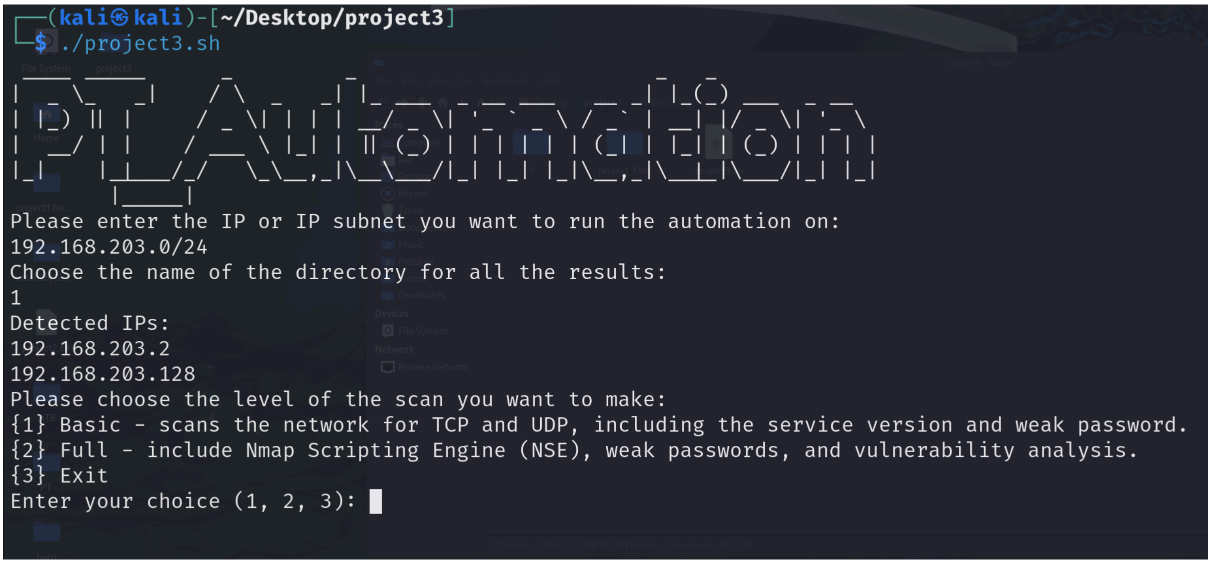
output of the script running - Yarin Martsiano

