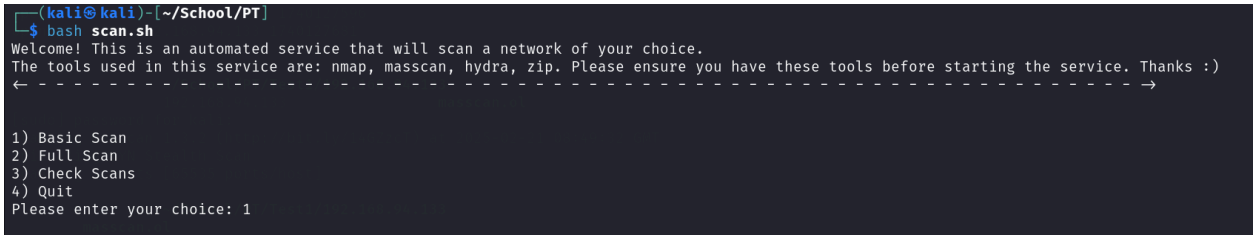
Vulner

Proof of Functionality

The menu shows the options to the user and the first line explains the use of the program.

For the Basic Scan, the program will scan all UDP ports, all TCP ports, show service versions and test weak passwords.

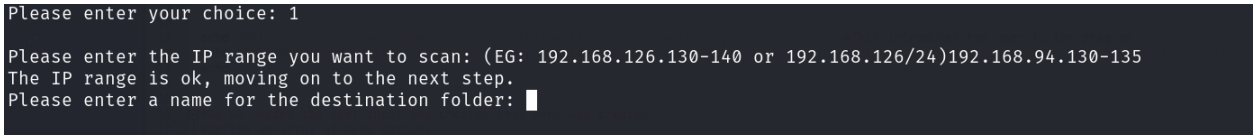
For the Full Scan, the program will do the Basic Scan and vulnerability analysis.



The Basic Scan was done first.

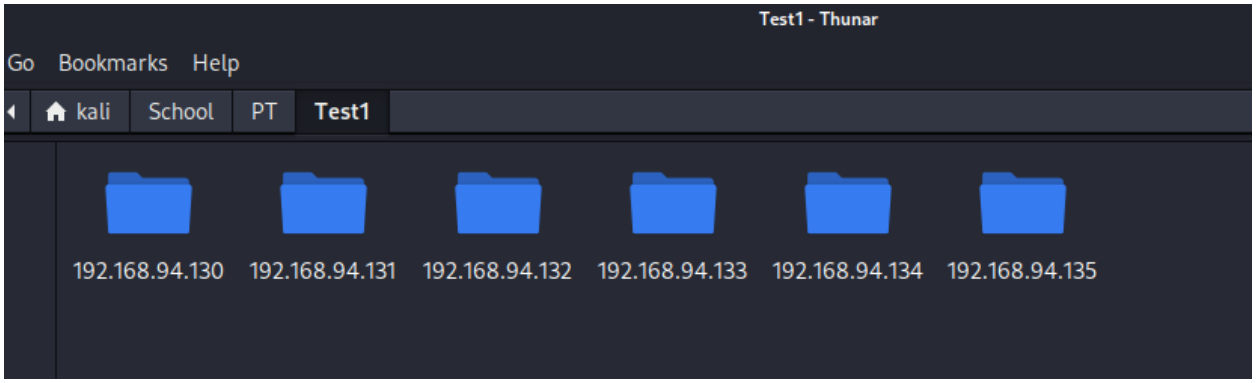
The first step is to ensure the right IP range is entered.

The prompt is given so the user knows both a range and CIDR is accepted. For this example we are using the small range of 192.168.94.130-135.



After the user enters the parent folder name, a folder for each IP address in the range will be created in the parent directory.

```
Please enter a name for the destination folder: Test1
Creating directory with the name Test1
```



If this program needs to be run regularly, the parent folder name can be the date or time.

The program will scan for all TCP and UDP ports of the IP addresses in the range.

