WiFi lab časť 3
WiFi operation – riadiaca a managementová prevádzka

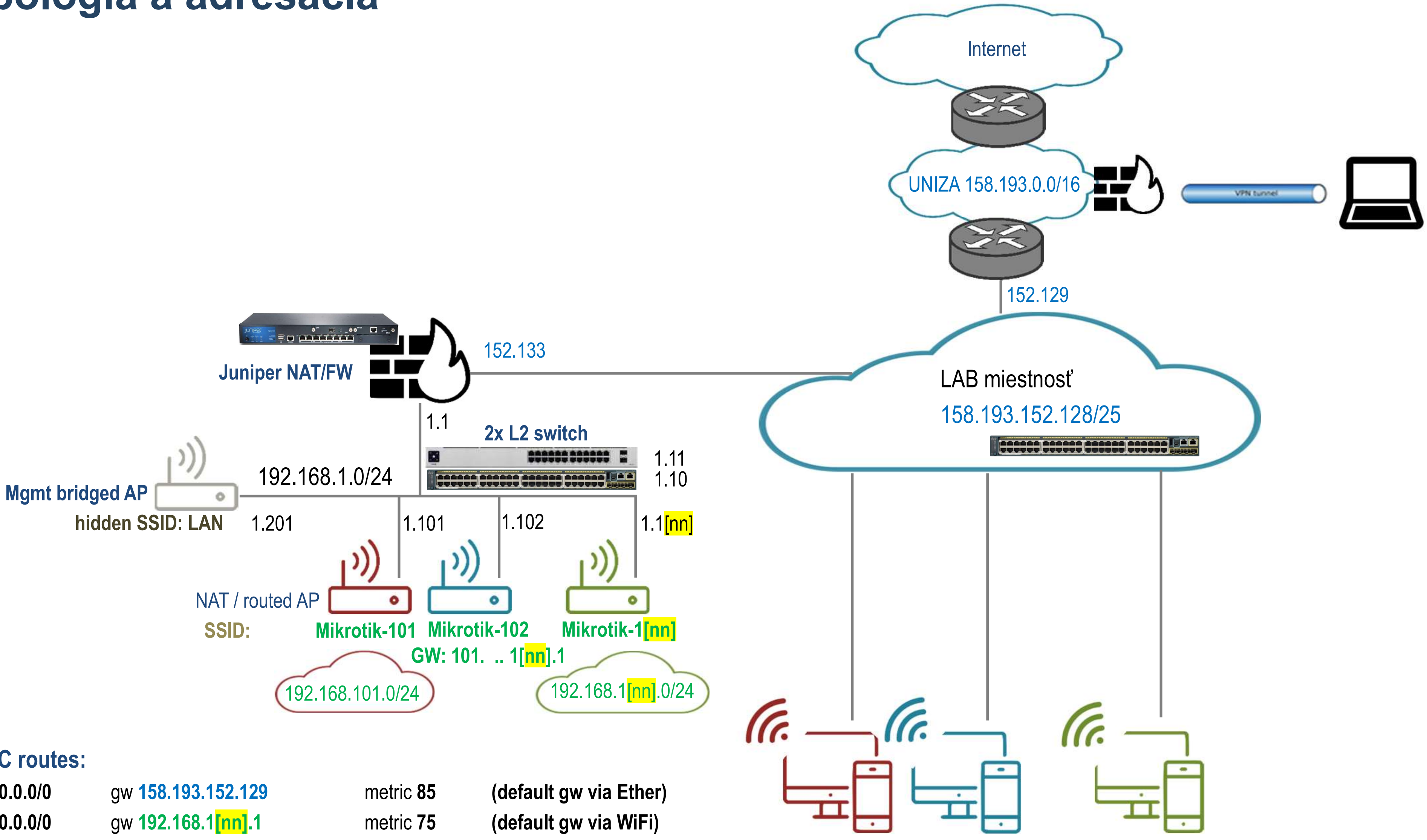
KIS FRI UNIZA

Vytvorené v rámci projektu **KEGA 026TUKE-4/2021**

Agenda

- Spustiť Oracle VM VirtualBox Manager & Kali linux appliance
- Zachytiť 802.11 asociačný proces klienta ku AP
- Odhaliť WPA2-PSK passprase (PSK) AP zariadenia

Topológia a adresácia



PC routes:

0.0.0.0/0	gw **158.193.152.129**	metric **85**	**(default gw via Ether)**
0.0.0.0/0	gw **192.168.1[nn].1**	metric **75**	**(default gw via WiFi)**
158.193.0.0/16	gw **158.193.152.129**	metric **25**	**(UNIZA net)**

Adresácia a skupiny

Skupina	Model	Meno	S/N	Wlan MAC	Ether MAC	SSID	WPA2 Pre-shared Key	NET	uplink	login	pass
1	411UAHR	Mikrotik 1	24D10199373A	00:0C:42:44:6F:8E	00:0C:42:44:6F:8D	Mikrotik-101	!234567*	192.168.101.1/24	192.168.1.101	admin	k!s143
2	411UAHR	Mikrotik 2	24D1019445AE	00:0C:42:49:1D:1A	00:0C:42:49:1D:19	Mikrotik-102	!234567*	192.168.102.1/24	192.168.1.102	admin	k!s143
3	411UAHR	Mikrotik 3	24D101944462	00:0C:42:49:1C:D6	00:0C:42:49:1C:D5	Mikrotik-103	!234567*	192.168.103.1/24	192.168.1.103	admin	k!s143
4	411UAHR	Mikrotik 4	24D1019445BE	00:0C:42:49:1D:0A	00:0C:42:49:1D:09	Mikrotik-104	!234567*	192.168.104.1/24	192.168.1.104	admin	k!s143
5	411UAHR	Mikrotik 5	24D10199371A	00:0C:42:44:6F:AE	00:0C:42:44:6F:AD	Mikrotik-105	!234567*	192.168.105.1/24	192.168.1.105	admin	k!s143
6	411UAHR	Mikrotik 6	24D1019445B4	00:0C:42:49:1D:04	00:0C:42:49:1D:03	Mikrotik-106	!234567*	192.168.106.1/24	192.168.1.106	admin	k!s143
7	411UAHR	Mikrotik 7	24D10194447C	00:0C:42:49:1C:CC	00:0C:42:49:1C:CB	Mikrotik-107	!234567*	192.168.107.1/24	192.168.1.107	admin	k!s143
8	411UAHR	Mikrotik 8	24D10199372A	00:0C:42:44:6F:9E	00:0C:42:44:6F:9D	Mikrotik-108	!234567*	192.168.108.1/24	192.168.1.108	admin	k!s143
9	411UAHR	Mikrotik 9	24D10194442A	00:0C:42:49:1C:9E	00:0C:42:49:1C:9D	Mikrotik-109	!234567*	192.168.109.1/24	192.168.1.109	admin	k!s143
10	411UAHR	Mikrotik 10	24D101993724	00:0C:42:44:6F:94	00:0C:42:44:6F:93	Mikrotik-110	!234567*	192.168.110.1/24	192.168.1.110	admin	k!s143
11	RB952Ui-5ac2nD	Mikrotik 11	CC3E0EDD4C25	2C:C8:1B:4C:F9:B6	2C:C8:1B:4C:F9:B0	Mikrotik-111	!234567*	192.168.111.1/24	192.168.1.111	admin	k!s143
12	RB952Ui-5ac2nD	Mikrotik 12	CC3E0E60402C	2C:C8:1B:4C:B0:40	2C:C8:1B:4C:B0:3A	Mikrotik-112	!234567*	192.168.112.1/24	192.168.1.112	admin	k!s143
13	RB952Ui-5ac2nD	Mikrotik 13	CC3E0E52B863	2C:C8:1B:4C:D3:E7	2C:C8:1B:4C:D3:E1	Mikrotik-113	!234567*	192.168.113.1/24	192.168.1.113	admin	k!s143
14	RB952Ui-5ac2nD	Mikrotik 14	CC3E0E83DB79	2C:C8:1B:25:F2:3A	2C:C8:1B:25:F2:34	Mikrotik-114	!234567*	192.168.114.1/24	192.168.1.114	admin	k!s143
15	RB952Ui-5ac2nD	Mikrotik 15	CC3E0EC59727	2C:C8:1B:26:04:26	2C:C8:1B:26:04:20	Mikrotik-115	!234567*	192.168.114.1/24	192.168.1.114	admin	k!s143

Prístupy

PC:

1.) Lokálny prístup alebo 2.) Remote Desktop Connection app - mstsc.exe (resp. iný program na vzdialené ovládanie počítača)

login/pass: RB03-[čísloPC]\student / student

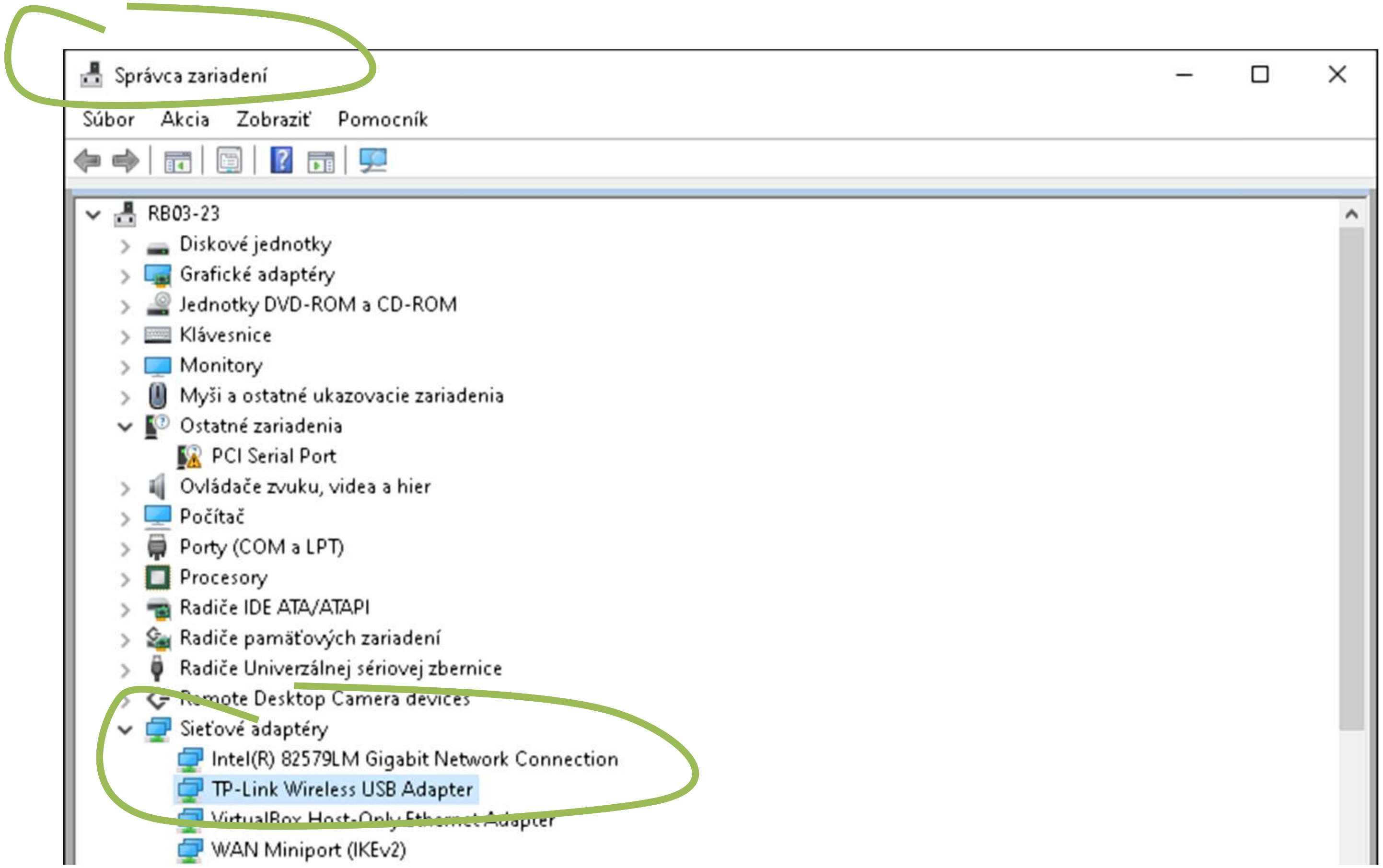
Mikrotik (v default móde):

