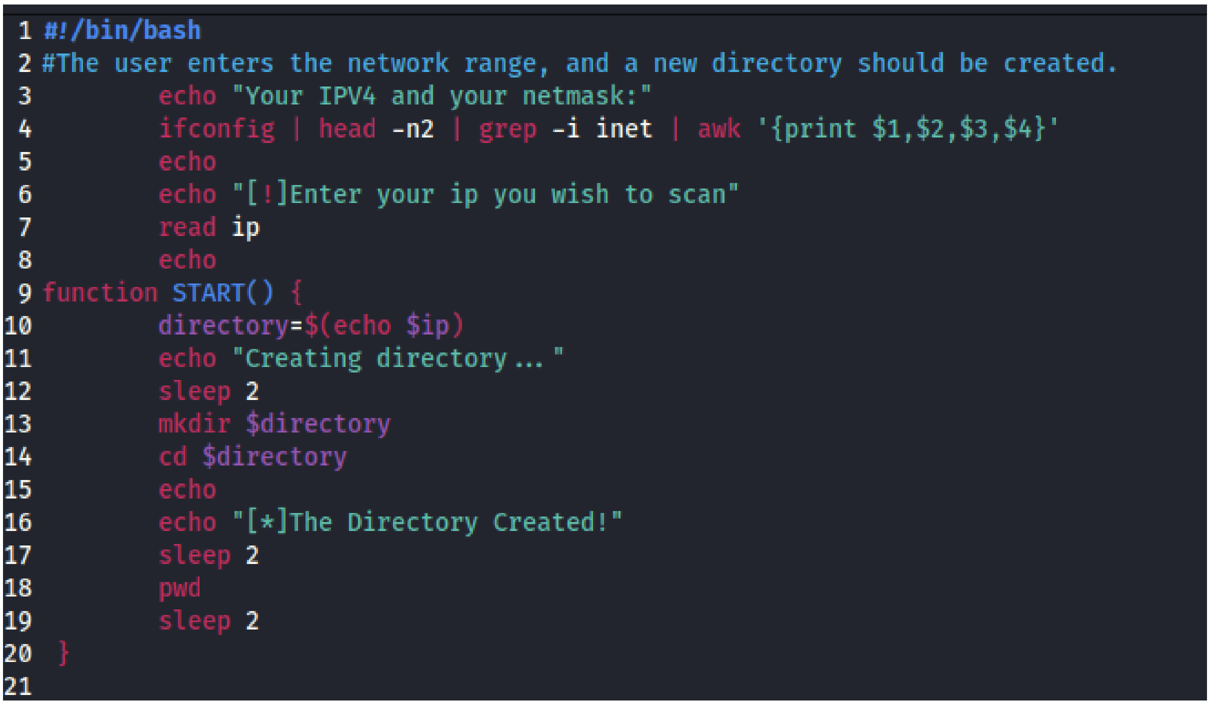
PT project

Name : ariel sapir

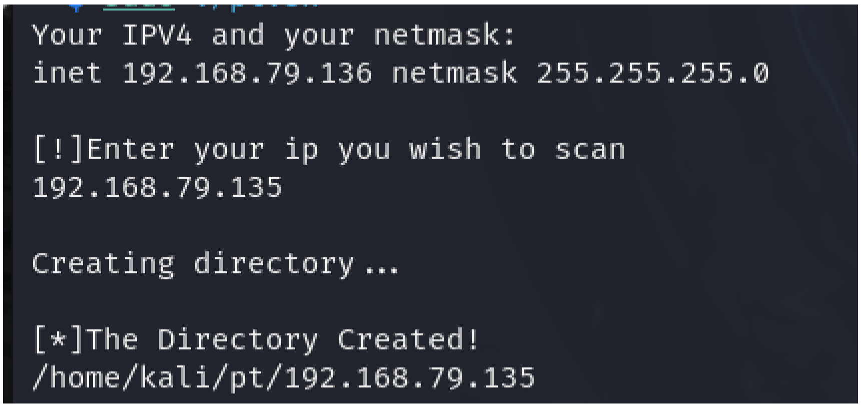
Function 1 start:

User enter ip to scan and a new directory created:



```bash
#!/bin/bash
#The user enters the network range, and a new directory should be created.
        echo "Your IPV4 and your netmask:"
        ifconfig | head -n2 | grep -i inet | awk '{print $1,$2,$3,$4}'
        echo
        echo "[!]Enter your ip you wish to scan"
        read ip
        echo
function START() {
        directory=$(echo $ip)
        echo "Creating directory ... "
        sleep 2
        mkdir $directory
        cd $directory
        echo
        echo "[*]The Directory Created!"
        sleep 2
        pwd
        sleep 2
 }

```

Output:

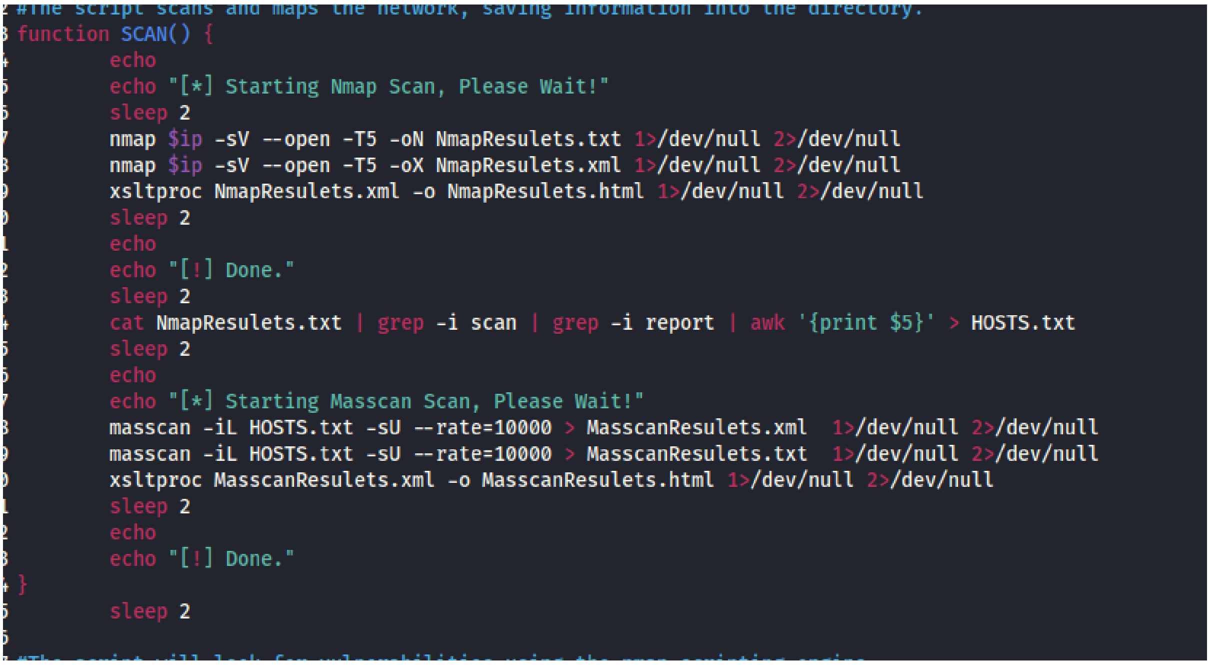


```
Your IPV4 and your netmask:
inet 192.168.79.136 netmask 255.255.255.0

[!]Enter your ip you wish to scan
192.168.79.135

Creating directory ...

[*]The Directory Created!
/home/kali/pt/192.168.79.135
```

Function 2

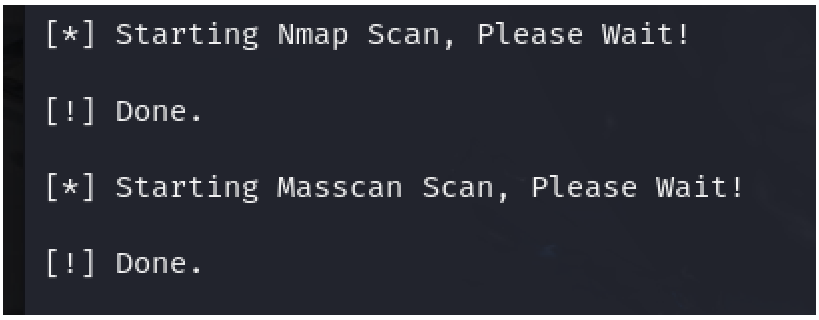
First scans of the Ip given by the user using Nmap and masscan for open hosts ports and services:

PT project



```
#The script scans and maps the network, saving information into the directory.
function SCAN() {
        echo
        echo "[*] Starting Nmap Scan, Please Wait!"
        sleep 2
        nmap $ip -sV --open -T5 -oN NmapResulets.txt 1>/dev/null 2>/dev/null
        nmap $ip -sV --open -T5 -oX NmapResulets.xml 1>/dev/null 2>/dev/null
        xsltproc NmapResulets.xml -o NmapResulets.html 1>/dev/null 2>/dev/null
        sleep 2
        echo
        echo "[!] Done."
        sleep 2
        cat NmapResulets.txt | grep -i scan | grep -i report | awk '{print $5}' > HOSTS.txt
        sleep 2
        echo
        echo "[*] Starting Masscan Scan, Please Wait!"
        masscan -iL HOSTS.txt -sU --rate=10000 > MasscanResulets.xml  1>/dev/null 2>/dev/null
        masscan -iL HOSTS.txt -sU --rate=10000 > MasscanResulets.txt  1>/dev/null 2>/dev/null
        xsltproc MasscanResulets.xml -o MasscanResulets.html 1>/dev/null 2>/dev/null
        sleep 2
        echo
        echo "[!] Done."
}
        sleep 2

#The script will look for vulnerabilities using the nmap scripting engine
```

