***REPORT***

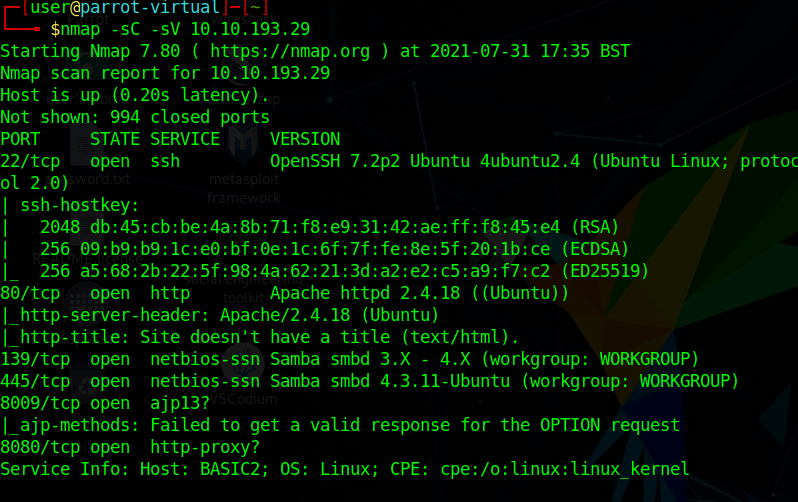
***BASIC PENTESTING MACHINE (TRYHACKME)***

***Starting with connecting to vpn we switched on the machine.***

***To fine open ports and services available on it, I did nmap scan.***

***The result of which shows us 4 open ports:***

***22,80,139,445***



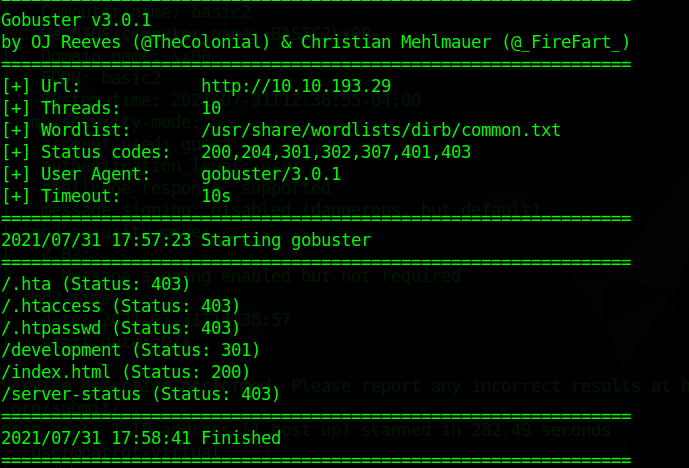


***Moving further :***

***We want to brute force it to find hidden directories***

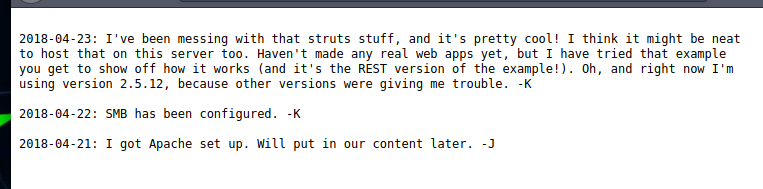
***For which we have gobuster***

***Gobuster gives us***

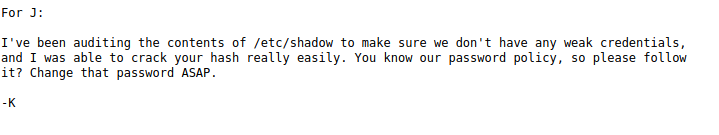


***This clearly indicates /development to be the only useful directory.***

***Opening this on chrome gives us a page that has further 2 txt files which says:***

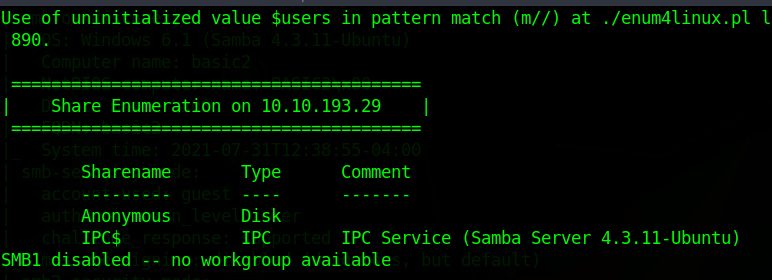


***And***



***We are going to use enumeration enum4linux tool which is used in extracting and detecting data from linux as well as windows.***

***Lets go with -a tag that gives us maximum of information needed.***



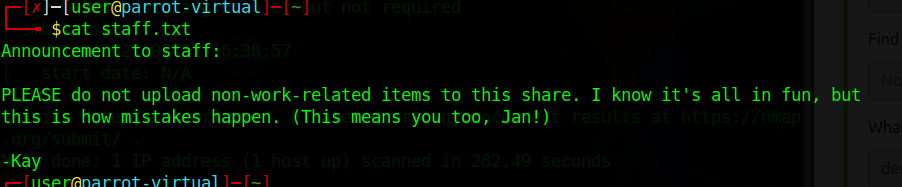
***This is something useful so I just fetched this here.***