default login/pass: admin / <blank>

default net: 192.168.88.1/24, alebo 0.0.0.0/0

prístup cez program Winbox a MAC adresu

Ethernet interfaces

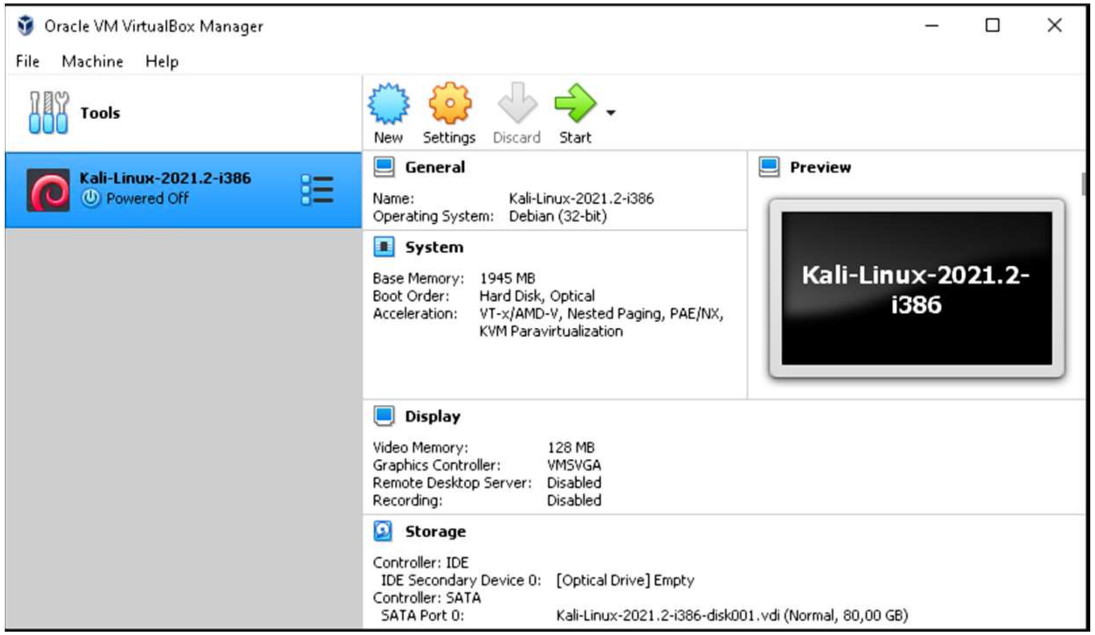


- RB03-23
  - Diskové jednotky
  - Grafické adaptéry
  - Jednotky DVD-ROM a CD-ROM
  - Klávesnice
  - Monitory
  - Myši a ostatné ukazovacie zariadenia
  - Ostatné zariadenia
    - PCI Serial Port
  - Ovládače zvuku, videa a hier
  - Počítač
  - Porty (COM a LPT)
  - Procesory
  - Radiče IDE ATA/ATAPI
  - Radiče pamäťových zariadení
  - Radiče Univerzálnej sériovej zbernice
  - Remote Desktop Camera devices
  - Sieťové adaptéry
    - Intel(R) 82579LM Gigabit Network Connection
    - TP-Link Wireless USB Adapter
    - VirtualBox Host-Only Ethernet Adapter
    - WAN Miniport (IKEv2)

Oracle VM VirtualBox Manager & Kali linux appliance

Kali:

login/pass: kali/kali



General

Name: Kali-Linux-2021.2-i386
Operating System: Debian (32-bit)

System

Base Memory: 1945 MB
Boot Order: Hard Disk, Optical
Acceleration: VT-x/AMD-V, Nested Paging, PAE/NX, KVM Paravirtualization

Display

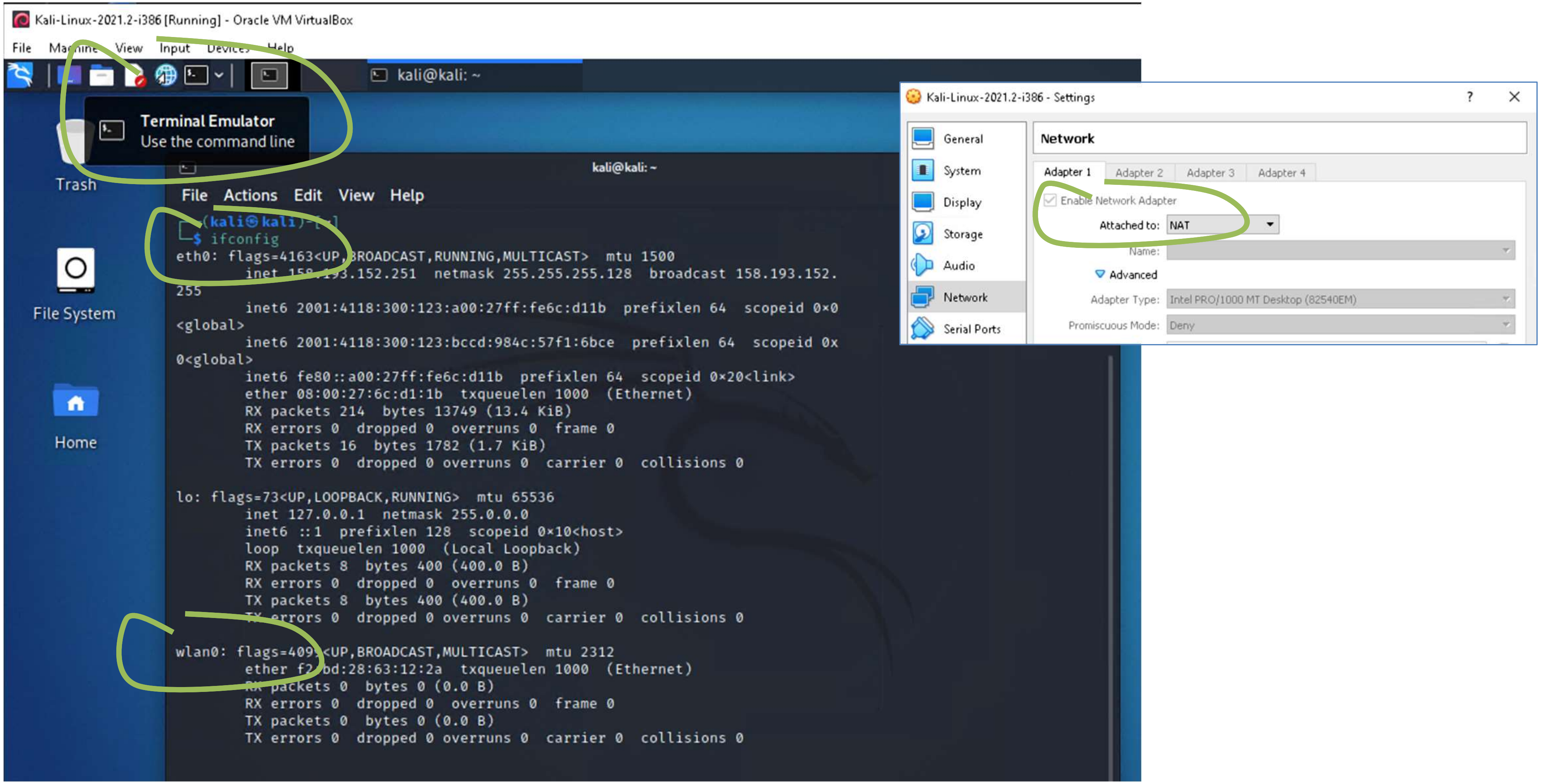
Video Memory: 128 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage

Controller: IDE
IDE Secondary Device 0: [Optical Drive] Empty
Controller: SATA
SATA Port 0: Kali-Linux-2021.2-i386-disk001.vdi (Normal, 80,00 GB)

Dôležité upozornenie: Zneužitie nástrojov, ktoré sú súčasťou Kali linuxu, je protiprávne a môže viesť ku trestnému vyšetrovaniu voči osobám, ktoré ich zneužili. Informácie v tomto učebnom materiáli a zmienené nástroje musia byť použité len na výukové účely a so zariadeniami na tento účel určenými.