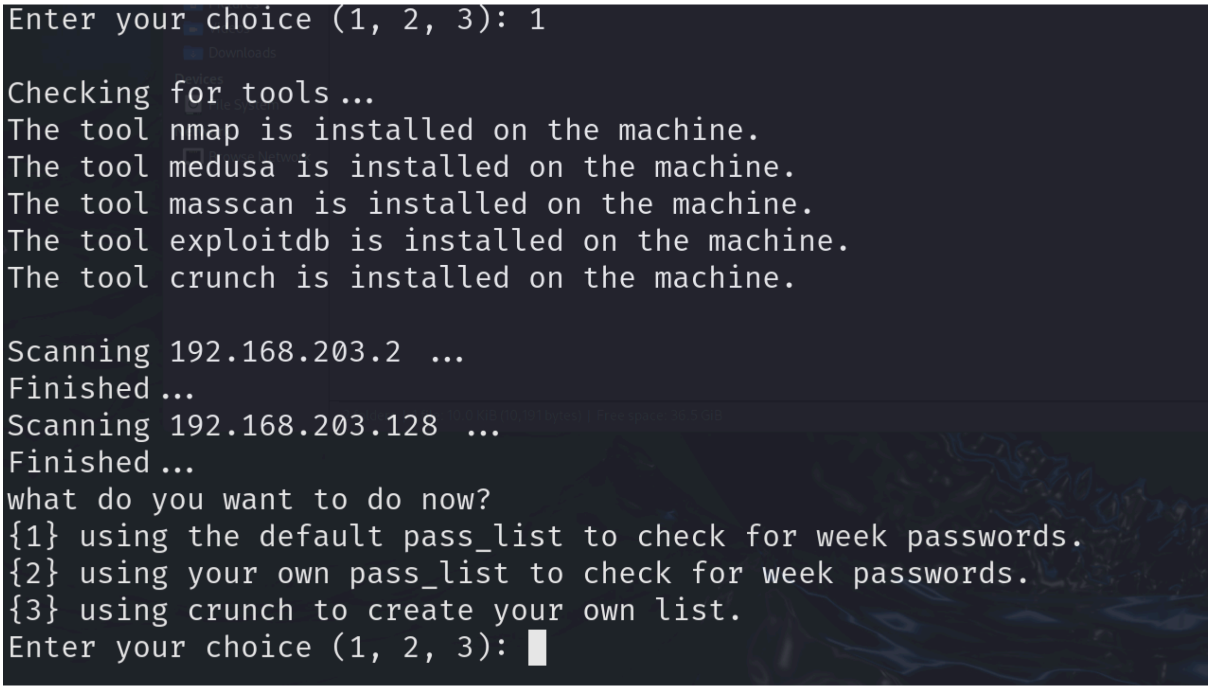


```
┌──(kali㉿kali)-[~/Desktop/project3]
└─$ ./project3.sh
 ____ _____        _         _                        _   _
|  _ \_   _|      / \  _   _| |_ ___  _ __ ___   __ _| |_(_) ___  _ __
| |_) || |       / _ \| | | | __/ _ \| '_ ` _ \ / _` | __| |/ _ \| '_ \
|  __/ | |      / ___ \ |_| | || (_) | | | | | | (_| | |_| | (_) | | | |
|_|    |_|_____/_/   \_\__,_|\__\___/|_| |_| |_|\__,_|\__|_|\___/|_| |_|
         |_____|
Please enter the IP or IP subnet you want to run the automation on:
192.168.203.0/24
Choose the name of the directory for all the results:
1
Detected IPs:
192.168.203.2
192.168.203.128
Please choose the level of the scan you want to make:
{1} Basic - scans the network for TCP and UDP, including the service version and weak password.
{2} Full - include Nmap Scripting Engine (NSE), weak passwords, and vulnerability analysis.
{3} Exit
Enter your choice (1, 2, 3): 
```

1. asking the user of the script what is the ip address or ip subnet input he want to use and what is the name of the directory he want for the results

2. the user can now choose what he want to do, which scan to use, and an option for exit

option 1 (Basic):

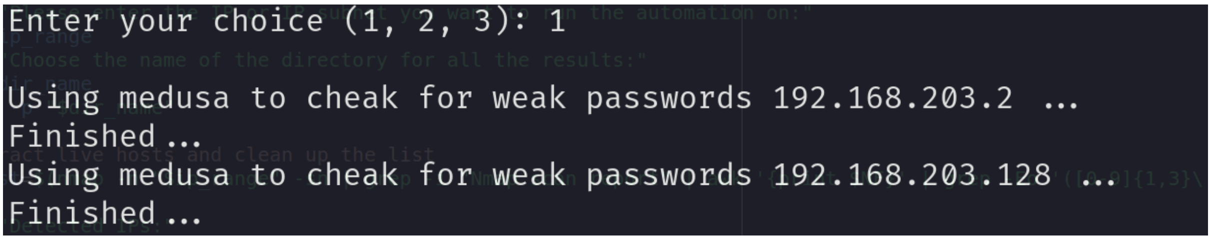


```
Enter your choice (1, 2, 3): 1

Checking for tools...
The tool nmap is installed on the machine.
The tool medusa is installed on the machine.
The tool masscan is installed on the machine.
The tool exploitdb is installed on the machine.
The tool crunch is installed on the machine.

Scanning 192.168.203.2 ...
Finished...
Scanning 192.168.203.128 ...
Finished...
what do you want to do now?
{1} using the default pass_list to check for week passwords.
{2} using your own pass_list to check for week passwords.
{3} using crunch to create your own list.
Enter your choice (1, 2, 3): 
```

