Project Name:

CYBER WARFARE ATTACKER

Course:

RTS77381

JOHN BRYCE

Student Name:

Tomer Dahan

Table of Contents:

Contents

Objectives

Project Cyber Warfare - Attacker - an attack tool to run on a remote server 24/7 and have the following capabilities:

1. **Scanning and Enumeration**
   -The code should scan and enumerate random ports and IPs
   -Scanning can be done by Shodan, Masscan, and Nmap (This version only nmap!!).
2. **Brute Force**
   -five login services to brute force (chosen: ssh ftp smb smtp irc).
3. **Exploit Analysis**
   - Run infrastructure exploits analysis using NSE and Banner Grabbing.
4. **Logs and Reports**
   -Logs should be displayed via the webserver.
   -Government IPs should be saved in sensitive.log. (Government IPs sensitive list in this version only for IR - Iran)
5. **General**
   -Prepare the server to be anonymous.
   -The server should be able to scan 24/7 an entire country (countries in this version: IL - Israel and IR - Iran)

Requirements

There are three program modules:

attacker.sh:

• Internet Connection

• Running Linux

• Root privileges user

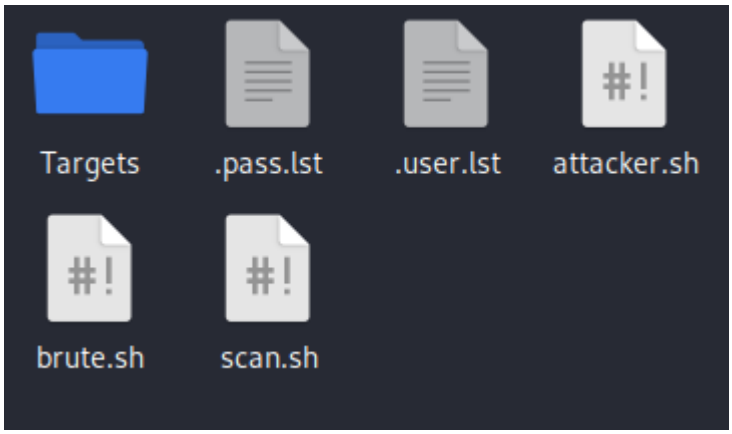
scan.sh:

• Targets folder and files (a target list and a sensitive target list)

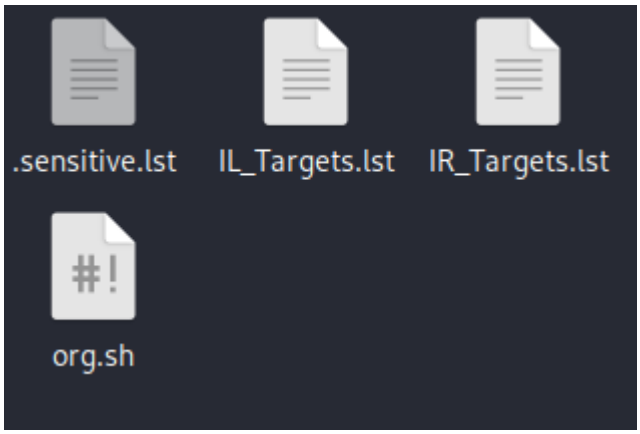
brute.sh:

• Files .user.lst and .pass.lst - lists of common usernames and passwords. User can configure as desired.

Needed files in running folder:



In Targets:



Run attacker.sh with root privileges:

```
┌──(kali㉿kali)-[~/Desktop/red/projects/attacker]
└─$ sudo ./attacker.sh
```

