Lab#5

Wired Equivalent Privacy Hack

NACT-261 Network Security

2025-2026 Spring Semester

Submitted by Jibreal Id-deen

Due by April 6

Professor Mark Jeremy

TABLE OF CONTENTS

TABLE OF FIGURES

OBJECTIVE

My objective is to demonstrate the vulnerability of WEP encryption by using Wifite on Kali Linux to crack the WEP key of a target network. This involves configuring the Alfa USB adapter, capturing IVs through fake authentication and documenting the process with a network diagram.

PROCEDURE

- Walked to the ICS Equipment room
- Got the Aruba AP-315 model, two Dell laptop, Switch, Alfa USB adapter, wireless router and Kali Live USB.
- Set the Switch and AP-315 up and configure AP-315 with SSID NetSec-lastnameJ, WEP security and 2.4GHz only.
- Connect the victim laptop to the SSID and start downloading a large file.
- Boot Kali Linux on the Black Dell laptop from the Live USB
- Plug in the Alfa USB adapter and disable built-in Wi-Fi
- Run the Alfa Adapter inro monitor mode in Kali Linux
- Launch Wifite to select NetSec-lastnameF and crack the WEP key!
- Clean the stuffs
- Return the stuff to the ICS Equipment room

NETWORK DIAGRAM

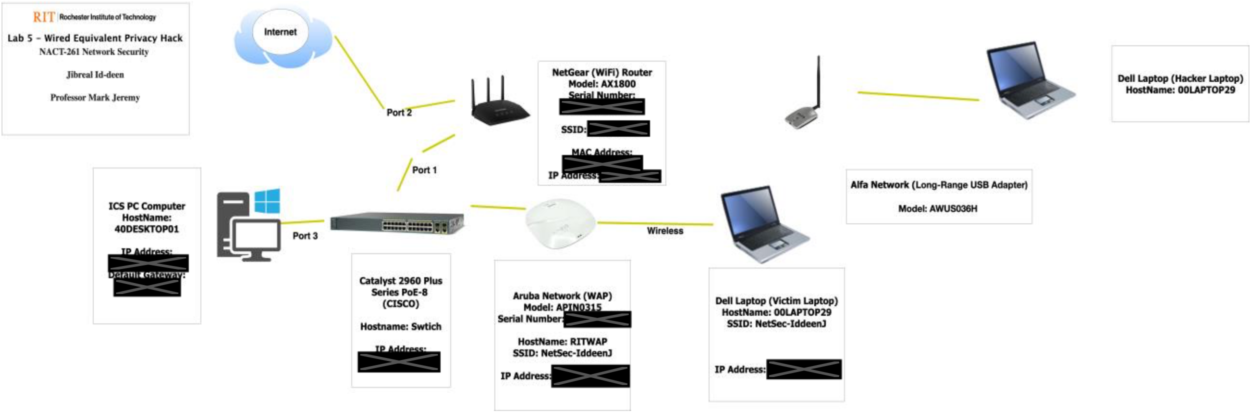


FIGURE 1 - NETWORK DIAGRAM

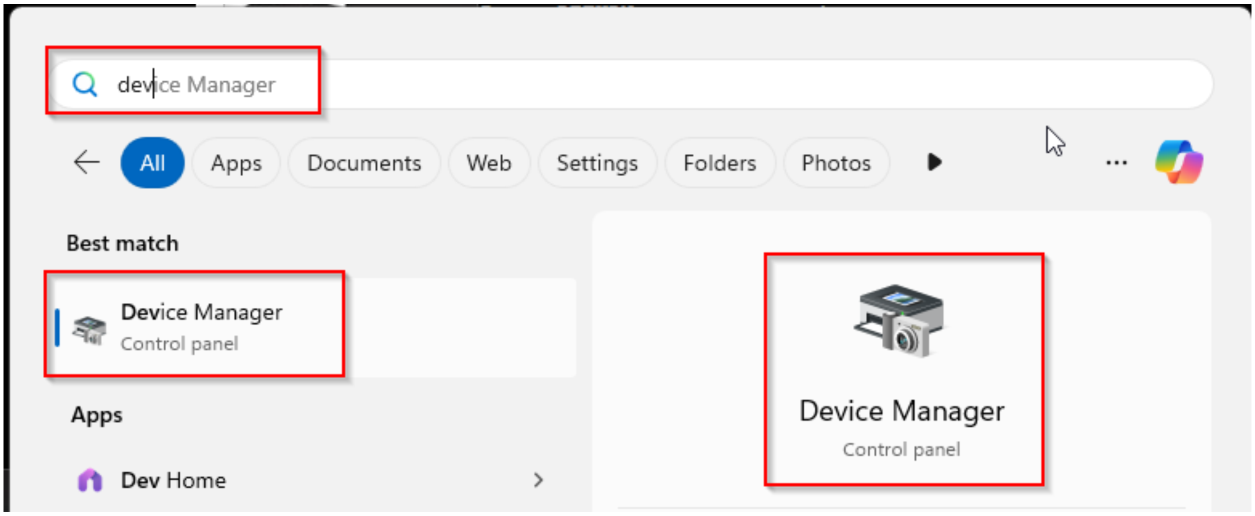


FIGURE 2 - OPEN THE DEVICE MANAGER

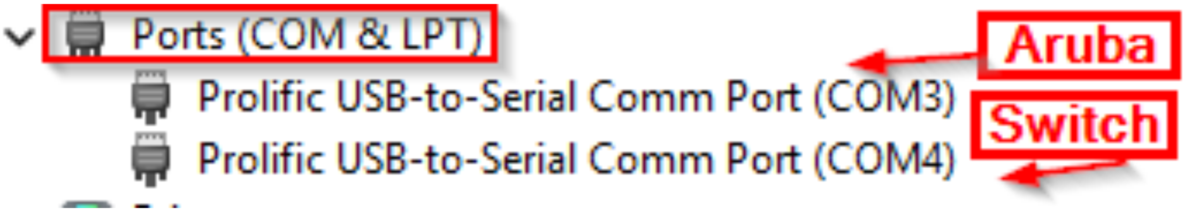
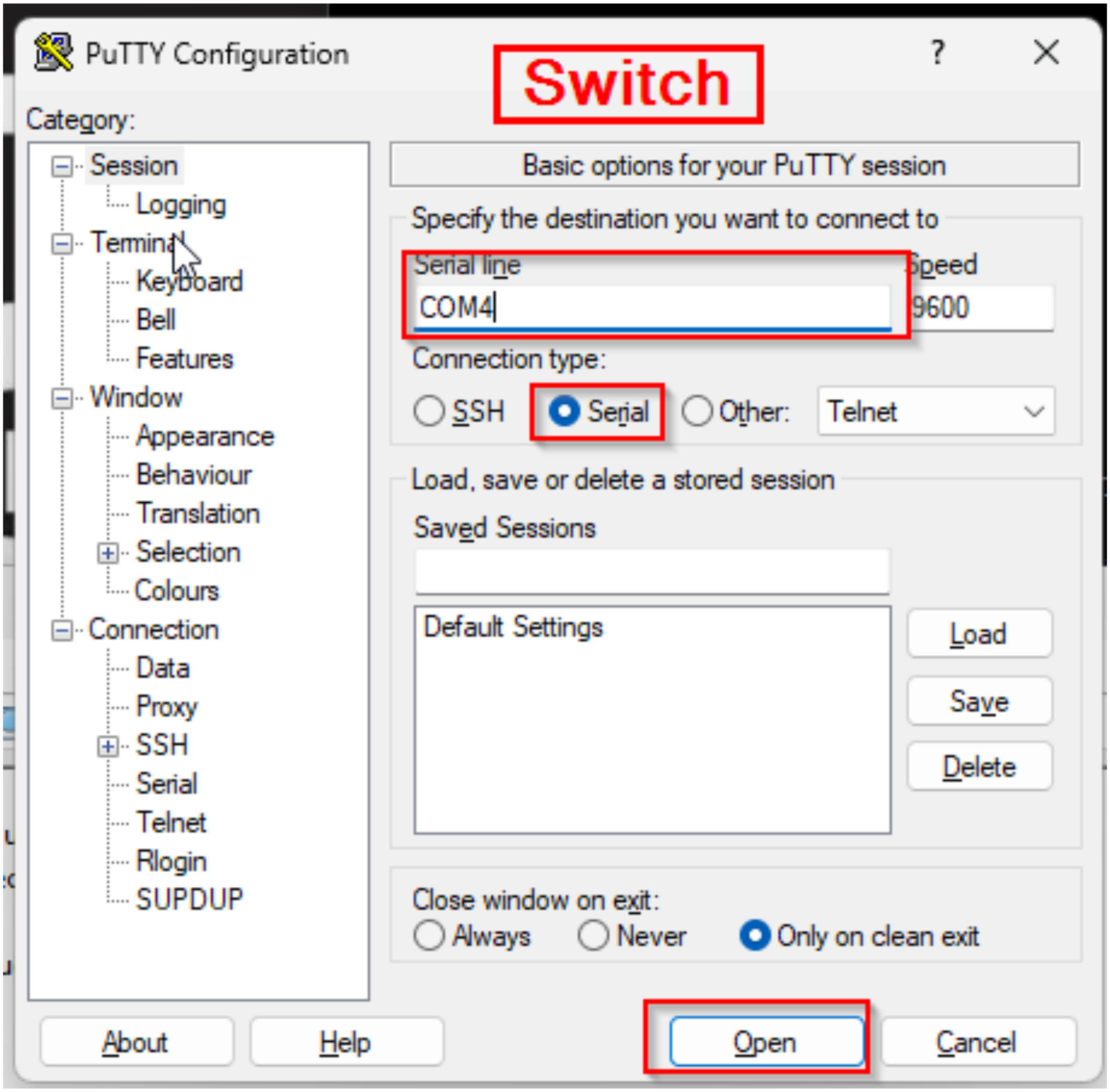

Ports (COM & LPT)
Prolific USB-to-Serial Comm Port (COM3)
Prolific USB-to-Serial Comm Port (COM4)
Aruba
Switch

FIGURE 3 – CHECK THE USB TO SERIAL COMM PORT TO OPEN PUTTY



Specify the destination you want to connect to

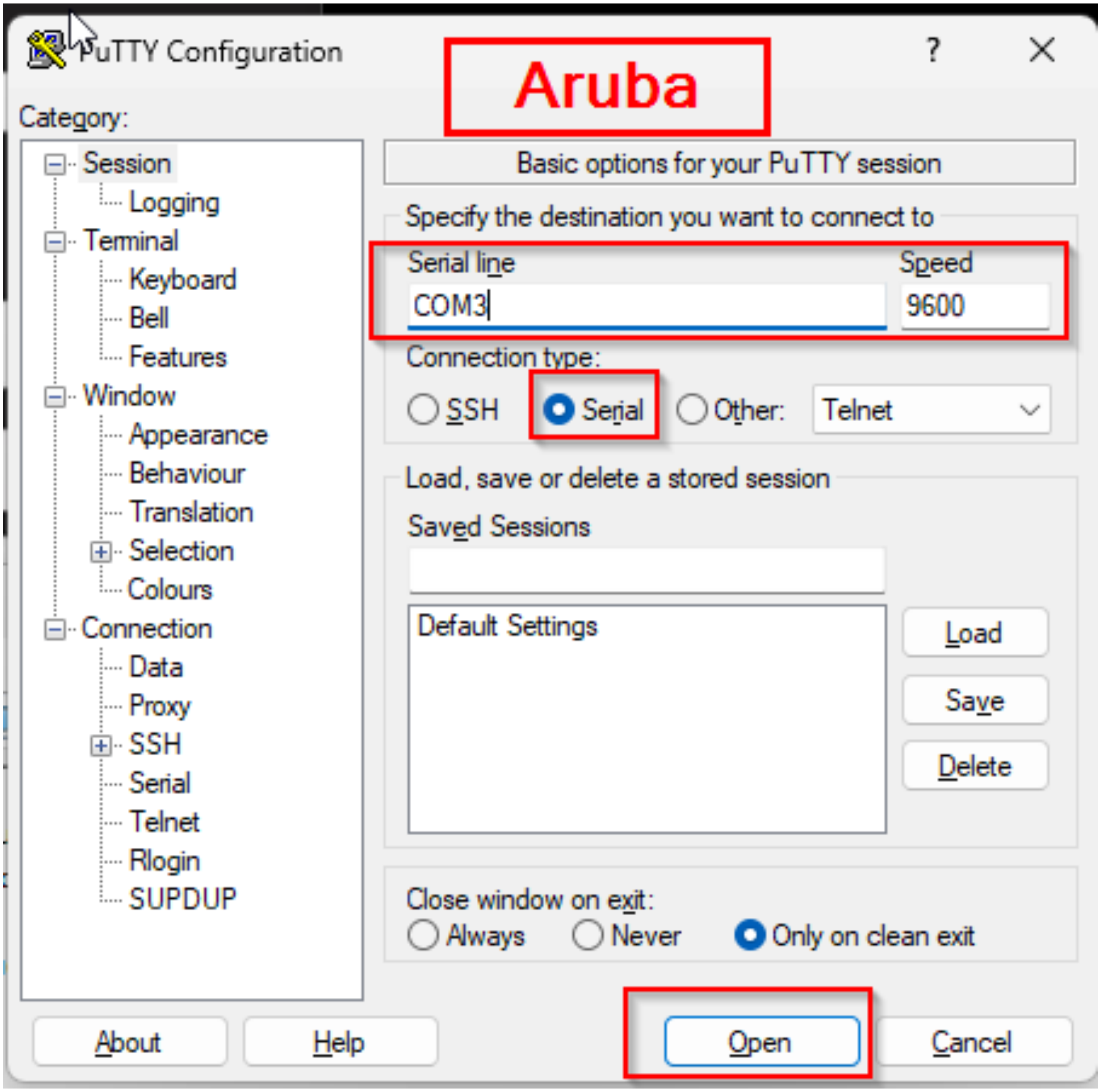
Serial line: COM4

Speed: 9600

Connection type: ○ SSH ● Serial ○ Other: Telnet

Close window on exit: ○ Always ○ Never ● Only on clean exit

Figure 4 – Type the COM4 with SERIAL to open switch CLI



Specify the destination you want to connect to

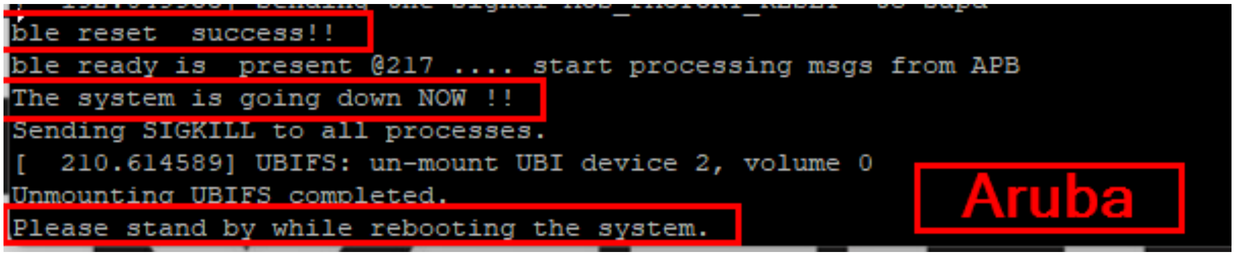
Serial line: COM3

Speed: 9600

Connection type: ○ SSH ● Serial ○ Other: Telnet

Close window on exit: ○ Always ○ Never ● Only on clean exit

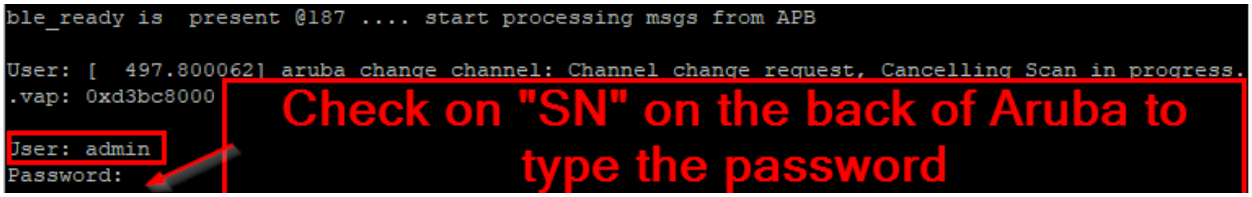
Figure 5 – Type the COM3 with SERIAL to open Aruba CLI



```
ble reset  success!!
ble ready is  present @217 .... start processing msgs from APB
The system is going down NOW !!
Sending SIGKILL to all processes.
[  210.614589] UBIFS: un-mount UBI device 2, volume 0
Unmounting UBIFS completed.
Please stand by while rebooting the system.
```