1. checking if the tools that are required for the script are installed if not they will be installed
2. scanning the 2 ips in the network and saved the results in the directory that the user choose in the beginning

3. now we can choose how to check for weak passwords with using the default list (from my github), using the user own list or using crunch to create a new list

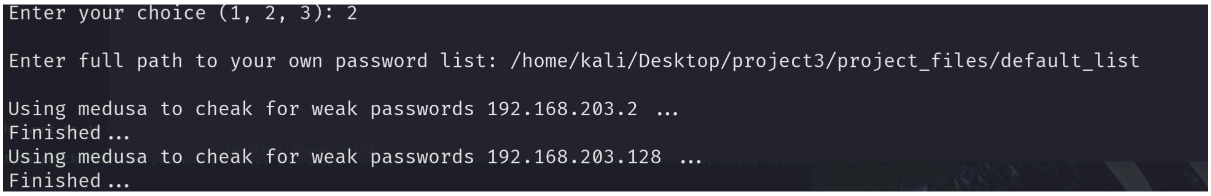
option 1:



```
Enter your choice (1, 2, 3): 1

Using medusa to cheak for weak passwords 192.168.203.2  ...
Finished ...
Using medusa to cheak for weak passwords 192.168.203.128  ...
Finished ...
```

using medusa and saving the results to the existing file

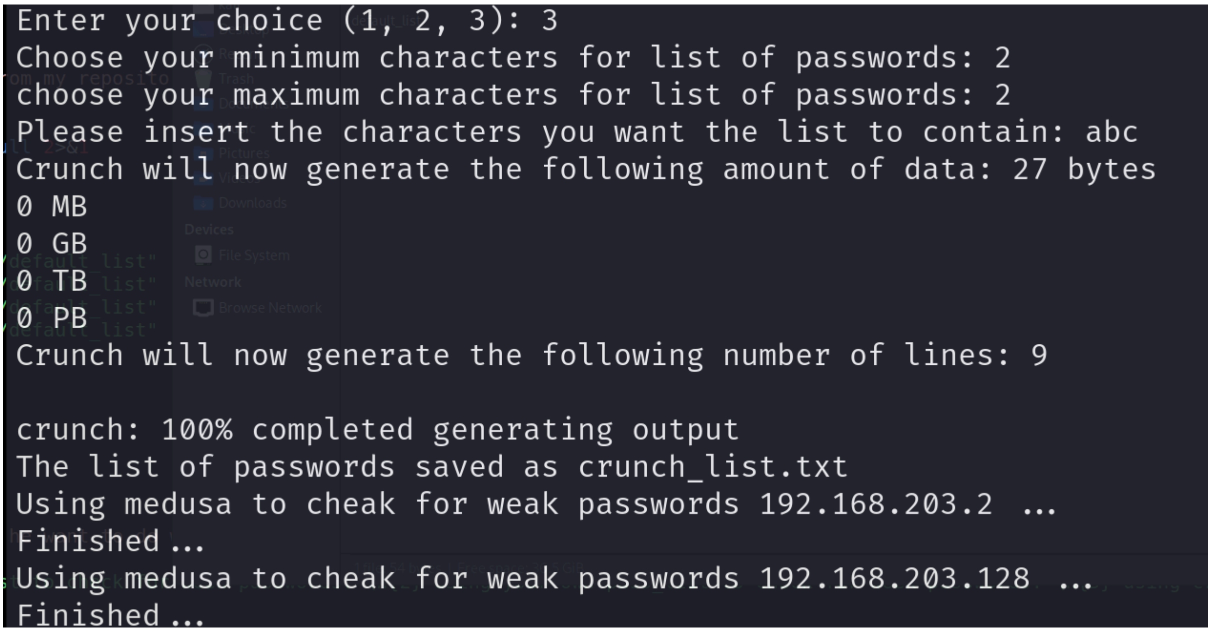
option 2:



```
Enter your choice (1, 2, 3): 2

Enter full path to your own password list: /home/kali/Desktop/project3/project_files/default_list

Using medusa to cheak for weak passwords 192.168.203.2  ...
Finished ...
Using medusa to cheak for weak passwords 192.168.203.128  ...
Finished ...
```