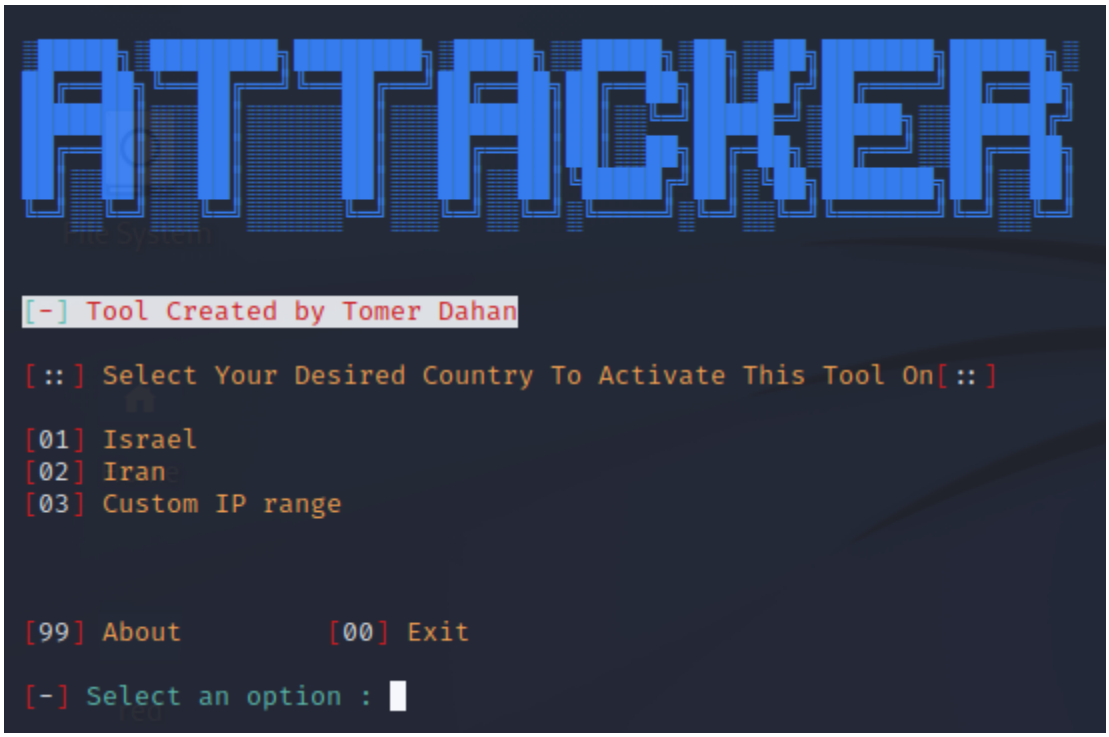
User manual

Description

The user interface is an advanced menu-based command line interface (CLI). After running the main program, the user can simply enter and choose the prompted options and follow the intuitive steps using the displayed menu.
The program is immune to Ctrl+C (exit) from the user, by implementing the controlled trap.
The program creates temporary files to help the implementation of the various commands.
On program exit, all temporary created files are deleted from system.

User Interface

Main menu:



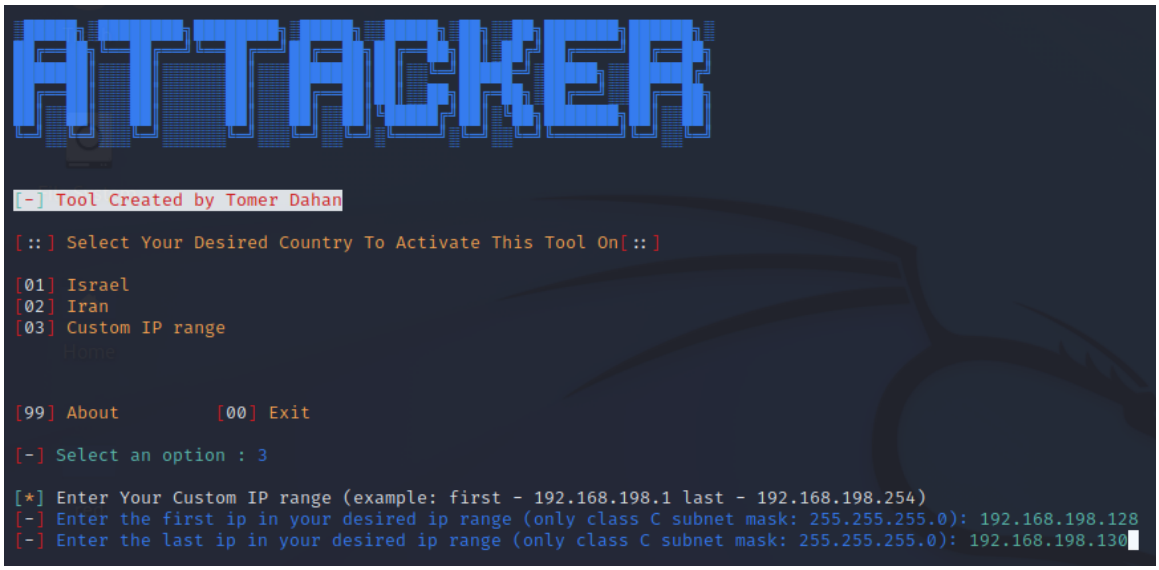
! Warning ! - When choosing either countries, the program will run for a long period of time seeing that their IP list are long and contain up to 350,000 IP targets.