Ethernet interfaces & Kali linux



```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 158.193.152.251  netmask 255.255.255.128  broadcast 158.193.152.
255
        inet6 2001:4118:300:123:a00:27ff:fe6c:d11b  prefixlen 64  scopeid 0x0
<global>
        inet6 2001:4118:300:123:bccd:984c:57f1:6bce  prefixlen 64  scopeid 0x
0<global>
        inet6 fe80::a00:27ff:fe6c:d11b  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:6c:d1:1b  txqueuelen 1000  (Ethernet)
        RX packets 214  bytes 13749 (13.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 16  bytes 1782 (1.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 400 (400.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 400 (400.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 2312
        ether f2:bd:28:63:12:2a  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

☑ Enable Network Adapter

Attached to: NAT

Name:

Advanced

Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

Promiscuous Mode: Deny

802.11 framing - summary

802.11 rámec

- **FC** - riadiace údaje – na ďalšom snímku
- Trvanie – čas potrebný pre prenos rámca medzi bezdrôtovými zariadeniami
- Adresa 1 – MAC adresa hostu alebo AP, ktorý má rámec prijať
- Adresa 2 – MAC adresa hostu alebo AP, ktorý rámec vysiela
- Adresa 3 – MAC adresa rozhrania smerovača, na ktorý je pripojený AP
- SEQ číslo – poradové číslo rámca v komunikácii (prebieha potvrdzovanie - Ack)
- Adresa 4 – používa sa len v ad-hoc móde
- Dáta – dáta zo sieťovej vrstvy
- FCS – kontrolný súčet (pre overenie správnosti)

FC	Duration /ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	DATA	FCS	
2	2	6	6	6	2	6	0-2312	4	**Bytes**

802.11 rámec – Frame Control

- Protocol version – číslo verzie protokolu 802.11
- Frame type – kontrolný, dátový
- Subtypes – napr. beacon, asociačný, autentifikačný, ..
- To AP / From AP – hodnota 1 identifikuje, či rámec ide smerom k AP alebo od AP
- More fragments – určuje, či je rámec fragmentovaný
- Retry – niekedy je nutné preposlať rovnaký rámec ešte raz a tento bit zabezpečí, že ostatné stanice si tento rámec nepomýlia s už raz odoslaným
- Power mngmt – indikuje, či sa po prenose prepne host do úsporného režimu
- Viac dát – nastavené na 1, ak host ešte bude vysielať
- WEP – nastavené na 1, ak je použitý WEP protokol

Protocol version	Frame type	Subtypy	To AP	From AP	More frag	Retry	Power mngmt	More data	WEP	Rsvd	
2	2	4	1	1	1	1	1	1	1	1	**bits**

Frame Subtypes

MANAGEMENT

- Beacon
- Probe Request & Response
- Authentication
- Deauthentication
- Association Request & Response
- Reassociation Request & Response
- Disassociation
- Announcement Traffic Indication Message (ATIM)

CONTROL

- RTS
- CTS
- ACK
- PS-Poll
- CF-End & CF-End ACK

DATA

- Data
- Data+CF-ACK
- Data+CF-Poll
- Data+CF-ACK+CF-Poll
- Null Function
- CF-ACK (nodata)
- CF-Poll (nodata)
- CF-ACK+CF+Poll

- Management frames are used to manage the BSS (Basic Service Sets)
  - Service Set is a group of wireless network devices which share a Service Set identifier (SSID)
- Control frames control access to the medium
- Data frames contain payloads that are the layer 3-7 information

802.11 association process

802.11 Association process

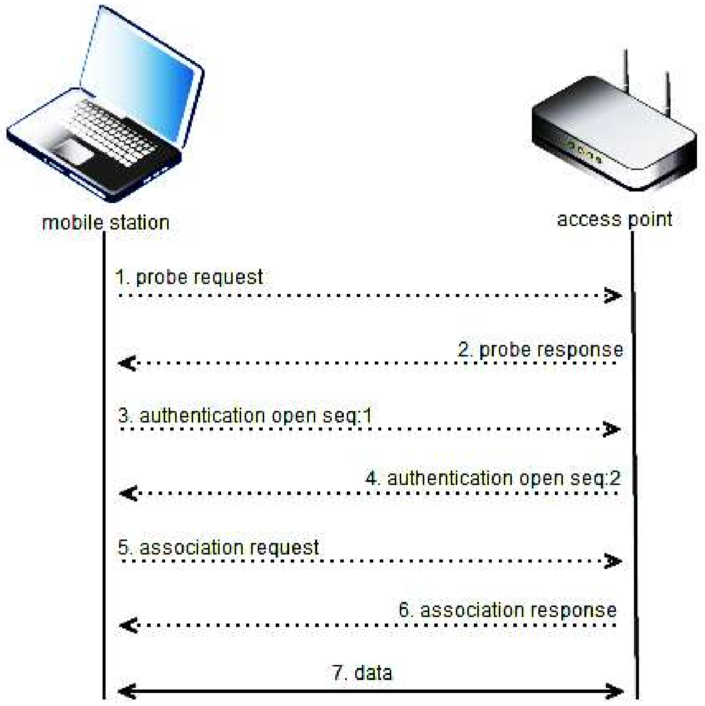
The three 802.11 connection states are:

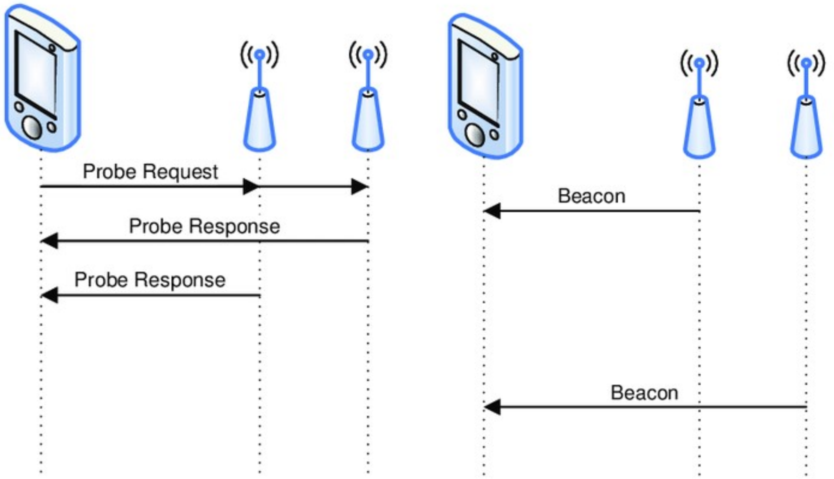
- Not authenticated or associated
- Authenticated but not yet associated
- Authenticated and associated

Two scanning methods to determine a suitable AP to which the client may need to connect:

- Active - the client transmits a probe request and listens for a probe response from an AP
- Passive - the client listens on each channel for *beacon* frames sent periodically by an AP. Typically it takes more time to connect

Note: If WPA/WPA2 or 802.1X authentication is required on the wireless network, the mobile station will not be able to send data until dynamic keying and authentication have taken place **after** the 802.11 Association is complete.

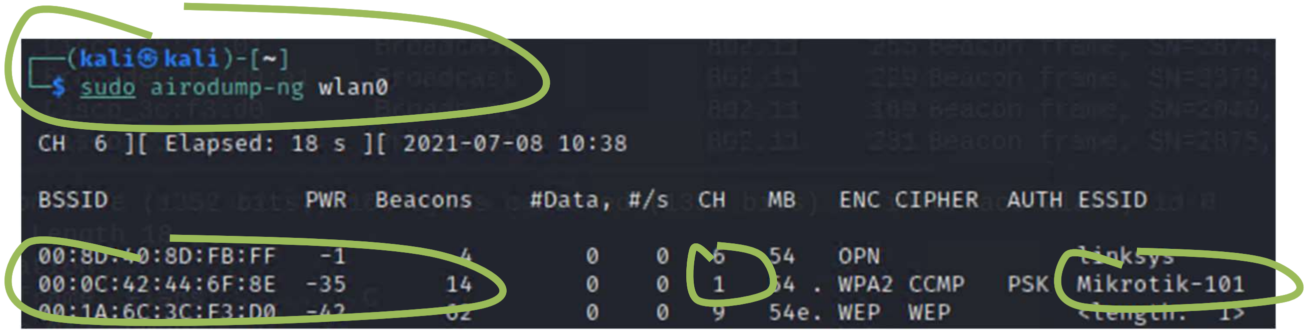




BSSID & client MAC address

Check status and MAC address: **sudo airdump-ng wlan0**

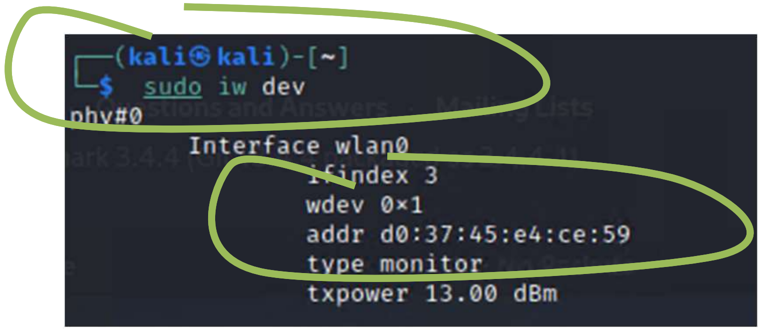
Note: Basic Service Set Identifier (BSSID) means simply MAC address of Access Point (AP)



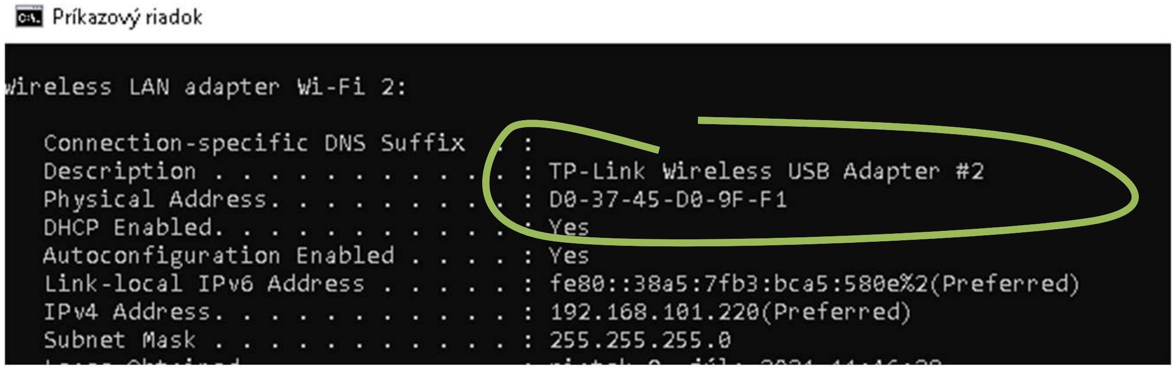
```
┌──(kali㉿kali)-[~]
└─$ sudo airodump-ng wlan0

 CH  6 ][ Elapsed: 18 s ][ 2021-07-08 10:38

 BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

 00:8D:40:8D:FB:FF   -1        4        0    0   6   54   OPN              Linksys
 00:0C:42:44:6F:8E  -35       14        0    0   1   54 . WPA2 CCMP   PSK  Mikrotik-101
 00:1A:6C:3C:F3:D0  -42       62        0    0   9   54e. WEP  WEP         <length:  1>
```

Check the wireless interface status and Linux & Windows client's MAC address:

sudo iw dev