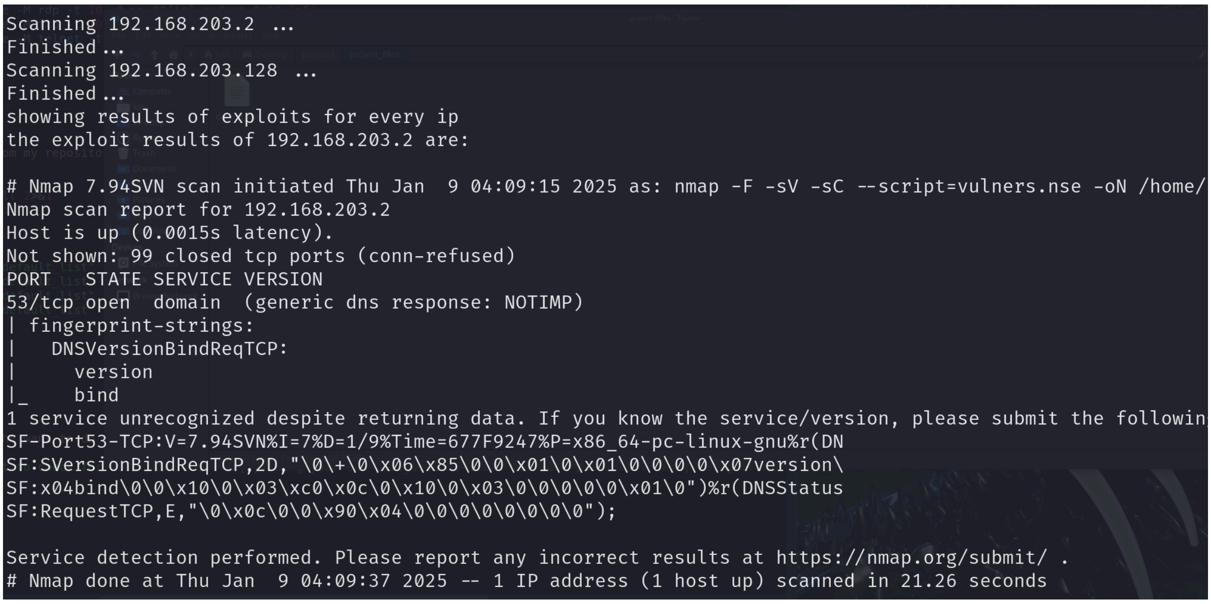
using medusa and saving the results to the existing file

option 3:



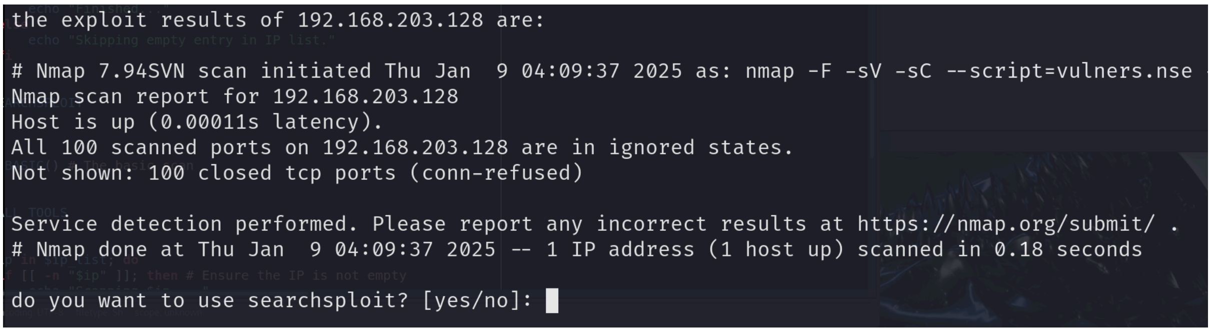
```
Enter your choice (1, 2, 3): 3
Choose your minimum characters for list of passwords: 2
choose your maximum characters for list of passwords: 2
Please insert the characters you want the list to contain: abc
Crunch will now generate the following amount of data: 27 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 9

crunch: 100% completed generating output
The list of passwords saved as crunch_list.txt
Using medusa to cheak for weak passwords 192.168.203.2  ...
Finished ...
Using medusa to cheak for weak passwords 192.168.203.128  ...
Finished ...
```