TCP scans were done using Nmap.

```
Procceding with basic scan for TCP ports on 192.168.94.130 starting with Nmap.
[+] Nmap scan is done. Results are saved as nmapbasicscan.on in the folder 192.168.94.130.
Procceding with basic scan for UDP ports on 192.168.94.130 with Masscan.
[+] Masscan is done. Results are saved as masscan.og in the folder 192.168.94.130.
Procceding with basic scan for TCP ports on 192.168.94.131 starting with Nmap.
[+] Nmap scan is done. Results are saved as nmapbasicscan.on in the folder 192.168.94.131.
Procceding with basic scan for UDP ports on 192.168.94.131 with Masscan.
[+] Masscan is done. Results are saved as masscan.og in the folder 192.168.94.131.
Procceding with basic scan for TCP ports on 192.168.94.132 starting with Nmap.
[+] Nmap scan is done. Results are saved as nmapbasicscan.on in the folder 192.168.94.132.
Procceding with basic scan for UDP ports on 192.168.94.132 with Masscan.
[+] Masscan is done. Results are saved as masscan.og in the folder 192.168.94.132.
Procceding with basic scan for TCP ports on 192.168.94.133 starting with Nmap.
```

The screenshot below shows the results of the Nmap scan done.

~/School/PT/Test1/192.168.94.133/nmapbasicscan.on - Mousepad

File Edit Search View Document Help

```
# Nmap 7.94SVN scan initiated Fri Feb 21 02:36:30 2025 as: /usr/lib/nmap/nmap --privileged -p- -sV --script=brute --open -oN nmapbasicscan.on 192.168.94.133
Nmap scan report for 192.168.94.133 (192.168.94.133)
Host is up (0.0047s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
| ftp-brute:
|   Accounts: No valid accounts found
|   Statistics: Performed 0 guesses in 1 seconds, average tps: 0.0
|_  ERROR: The service seems to have failed or is heavily firewalled...
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-brute:
|   Accounts: No valid accounts found
|   Statistics: Performed 0 guesses in 1 seconds, average tps: 0.0
|_  ERROR: The service seems to have failed or is heavily firewalled...
23/tcp    open  telnet      Linux telnetd
|_vtam-enum: Not VTAM or 'logon applid' command not accepted. Try with script arg 'vtam-enum.macros=true'
|_tso-enum: ERROR: Script execution failed (use -d to debug)
| telnet-brute:
|   Accounts: No valid accounts found
|   Statistics: Performed 0 guesses in 1 seconds, average tps: 0.0
|_  ERROR: The service seems to have failed or is heavily firewalled...
25/tcp    open  smtp        Postfix smtpd
53/tcp    open  domain      ISC BIND 9.4.2
80/tcp    open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
| http-brute:
|_  Path "/" does not require authentication
|_citrix-brute-xml: FAILED: No domain specified (use ntdomain argument)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp   open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      41331/tcp   mountd
|   100005  1,2,3      48869/udp   mountd
|   100021  1,3,4      34715/udp   nlockmgr
|   100021  1,3,4      46587/tcp   nlockmgr
|   100024  1          48457/tcp   status
|_  100024  1          59222/udp   status
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec?
| rexec-brute:
|   Accounts: No valid accounts found
```

The scan for open UDP ports was done with Masscan. The screenshot below shows the results of Masscan.

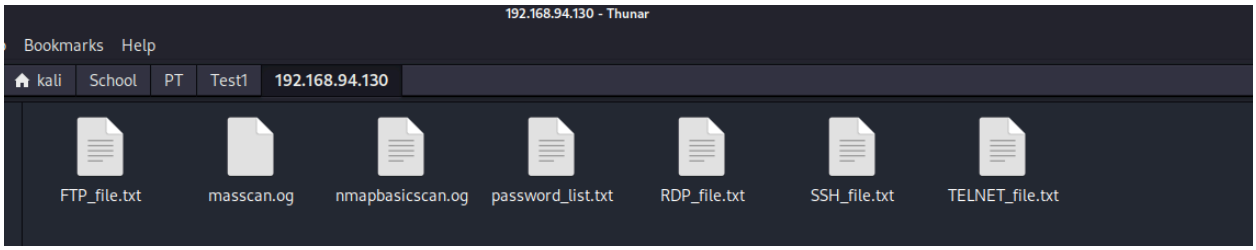
~/School/PT/Test1/192.168.94.133/masscan.ol [Read Only] - Mousepad

