ID-Networkers
from engineer to engineer

MikroTik

Reactive Intrusion Detecting System

Rofiq Fauzi, MTCNA, MTCRE, MTCWE, MTCINE, Certified Trainer
www.id-networkers.com
www.training-mikrotik.com

About Us

- Using MikroTik (v.2.97) since 2005, as Network Engineer at WISP company.
- 2007, Network & Wireless Engineer at INDOSAT (Internet Network Provider Division).
- 2008, IT & Telco Procurement (Procurement Group) at INDOSAT
- 2012, MikroTik Certified Trainer (MTCNA, MTCRE, MTCWE, MTCINE, Certified Trainer) at ID-Networkers.

ID Networkers

Trainer	CCNA	CCNP	CCIP	CCIE	JNCIA	JNCIS	JNCIP	JNCIE	MTCNA	MTCRE	MTCTCE	MTCWE	MTCINE	Mikrotik Certified trainer
Dedi Gunawan	V	V	V	V					V	V	V			
Rofiq Fauzi									V	V		V	V	V
M. Amin					V	V	V	V						
Hadi Subowo	V		V						V					
Albertus Danar W	V				V	V								

Objective

- To make us aware the importance of MikroTik security risk.
- Make easy to monitoring & securing our MikroTik network.
- To built intrusion detecting system by our self in mikrotik box.

Background

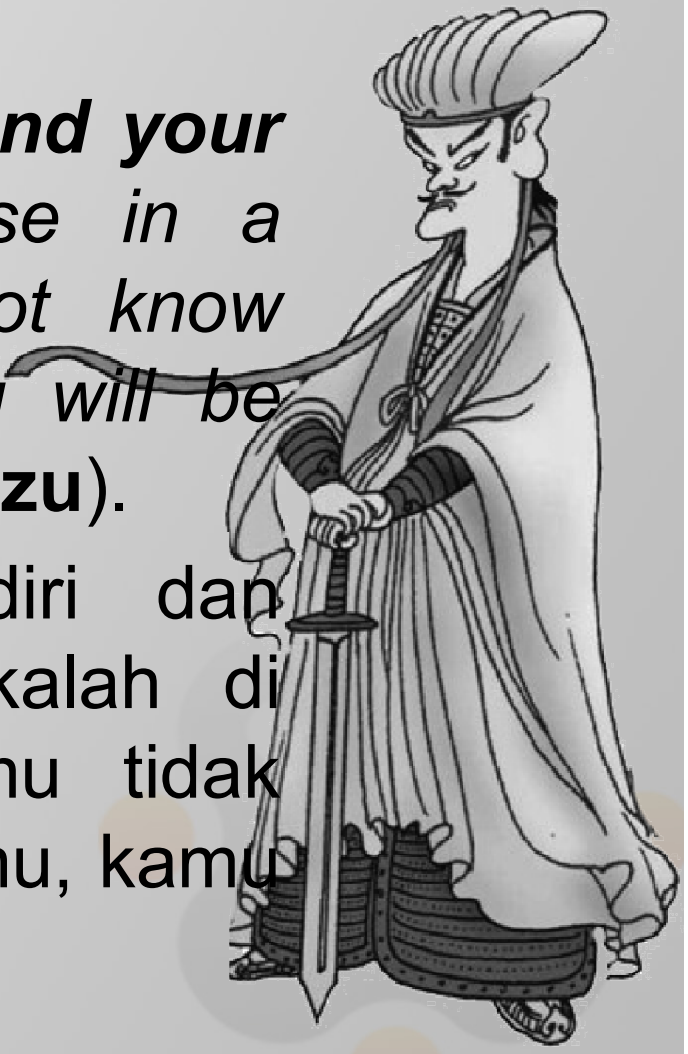
- Admin can not always monitor the servers directly or always login in to check the servers for intruder.
- We need firewall not just to blocking intruder, but also log and report them to admin immediately.
- In wide network with many MikroTik router, we don't know which is under attack.
- We can report the to the IP owner of the intruders as abuse.

What is IDS

- **IDS (Intrusion Detecting System):** system that can detect intrusion, it is like the alarm system
- **Intrusion:** activities that are anomalies, incorrect, inappropriate occurring on the network or host

Know the Attack

- *If you **know both of yourself and your enemies**, you will not be lose in a hundred battles. If you do not know yourself nor your enemies, you will be lose in every single battle.* (**Sun Tzu**).
- Jika kamu tahu dirimu sendiri dan musuhmu, kamu tidak akan kalah di ratusan pertempuran, jika kamu tidak tahu dirimu sendiri serta musuhmu, kamu akan kalah disetiap pertempuran



