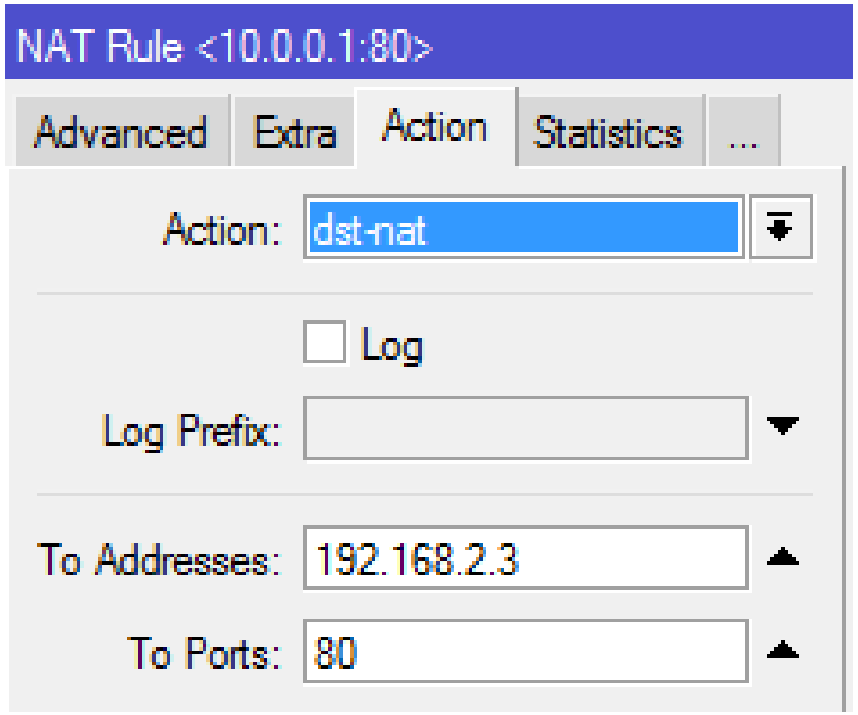
Simple NAT for Web Server



NAT (Port Mapping)



Chain



Action

Add Additional NAT for Bait

NAT Rule <10.0.0.1> **Chain**

General | Advanced | Extra | Action | ...

Chain: dstnat

Src. Address:

Dst. Address: 10.0.0.1

Protocol:

Src. Port:

Dst. Port:

NAT Rule <10.0.0.1> **Action**

Advanced | Extra | Action | Statistics | ...

Action: dst-nat

Log

Log Prefix:

To Addresses: 192.168.2.4

To Ports:

Web Server
192.168.2.3

Fake Server
(Honey Pot)
192.168.2.4

#		Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	To Addresses	To Ports	Bytes	Packets
;;; Real Web Server												
0		dst-nat	dstnat		10.0.0.1	6 (tcp)		80	192.168.2.3	80	916 B	18
;;; Fake Server (Honey Pot)												
1		dst-nat	dstnat		10.0.0.1				192.168.2.4		0 B	0

Fake Server at your Server Farm Network

Only one legitimate server

Others are Fake Server

Another Example

NAT Rule <10.0.0.0/24> **Chain**

General | Advanced | Extra | Action | ...

Chain: dstnat

Src. Address:

Dst. Address: 10.0.0.0/24

Protocol:

Src. Port:

Dst. Port:

NAT Rule <10.0.0.0/24> **Action**

Advanced | Extra | Action | Statistics | ...

Action: dst-nat

Log

Log Prefix:

To Addresses: 192.168.2.4

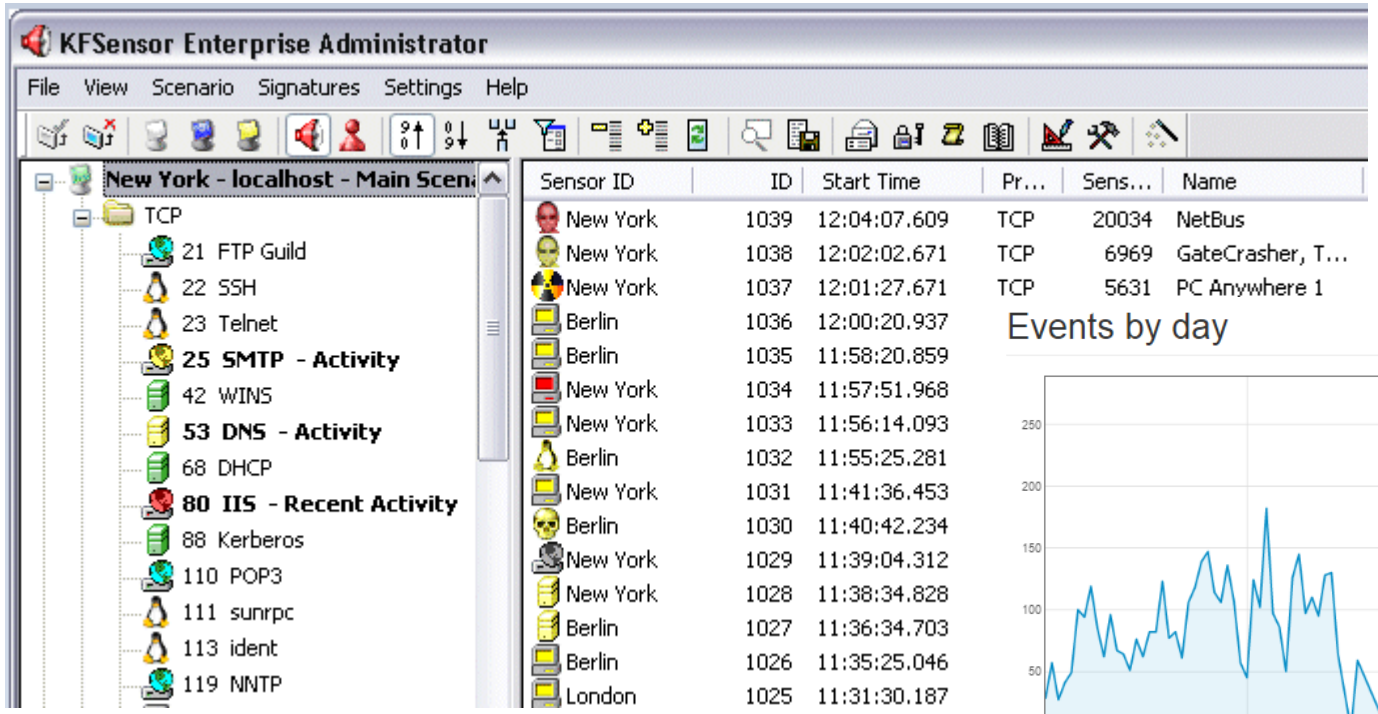
To Ports:

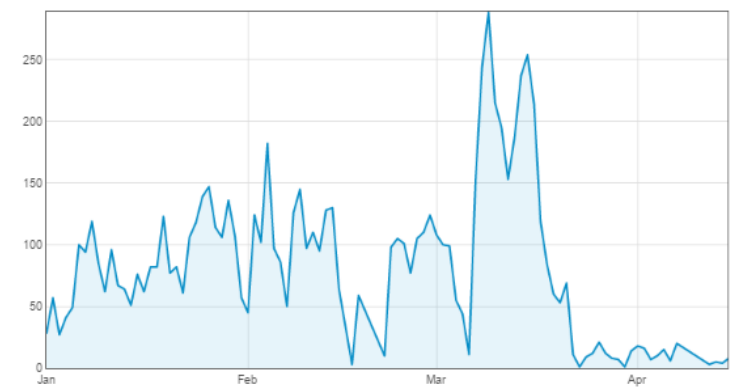
Web Server
192.168.2.3

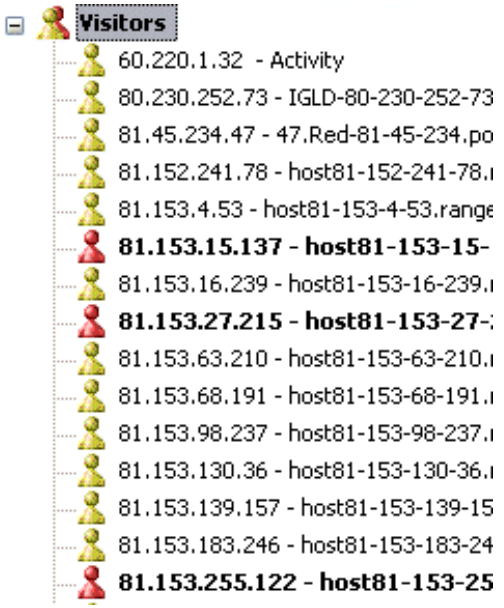
Fake Server
(Honey Pot)
192.168.2.4

#		Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	To Addresses	To Ports	Bytes	Packets
;;; Real Web Server												
0		dst-nat	dstnat		10.0.0.1	6 (tcp)		80	192.168.2.3	80	2588 B	49
;;; Fake Server (Honey Pot)												
1		dst-nat	dstnat		10.0.0.0/24				192.168.2.4		0 B	0

Combine with Honey Pot







KFSensor

Others HoneyPot: Honeyd, Kippo, Dionaea, Nepenthes

What Hacker See (NMAP)

Nmap / Zenmap

Nmap Output | Ports / Hosts | Topology | Host Details | Scans

Port	Protocol	State	Service	Version
22	tcp	open	ssh	OpenSSH 6.6.1 (protocol 2.0)
80	tcp	open	http	Apache httpd 2.4.6 ((CentOS))

Before

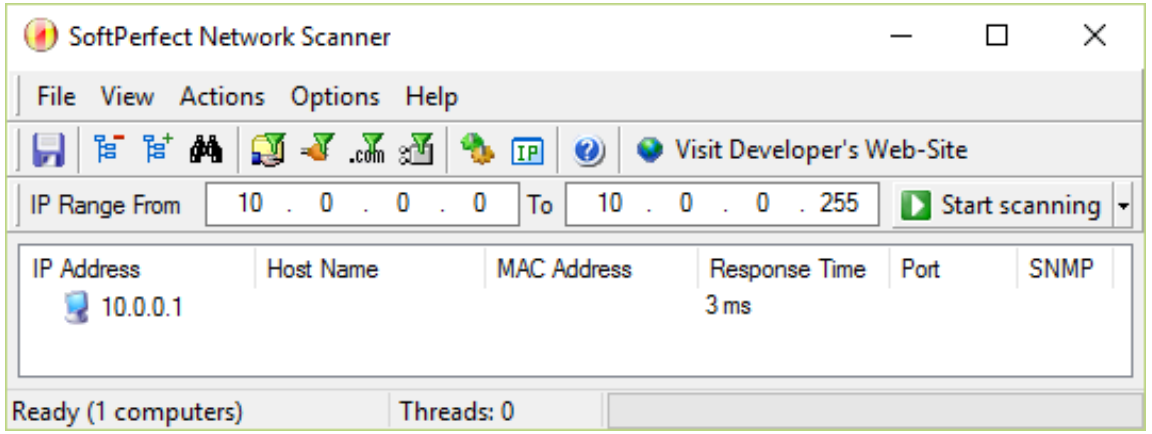
Nmap Output | Ports / Hosts | Topology | Host Details | Scans

Port	Protocol	State	Service	Version
22	tcp	open	tcpwrapped	
23	tcp	open	tcpwrapped	
25	tcp	open	tcpwrapped	
42	tcp	open	tcpwrapped	
53	tcp	open	tcpwrapped	
80	tcp	open	http	Apache httpd 2.4.6 ((CentOS))
81	tcp	open	tcpwrapped	
82	tcp	open	tcpwrapped	
83	tcp	open	tcpwrapped	
110	tcp	open	tcpwrapped	
111	tcp	open	tcpwrapped	
113	tcp	open	tcpwrapped	
119	tcp	open	tcpwrapped	
135	tcp	open	msrpc	Microsoft Windows RPC

