Documentation of EnDa Wi-Fi Exposer

Basmaci Enes (EnDaTeam on GITHUB)

June 4, 2023

1 Introduction

I had a problem with a customized capture flag challenge that I created, I needed a tool that gets all WiFi network saved passwords from a hacked laptop, but there was a ton of SSIDs that I needed to check it, so I had an idea: To create a functional tool that people can use. I start the timer, I set it to 2 hours (because this tool was a part of my challenge - Create a perfect tool in 2 hours, all in 1) end I started the work. I searched in many sources, I investigate the windows and Linux principals and ended with an application for Ethical Hackers (White Hat).

2 Situation where you can use this tool

2.1 The meeting of twined faces

Let's imagine a situation: You have been invited to a group study meeting, and your target that you are trying to is here, so your evil brain thinks about a hacking plan. You get your fancy USB full with Hacking Tools, but you are using them for illegal activities, because your are a red-hat hacker. So you arrived to established location and the meeting started. You are waiting the perfect time: Target asks permission to go to bathroom or something distracted his attention. This is the time. You plug-in the USB, run the 'EnDa Wi-Fi Exposer.exe', the records of registered WiFi started listing. Then you take a picture of Display, and unplug the USB or you just screenshot the tab and save it into USB, then you unplug the it. The operation was completed successfully, now you have the a list of saved WiFi passwords. You can continue executing your operation with another types of attacks, and maybe, if the home network's WiFi password is customized, that is the password for all his accounts on internet.

2.2 Tester of Networks

Another situation : You are have opportunity to infiltrate to a company, and you have an initial access or just time to get an empty laptop which has the network of company. You get the password with this application, connect to network and you can start the attacks.

2.3 Betrayal of the neighbor

Objective : Hack the neighbour (someone near you or just a person who gives you an opportunity, to get closer to him) Situation : You want to hack someone which is very close to you (like distance) for interest. You can't find a vulnerability in his devices or his network, so you have to create your own vulnerability. To initial access you can use his network: infiltrate to his network and manipulate the traffic with MITM (Man in the middle) or another attacks.

2.4 Basic information harvesting

The main situation where you will be in need of this tool if for getting more information of principal target that you want to hack. It maybe be from someone with who he is sharing his network, which maybe is much naive and easier to manipulate to get the opportunity of making a escalation to an admin privileges (with an initial access) and get more information about the network, then control the whole internet traffic.

3 How this application works

3.1 The main principle of application

There are some commands that you can execute windows to give you the SSID which are stored (*netsh wlan show profiles*), after that you can use another command to get the key (password) of that WiFi network (*netsh wlan show profile -ssid- key=clear*). At Linux the all credentials are stored in a file in a path (*/etc/NetworkManager/system-connections/*), that you can open and get the data. This program does it very easy and very fast that you can do it. So basically the application gets the data from this outputs and prints it out for you.

3.2 The function for windows

It runs the command ("netsh wlan show profiles") and decodes the output. Then creates a list to store the whole SSID that have been founded. After that, the script executes a command ("netsh wlan show profile "ssid" key=clear") for every SSID found and append the results on the 'winlist' empty list to be easier to implement into a table.

3.3 The function for Linux

It access the file from a path ("/etc/NetworkManager/system-connections"), splits the output and stores it in a table to print it.

3.4 Style of script

When the script is run, it clears the previous commands and prints a fancy banner with random colors. After that, some messages and the main table (structured in columns and rows). Then, an option if you wanna refresh the program, if you type 'n' it will close else if will refresh the application. If you will try exiting script with 'CTRL-C',it will handle it and asks you a question : Do you want to refresh the program?