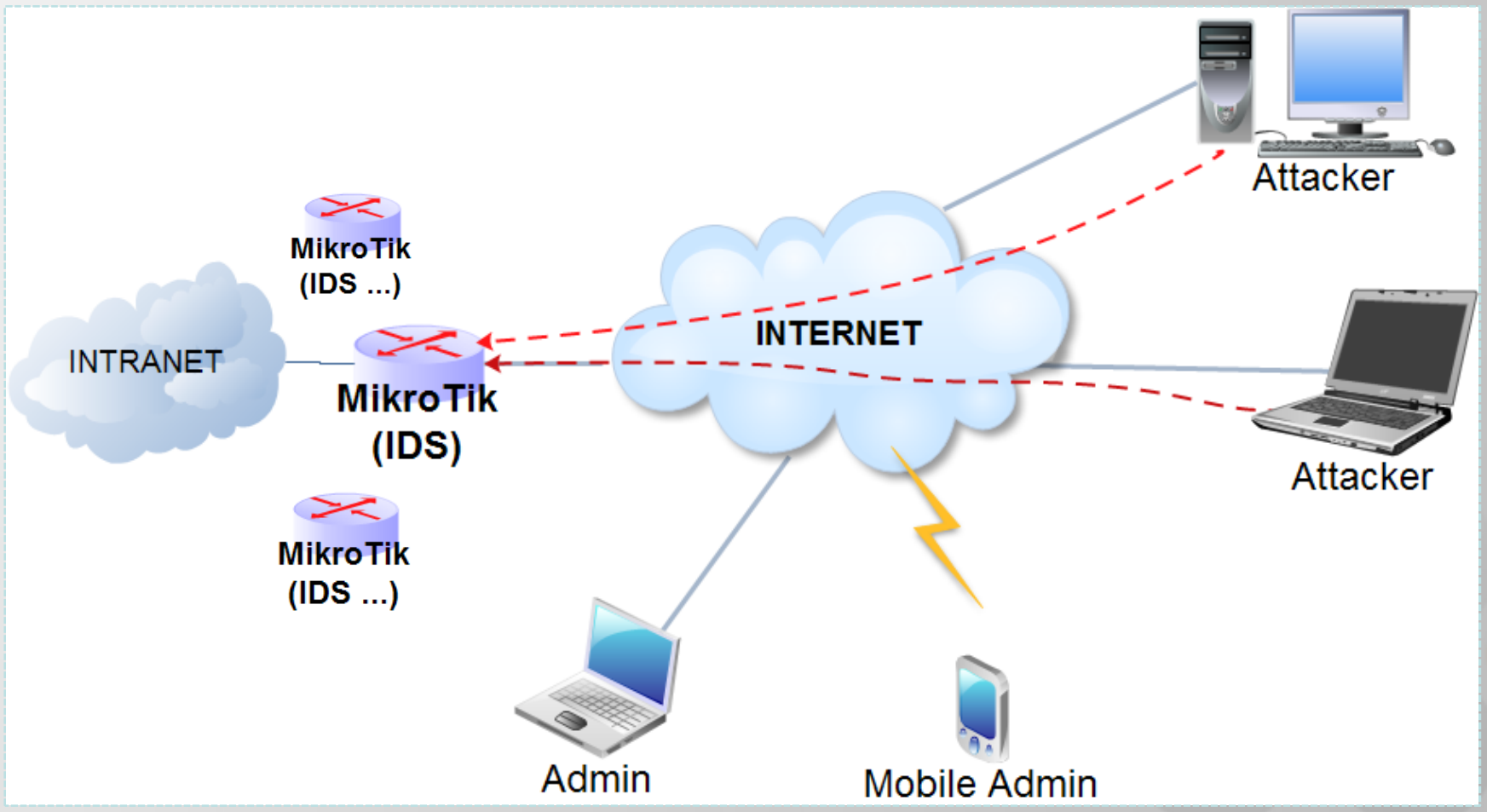
How To Know The Attack

- System Logging
- Tool Torch
- Packet Sniffer

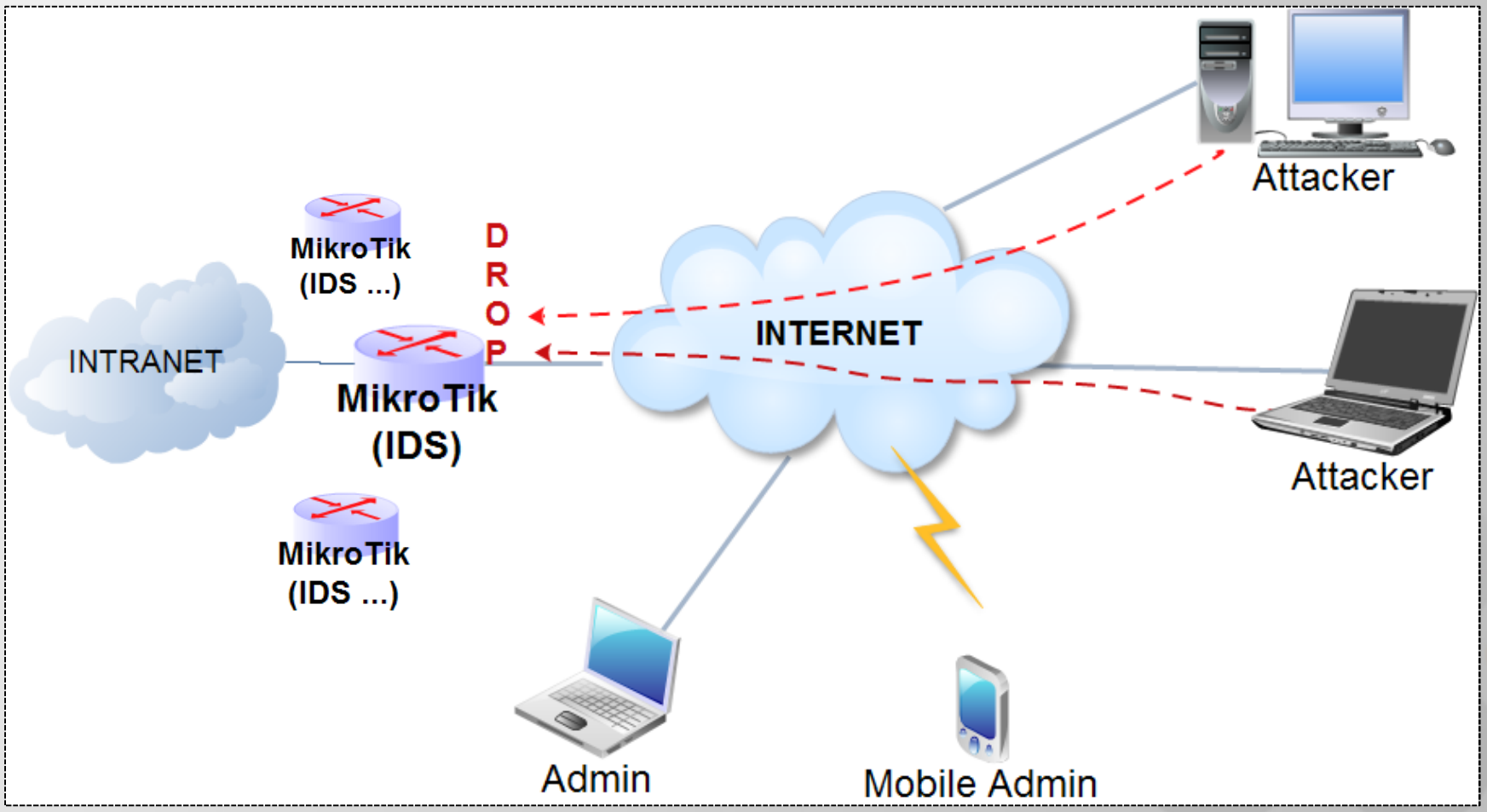
How IDS Work

- **Passive System**
  - ✓sensor detects a potential security breach
  - ✓logs the information
  - ✓alert on the console
- **Reactive System**
  - ✓Like **Passive Syste,** but plus:
  - ✓auto-responds (resetting the connection or drop the traffic) from intruders
  - ✓Send the report to admin