File Edit Search View Document Help

```
#masscan
open udp 137 192.168.94.133 1740127790
open udp 53 192.168.94.133 1740128071
# end
```

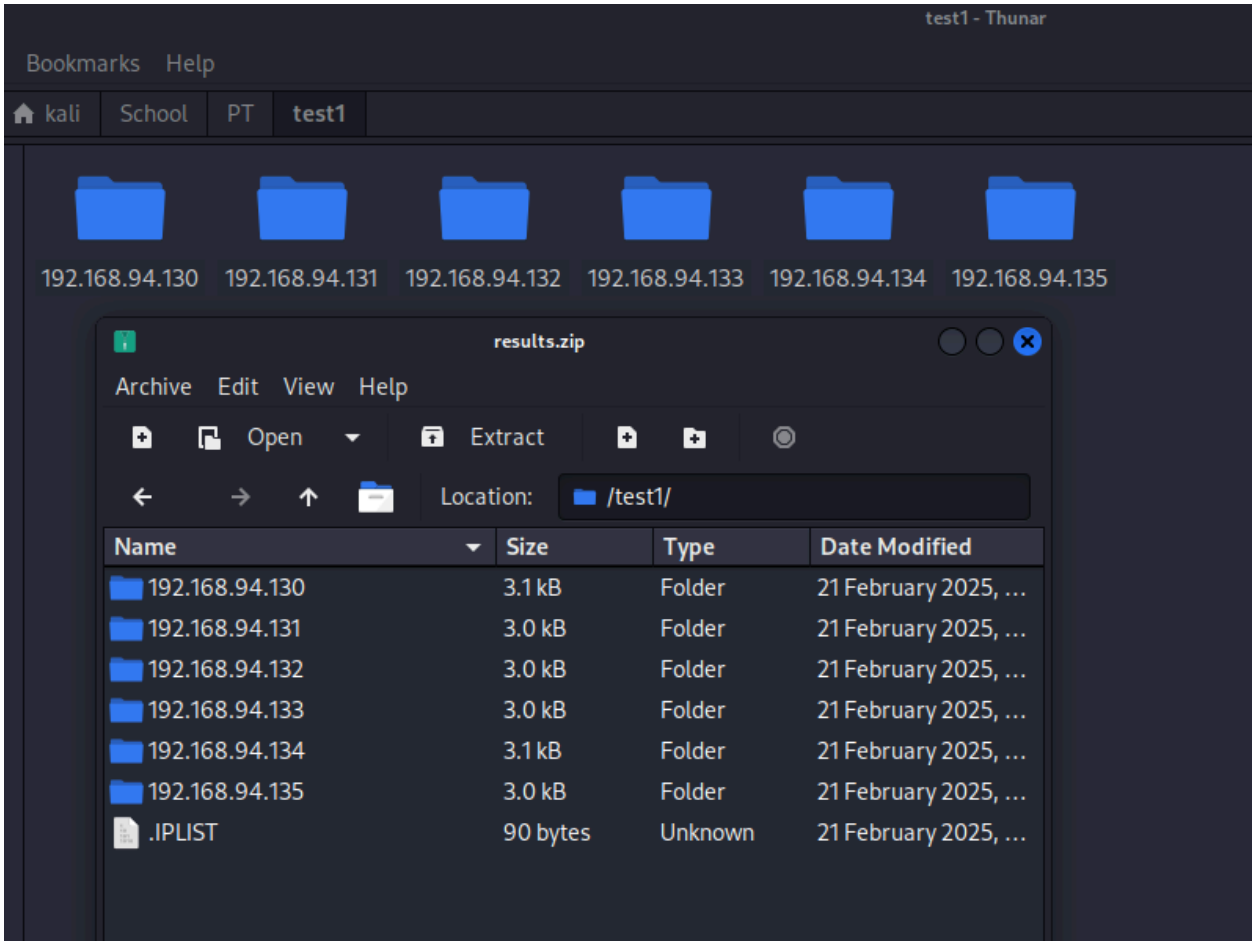
Next step is to test for weak credentials.

```
1) Use default list
2) Use my own list
3) Quit

[?] Now proceeding to test for weak credentials. Please enter your choice: 1
Default password list from SecList will be used.
Proceeding to test weak passwords via SSH,RDP,FTP and TELNET with Hydra.
Now testing 192.168.94.130 ... this may take some time. Please take a well deserved break. Thanks for your patience. :)
[+] Bruteforcing done for 192.168.94.130! Results are saved in the folder 192.168.94.130.
Now testing 192.168.94.131 ... this may take some time. Please take a well deserved break. Thanks for your patience. :)
```