using crunch and medusa and saving the results to the existing file option 2 (Full):



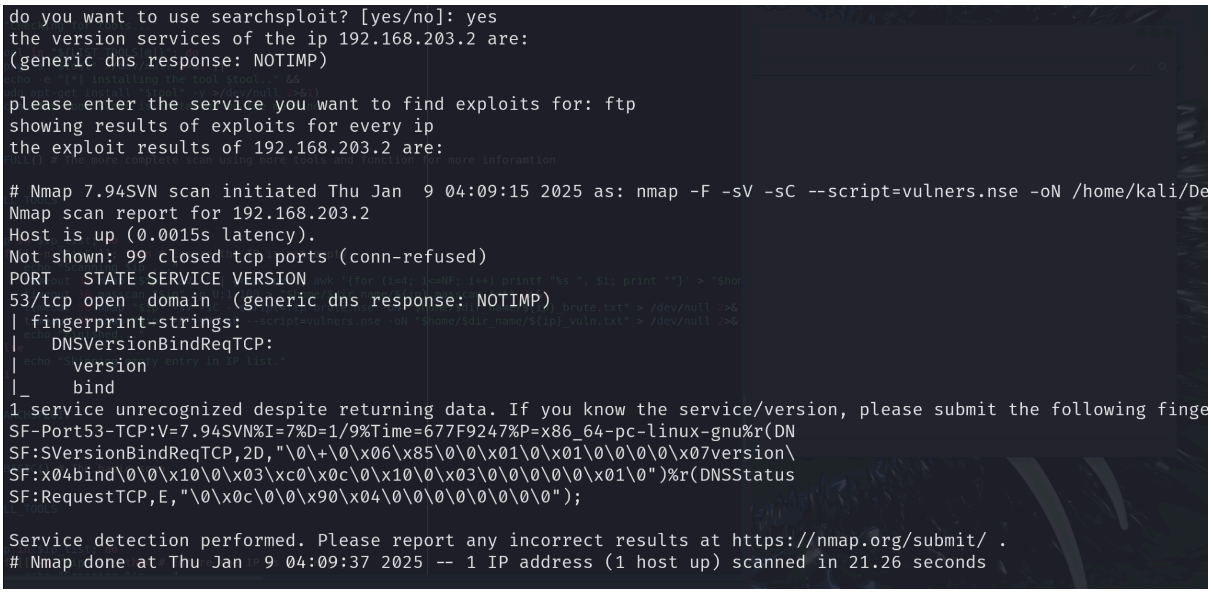
```
Scanning 192.168.203.2 ...
Finished...
Scanning 192.168.203.128 ...
Finished...
showing results of exploits for every ip
the exploit results of 192.168.203.2 are:

# Nmap 7.94SVN scan initiated Thu Jan  9 04:09:15 2025 as: nmap -F -sV -sC --script=vulners.nse -oN /home/
Nmap scan report for 192.168.203.2
Host is up (0.0015s latency).
Not shown: 99 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
53/tcp open  domain  (generic dns response: NOTIMP)
| fingerprint-strings:
|   DNSVersionBindReqTCP:
|     version
|_    bind
1 service unrecognized despite returning data. If you know the service/version, please submit the followin
SF-Port53-TCP:V=7.94SVN%I=7%D=1/9%Time=677F9247%P=x86_64-pc-linux-gnu%r(DN
SF:SVersionBindReqTCP,2D,"\0\+\0\x06\x85\0\0\x01\0\x01\0\0\0\0\x07version\
SF:x04bind\0\0\x10\0\x03\xc0\x0c\0\x10\0\x03\0\0\0\0\0\x01\0")%r(DNSStatus
SF:RequestTCP,E,"\0\x0c\0\0\x90\x04\0\0\0\0\0\0\0\0");

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Thu Jan  9 04:09:37 2025 -- 1 IP address (1 host up) scanned in 21.26 seconds
```

