MikroTik
DNS Spoofing

Presented by Michael Takeuchi

MUM, 14 October 2016 - Indonesia

michael@takeuchi.id

Let’s Securing Your Network And Yourself !

About Michael Takeuchi

- Using MikroTik RouterOS (v5.20) Since 14 December 2014
  - RouterOS x86 at PC
- Using MikroTik RouterBoard (v6.25) Since 10 July 2015
  - RB941-2ND
- 24 April 2016, MTCNA 1604NA934 with Kakek Guru-ku (Ziad Sobri)
- 31 July 2016, MTCRE 1607RE248 with Kakek Guru-ku (Ziad Sobri)
- 3 August 2016, MikroTik Certified Consultant on Indonesia
- Still in School, SMK Taruna Bhakti Depok
- Wanna Be MikroTik Certified Trainer

About SMK Taruna Bhakti Depok (STARBHAK)

- A Vocational School was placed at
  - Jl. Raya Pekapuran, RT 02/RW 07, Kel. Curug, Kec. Cimanggis, Depok City, West Java
  - (021) 8744810
- Informatics School
- STARBHAK = **S**MK **Tar**una **Bhak**ti
- Motto: Our Quality Ask to Be Different
- Network Engineering, Multimedia, Software Engineering, Broadcasting, Electrical Engineering Industry
- MikroTik Academy and many more
- Website: www.smktarunabhakti.net

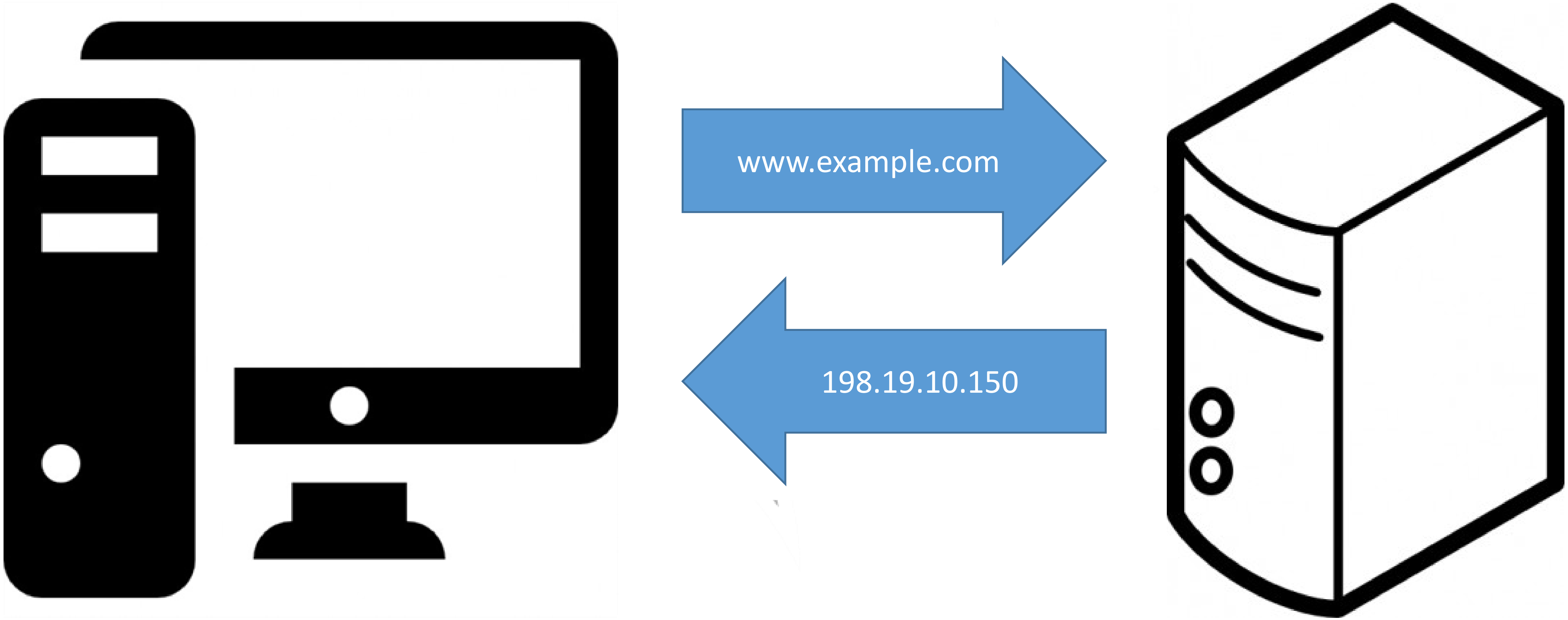
About SMK Taruna Bhakti Depok (STARBHAK)

About DNS (Domain Name System)

- As a Translator from Domain to Number (IP)
- A MikroTik router with DNS feature enabled can be set as a DNS Server
- MikroTik router can be specified as a Primary DNS Server under dhcp-server settings
- When allow-remote-request=yes The MikroTik router respond to TCP and UDP DNS request on port 53

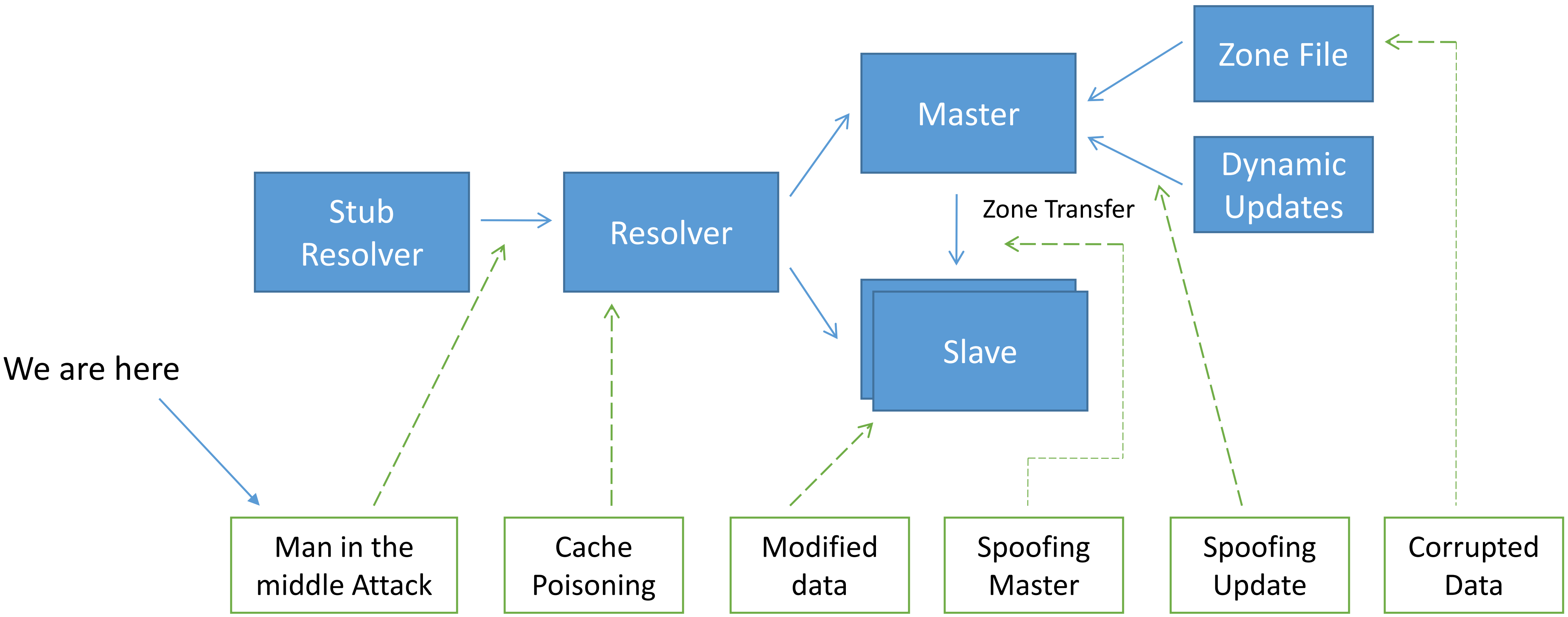
From http://wiki.mikrotik.com/wiki/Manual:IP/DNS