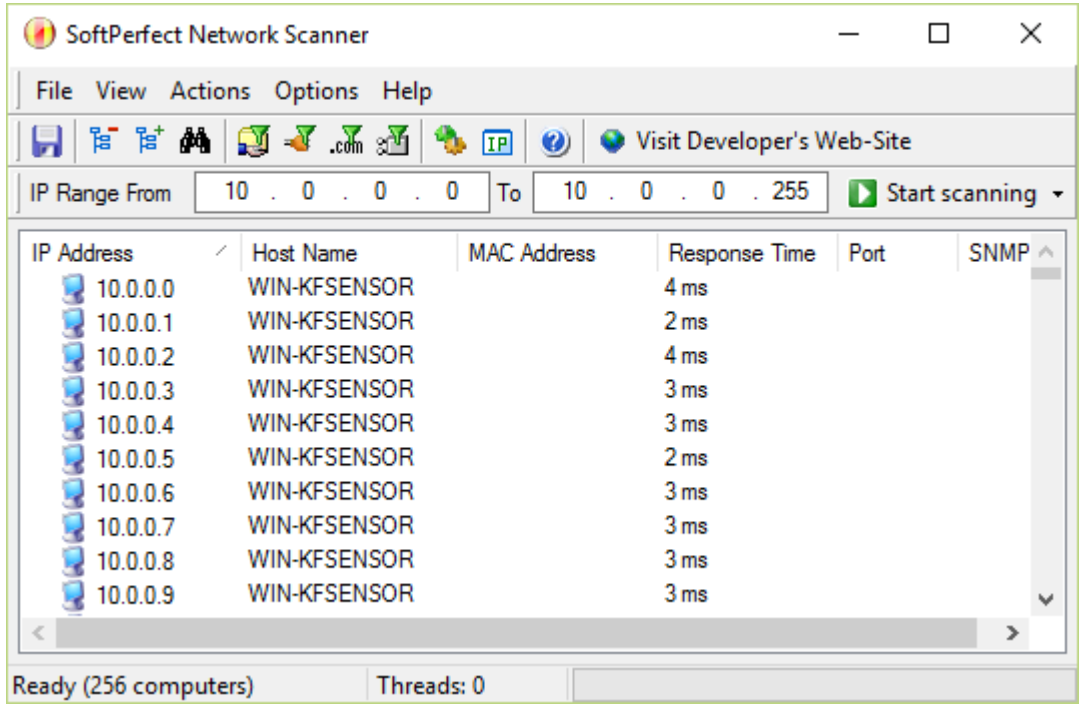
After

What Hacker See (SoftPerfect NetScan)