```
┌──(kali㉿kali)-[~]
└─$ sudo iw dev
phy#0
        Interface wlan0
                ifindex 3
                wdev 0x1
                addr d0:37:45:e4:ce:59
                type monitor
                txpower 13.00 dBm
```

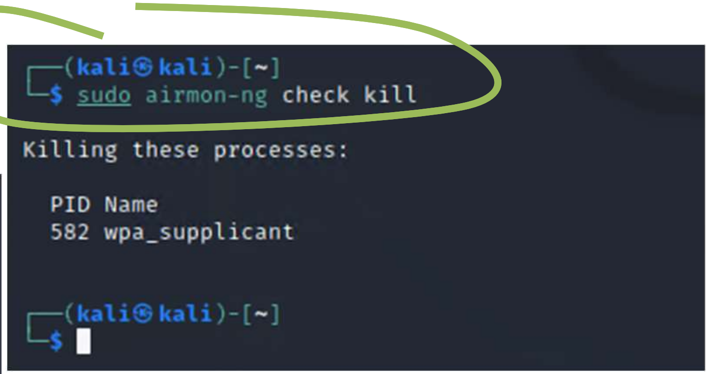


Príkazový riadok

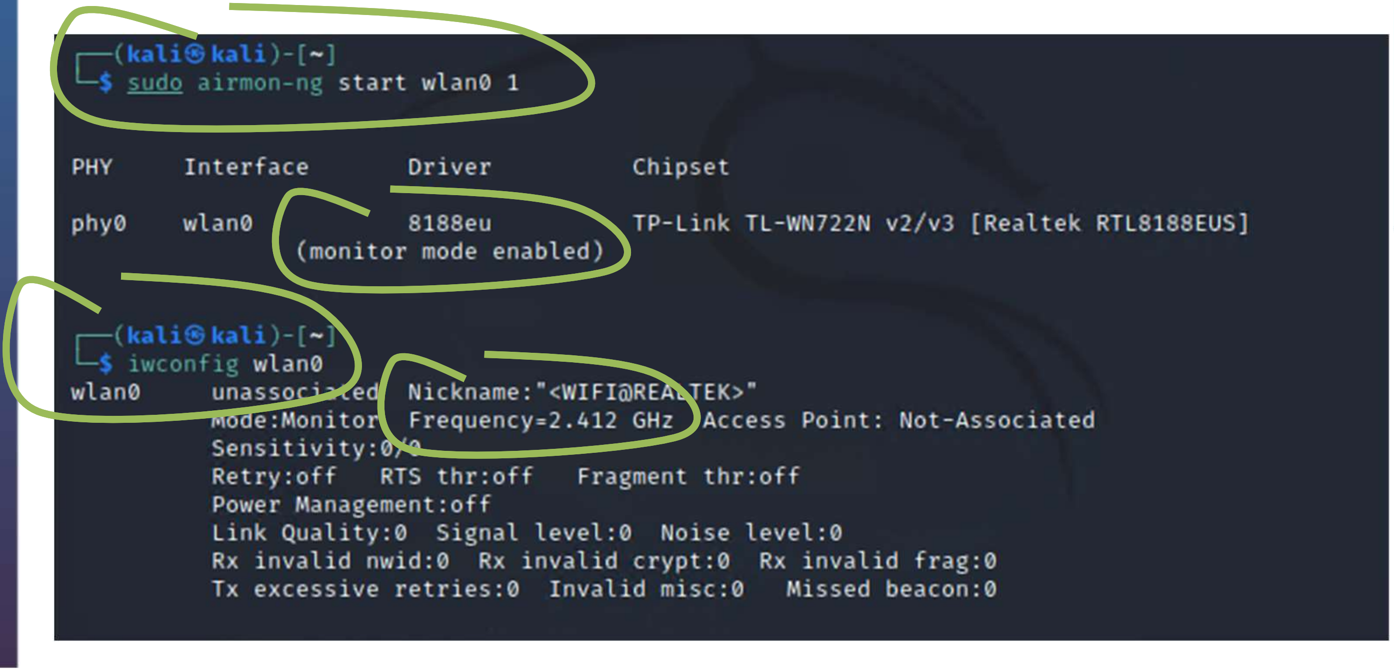
```
Wireless LAN adapter Wi-Fi 2:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : TP-Link Wireless USB Adapter #2
   Physical Address. . . . . . . . . : D0-37-45-D0-9F-F1
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::38a5:7fb3:bca5:580e%2(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.101.220(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : piatok 9. júla 2021 11:46:28
```

Enable wireless monitor mode

- "**Monitor mode**" allows to set the format of captured traffic to "802.11" format plus radiotap header. It enables to capture all packets on wireless interface, which are not only directed to our device but also other frames directed to devices connected to the network
  - *Highly preferred to monitor on relevant channel used by the specific AP (see previous slide)*
- To kill processes associated with wireless interface: **sudo airmon-ng check kill**
- Enable monitor mode: **sudo airmon-ng start wlan0 [channel]**
- Disable monitor mode: **sudo airmon-ng stop wlan0**
- Check interface status and frequency: **iwconfig wlan0**

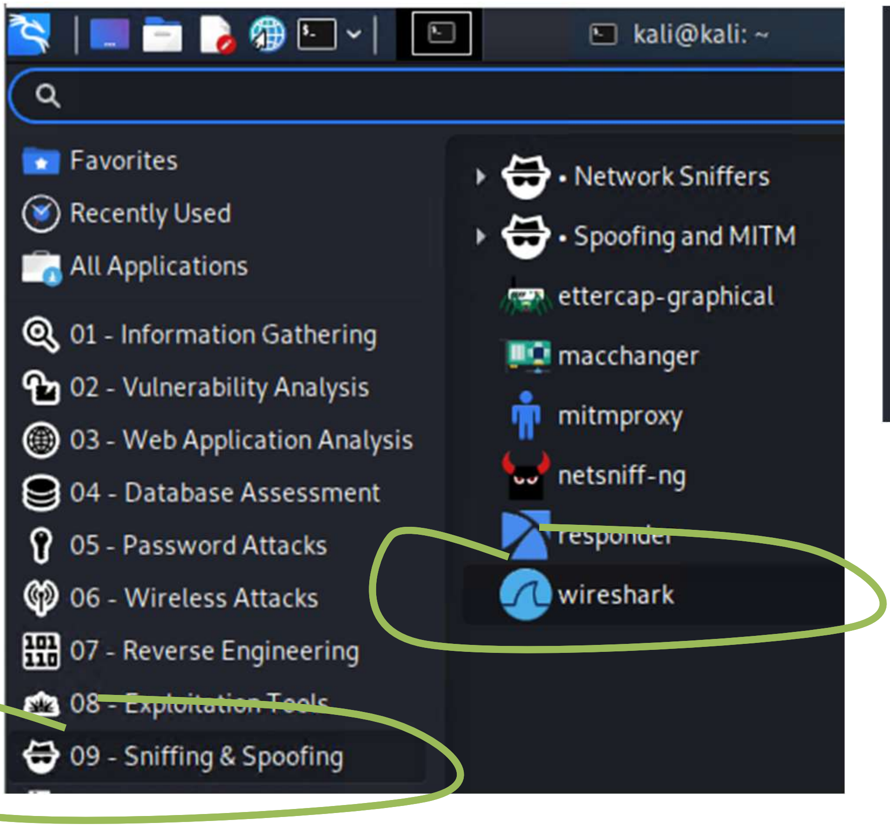


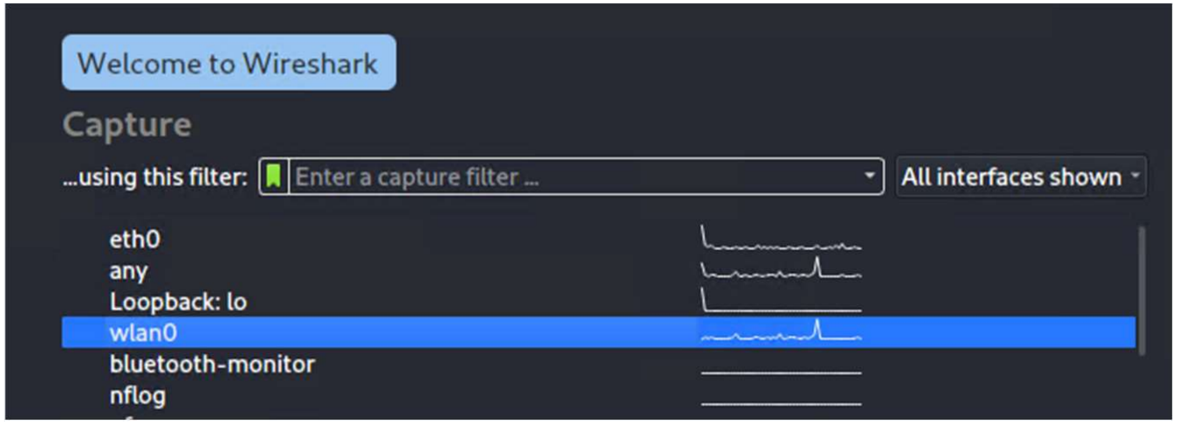
```
┌──(kali㉿kali)-[~]
└─$ sudo airmon-ng check kill

Killing these processes:

  PID Name
  582 wpa_supplicant


┌──(kali㉿kali)-[~]
└─$ █
```



```
┌──(kali㉿kali)-[~]
└─$ sudo airmon-ng start wlan0 1


PHY     Interface       Driver          Chipset

phy0    wlan0           8188eu          TP-Link TL-WN722N v2/v3 [Realtek RTL8188EUS]
                (monitor mode enabled)


┌──(kali㉿kali)-[~]
└─$ iwconfig wlan0
wlan0     unassociated  Nickname:"<WIFI@REALTEK>"
          Mode:Monitor  Frequency=2.412 GHz  Access Point: Not-Associated
          Sensitivity:0/0
          Retry:off   RTS thr:off   Fragment thr:off
          Power Management:off
          Link Quality:0  Signal level:0  Noise level:0
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0
```

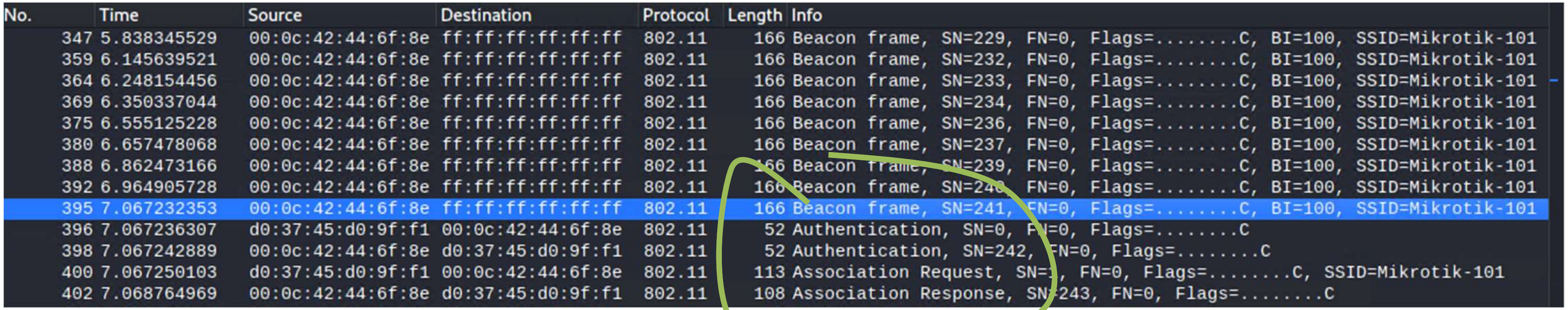
Wireshark





1. Run capturing on wireless interface
2. Connect from another (Windows) client to the AP

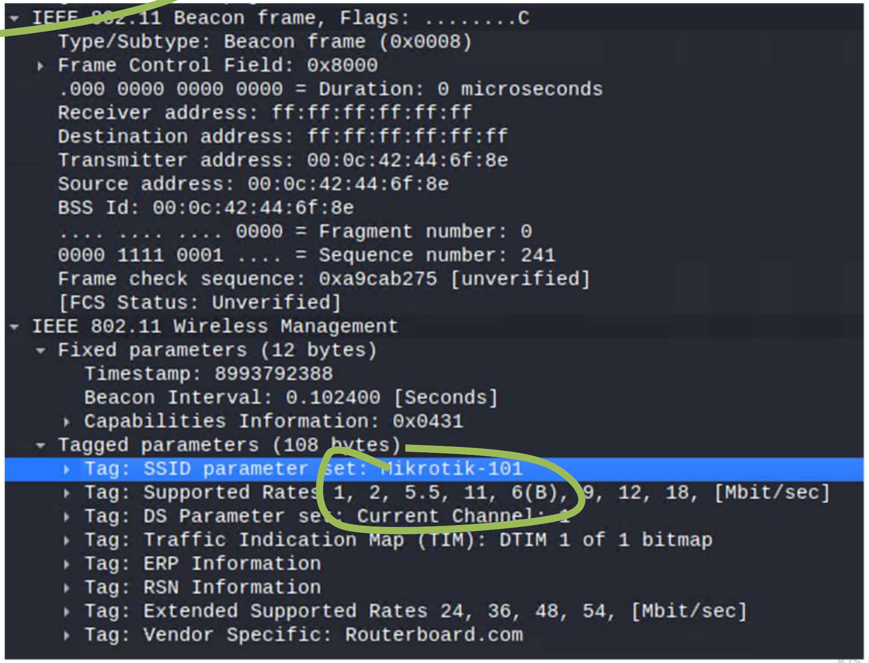
Wireshark: 802.11 Association process (unknown AP)



