

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

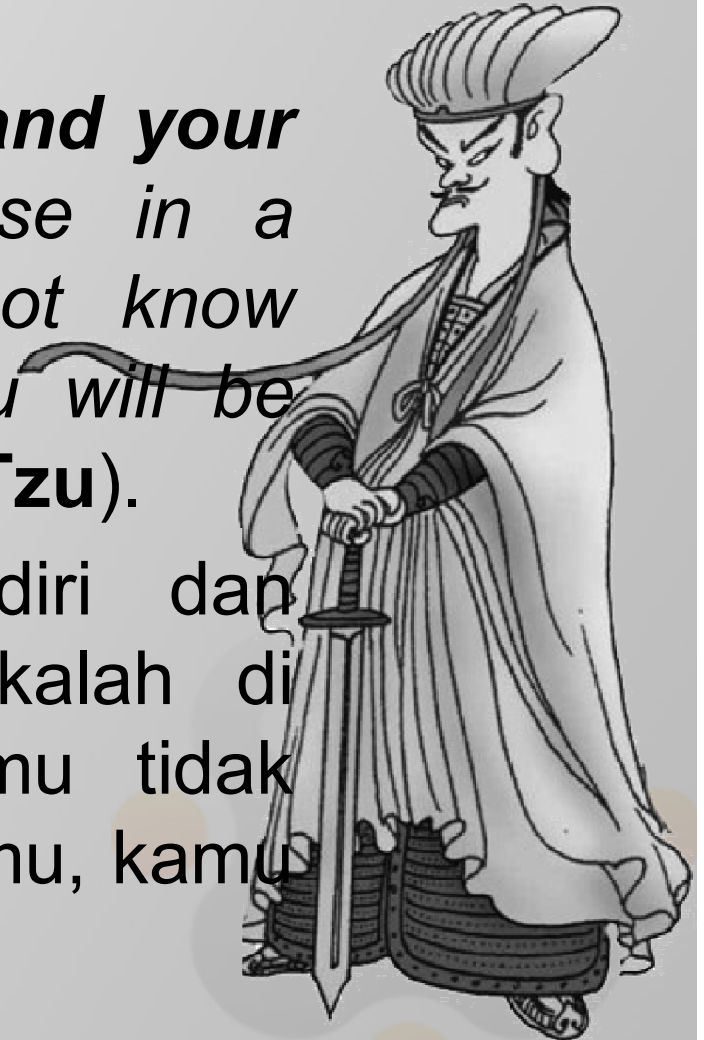
- Admin can not always monitor the servers directly or always login in to check the servers for intruder.
- We need firewall not just to blocking intruder, but also log and report them to admin immediately.
- In wide network with many MikroTik router, we don't know which is under attack.
- We can report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