Aruba

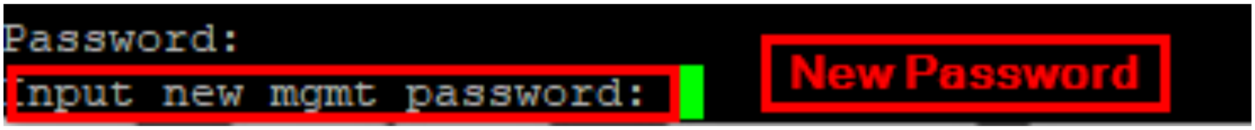
FIGURE 6 – FACTORY RESET SUCCESSFULLY!



```
ble_ready is  present @187 .... start processing msgs from APB

User: [  497.800062] aruba change channel: Channel change request, Cancelling Scan in progress.
.vap: 0xd3bc8000

User: admin
Password:
```

Check on "SN" on the back of Aruba to type the password

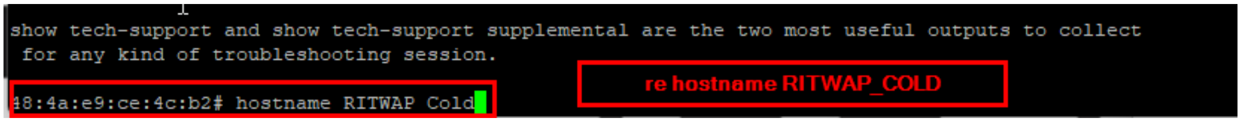
FIGURE 7 – LOGGING THE ARUBA ADMIN ACCOUNT ON



```
Password:
Input new mgmt password:
```

New Password

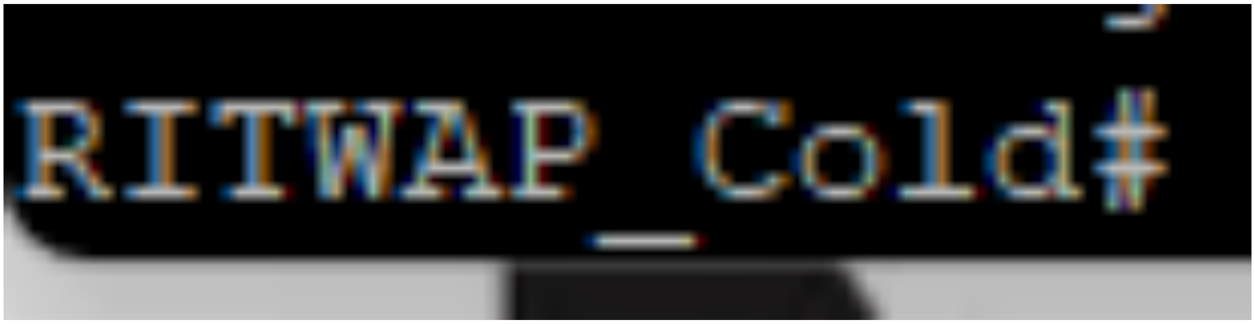
FIGURE 8 – TYPING THE NEW PASSWORD



```
show tech-support and show tech-support supplemental are the two most useful outputs to collect
 for any kind of troubleshooting session.

48:4a:e9:ce:4c:b2# hostname RITWAP_Cold
```

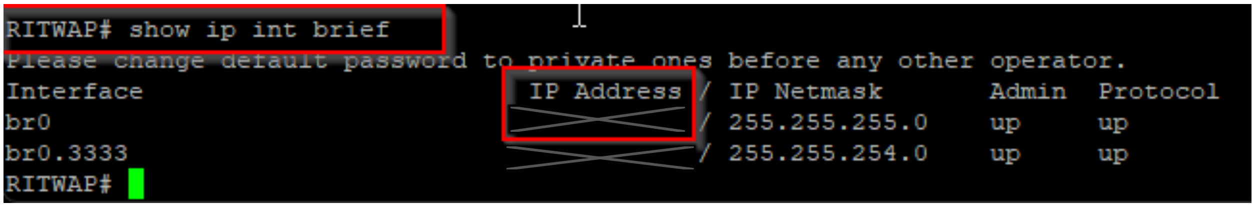
re hostname RITWAP_COLD

FIGURE 9 – CHANGING THE HOSTNAME IN ARUBA



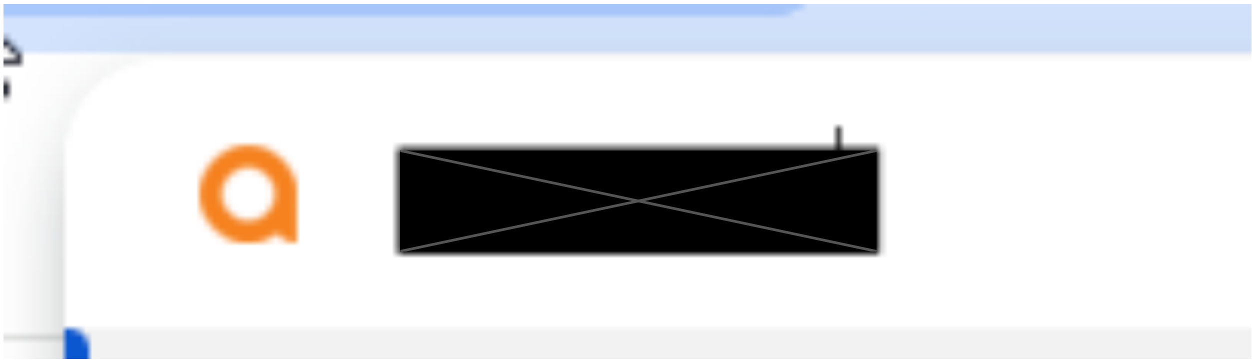
```
RITWAP_Cold#
```

FIGURE 10 – THE HOSTNAME CHANGED SUCCESSFULLY!



```
RITWAP# show ip int brief
Please change default password to private ones before any other operator.
Interface                         IP Address / IP Netmask       Admin    Protocol
br0                               [redacted] / 255.255.255.0    up       up
br0.3333                          [redacted] / 255.255.254.0    up       up
RITWAP#
```

FIGURE 11 -TYPE THE COMMAND TO LOOK UP ON IP ADDRESS



[redacted]

FIGURE 12 - COPY THE IP ADDRESS TO PASTE ON GOOGLE URL

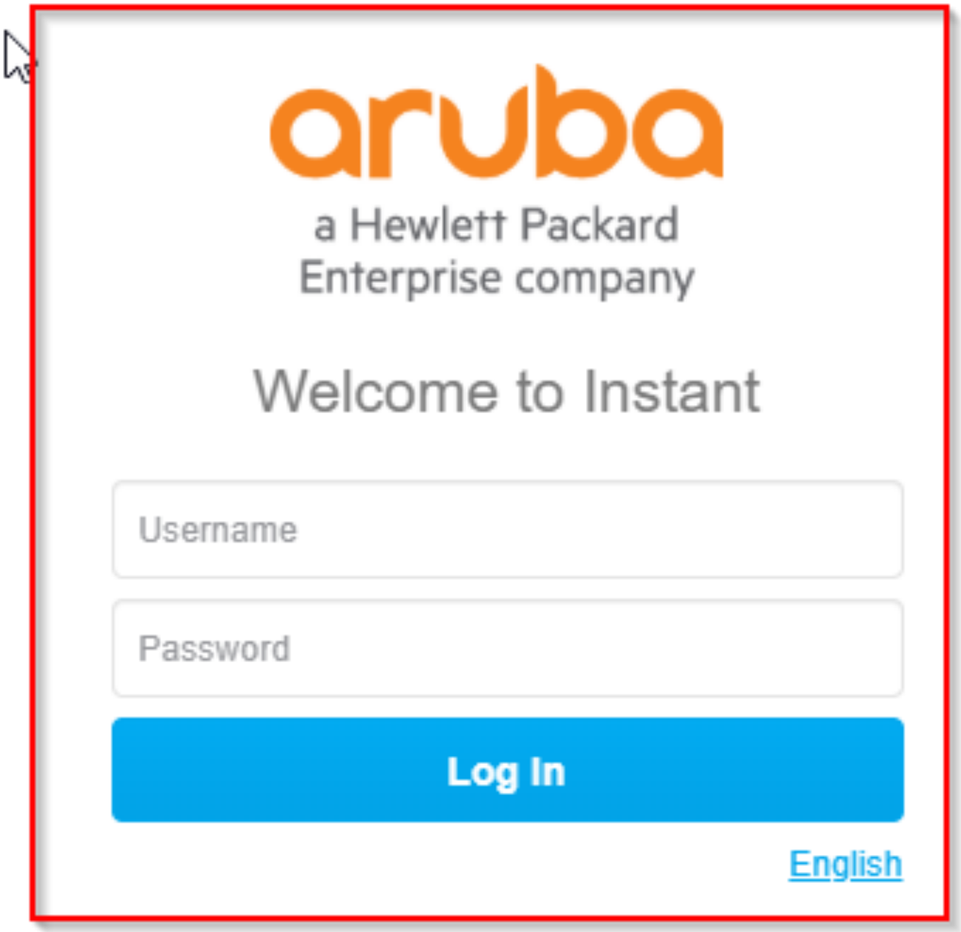


Figure 13 - Log the Admin Account on

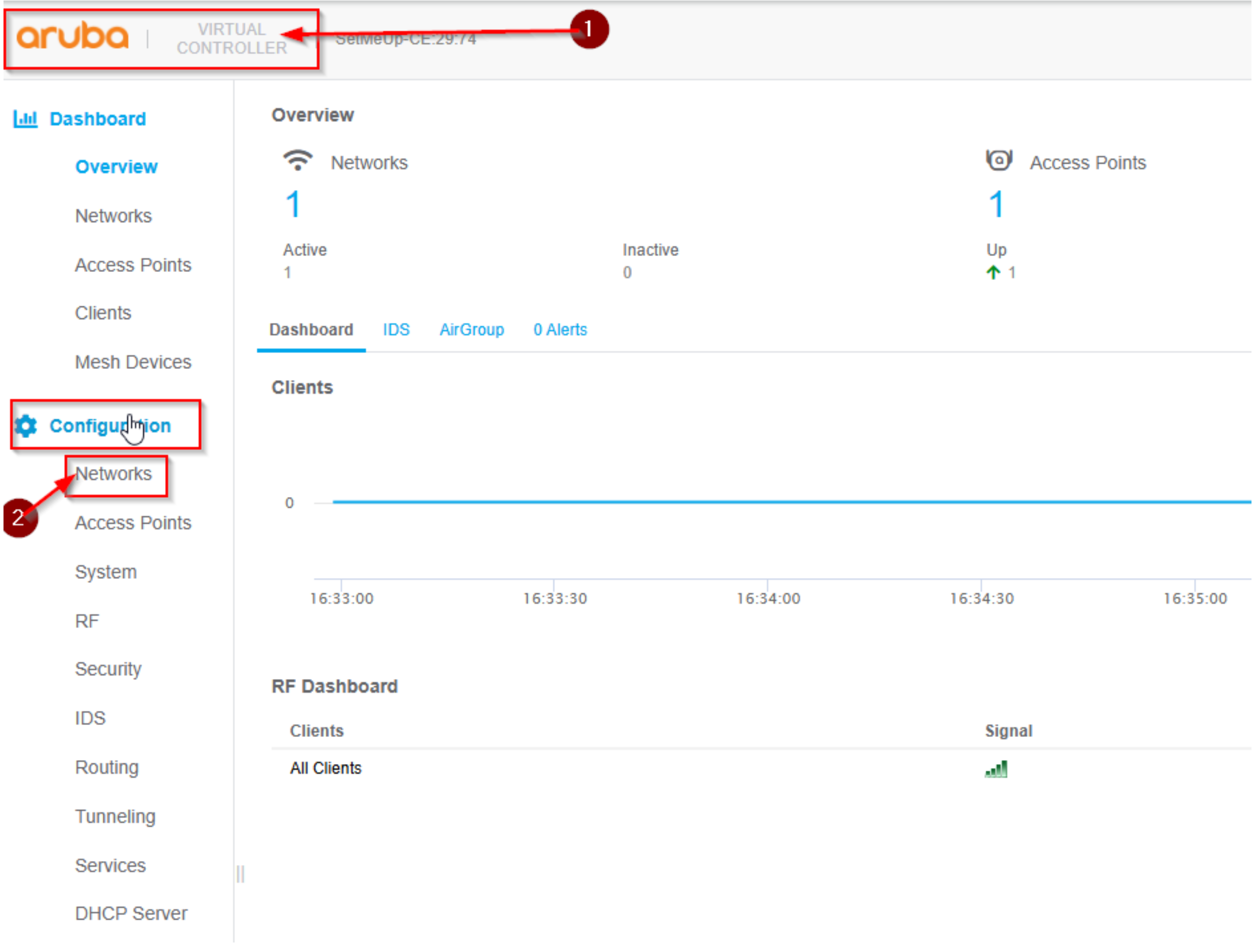
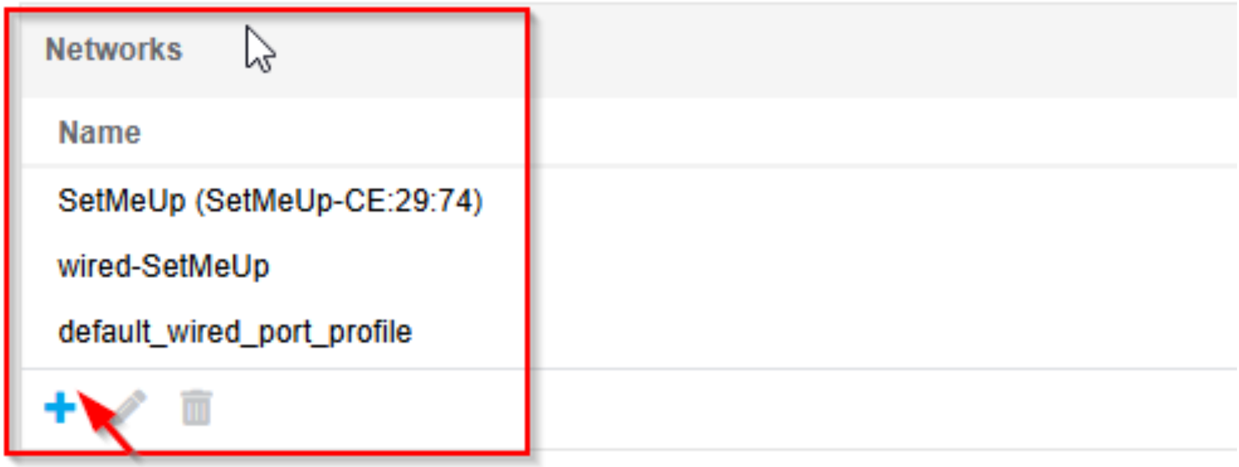