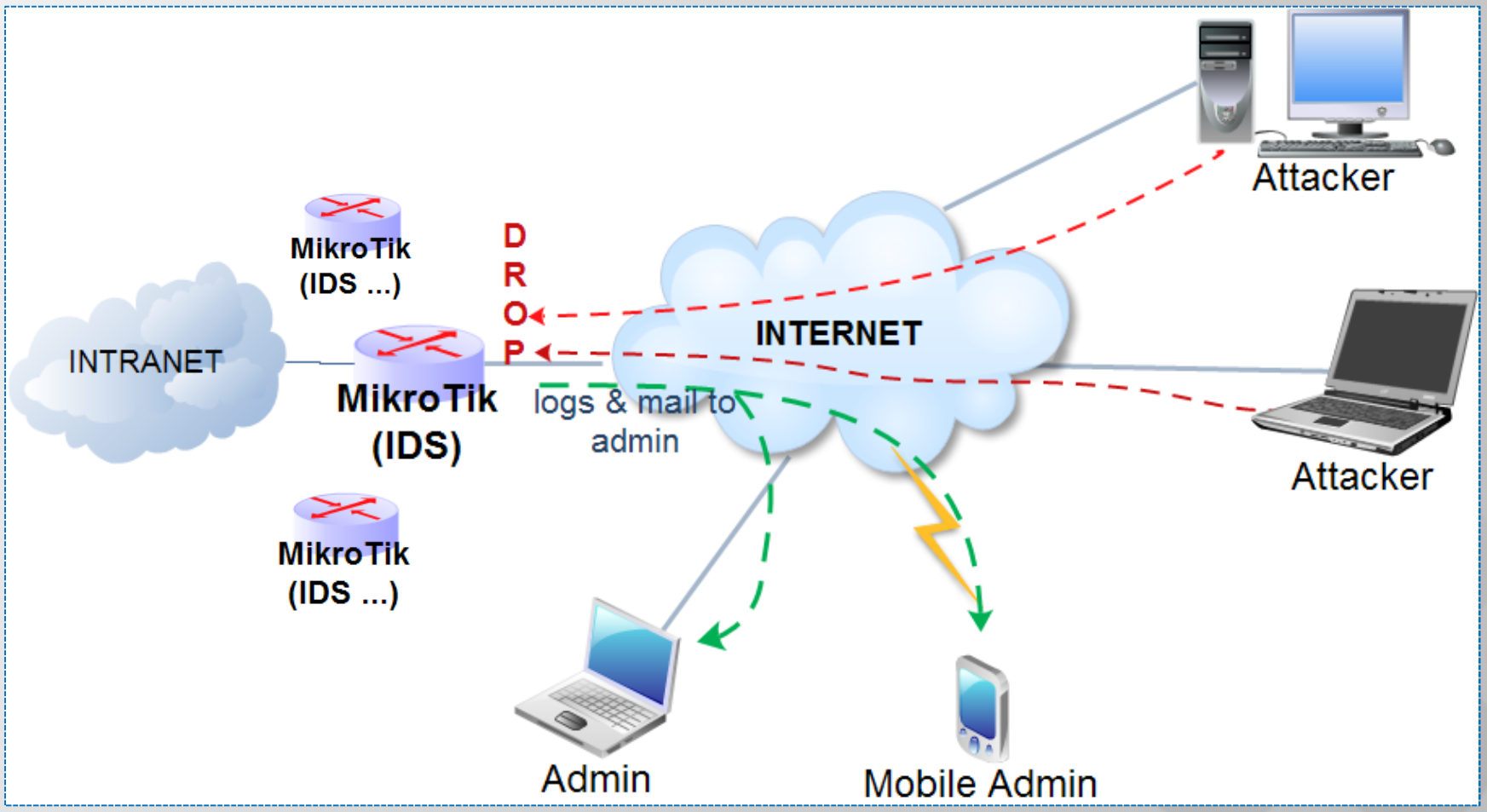
Attack Process



Drop by IP>Firewall

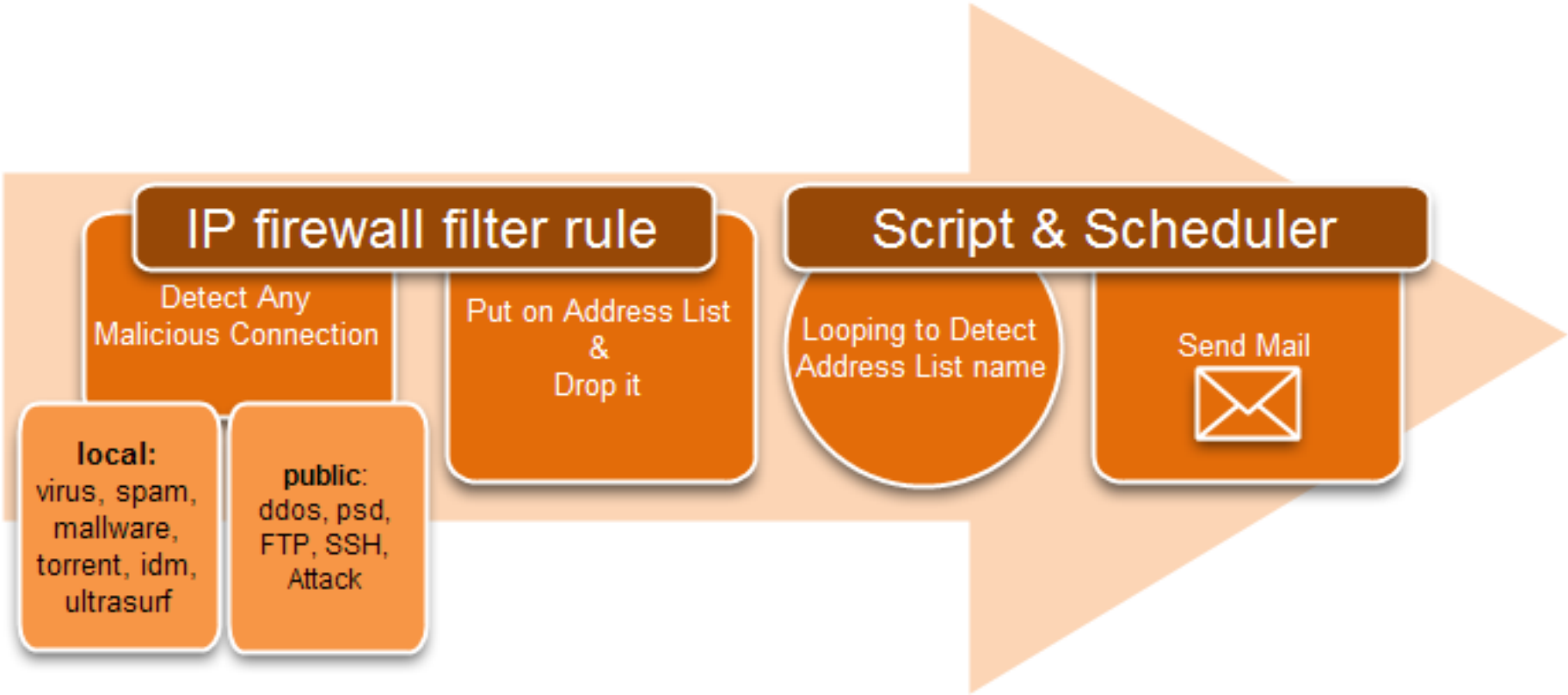


Logging & Mail Report



IDS on RouterOS Work Flow

We can use it to any malicious connection either from Public or local connection like a virus, spam, malware



Malicious Connection

Kind of Malicious Connection

- From outside:

  Port Scanning, Brute Force, DDoS attack

- From inside:

  Virus, Peer to Peer Connection, Ilegal Tunneling (utrasurf), Anonymous Proxy, Internet Download manager, url filtered.

Simulation

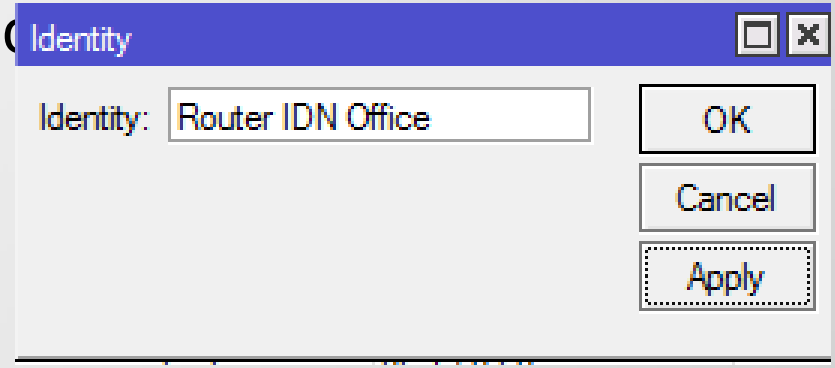
We want simulation with the following points:

- MikroTik (I am using RB 751)
  as IDS machine
- Attacker (my laptop)
  it will attack the MikroTik with different method
- Email Account
  there are 1 email for smtp relay and some mail as mail of administrator.

MikroTik Configuration

Router Identity

Pada menu **/system identity**, set the router name, ex :



Why we must set the router id?

- If we have many router, which one is being attacked.
- Because router identity will be sent by mail to admin.