How DNS Works



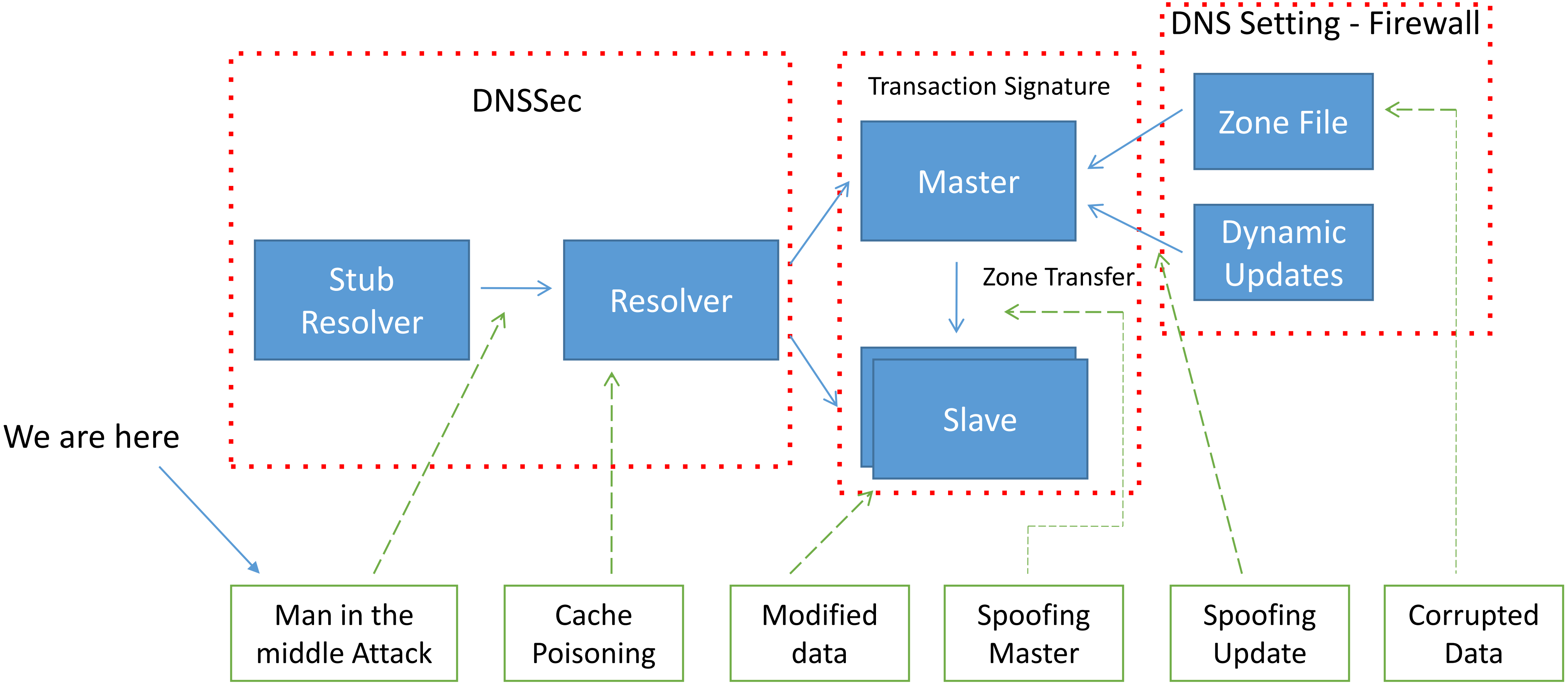
Requested with alphabet (Uniform Resource Locator, **URL**) and replied with number (IP)
Read More: https://howdns.works
images was taken from google images and modified by me

DNS Vulnerability



From ID-SIRTII/CC

Prevention



From ID-SIRTII/CC

DNSSec/DNSCrypt

- DNS Security Extension
- DNSSec used for verifying domain data with data on Authoritative DNS Server or Root DNS with Public Key/Digital Signature

- DNSCrypt are use Public Key to verifying DNS Server and using TCP/443

From ID-SIRTII/CC

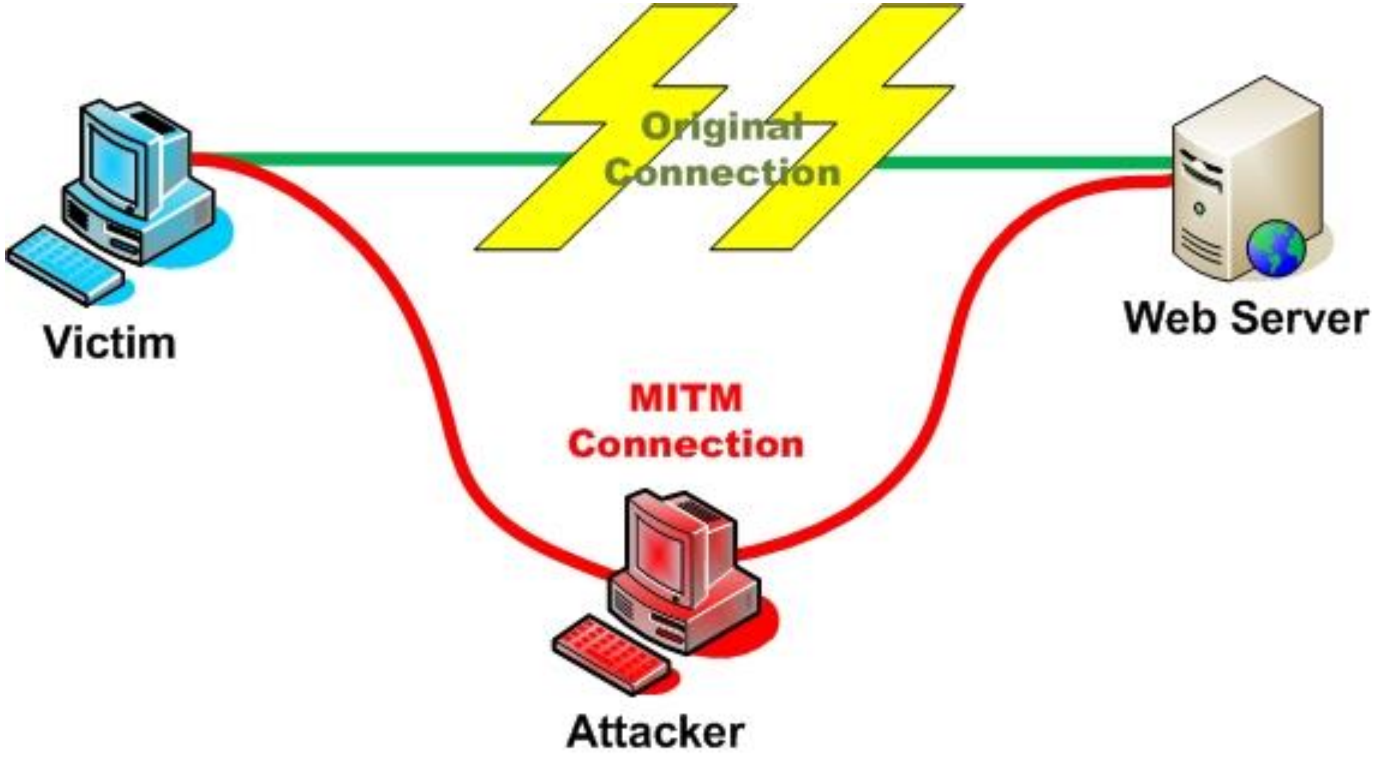
TSIG

- Transaction Signature
- Is a method in which the master DNS server and secondary DNS server can do *zone-transfer* and *dynamic-update* if have same signature code

From ID-SIRTII/CC

About MITM (Man in The Middle) Attack

- MITM was Performed by Insider Attacker (On LAN)



Images was Taken from Google Images

How DNS Spoofing Works?