1. showing the results to the user and saving them to a file in the directory for after use



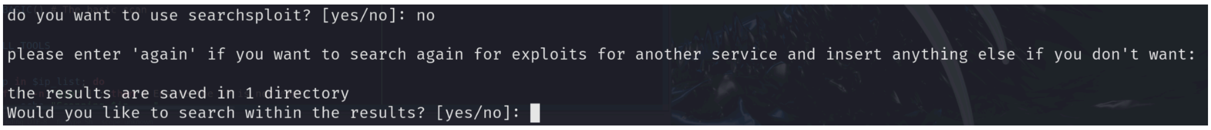
```
the exploit results of 192.168.203.128 are:

# Nmap 7.94SVN scan initiated Thu Jan  9 04:09:37 2025 as: nmap -F -sV -sC --script=vulners.nse
Nmap scan report for 192.168.203.128
Host is up (0.00011s latency).
All 100 scanned ports on 192.168.203.128 are in ignored states.
Not shown: 100 closed tcp ports (conn-refused)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Thu Jan  9 04:09:37 2025 -- 1 IP address (1 host up) scanned in 0.18 seconds

do you want to use searchsploit? [yes/no]: 
```

asking the user if he want to use searchsploit for more info



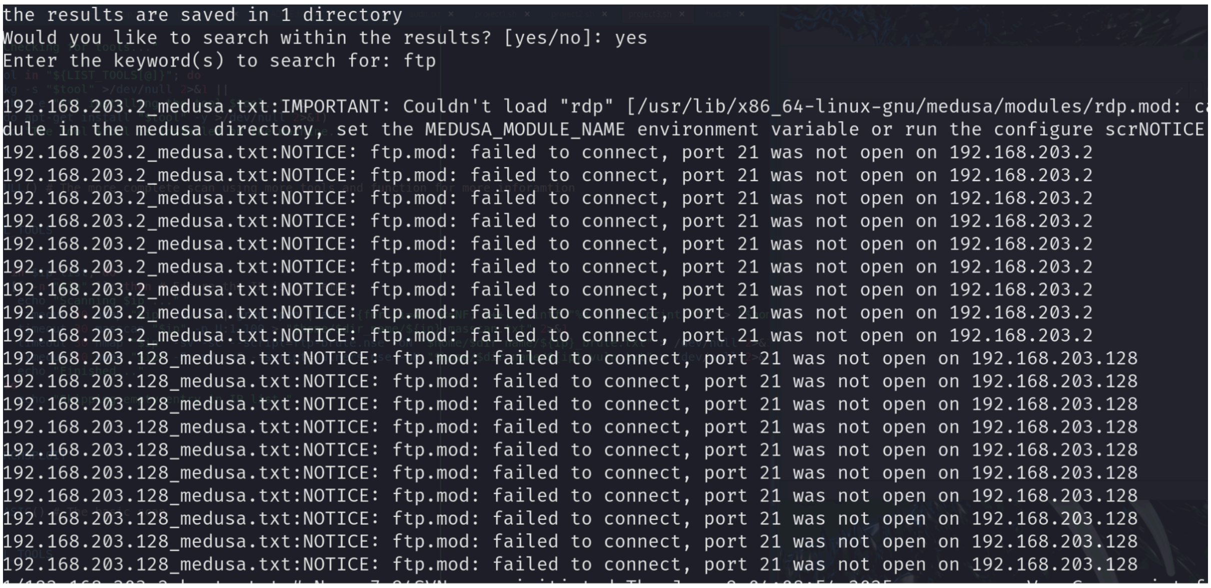
```
do you want to use searchsploit? [yes/no]: yes
the version services of the ip 192.168.203.2 are:
(generic dns response: NOTIMP)

please enter the service you want to find exploits for: ftp
showing results of exploits for every ip
the exploit results of 192.168.203.2 are:

# Nmap 7.94SVN scan initiated Thu Jan  9 04:09:15 2025 as: nmap -F -sV -sC --script=vulners.nse -oN /home/kali/De
Nmap scan report for 192.168.203.2
Host is up (0.0015s latency).
Not shown: 99 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
53/tcp open  domain  (generic dns response: NOTIMP)
| fingerprint-strings:
|   DNSVersionBindReqTCP:
|     version
|_    bind
1 service unrecognized despite returning data. If you know the service/version, please submit the following finge
SF-Port53-TCP:V=7.94SVN%I=7%D=1/9%Time=677F9247%P=x86_64-pc-linux-gnu%r(DN
SF:SVersionBindReqTCP,2D,"\0\+\0\x06\x85\0\0\x01\0\x01\0\0\0\0\x07version\
SF:x04bind\0\0\x10\0\x03\xc0\x0c\0\x10\0\x03\0\0\0\0\0\x01\0")%r(DNSStatus
SF:RequestTCP,E,"\0\x0c\0\0\x90\x04\0\0\0\0\0\0\0\0");

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Thu Jan  9 04:09:37 2025 -- 1 IP address (1 host up) scanned in 21.26 seconds
```