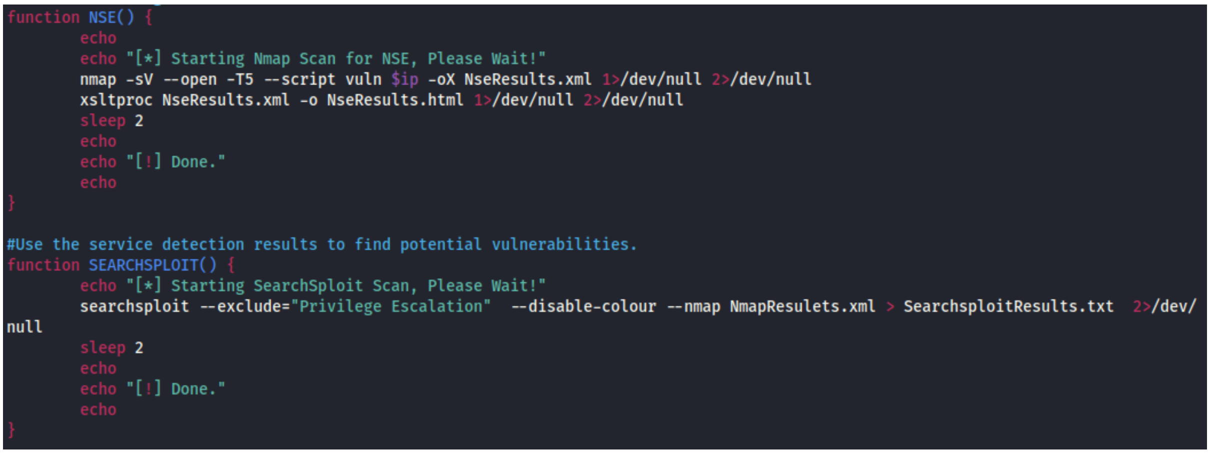
Output



```
[*] Starting Nmap Scan, Please Wait!

[!] Done.

[*] Starting Masscan Scan, Please Wait!

[!] Done.
```

Function 3+4

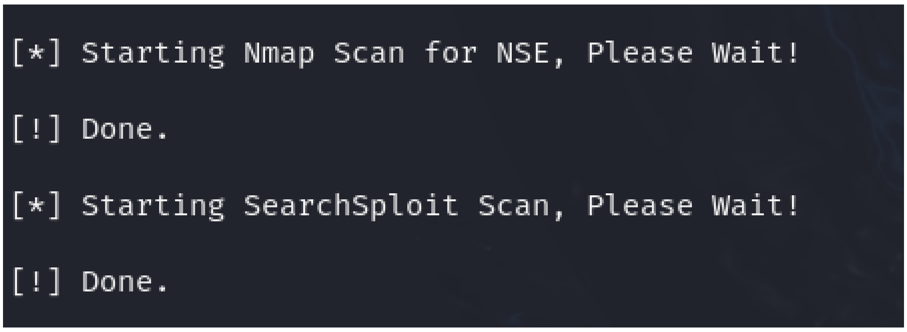
The nse and searchsploit used to find vulnerability and backdoors:



```
function NSE() {
        echo
        echo "[*] Starting Nmap Scan for NSE, Please Wait!"
        nmap -sV --open -T5 --script vuln $ip -oX NseResults.xml 1>/dev/null 2>/dev/null
        xsltproc NseResults.xml -o NseResults.html 1>/dev/null 2>/dev/null
        sleep 2
        echo
        echo "[!] Done."
        echo
}

#Use the service detection results to find potential vulnerabilities.
function SEARCHSPLOIT() {
        echo "[*] Starting SearchSploit Scan, Please Wait!"
        searchsploit --exclude="Privilege Escalation"  --disable-colour --nmap NmapResulets.xml > SearchsploitResults.txt  2>/dev/
null
        sleep 2
        echo
        echo "[!] Done."
        echo
}
```