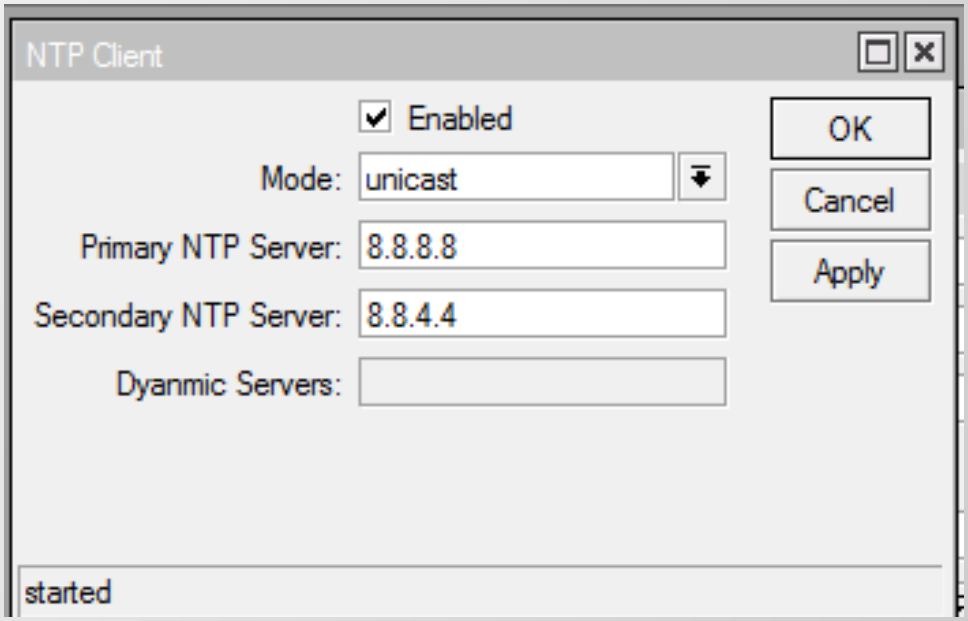
NTP Client

- Network Time Protocol is the protocol to synchronize the clock between router with other router or server
- We need NTP to get valid date and time to know exactly when the attack occurred.
- We can use The **NTP Public Services**, like www.ntp.org or google public NTP IP address 8.8.8.8 or 8.8.4.4

MikroTik Configuration

Set primary NTP server to id.pool.ntp.org, if it is set via winbox, it will automatic resolve to an IP address of NTP server.

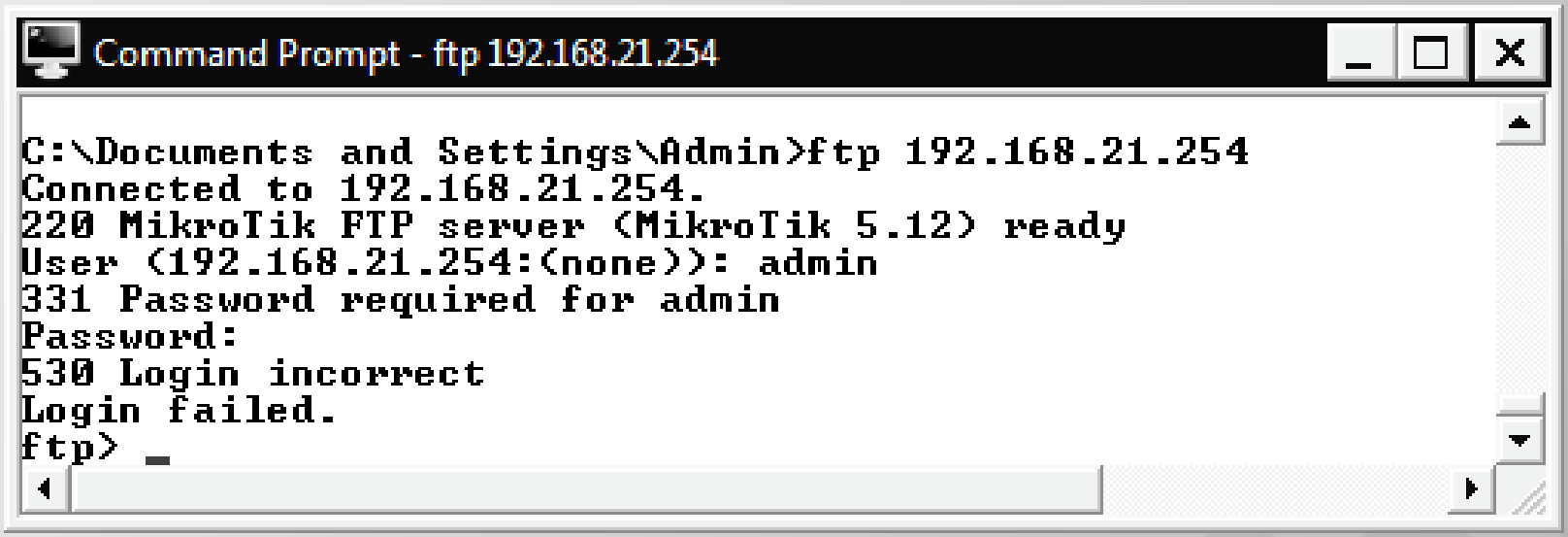
/system ntp client



Wait until bar status of ntp client going to “timeset”

Detecting FTP Brute Force

- Intruder that access our ftp services (port 21) continuously with incorrect username & password.
- Mikrotik routerOS will response FTP incorrect login with sending message " 530 Login Incorrect"