asking for the service he want to find exploit and prints the results to the user and saving it to the directory



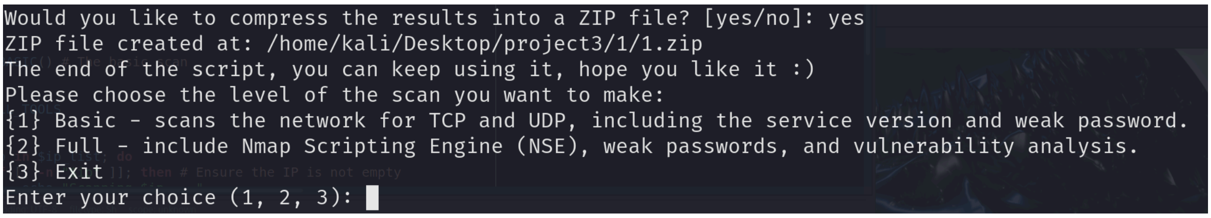
```
do you want to use searchsploit? [yes/no]: no

please enter 'again' if you want to search again for exploits for another service and insert anything else if you don't want:

the results are saved in 1 directory
Would you like to search within the results? [yes/no]: 
```

asking the user again if want to use searchsploit to check for other services if no the user can search within the results for keywords



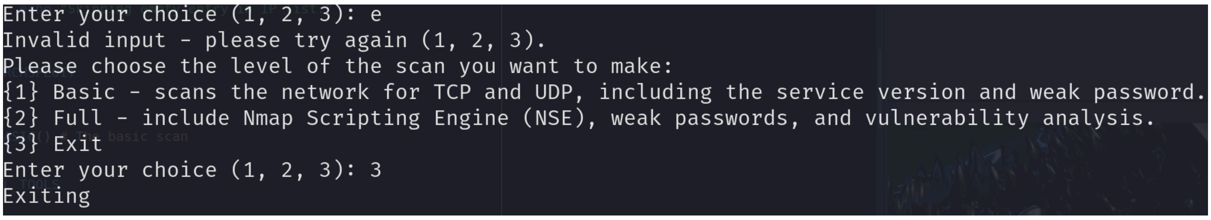
```
the results are saved in 1 directory
Would you like to search within the results? [yes/no]: yes
Enter the keyword(s) to search for: ftp

192.168.203.2_medusa.txt:IMPORTANT: Couldn't load "rdp" [/usr/lib/x86_64-linux-gnu/medusa/modules/rdp.mod: ca
dule in the medusa directory, set the MEDUSA_MODULE_NAME environment variable or run the configure scrNOTICE
192.168.203.2_medusa.txt:NOTICE: ftp.mod: failed to connect, port 21 was not open on 192.168.203.2
192.168.203.2_medusa.txt:NOTICE: ftp.mod: failed to connect, port 21 was not open on 192.168.203.2
192.168.203.2_medusa.txt:NOTICE: ftp.mod: failed to connect, port 21 was not open on 192.168.203.2
192.168.203.2_medusa.txt:NOTICE: ftp.mod: failed to connect, port 21 was not open on 192.168.203.2
192.168.203.2_medusa.txt:NOTICE: ftp.mod: failed to connect, port 21 was not open on 192.168.203.2
192.168.203.2_medusa.txt:NOTICE: ftp.mod: failed to connect, port 21 was not open on 192.168.203.2
192.168.203.2_medusa.txt:NOTICE: ftp.mod: failed to connect, port 21 was not open on 192.168.203.2
192.168.203.2_medusa.txt:NOTICE: ftp.mod: failed to connect, port 21 was not open on 192.168.203.2
192.168.203.2_medusa.txt:NOTICE: ftp.mod: failed to connect, port 21 was not open on 192.168.203.2
192.168.203.128_medusa.txt:NOTICE: ftp.mod: failed to connect, port 21 was not open on 192.168.203.128