The last step is to save into a zip file.

```
[?] Would you like to save the scans into a zip file ?(y/n)y
[+] All results will be saved in a zip file called results.zip

Thanks for using this service!
```



For the Full Scan, the process is the same but more information will be saved.

```
Procceding with full scan for TCP ports on 192.168.94.130 starting with Nmap.
[+] Nmap scan is done. Results are saved as nmapfullscan.on and vulners.on in the folder 192.168.94.130.
Searchsploit will be used to check for potential exploits and saved into exploits.txt in the folder 192.168.94.130
Procceding with full scan for UDP ports on 192.168.94.130 with Masscan.
[+] Masscan is done. Results are saved as masscan.og in the folder 192.168.94.130.
Procceding with full scan for TCP ports on 192.168.94.131 starting with Nmap.
[+] Nmap scan is done. Results are saved as nmapfullscan.on and vulners.on in the folder 192.168.94.131.
Searchsploit will be used to check for potential exploits and saved into exploits.txt in the folder 192.168.94.131
Procceding with full scan for UDP ports on 192.168.94.131 with Masscan.
[+] Masscan is done. Results are saved as masscan.og in the folder 192.168.94.131.
Procceding with full scan for TCP ports on 192.168.94.132 starting with Nmap.
[+] Nmap scan is done. Results are saved as nmapfullscan.on and vulners.on in the folder 192.168.94.132.
Searchsploit will be used to check for potential exploits and saved into exploits.txt in the folder 192.168.94.132
Procceding with full scan for UDP ports on 192.168.94.132 with Masscan.
```

```
└─$ cat exploits.txt
[i] SearchSploit's XML mode (without verbose enabled).   To enable: searchsploit -v --xml ...
[i] Reading: 'nmapfullscan.xml'

[-] Skipping term: ftp   (Term is too general. Please re-search manually: /usr/bin/searchsploit -t ftp)

[i] /usr/bin/searchsploit -t vsftpd
------------------------------------------------ ---------------------------------
 Exploit Title                                  |  Path
------------------------------------------------ ---------------------------------
vsftpd 2.0.5 - 'CWD' (Authenticated) Remote M | linux/dos/5814.pl
vsftpd 2.0.5 - 'deny_file' Option Remote Deni | windows/dos/31818.sh
vsftpd 2.0.5 - 'deny_file' Option Remote Deni | windows/dos/31819.pl
vsftpd 2.3.2 - Denial of Service              | linux/dos/16270.c
vsftpd 2.3.4 - Backdoor Command Execution     | unix/remote/49757.py
vsftpd 2.3.4 - Backdoor Command Execution (Me | unix/remote/17491.rb
vsftpd 3.0.3 - Remote Denial of Service       | multiple/remote/49719.py
------------------------------------------------ ---------------------------------
Shellcodes: No Results
Papers: No Results


[i] /usr/bin/searchsploit -t vsftpd 2.3.4
------------------------------------------------ ---------------------------------
 Exploit Title                                  |  Path
------------------------------------------------ ---------------------------------
vsftpd 2.3.4 - Backdoor Command Execution     | unix/remote/49757.py
vsftpd 2.3.4 - Backdoor Command Execution (Me | unix/remote/17491.rb
------------------------------------------------ ---------------------------------
Shellcodes: No Results
Papers: No Results


[-] Skipping term: ssh   (Term is too general. Please re-search manually: /usr/bin/searchsploit -t ssh)

[i] /usr/bin/searchsploit -t openssh
```

