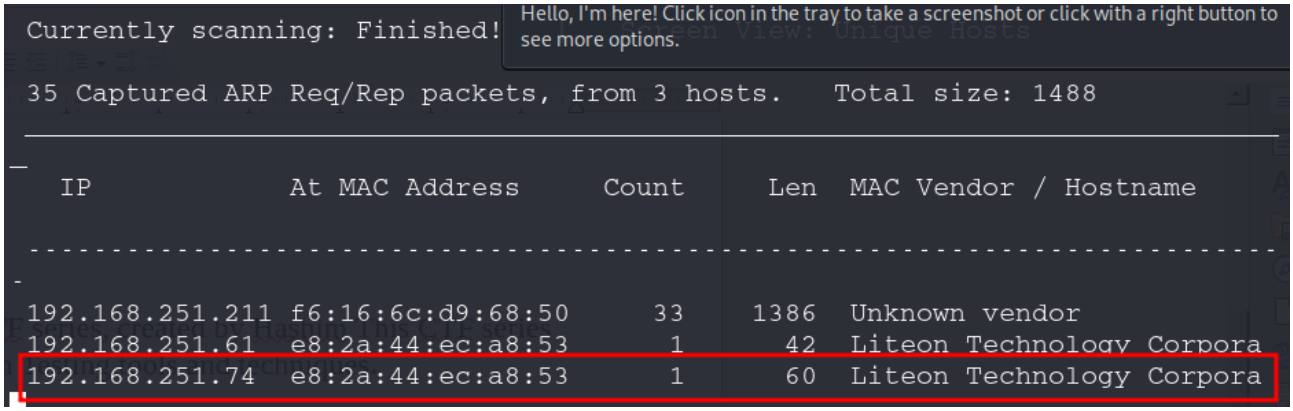
west-wild Walkthrough

Challenge name(Vm): westwild
Category: writeups
Goal: gaining root access
Challenge Points: --
Year/Date: 24/21

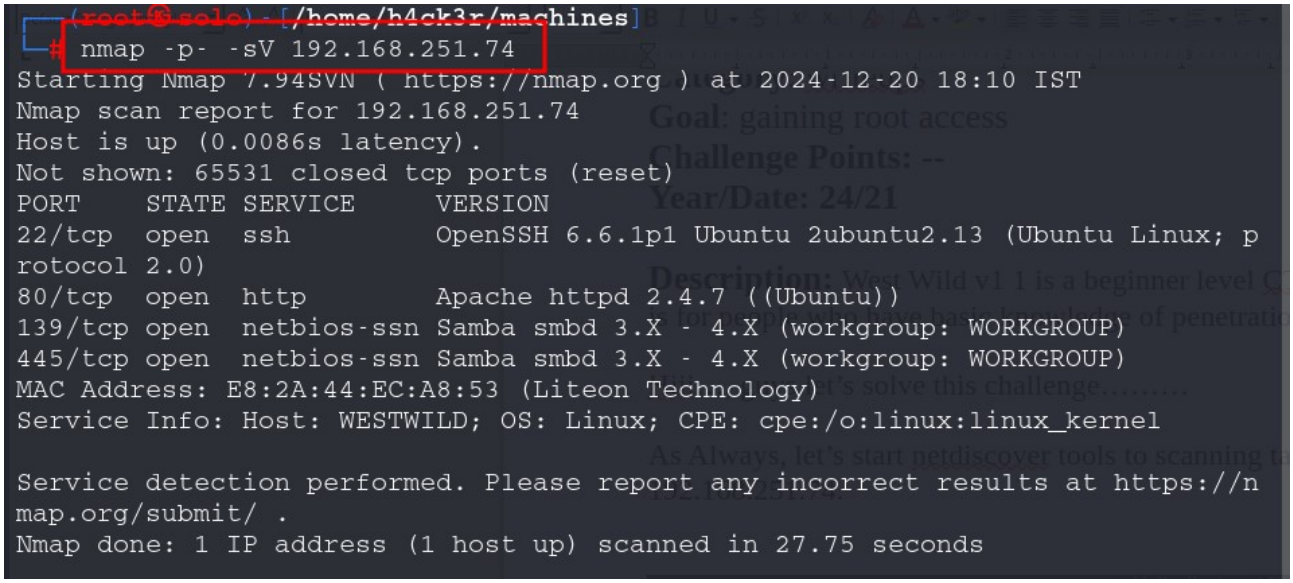
Description: West Wild v1 1 is a beginner level CTF series, created by Hashim This CTF series is for people who have basic knowledge of penetration Testing tools and techniques**.**