```
No.  Time         Source             Destination        Protocol  Length Info
 347 5.838345529  00:0c:42:44:6f:8e  ff:ff:ff:ff:ff:ff  802.11      166 Beacon frame, SN=229, FN=0, Flags=........C, BI=100, SSID=Mikrotik-101
 359 6.145639521  00:0c:42:44:6f:8e  ff:ff:ff:ff:ff:ff  802.11      166 Beacon frame, SN=232, FN=0, Flags=........C, BI=100, SSID=Mikrotik-101
 364 6.248154456  00:0c:42:44:6f:8e  ff:ff:ff:ff:ff:ff  802.11      166 Beacon frame, SN=233, FN=0, Flags=........C, BI=100, SSID=Mikrotik-101
 369 6.350337044  00:0c:42:44:6f:8e  ff:ff:ff:ff:ff:ff  802.11      166 Beacon frame, SN=234, FN=0, Flags=........C, BI=100, SSID=Mikrotik-101
 375 6.555125228  00:0c:42:44:6f:8e  ff:ff:ff:ff:ff:ff  802.11      166 Beacon frame, SN=236, FN=0, Flags=........C, BI=100, SSID=Mikrotik-101
 380 6.657478068  00:0c:42:44:6f:8e  ff:ff:ff:ff:ff:ff  802.11      166 Beacon frame, SN=237, FN=0, Flags=........C, BI=100, SSID=Mikrotik-101
 388 6.862473166  00:0c:42:44:6f:8e  ff:ff:ff:ff:ff:ff  802.11      166 Beacon frame, SN=239, FN=0, Flags=........C, BI=100, SSID=Mikrotik-101
 392 6.964905728  00:0c:42:44:6f:8e  ff:ff:ff:ff:ff:ff  802.11      166 Beacon frame, SN=240, FN=0, Flags=........C, BI=100, SSID=Mikrotik-101
 395 7.067232353  00:0c:42:44:6f:8e  ff:ff:ff:ff:ff:ff  802.11      166 Beacon frame, SN=241, FN=0, Flags=........C, BI=100, SSID=Mikrotik-101
 396 7.067236307  d0:37:45:d0:9f:f1  00:0c:42:44:6f:8e  802.11       52 Authentication, SN=0, FN=0, Flags=........C
 398 7.067242889  00:0c:42:44:6f:8e  d0:37:45:d0:9f:f1  802.11       52 Authentication, SN=242, FN=0, Flags=........C
 400 7.067250103  d0:37:45:d0:9f:f1  00:0c:42:44:6f:8e  802.11      113 Association Request, SN=1, FN=0, Flags=........C, SSID=Mikrotik-101
 402 7.068764969  00:0c:42:44:6f:8e  d0:37:45:d0:9f:f1  802.11      108 Association Response, SN=243, FN=0, Flags=........C
```

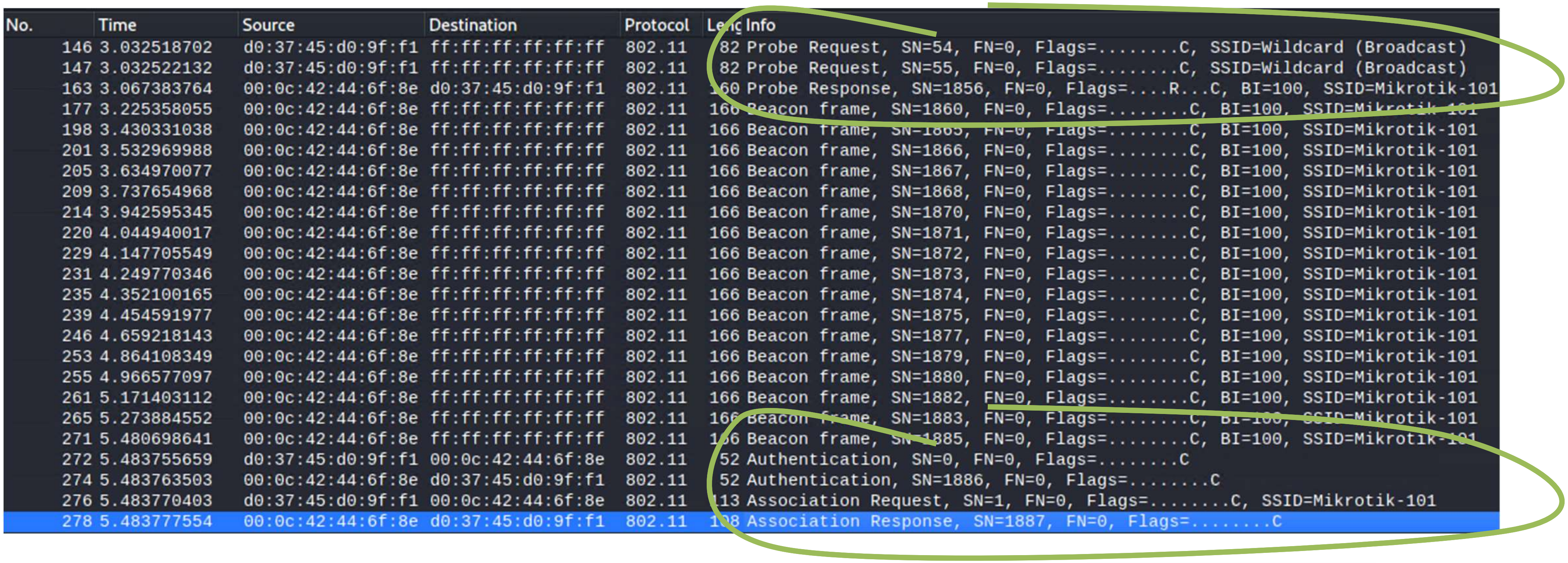
Wireshark filter:

(wlan.addr == 00:0c:42:44:6f:8e && wlan.addr == D0:37:45:D0:9F:F1) ||
(wlan.addr == 00:0c:42:44:6f:8e && wlan.addr == FF:FF:FF:FF:FF:FF) ||
(wlan.addr == FF:FF:FF:FF:FF:FF && wlan.addr == D0:37:45:D0:9F:F1)