~/School/PT/test1/192.168.94.133/vulners.on - Mousepad

File Edit Search View Document Help

```
# Nmap 7.94SVN scan initiated Fri Feb 21 20:39:30 2025 as: /usr/lib/nmap/nmap --privileged -sV --script vulners.nse -oN vulners.on 192.168.94.133
Nmap scan report for 192.168.94.133 (192.168.94.133)
Host is up (0.0025s latency).
Not shown: 978 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| vulners:
|   vsftpd 2.3.4:
|       PACKETSTORM:162145      10.0    https://vulners.com/packetstorm/PACKETSTORM:162145      *EXPLOIT*
|       EDB-ID:49757    9.8     https://vulners.com/exploitdb/EDB-ID:49757      *EXPLOIT*
|       CVE-2011-2523   9.8     https://vulners.com/cve/CVE-2011-2523
|_      1337DAY-ID-36095        9.8     https://vulners.com/zdt/1337DAY-ID-36095        *EXPLOIT*
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:4.7p1:
|       2C119FFA-ECE0-5E14-A4A4-354A2C38071A    10.0    https://vulners.com/githubexploit/2C119FFA-ECE0-5E14-A4A4-354A2C38071A  *EXPLOIT*
|       CVE-2023-38408  9.8     https://vulners.com/cve/CVE-2023-38408
|       CVE-2016-1908   9.8     https://vulners.com/cve/CVE-2016-1908
|       B8190CDB-3EB9-5631-9828-8064A1575B23    9.8     https://vulners.com/githubexploit/B8190CDB-3EB9-5631-9828-8064A1575B23  *EXPLOIT*
|       8FC9C5AB-3968-5F3C-825E-E8DB5379A623    9.8     https://vulners.com/githubexploit/8FC9C5AB-3968-5F3C-825E-E8DB5379A623  *EXPLOIT*
|       8AD01159-548E-546E-AA87-2DE89F3927EC    9.8     https://vulners.com/githubexploit/8AD01159-548E-546E-AA87-2DE89F3927EC  *EXPLOIT*
|       887EB570-27D3-11EE-ADBA-C80AA9043978    9.8     https://vulners.com/freebsd/887EB570-27D3-11EE-ADBA-C80AA9043978
|       5E6968B4-DBD6-57FA-BF6E-D9B2219DB27A    9.8     https://vulners.com/githubexploit/5E6968B4-DBD6-57FA-BF6E-D9B2219DB27A  *EXPLOIT*
|       33D623F7-98E0-5F75-80FA-81AA666D1340    9.8     https://vulners.com/githubexploit/33D623F7-98E0-5F75-80FA-81AA666D1340  *EXPLOIT*
|       0221525F-07F5-5790-912D-F4B9E2D1B587    9.8     https://vulners.com/githubexploit/0221525F-07F5-5790-912D-F4B9E2D1B587  *EXPLOIT*
|       95499236-C9FE-56A6-9D7D-E943A24B633A    8.6     https://vulners.com/githubexploit/95499236-C9FE-56A6-9D7D-E943A24B633A  *EXPLOIT*
|       CVE-2015-5600   8.5     https://vulners.com/cve/CVE-2015-5600
|       5B74A5BC-348F-11E5-BA05-C80AA9043978    8.5     https://vulners.com/freebsd/5B74A5BC-348F-11E5-BA05-C80AA9043978
|       PACKETSTORM:179290      8.1     https://vulners.com/packetstorm/PACKETSTORM:179290      *EXPLOIT*
|       FB2E9ED1-43D7-585C-A197-0D6628B20134    8.1     https://vulners.com/githubexploit/FB2E9ED1-43D7-585C-A197-0D6628B20134  *EXPLOIT*
|       FA3992CE-9C4C-5350-8134-177126E0BD3F    8.1     https://vulners.com/githubexploit/FA3992CE-9C4C-5350-8134-177126E0BD3F  *EXPLOIT*
|       F8981437-1287-5B69-93F1-657DFB1DCE59    8.1     https://vulners.com/githubexploit/F8981437-1287-5B69-93F1-657DFB1DCE59  *EXPLOIT*