Hiii…, guys let's solve this challenge……

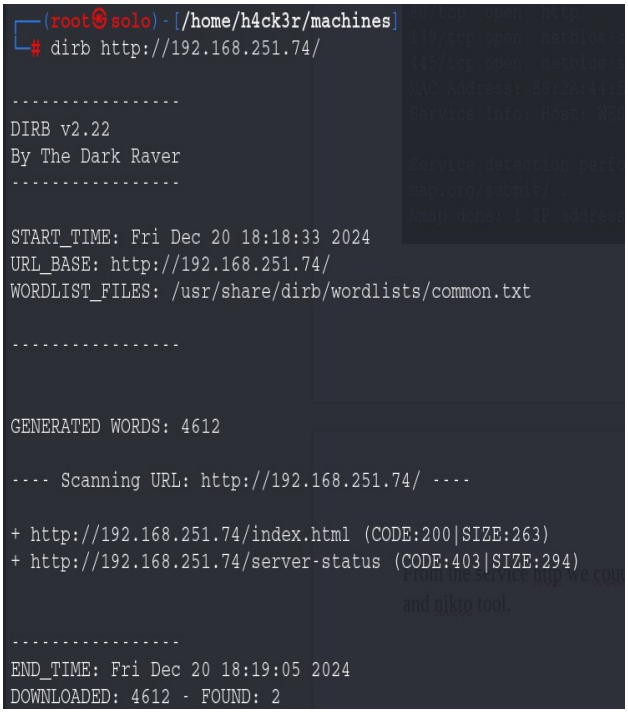
As Always, let's start netdiscover tools to scanning target ip addresss…., so our target ip address is 192.168.251.74.

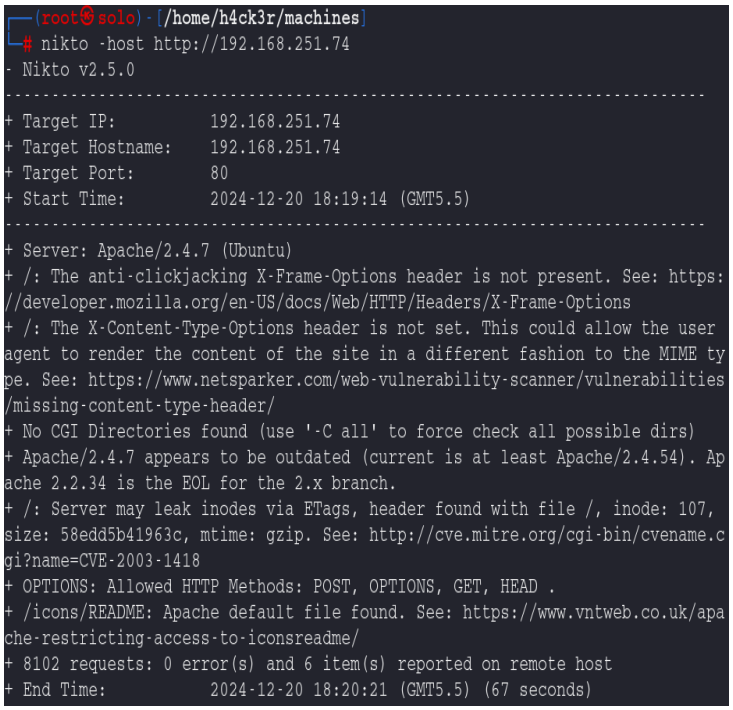


After discovering the target ip address, let's scan with nmap tool for detecting service and version detection of our target ip address. Here -p- which scan all port number that in between 1-65535.