PT project

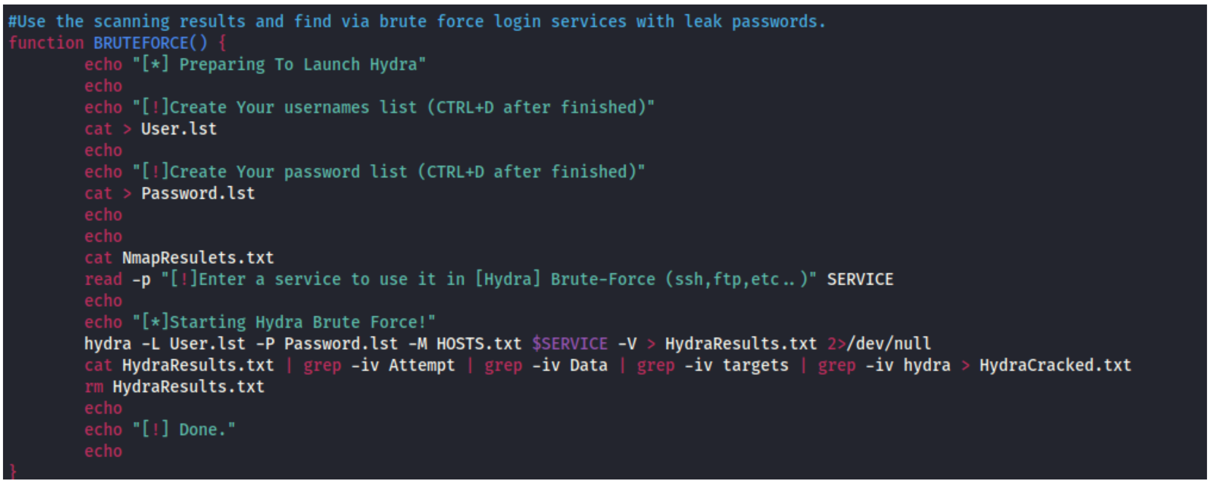
Output



```
[*] Starting Nmap Scan for NSE, Please Wait!

[!] Done.

[*] Starting SearchSploit Scan, Please Wait!

[!] Done.
```

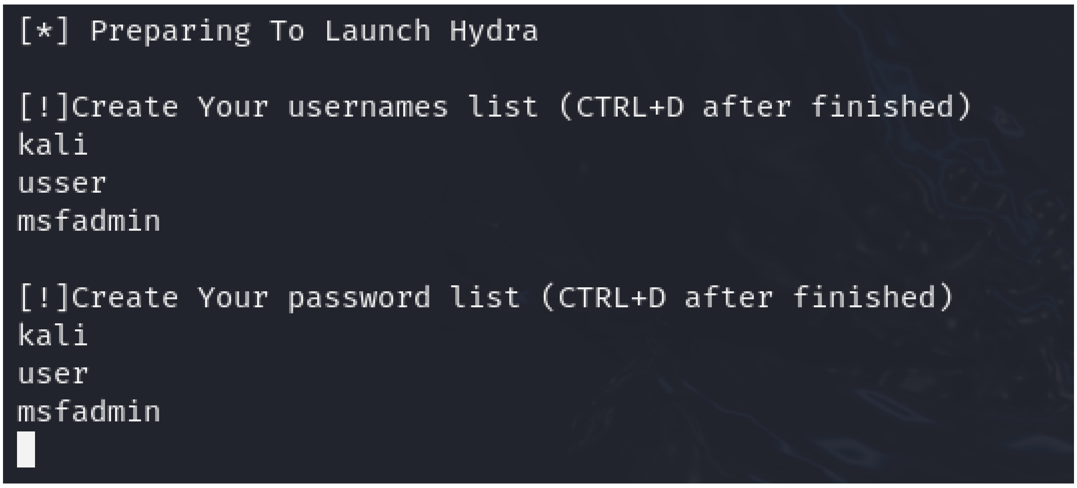
Function 5

Getting a list of ussernames and passsswords and using hydra we will try to brute force:



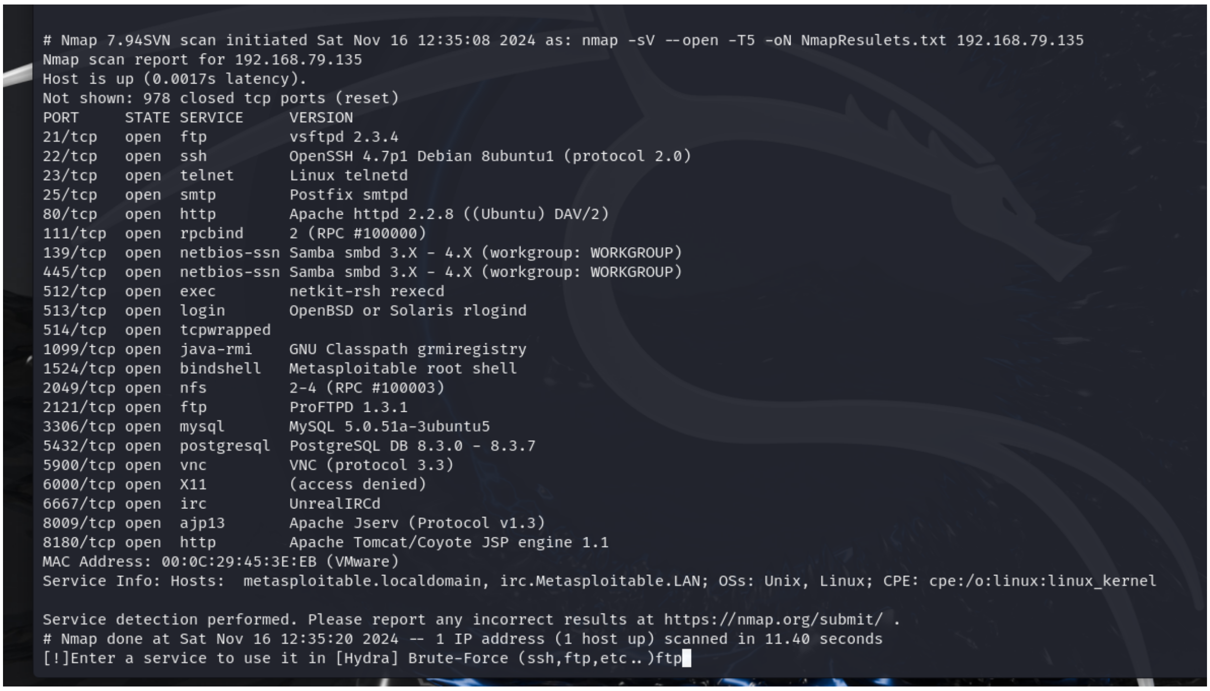
```
#Use the scanning results and find via brute force login services with leak passwords.
function BRUTEFORCE() {
	echo "[*] Preparing To Launch Hydra"
	echo
	echo "[!]Create Your usernames list (CTRL+D after finished)"
	cat > User.lst
	echo
	echo "[!]Create Your password list (CTRL+D after finished)"
	cat > Password.lst
	echo
	echo
	cat NmapResulets.txt
	read -p "[!]Enter a service to use it in [Hydra] Brute-Force (ssh,ftp,etc..)" SERVICE
	echo
	echo "[*]Starting Hydra Brute Force!"
	hydra -L User.lst -P Password.lst -M HOSTS.txt $SERVICE -V > HydraResults.txt 2>/dev/null
	cat HydraResults.txt | grep -iv Attempt | grep -iv Data | grep -iv targets | grep -iv hydra > HydraCracked.txt
	rm HydraResults.txt
	echo
	echo "[!] Done."
	echo
}
```

Output