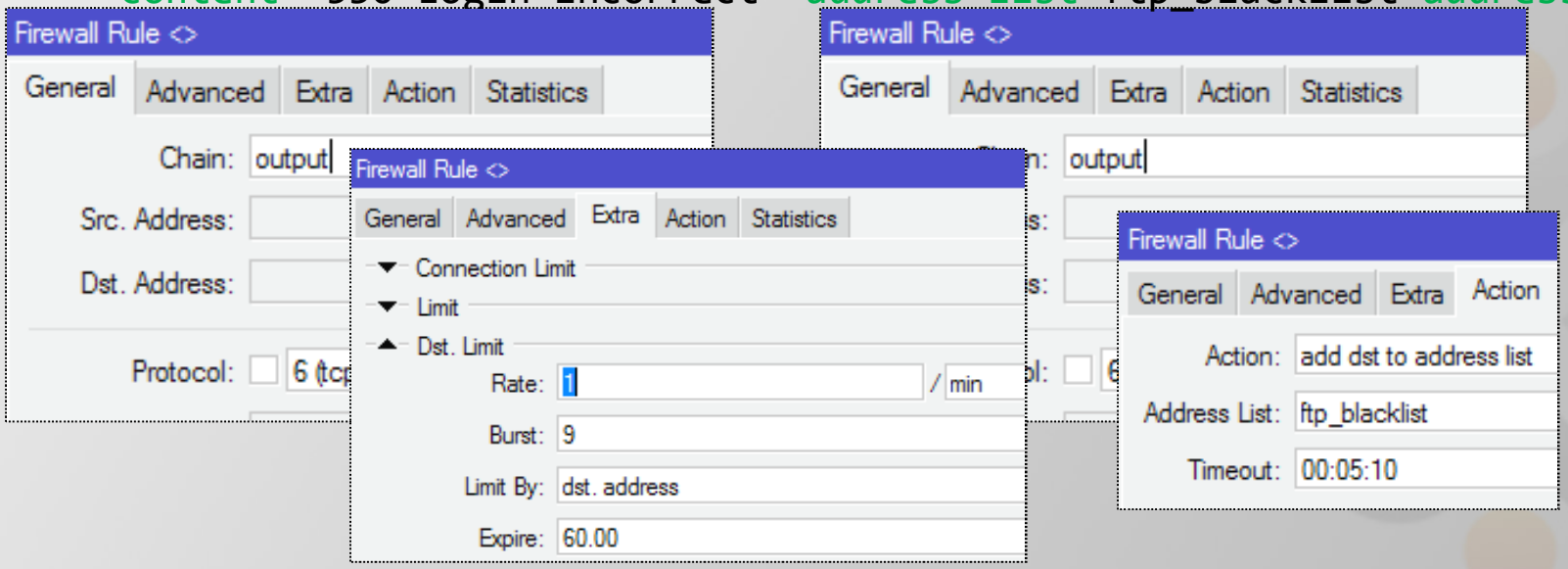
MikroTik Configuration

Configure Firewall to Add Attacker IP address in Address List

in **/ip firewall filter**, add new rule to detect ftp brute force:

allows only 10 FTP login incorrect per minute, others are put on address-list:

```
add chain=output action=accept protocol=tcp content="530 Login
    incorrect" dst-limit=1/1m,9,dst-address/1m
add chain=output action=add-dst-to-address-list protocol=tcp
    content="530 Login incorrect" address-list=ftp_blacklist address-
```

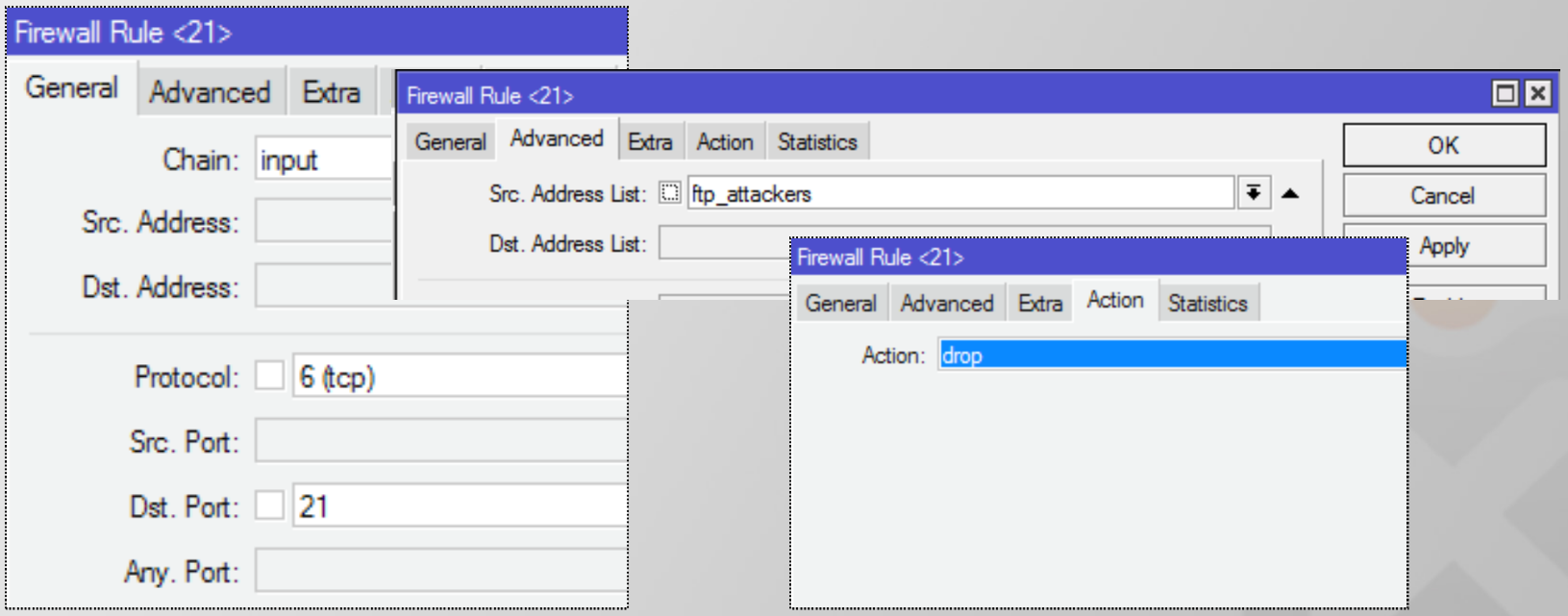


MikroTik Configuration

Configure Firewall to block FTP brute force

in **/ip firewall filter**, rule to drop the ftp attacker in address list:

```
add chain=input protocol=tcp dst-port=21 src-address-list=ftp_blacklist
    action=drop comment="drop ftp brute forcers"
```



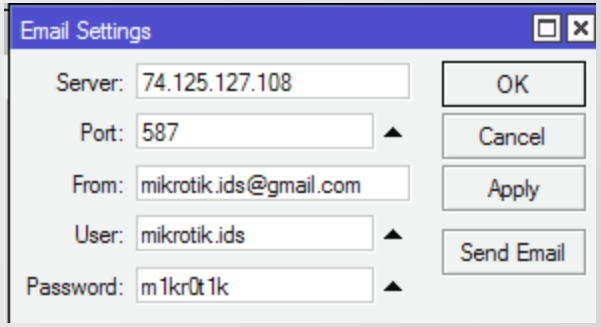
MikroTik Configuration

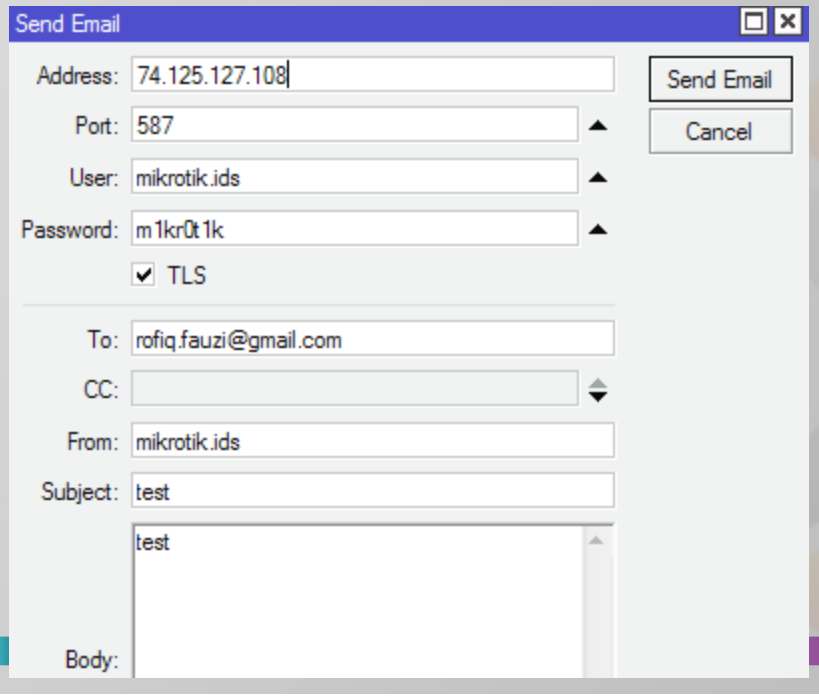
Configure Send e-mail

Create mail account for the smtp relay, In this lab we using Gmail.
In **/tool e-mail** , set the smtp server, username & password

```
set address=74.125.141.108 user=mikrotik.ids password=xxxx
port=587
```

