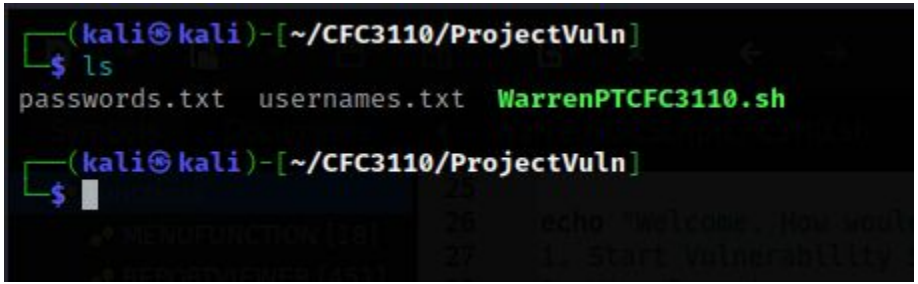
Warren’s PT Project

Goal: To discover devices on the network and then run a scan to find open ports. User can then choose which network and port they would like to scan for vulnerabilities, and if a login service is available, brute force it. The results are then compiled into a report which can be view using the script.

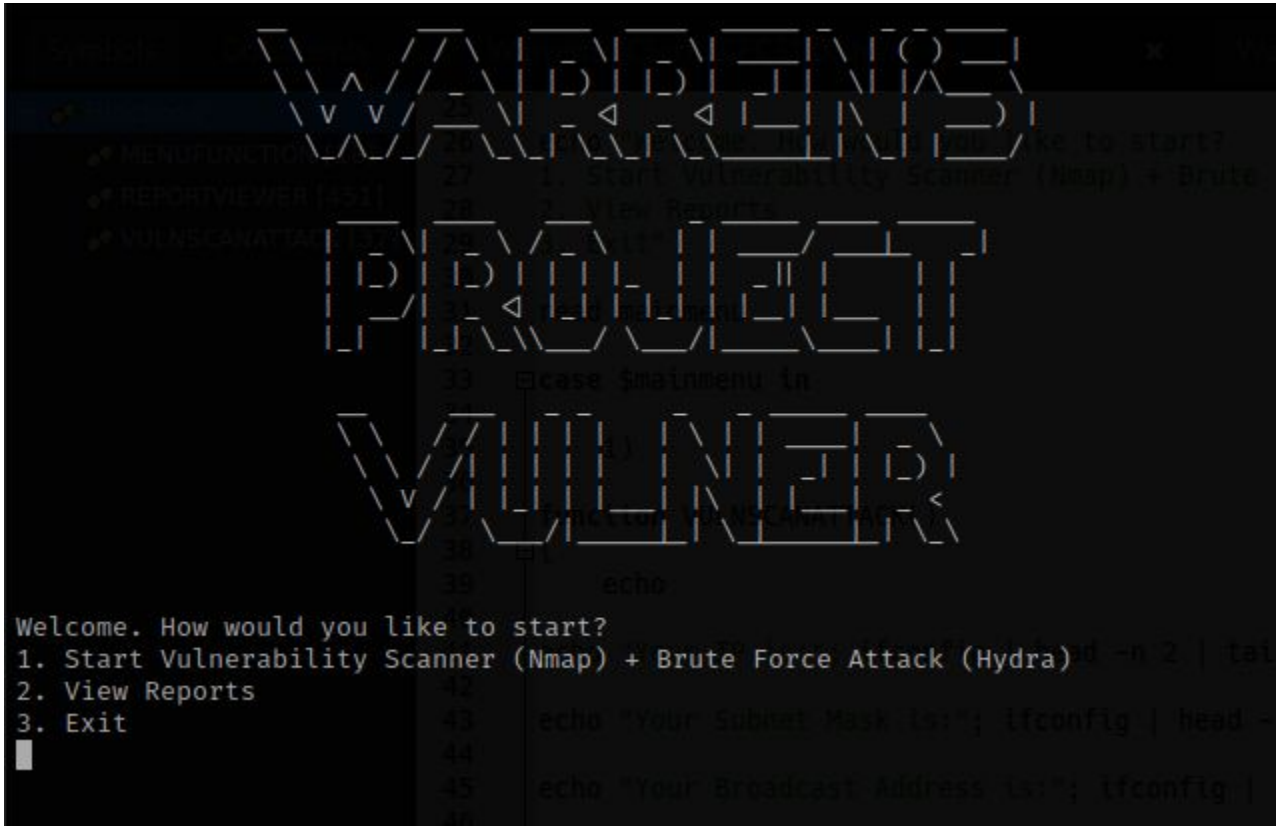
Tools: netmask, nmap, hydra

Created by: Warren Justin Chan

Before starting..