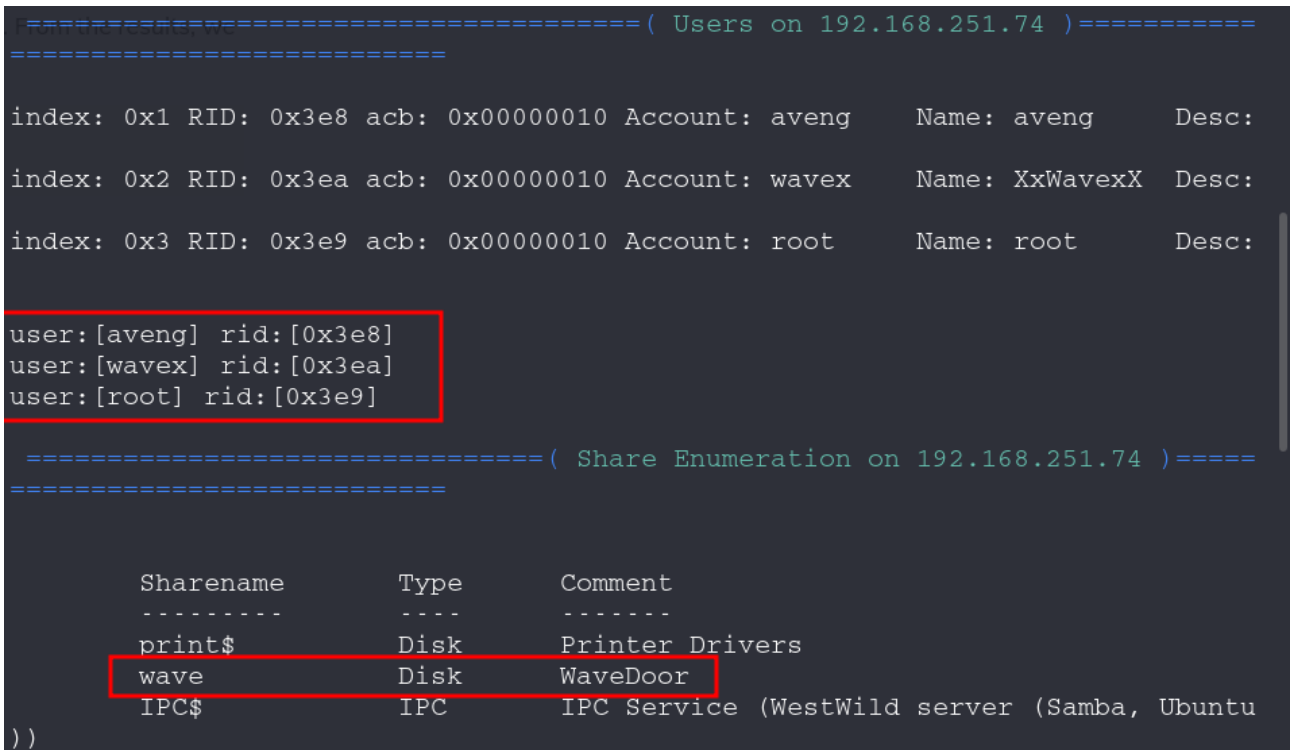


From the service http we coudn’t find anything use able information about target when we used dirb and nikto tool.

