System Hacking

-> Ashutosh Chauhan

CHALLENGES:

**Task 1:** Password Attacks using Hydra

**Task 2:** Password Attacks usingAuxiliary Module

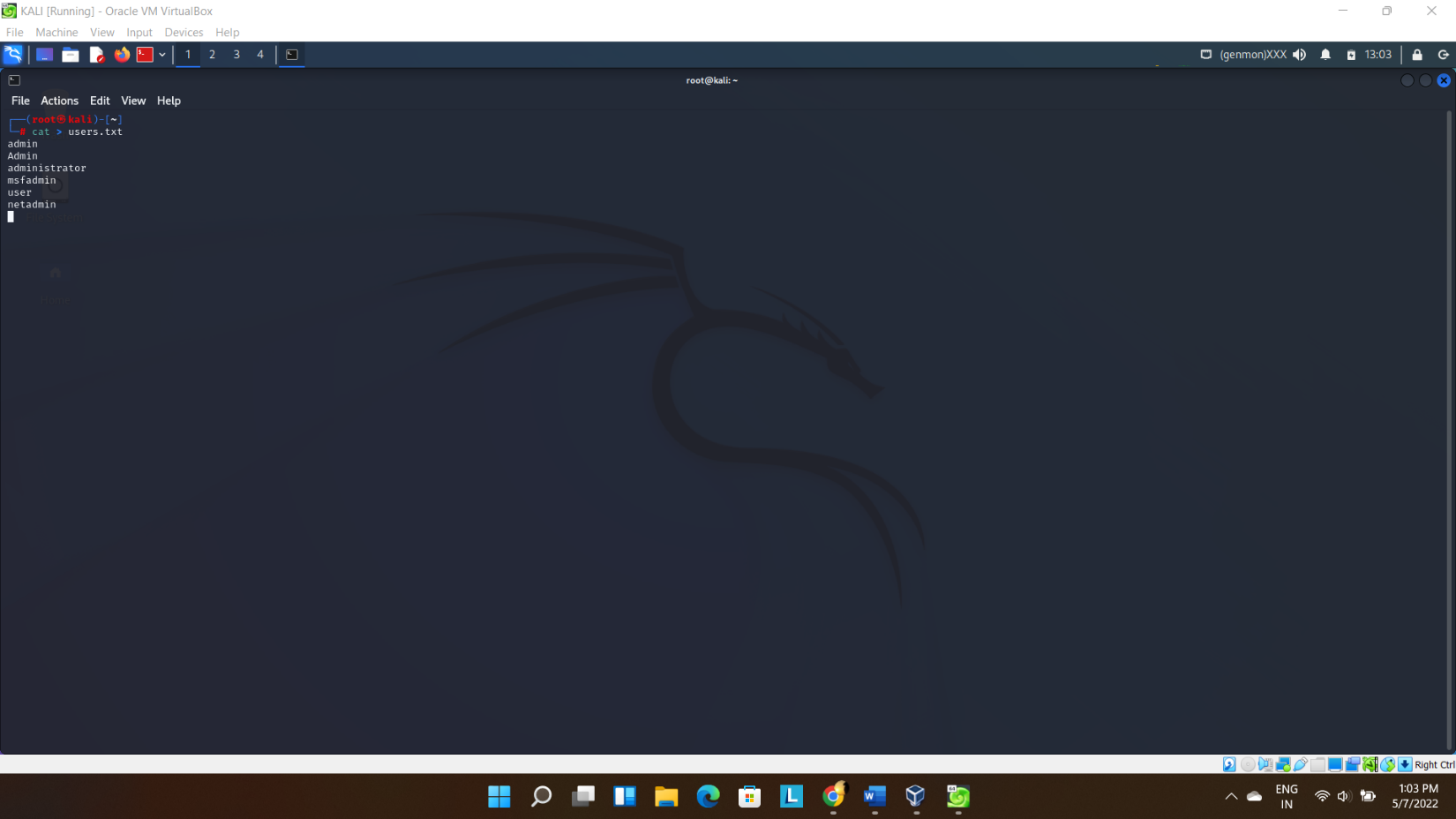
**Task 3:** Password Attacks usingNSE Scripts

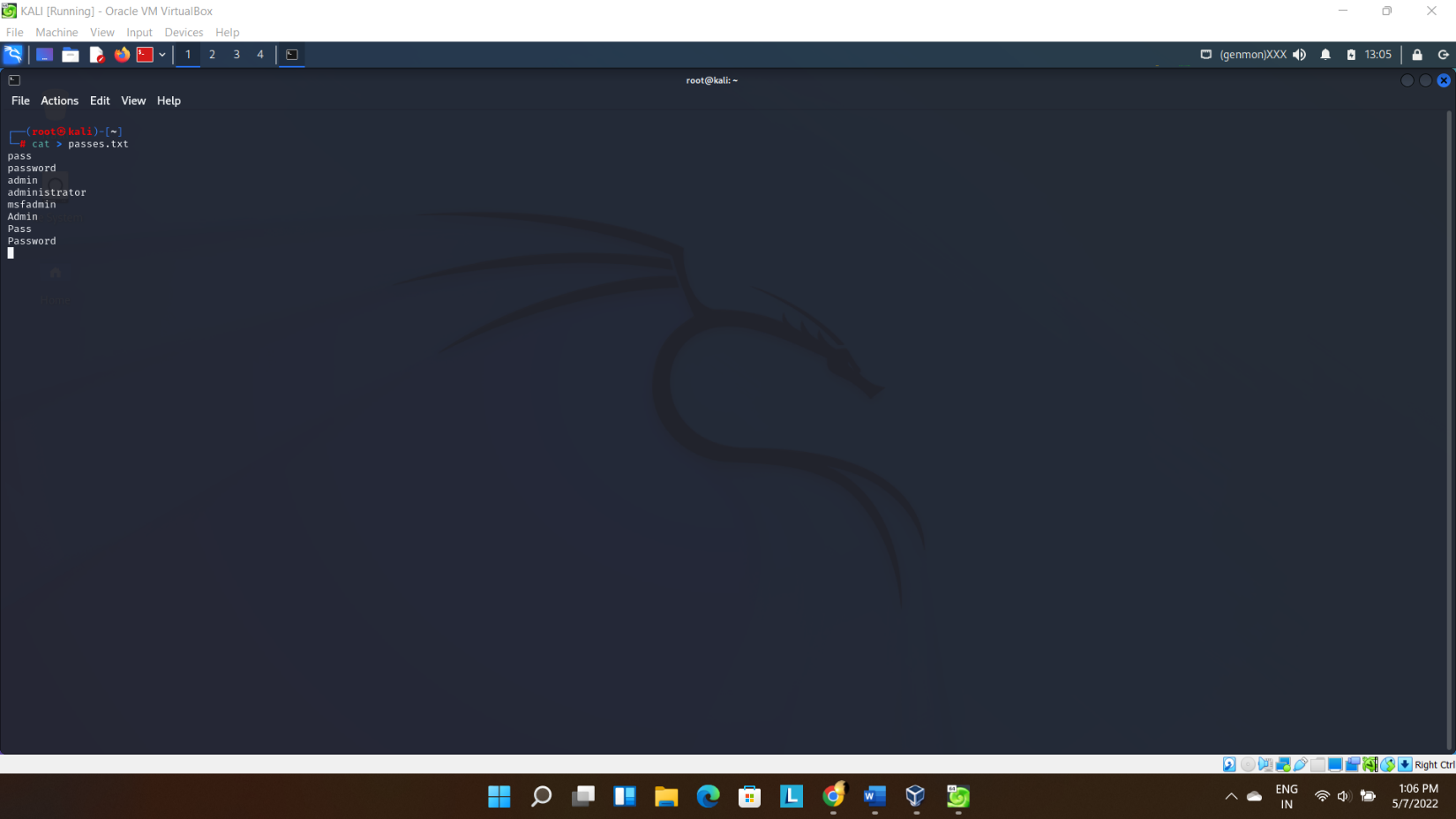
**Task 4:** Password Attacks usingJohn the ripper