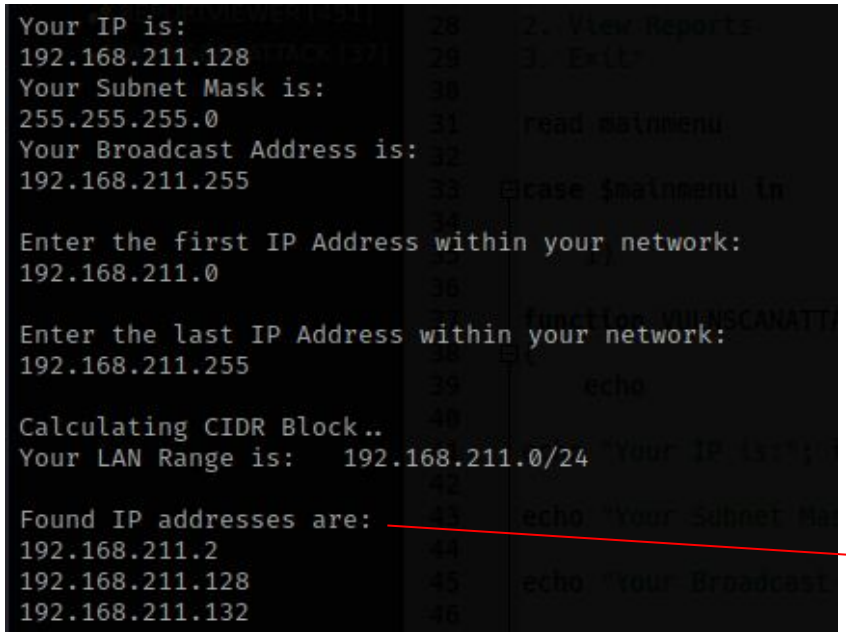
Before we begin, we can see that there are only 3 files in the folder, after we run the script there will be created usernames, passwords, and report files created which will be viewed at the end of this document.



The user is given 3 choices when starting the script.