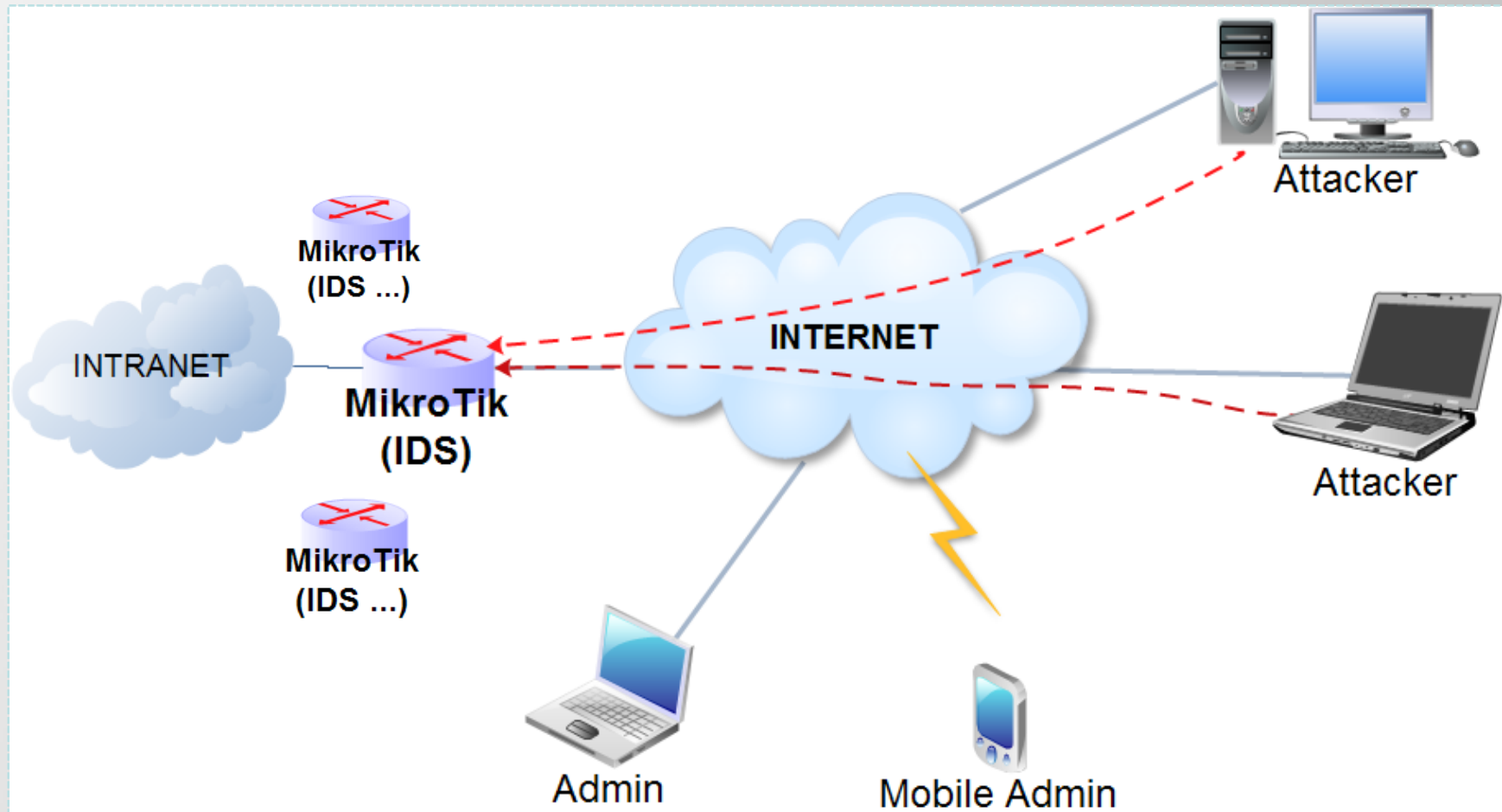
- **Passive System**

- ✓ sensor detects a potential security breach
- ✓ logs the information
- ✓ alert on the console

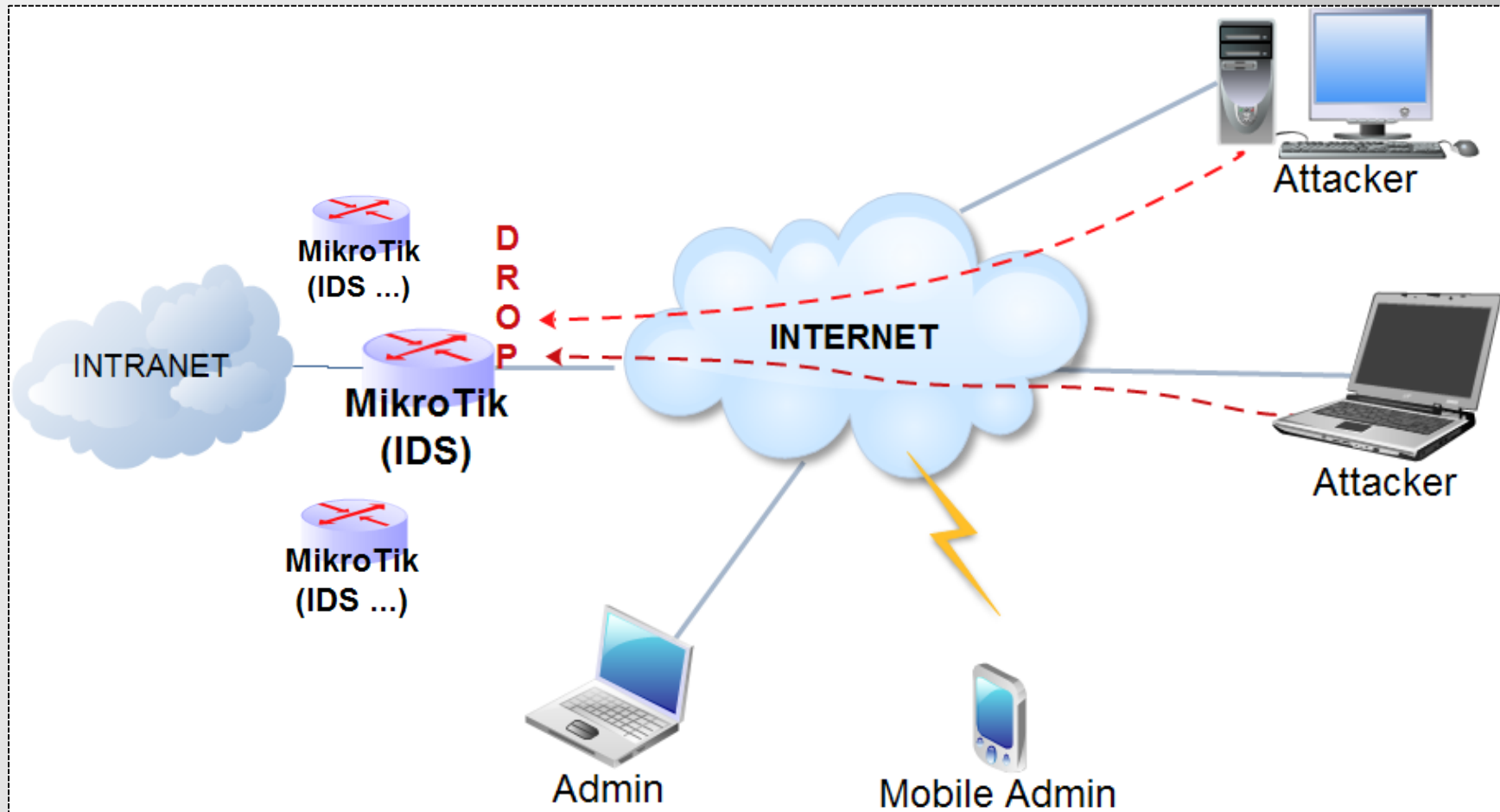
- **Reactive System**

- ✓ Like **Passive System**, but plus:
- ✓ auto-responds (resetting the connection or drop the traffic) from intruders
- ✓ Send the report to admin