**Task 5:** Password generating using Crunch

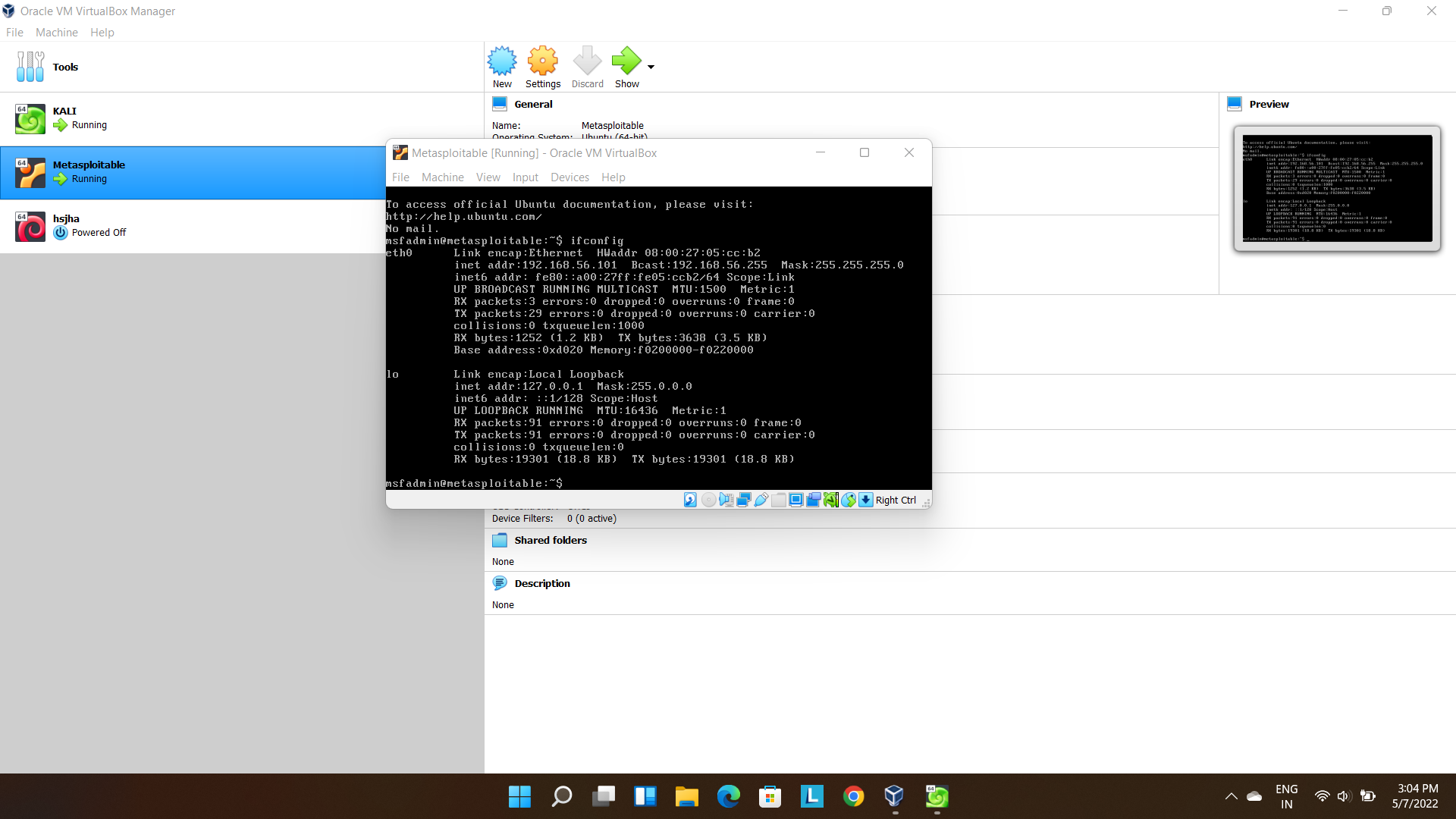
PROCEDURE:

*Password Attacks using Hydra: -*

Here I created the files named ‘users.txt’ and ‘passes.txt’ (using concatenate[cat] command) which contain usernames and passwords:



Log in to metasploitable Linux (using login: msfadmin, password: msfadmin) And then Using ifconfig to find the ip address:

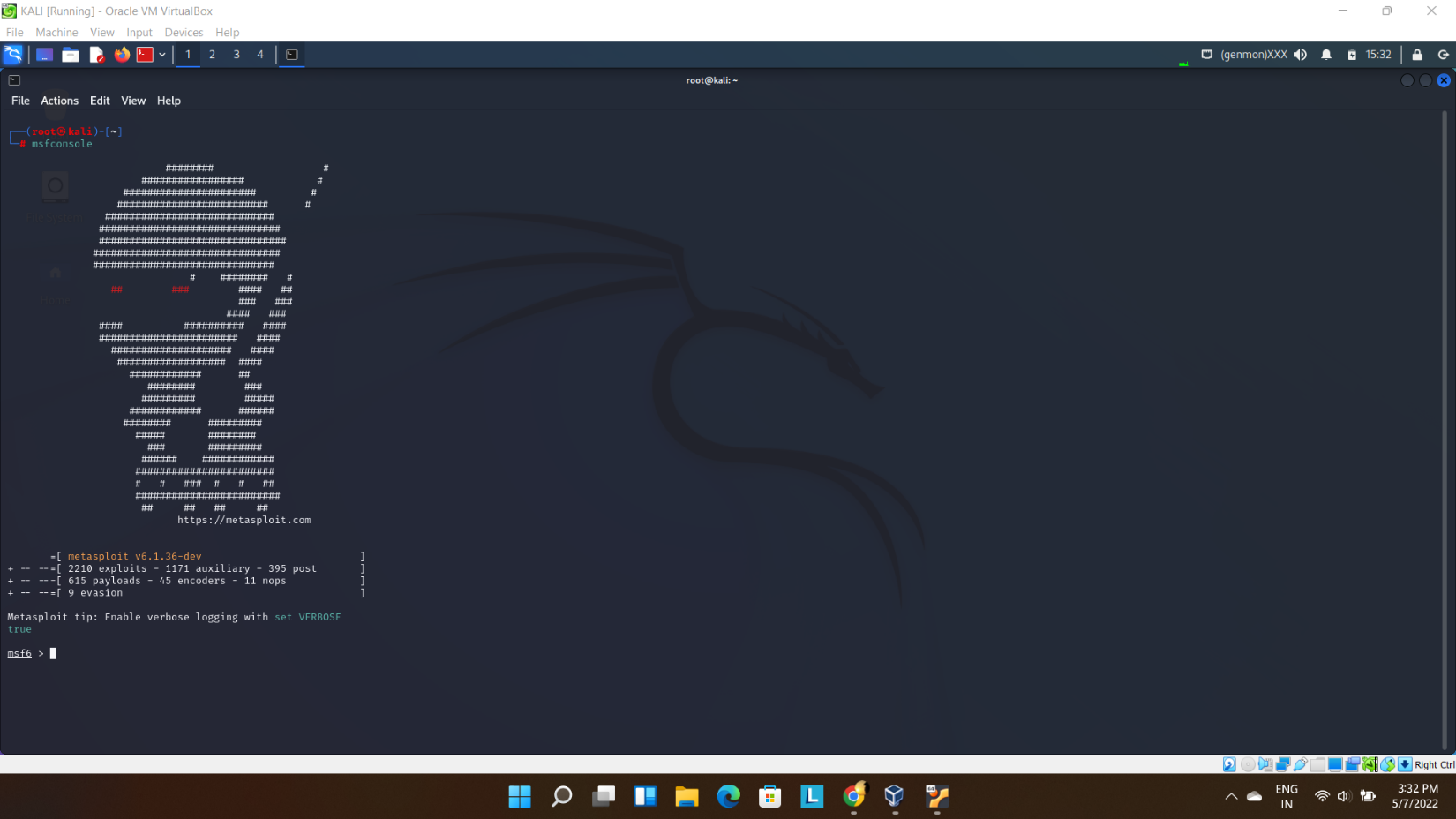


Then using hydra to crack the username and password (first using the telnet port which didn’t give the expected result, so I proceeded with ssh port):

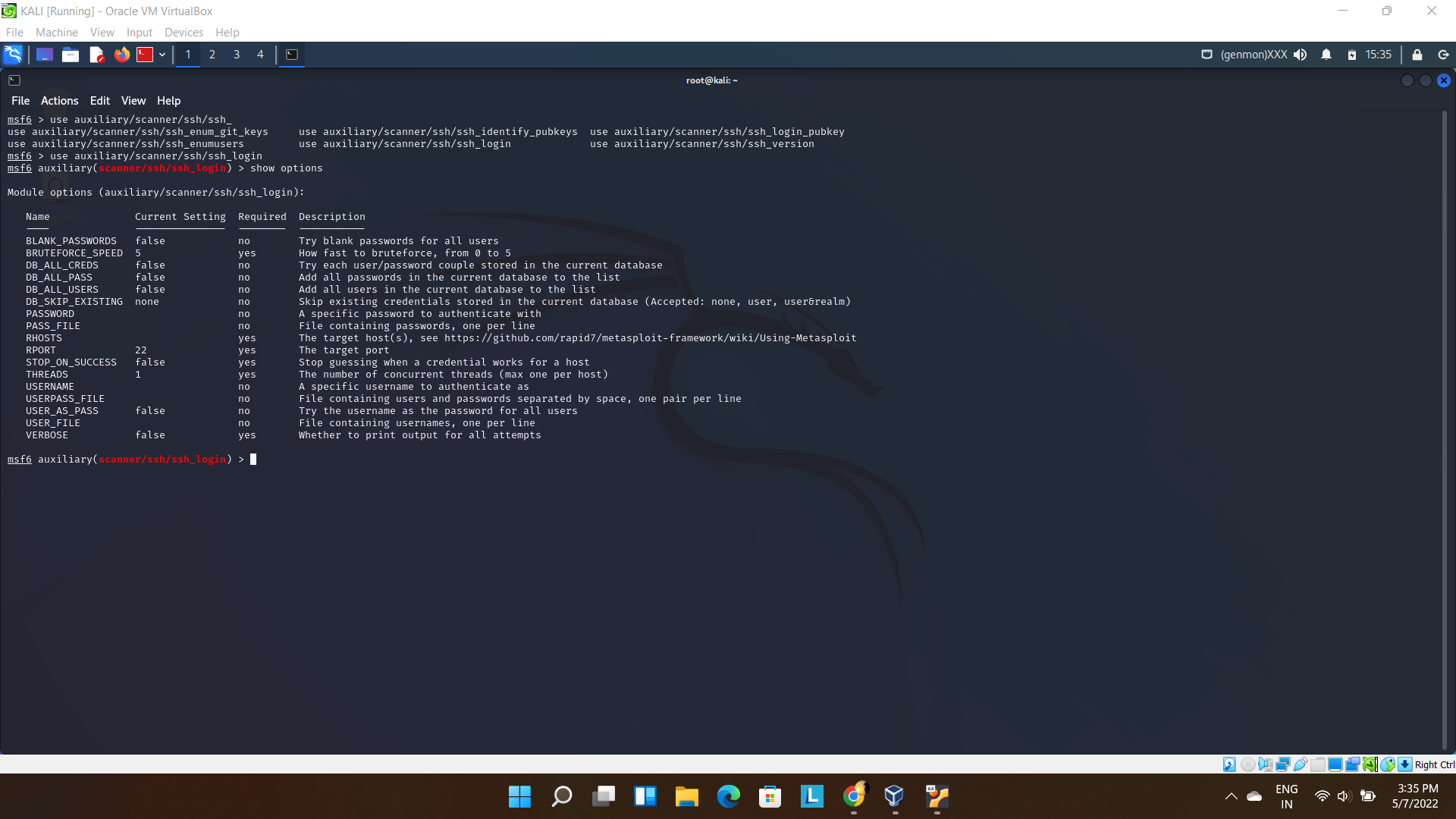
**

Thus, we successfully get the login and password.