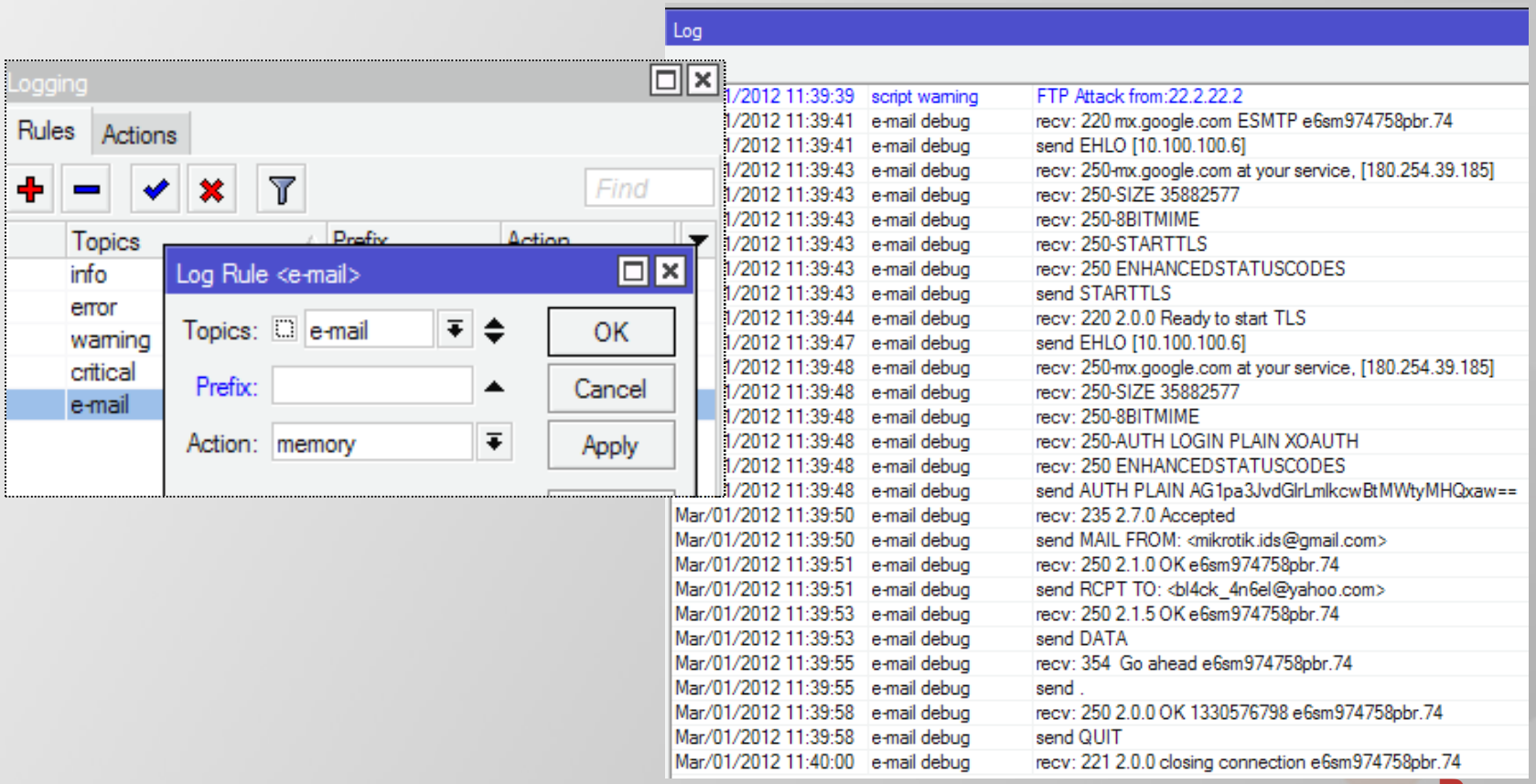
Lets try to send some email to make sure its work





Logging

In **/system log,** add logging for mail topics, Its make us easy to get the log if there are troubleshoot in send mail



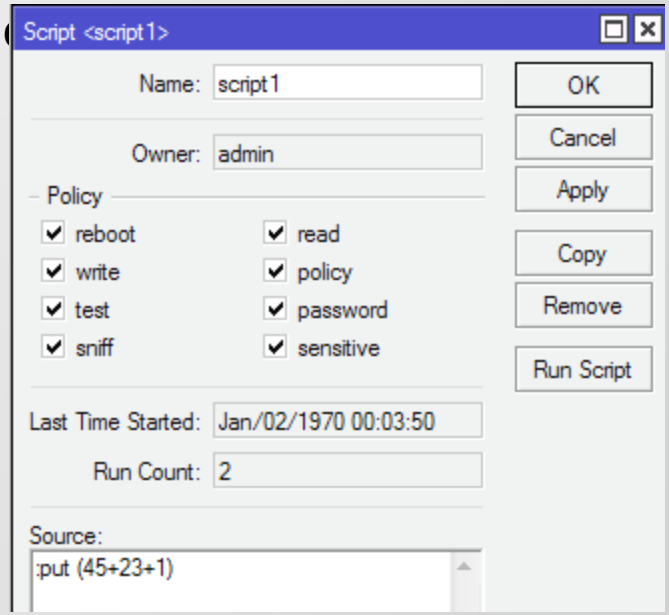
Mikrotik Script

Scripts can be written directly to **console** or can be stored in **Script repository**

- Example script that directly run in console:

```
[admin@MikroTik]>:put(45+23+1)
```

- Script repository (/system script) can be run by running other script, on



MikroTik Configuration

Configuration of the Script

```
name="send_ftp" owner="admin"
policy=ftp,reboot,read,write,policy,test,winbox,password,sniff,sensitive,api
source=
 :foreach a in=[/ip firewall address-list find list=ftp_blacklist] do={
 :local ftpip [/ip firewall address-list get $a address];
 :log warning ("FTP Attack from:" .$ftpip)
 :local sysname [/system identity get name];
 :local date [/system clock get date];
 :local time [/system clock get time];
 /tool e-mail send from="$sysname<mikrotik.ids@gmail.com>" to=rofiq.fauzi@gmail.com
 tls=yes server=74.125.127.108  port=587 password=m1kr0t1k  subject=" FTP Attack!
 body=" Dear Admin,
 \n \n We have note that on $date at $time. There are FTP attack to  sysname from IP
 $ftpip, and has been blocked by firewall.
 \n See http://whois.sc/$ftpip for detail IP attacker information.
 \n \n Thanks & Regard"}
```

Find match address list

Get the IP address

Log it on machine

Get router id, date & time

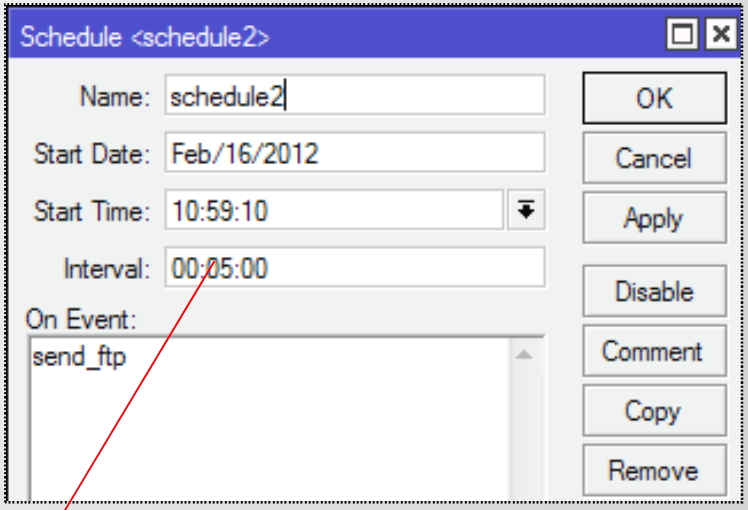
send the report

link to whois.sc, who the IP owner?