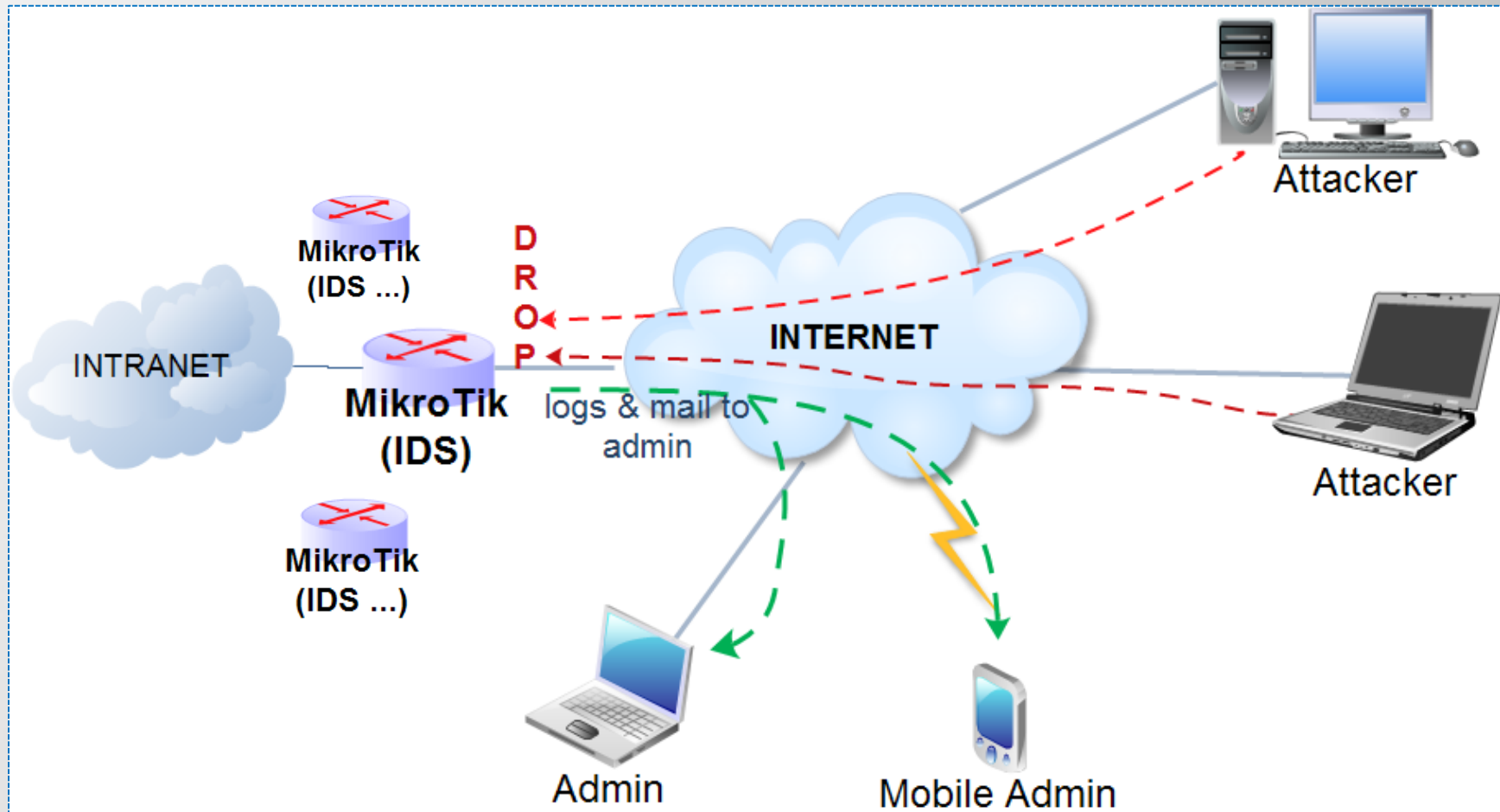
Attack Process



Drop by IP>Firewall

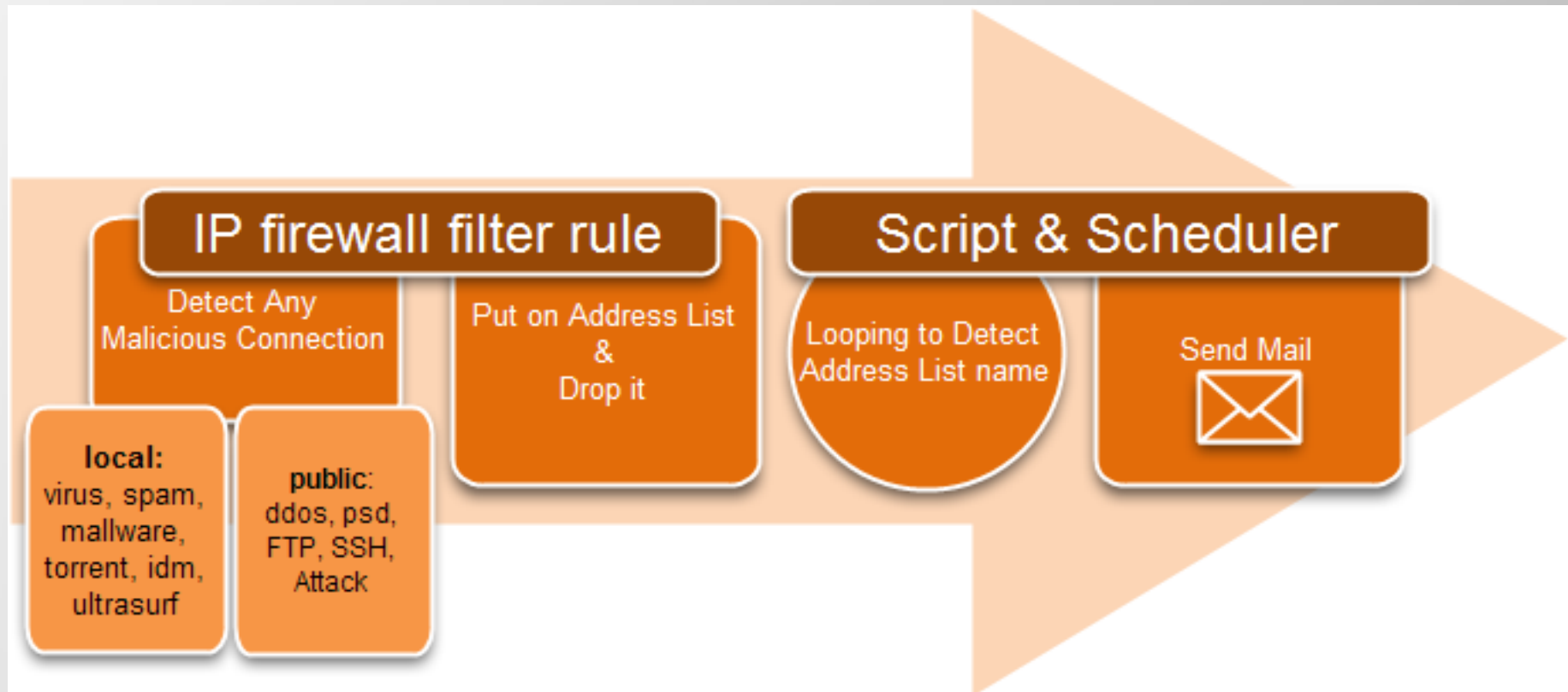


Logging & Mail Report



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, Illegal Tunneling (utrasurf), Anonymous Proxy, Internet Download manager, url filtered.