It is recommended to use and enter a custom IP list.

Workflow example

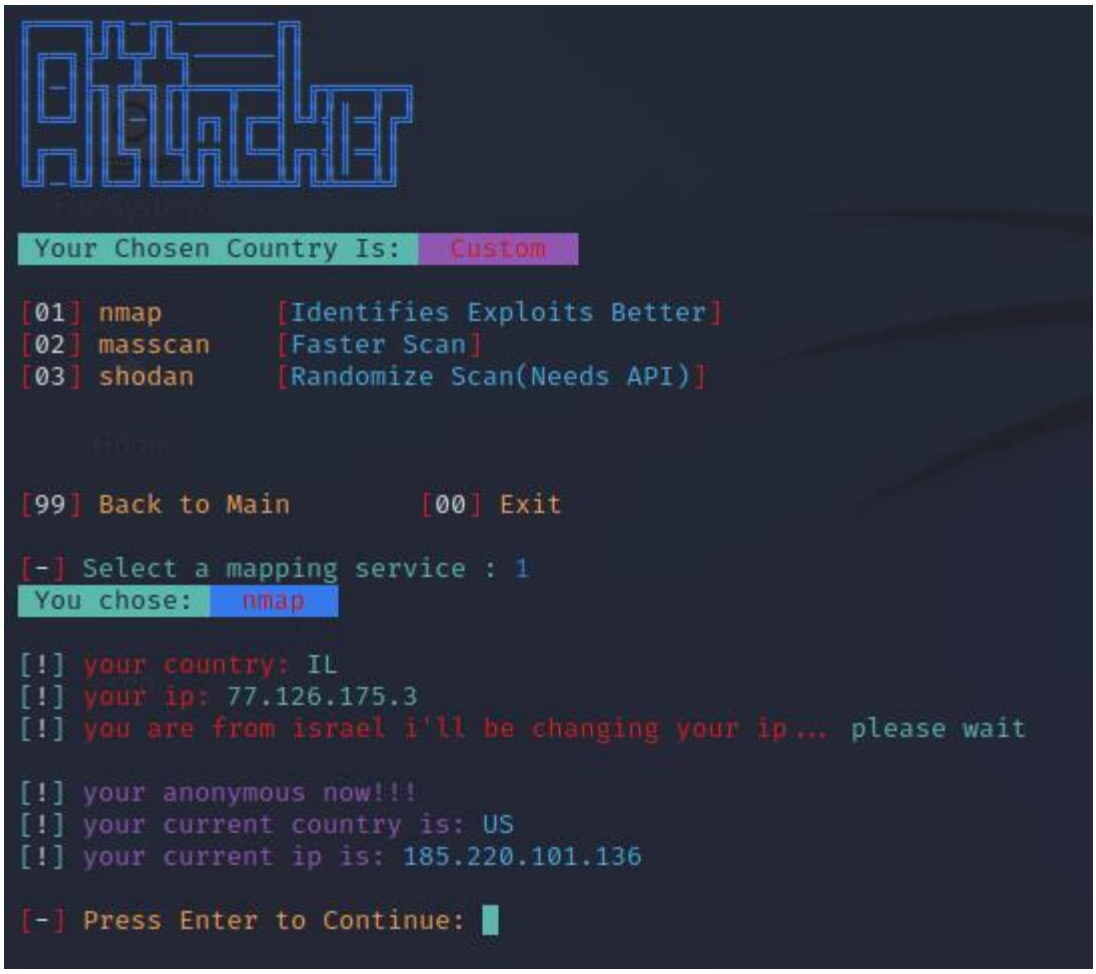
This example uses the custom IP range as recommended above:

Enter Your desired IP range (in this example 192.168.198.128-192.168.198.130):