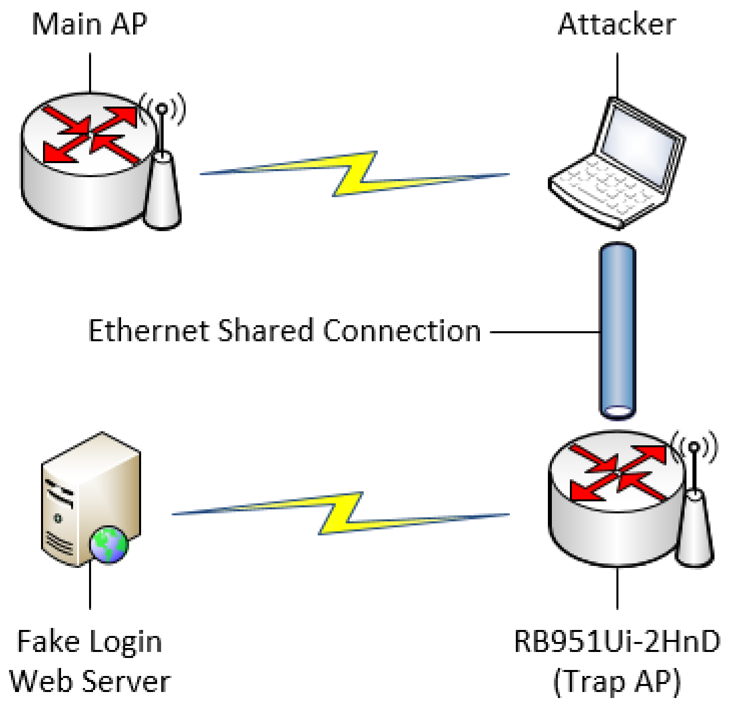
- When you are request www.example.com on browser, DNS will translate it to IP, Because Computer works with number, and we interact with name or domain when accessing website
- DNS Spoofing can manipulating an IP of Domain
- www.example.com IP is 198.19.10.150 and we will change to 192.168.1.4 (Fake Login Web Server IP)
- And we will using **MikroTik** feature to do DNS Spoofing

Static DNS

*Yes, we will using **Static DNS** feature to do it*

Demonstration

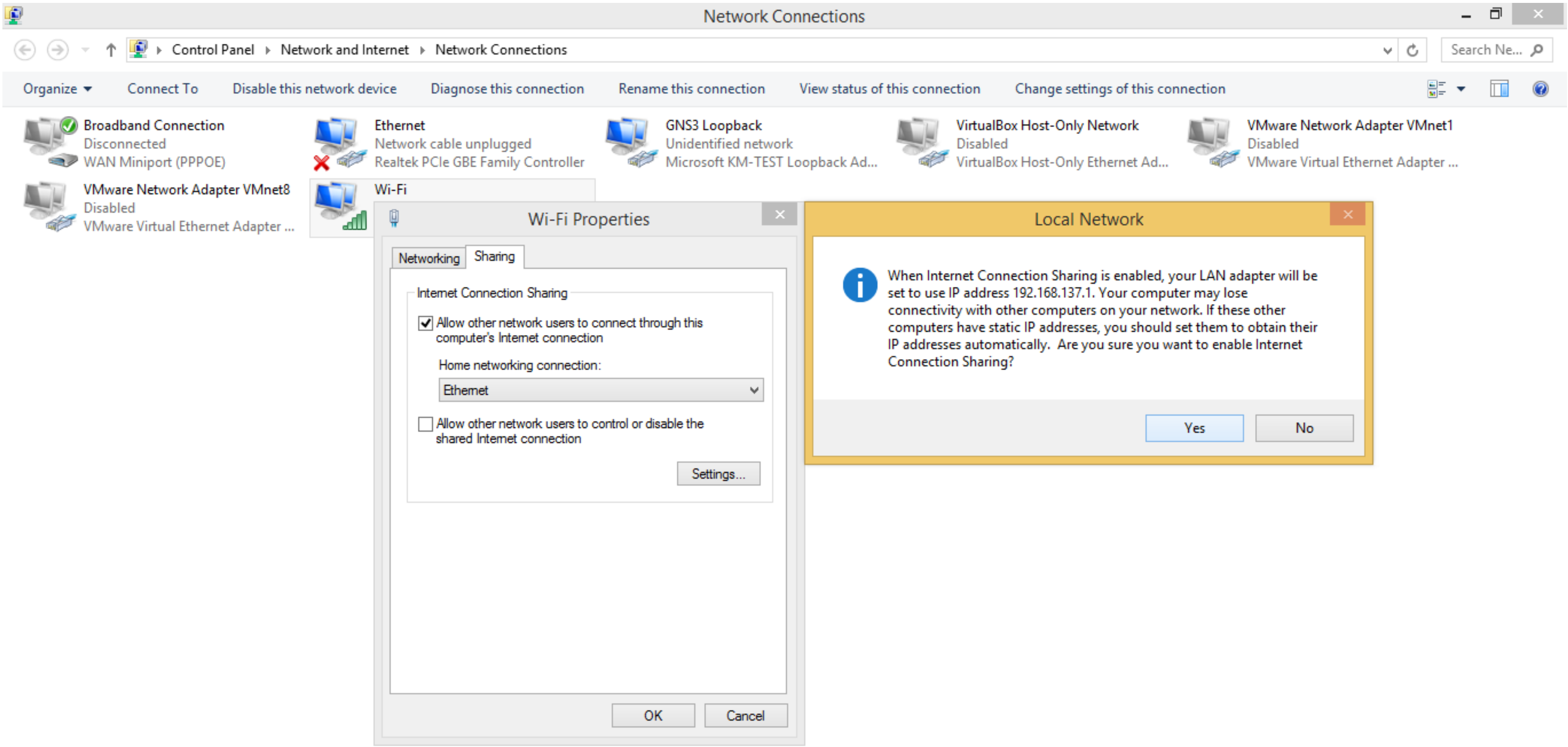
0. Topology



Main AP (victim) – Attacker – Ethernet Shared Connection

RouterBoard AP as Attacker AP (With Connected Attacker Web Server And Your Victim)

1. Ethernet Shared Connection (Attacker Windows)



Broadband Connection
Disconnected
WAN Miniport (PPPOE)

Ethernet
Network cable unplugged
Realtek PCIe GBE Family Controller

GNS3 Loopback
Unidentified network
Microsoft KM-TEST Loopback Ad...

VirtualBox Host-Only Network
Disabled
VirtualBox Host-Only Ethernet Ad...

VMware Network Adapter VMnet1
Disabled
VMware Virtual Ethernet Adapter ...

VMware Network Adapter VMnet8
Disabled
VMware Virtual Ethernet Adapter ...