Simulation

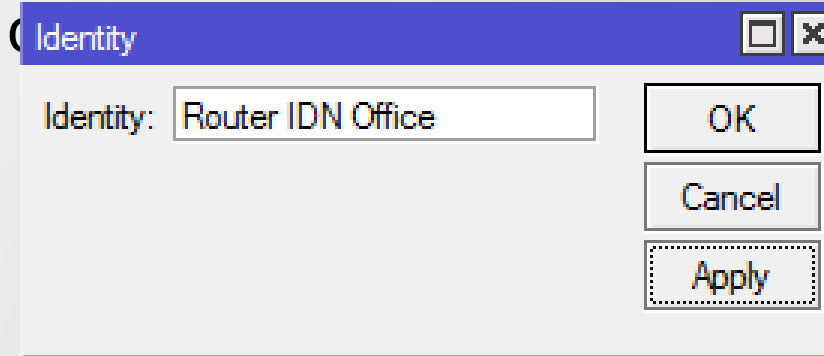
We want simulation with the following points:

- 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.

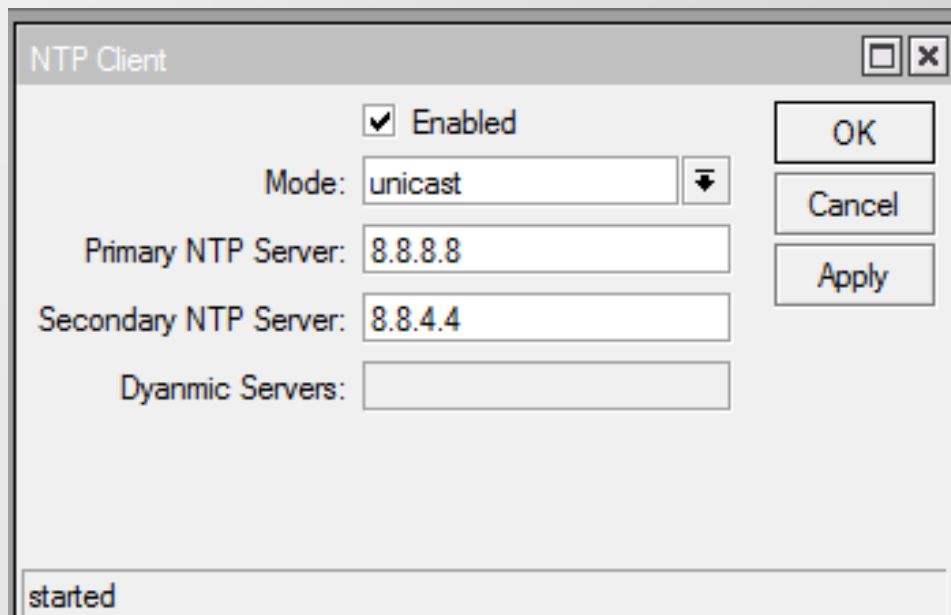
NTP Client

- 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.