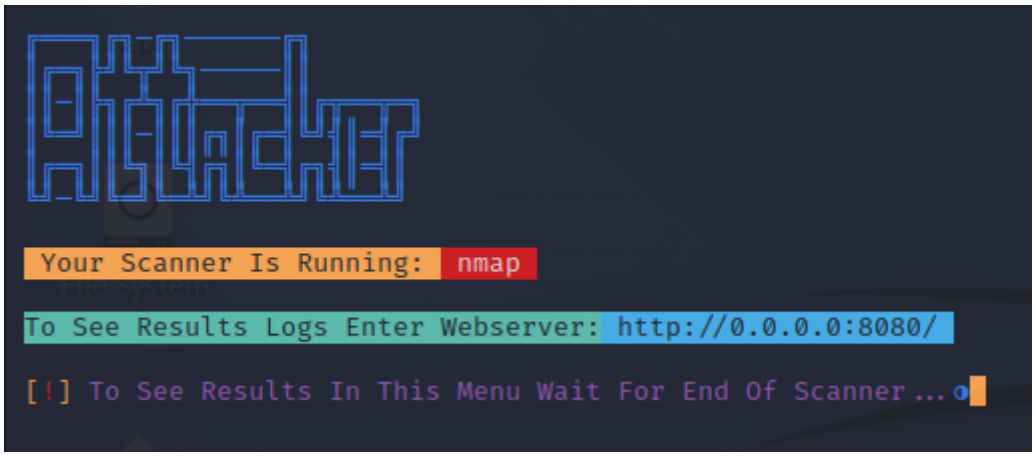


Next, select a scanner (in this version only Nmap is configured):

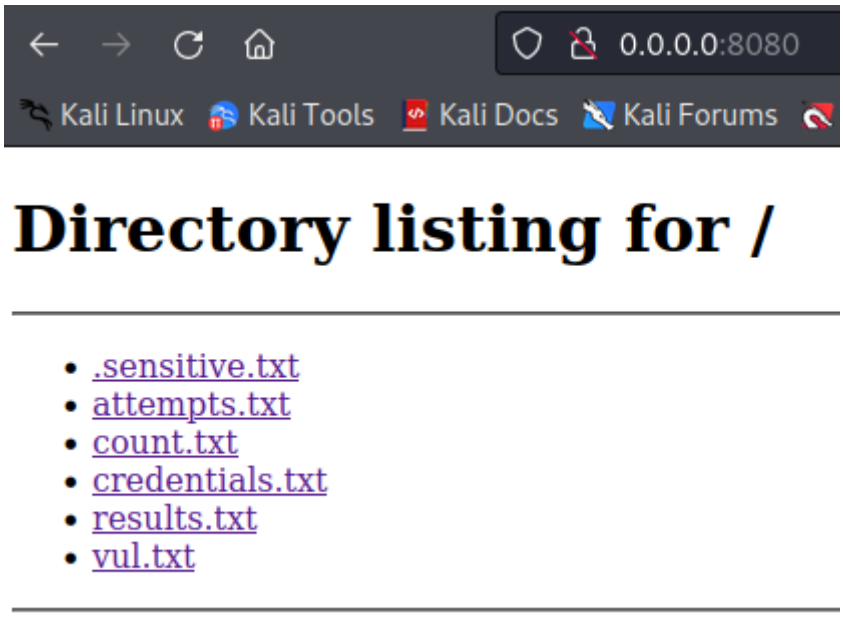
Next, the server prepares to be anonymous. Wait till finished and press Enter.