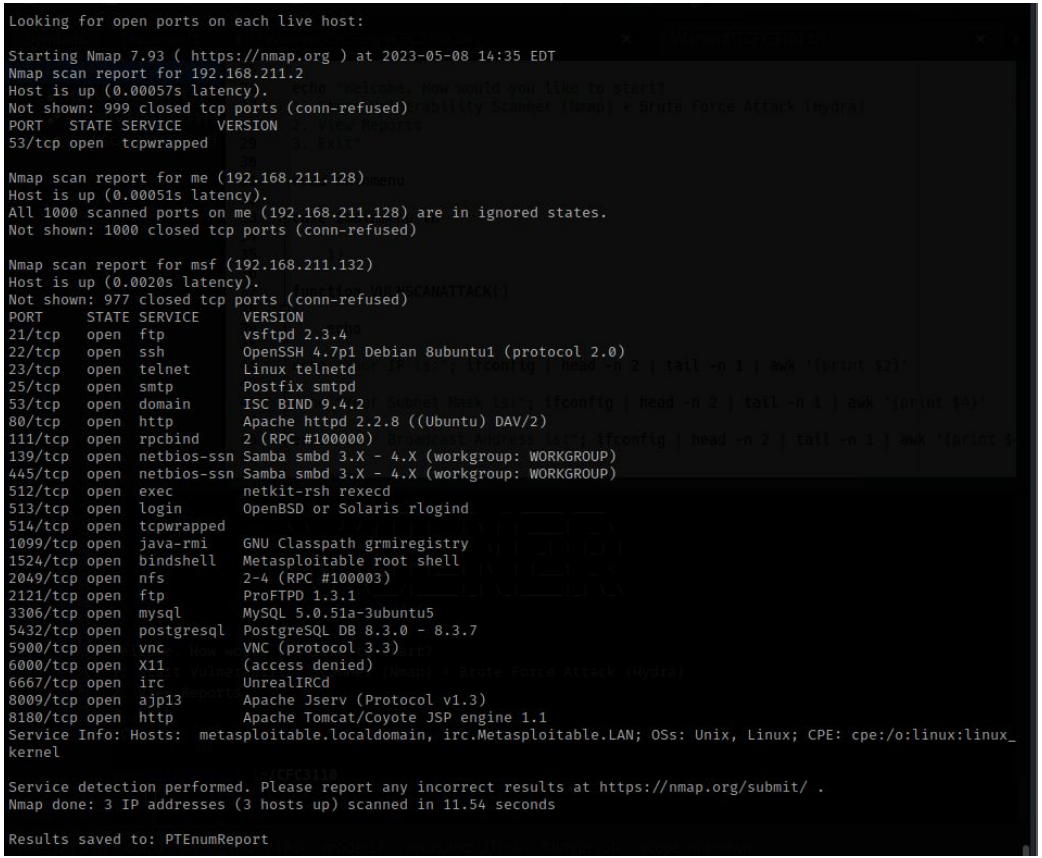
Vulnerability Scanner

The expected output is as such:
The script will first ask for the users first IP Address in the network followed by the last IP Address and uses netmask to calculate the CIDR Range



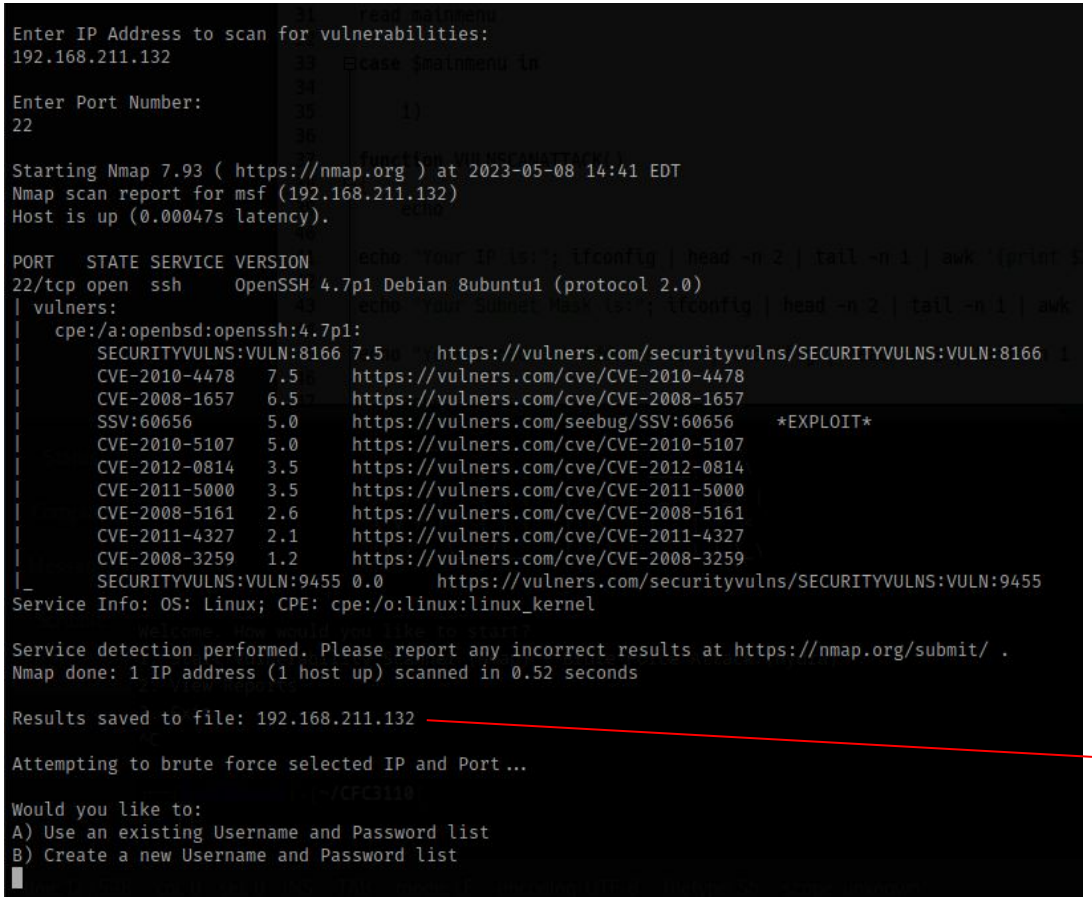
The found IP Address are then put into a list file.