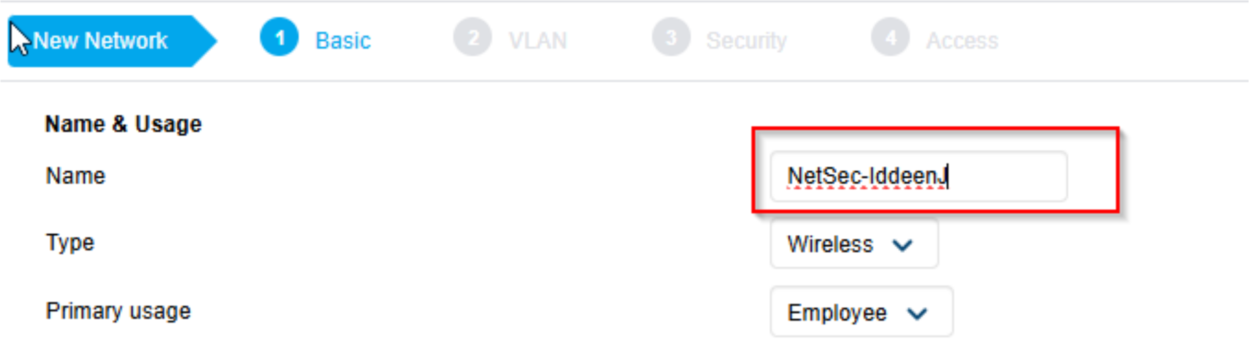
Figure 14 - Seeing the Dashboard and click Networks on Configuration



Networks

Name
SetMeUp (SetMeUp-CE:29:74)
wired-SetMeUp
default_wired_port_profile

Figure 15 - Click ADD to make new SSID (Network)



Name & Usage

Name: NetSec-IddeenJ

Type: Wireless

Primary usage: Employee

Figure 16 - Type the new SSID name

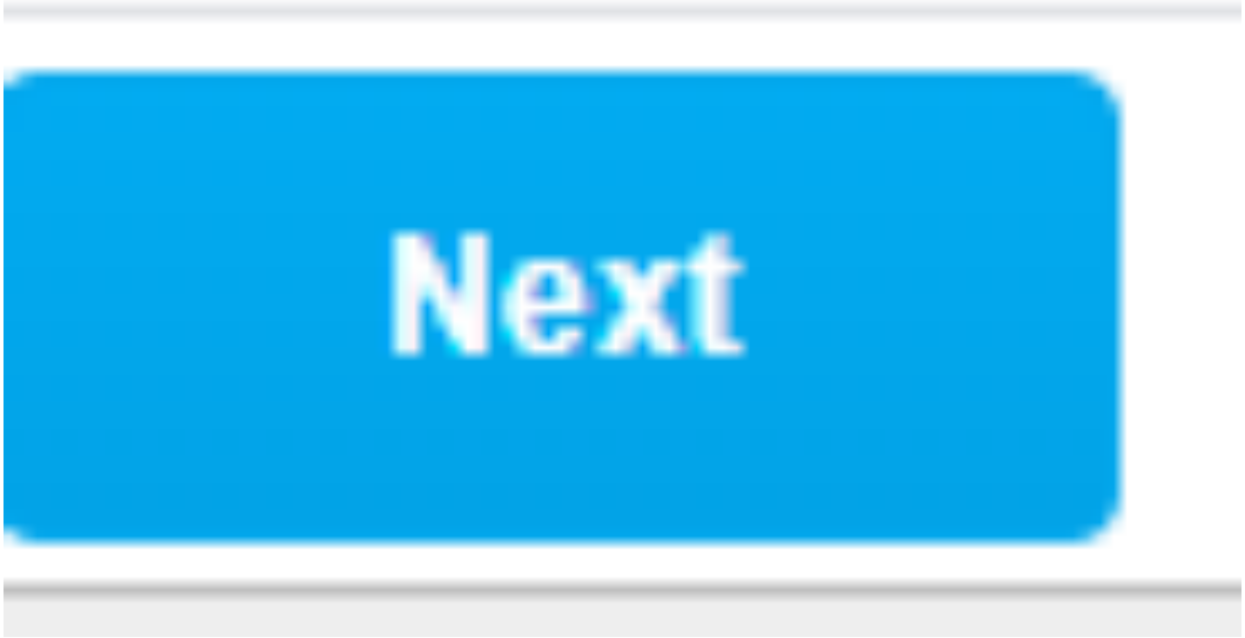
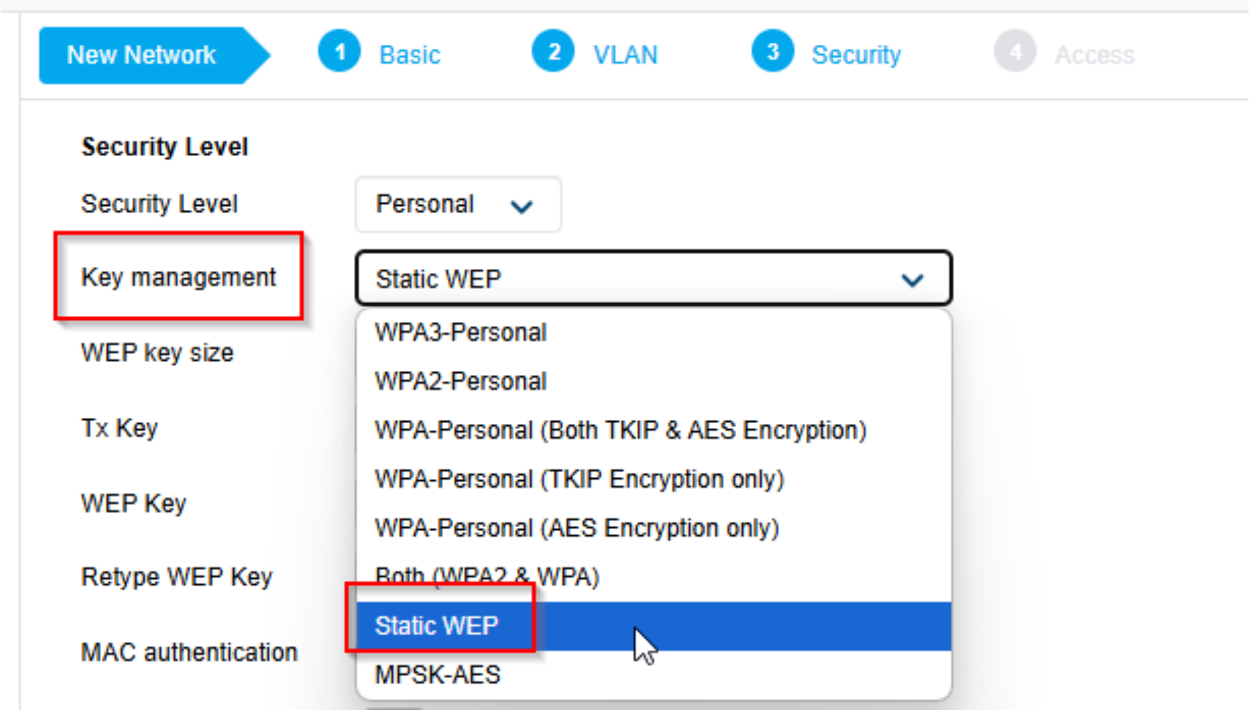


Figure 17 - Click NEXT


New Network
1 Basic
2 VLAN
3 Security
4 Access
WPA3-Personal
WPA2-Personal
WPA-Personal (Both TKIP & AES Encryption)
WPA-Personal (TKIP Encryption only)
WPA-Personal (AES Encryption only)
Both (WPA2 & WPA)
Static WEP
MPSK-AES

Security Level

Security Level: Personal

Key management: Static WEP

WEP key size

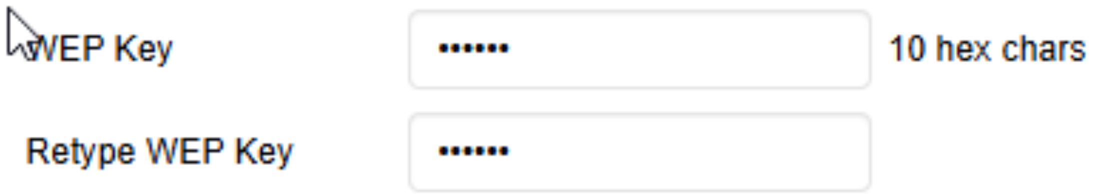
Tx Key

WEP Key

Retype WEP Key

MAC authentication

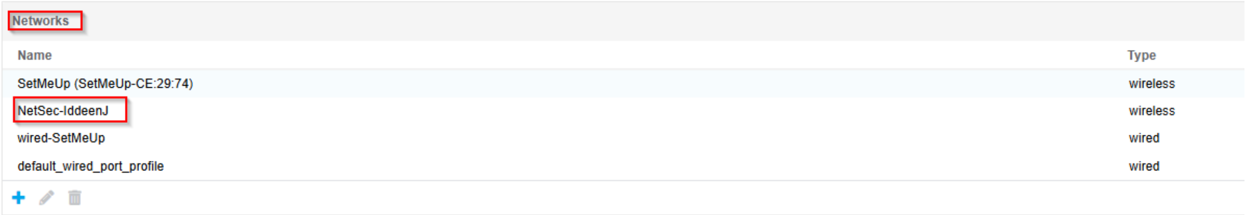
FIGURE 18 - CLICK WEP



WEP Key: •••••• 10 hex chars

Retype WEP Key: ••••••

FIGURE 19 - TYPE THE HEX CHARS (PASSWORDS)



Networks

Name	Type
SetMeUp (SetMeUp-CE:29:74)	wireless
NetSec-IddeenJ	wireless
wired-SetMeUp	wired
default_wired_port_profile	wired

FIGURE 20 - HERE WE GO! THE NEW SSID NETWORK IS HERE.

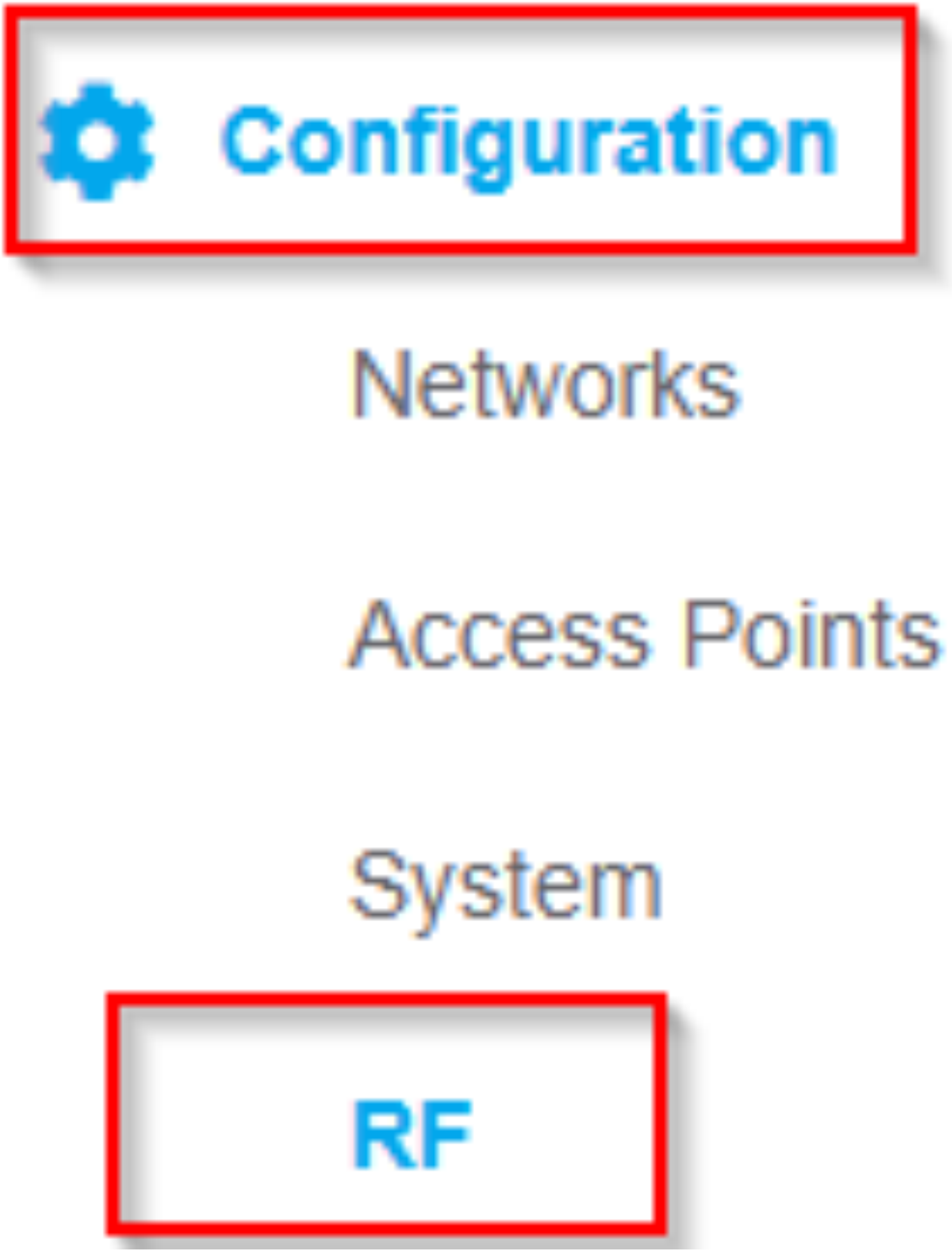
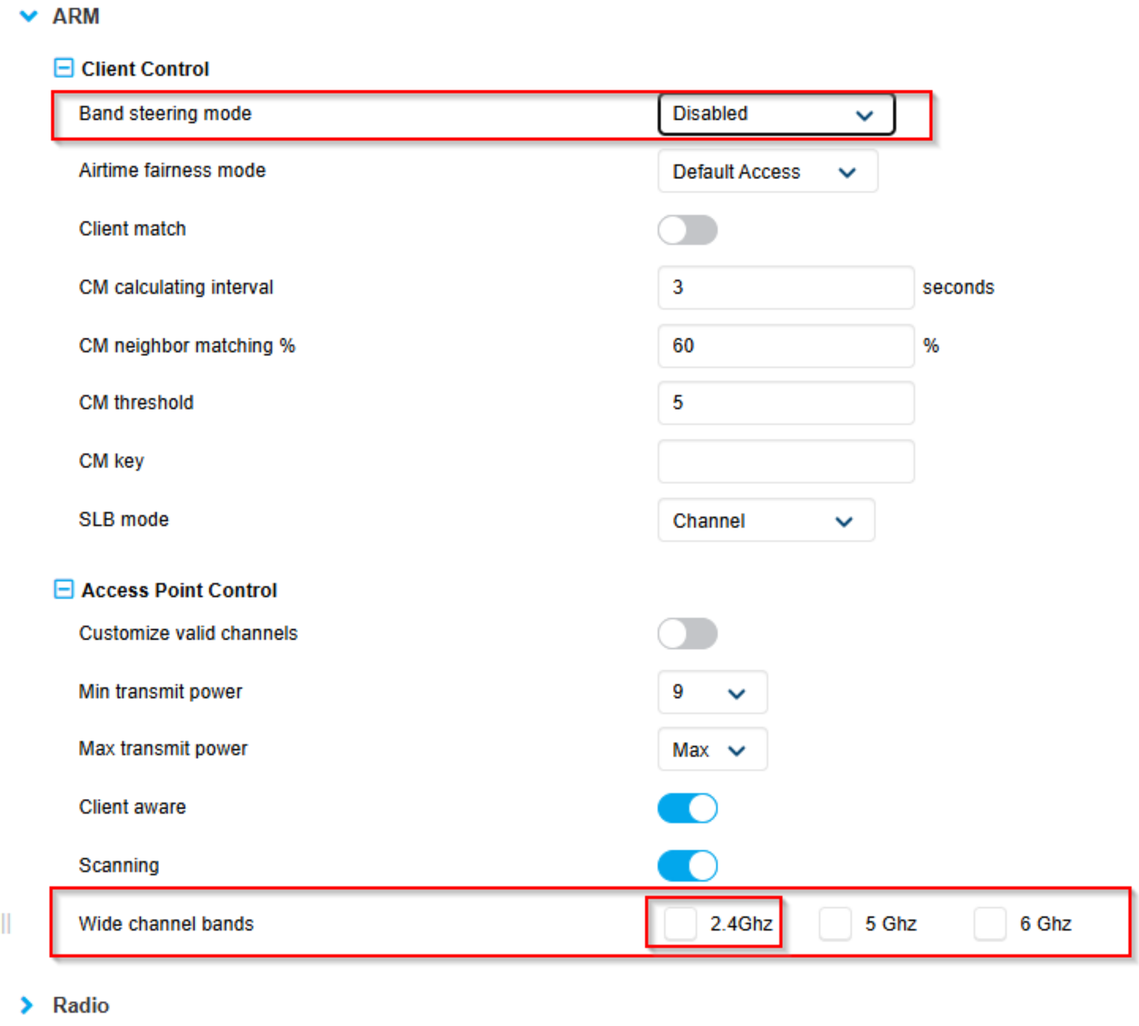