MikroTik Configuration

System Schedule

In **/system schedule** add schedule in order to run the scripts within a certain



Interval set to 5m, because the ip address list time out set to 5m 10s, its to ensure that the IP in address-list sent once.

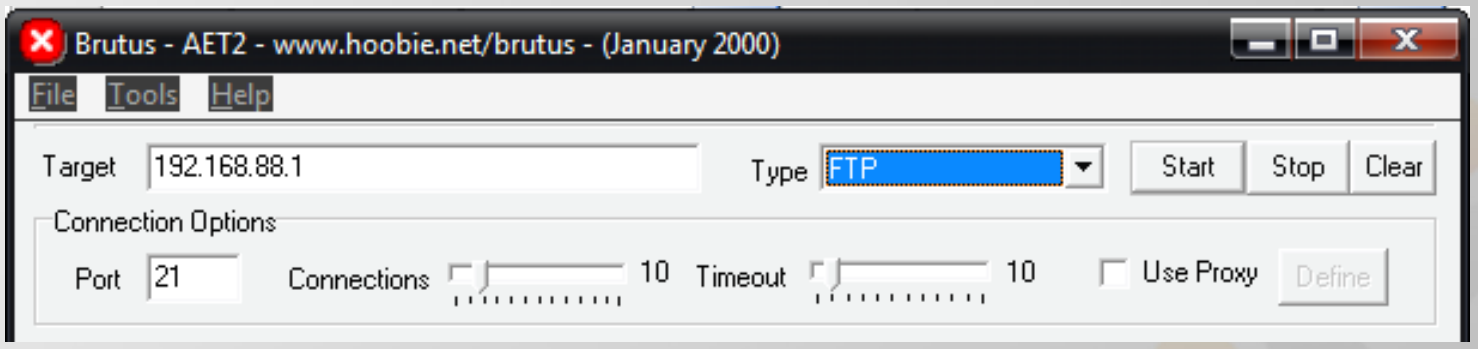
Attacker

- Today most of the attackers who attacked continuously usually is a machine or boot
- In this demonstration, we will use Software for testing/simulation
- For demo, We will using **Brute Force** involves systematically checking all possible code, combination, or password until the correct one is found

Test Attacker

FTP Attack

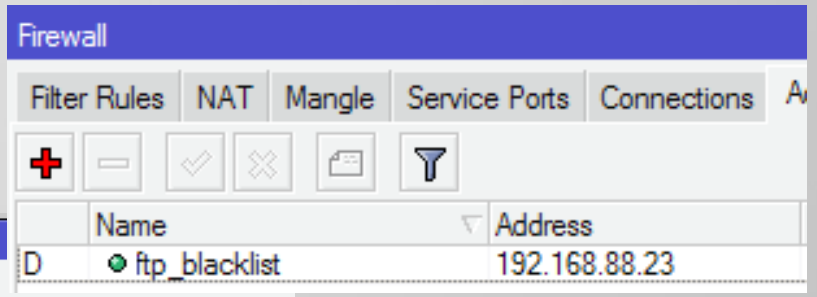
- Download brute force from www.hoobie.net/brutus and install it to your laptop.
- Input the target IP and type of attack and port
- Start Attack



Test Attacker

What going on in our Mikrotik?