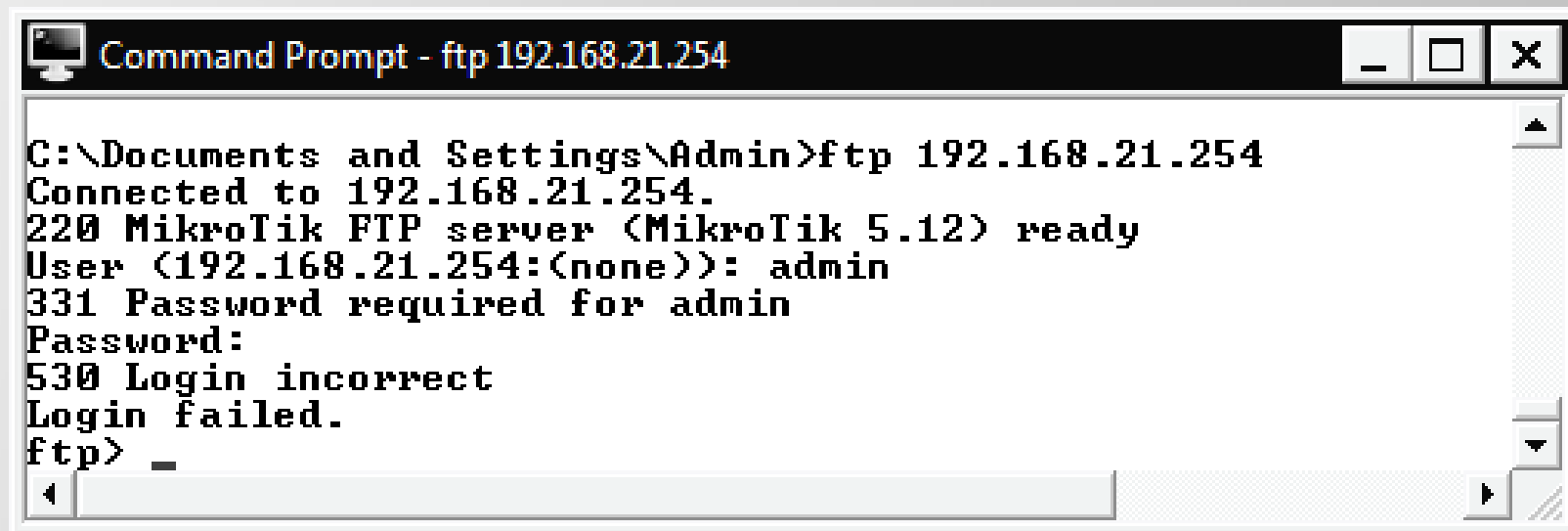
/system ntp client



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”



```
C:\Documents and Settings\Admin>ftp 192.168.21.254
Connected to 192.168.21.254.
220 Mikrotik FTP server (MikroTik 5.12) ready
User (192.168.21.254:(none)): admin
331 Password required for admin
Password:
530 Login incorrect
Login failed.
ftp> _
```

MikroTik Configuration

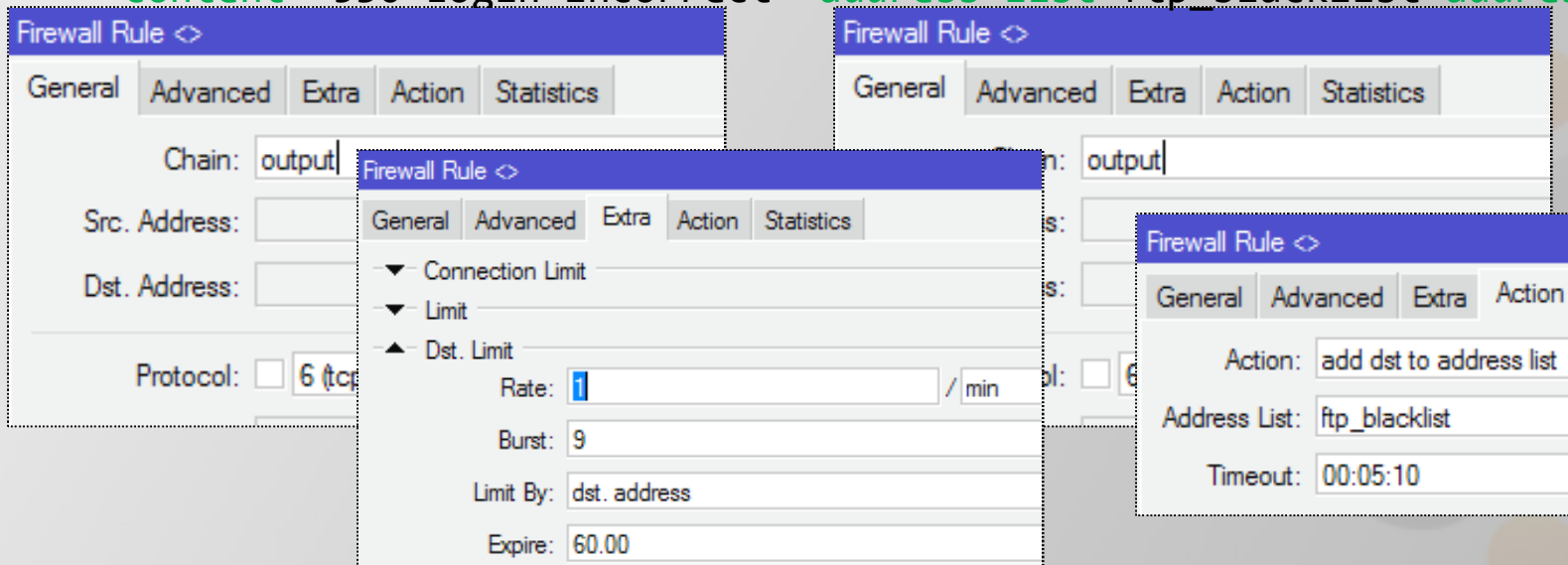
Configure Firewall to Add Attacker IP address in Address List