4 Some screenshots of product

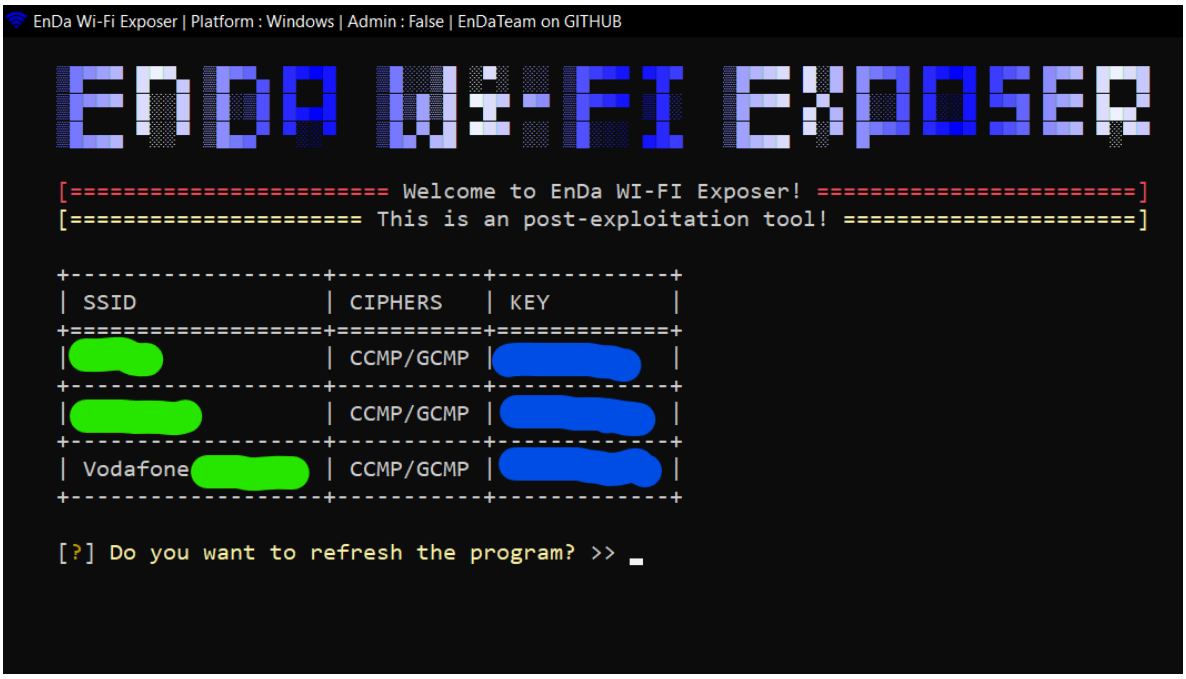

Figure 1: The main program

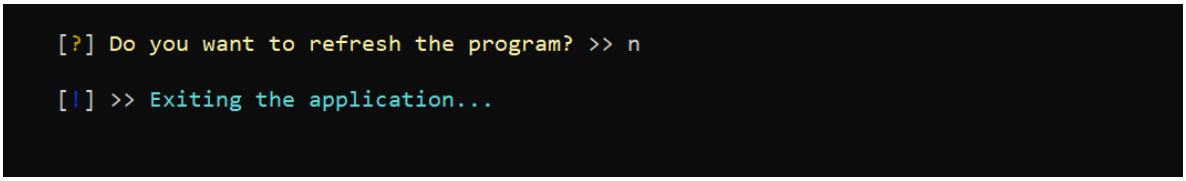

Figure 2: The answer to no of input

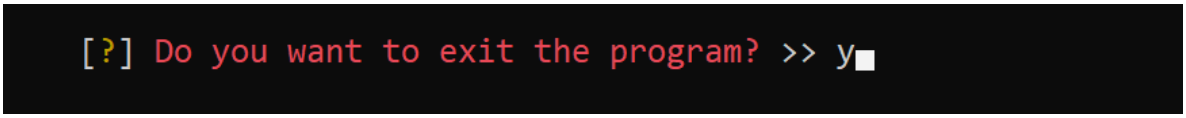

Figure 3: The KeyboardInterrupt error handler