Mikrotik will detect the attack, drop it, put on address list & send it by mail

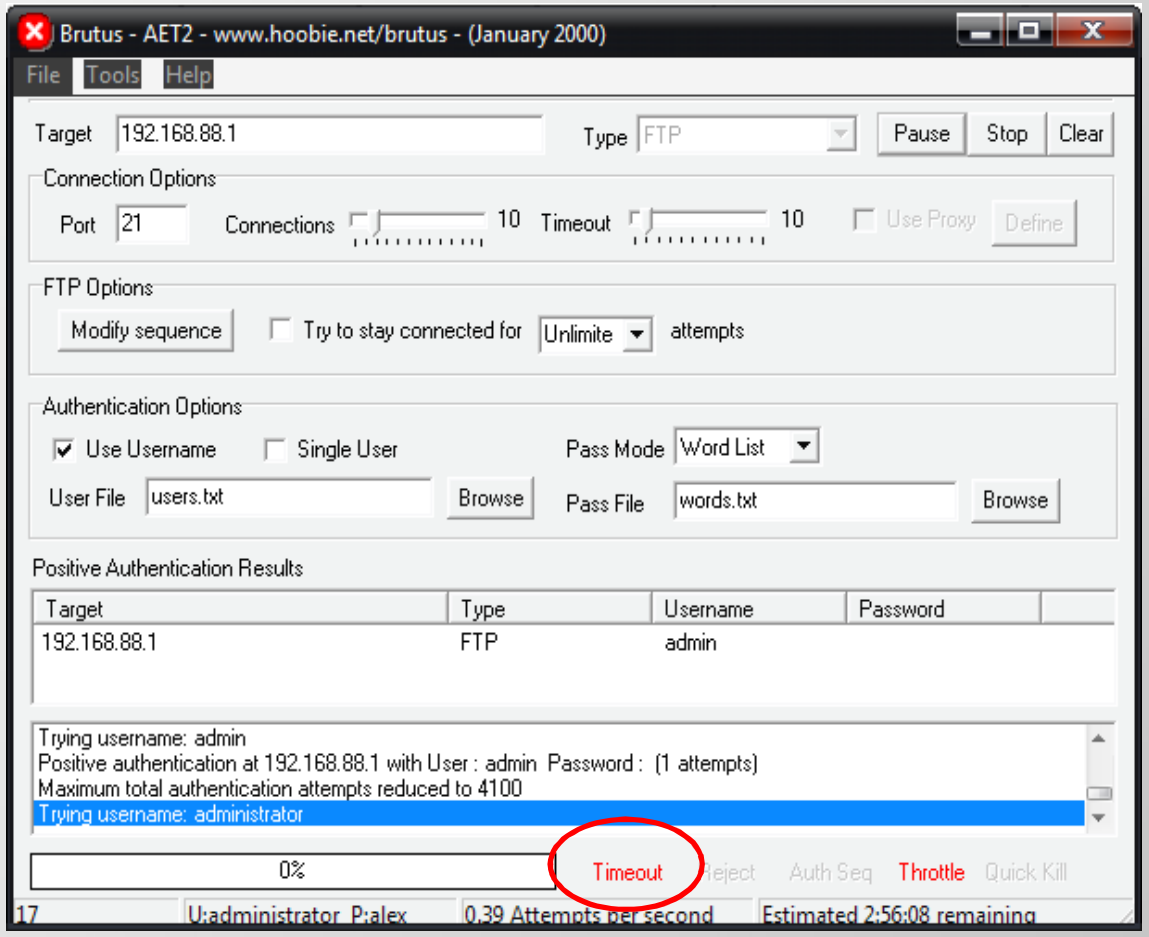


Log

Mar/01/2012 11:39:39	script warning	FTP Attack from:22.2.22.2
Mar/01/2012 11:39:41	e-mail debug	recv: 220 mx.google.com ESMTP e6sm974758pbr.74
Mar/01/2012 11:39:41	e-mail debug	send EHLO [10.100.100.6]
Mar/01/2012 11:39:43	e-mail debug	recv: 250-mx.google.com at your service, [180.254.39.185]
Mar/01/2012 11:39:43	e-mail debug	recv: 250-SIZE 35882577
Mar/01/2012 11:39:43	e-mail debug	recv: 250-8BITMIME
Mar/01/2012 11:39:43	e-mail debug	recv: 250-STARTTLS
Mar/01/2012 11:39:43	e-mail debug	recv: 250 ENHANCEDSTATUSCODES
Mar/01/2012 11:39:43	e-mail debug	send STARTTLS
Mar/01/2012 11:39:44	e-mail debug	recv: 220 2.0.0 Ready to start TLS
Mar/01/2012 11:39:47	e-mail debug	send EHLO [10.100.100.6]
Mar/01/2012 11:39:48	e-mail debug	recv: 250-mx.google.com at your service, [180.254.39.185]
Mar/01/2012 11:39:48	e-mail debug	recv: 250-SIZE 35882577
Mar/01/2012 11:39:48	e-mail debug	recv: 250-8BITMIME
Mar/01/2012 11:39:48	e-mail debug	recv: 250-AUTH LOGIN PLAIN XOAUTH
Mar/01/2012 11:39:48	e-mail debug	recv: 250 ENHANCEDSTATUSCODES
Mar/01/2012 11:39:48	e-mail debug	send AUTH PLAIN AG1pa3JvdGlrLmlkcwBtMWtyMHQxaw==

Test Attacker

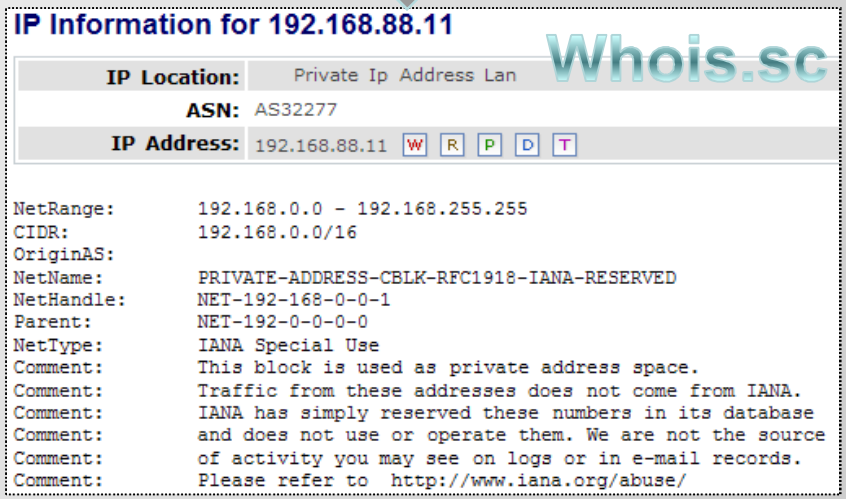
What going on in attacker?

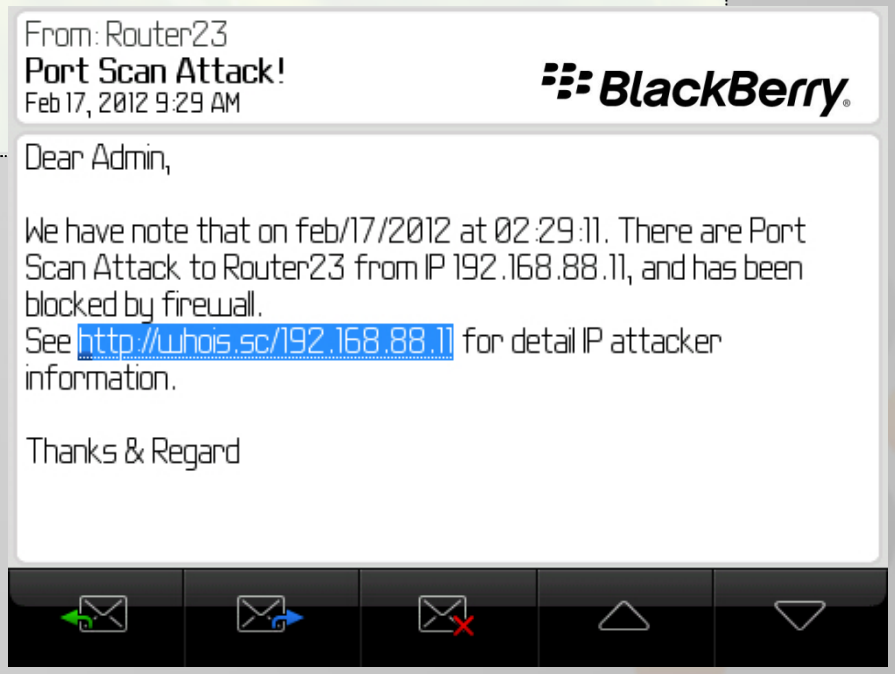


The IP attacker or the connection will be blocked

Test Attacker

Mail Report





Port Scanning Attack

Test Attacker

```
C:\Users\ropix>nmap 192.168.88.1
Starting Nmap 5.51 ( http://nmap.org ) at 2012-10-19 23:47 SE Asia Standard Time
Nmap scan report for 192.168.88.1
Host is up (0.00087s latency).
Not shown: 993 filtered ports
PORT     STATE  SERVICE
22/tcp   open   ssh
110/tcp  closed pop3
111/tcp  closed rpcbind
135/tcp  closed msrpc
139/tcp  closed netbios-ssn
995/tcp  closed pop3s
8291/tcp open   unknown
MAC Address: D4:CA:6D:26:86:4E (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 4.73 seconds
```

Port Scanning Attack

Test Attacker

C:\Users\ropix>nmap 192.168.88.1

Starting Nmap 5.51 (http://nmap.org) at 2012-10-19 23:53

Nmap scan report for 192.168.88.1

Host is up (0.0011s latency).

Not shown: 999 filtered ports

PORT STATE SERVICE

8291/tcp open unknown

MAC Address: D4:CA:6D:26:86:4E (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 4.78 seconds

Another attacker

In the IP firewall we can detect any malicious like:

- Who is accessing IDM
- Who is accessing Ultra surf/ vpn client
- Who is using anonymous proxy
- Who is using Download manager
- Who is accessing one specific url (porn, sex, etc)
- Who is accessing p2p connection

Put them on address-list with different name, block the address-list & send their IP by email to us.

Conclusion

- ✓We can change our mikrotik box to a smart machine that inform us if it's attacked by intruders.
- ✓We can improve this method to any malicious connection

Thank You

- All scripts & material can be downloaded at http://trainingmikrotik.com/mum
- Any question?

Rofiq Fauzi
training@id-networkers.com