192.168.203.128_medusa.txt:NOTICE: ftp.mod: failed to connect, port 21 was not open on 192.168.203.128
192.168.203.128_medusa.txt:NOTICE: ftp.mod: failed to connect, port 21 was not open on 192.168.203.128
192.168.203.128_medusa.txt:NOTICE: ftp.mod: failed to connect, port 21 was not open on 192.168.203.128
192.168.203.128_medusa.txt:NOTICE: ftp.mod: failed to connect, port 21 was not open on 192.168.203.128
192.168.203.128_medusa.txt:NOTICE: ftp.mod: failed to connect, port 21 was not open on 192.168.203.128
192.168.203.128_medusa.txt:NOTICE: ftp.mod: failed to connect, port 21 was not open on 192.168.203.128
192.168.203.128_medusa.txt:NOTICE: ftp.mod: failed to connect, port 21 was not open on 192.168.203.128
192.168.203.128_medusa.txt:NOTICE: ftp.mod: failed to connect, port 21 was not open on 192.168.203.128
192.168.203.128_medusa.txt:NOTICE: ftp.mod: failed to connect, port 21 was not open on 192.168.203.128
```

searching for keywords within the results using simple text manipulation



```
Would you like to compress the results into a ZIP file? [yes/no]: yes
ZIP file created at: /home/kali/Desktop/project3/1/1.zip
The end of the script, you can keep using it, hope you like it :)
Please choose the level of the scan you want to make:
{1} Basic - scans the network for TCP and UDP, including the service version and weak password.
{2} Full - include Nmap Scripting Engine (NSE), weak passwords, and vulnerability analysis.
{3} Exit
Enter your choice (1, 2, 3): 
```

asking the user if he want to zip the results and where the location is for the file and going back to choose the scan he want to perform or exiting to finish the script



```
Enter your choice (1, 2, 3): e
Invalid input - please try again (1, 2, 3).
Please choose the level of the scan you want to make:
{1} Basic - scans the network for TCP and UDP, including the service version and weak password.
{2} Full - include Nmap Scripting Engine (NSE), weak passwords, and vulnerability analysis.
{3} Exit
Enter your choice (1, 2, 3): 3
Exiting
```

end of the script