Figure 21 - Back to Configuration, then click RF



ARM

Client Control

Band steering mode: Disabled

Airtime fairness mode: Default Access

Client match

CM calculating interval: 3 seconds

CM neighbor matching %: 60 %

CM threshold: 5

CM key

SLB mode: Channel

Access Point Control

Customize valid channels

Min transmit power: 9

Max transmit power: Max

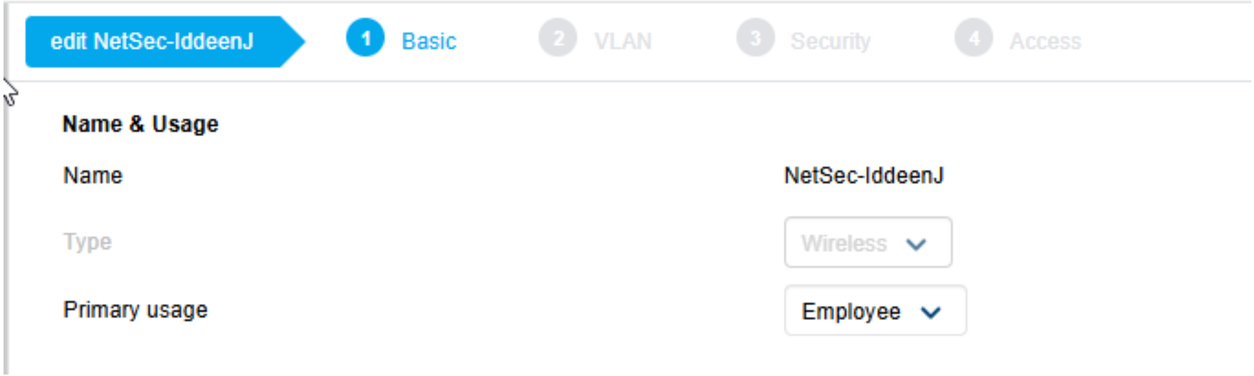
Client aware

Scanning

Wide channel bands: □ 2.4Ghz □ 5 Ghz □ 6 Ghz

Radio

FIGURE 22 - MAKE SURE TO FORCE THE BAND BECOME 2.4GHZ



Name & Usage

Name: NetSec-IddeenJ

Type: Wireless

Primary usage: Employee

FIGURE 23 - BACK TO NETWORK FROM CONFIGURATION, THEN SCROLL DOWN

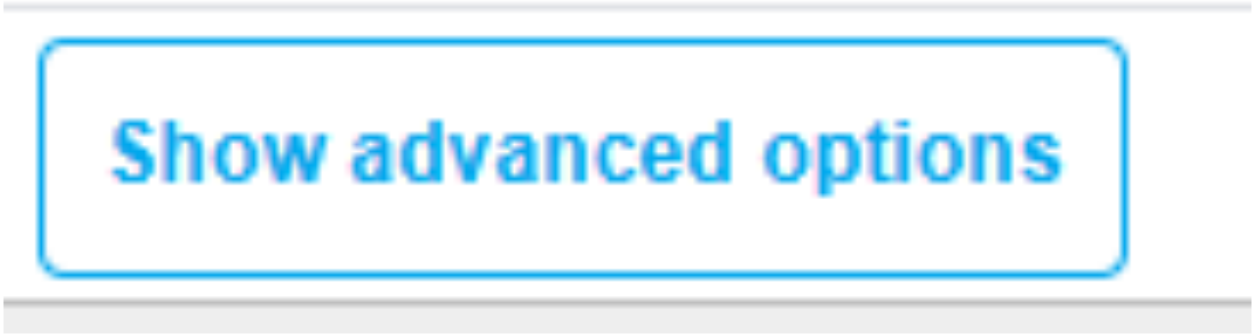
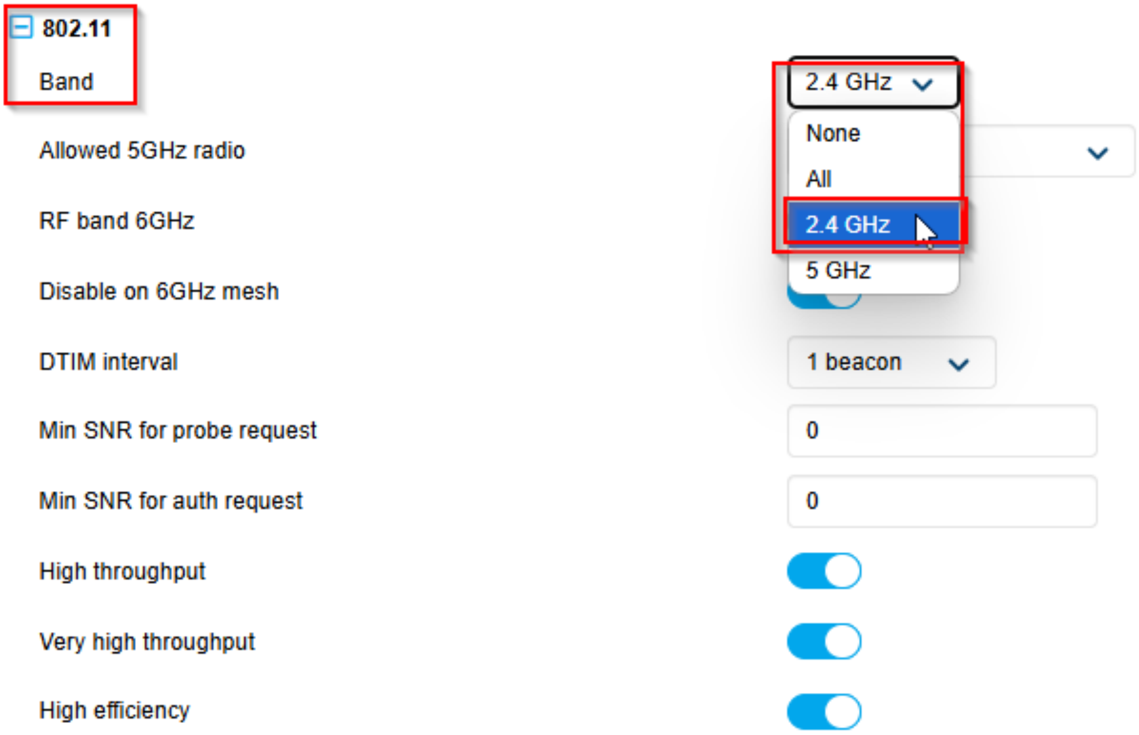


FIGURE 24 - CLICK SHOW ADVANCED OPTIONS



802.11

Band: 2.4 GHz

Allowed 5GHz radio

RF band 6GHz

Disable on 6GHz mesh

DTIM interval: 1 beacon

Min SNR for probe request: 0

Min SNR for auth request: 0

High throughput

Very high throughput

High efficiency

FIGURE 25 - CLICK THE BAND TO SELECT 2.4GHZ

FIGURE 26 - CLICK FINISH

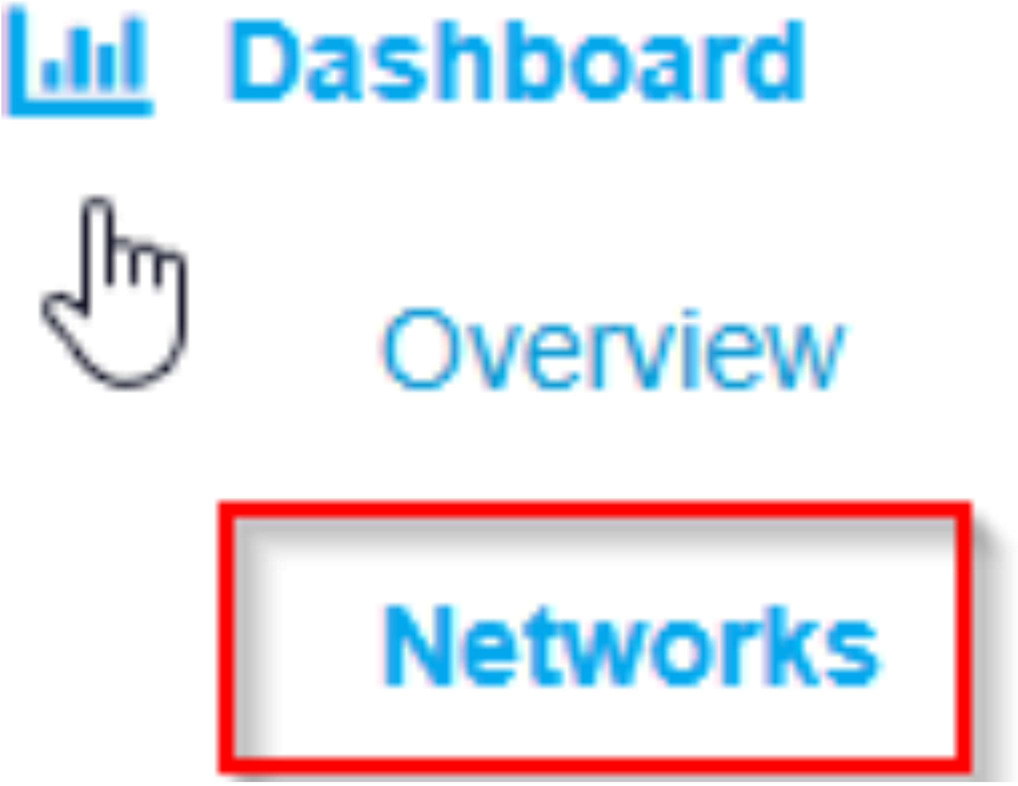
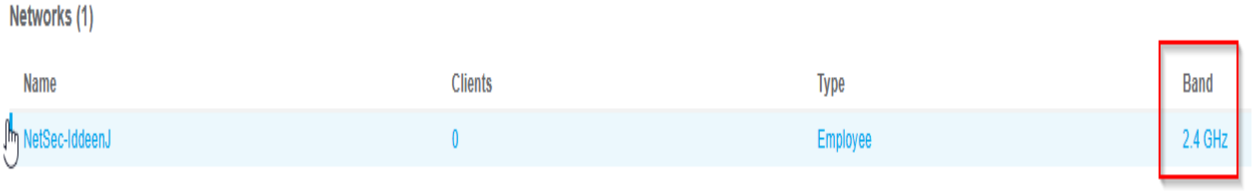


Figure 27 - After clicking FINISH, go back to Network



Networks (1)

Name	Clients	Type	Band
NetSec-IddeenJ	0	Employee	2.4 GHz

Figure 28 - Here we go! The band on the SSID network is 2.4GHz now!