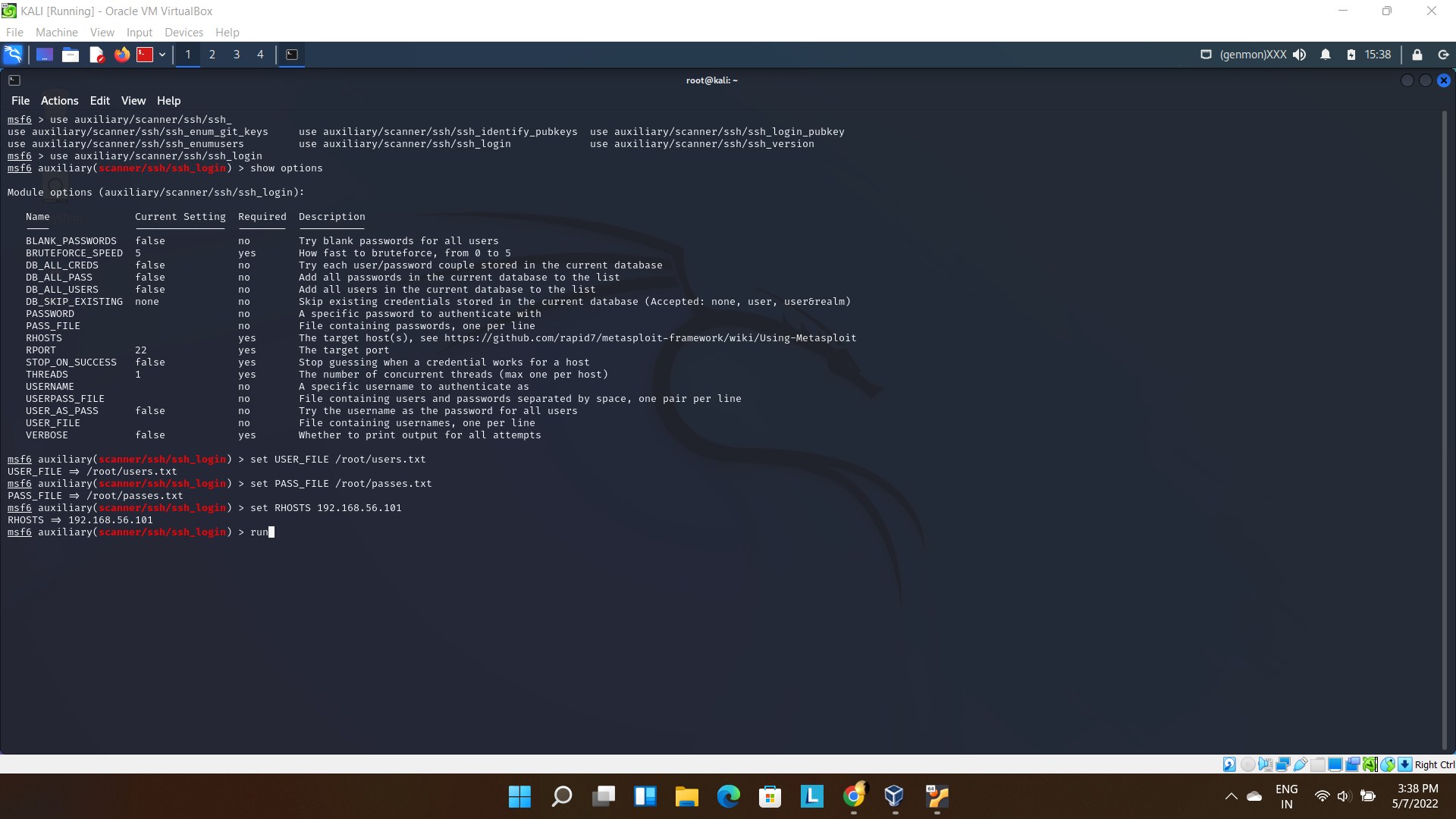
*Password Attacks using Auxiliary Module: -*

For this we start with using msfconsole: 