```
[*] Preparing To Launch Hydra

[!]Create Your usernames list (CTRL+D after finished)
kali
usser
msfadmin

[!]Create Your password list (CTRL+D after finished)
kali
user
msfadmin
█
```

PT project

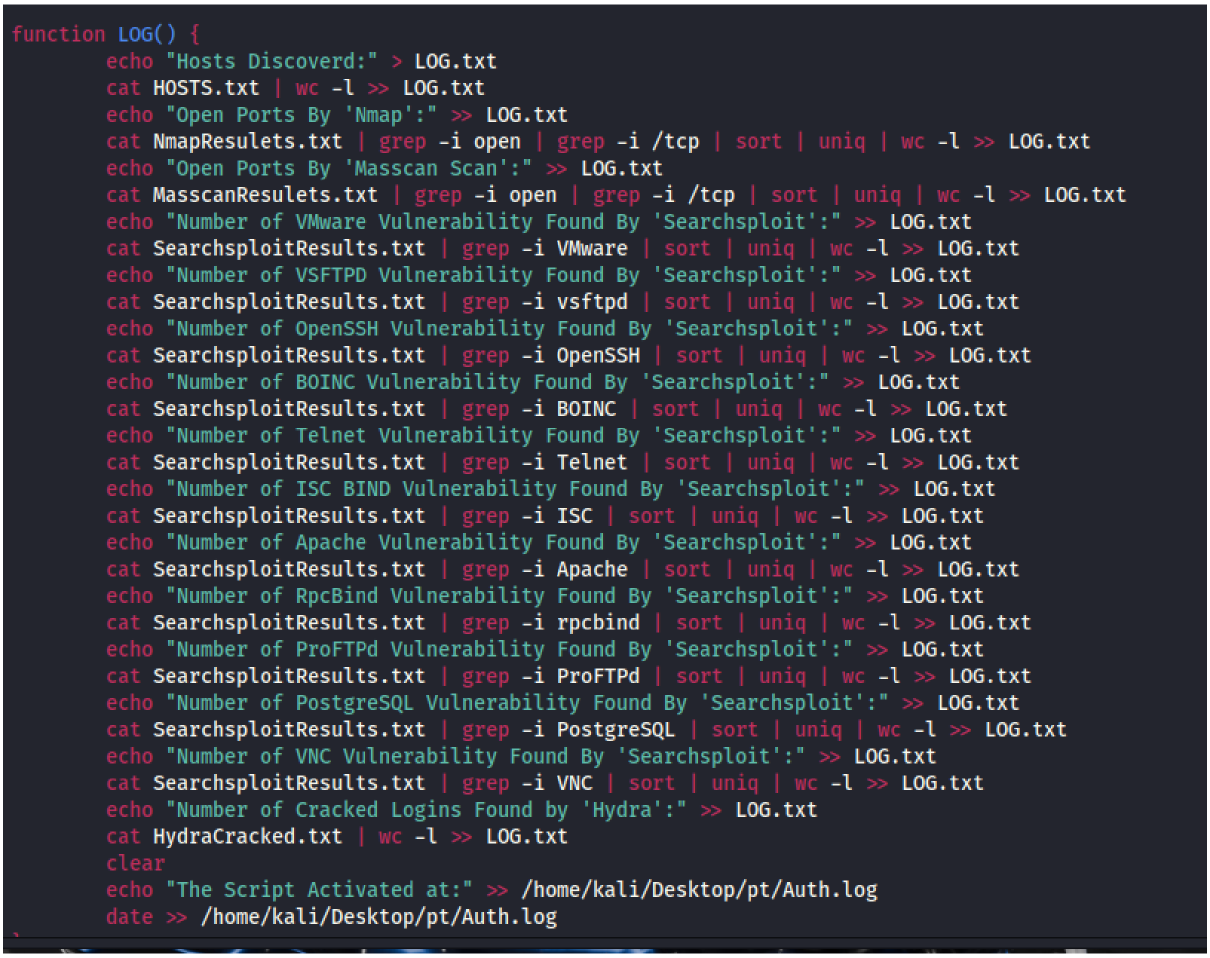


```
# Nmap 7.94SVN scan initiated Sat Nov 16 12:35:08 2024 as: nmap -sV --open -T5 -oN NmapResulets.txt 192.168.79.135
Nmap scan report for 192.168.79.135
Host is up (0.0017s latency).
Not shown: 978 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
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
MAC Address: 00:0C:29:45:3E:EB (VMware)
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 at Sat Nov 16 12:35:20 2024 -- 1 IP address (1 host up) scanned in 11.40 seconds
[!]Enter a service to use it in [Hydra] Brute-Force (ssh,ftp,etc..)ftp
```