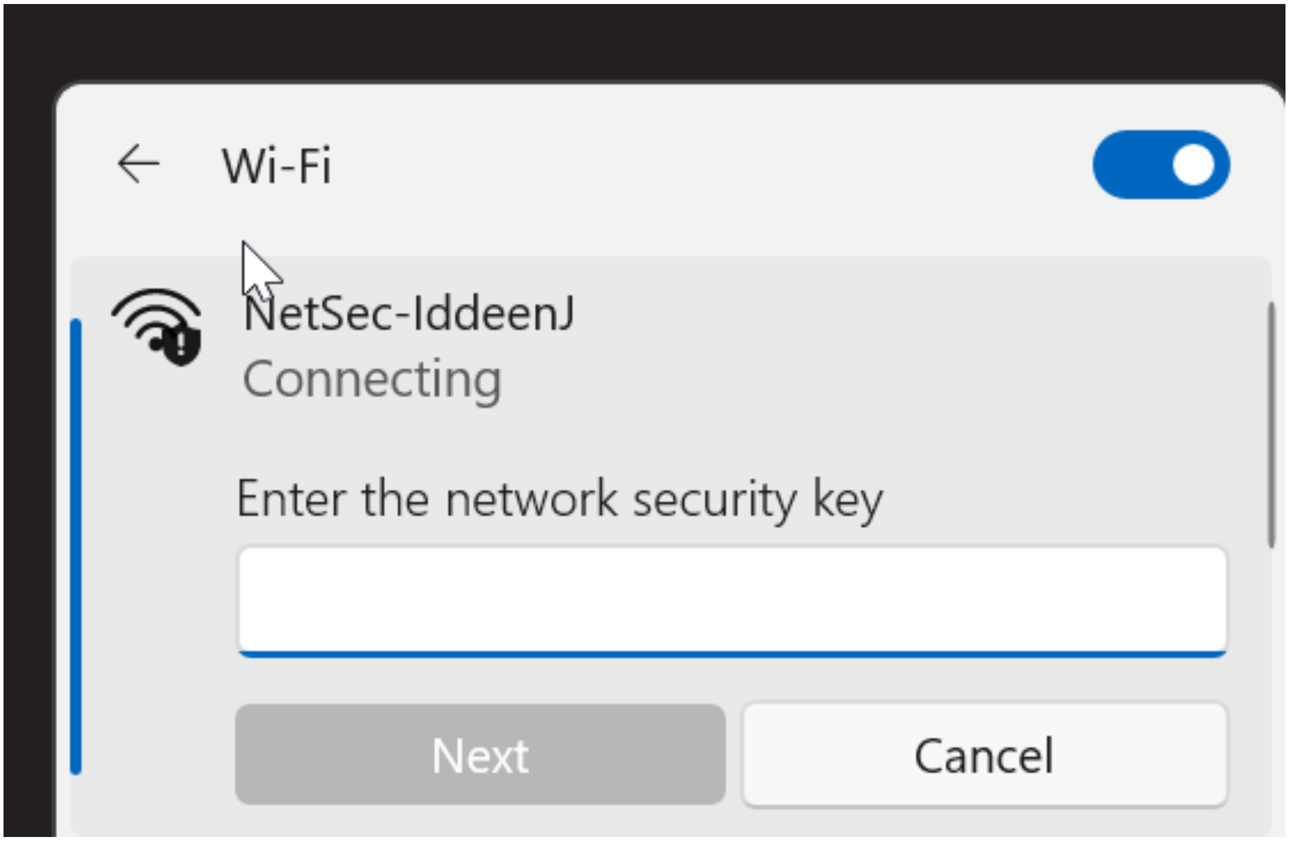


Figure 29 - Use the Dell laptop to get internet

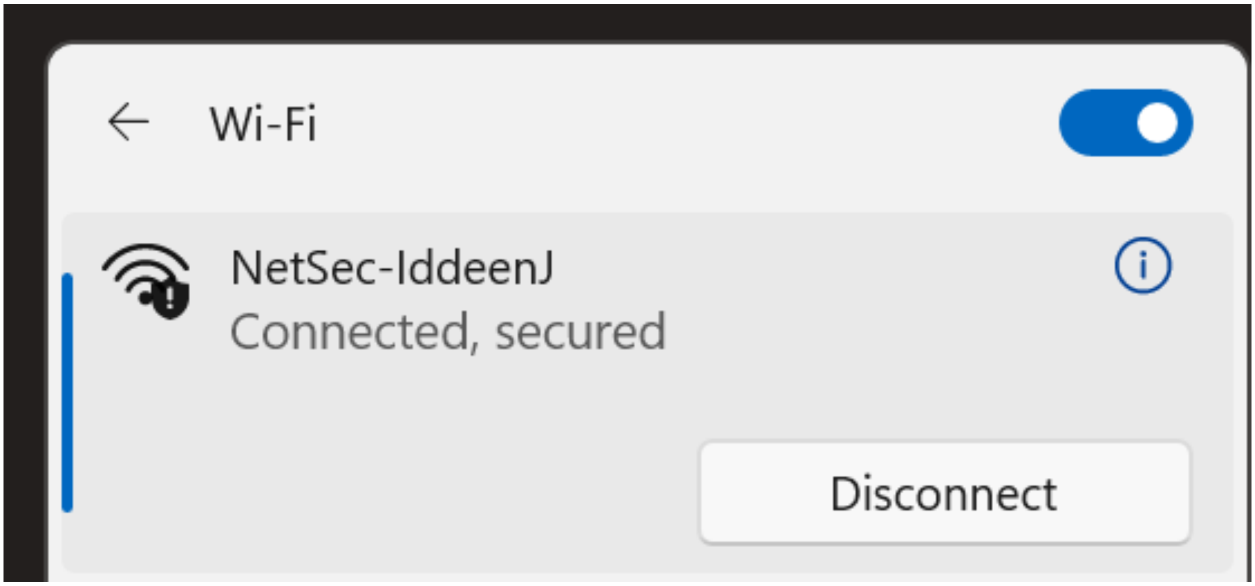
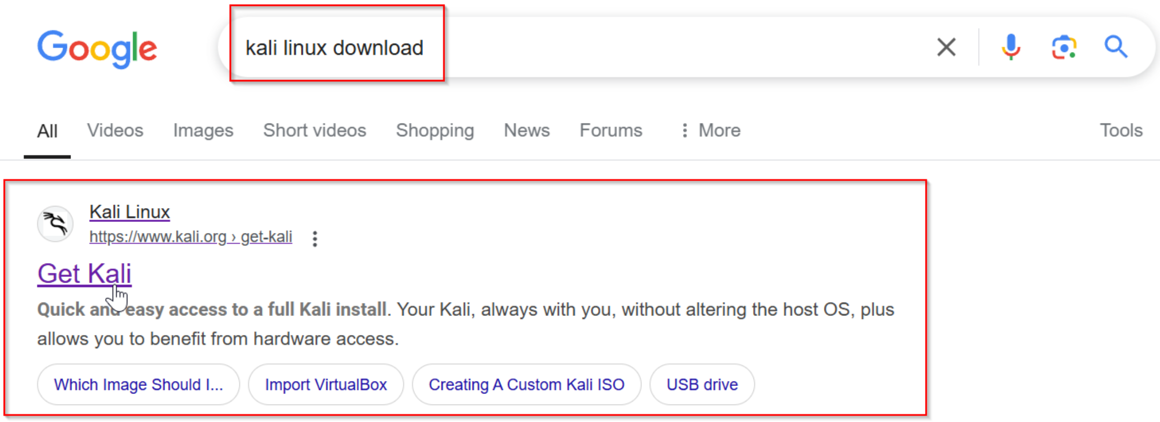


Figure 30 - Ok! WIFI connected successfully!

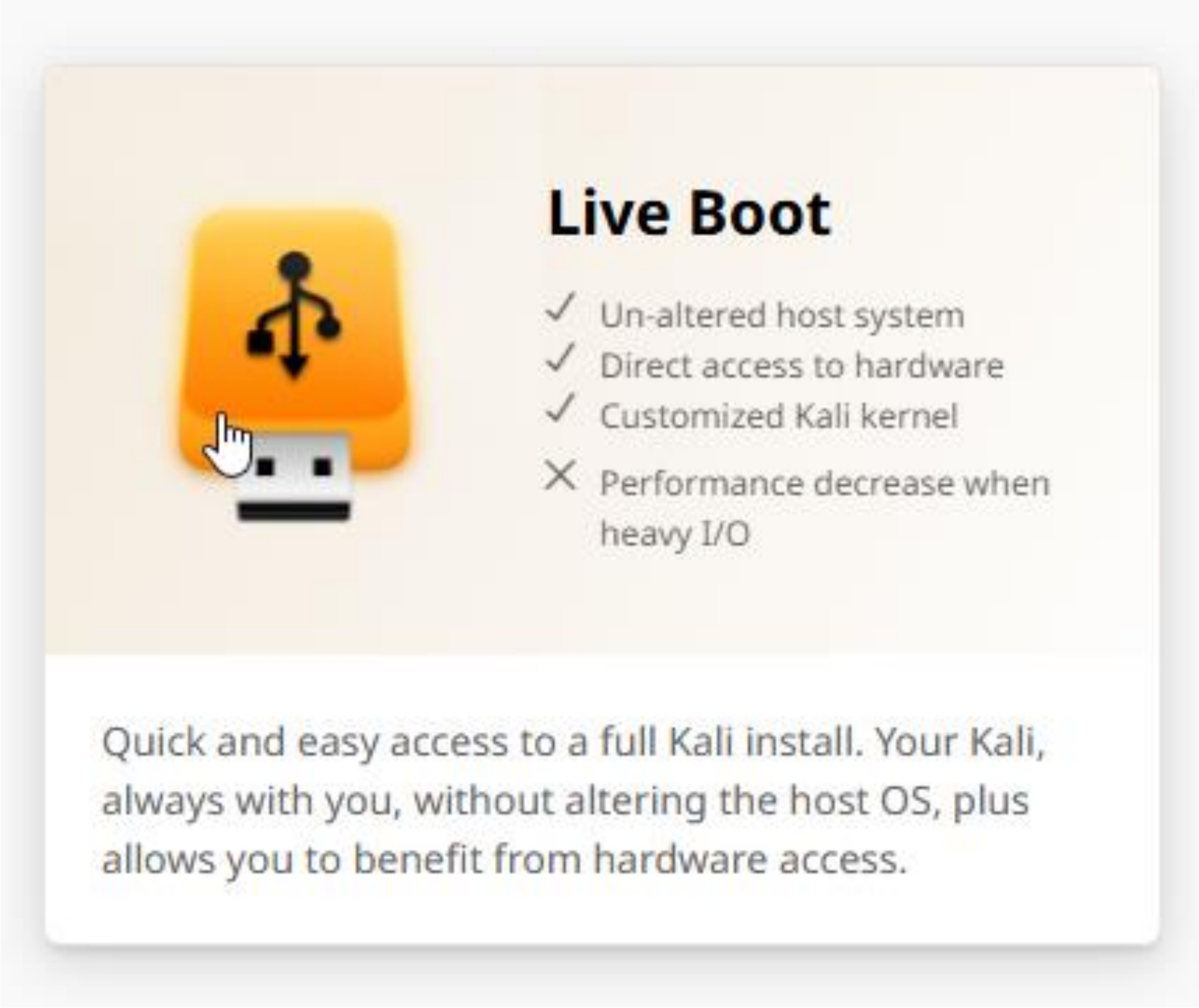


Kali Linux
https://www.kali.org › get-kali

Get Kali

Quick and easy access to a full Kali install. Your Kali, always with you, without altering the host OS, plus allows you to benefit from hardware access.

FIGURE 31 = TYPE 'KALI LINUX' ON GOOGLE URL AND CLICK 'GET KALI" ON THE LINK



Live Boot

✓ Un-altered host system

✓ Direct access to hardware

✓ Customized Kali kernel

✕ Performance decrease when heavy I/O

Quick and easy access to a full Kali install. Your Kali, always with you, without altering the host OS, plus allows you to benefit from hardware access.

FIGURE 32 - CLICK LIVE BOOT

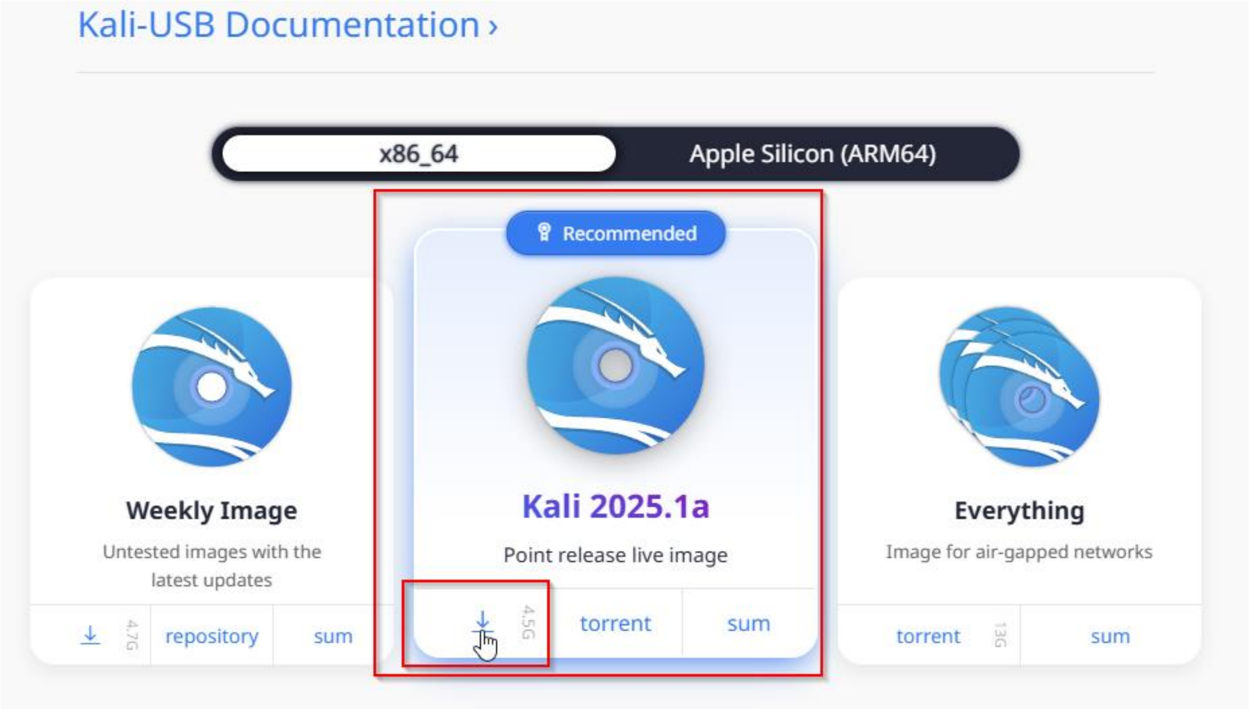
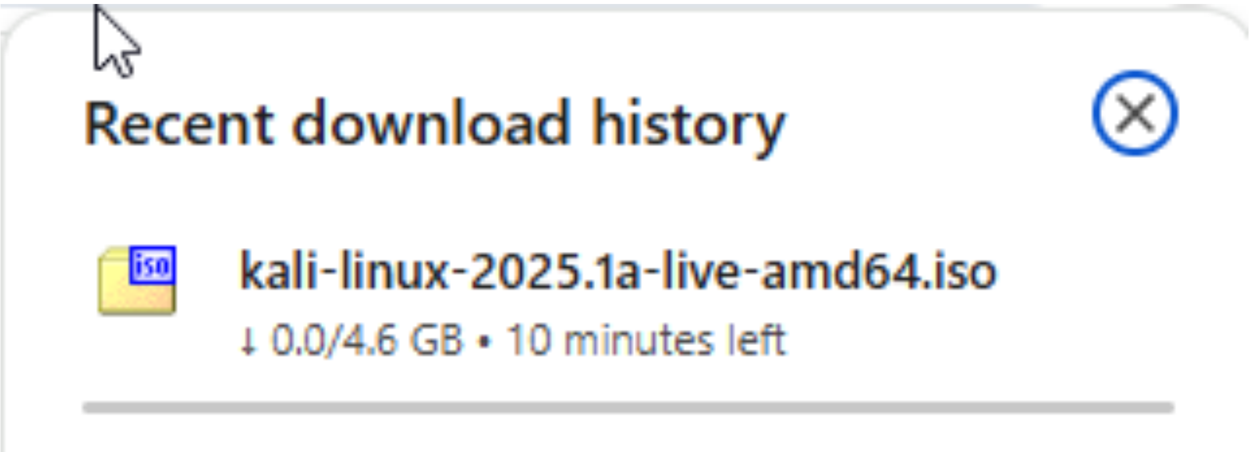


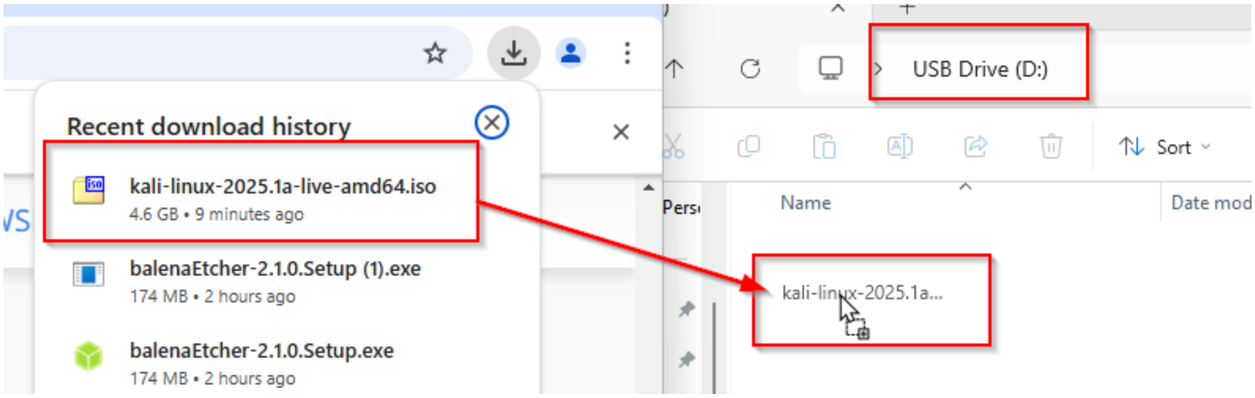
FIGURE 33 - CLICK KALI 2025.1A TO DOWNLOAD



kali-linux-2025.1a-live-amd64.iso

↓ 0.0/4.6 GB • 10 minutes left

FIGURE 34 - DOWNLOADING....