Wi-Fi

Internet Connection Sharing

☑ Allow other network users to connect through this computer's Internet connection

Home networking connection:
Ethernet

☐ Allow other network users to control or disable the shared Internet connection

When Internet Connection Sharing is enabled, your LAN adapter will be set to use IP address 192.168.137.1. Your computer may lose connectivity with other computers on your network. If these other computers have static IP addresses, you should set them to obtain their IP addresses automatically. Are you sure you want to enable Internet Connection Sharing?

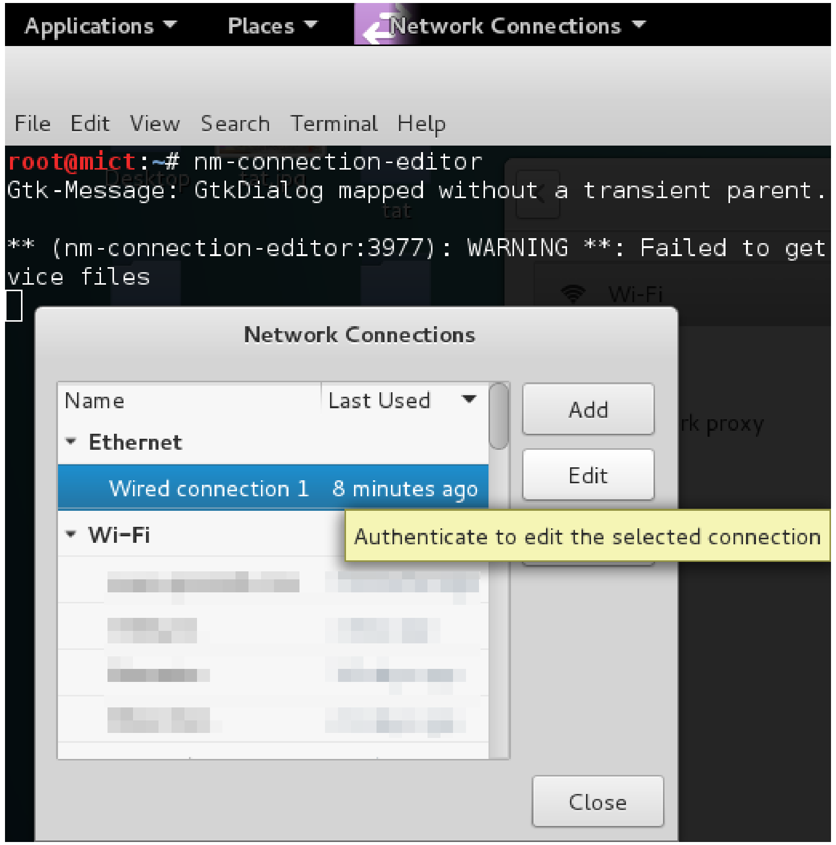
Go To Control Panel\Network and Internet\Network Connections

And do Right Click on Your Internet Connection Adapter (wifi) then choose properties, and then click Sharing Tab and **Check Allow other network users to connect through this computer's Internet Connection**

Click yes to create DHCP Server on your Ethernet Adapter

1. Ethernet Shared Connection (Attacker Linux)

Type **nm-connection-editor** on terminal than edit Wired connection 1

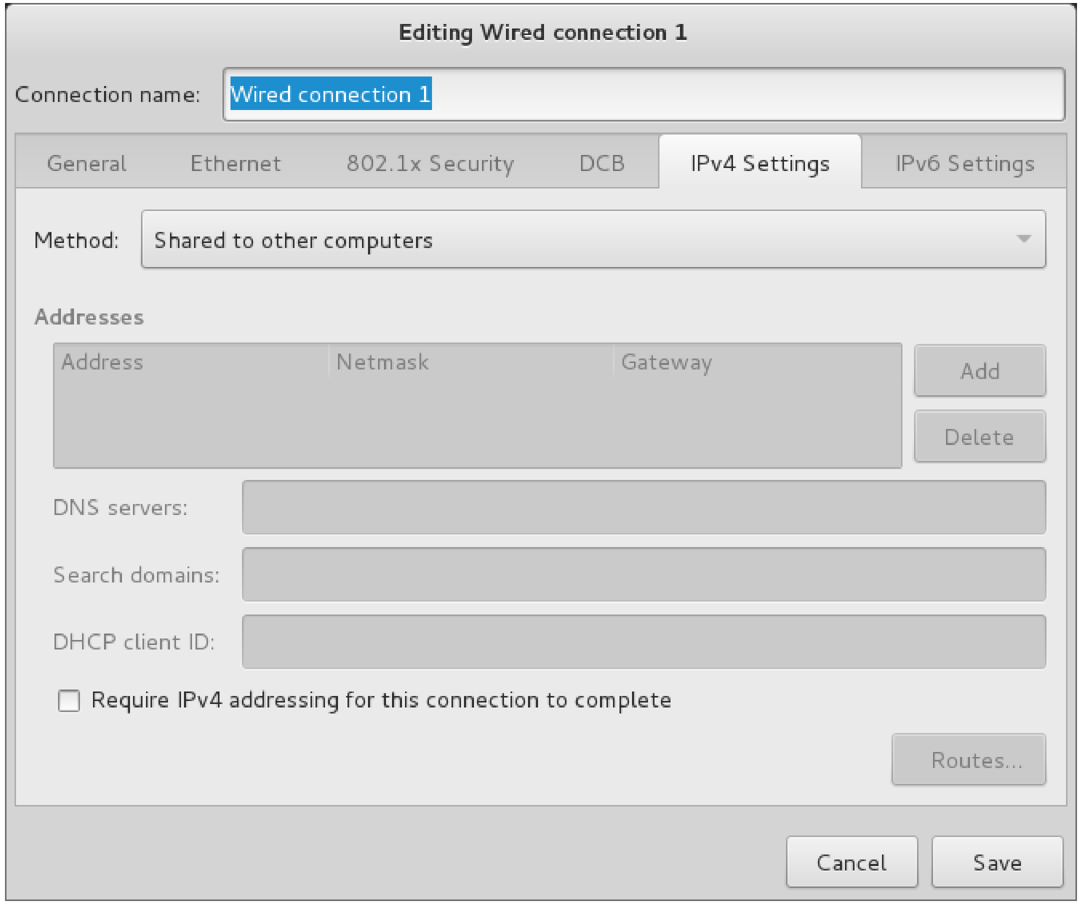


```
root@mict:~# nm-connection-editor
Gtk-Message: GtkDialog mapped without a transient parent.

** (nm-connection-editor:3977): WARNING **: Failed to get
vice files
```

1. Ethernet Shared Connection (Attacker Linux)

Go To IPv4 Settings than change method to **Shared to other computers**



Editing Wired connection 1

Connection name: Wired connection 1

Method: Shared to other computers

Addresses

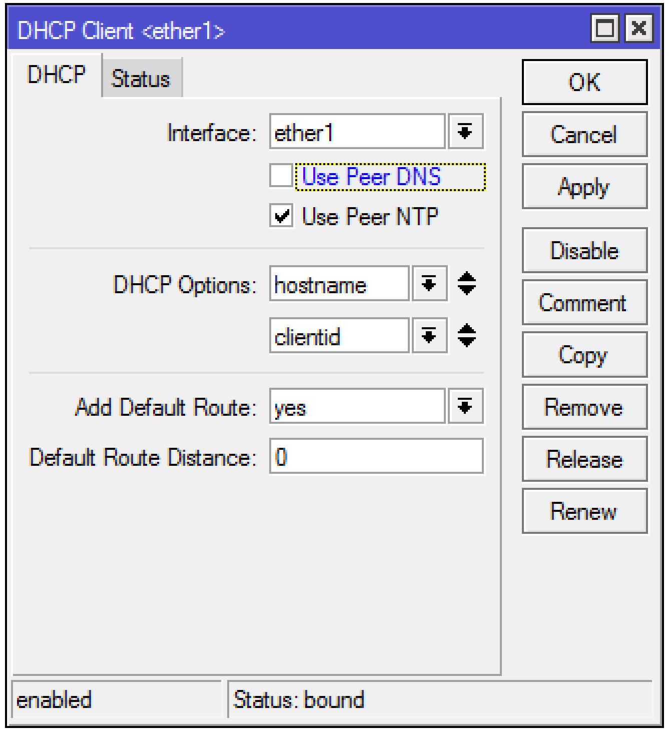
DNS servers:

Search domains:

DHCP client ID:

☐ Require IPv4 addressing for this connection to complete

2. Configure Internet on RouterBoard (DHCP & DNS)



DHCP Client <ether1>

Interface: ether1

□ Use Peer DNS

☑ Use Peer NTP

DHCP Options: hostname

clientid

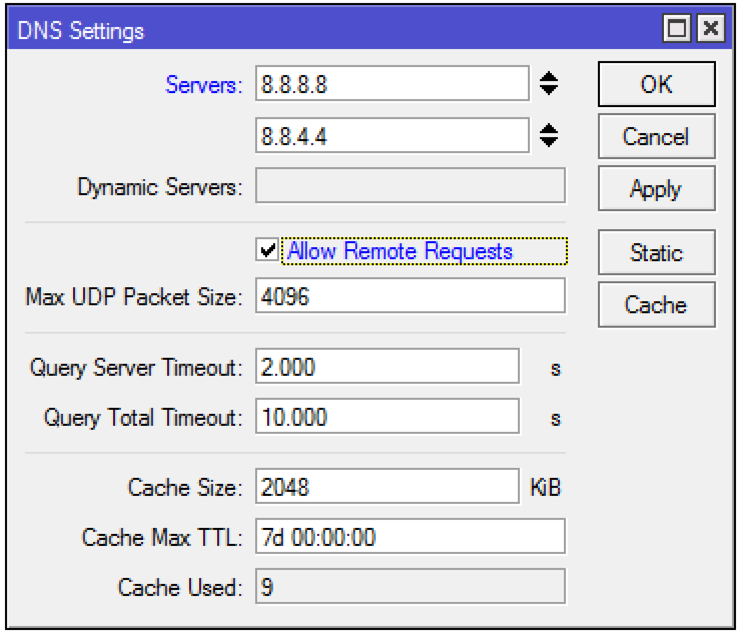
Add Default Route: yes

Default Route Distance: 0

enabled

Status: bound

Create DHCP Client without Dynamic DNS



DNS Settings

Servers: 8.8.8.8

8.8.4.4

Dynamic Servers:

☑ Allow Remote Requests

Max UDP Packet Size: 4096

Query Server Timeout: 2.000 s

Query Total Timeout: 10.000 s

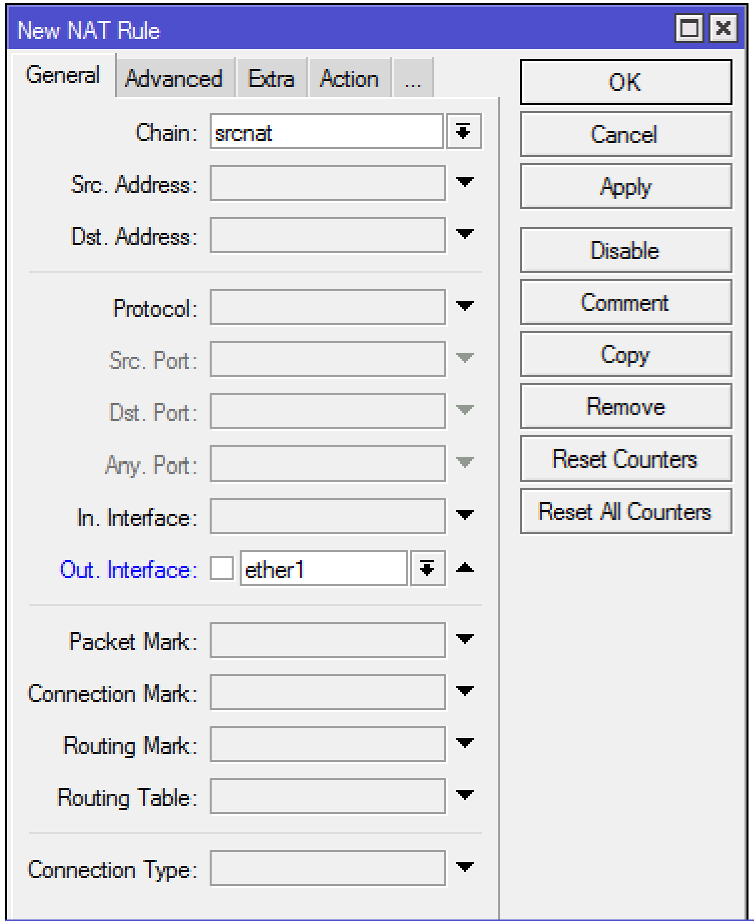
Cache Size: 2048 KiB

Cache Max TTL: 7d 00:00:00

Cache Used: 9

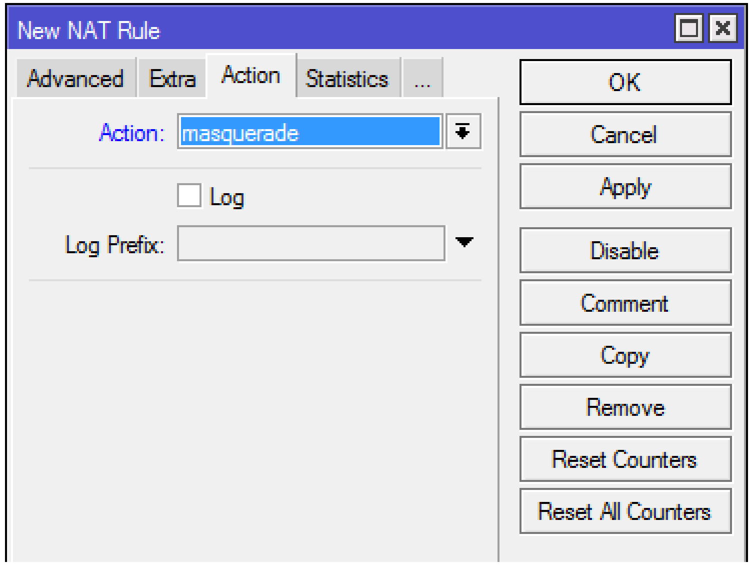
Create DNS & Allow Remote Request

2. Configure Internet on RouterBoard (NAT)



Chain: srcnat

Out. Interface: □ ether1

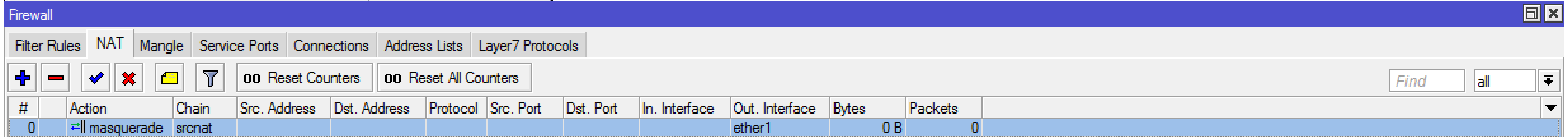


Action: masquerade

□ Log

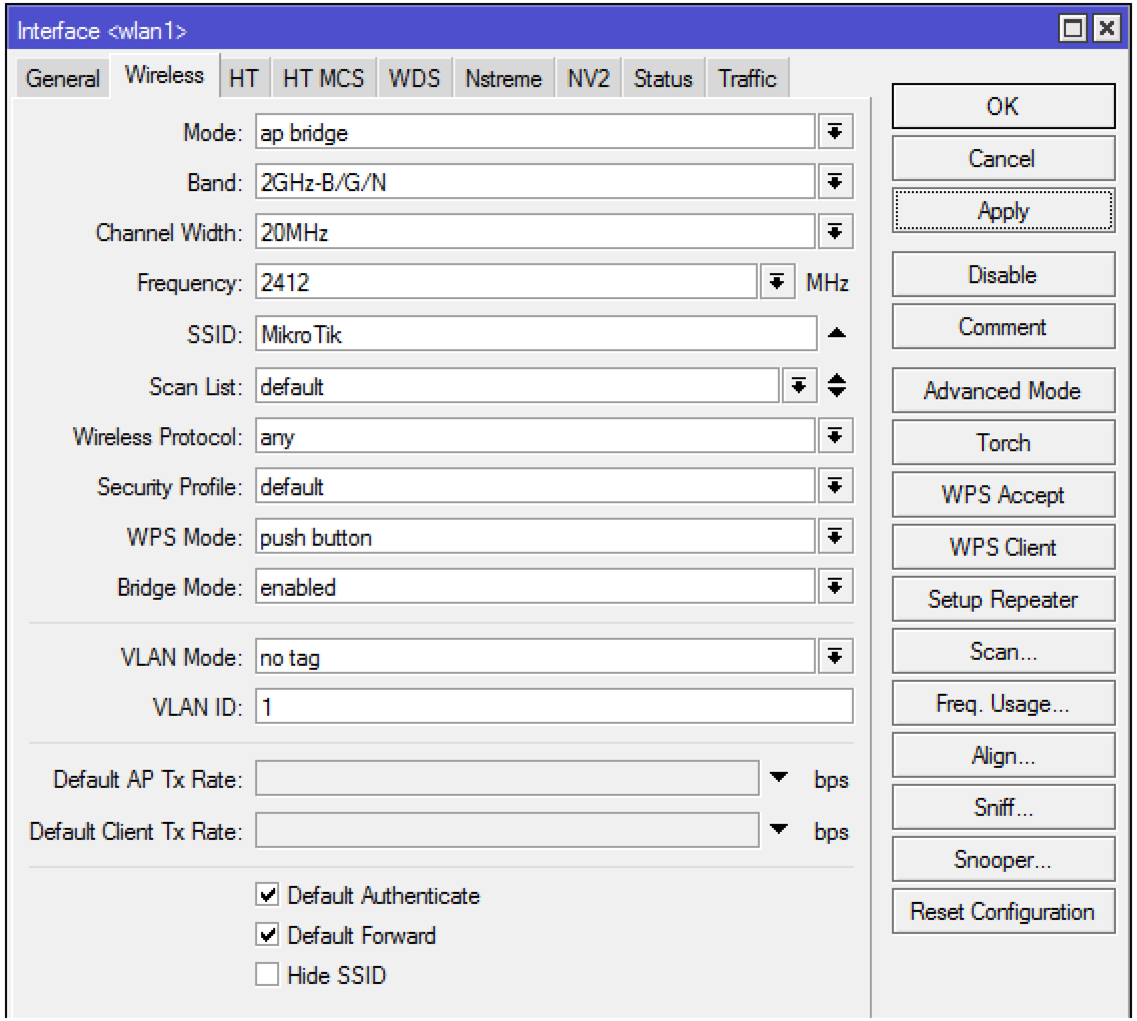
NAT Configuration

```
/ip firewall nat add chain=srcnat out-interface=ether1 action=masquerade
```



#		Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Interface	Out. Interface	Bytes	Packets
0		masquerade	srcnat							ether1	0 B	0

3. Configure Access Point



Interface <wlan1>

Mode: ap bridge

Band: 2GHz-B/G/N

Channel Width: 20MHz

Frequency: 2412 MHz

SSID: MikroTik

Scan List: default

Wireless Protocol: any

Security Profile: default

WPS Mode: push button

Bridge Mode: enabled

VLAN Mode: no tag

VLAN ID: 1

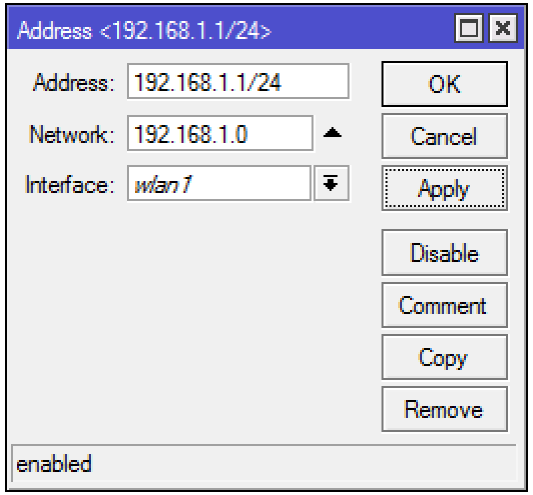
Default AP Tx Rate: bps

Default Client Tx Rate: bps

☑ Default Authenticate

☑ Default Forward

☐ Hide SSID



Address <192.168.1.1/24>

Address: 192.168.1.1/24

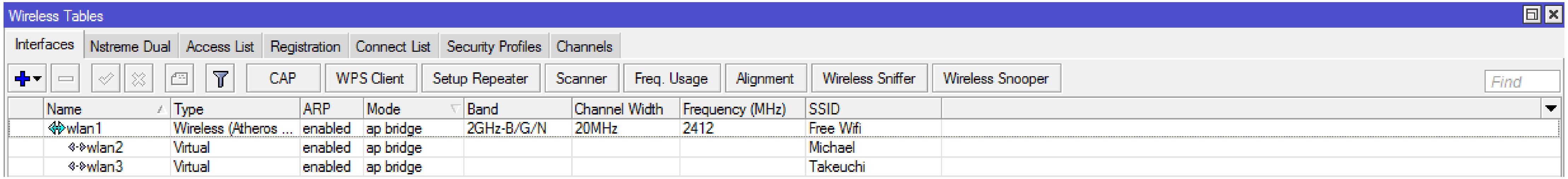
Network: 192.168.1.0

Interface: wlan1

enabled

Create AP with AP Bridge Mode and set an IP Address

4. DHCP Server & Multiple SSID

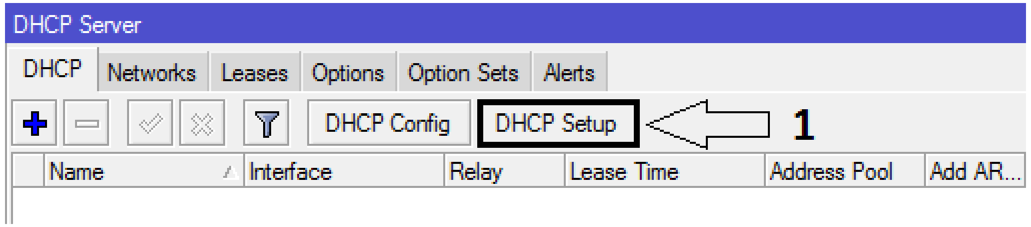


Wireless Tables

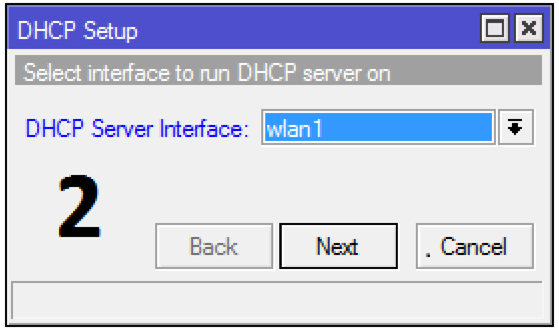
Name	Type	ARP	Mode	Band	Channel Width	Frequency (MHz)	SSID
wlan1	Wireless (Atheros ...	enabled	ap bridge	2GHz-B/G/N	20MHz	2412	Free Wifi
wlan2	Virtual	enabled	ap bridge				Michael
wlan3	Virtual	enabled	ap bridge				Takeuchi