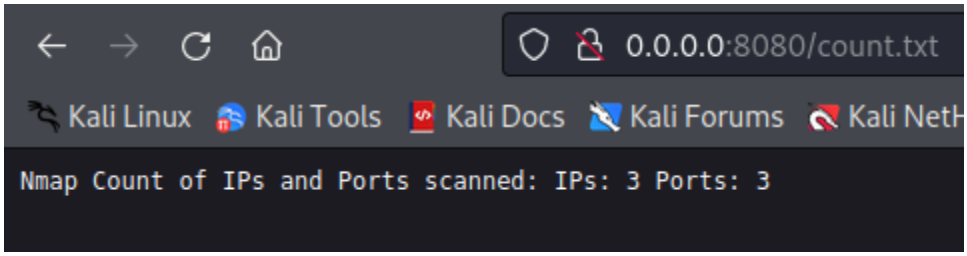


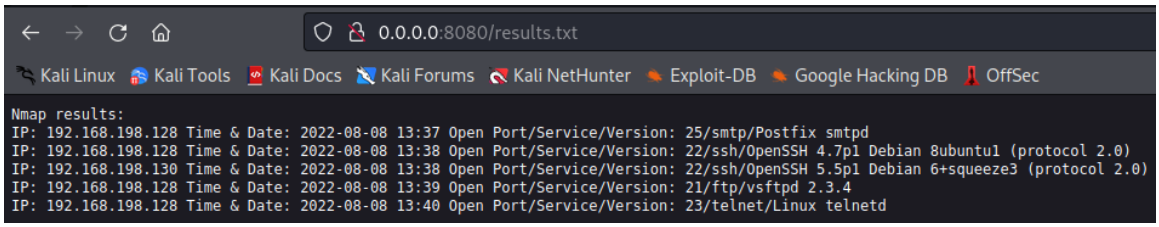
Now, the server started scanning and brute forcing. To see progress and results enter to Webserver as shown in the loading menu.

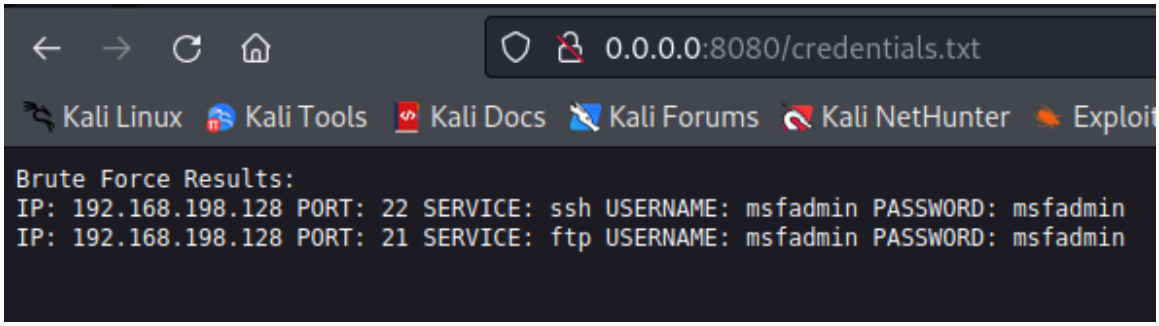


Here are examples of program self-generated results displayed in the webserver.









When the server ends scanning and brute forcing all of the IP range, the program will display in terminal the result menu. The result menu and the webserver in this stage are similar.

```
Attacker

Your Scanner Finished: nmap

To See Results Logs Enter Webserver: http://0.0.0.0:8080/

[01] Number of IPs & Ports
[02] IP Mapping
[03] Sensitive IPs
[04] Choose IP for more information
[05] All Possible Exploits
[06] Brute Force Results
[07] Brute Force Attempts

[99] Back to Main        [00] Exit

[-] Select data to see:
```