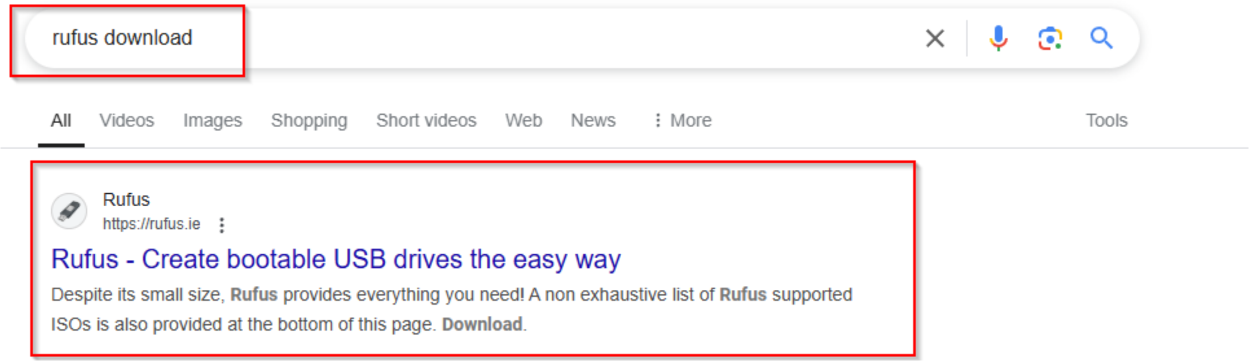
Recent download history

kali-linux-2025.1a-live-amd64.iso
4.6 GB • 9 minutes ago

balenaEtcher-2.1.0.Setup (1).exe
174 MB • 2 hours ago

balenaEtcher-2.1.0.Setup.exe
174 MB • 2 hours ago

Figure 35 - Drag the ISO file to the USB



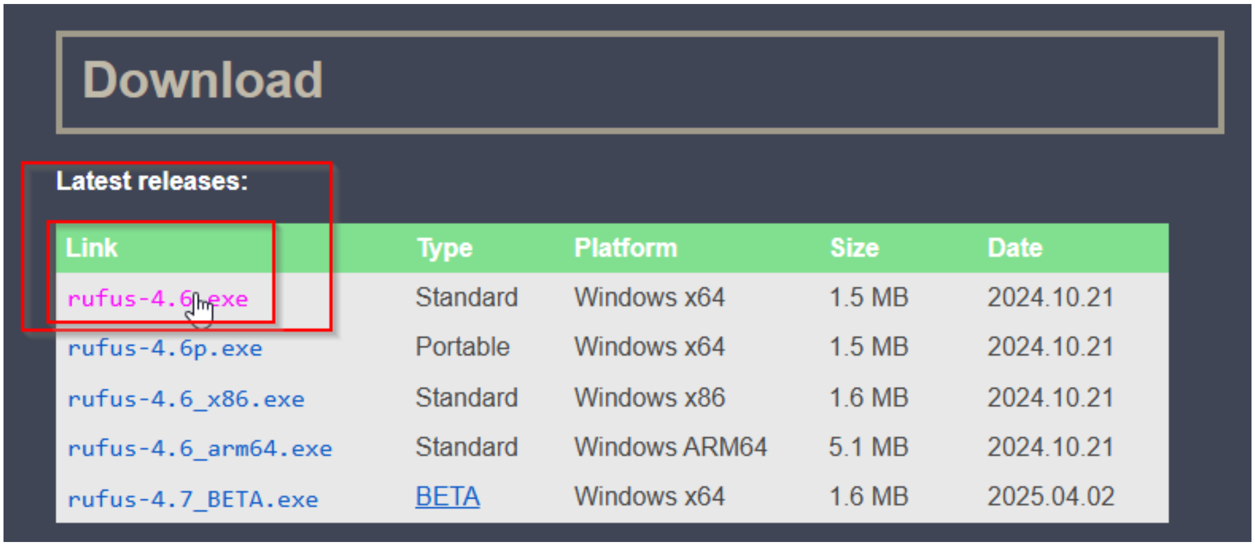
rufus download

Rufus
https://rufus.ie

Rufus - Create bootable USB drives the easy way

Despite its small size, **Rufus** provides everything you need! A non exhaustive list of **Rufus** supported ISOs is also provided at the bottom of this page. **Download**.

Figure 36 - Type 'Rufus' on the google URL then click Rufus on the link

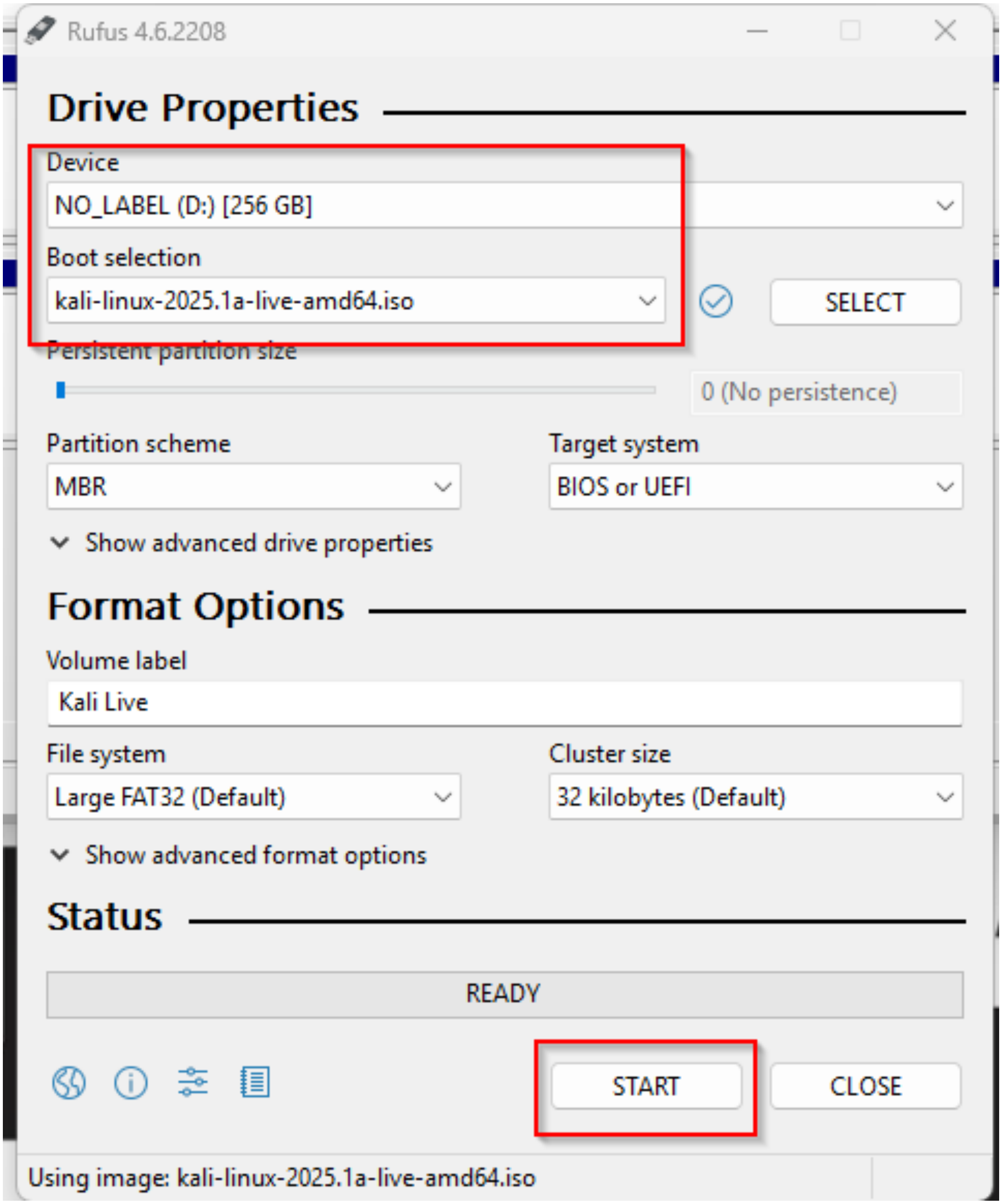


Download

Latest releases:

Link	Type	Platform	Size	Date
rufus-4.6.exe	Standard	Windows x64	1.5 MB	2024.10.21
rufus-4.6p.exe	Portable	Windows x64	1.5 MB	2024.10.21
rufus-4.6_x86.exe	Standard	Windows x86	1.6 MB	2024.10.21
rufus-4.6_arm64.exe	Standard	Windows ARM64	5.1 MB	2024.10.21
rufus-4.7_BETA.exe	BETA	Windows x64	1.6 MB	2025.04.02

Figure 37 - Download Rufus.exe



Rufus 4.6.2208

Drive Properties

Device: NO_LABEL (D:) [256 GB]

Boot selection: kali-linux-2025.1a-live-amd64.iso

Persistent partition size: 0 (No persistence)

Partition scheme: MBR

Target system: BIOS or UEFI

Format Options

Volume label: Kali Live

File system: Large FAT32 (Default)

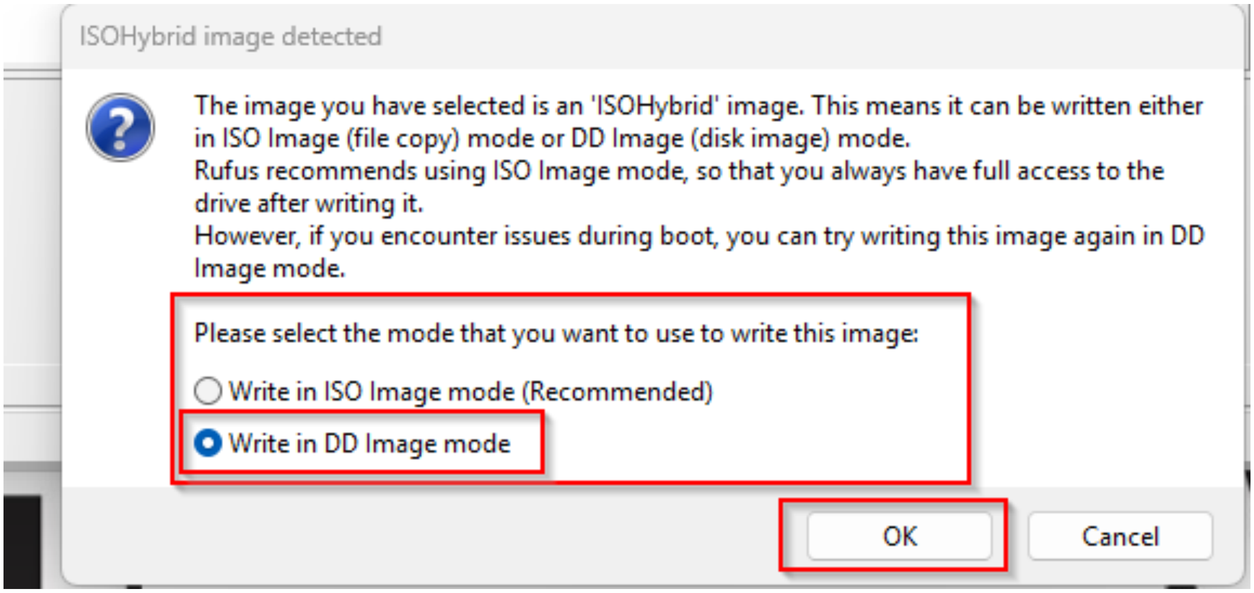
Cluster size: 32 kilobytes (Default)

Status

READY

Using image: kali-linux-2025.1a-live-amd64.iso

Figure 38 - Use the USB as device then boot as kali then get start!



ISOHybrid image detected

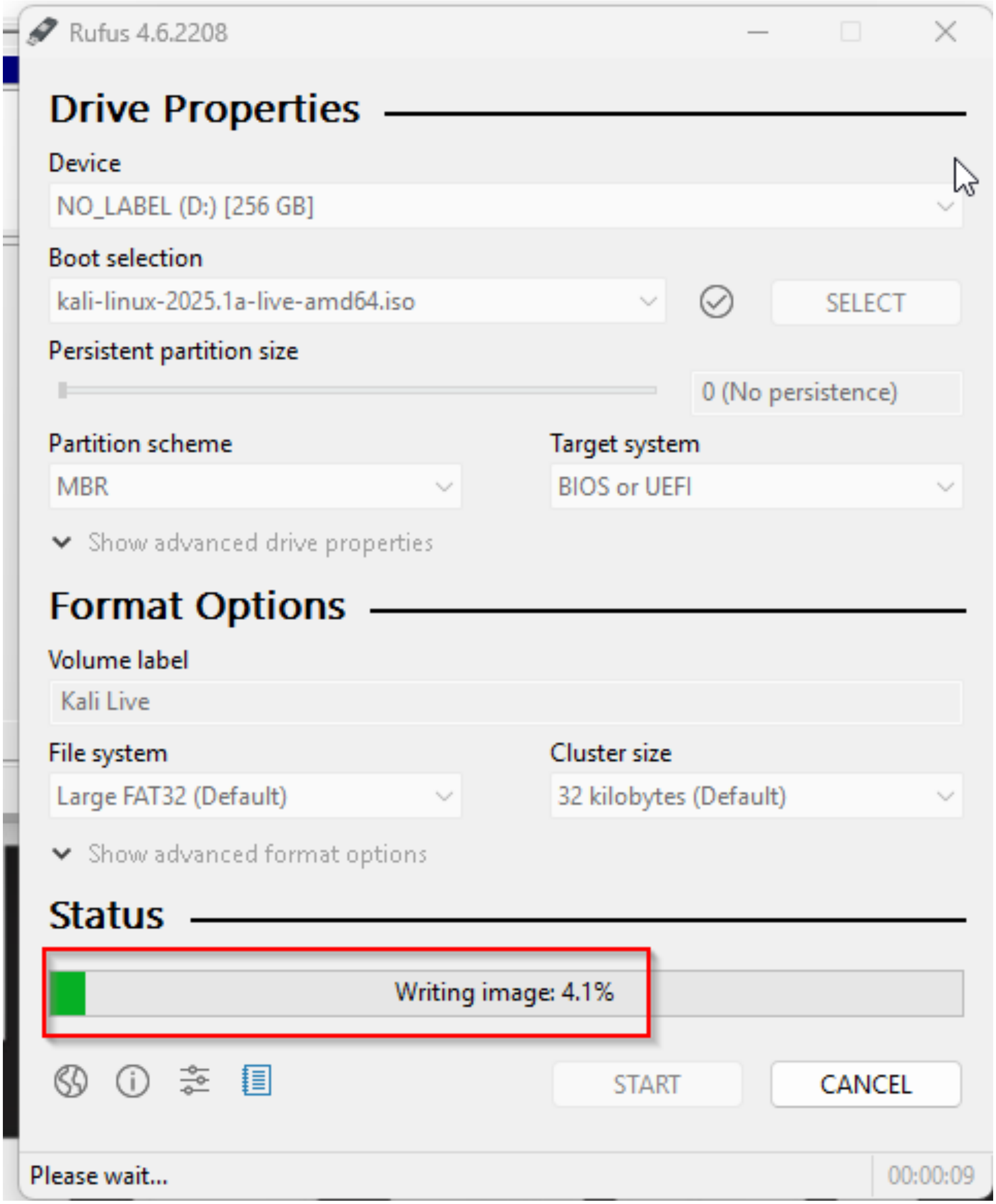
The image you have selected is an 'ISOHybrid' image. This means it can be written either in ISO Image (file copy) mode or DD Image (disk image) mode.
Rufus recommends using ISO Image mode, so that you always have full access to the drive after writing it.
However, if you encounter issues during boot, you can try writing this image again in DD Image mode.