SoftPerfect Network Scanner



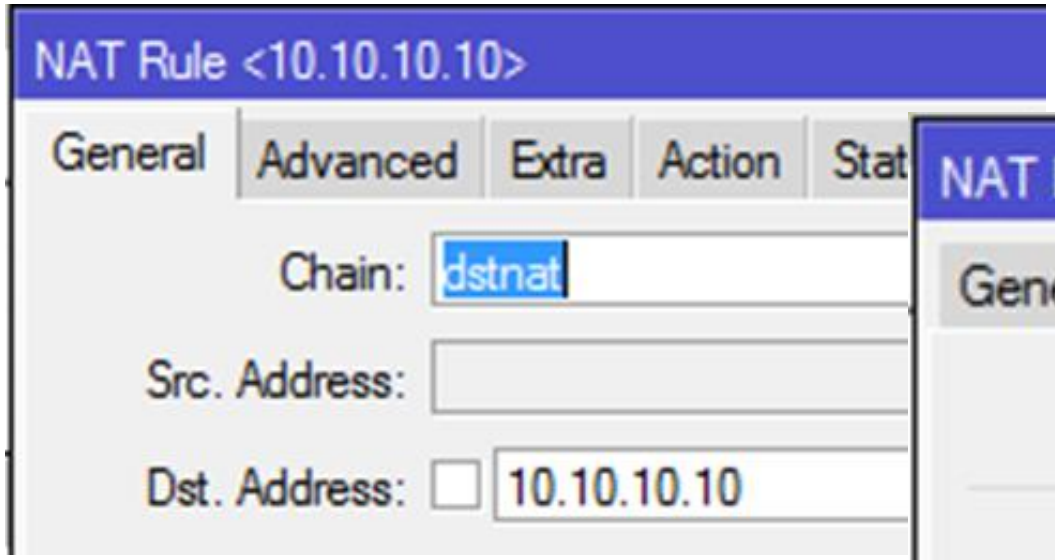
Before



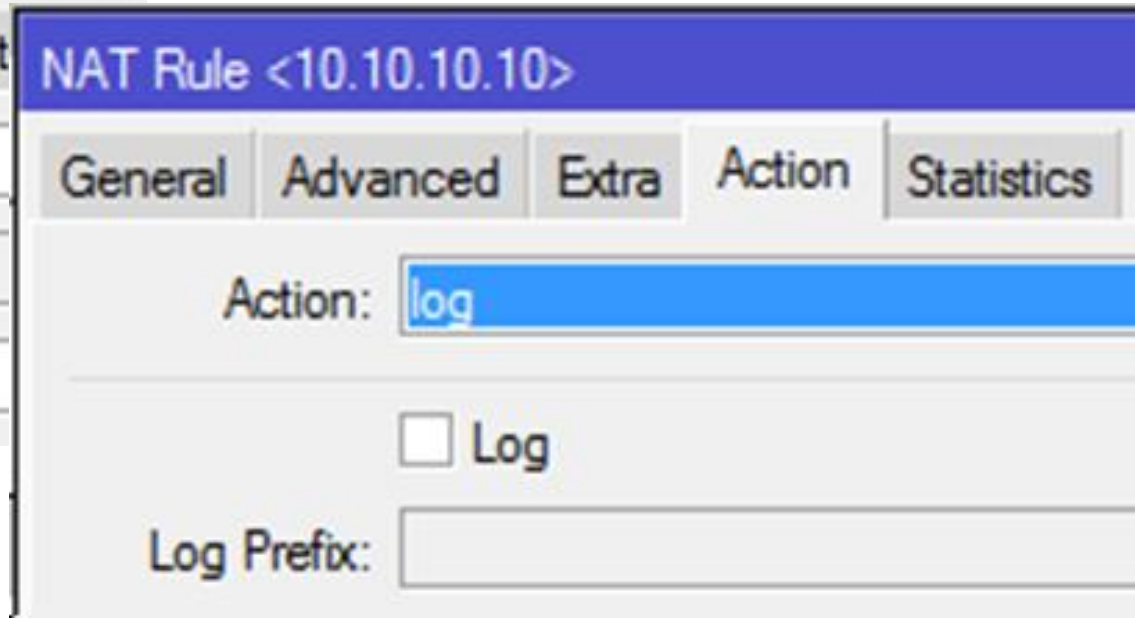
After

I don't want to use HoneyPot

Step 1: Chain



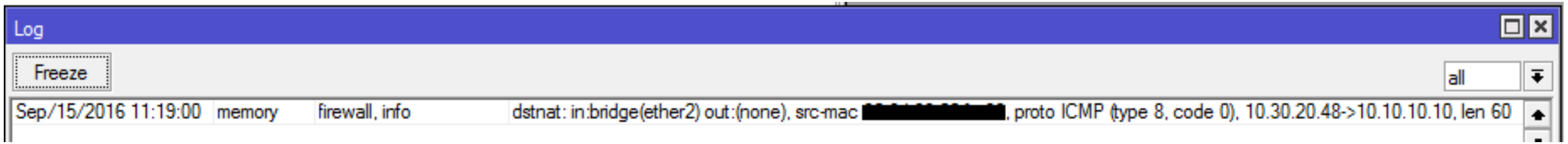
Step 2: Action



What we see, If someone PING

```
>ping 10.10.10.10
Pinging 10.10.10.10 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.10.10.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```



SRC-MAC ADDRESS
SRC-IP ADDRESS

What we see, If someone NMAP

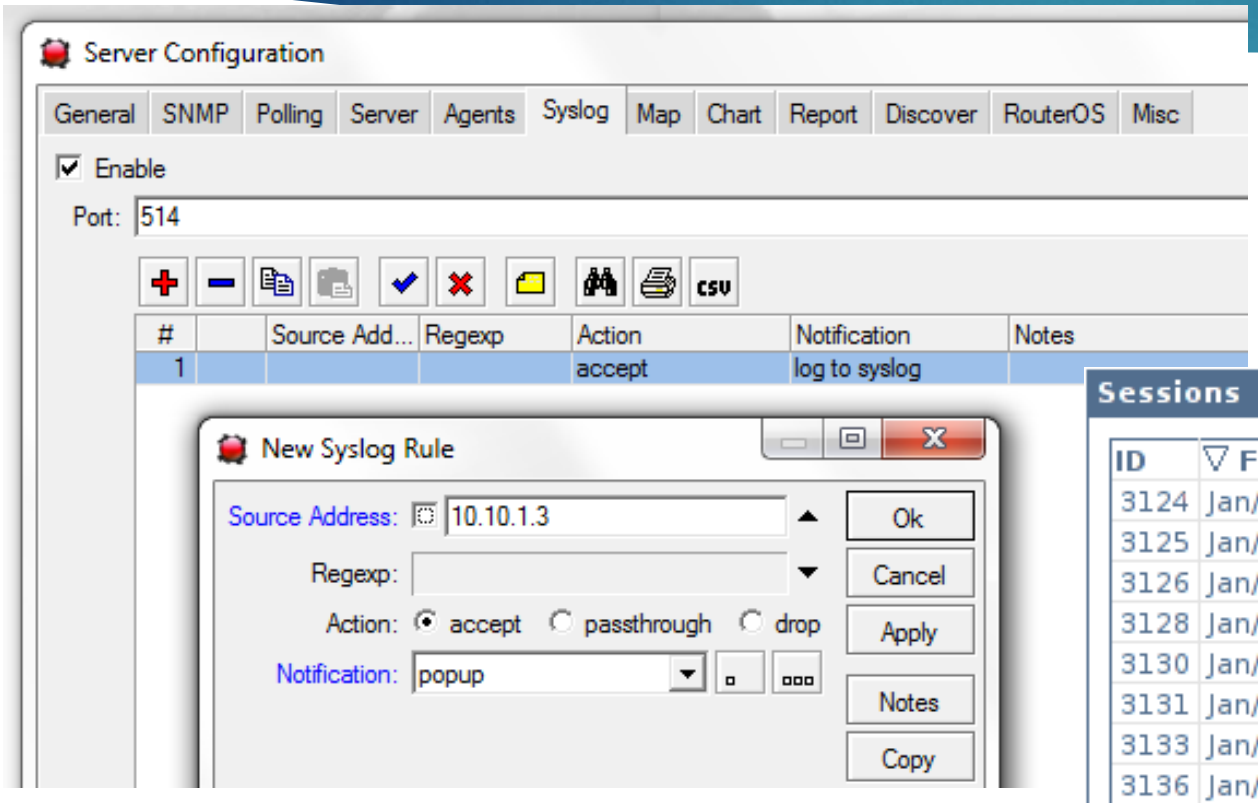
nmap -T4 -A -v 10.10.10.10 Details

```
Starting Nmap 6.47 ( http://nmap.org ) at 2016-09-15
11:12 SE Asia Standard Time
NSE: Loaded 118 scripts for scanning.
NSE: Script Pre-scanning.
Initiating Ping Scan at 11:12
Scanning 10.10.10.10 [4 ports]
Completed Ping Scan at 11:12, 2.46s elapsed (1 total
hosts)
Nmap scan report for 10.10.10.10 [host down]
mass_dns: warning: Unable to determine any DNS servers.
Reverse DNS is disabled. Try using --system-dns or
specify valid servers with --dns-servers
NSE: Script Post-scanning.
Read data files from: C:\Program Files (x86)\Nmap
Note: Host seems down. If it is really up, but blocking
our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 56.39
seconds
           Raw packets sent: 8 (304B) | Rcvd: 0 (0B)
```

Mikrotik LOG:

```
proto ICMP (type 8, code 0), 10.30.20.48->10.10.10.10, len 28
proto TCP (SYN), 10.30.20.48:33447->10.10.10.10:443, len 44
proto TCP (ACK), 10.30.20.48:33447->10.10.10.10:80, len 40
proto ICMP (type 13, code 0), 10.30.20.48->10.10.10.10, len 40
proto ICMP (type 13, code 0), 10.30.20.48->10.10.10.10, len 40
proto TCP (ACK), 10.30.20.48:33448->10.10.10.10:80, len 40
proto TCP (SYN), 10.30.20.48:33448->10.10.10.10:443, len 44
proto ICMP (type 8, code 0), 10.30.20.48->10.10.10.10, len 28
```

The Dude, Hotspot & Userman



MikroTik
RouterOS User Manager

Sessions

ID	From Time	Till Time	Uptime	Download	Upload
3124	Jan/18/2006 17:15:36	Jan/18/2006 17:15:40	4s	3.6 KiB	1235 B
3125	Jan/18/2006 17:15:57	Jan/18/2006 17:16:36	38s	13.9 KiB	7.5 KiB
3126	Jan/18/2006 17:16:41	Jan/18/2006 17:23:45	7m:4s	61.9 KiB	38.6 KiB
3128	Jan/18/2006 17:21:07	Jan/18/2006 17:23:45	2m:37s	61.8 KiB	34.9 KiB
3130	Jan/18/2006 17:29:56	Jan/18/2006 17:32:01	2m:5s	5.5 KiB	1844 B
3131	Jan/18/2006 17:34:24	Jan/18/2006 17:36:51	2m:26s	108.4 KiB	59.5 KiB
3133	Jan/18/2006 17:37:09	Jan/18/2006 17:38:21	1m:12s	91.1 KiB	18.0 KiB
3136	Jan/18/2006 18:08:58	Jan/18/2006 18:25:31	16m:34s	596.0 KiB	545.0 KiB

IP Address → MAC Address → User ID → Person

Use Case 1

Internet Café (WARNET)

Insider Threat

University

Office

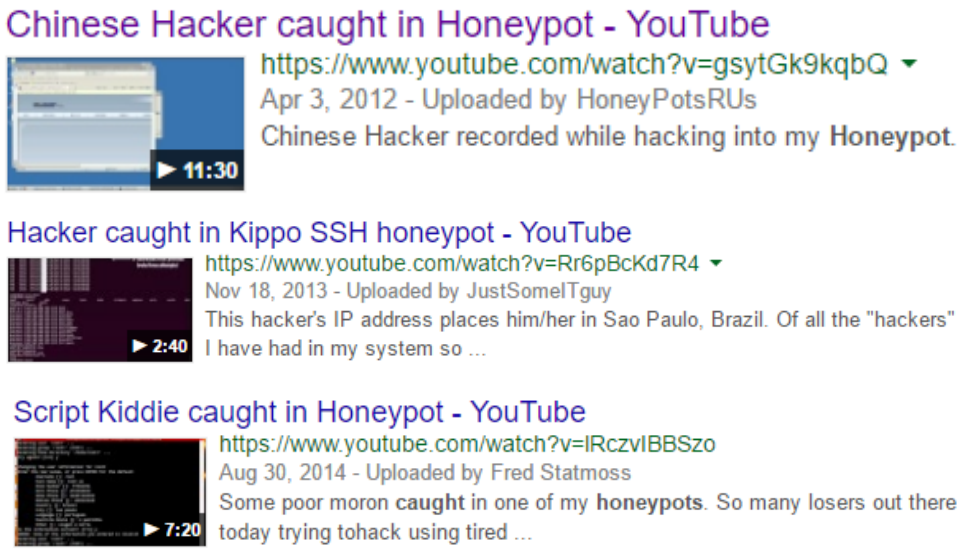
Use Case 2

http://public.honeynet.id

Analytics

(Low Interaction Honeypot)

Research



~~**For Fun**~~

Learn hacking method from hacker / script kiddies

(High Interaction Honeypot)

Thank you

.

.

Question?

mitra solusi telematika

Arch NETWORKS

DIDIET KUSUMADIHARDJA

didiet@arch.web.id
http://didiet.arch.web.id/
https://www.facebook.com/ArchNetID/