```
▾ IEEE 802.11 Beacon frame, Flags: ........C
    Type/Subtype: Beacon frame (0x0008)
  ▸ Frame Control Field: 0x8000
    .000 0000 0000 0000 = Duration: 0 microseconds
    Receiver address: ff:ff:ff:ff:ff:ff
    Destination address: ff:ff:ff:ff:ff:ff
    Transmitter address: 00:0c:42:44:6f:8e
    Source address: 00:0c:42:44:6f:8e
    BSS Id: 00:0c:42:44:6f:8e
    .... .... .... 0000 = Fragment number: 0
    0000 1111 0001 .... = Sequence number: 241
    Frame check sequence: 0xa9cab275 [unverified]
    [FCS Status: Unverified]
▾ IEEE 802.11 Wireless Management
  ▾ Fixed parameters (12 bytes)
      Timestamp: 8993792388
      Beacon Interval: 0.102400 [Seconds]
    ▸ Capabilities Information: 0x0431
  ▾ Tagged parameters (108 bytes)
    ▸ Tag: SSID parameter set: Mikrotik-101
    ▸ Tag: Supported Rates 1, 2, 5.5, 11, 6(B), 9, 12, 18, [Mbit/sec]
    ▸ Tag: DS Parameter set: Current Channel: 1
    ▸ Tag: Traffic Indication Map (TIM): DTIM 1 of 1 bitmap
    ▸ Tag: ERP Information
    ▸ Tag: RSN Information
    ▸ Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
    ▸ Tag: Vendor Specific: Routerboard.com
```

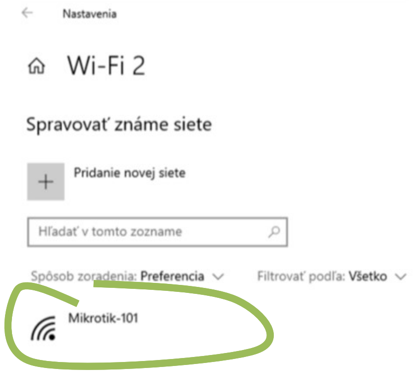
Wireshark: 802.11 Association process (known AP to Windows system)



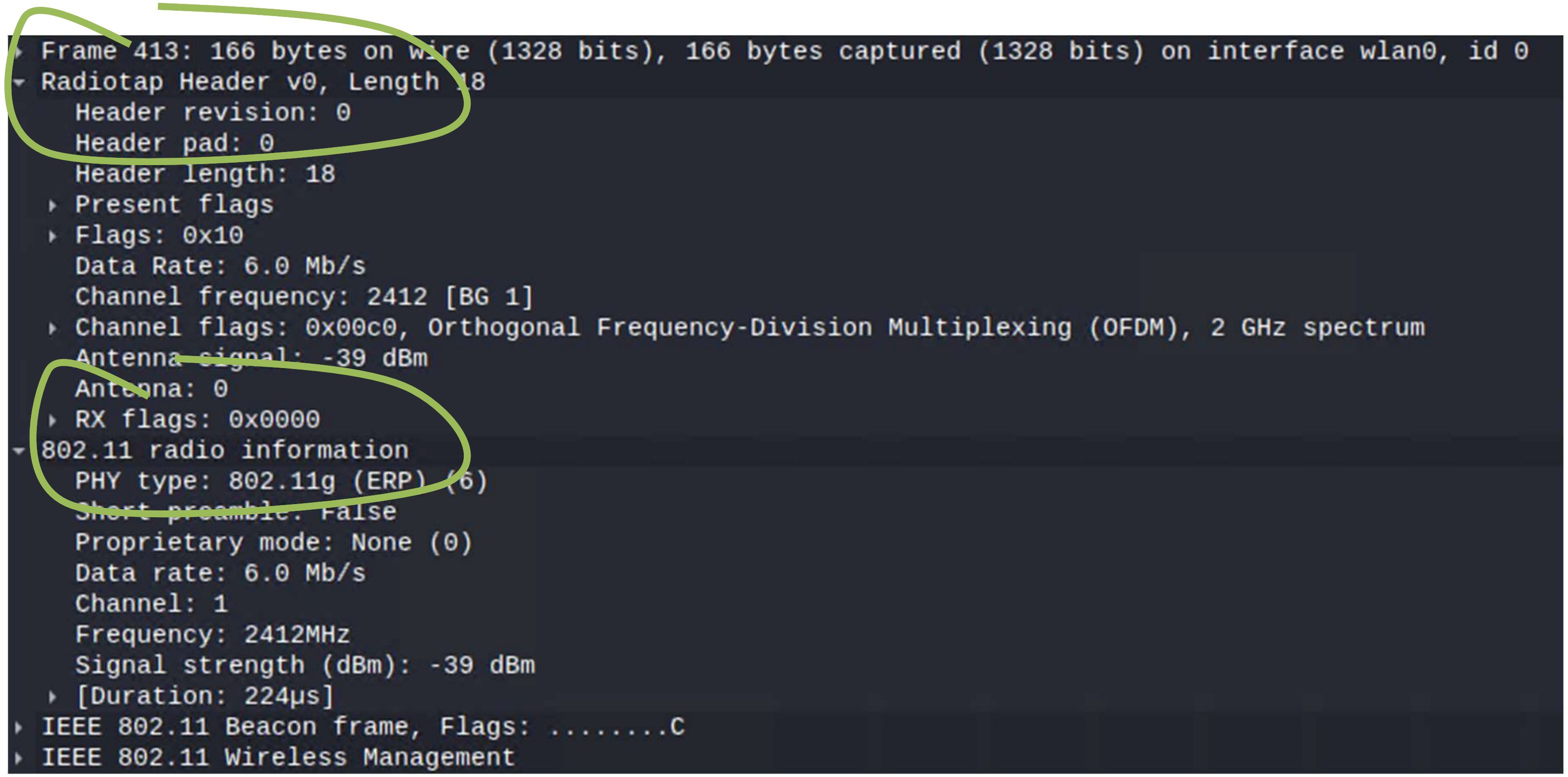
```
No.      Time         Source             Destination        Protocol  Leng Info
     146 3.032518702  d0:37:45:d0:9f:f1  ff:ff:ff:ff:ff:ff  802.11     82 Probe Request, SN=54, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
     147 3.032522132  d0:37:45:d0:9f:f1  ff:ff:ff:ff:ff:ff  802.11     82 Probe Request, SN=55, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
     163 3.067383764  00:0c:42:44:6f:8e  d0:37:45:d0:9f:f1  802.11    160 Probe Response, SN=1856, FN=0, Flags=....R...C, BI=100, SSID=Mikrotik-101
     177 3.225358055  00:0c:42:44:6f:8e  ff:ff:ff:ff:ff:ff  802.11    166 Beacon frame, SN=1860, FN=0, Flags=........C, BI=100, SSID=Mikrotik-101
     198 3.430331038  00:0c:42:44:6f:8e  ff:ff:ff:ff:ff:ff  802.11    166 Beacon frame, SN=1865, FN=0, Flags=........C, BI=100, SSID=Mikrotik-101
     201 3.532969988  00:0c:42:44:6f:8e  ff:ff:ff:ff:ff:ff  802.11    166 Beacon frame, SN=1866, FN=0, Flags=........C, BI=100, SSID=Mikrotik-101
     205 3.634970077  00:0c:42:44:6f:8e  ff:ff:ff:ff:ff:ff  802.11    166 Beacon frame, SN=1867, FN=0, Flags=........C, BI=100, SSID=Mikrotik-101
     209 3.737654968  00:0c:42:44:6f:8e  ff:ff:ff:ff:ff:ff  802.11    166 Beacon frame, SN=1868, FN=0, Flags=........C, BI=100, SSID=Mikrotik-101
     214 3.942595345  00:0c:42:44:6f:8e  ff:ff:ff:ff:ff:ff  802.11    166 Beacon frame, SN=1870, FN=0, Flags=........C, BI=100, SSID=Mikrotik-101
     220 4.044940017  00:0c:42:44:6f:8e  ff:ff:ff:ff:ff:ff  802.11    166 Beacon frame, SN=1871, FN=0, Flags=........C, BI=100, SSID=Mikrotik-101
     229 4.147705549  00:0c:42:44:6f:8e  ff:ff:ff:ff:ff:ff  802.11    166 Beacon frame, SN=1872, FN=0, Flags=........C, BI=100, SSID=Mikrotik-101
     231 4.249770346  00:0c:42:44:6f:8e  ff:ff:ff:ff:ff:ff  802.11    166 Beacon frame, SN=1873, FN=0, Flags=........C, BI=100, SSID=Mikrotik-101
     235 4.352100165  00:0c:42:44:6f:8e  ff:ff:ff:ff:ff:ff  802.11    166 Beacon frame, SN=1874, FN=0, Flags=........C, BI=100, SSID=Mikrotik-101
     239 4.454591977  00:0c:42:44:6f:8e  ff:ff:ff:ff:ff:ff  802.11    166 Beacon frame, SN=1875, FN=0, Flags=........C, BI=100, SSID=Mikrotik-101
     246 4.659218143  00:0c:42:44:6f:8e  ff:ff:ff:ff:ff:ff  802.11    166 Beacon frame, SN=1877, FN=0, Flags=........C, BI=100, SSID=Mikrotik-101
     253 4.864108349  00:0c:42:44:6f:8e  ff:ff:ff:ff:ff:ff  802.11    166 Beacon frame, SN=1879, FN=0, Flags=........C, BI=100, SSID=Mikrotik-101
     255 4.966577097  00:0c:42:44:6f:8e  ff:ff:ff:ff:ff:ff  802.11    166 Beacon frame, SN=1880, FN=0, Flags=........C, BI=100, SSID=Mikrotik-101
     261 5.171403112  00:0c:42:44:6f:8e  ff:ff:ff:ff:ff:ff  802.11    166 Beacon frame, SN=1882, FN=0, Flags=........C, BI=100, SSID=Mikrotik-101
     265 5.273884552  00:0c:42:44:6f:8e  ff:ff:ff:ff:ff:ff  802.11    166 Beacon frame, SN=1883, FN=0, Flags=........C, BI=100, SSID=Mikrotik-101
     271 5.480698641  00:0c:42:44:6f:8e  ff:ff:ff:ff:ff:ff  802.11    166 Beacon frame, SN=1885, FN=0, Flags=........C, BI=100, SSID=Mikrotik-101
     272 5.483755659  d0:37:45:d0:9f:f1  00:0c:42:44:6f:8e  802.11     52 Authentication, SN=0, FN=0, Flags=........C
     274 5.483763503  00:0c:42:44:6f:8e  d0:37:45:d0:9f:f1  802.11     52 Authentication, SN=1886, FN=0, Flags=........C
     276 5.483770403  d0:37:45:d0:9f:f1  00:0c:42:44:6f:8e  802.11    113 Association Request, SN=1, FN=0, Flags=........C, SSID=Mikrotik-101
     278 5.483777554  00:0c:42:44:6f:8e  d0:37:45:d0:9f:f1  802.11    108 Association Response, SN=1887, FN=0, Flags=........C
```

Wireshark filter:

(wlan.addr == 00:0c:42:44:6f:8e && wlan.addr == D0:37:45:D0:9F:F1) ||
(wlan.addr == 00:0c:42:44:6f:8e && wlan.addr == FF:FF:FF:FF:FF:FF) ||
(wlan.addr == FF:FF:FF:FF:FF:FF && wlan.addr == D0:37:45:D0:9F:F1)



802.11 frame structure