Vulnerability Scanner



The script then takes the list of IP Addresses that were found in the network and automatically looks for open ports for each IP Address, the results are then saved into a file (PTEnumReport) which can be viewed later on.

Brute Force



The user is then prompted for a target IP and specific port. It is then run through a vulnerability checker script through nmap to find potential vulnerabilities for the open port. In this example port 22 (SSH) is used and the output for found vulnerabilities include CVE number, severity rating, and link to the CVE found.

Results of found vulnerabilities are then saved into a file with the name of the target IP in order to facilitate searching

Brute Force

```
Would you like to:
A) Use an existing Username and Password list
B) Create a new Username and Password list
a
Enter Username File:
usernames.txt

Using username file: usernames.txt

Enter Password File:
passwords.txt

Using password file: passwords.txt

Currently supported brute force services:
adam6500  afp asterisk cisco cisco-enable cvs firebird ftp ftps http[s]-{head|get|post}
http[s]-{get|post}-form  http-proxy  http-proxy-urlenum  icq  imap[s]  irc  ldap2[s]
ldap3[-{cram|digest}md5][s] mssql mysql(v4) mysql5 ncp nntp oracle oracle-listener ora-
cle-sid pcanywhere pcnfs pop3[s] postgres rdp radmin2 redis rexec rlogin rpcap rsh rtsp
s7-300  sapr3  sip smb smtp[s] smtp-enum snmp socks5 ssh sshkey svn teamspeak telnet[s]
vmauthd vnc xmpp

Enter login service to brute force:
ssh

Selected login service is: ssh

[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t
4
[22][ssh] host: 192.168.211.132   login: msfadmin   password: msfadmin

Results saved to file: 192.168.211.132

Would you like to:
1. Run Vulnerability Scanner + Brute Force Attack again
2. Return to Main Menu
3. Exit
```

Users can choose to use a username and password file or to create their own

List of possible login services to brute force through Hydra

Results are saved into target IP file.

Users can then choose if they would like to run the script again or look at a report for the findings.

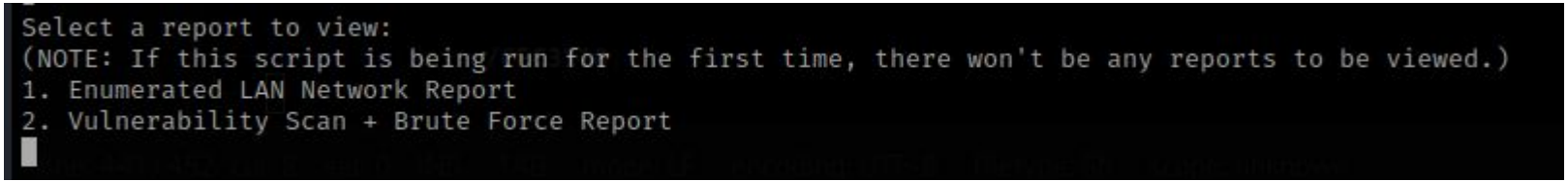
Brute Force

```
Would you like to:
A) Use an existing Username and Password list
B) Create a new Username and Password list
b
Creating Username List..

Enter minimum number of characters:
2

Enter maximum number of characters:
2

Do you want to specify A) Patterns or B) Symbols/Characters
a
Pattern list:
@ = lower case characters
, = upper case characters
% = numbers
^ = symbols
Enter Pattern:
@,
Crunch will now generate the following amount of data: 2028 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 676

crunch: 100% completed generating output

Username List saved to PTusernames.txt
```

Creating username and password list using crunch then to be used in the Hydra attack.