Create Multiple SSID, Choose Intresting Wifi Name (SSID)

Then go to IP > DHCP Server > DHCP Setup



DHCP Server

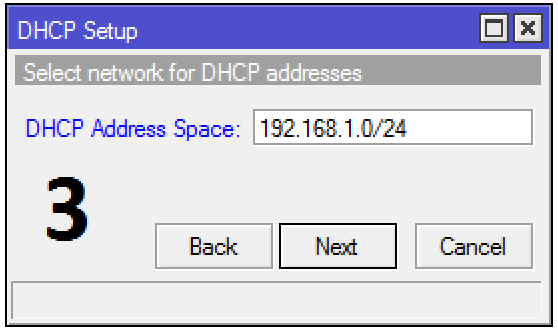


DHCP Setup

Select interface to run DHCP server on

DHCP Server Interface: wlan1

2

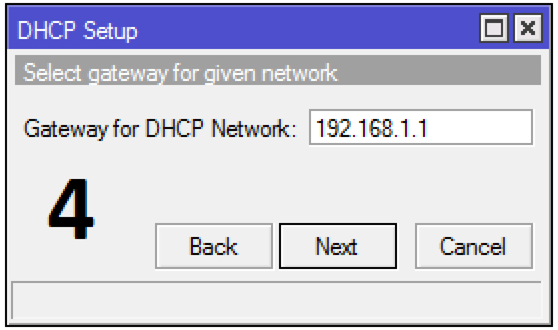


DHCP Setup

Select network for DHCP addresses

DHCP Address Space: 192.168.1.0/24

3

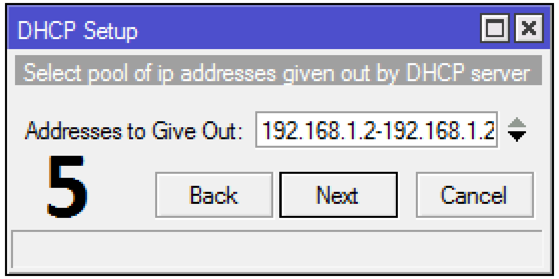


DHCP Setup

Select gateway for given network

Gateway for DHCP Network: 192.168.1.1

4

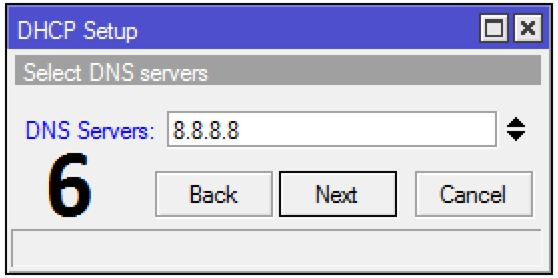


DHCP Setup

Select pool of ip addresses given out by DHCP server

Addresses to Give Out: 192.168.1.2-192.168.1.2

5

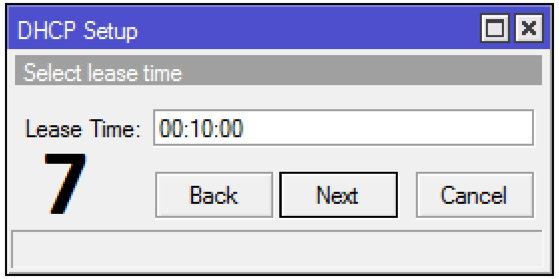


DHCP Setup

Select DNS servers

DNS Servers: 8.8.8.8

6



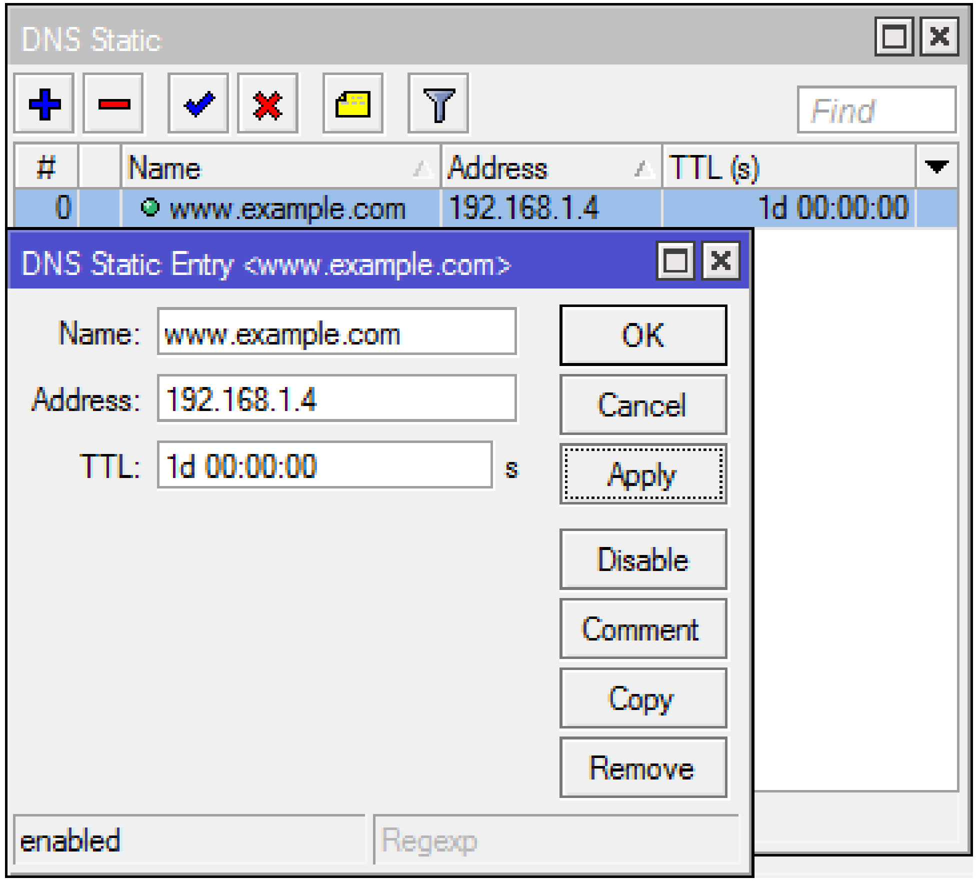
DHCP Setup

Select lease time

Lease Time: 00:10:00

7

5. Spoofing



DNS Static

#	Name	Address	TTL (s)
0	www.example.com	192.168.1.4	1d 00:00:00

DNS Static Entry <www.example.com>

Name: www.example.com

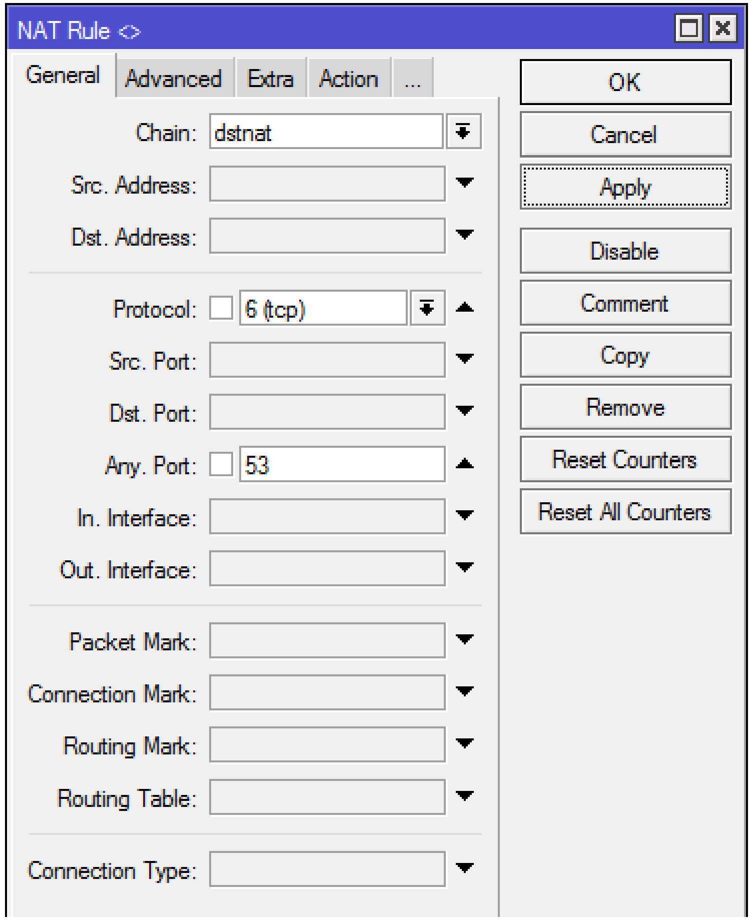
Address: 192.168.1.4

TTL: 1d 00:00:00 s

enabled

Address are filled with Attacker Web Server IP Address
Name are filled with Domain Name that we want to Spoof

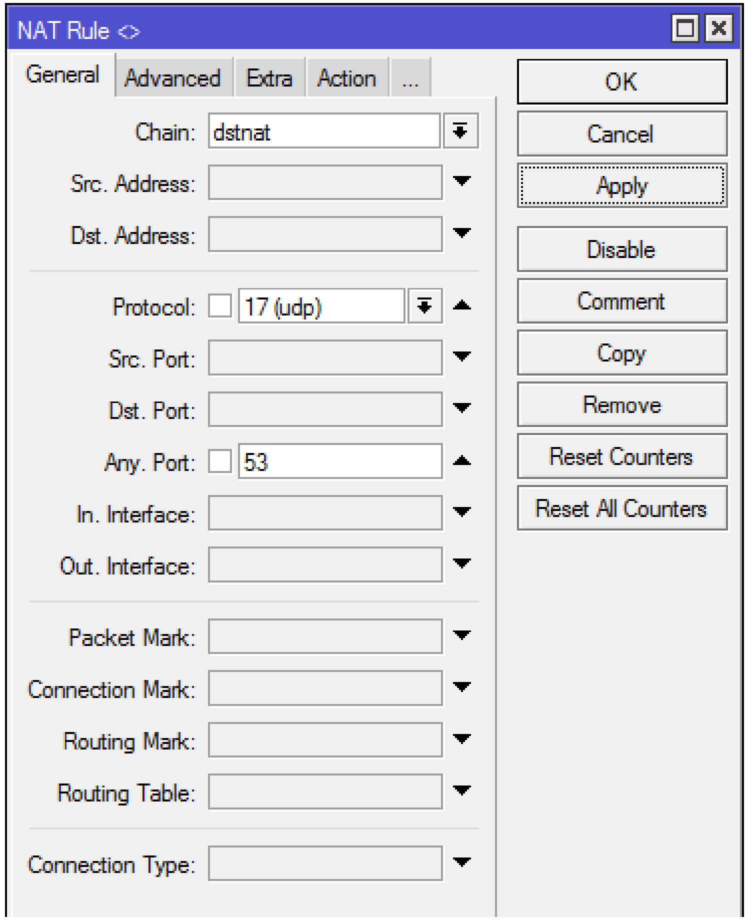
6. Transparent DNS (TCP & UDP)


NAT Rule <>

Chain: dstnat

Protocol: □ 6 (tcp)

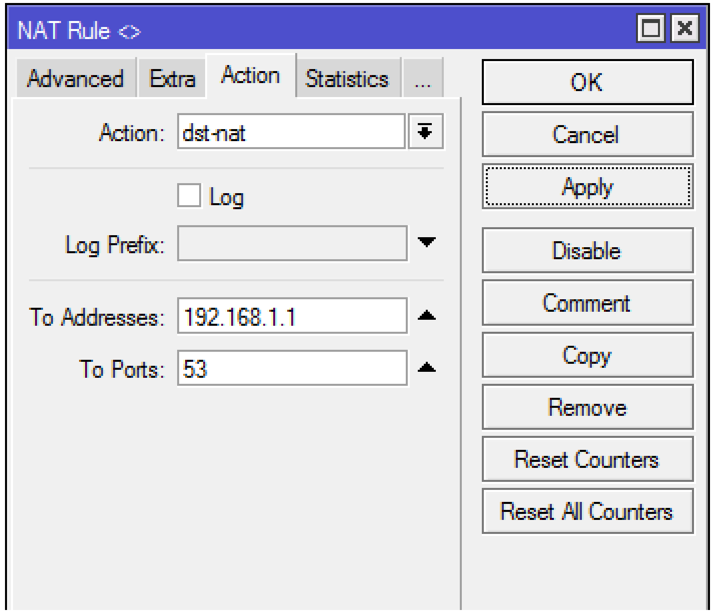
Any. Port: □ 53


NAT Rule <>

Chain: dstnat

Protocol: □ 17 (udp)

Any. Port: □ 53


NAT Rule <>

Action: dst-nat

□ Log

Log Prefix:

To Addresses: 192.168.1.1

To Ports: 53