```
▸ Frame 413: 166 bytes on wire (1328 bits), 166 bytes captured (1328 bits) on interface wlan0, id 0
▾ Radiotap Header v0, Length 18
    Header revision: 0
    Header pad: 0
    Header length: 18
  ▸ Present flags
  ▸ Flags: 0x10
    Data Rate: 6.0 Mb/s
    Channel frequency: 2412 [BG 1]
  ▸ Channel flags: 0x00c0, Orthogonal Frequency-Division Multiplexing (OFDM), 2 GHz spectrum
    Antenna signal: -39 dBm
    Antenna: 0
  ▸ RX flags: 0x0000
▾ 802.11 radio information
    PHY type: 802.11g (ERP) (6)
    Short preamble: False
    Proprietary mode: None (0)
    Data rate: 6.0 Mb/s
    Channel: 1
    Frequency: 2412MHz
    Signal strength (dBm): -39 dBm
  ▸ [Duration: 224µs]
▸ IEEE 802.11 Beacon frame, Flags: ........C
▸ IEEE 802.11 Wireless Management
```

- Radiotap & “802.11 radio information” is a record created by Wireshark to capture and present physical layer parameters. This is not part of 802.11 header

Úlohy

- Požiadajte inú skupinu aby sa vo vhodnom okamžiku pripojili na vaše AP
- Zachytiť a stručne zdokumentovať prostredníctvom programu Wireshark v Kali linuxe fázu vyhľadania AP, autentifikácie a vytvorenia asociácie
- Odpovedzte aj na nasledujúce otázky:
  - Aká je zdrojová a cieľová L2 adresa *Probe request* rámca?
  - Aké sú sekvenčné hodnoty pri autentifikačných rámcoch?
  - Aký typ šifrovania si klient zvolil na komunikáciu v asociačnej požiadavke?

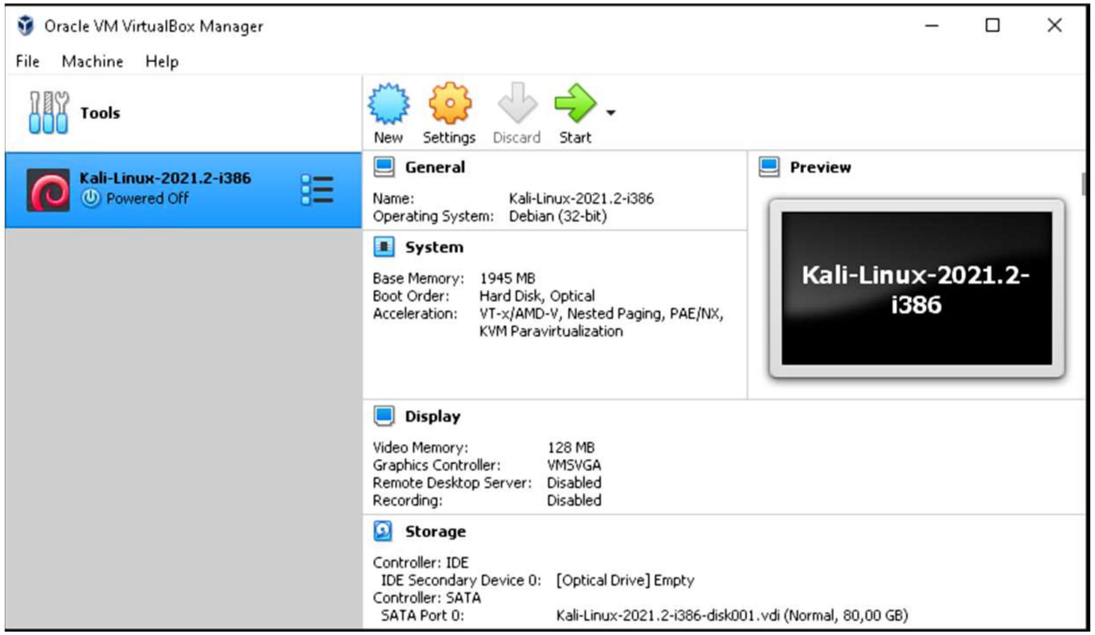
Poznámka: príkaz sudo alebo “super user do!” umožňuje spustit program s privilégiami iného užívateľa, zvyčajne ako superuser, resp. administrátor systému.

Penetration testing: Wifite

Oracle VM VirtualBox Manager & Kali linux appliance

Kali:

login/pass: kali/kali



General

Name: Kali-Linux-2021.2-i386
Operating System: Debian (32-bit)

System

Base Memory: 1945 MB
Boot Order: Hard Disk, Optical
Acceleration: VT-x/AMD-V, Nested Paging, PAE/NX, KVM Paravirtualization

Display

Video Memory: 128 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled

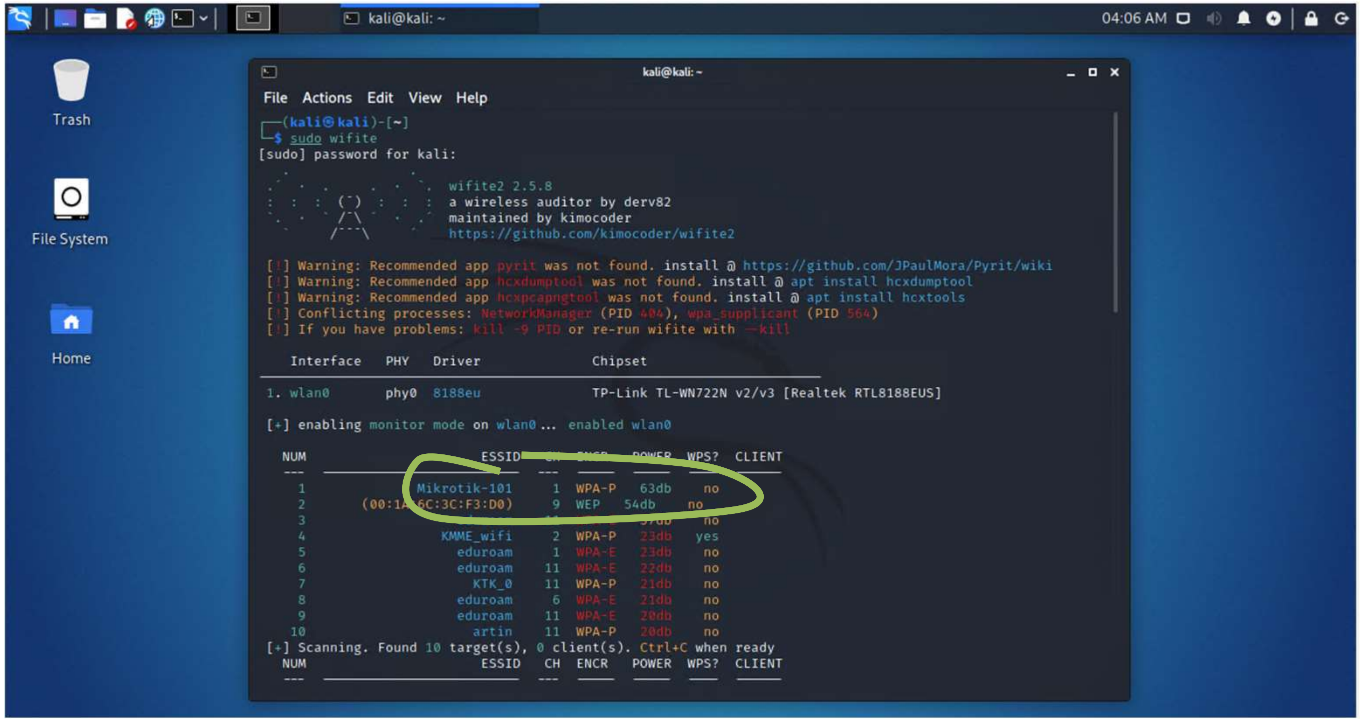
Storage

Controller: IDE
IDE Secondary Device 0: [Optical Drive] Empty
Controller: SATA
SATA Port 0: Kali-Linux-2021.2-i386-disk001.vdi (Normal, 80,00 GB)

Dôležité upozornenie: Zneužitie nástrojov, ktoré sú súčasťou Kali linuxu, je protiprávne a môže viesť ku trestnému vyšetrovaniu voči osobám, ktoré ich zneužili. Informácie v tomto učebnom materiáli a zmienené nástroje musia byť použité len na výukové účely a so zariadeniami na tento účel určenými.

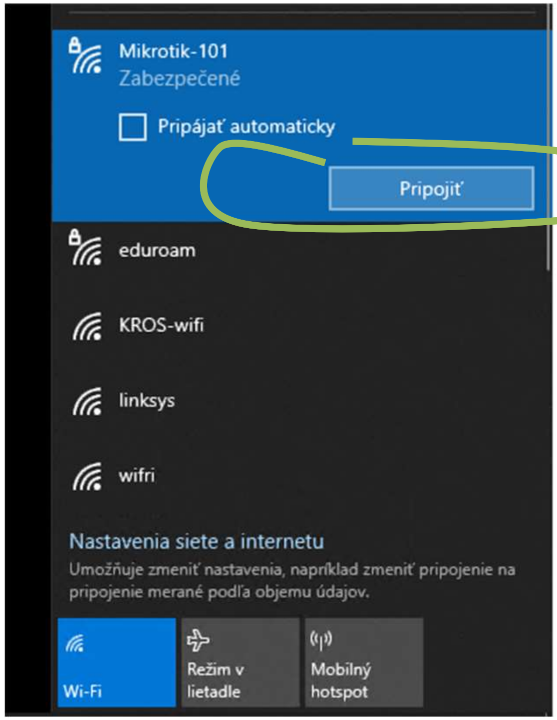
Wifite – scanning wireless networks & listening for handshake

1. kali> sudo wifite --kill
2. Select wireless network



```
┌──(kali㉿kali)-[~]
└─$ sudo wifite
[sudo] password for kali:
   .               .
 .´  ·  .     .  ·  `.  wifite2 2.5.8
 :  :  :  (¯)  :  :  :  a wireless auditor by derv82
 `.  ·  ` /¯\ ´  ·  .´  maintained by kimocoder
   `     /¯¯¯\     ´    https://github.com/kimocoder/wifite2

 [!] Warning: Recommended app pyrit was not found. install @ https://github.com/JPaulMora/Pyrit/wiki
 [!] Warning: Recommended app hcxdumptool was not found. install @ apt install hcxdumptool
 [!] Warning: Recommended app hcxpcapngtool was not found. install @ apt install hcxtools
 [!] Conflicting processes: NetworkManager (PID 404), wpa_supplicant (PID 564)
 [!] If you have problems: kill -9 PID or re-run wifite with --kill

   Interface   PHY   Driver              Chipset
 -----------------------------------------------------------------------
 1. wlan0      phy0  8188eu              TP-Link TL-WN722N v2/v3 [Realtek RTL8188EUS]

 [+] enabling monitor mode on wlan0... enabled wlan0

   NUM                      ESSID   CH  ENCR   POWER  WPS?  CLIENT
   ---  -------------------------  ---  -----  -----  ----  ------
     1                Mikrotik-101    1  WPA-P   63db    no
     2          (00:1A:6C:3C:F3:D0)   9  WEP   54db    no
     3                     eduroam   11  WPA-E   37db    no
     4                   KMME_wifi    2  WPA-P   23db   yes
     5                     eduroam    1  WPA-E   23db    no
     6                     eduroam   11  WPA-E   22db    no
     7                       KTK_0   11  WPA-P   21db    no
     8                     eduroam    6  WPA-E   21db    no
     9                     eduroam   11  WPA-E   20db    no
    10                       artin   11  WPA-P   20db    no
 [+] Scanning. Found 10 target(s), 0 client(s). Ctrl+C when ready
   NUM                      ESSID   CH  ENCR   POWER  WPS?  CLIENT
   ---  -------------------------  ---  -----  -----  ----  ------
```

3. Connect to AP via another PC client



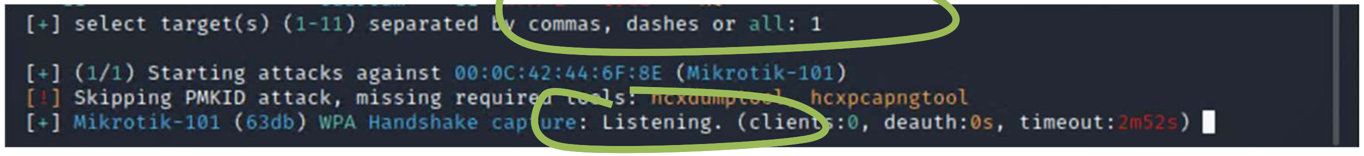
Mikrotik-101
Zabezpečené

□ Pripájať automaticky

Nastavenia siete a internetu

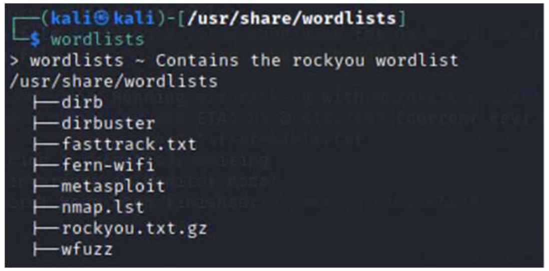
Umožňuje zmeniť nastavenia, napríklad zmeniť pripojenie na pripojenie merané podľa objemu údajov.

2. Listening for a handshake



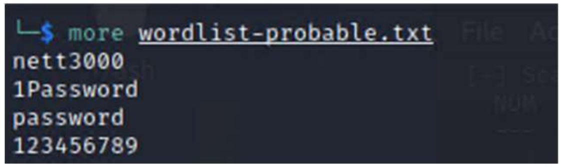
```
[+] select target(s) (1-11) separated by commas, dashes or all: 1

[+] (1/1) Starting attacks against 00:0C:42:44:6F:8E (Mikrotik-101)
[!] Skipping PMKID attack, missing required tools: hcxdumptool, hcxpcapngtool
[+] Mikrotik-101 (63db) WPA Handshake capture: Listening. (clients:0, deauth:0s, timeout:2m52s)
```

Wifite – handshake capture and key searching

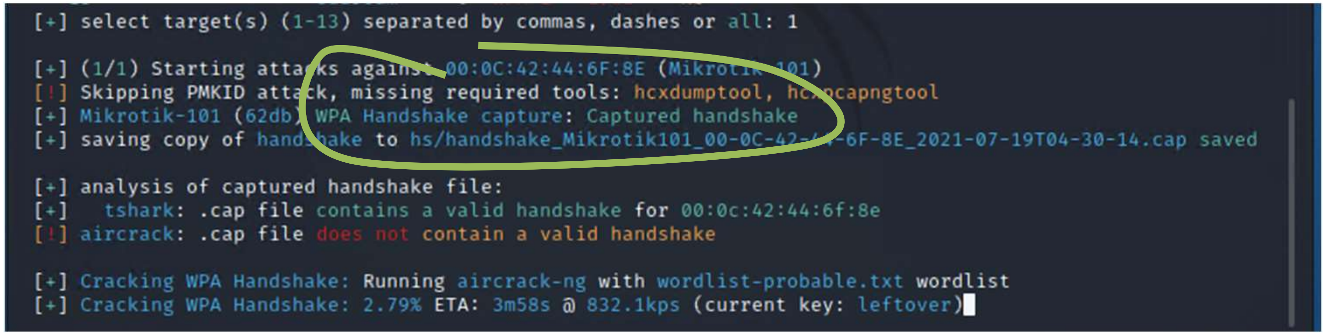