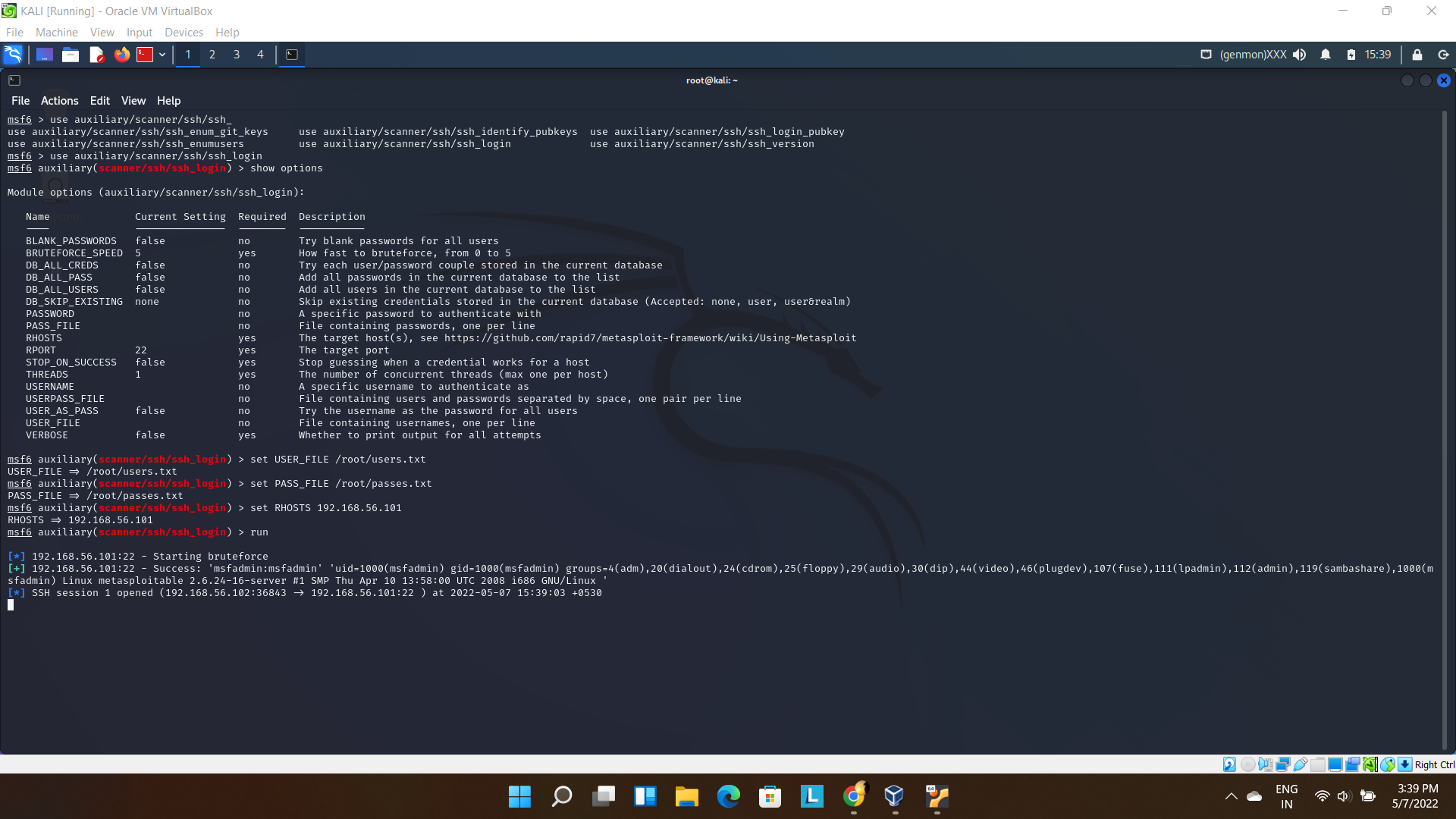
Going further:



Then I set the files containing probable usernames and passwords along with target ip address:

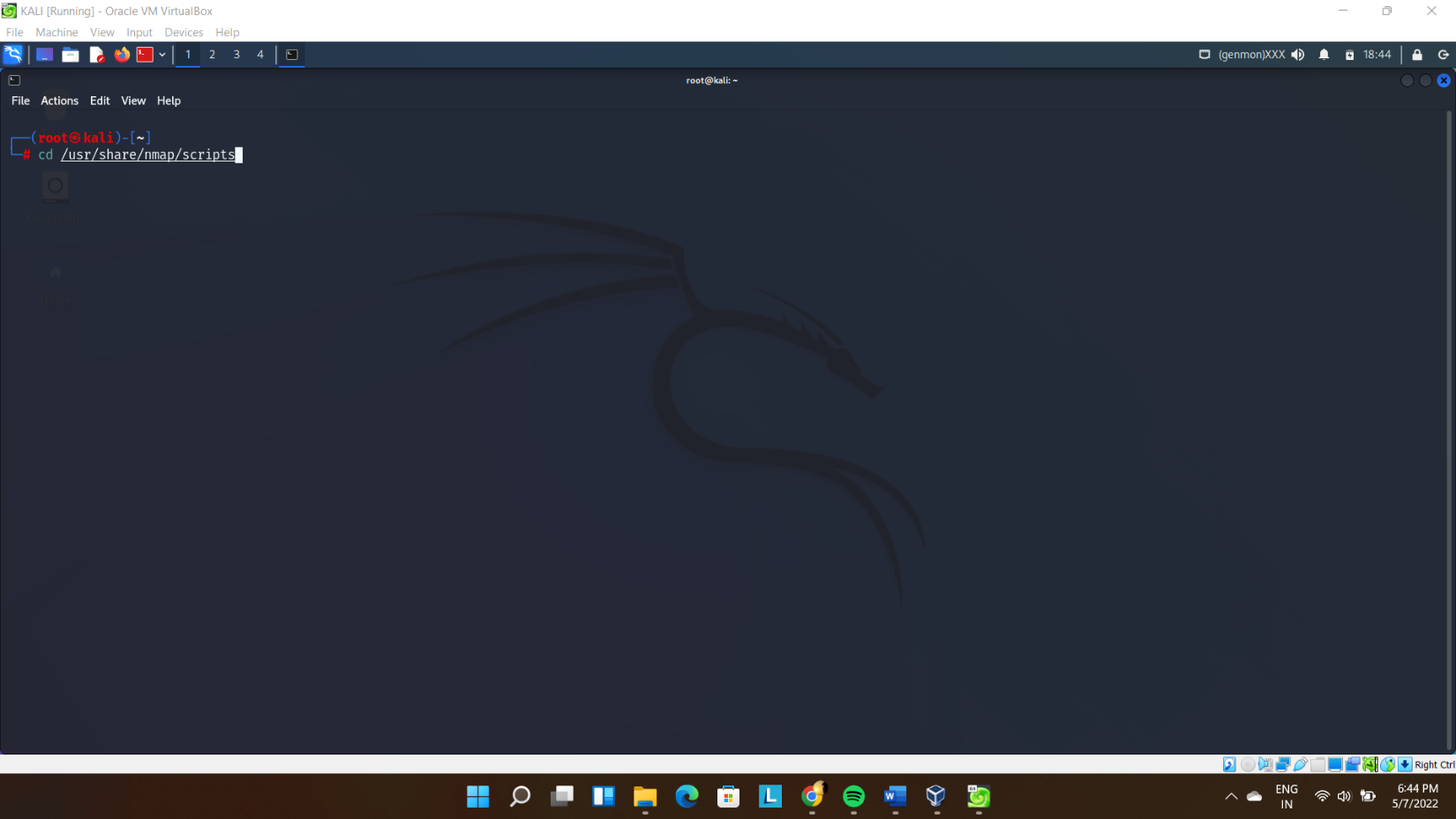


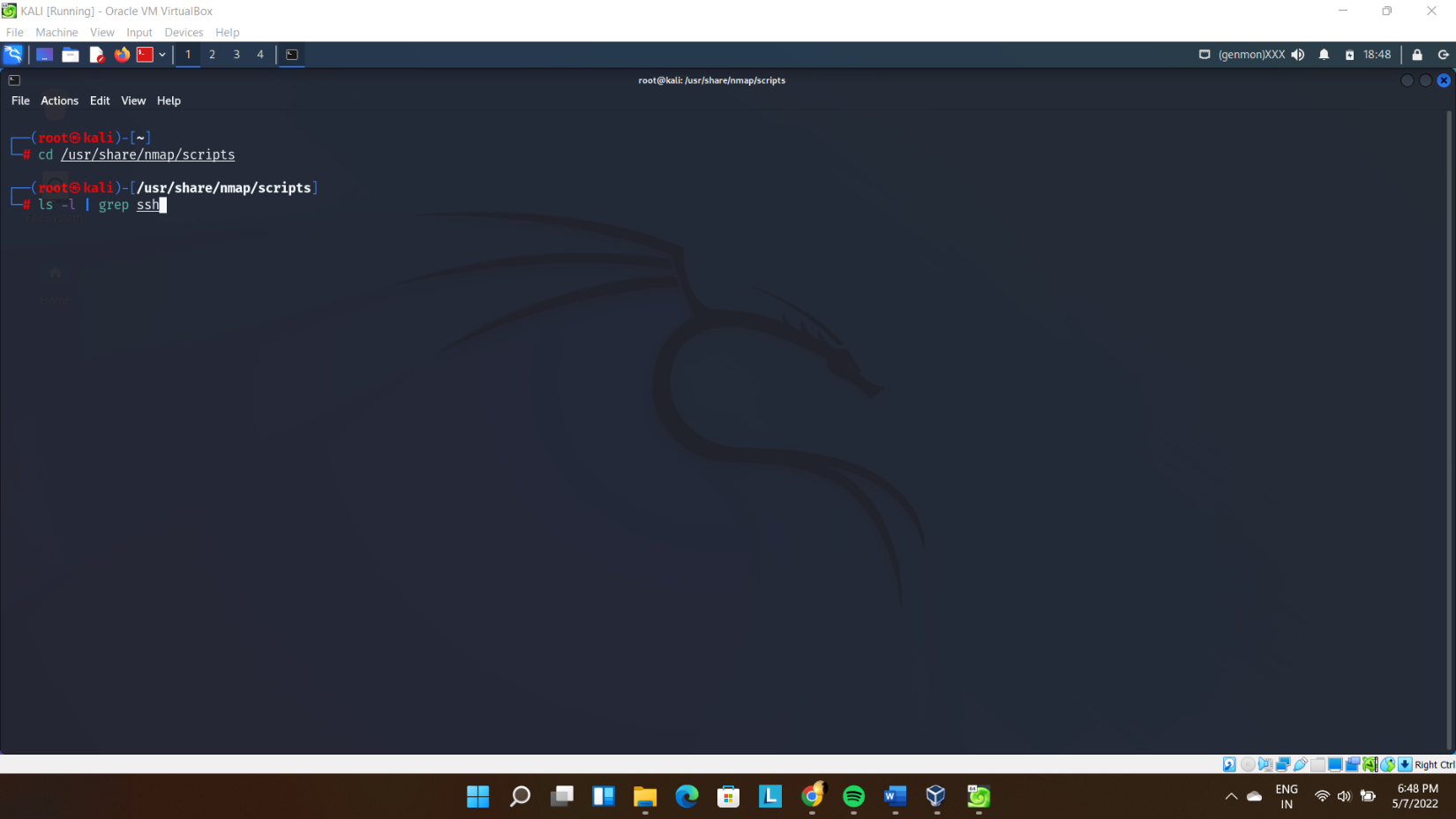
Finally, successfully got the following result:



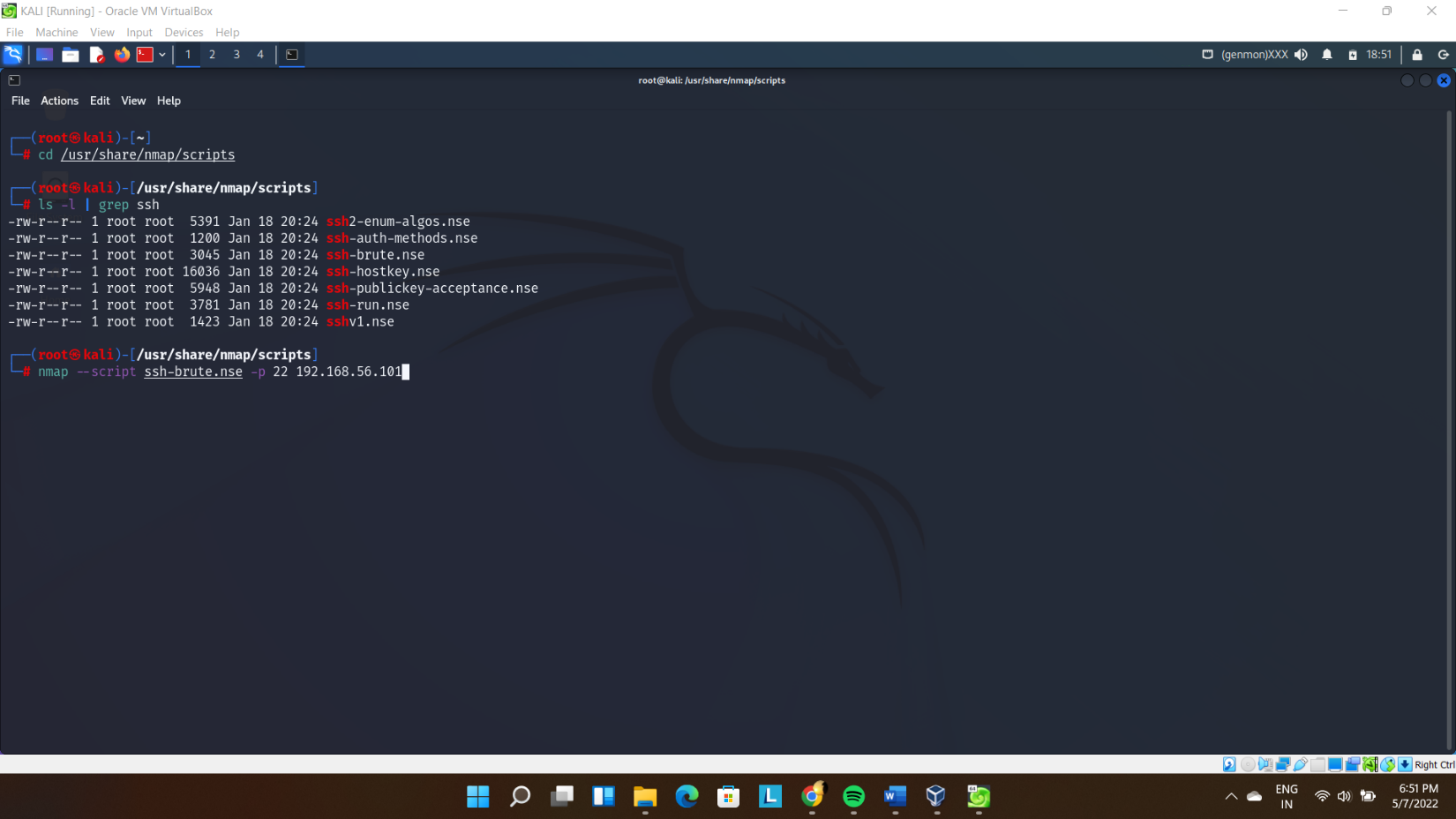
*Password Attacks using**NSE Scripts: -*