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-
```



The image displays three overlapping screenshots of the MikroTik WinBox Firewall Rule configuration interface:

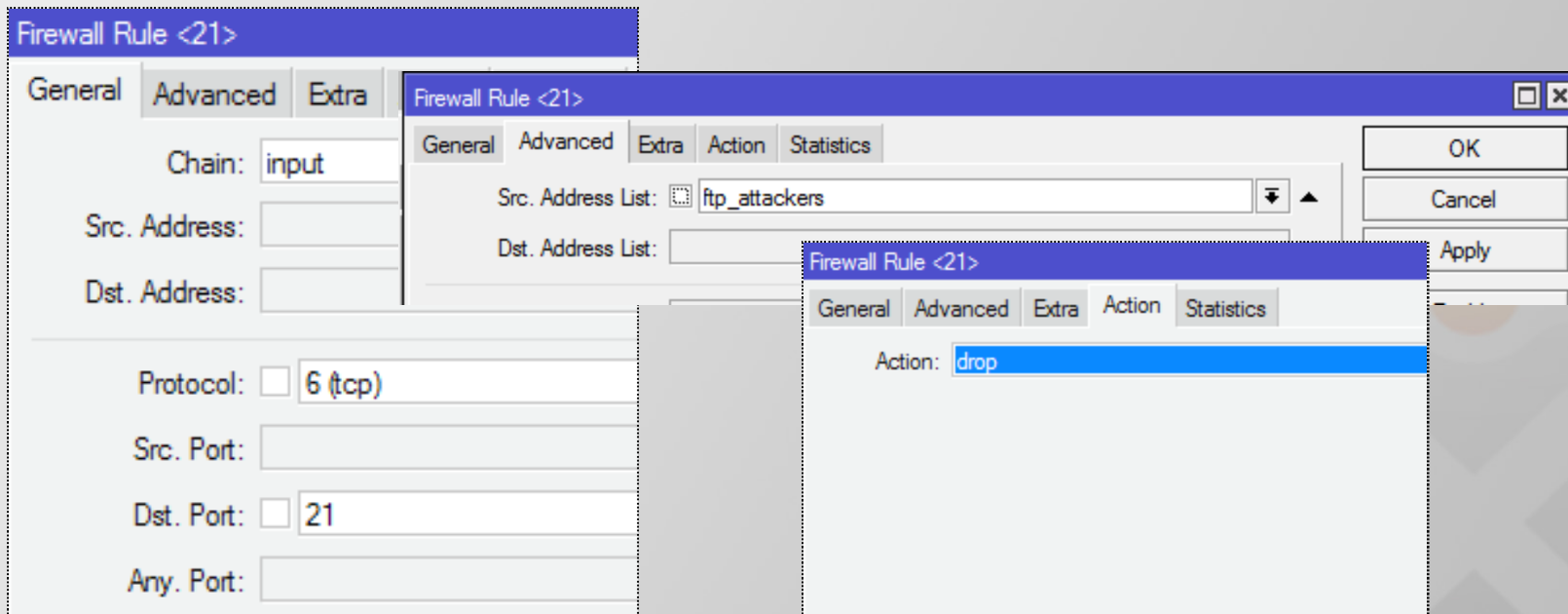
- Top Left Screenshot (General tab):** Shows the Chain set to `output`, Protocol set to `tcp`, and Content set to `"530 Login incorrect"`.
- Bottom Left Screenshot (Advanced tab):** Shows the Dst. Limit section expanded with Rate set to `1` / min, Burst set to `9`, Limit By set to `dst. address`, and Expire set to `60.00`.
- Right Screenshot (Action tab):** Shows the Action set to `add dst to address list`, Address List set to `ftp_blacklist`, and Timeout set to `00:05:10`.

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"
```



The screenshot shows the MikroTik WinBox interface for configuring a Firewall Rule. The main window is titled "Firewall Rule <21>" and has tabs for General, Advanced, Extra, Action, and Statistics. The General tab is active, showing the following fields:

- Chain: input
- Src. Address: (empty)
- Dst. Address: (empty)
- Protocol: ☒ 6 (tcp)
- Src. Port: (empty)
- Dst. Port: ☒ 21
- Any. Port: (empty)

Overlaid on this is a smaller window titled "Firewall Rule <21>" with tabs for General, Advanced, Extra, Action, and Statistics. The Action tab is active, showing the Action: drop. Another window titled "Firewall Rule <21>" is also overlaid, showing the General tab with the Src. Address List set to ftp_attackers and the Dst. Address List set to (empty). The OK, Cancel, and Apply buttons are visible in the bottom right of the windows.

MikroTik Configuration

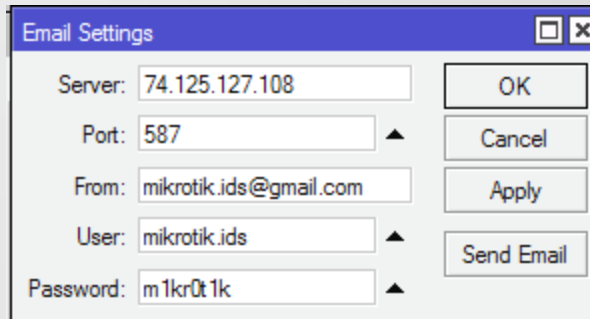
Configure Send e-mail

Create mail account for the smtp relay, In this lab we using Gmail.

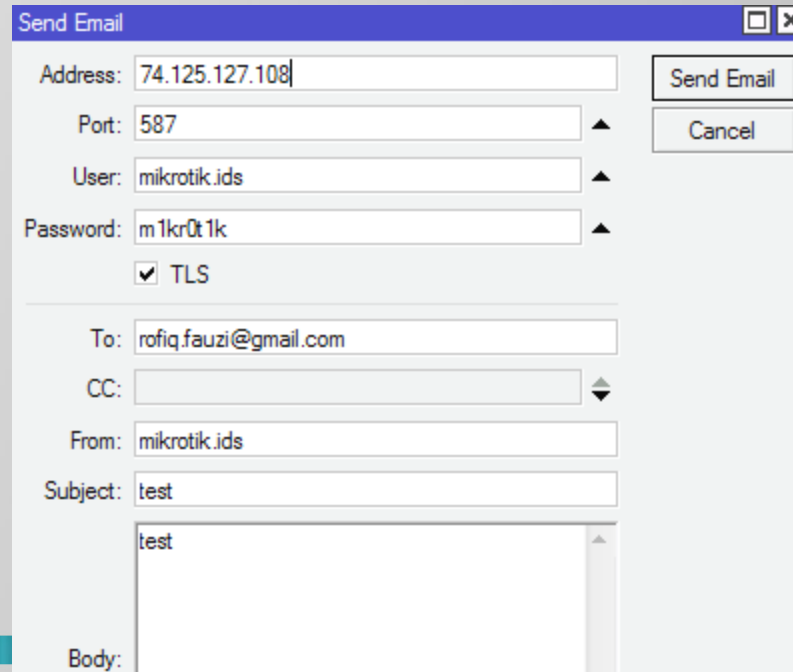
In **/tool e-mail** , set the smtp server, username & password

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

Lets try to send some email to make sure its work



Dialog box titled "Email Settings" with fields for Server, Port, From, User, and Password. The values are: Server: 74.125.127.108, Port: 587, From: mikrotik.ids@gmail.com, User: mikrotik.ids, Password: m1kr0t1k. Buttons include OK, Cancel, Apply, and Send Email.