```
┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ wordlists
> wordlists ~ Contains the rockyou wordlist
/usr/share/wordlists
  ├─dirb
  ├─dirbuster
  ├─fasttrack.txt
  ├─fern-wifi
  ├─metasploit
  ├─nmap.lst
  ├─rockyou.txt.gz
  ├─wfuzz
```

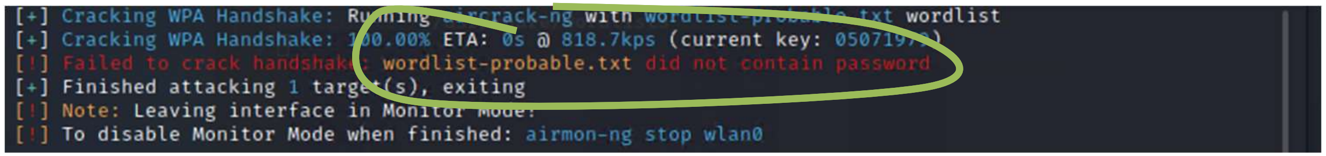
Wifite uses default wordlist file: **/usr/share/dict/wordlist-probable.txt**



```
└─$ more wordlist-probable.txt
nett3000
1Password
password
123456789
```



```
 [+] select target(s) (1-13) separated by commas, dashes or all: 1

 [+] (1/1) Starting attacks against 00:0C:42:44:6F:8E (Mikrotik-101)
 [!] Skipping PMKID attack, missing required tools: hcxdumptool, hcxpcapngtool
 [+] Mikrotik-101 (62db) WPA Handshake capture: Captured handshake
 [+] saving copy of handshake to hs/handshake_Mikrotik101_00-0C-42-44-6F-8E_2021-07-19T04-30-14.cap saved

 [+] analysis of captured handshake file:
 [+]   tshark: .cap file contains a valid handshake for 00:0c:42:44:6f:8e
 [!] aircrack: .cap file does not contain a valid handshake

 [+] Cracking WPA Handshake: Running aircrack-ng with wordlist-probable.txt wordlist
 [+] Cracking WPA Handshake: 2.79% ETA: 3m58s @ 832.1kps (current key: leftover)
```



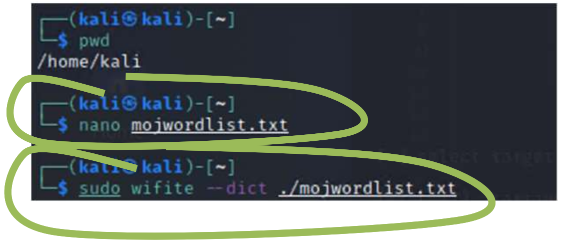
```
[+] Cracking WPA Handshake: Running aircrack-ng with wordlist-probable.txt wordlist
[+] Cracking WPA Handshake: 100.00% ETA: 0s @ 818.7kps (current key: 05071979)
[!] Failed to crack handshake: wordlist-probable.txt did not contain password
[+] Finished attacking 1 target(s), exiting
[!] Note: Leaving interface in Monitor Mode!
[!] To disable Monitor Mode when finished: airmon-ng stop wlan0
```

Úloha

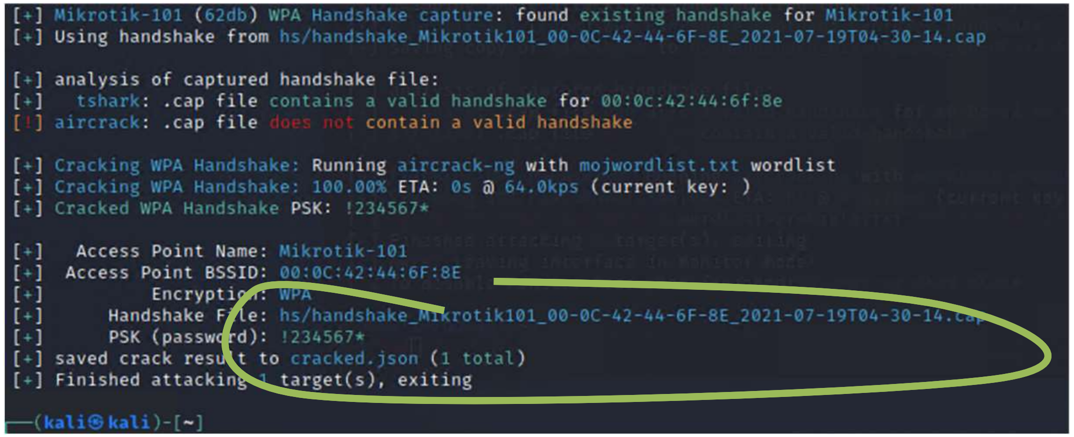
- Vytvorte vlastný súbor s WPA kľúčom
- Spustiť Wifite s vlastným súborom kľúčov
- Zdokumentovať handskake CAP súbor v ./hs adresári ; Key messages 1,2,3,4.

  (Použiť program Wireshark)
- Zmazať vytvorené súbory

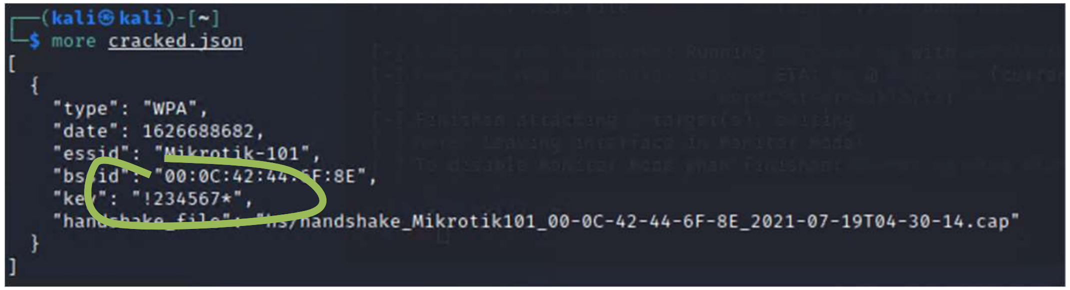
  (./cracked.json a adresár ./hs s CAP súborom)



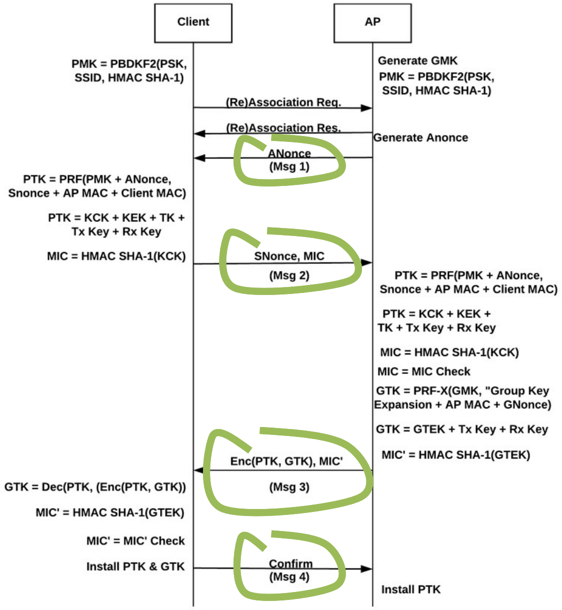
```
┌──(kali㉿kali)-[~]
└─$ pwd
/home/kali

┌──(kali㉿kali)-[~]
└─$ nano mojwordlist.txt

┌──(kali㉿kali)-[~]
└─$ sudo wifite --dict ./mojwordlist.txt
```



```
[+] Mikrotik-101 (62db) WPA Handshake capture: found existing handshake for Mikrotik-101
[+] Using handshake from hs/handshake_Mikrotik101_00-0C-42-44-6F-8E_2021-07-19T04-30-14.cap

[+] analysis of captured handshake file:
[+]   tshark: .cap file contains a valid handshake for 00:0c:42:44:6f:8e
[!] aircrack: .cap file does not contain a valid handshake

[+] Cracking WPA Handshake: Running aircrack-ng with mojwordlist.txt wordlist
[+] Cracking WPA Handshake: 100.00% ETA: 0s @ 64.0kps (current key: )
[+] Cracked WPA Handshake PSK: !234567*

[+]   Access Point Name: Mikrotik-101
[+]  Access Point BSSID: 00:0C:42:44:6F:8E
[+]          Encryption: WPA
[+]      Handshake File: hs/handshake_Mikrotik101_00-0C-42-44-6F-8E_2021-07-19T04-30-14.cap
[+]      PSK (password): !234567*
[+] saved crack result to cracked.json (1 total)
[+] Finished attacking 1 target(s), exiting

──(kali㉿kali)-[~]
```



```
┌──(kali㉿kali)-[~]
└─$ more cracked.json
[
  {
    "type": "WPA",
    "date": 1626688682,
    "essid": "Mikrotik-101",
    "bssid": "00:0C:42:44:6F:8E",
    "key": "!234567*",
    "handshake_file": "hs/handshake_Mikrotik101_00-0C-42-44-6F-8E_2021-07-19T04-30-14.cap"
  }
]
```


Client
AP
PMK = PBDKF2(PSK, SSID, HMAC SHA-1)
Generate GMK
PMK = PBDKF2(PSK, SSID, HMAC SHA-1)
(Re)Association Req.
(Re)Association Res.
Generate Anonce
ANonce (Msg 1)
PTK = PRF(PMK + ANonce, Snonce + AP MAC + Client MAC)
PTK = KCK + KEK + TK + Tx Key + Rx Key
MIC = HMAC SHA-1(KCK)
SNonce, MIC (Msg 2)
PTK = PRF(PMK + ANonce, Snonce + AP MAC + Client MAC)
PTK = KCK + KEK + TK + Tx Key + Rx Key
MIC = HMAC SHA-1(KCK)
MIC = MIC Check
GTK = PRF-X(GMK, "Group Key Expansion + AP MAC + GNonce)
GTK = GTEK + Tx Key + Rx Key
MIC' = HMAC SHA-1(GTEK)
Enc(PTK, GTK), MIC' (Msg 3)
GTK = Dec(PTK, (Enc(PTK, GTK))
MIC' = HMAC SHA-1(GTEK)
MIC' = MIC' Check
Install PTK & GTK
Confirm (Msg 4)
Install PTK

NOTE: For each PSK guess, the attacker computes the PMK and the PTK. It uses his PTK to compute a MIC for packet 2, 3 or 4 of the handshake. If the computed MIC is equal to the MIC of the original packets, the PSK guess is correct.

Ďakujem za pozornosť.

roman dot kaloc at uniza dot sk

- Vytvorené v rámci projektu KEGA 026TUKE-4/2021