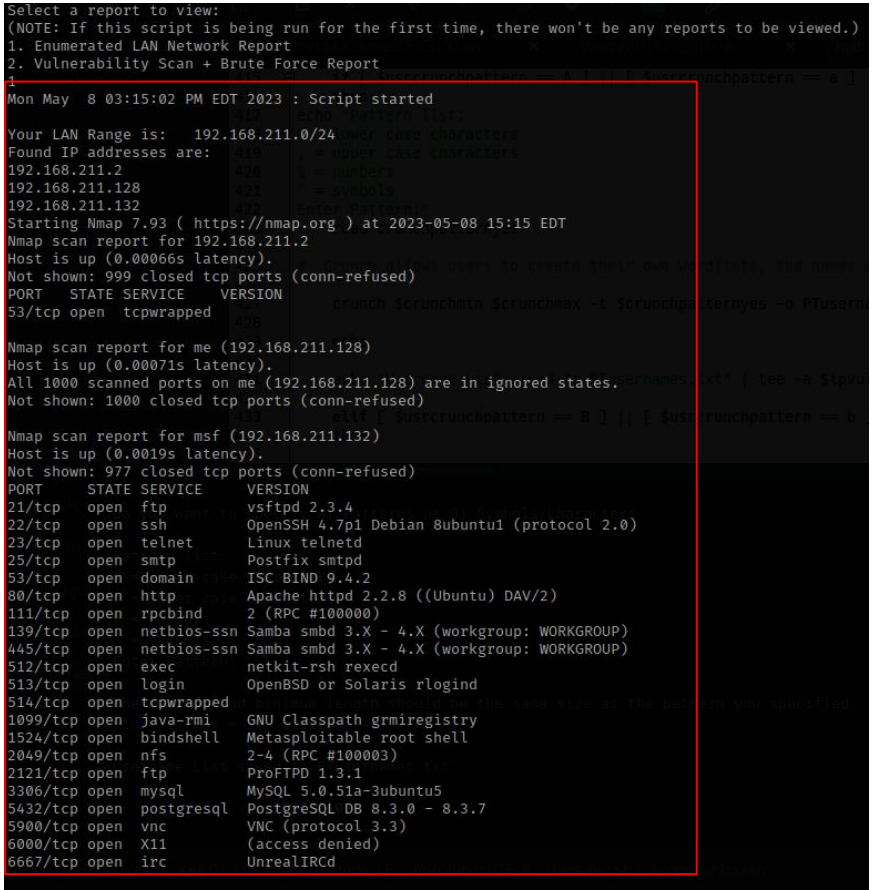
```
Creating Password List..

Enter minimum number of characters:
2
Enter maximum number of characters:
2

Do you want to specify A) Patterns or B) Symbols/Characters
b

Enter characters/symbols to use:
ad

Crunch will now generate the following amount of data: 12 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 4

crunch: 100% completed generating output
Password List saved to PTpasswords.txt
```