|       F58A5CB2-2174-586F-9CA9-4C47F8F38B5E    8.1     https://vulners.com/githubexploit/F58A5CB2-2174-586F-9CA9-4C47F8F38B5E  *EXPLOIT*
|       F1A00122-3797-11EF-B611-84A93843EB75    8.1     https://vulners.com/freebsd/F1A00122-3797-11EF-B611-84A93843EB75
|       EFD615F0-8F17-5471-AA83-0F491FD497AF    8.1     https://vulners.com/githubexploit/EFD615F0-8F17-5471-AA83-0F491FD497AF  *EXPLOIT*
|       EC20B9C2-6857-5848-848A-A9F430D13EEB    8.1     https://vulners.com/githubexploit/EC20B9C2-6857-5848-848A-A9F430D13EEB  *EXPLOIT*
|       EB13CBD6-BC93-5F14-A210-AC0B5A1D8572    8.1     https://vulners.com/githubexploit/EB13CBD6-BC93-5F14-A210-AC0B5A1D8572  *EXPLOIT*
|       E660E1AF-7A87-57E2-AEEF-CA14E1FEF7CD    8.1     https://vulners.com/githubexploit/E660E1AF-7A87-57E2-AEEF-CA14E1FEF7CD  *EXPLOIT*
|       E543E274-C20A-582A-8F8E-F8E3F381C345    8.1     https://vulners.com/githubexploit/E543E274-C20A-582A-8F8E-F8E3F381C345  *EXPLOIT*
|       E34FCCEC-226E-5A46-9B1C-BCD6EF7D3257    8.1     https://vulners.com/githubexploit/E34FCCEC-226E-5A46-9B1C-BCD6EF7D3257  *EXPLOIT*
|       E24EEC0A-40F7-5BBC-9E4D-7B13522FF915    8.1     https://vulners.com/githubexploit/E24EEC0A-40F7-5BBC-9E4D-7B13522FF915  *EXPLOIT*
|       DC798E98-BA77-5F86-9C16-0CF8CD540EBB    8.1     https://vulners.com/githubexploit/DC798E98-BA77-5F86-9C16-0CF8CD540EBB  *EXPLOIT*
|       DC473885-F54C-5F76-BAFD-0175E4A90C1D    8.1     https://vulners.com/githubexploit/DC473885-F54C-5F76-BAFD-0175E4A90C1D  *EXPLOIT*
|       D85F08E9-DB96-55E9-8DD2-22F01980F360    8.1     https://vulners.com/githubexploit/D85F08E9-DB96-55E9-8DD2-22F01980F360  *EXPLOIT*
|       D572250A-BE94-501D-90C4-14A6C9C0AC47    8.1     https://vulners.com/githubexploit/D572250A-BE94-501D-90C4-14A6C9C0AC47  *EXPLOIT*
|       D1E049F1-393E-552D-80D1-675022B26911    8.1     https://vulners.com/githubexploit/D1E049F1-393E-552D-80D1-675022B26911  *EXPLOIT*
|       CFEBF7AF-651A-5302-80B8-F8146D5B33A6    8.1     https://vulners.com/githubexploit/CFEBF7AF-651A-5302-80B8-F8146D5B33A6  *EXPLOIT*
```

The user can also use their own password list.

```
1) Use default list
2) Use my own list
3) Quit

[?] Now proceeding to test for weak credentials. Please enter your choice: 2
[?] Please enter full path of the password list file of your choice: /home/kali/Desktop/100.txt
Your password list will be used.
Proceeding to test weak passwords via SSH,RDP,FTP and TELNET.
```

There is also an option to search for the past scans.

```
┌──(kali㉿kali)-[~/School/PT]
└─$ bash scan.sh
Welcome! This is an automated service that will scan a network of your choice.
The tools used in this service are: Nmap, Masscan, Hydra, Zip and Searchsploit. Please ensure you have these tools before starting the service. Thanks :)
← - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - →

1) Basic Scan
2) Full Scan
3) Check Scans
4) Quit

[?] What would you like to do? Please enter your choice: 3
[?] Please provide the name of the folder: test1
./Test1

[?] What would you like to do? Please enter your choice: 
```