***Now we have 2 user and among which IPC$ is generally common to all and seems of no importance so lets go with Anonymous.***

***To login in Anonymous let’s use the SMB(service message block) enumeration which is basically a protocol used for sharing files, printers and stuff.***

***Remember that ls -la command does not work in smb.***

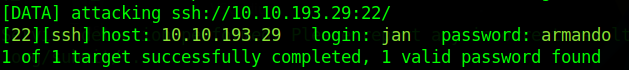
***We got 1 text file which cannot display its contents with cat so we will do get command to get it.***



***From here we can easily figure out the names of the 2 users.***

***Since we have the users now lets try to find their passwords.***

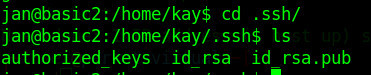
***I am using hydra brute forcing tool for this. It uses a lot of ssh configurations at once therefor limit them to 4 or some small number by using the tag -t 4.***



***Lets connect ssh with jan as user and Armando as password.***

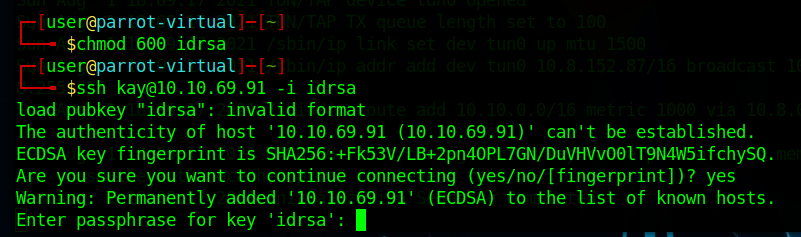
***In /home directory we jan and kay.***

***There is nothing in jan but kay has a file. That file is not accessable. So moving on we change directory to ssh and found public and private keys there.***

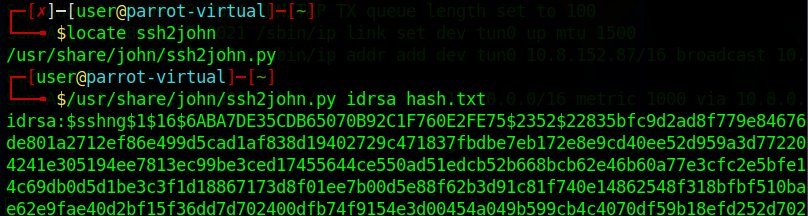


***I saved the private key in my machine. Now I tried to login as kay which is the other user using his private key .***

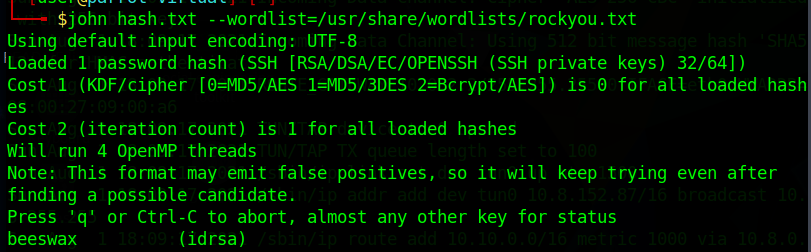
***chmod 600 idrsa – I did this command first to change the permissions of the key to be only read and seen by the root user.***



***Oh no! it seems like the key has a passphrase on it. Lets try to crack it using john the ripper. To do that we will first change private key to hash file using ssh2john.***

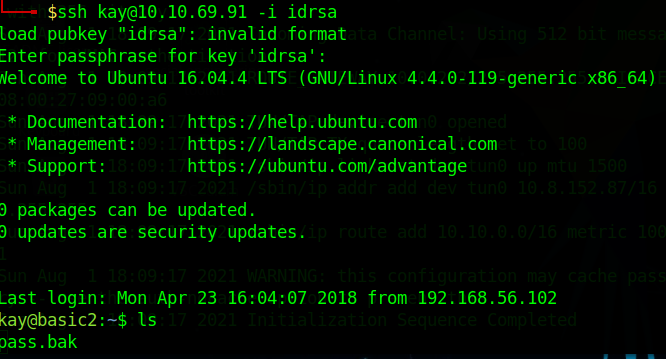


***Lets brute force this file using john the ripper and decode its password.***



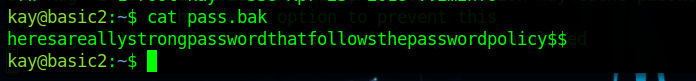
***From here we got the passphrase “beeswax”***

***Now lets try login again.***



***Hurray!! We got into the system.***

***Lets try finding our last flag.***



***And yes!!! We found it as well.***