Viewing Reports



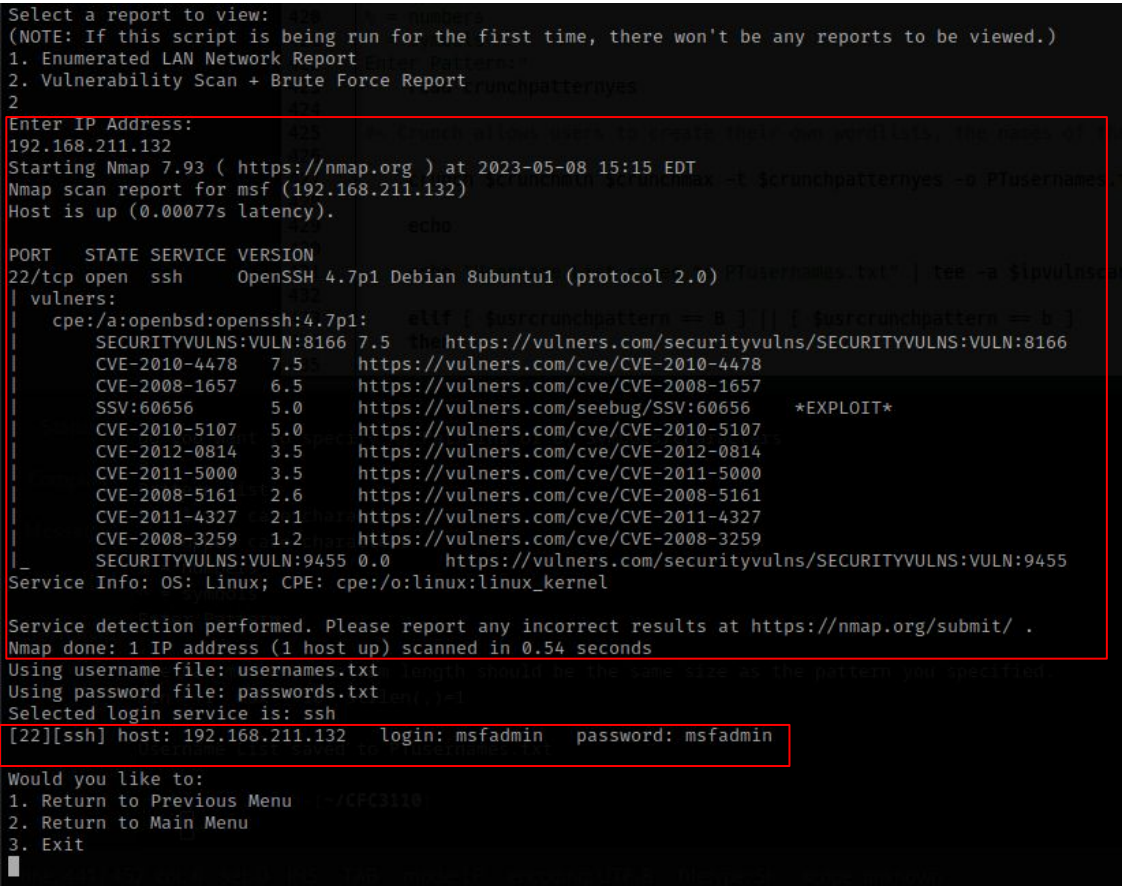
Reports are broken down into two sections, the overall network scan results and the specific targeted IP results.

Enumerated LAN Network Report



The Enumerated Report shows results of searches, including time & date of searches and the list of IP Addresses found within the network. This can be accessed to see previous searches as well.

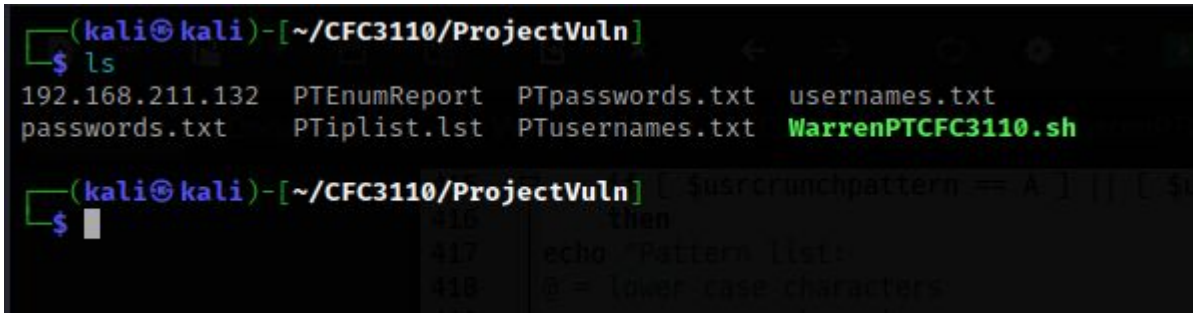
Vulnerability + Brute Force Report



Vulnerability scan report can be viewed via keying in the targeted IP Address.

Results of the Hydra attack are also recorded. If there are no results, that means the attack was unsuccessful.

Misc.



After running the script we can now see several files created to supplement the running of the script and the generated reports.