Here are examples of seeing results in the result menu.

```
[-] Select data to see: 1

Nmap Count of IPs and Ports scanned: IPs: 3 Ports: 11

[-] Press Enter to return:
```

```
[-] Select data to see: 2

Nmap results:
IP: 192.168.198.128 Time & Date: 2022-08-08 13:37 Open Port/Service/Version: 25/smtp/Postfix smtpd
IP: 192.168.198.128 Time & Date: 2022-08-08 13:38 Open Port/Service/Version: 22/ssh/OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
IP: 192.168.198.130 Time & Date: 2022-08-08 13:38 Open Port/Service/Version: 22/ssh/OpenSSH 5.5p1 Debian 6+squeeze3 (protocol 2.0)
IP: 192.168.198.128 Time & Date: 2022-08-08 13:39 Open Port/Service/Version: 21/ftp/vsftpd 2.3.4
IP: 192.168.198.128 Time & Date: 2022-08-08 13:40 Open Port/Service/Version: 23/telnet/Linux telnetd

[-] Press Enter to return:
```

```
[-] Select data to see: 4

[-] Enter an IP: 192.168.198.128
```

```
[-] Enter an IP: 192.168.198.128

[!] Whois information:

NetRange:       192.168.0.0 - 192.168.255.255
CIDR:           192.168.0.0/16
NetName:        PRIVATE-ADDRESS-CBLK-RFC1918-IANA-RESERVED
NetHandle:      NET-192-168-0-0-1
Parent:         NET192 (NET-192-0-0-0-0)
NetType:        IANA Special Use
OriginAS:
Organization:   Internet Assigned Numbers Authority (IANA)
RegDate:        1994-03-15
Updated:        2013-08-30
Ref:            https://rdap.arin.net/registry/ip/192.168.0.0
OrgName:        Internet Assigned Numbers Authority
OrgId:          IANA
Address:        12025 Waterfront Drive
Address:        Suite 300
City:           Los Angeles
StateProv:      CA
PostalCode:     90292
Country:        US
RegDate:
Updated:        2012-08-31
Ref:            https://rdap.arin.net/registry/entity/IANA
OrgAbuseHandle: IANA-IP-ARIN
OrgAbuseName:   ICANN
OrgAbusePhone:  +1-310-301-5820
OrgAbuseEmail:  abuse@iana.org
OrgAbuseRef:    https://rdap.arin.net/registry/entity/IANA-IP-ARIN
OrgTechHandle:  IANA-IP-ARIN
OrgTechName:    ICANN
OrgTechPhone:   +1-310-301-5820
OrgTechEmail:   abuse@iana.org
OrgTechRef:     https://rdap.arin.net/registry/entity/IANA-IP-ARIN

[!] Ports & Services:

IP: 192.168.198.128 Time & Date: 2022-08-08 13:37 Open Port/Service/Version: 25/smtp/Postfix smtpd
IP: 192.168.198.128 Time & Date: 2022-08-08 13:38 Open Port/Service/Version: 22/ssh/OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
IP: 192.168.198.128 Time & Date: 2022-08-08 13:39 Open Port/Service/Version: 21/ftp/vsftpd 2.3.4
IP: 192.168.198.128 Time & Date: 2022-08-08 13:40 Open Port/Service/Version: 23/telnet/Linux telnetd

[!] Login Services:

IP: 192.168.198.128 PORT: 22 SERVICE: ssh USERNAME: msfadmin PASSWORD: msfadmin
IP: 192.168.198.128 PORT: 21 SERVICE: ftp USERNAME: msfadmin PASSWORD: msfadmin
```

```
[-] Select data to see: 5

vulnerabilities results:
IP: 192.168.198.128 Port: 25 Version: Postfix smtpd  Vulnerabilities:

 Exploit Title                                      |  Path
 ---------------------------------------------------------------------------------------
AA SMTP Server 1.1 - Crash (PoC)                    | windows/dos/14990.txt
Alt-N MDaemon 6.5.1 - IMAP/SMTP Remote Buffer       | windows/remote/473.c
Alt-N MDaemon 6.5.1 SMTP Server - Multiple Co       | windows/remote/24624.c
Alt-N MDaemon Server 2.71 SP1 - SMTP HELO Arg       | windows/dos/23146.c
Apache James Server 2.2 - SMTP Denial of Serv       | multiple/dos/27915.pl
BaSoMail 1.24 - SMTP Server Command Buffer Ov       | windows/dos/22668.txt
BaSoMail Server 1.24 - POP3/SMTP Remote Denia       | windows/dos/594.pl
BL4 SMTP Server < 0.1.5 - Remote Buffer Overf       | windows/dos/1721.pl
Blat 2.7.6 SMTP / NNTP Mailer - Local Buffer        | windows/local/38472.py
BulletProof FTP Server 2019.0.0.50 - 'SMTP Se       | windows/dos/46422.py
Cisco PIX Firewall 4.x/5.x - SMTP Content Fil       | hardware/remote/20231.txt
Citadel SMTP 7.10 - Remote Overflow                 | windows/remote/4949.txt
Cobalt Raq3 PopRelayD - Arbitrary SMTP Relay        | linux/remote/20994.txt
```

```
[-] Select data to see: 6


Brute Force Results:
IP: 192.168.198.128 PORT: 22 SERVICE: ssh USERNAME: msfadmin PASSWORD: msfadmin
IP: 192.168.198.128 PORT: 21 SERVICE: ftp USERNAME: msfadmin PASSWORD: msfadmin


[-] Press Enter to return:
```

```
[-] Select data to see: 7


Brute Force Attempts:
ATTEMPTS ON: IP: 192.168.198.128 PORT: 25 SERVICE: smtp
[ATTEMPT] target 192.168.198.128 - login "Admin" - pass "Admin" - 1 of 154 [child 0] (0/0)
[ATTEMPT] target 192.168.198.128 - login "Admin" - pass "" - 2 of 154 [child 1] (0/0)
[ATTEMPT] target 192.168.198.128 - login "Admin" - pass "nimdA" - 3 of 154 [child 2] (0/0)
[ATTEMPT] target 192.168.198.128 - login "Admin" - pass "p@ssword" - 4 of 154 [child 3] (0/0)
[ATTEMPT] target 192.168.198.128 - login "Admin" - pass "Passw0rd!" - 5 of 154 [child 4] (0/0)
[ATTEMPT] target 192.168.198.128 - login "Admin" - pass "toor" - 6 of 154 [child 5] (0/0)
[ATTEMPT] target 192.168.198.128 - login "Admin" - pass "password" - 7 of 154 [child 6] (0/0)
[ATTEMPT] target 192.168.198.128 - login "Admin" - pass "admin" - 8 of 154 [child 7] (0/0)
[ATTEMPT] target 192.168.198.128 - login "Admin" - pass "administrator" - 9 of 154 [child 0] (0/0)
[ATTEMPT] target 192.168.198.128 - login "Admin" - pass "st@rt123" - 10 of 154 [child 1] (0/0)
[ATTEMPT] target 192.168.198.128 - login "Admin" - pass "123456" - 11 of 154 [child 2] (0/0)
[ATTEMPT] target 192.168.198.128 - login "Admin" - pass "1234567890" - 12 of 154 [child 3] (0/0)
[ATTEMPT] target 192.168.198.128 - login "Admin" - pass "123456aA" - 13 of 154 [child 5] (0/0)
[ATTEMPT] target 192.168.198.128 - login "Admin" - pass "msfadmin" - 14 of 154 [child 6] (0/0)
[ATTEMPT] target 192.168.198.128 - login "admin" - pass "admin" - 15 of 154 [child 4] (0/0)
[ATTEMPT] target 192.168.198.128 - login "admin" - pass "" - 16 of 154 [child 7] (0/0)
[ATTEMPT] target 192.168.198.128 - login "admin" - pass "nimda" - 17 of 154 [child 0] (0/0)
```

