this is how the script lock like in the terminal we can see all the steps we made

```
┌──(kali㉿kali)-[~]
└─$ sudo ./project_pt.sh
[#] Analysis started at: 2024-02-07 17:19:26
[#] All the tools we will need have been downloaded or are already in the system
[#] Choose scan type ('basic' or 'full'): full
[#] Full type was chosen
[#] Enter name for the output directory:trash
[#] Enter network to scan: 192.168.146.139
[#] valid net!
[#] Scanning for open TCP ports with service version detection ...
[#] TCP scan saved into trash/tcp_scan.txt

[#] Scanning for open UDP ports with service version detection ...
[#] udp scan saved into trash/udp_scan.txt

[#] searching for vulnerability
[#] searching for vulnerability saved into trash/vulnerability_scan.txt

[#] searching for weak passwords used in the network for login services
[#] searching for weak passwords saved into trash/weekpass_scan.txt

[#] Starting password brute-force scan ...
[#] Do you want to use the built-in password list? (yes/no): yes
[#] Enter the username for brute-force attack: kali
[#] Full scan completed. Results saved in trash directory.
```

```
Do you want to compress the results into a zip file? (yes/no): yes
Enter the name for the zip file: trash.zip
        zip warning: name not matched: trash

zip error: Nothing to do! (try: zip -r trash.zip.zip . -i trash)
Results compressed and saved as trash.zip.zip
```