Please select the mode that you want to use to write this image:

○ Write in ISO Image mode (Recommended)

● Write in DD Image mode

FIGURE 39 - CLICK 'WRITE IN DD IMAGE MODE" THEN CLICK OK



Drive Properties

Device: NO_LABEL (D:) [256 GB]

Boot selection: kali-linux-2025.1a-live-amd64.iso

Persistent partition size: 0 (No persistence)

Partition scheme: MBR

Target system: BIOS or UEFI

Format Options

Volume label: Kali Live

File system: Large FAT32 (Default)

Cluster size: 32 kilobytes (Default)

Status

Writing image: 4.1%

Please wait...

00:00:09

FIGURE 40 - WRITING IMAGE....

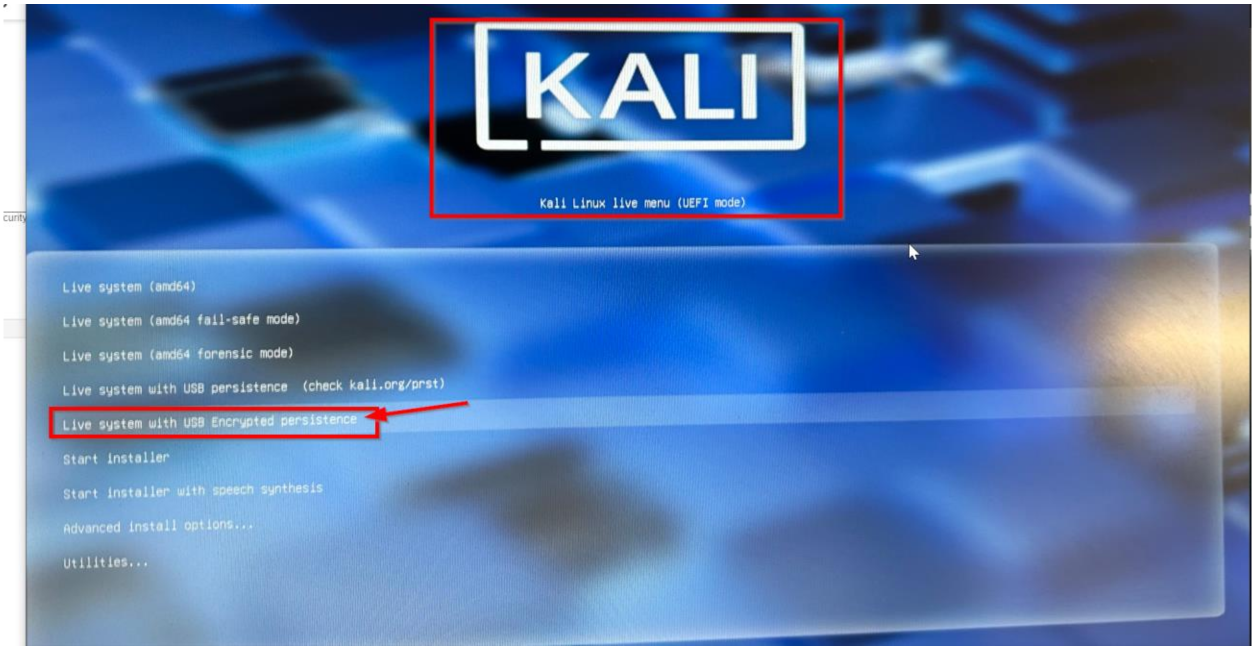
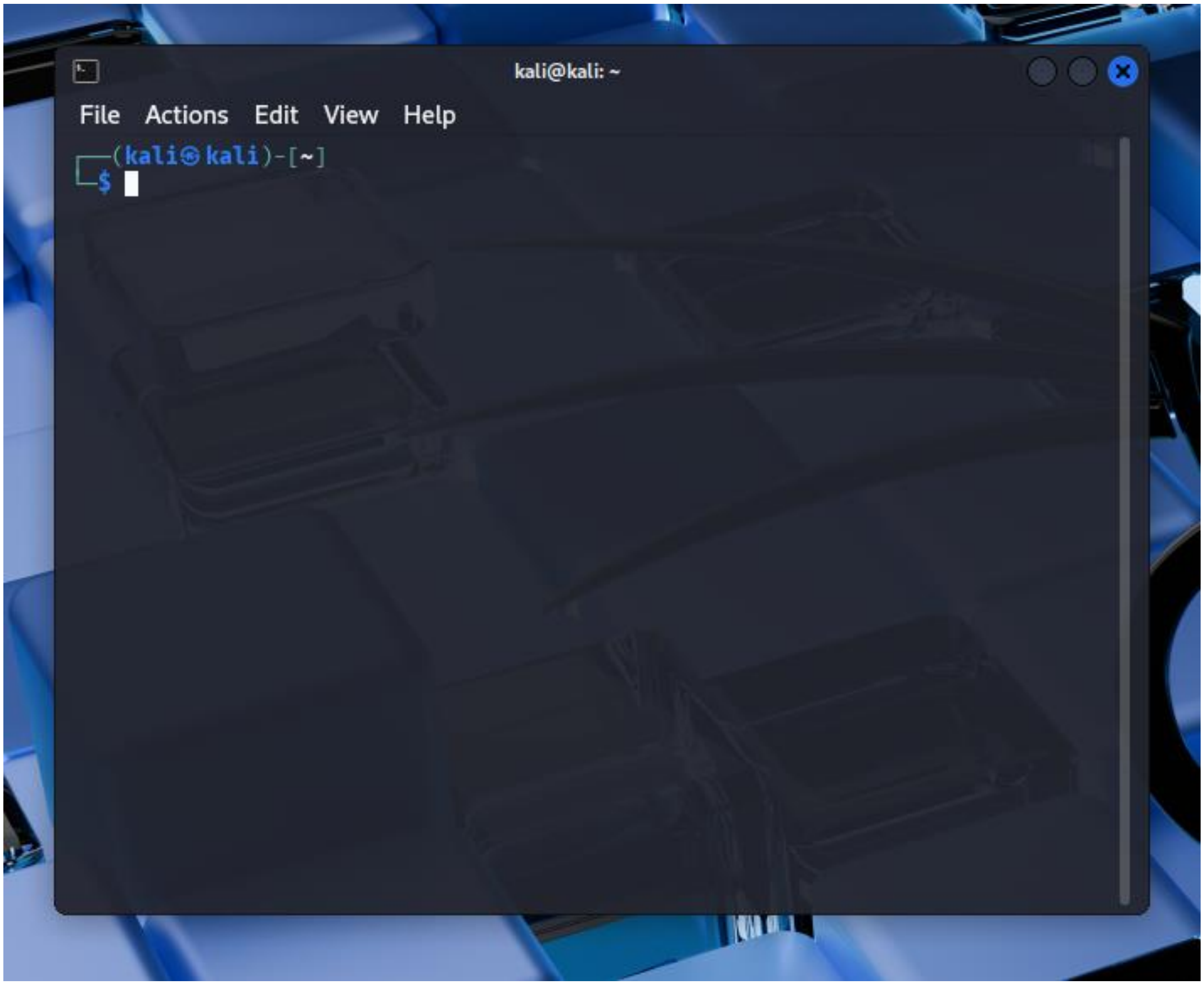

KALI
Kali Linux live menu (UEFI mode)
Live system (amd64)
Live system (amd64 fail-safe mode)
Live system (amd64 forensic mode)
Live system with USB persistence (check kali.org/prst)
Live system with USB Encrypted persistence
Start installer
Start installer with speech synthesis
Advanced install options...
Utilities...

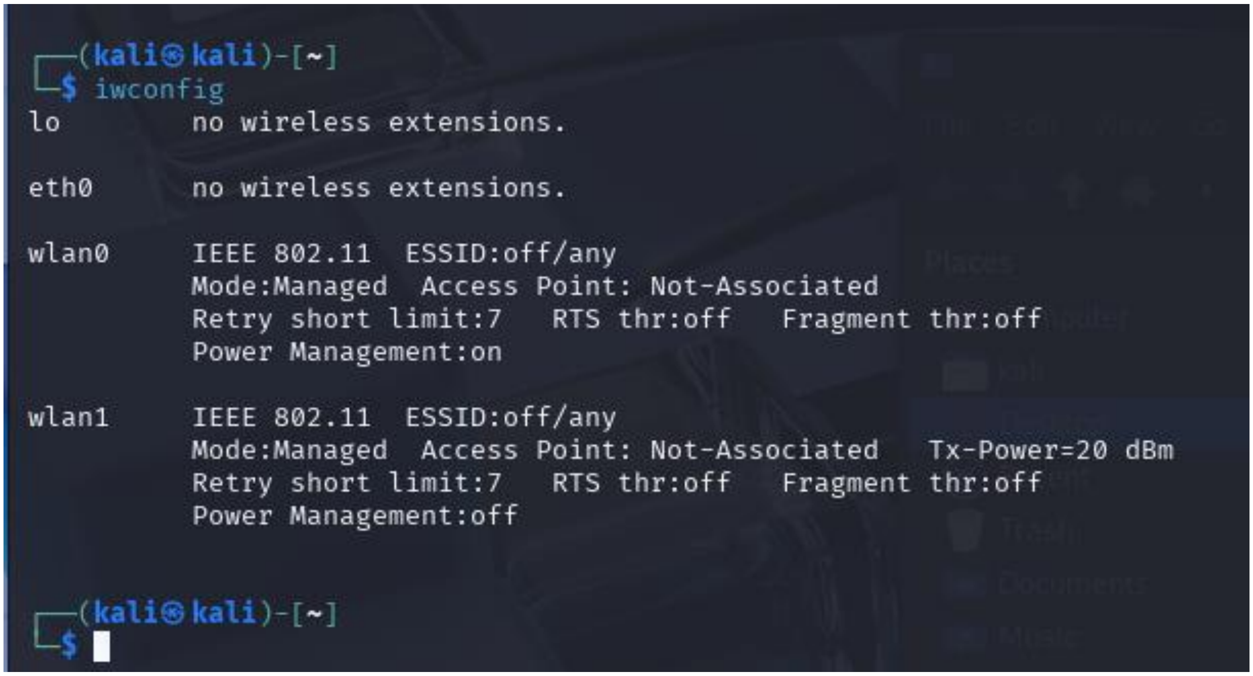
FIGURE 41 - CLICK LIVE SYSTEM TO BOOT KALI UP

FIGURE 42 - BOOTING UP...



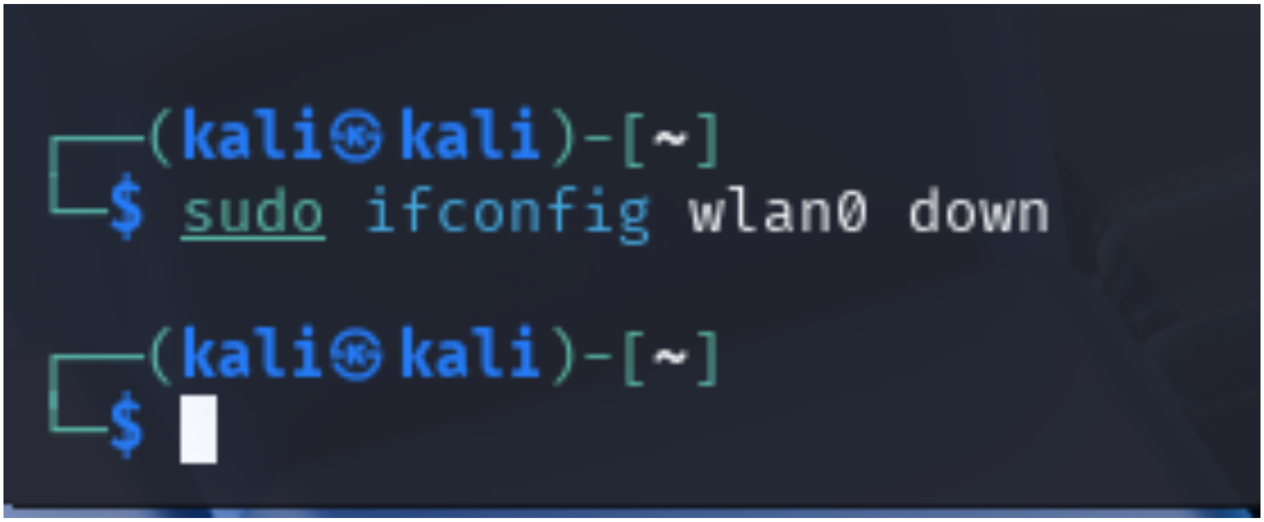
```
┌──(kali㉿kali)-[~]
└─$ 
```

FIGURE 43 - OPEN THE KALI TERMINAL



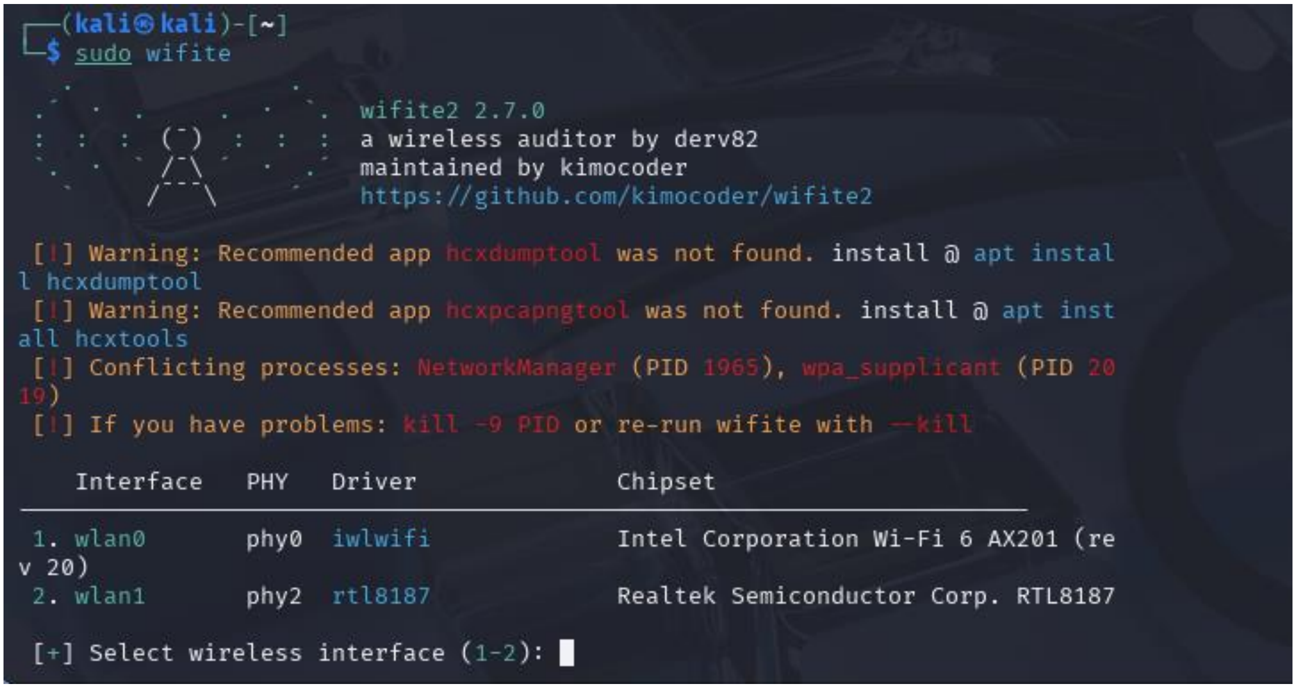
```
┌──(kali㉿kali)-[~]
└─$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:on

wlan1     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off


┌──(kali㉿kali)-[~]
└─$ 
```