Function 6+7

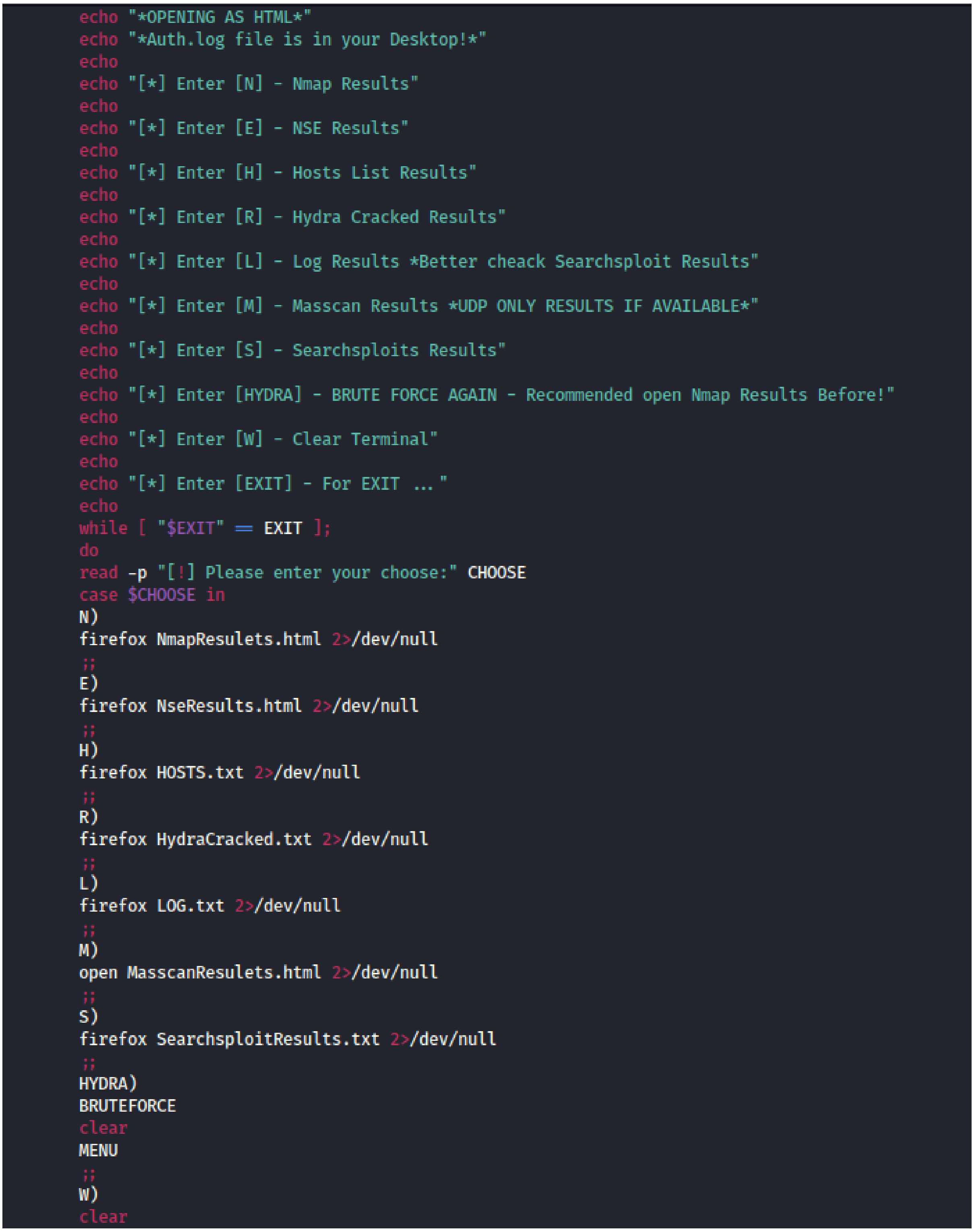
Log and menu

PT project



```
function LOG() {
        echo "Hosts Discoverd:" > LOG.txt
        cat HOSTS.txt | wc -l >> LOG.txt
        echo "Open Ports By 'Nmap':" >> LOG.txt
        cat NmapResulets.txt | grep -i open | grep -i /tcp | sort | uniq | wc -l >> LOG.txt
        echo "Open Ports By 'Masscan Scan':" >> LOG.txt
        cat MasscanResulets.txt | grep -i open | grep -i /tcp | sort | uniq | wc -l >> LOG.txt
        echo "Number of VMware Vulnerability Found By 'Searchsploit':" >> LOG.txt
        cat SearchsploitResults.txt | grep -i VMware | sort | uniq | wc -l >> LOG.txt
        echo "Number of VSFTPD Vulnerability Found By 'Searchsploit':" >> LOG.txt
        cat SearchsploitResults.txt | grep -i vsftpd | sort | uniq | wc -l >> LOG.txt
        echo "Number of OpenSSH Vulnerability Found By 'Searchsploit':" >> LOG.txt
        cat SearchsploitResults.txt | grep -i OpenSSH | sort | uniq | wc -l >> LOG.txt
        echo "Number of BOINC Vulnerability Found By 'Searchsploit':" >> LOG.txt
        cat SearchsploitResults.txt | grep -i BOINC | sort | uniq | wc -l >> LOG.txt
        echo "Number of Telnet Vulnerability Found By 'Searchsploit':" >> LOG.txt
        cat SearchsploitResults.txt | grep -i Telnet | sort | uniq | wc -l >> LOG.txt
        echo "Number of ISC BIND Vulnerability Found By 'Searchsploit':" >> LOG.txt
        cat SearchsploitResults.txt | grep -i ISC | sort | uniq | wc -l >> LOG.txt
        echo "Number of Apache Vulnerability Found By 'Searchsploit':" >> LOG.txt
        cat SearchsploitResults.txt | grep -i Apache | sort | uniq | wc -l >> LOG.txt
        echo "Number of RpcBind Vulnerability Found By 'Searchsploit':" >> LOG.txt
        cat SearchsploitResults.txt | grep -i rpcbind | sort | uniq | wc -l >> LOG.txt
        echo "Number of ProFTPd Vulnerability Found By 'Searchsploit':" >> LOG.txt
        cat SearchsploitResults.txt | grep -i ProFTPd | sort | uniq | wc -l >> LOG.txt
        echo "Number of PostgreSQL Vulnerability Found By 'Searchsploit':" >> LOG.txt
        cat SearchsploitResults.txt | grep -i PostgreSQL | sort | uniq | wc -l >> LOG.txt
        echo "Number of VNC Vulnerability Found By 'Searchsploit':" >> LOG.txt
        cat SearchsploitResults.txt | grep -i VNC | sort | uniq | wc -l >> LOG.txt
        echo "Number of Cracked Logins Found by 'Hydra':" >> LOG.txt
        cat HydraCracked.txt | wc -l >> LOG.txt
        clear
        echo "The Script Activated at:" >> /home/kali/Desktop/pt/Auth.log
        date >> /home/kali/Desktop/pt/Auth.log
}
```

