

Opening with a prompt for the user to choose from.

giving him an option to scan the wide network range and then showing him the Number of Hosts found UP, after that the script runs a vulnerability scan on them and displaying on which IP addresses were found - OS, open ports and vulnerabilities.

and also saving all results in the Scanner directory that was made in the start of the script automatically.

```
$ sudo bash vulners.sh
VULNERS
1) Start Scan
2) Create Lists
3) Run All
4) Display Statistics
5) Save Report
6) Search IP
7) Quit
Select an action: 1
[+] Local IP address: 192.168.86.129
[+] Net range: 192.168.86.0/24
[+] Scanning the LAN...
[+] Total hosts (UP): 5
Host: 192.168.86.1 Status: Up
Host: 192.168.86.2 Status: Up
Host: 192.168.86.214 Status: Up
Host: 192.168.86.254 Status: Up
Host: 192.168.86.129 Status: Up
[+] Found open ports for 192.168.86.1: ()
()
OS found
[+] Found open ports for 192.168.86.2: ()
()
[-] Couldn't recognize the OS being used by the device.
[+] Found open ports for 192.168.86.214: ()
()
[-] Couldn't recognize the OS being used by the device.
[+] Found open ports for 192.168.86.254: ()
()
[-] Couldn't recognize the OS being used by the device.
[+] Found open ports for 192.168.86.129: ()
()
[-] Couldn't recognize the OS being used by the device.

[+] Looking for possible vulnerabilities:
[-] No vulnerabilities were found for 192.168.86.1.

[!] Vulnerabilities were found for 192.168.86.2. File saved - /home/kali/Scanner/192.168.86.129/Vulns_192.168.86.2.txt.
[!] Vulnerabilities were found for 192.168.86.214. File saved - /home/kali/Scanner/192.168.86.129/Vulns_192.168.86.214.txt.
[-] No vulnerabilities were found for 192.168.86.254.
```

In the next option the user is given the option to create his own list of usernames and passwords or use a list of his own that is located in the path the user provides so that the Medusa tool can use it.

```

VULNERABILITIES=$(cat $HOME/Scanner/$LOCAL_IP/Scan.txt | grep Up | sed 's/(/ /g; s/)/ /g' | wc -l)

function Lists() {
125
126
127
128
129     echo "Do you want to create your own passlist? (y/n)"
130     read answer
131     if [ "$answer" = "n" ]; then
132         BRUTEFORCE
133     elif [ "$answer" = "y" ]; then
134         echo "Enter passwords one by one and press Enter. Type 'done' when finished."
135         touch $HOME/Scanner/$LOCAL_IP/passlist.txt
136         while true; do
137             read password
138             if [ "$password" = "done" ]; then
139                 echo "The password list was saved in - $HOME/Scanner/$LOCAL_IP/passlist.txt"
140                 break
141             else
142                 echo "$password" >> $HOME/Scanner/$LOCAL_IP/passlist.txt
143             fi
144         done
145     fi
146 }

1) Start Scan
2) Create Lists
3) Run All
4) Run medusa
5) Display Statistics
6) Save Report
7) Search IP
8) Quit
Select an action: 2
Do you want to create your own passlist? (y/n)
y
Enter passwords one by one and press Enter. Type 'done' when finished.
lala
s1s1s
lalalalaa
done
The password list was saved in - /home/kali/Scanner/192.168.86.129/passlist.txt
Provide full path to a username list:/home/kali/Scanner/192.168.86.129/passlist.txt
Provide full path to password list:/home/kali/Scanner/192.168.86.129/passlist.txt
Choose IP to bruteforce192.168.86.214
Choose service to bruteforce
Available options: ssh, http, ftp , telnet
ftp
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [ftp] Host: 192.168.86.214 (1 of 1, 0 complete) User: a (1 of 16, 0 complete) Password: a (1 of 19 complete)
ACCOUNT CHECK: [ftp] Host: 192.168.86.214 (1 of 1, 0 complete) User: a (1 of 16, 0 complete) Password: a (2 of 19 complete)
ACCOUNT CHECK: [ftp] Host: 192.168.86.214 (1 of 1, 0 complete) User: a (1 of 16, 0 complete) Password: a (3 of 19 complete)
ACCOUNT CHECK: [ftp] Host: 192.168.86.214 (1 of 1, 0 complete) User: a (1 of 16, 0 complete) Password: s (4 of 19 complete)
ACCOUNT CHECK: [ftp] Host: 192.168.86.214 (1 of 1, 0 complete) User: a (1 of 16, 0 complete) Password: msfadmin (5 of 19 complete)
ACCOUNT CHECK: [ftp] Host: 192.168.86.214 (1 of 1, 0 complete) User: a (1 of 16, 0 complete) Password: user (6 of 19 complete)
ACCOUNT CHECK: [ftp] Host: 192.168.86.214 (1 of 1, 0 complete) User: a (1 of 16, 0 complete) Password: admin (7 of 19 complete)
ACCOUNT CHECK: [ftp] Host: 192.168.86.214 (1 of 1, 0 complete) User: a (1 of 16, 0 complete) Password: kali (8 of 19 complete)
ACCOUNT CHECK: [ftp] Host: 192.168.86.214 (1 of 1, 0 complete) User: a (1 of 16, 0 complete) Password: s (9 of 19 complete)
ACCOUNT CHECK: [ftp] Host: 192.168.86.214 (1 of 1, 0 complete) User: a (1 of 16, 0 complete) Password: d (10 of 19 complete)
ACCOUNT CHECK: [ftp] Host: 192.168.86.214 (1 of 1, 0 complete) User: a (1 of 16, 0 complete) Password: asdff (11 of 19 complete)
ACCOUNT CHECK: [ftp] Host: 192.168.86.214 (1 of 1, 0 complete) User: a (1 of 16, 0 complete) Password: okay (12 of 19 complete)
ACCOUNT CHECK: [ftp] Host: 192.168.86.214 (1 of 1, 0 complete) User: a (1 of 16, 0 complete) Password: yolo (13 of 19 complete)
ACCOUNT CHECK: [ftp] Host: 192.168.86.214 (1 of 1, 0 complete) User: a (1 of 16, 0 complete) Password: topa (14 of 19 complete)
ACCOUNT CHECK: [ftp] Host: 192.168.86.214 (1 of 1, 0 complete) User: a (1 of 16, 0 complete) Password: okayyyy (15 of 19 complete)
ACCOUNT CHECK: [ftp] Host: 192.168.86.214 (1 of 1, 0 complete) User: a (1 of 16, 0 complete) Password: pssss (16 of 19 complete)
ACCOUNT CHECK: [ftp] Host: 192.168.86.214 (1 of 1, 0 complete) User: a (1 of 16, 0 complete) Password: lala (17 of 19 complete)

```