About menu

```
ATTACKER

[-] Tool Created by Tomer Dahan

Authors  :  TOMER DAHAN
Github   :  https://github.com/tomer333/
Social   :  https:https://www.linkedin.com/in/tomer-dahan-375540235/
Version  :  1.0

 Thanks To: TAHMID RAYAT creater of zphisher

Warning:
This Tool is made for educational purpose only !
Authors will not be responsible for any misuse of this toolkit !

[00] Main Menu     [99] Exit

[-] Select an option :
```

Programmer manual

attacker.sh

- Main code, contains the Menu.

Global variables:

- ANSI colors – font and background colors

```
## ANSI colors (FG & BG)
RED="$(printf '\033[31m')"  GREEN="$(printf '\033[32m')"  ORANGE="$(printf '\033[33m')"  BLUE="$(printf '\033[34m')"
MAGENTA="$(printf '\033[35m')"  CYAN="$(printf '\033[36m')"  WHITE="$(printf '\033[37m')" BLACK="$(printf '\033[30m')"
REDBG="$(printf '\033[41m')"  GREENBG="$(printf '\033[42m')"  ORANGEBG="$(printf '\033[43m')"  BLUEBG="$(printf '\033[44m')"
MAGENTABG="$(printf '\033[45m')"  CYANBG="$(printf '\033[46m')"  WHITEBG="$(printf '\033[47m')" BLACKBG="$(printf '\033[40m')"
RESETBG="$(printf '\e[0m\n')"
```

- Country/Scanner_Type – Sets default – user can configure

```
#Global vars
Country='IL'
Scanner_Type='nmap'
```

- Immune to ctrl+c – trap command

```
##immune to ctrl+c
trap '' INT
```

- Creating startup directories

```
#create necessary directories
#logs for viewing logs in terminal with ANSI colors
#txt for viewing logs in webserver
mkdir ./logs
mkdir ./logs/txt
```

Start of Program:

```
##start of program
main menu
```

Functions (attacker.sh):