Dialog box titled "Send Email" with fields for Address, Port, User, Password, and TLS. The values are: Address: 74.125.127.108, Port: 587, User: mikrotik.ids, Password: m1kr0t1k, TLS: checked. Below these are fields for To (rofiq.fauzi@gmail.com), CC, From (mikrotik.ids), Subject (test), and Body (test). Buttons include Send Email and Cancel.

Logging

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

Logging

Rules Actions

Topics	Prefix	Action
info		
error		
warning		
critical		
e-mail		

Log Rule <e-mail>

Topics: ☐ e-mail

Prefix:

Action:

Log

/2012 11:39:39	script warning	FTP Attack from:22.2.22.2
/2012 11:39:41	e-mail debug	recv: 220 mx.google.com ESMTP e6sm974758pbr.74
/2012 11:39:41	e-mail debug	send EHLO [10.100.100.6]
/2012 11:39:43	e-mail debug	recv: 250-mx.google.com at your service, [180.254.39.185]
/2012 11:39:43	e-mail debug	recv: 250-SIZE 35882577
/2012 11:39:43	e-mail debug	recv: 250-8BITMIME
/2012 11:39:43	e-mail debug	recv: 250-STARTTLS
/2012 11:39:43	e-mail debug	recv: 250 ENHANCEDSTATUSCODES
/2012 11:39:43	e-mail debug	send STARTTLS
/2012 11:39:44	e-mail debug	recv: 220 2.0.0 Ready to start TLS
/2012 11:39:47	e-mail debug	send EHLO [10.100.100.6]
/2012 11:39:48	e-mail debug	recv: 250-mx.google.com at your service, [180.254.39.185]
/2012 11:39:48	e-mail debug	recv: 250-SIZE 35882577
/2012 11:39:48	e-mail debug	recv: 250-8BITMIME
/2012 11:39:48	e-mail debug	recv: 250-AUTH LOGIN PLAIN XOAUTH
/2012 11:39:48	e-mail debug	recv: 250 ENHANCEDSTATUSCODES
/2012 11:39:48	e-mail debug	send AUTH PLAIN AG1pa3JvdGlrLmlkcwBtMWtyMHQxaw==
/2012 11:39:48	e-mail debug	recv: 235 2.7.0 Accepted
Mar/01/2012 11:39:50	e-mail debug	send MAIL FROM: <mikrotik.ids@gmail.com>
Mar/01/2012 11:39:51	e-mail debug	recv: 250 2.1.0 OK e6sm974758pbr.74
Mar/01/2012 11:39:51	e-mail debug	send RCPT TO: <bl4ck_4n6el@yahoo.com>
Mar/01/2012 11:39:53	e-mail debug	recv: 250 2.1.5 OK e6sm974758pbr.74
Mar/01/2012 11:39:53	e-mail debug	send DATA
Mar/01/2012 11:39:55	e-mail debug	recv: 354 Go ahead e6sm974758pbr.74
Mar/01/2012 11:39:55	e-mail debug	send .
Mar/01/2012 11:39:58	e-mail debug	recv: 250 2.0.0 OK 1330576798 e6sm974758pbr.74
Mar/01/2012 11:39:58	e-mail debug	send QUIT
Mar/01/2012 11:40:00	e-mail debug	recv: 221 2.0.0 closing connection e6sm974758pbr.74

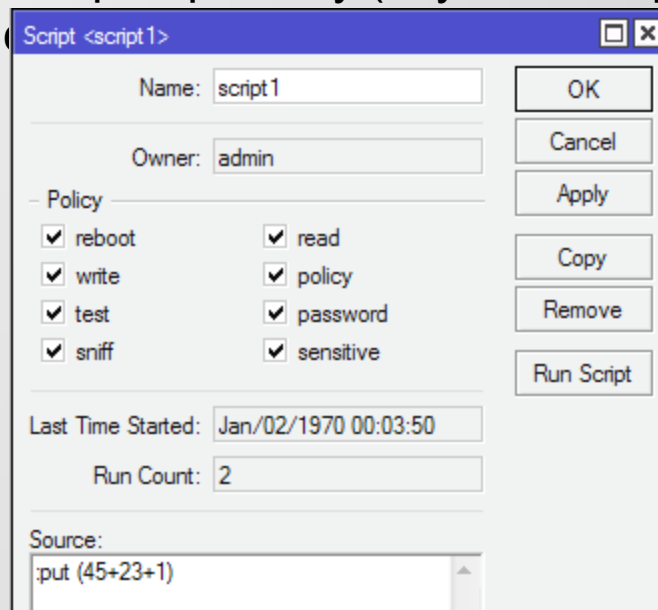
Mikrotik Script

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



The screenshot shows a window titled "Script <script1>". It contains the following fields and controls:

- Name: script1
- Owner: admin
- Policy section with checkboxes:
 - reboot (checked)
 - write (checked)
 - test (checked)
 - sniff (checked)
 - read (checked)
 - policy (checked)
 - password (checked)
 - sensitive (checked)
- Last Time Started: Jan/02/1970 00:03:50
- Run Count: 2
- Source: :put (45+23+1)
- Buttons on the right: OK, Cancel, Apply, Copy, Remove, Run Script

MikroTik Configuration

Configuration of the Script

```

name="send_ftp" owner="admin"
policy=ftp,reboot,read,write,policy,test,winbox,password,sniff,sensitive,ani
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 & Regards"
  