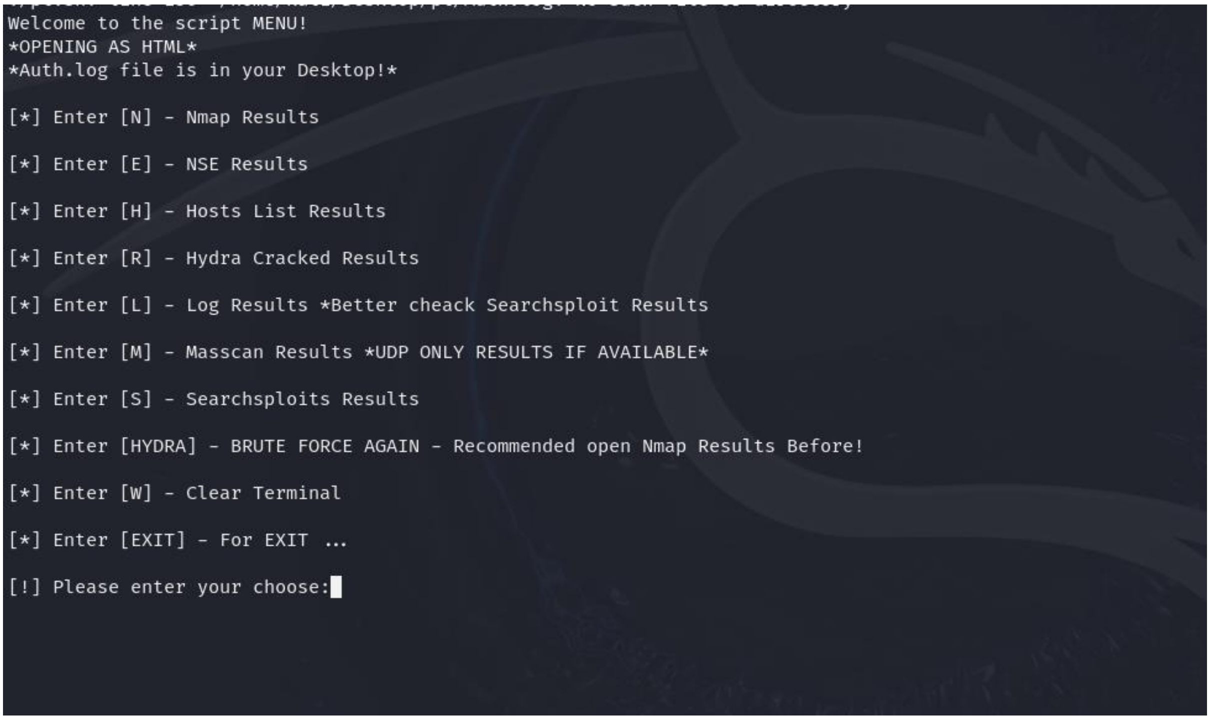
PT project



```
        echo "*OPENING AS HTML*"
        echo "*Auth.log file is in your Desktop!*"
        echo
        echo "[*] Enter [N] - Nmap Results"
        echo
        echo "[*] Enter [E] - NSE Results"
        echo
        echo "[*] Enter [H] - Hosts List Results"
        echo
        echo "[*] Enter [R] - Hydra Cracked Results"
        echo
        echo "[*] Enter [L] - Log Results *Better cheack Searchsploit Results"
        echo
        echo "[*] Enter [M] - Masscan Results *UDP ONLY RESULTS IF AVAILABLE*"
        echo
        echo "[*] Enter [S] - Searchsploits Results"
        echo
        echo "[*] Enter [HYDRA] - BRUTE FORCE AGAIN - Recommended open Nmap Results Before!"
        echo
        echo "[*] Enter [W] - Clear Terminal"
        echo
        echo "[*] Enter [EXIT] - For EXIT ... "
        echo
        while [ "$EXIT" == EXIT ];
        do
        read -p "[!] Please enter your choose:" CHOOSE
        case $CHOOSE in
        N)
        firefox NmapResulets.html 2>/dev/null
        ;;
        E)
        firefox NseResults.html 2>/dev/null
        ;;
        H)
        firefox HOSTS.txt 2>/dev/null
        ;;
        R)
        firefox HydraCracked.txt 2>/dev/null
        ;;
        L)
        firefox LOG.txt 2>/dev/null
        ;;
        M)
        open MasscanResulets.html 2>/dev/null
        ;;
        S)
        firefox SearchsploitResults.txt 2>/dev/null
        ;;
        HYDRA)
        BRUTEFORCE
        clear
        MENU
        ;;
        W)
        clear
```

Output

PT project



```
Welcome to the script MENU!
*OPENING AS HTML*
*Auth.log file is in your Desktop!*

[*] Enter [N] - Nmap Results

[*] Enter [E] - NSE Results

[*] Enter [H] - Hosts List Results

[*] Enter [R] - Hydra Cracked Results

[*] Enter [L] - Log Results *Better cheack Searchsploit Results

[*] Enter [M] - Masscan Results *UDP ONLY RESULTS IF AVAILABLE*

[*] Enter [S] - Searchsploits Results

[*] Enter [HYDRA] - BRUTE FORCE AGAIN - Recommended open Nmap Results Before!

[*] Enter [W] - Clear Terminal

[*] Enter [EXIT] - For EXIT ...

[!] Please enter your choose:
```