Setup new rule with same action, port and chain, but has diffrent protocol

7. Force people Connect to Your AP

- Disconnecting other people from Main Access Point (Deauth) and make them connect to your Trap Access Point (without password)

How to do it? It’s Secret :P it’s too dangerous

But… I will tell you on back stage if you ask something to me on Questions & Answers Session

8. DNS Spoofing Target

- Social Media Account
- Bank Account
- Forum Account
- Another Account
- Create Fake Website
- **Sending Malware**

9. How to Secure Your System and Your Self?

Yourself :

- Don’t Trust Free Wifi
- Awareness

Network Engineer :

- Use Transport Layer Security (TLS)

Web Developer :

- Use Secure Socket Layer (SSL)

10. Summary

I was setup a fake login web server on 192.168.1.4 and when an user access www.example.com they will redirected to my fake login pages with domain www.example.com , this is so tricky for common users and this things can be applied on another login pages or you can manipulate some software link download and change it with your malware and controll they device hahaha *so evils, be aware !

Questions & Answers

Images was Taken from Google Images

Contact Me

- Facebook: https://www.facebook.com/mict404 (Michael Takeuchi)
- LinkedIn: https://www.linkedin.com/in/michael-takeuchi (Michael Takeuchi)
- WhatApps: +62 812-8188-9660
- Phone: +62 896-2626-2669
- Twitter: @mict404
- Blog: http://www.takeuchi.id
- Email: michael@takeuchi.id

Thank You !
For Time and Your Attention

and see u in the next MUM