```

Find match address list

Get the IP address

Log it on machine

Get router id, date & time

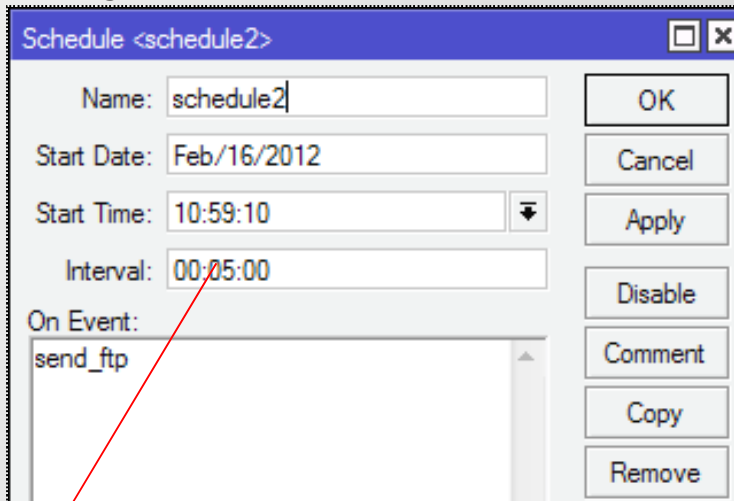
send the report

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.

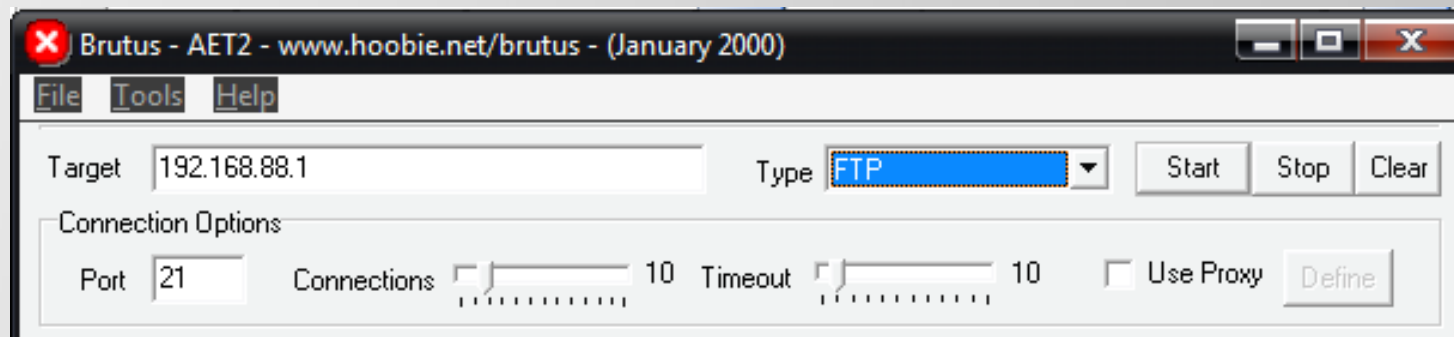
Attacker

- 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==

Firewall

Filter Rules NAT Mangle Service Ports Connections Av

	Name	Address
D	ftp_blacklist	192.168.88.23

Test Attacker

What going on in attacker?

Brutus - AET2 - www.hoobie.net/brutus - (January 2000)

File Tools Help

Target: 192.168.88.1 Type: FTP [Pause] [Stop] [Clear]

Connection Options

Port: 21 Connections: 10 Timeout: 10 [Use Proxy] [Define]

FTP Options

[Modify sequence] [Try to stay connected for] Unlimite attempts

Authentication Options

☒ Use Username ☐ Single User Pass Mode: Word List

User File: users.txt [Browse] Pass File: words.txt [Browse]

Positive Authentication Results

Target	Type	Username	Password
192.168.88.1	FTP	admin	

Trying username: admin
 Positive authentication at 192.168.88.1 with User : admin Password : (1 attempts)
 Maximum total authentication attempts reduced to 4100
 Trying username: administrator

0% [Timeout] [reject] [Auth Seq] [Throttle] [Quick Kill]


17 Uadministrator P:alex 0.39 Attempts per second Estimated 2:56:08 remaining


The IP attacker or the connection will be blocked

Test Attacker

Mail Report

Port Scan Attack!
Inbox x
Rofiq x





Router23 mikrotik.ids@gmail.com
 to me ▾

9:29 AM (0 minutes ago) ☆ ↶ ▾

Dear Admin,

 We have note that on feb/17/2012 at 02:29:11. There are Port Scan Attack to Router23 from IP 192.168.88.11, and has been blocked by firewall.
 See <http://whois.sc/192.168.88.11> for detail IP attacker information.


 Thanks & Regard

IP Information for 192.168.88.11


IP Location:	Private Ip Address Lan
ASN:	AS32277
IP Address:	192.168.88.11 W R P D T

NetRange: 192.168.0.0 - 192.168.255.255
 CIDR: 192.168.0.0/16
 OriginAS:
 NetName: PRIVATE-ADDRESS-CBLK-RFC1918-IANA-RESERVED
 NetHandle: NET-192-168-0-0-1
 Parent: NET-192-0-0-0-0
 NetType: IANA Special Use
 Comment: This block is used as private address space.
 Comment: Traffic from these addresses does not come from IANA.
 Comment: IANA has simply reserved these numbers in its database and does not use or operate them. We are not the source of activity you may see on logs or in e-mail records.
 Comment: Please refer to <http://www.iana.org/abuse/>


From: Router23
Port Scan Attack!
 Feb 17, 2012 9:29 AM



Dear Admin,

 We have note that on feb/17/2012 at 02:29:11. There are Port Scan Attack to Router23 from IP 192.168.88.11, and has been blocked by firewall.
 See <http://whois.sc/192.168.88.11> for detail IP attacker information.

 Thanks & Regard



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