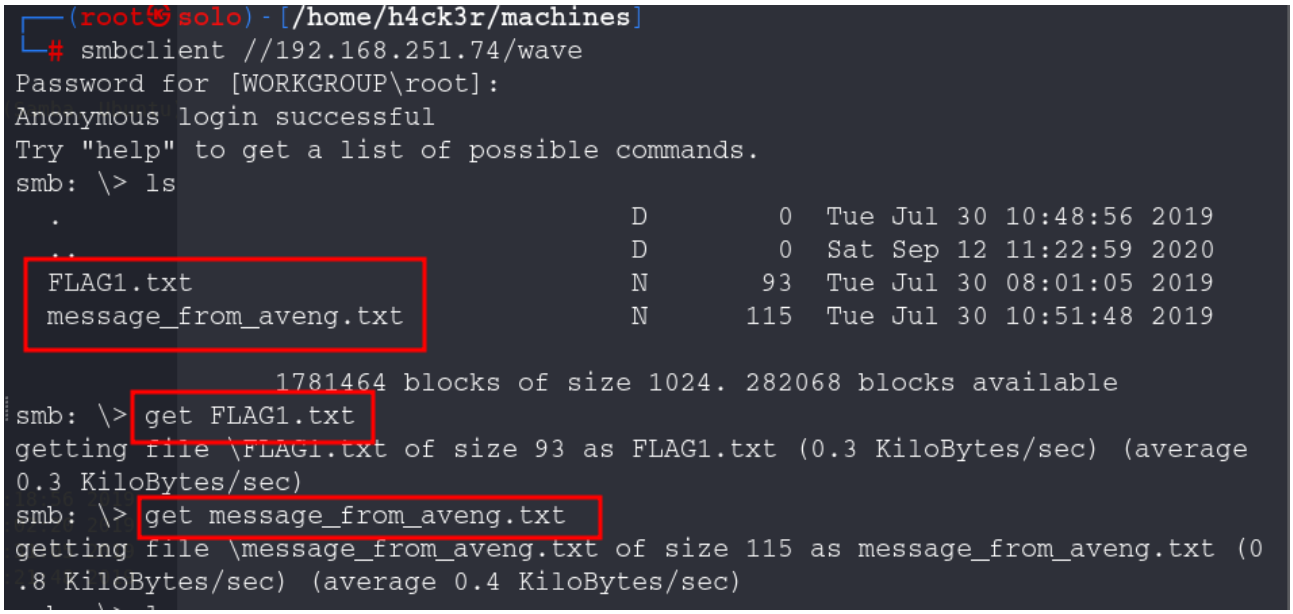




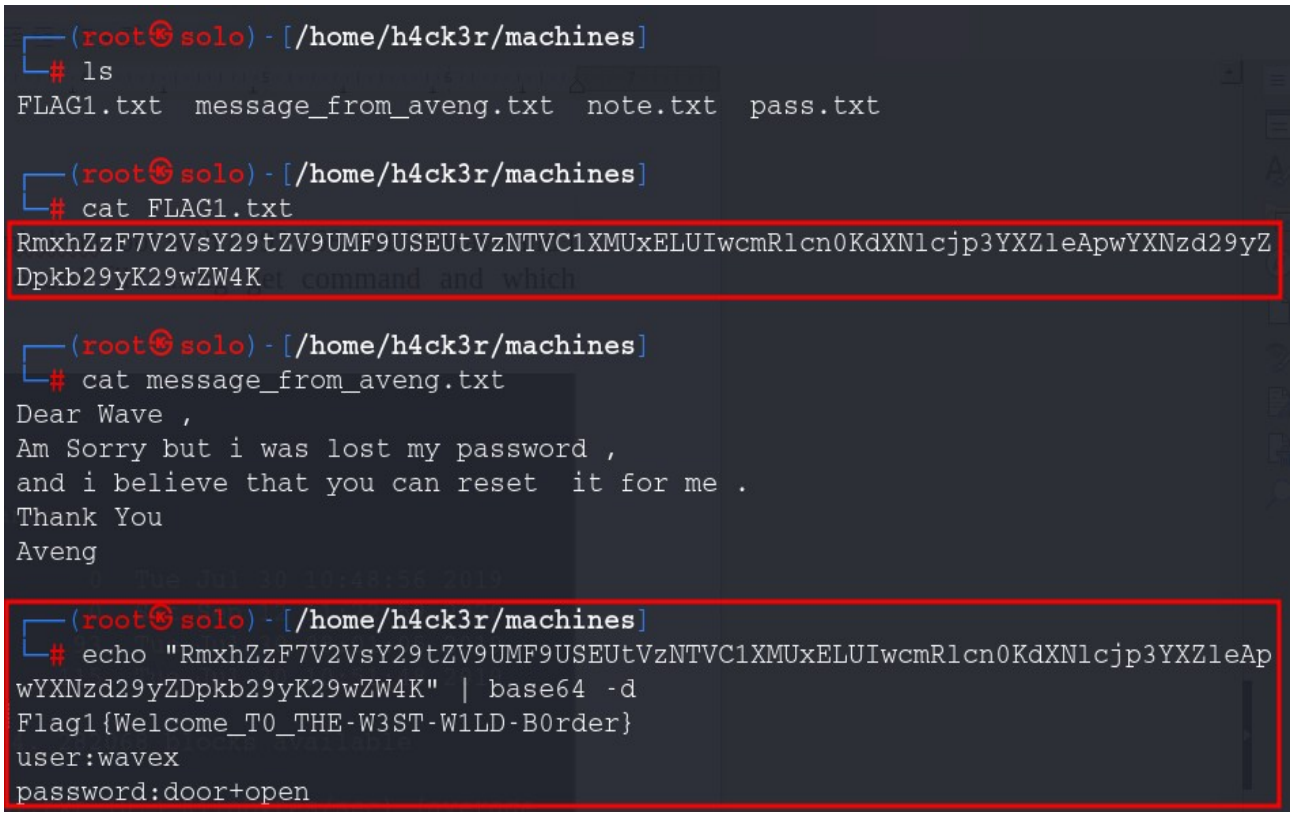
As we can see from the nmap scanning the smb server is running on both port number that is 139 and 445, so let’s enumarate smb service using enum4linux tool(which this tool is used for discovering information about smb server). From result its enumerates that there are three users and share directory name is wave.



