Nmap -A output was huge, the open ports were 20, 21, 22, 53, 80, 139, 666, 3306
20 is closed
21 is an open FTP port
22 ssh, 53 is DNS
80 is web server
139 is samba
666 is “doom?” → After some research I found this was used by the vídeo game Doom. Cool!
3306 mysql

MySQL is probably only worth exploring after getting some credentials, same for port 22
For now we can start by exploring port 80 or the FTP server

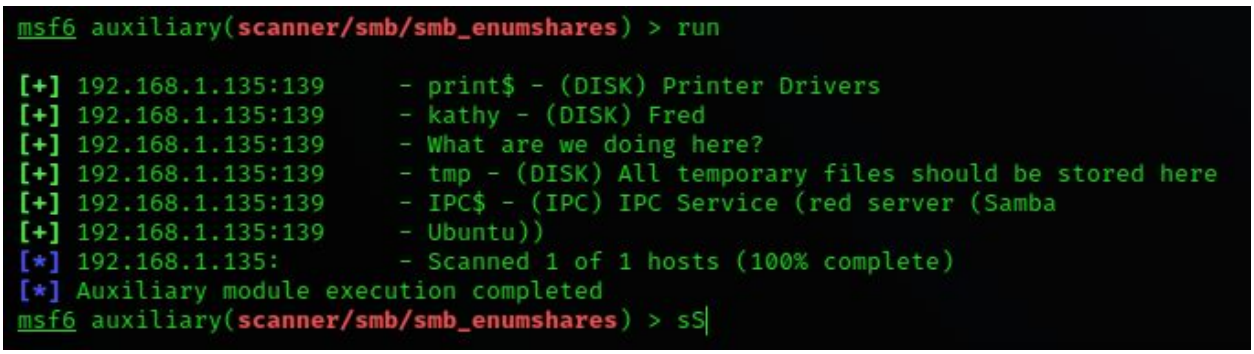
Lol… But we still don’t have a password
I can login as ftp and get the file “note” which says

“Elly, make sure you update the payload information. Leave it in your FTP account once your are done, John.”

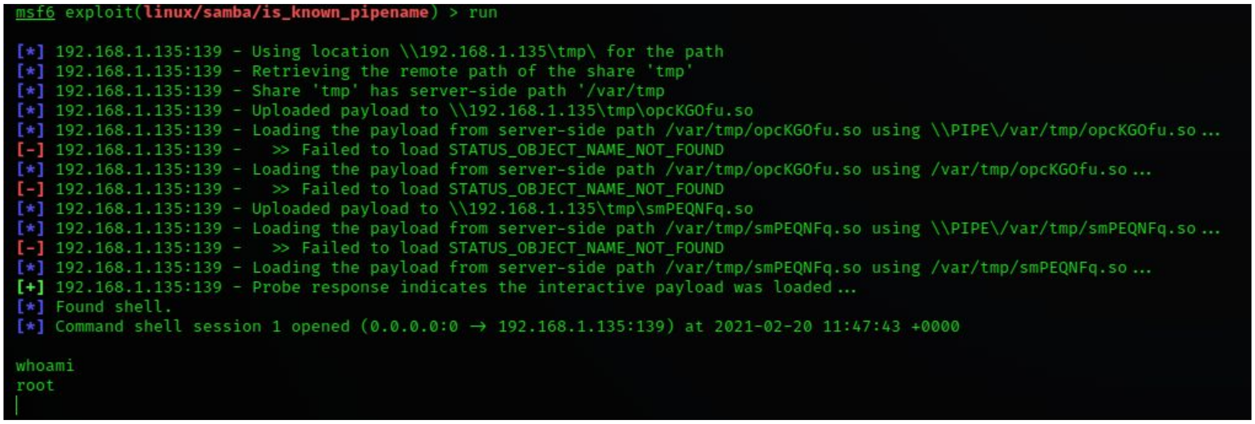
So there’s user John, Harry and Elly. Elly has the payload information so that’s what we’re after. Then, Harry will probably be the target. Also, John, it’s “you’re” not “your”

I guess that’s everything in the FTP port…
Port 80 is not found. That leaves us with samba and mySQL. MySQL doesn’t seem to be exploitable. Samba is our target now

Msfconsole → smb enum shares



After some searching, I found about SambaCry



Upgraded to interactive shell with /bin/bash -i

That easy? Was expecting something more tbh…

I read some walkthroughs and it seems like there were several other paths to root with a lot more steps than this one. Maybe I got lucky choosing the right path ;)