Function Name	Description
reset_color()	Reset terminal colors
icon()	the script name icon and creater
icon_small()	Small icon
check_if_ip_addr()	checks if input of ip is valid $1 as ip that is being checked
ip_information()	The user should be able to choose an IP address from the found data, and the server should display: Whois Information, Ports and Services and Login Services. $1 as ip that user entered
install_nipe()	Installation of nipe
print_country_after_nipe()	print your current ip origin country
change_ip()	start Nipe
check_ano_change()	checks if current ip is IL if true changes ip
stop_nipe()	Stops nipe
remove_trash()	removes all trash files and directories at end of program
kill_procs()	kills all thread processes at end of program
msg_exit()	Exit message
update_files()	updates all files that are displayed via webserver as long as scan.sh is running
web_setup()	start webserver on directory ./log/txt
waiting()	Waits for scan.sh to finish while printing on screen loading spinner
start_scanner()	Firsts checks if ip is anonymous Initializes files ./logs/credentials.log and ./logs/attempts.log for brute force logs (brute.sh) Runs scan.sh as a thread and captures the thread pid
custom_ip_list()	Creates custom ip list for user using the script - ./Targets/org.sh User requires to enter first and last ip in desired ip range
result_menu()	Result selection menu
tunnel_menu()	Tunnel selection
main_menu()	main menu
about()	About menu

scan.sh

- A thread program for attacker.sh
- Mapping ports, services, versions and versions vulnerabilities of the ip.

Global variables:

- ANSI colors – font and background colors

```
## ANSI colors (FG & BG)
RED="$(printf '\033[31m')"  GREEN="$(printf '\033[32m')"  ORANGE="$(printf '\033[33m')"  BLUE="$(printf '\033[34m')"
MAGENTA="$(printf '\033[35m')"  CYAN="$(printf '\033[36m')"  WHITE="$(printf '\033[37m')" BLACK="$(printf '\033[30m')"
REDBG="$(printf '\033[41m')"  GREENBG="$(printf '\033[42m')"  ORANGEBG="$(printf '\033[43m')"  BLUEBG="$(printf '\033[44m')"
MAGENTABG="$(printf '\033[45m')"  CYANBG="$(printf '\033[46m')"  WHITEBG="$(printf '\033[47m')" BLACKBG="$(printf '\033[40m')"
RESETBG="$(printf '\e[0m\n')"
```

- $1 target list entered from attacker.sh
- Port range currently short and contains only brute forced ports for fast running. User can configure, as commented in code, for all ports.

```
#Global vars
targetList=$1
sensitiveList="./Targets/.sensitive.lst"
startPort=20 #1
endPort=25 #65535
ip_count=0
port_count=0
```

- Initializing log files that will be displayed in result menu.

```
#initializes files for logs
echo "${BLUE}Nmap results:" > ./logs/results.log
echo "${BLUE}vulnerabilities results:" > ./logs/vul.log
echo "${BLUE}Sensitive IPs log:" > ./logs/.sensitive.log
echo "${WHITE}Nmap Count of IPs and Ports scanned: ${RED}IPs: 0 ${GREEN}Ports: 0" > ./logs/count.log
```

brute.sh

- A program for scan.sh
- Brute forces all targets found with open ports and saves data in to logs.

Global variables:

- ANSI colors – font and background colors

```
## ANSI colors (FG & BG)
RED="$(printf '\033[31m')"  GREEN="$(printf '\033[32m')"  ORANGE="$(printf '\033[33m')"  BLUE="$(printf '\033[34m')"
MAGENTA="$(printf '\033[35m')"  CYAN="$(printf '\033[36m')"  WHITE="$(printf '\033[37m')" BLACK="$(printf '\033[30m')"
REDBG="$(printf '\033[41m')"  GREENBG="$(printf '\033[42m')"  ORANGEBG="$(printf '\033[43m')"  BLUEBG="$(printf '\033[44m')"
MAGENTABG="$(printf '\033[45m')"  CYANBG="$(printf '\033[46m')"  WHITEBG="$(printf '\033[47m')" BLACKBG="$(printf '\033[40m')"
RESETBG="$(printf '\e[0m\n')"
```

- $1 target list entered from attacker.sh
- Services list currently short and contains only ports that were declared in scan.sh for fast running. User can configure, as commented in code, for many more services.

```
services_list="ssh ftp smtp telnet" #smb irc http (and many other can be added)
```

Credits

- TAHMID RAYAT - Creator of zphisher - https://github.com/htr-tech/zphisher