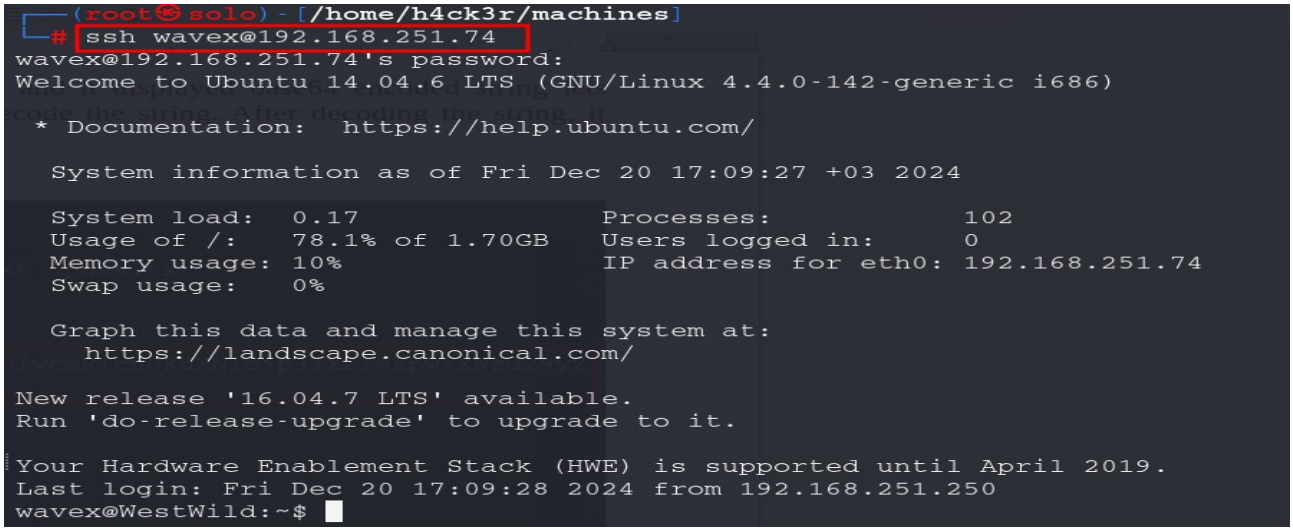
From this figure, I have connected smb server with smbclient tool with //192.168.251.74/wave and I have logged in with no password. I have downloaded file using get command and which downloaded in current directory.