FIGURE 44 - TYPE THE COMMAND TO SEE THE LIST OF WIRELESS INTERFACES



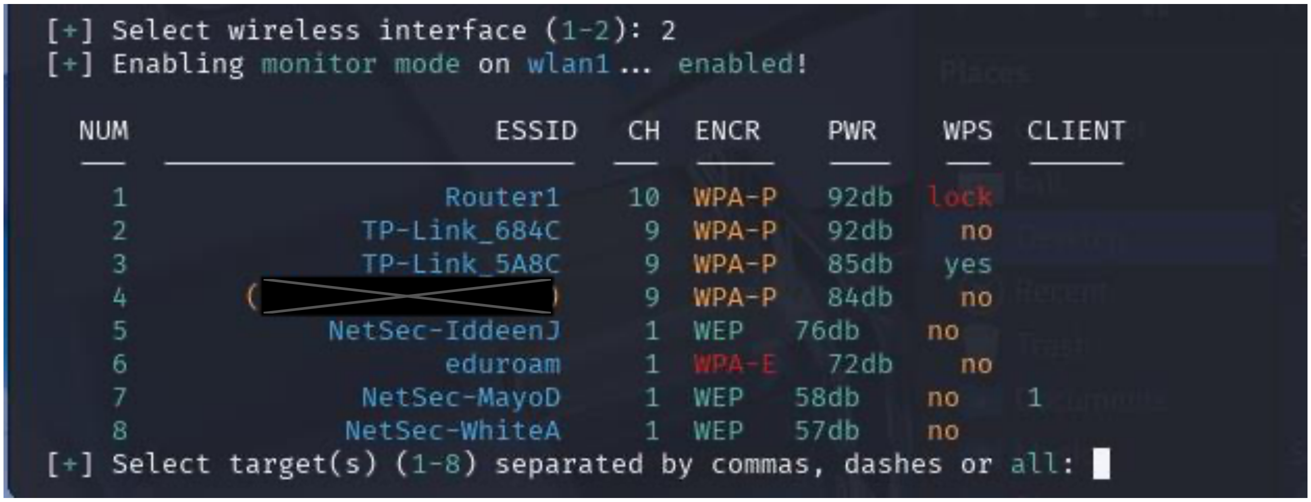
```
┌──(kali㉿kali)-[~]
└─$ sudo ifconfig wlan0 down

┌──(kali㉿kali)-[~]
└─$ 
```

FIGURE 45 - TYPE THE COMMAND TO KILL THE FIRST WIRELESS NETWORK (WI-FI)



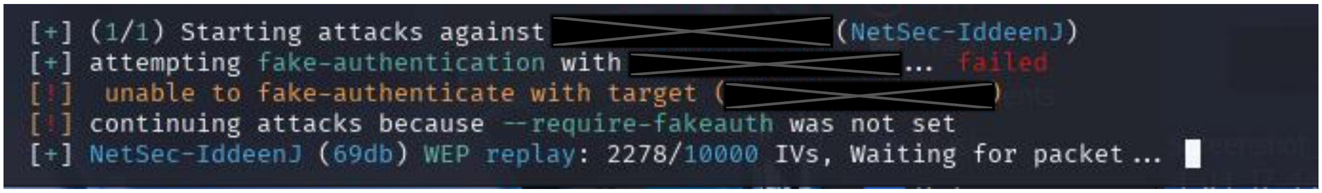
```
┌──(kali㉿kali)-[~]
└─$ sudo wifite
   .               .
 .´  ·  .     .  ·  `.  wifite2 2.7.0
 :  :  :  (¯)  :  :  :  a wireless auditor by derv82
 `.  ·  ` /¯\ ´  ·  .´  maintained by kimocoder
   `     /¯¯¯\     ´    https://github.com/kimocoder/wifite2

 [!] Warning: Recommended app hcxdumptool was not found. install @ apt instal
l hcxdumptool
 [!] Warning: Recommended app hcxpcapngtool was not found. install @ apt inst
all hcxtools
 [!] Conflicting processes: NetworkManager (PID 1965), wpa_supplicant (PID 20
19)
 [!] If you have problems: kill -9 PID or re-run wifite with --kill

    Interface   PHY   Driver              Chipset
 ───────────────────────────────────────────────────────────────────────
  1. wlan0      phy0  iwlwifi             Intel Corporation Wi-Fi 6 AX201 (re
v 20)
  2. wlan1      phy2  rtl8187             Realtek Semiconductor Corp. RTL8187

 [+] Select wireless interface (1-2): 
```

FIGURE 46 - TYPE THE COMMAND TO START HACKING



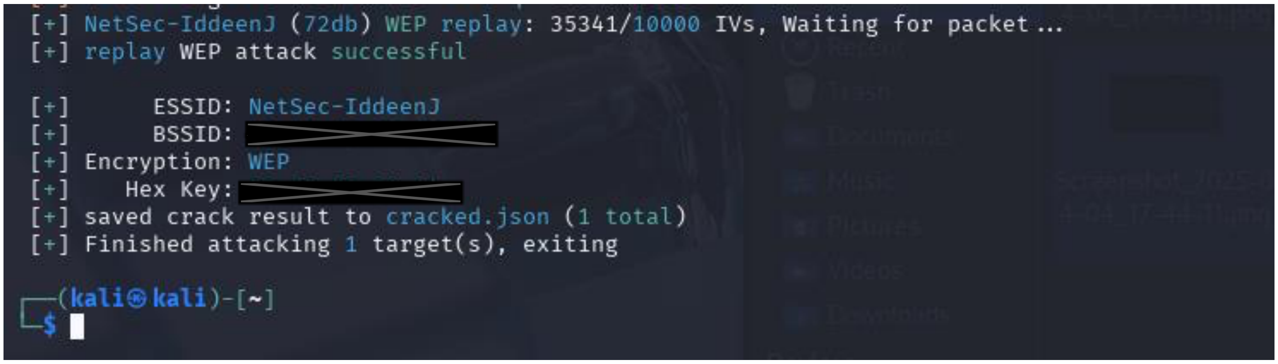
```
[+] Select wireless interface (1-2): 2
[+] Enabling monitor mode on wlan1... enabled!

   NUM                     ESSID   CH  ENCR    PWR   WPS  CLIENT
   ───   ──────────────────────── ──  ─────  ─────  ───  ──────
     1                   Router1   10  WPA-P   92db  lock
     2              TP-Link_684C    9  WPA-P   92db   no
     3              TP-Link_5A8C    9  WPA-P   85db  yes
     4           ([redacted])       9  WPA-P   84db   no
     5           NetSec-IddeenJ     1  WEP   76db    no
     6                   eduroam    1  WPA-E   72db   no
     7           NetSec-MayoD       1  WEP   58db    no      1
     8           NetSec-WhiteA      1  WEP   57db    no
[+] Select target(s) (1-8) separated by commas, dashes or all: 
```

FIGURE 47 - LOOKING FOR THE WI-FI TO HACK



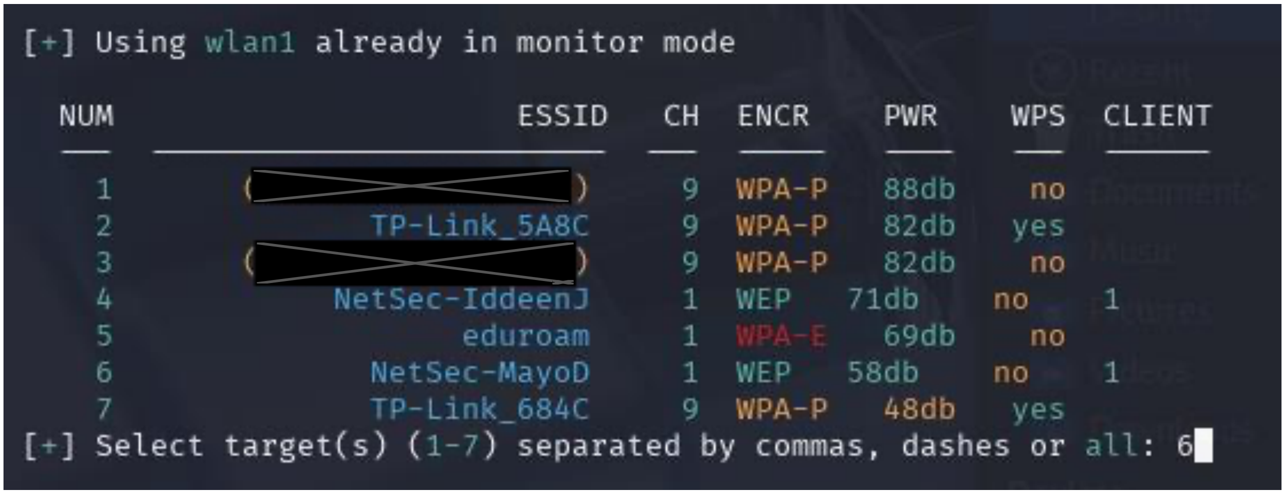
```
[+] (1/1) Starting attacks against [redacted] (NetSec-IddeenJ)
[+] attempting fake-authentication with [redacted]... failed
[!]  unable to fake-authenticate with target ([redacted])
[!] continuing attacks because --require-fakeauth was not set
[+] NetSec-IddeenJ (69db) WEP replay: 2278/10000 IVs, Waiting for packet... 
```

FIGURE 48 - SENDING IVS TO THE WI-FI



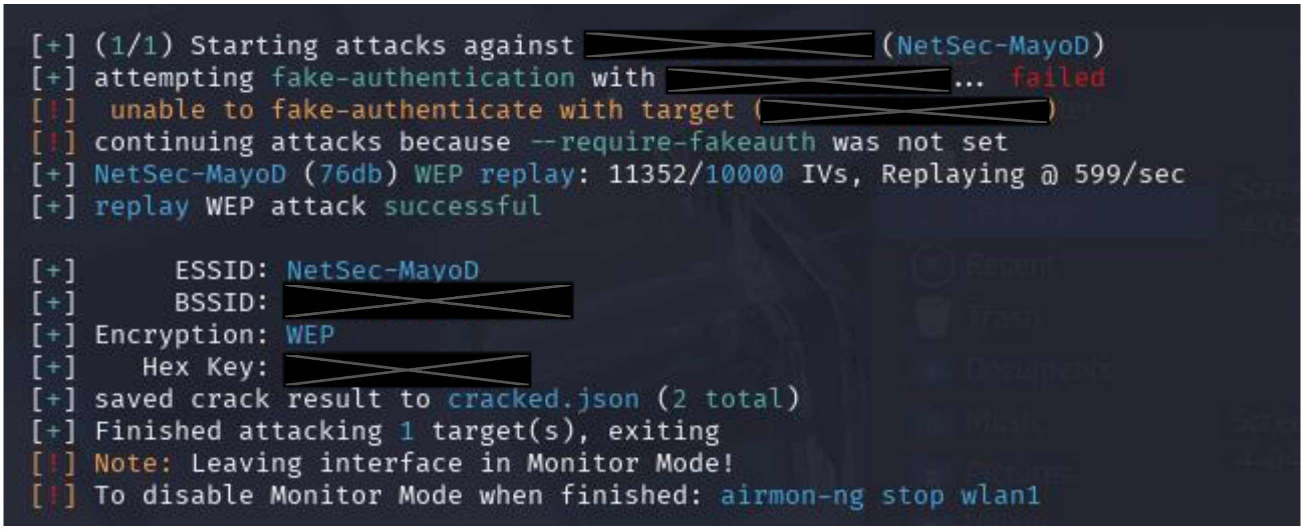
```
[+] NetSec-IddeenJ (72db) WEP replay: 35341/10000 IVs, Waiting for packet...
[+] replay WEP attack successful

[+]      ESSID: NetSec-IddeenJ
[+]      BSSID: [redacted]
[+] Encryption: WEP
[+]    Hex Key: [redacted]
[+] saved crack result to cracked.json (1 total)
[+] Finished attacking 1 target(s), exiting

┌──(kali㉿kali)-[~]
└─$ 
```

FIGURE 49 - GOT THE PASSWORD!



```
[+] Using wlan1 already in monitor mode

  NUM                      ESSID   CH  ENCR    PWR    WPS  CLIENT
  ---   ------------------------   --  -----   -----  ---  ------
    1          ([redacted])         9  WPA-P   88db    no
    2              TP-Link_5A8C     9  WPA-P   82db   yes
    3          ([redacted])         9  WPA-P   82db    no
    4            NetSec-IddeenJ     1  WEP    71db    no     1
    5                   eduroam     1  WPA-E   69db    no
    6              NetSec-MayoD     1  WEP    58db    no     1
    7              TP-Link_684C     9  WPA-P   48db   yes
[+] Select target(s) (1-7) separated by commas, dashes or all: 6
```

FIGURE 50 - TRYING TO HACK DIFFERENT WI-FI AGAIN



```
[+] (1/1) Starting attacks against [redacted] (NetSec-MayoD)
[+] attempting fake-authentication with [redacted]... failed
[!]  unable to fake-authenticate with target ([redacted])
[!] continuing attacks because --require-fakeauth was not set
[+] NetSec-MayoD (76db) WEP replay: 11352/10000 IVs, Replaying @ 599/sec
[+] replay WEP attack successful

[+]      ESSID: NetSec-MayoD
[+]      BSSID: [redacted]
[+] Encryption: WEP
[+]    Hex Key: [redacted]
[+] saved crack result to cracked.json (2 total)
[+] Finished attacking 1 target(s), exiting
[!] Note: Leaving interface in Monitor Mode!
[!] To disable Monitor Mode when finished: airmon-ng stop wlan1
```

FIGURE 51 - GOT THE PASSWORD!

QUESTIONS AND ANSWERS

- NONE.

OBSERVATIONS

Easy to understand but also cracking the WEP key was easy once the setup was correct. But also, I tried to do another second attempt failed due to tricky authentication issues.