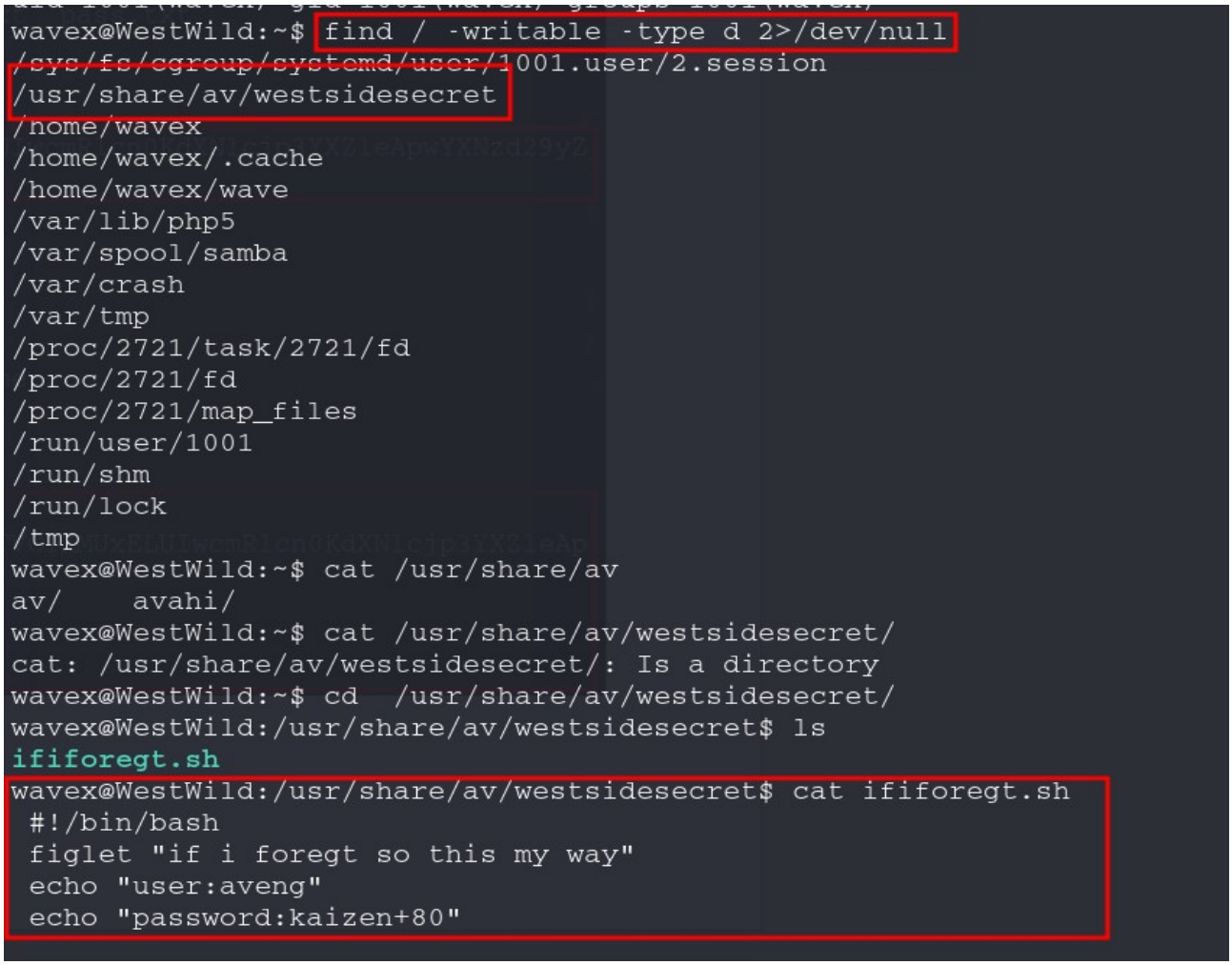
I have opened that FLAG1.txt using cat command and it displayed base64 encoded string lets decode with base64 -d where -d switch used for decode the string. After decoding the string, it reveal flag with username and password of wavex.



I have logged in with given username and password with using ssh service.



After logged in, I used find command to find writable directory for aveng user where clue was given in messeage_from_aveng.txt file. So we found /usr/share/a/westsidesecret directory and also found ififoregt.sh. When I opened that sh file with cat command and it's revealing username and password for aveng.



After logged into aveng user, I used sudo su command for root user and after putting aveng password, it’s successfully llogged in as root user. And then I used root directory for root acecess flag.