Changing the directory to the one where NSE Scripts are present:

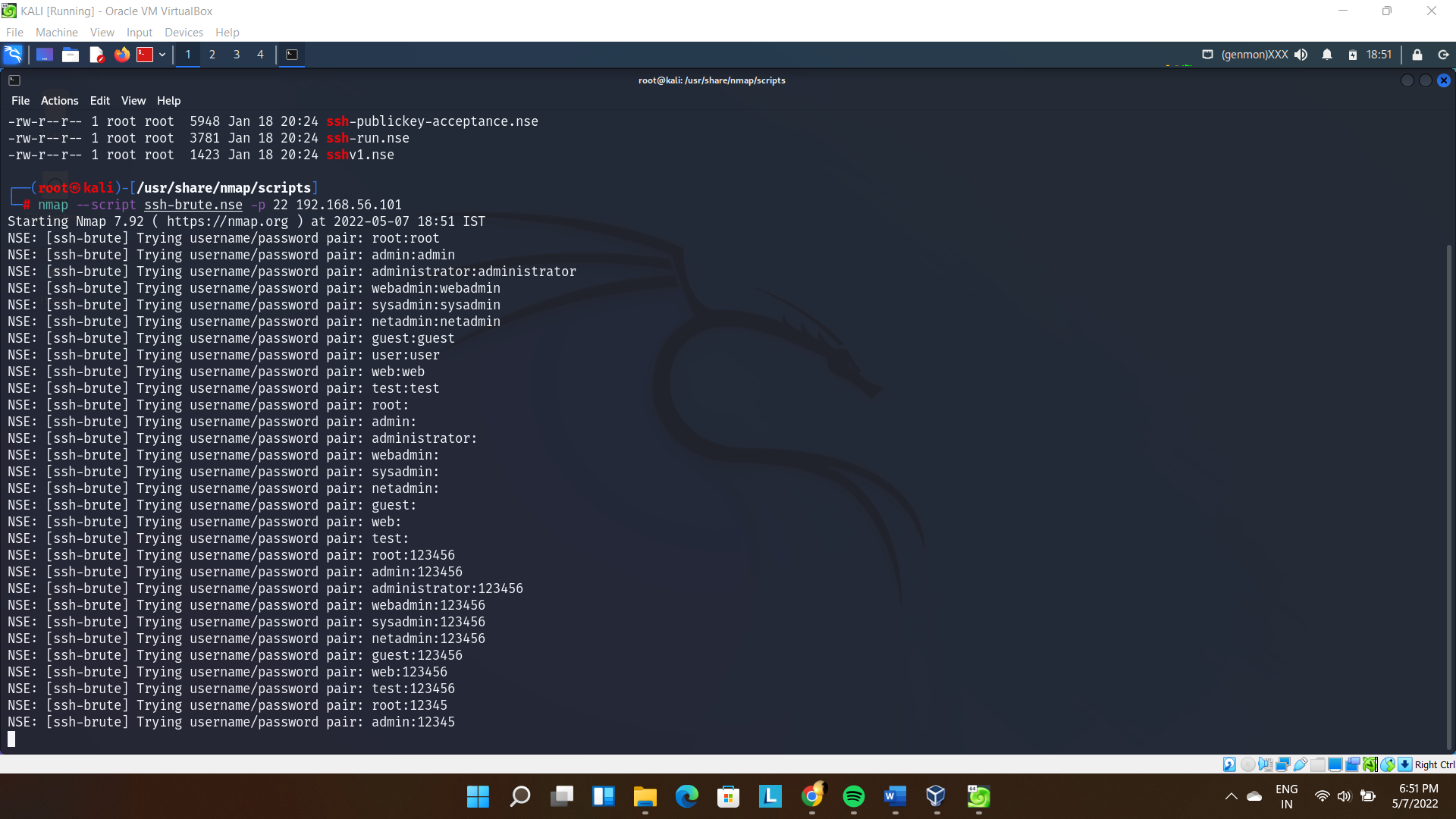


Listing the Scripts involving ssh:

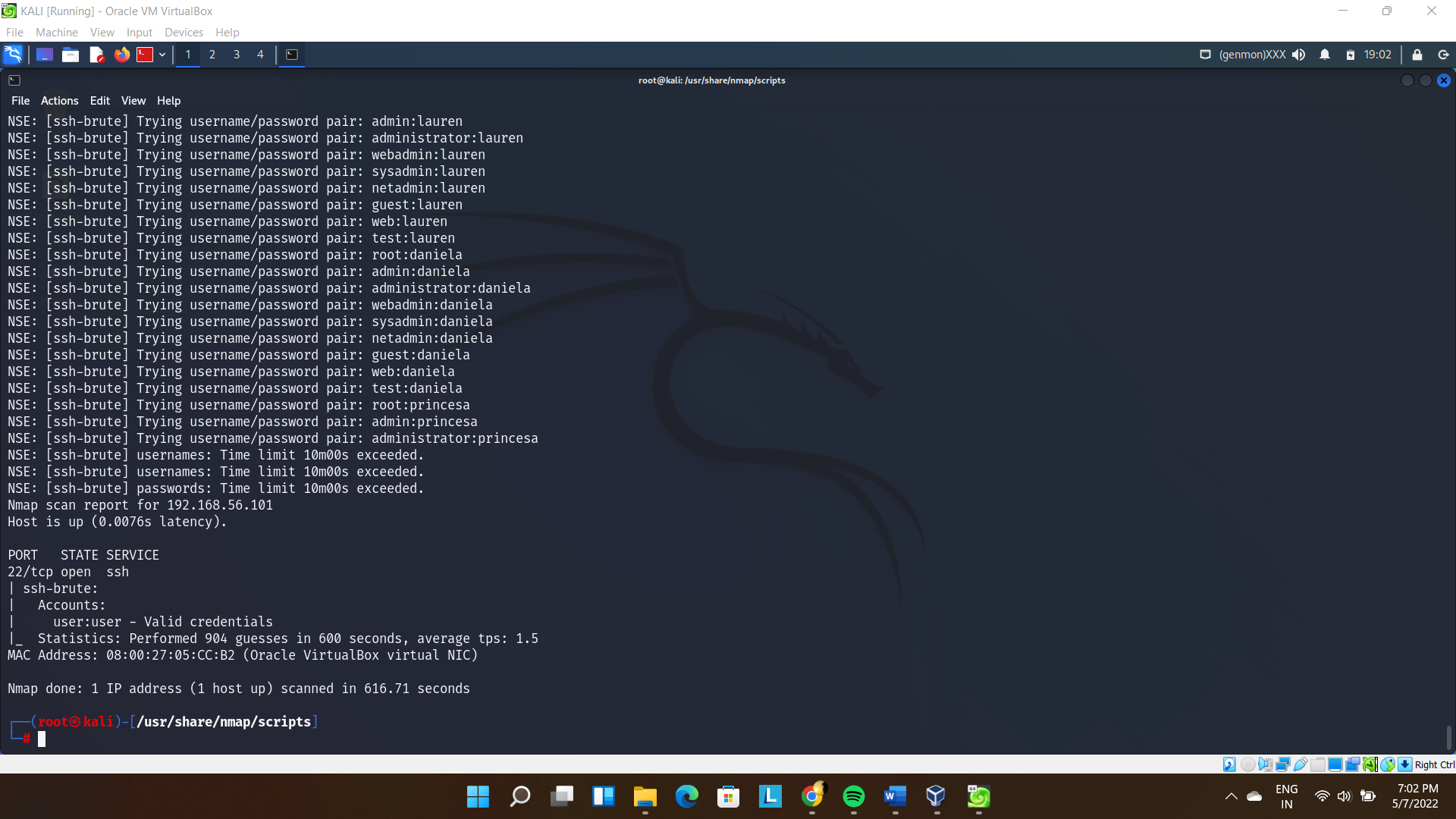
Executing the required script (brute force) with port 22(ssh) and target ip address:



Brute Force NSE script starts:

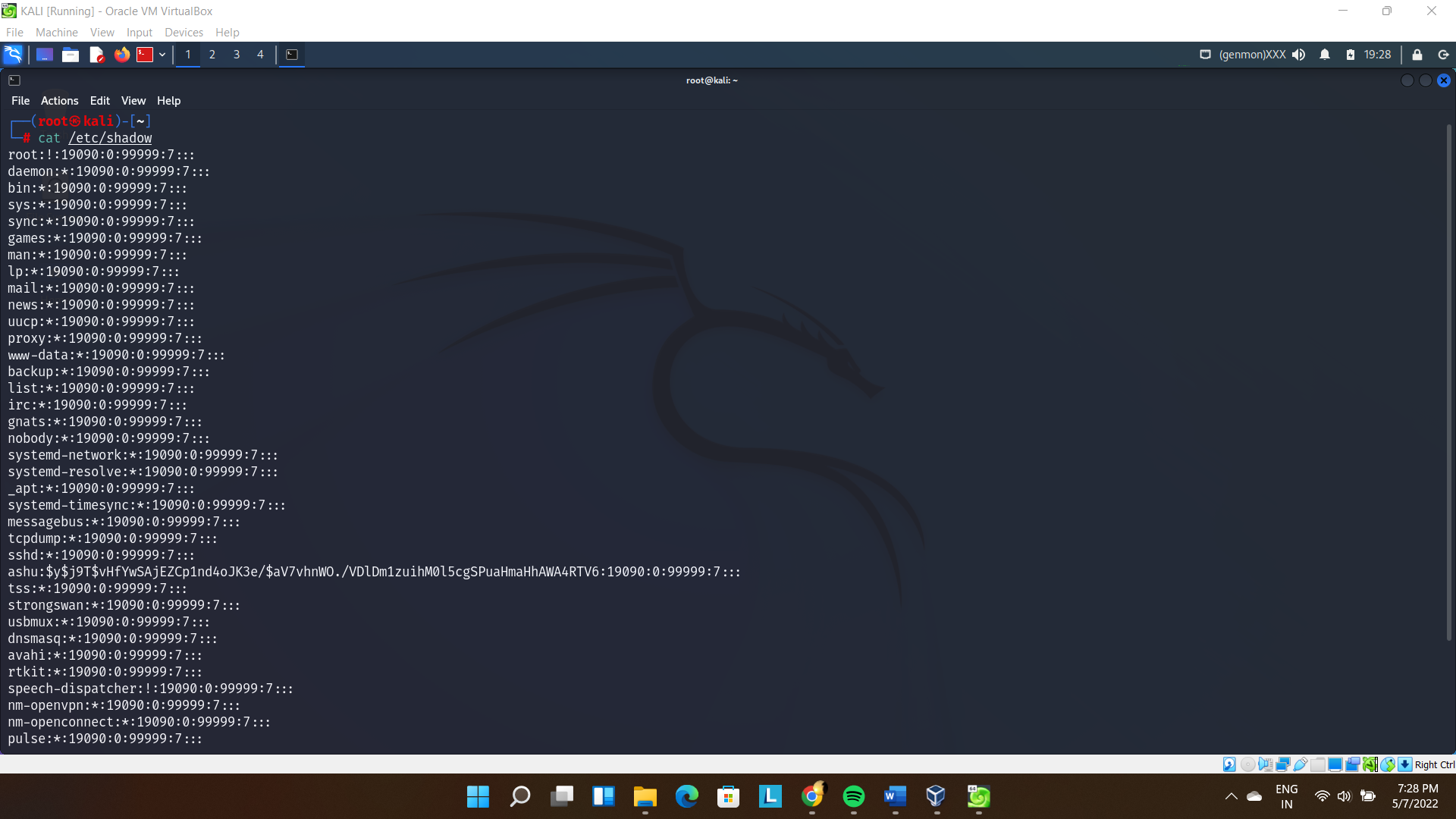


Finally the Outcome:

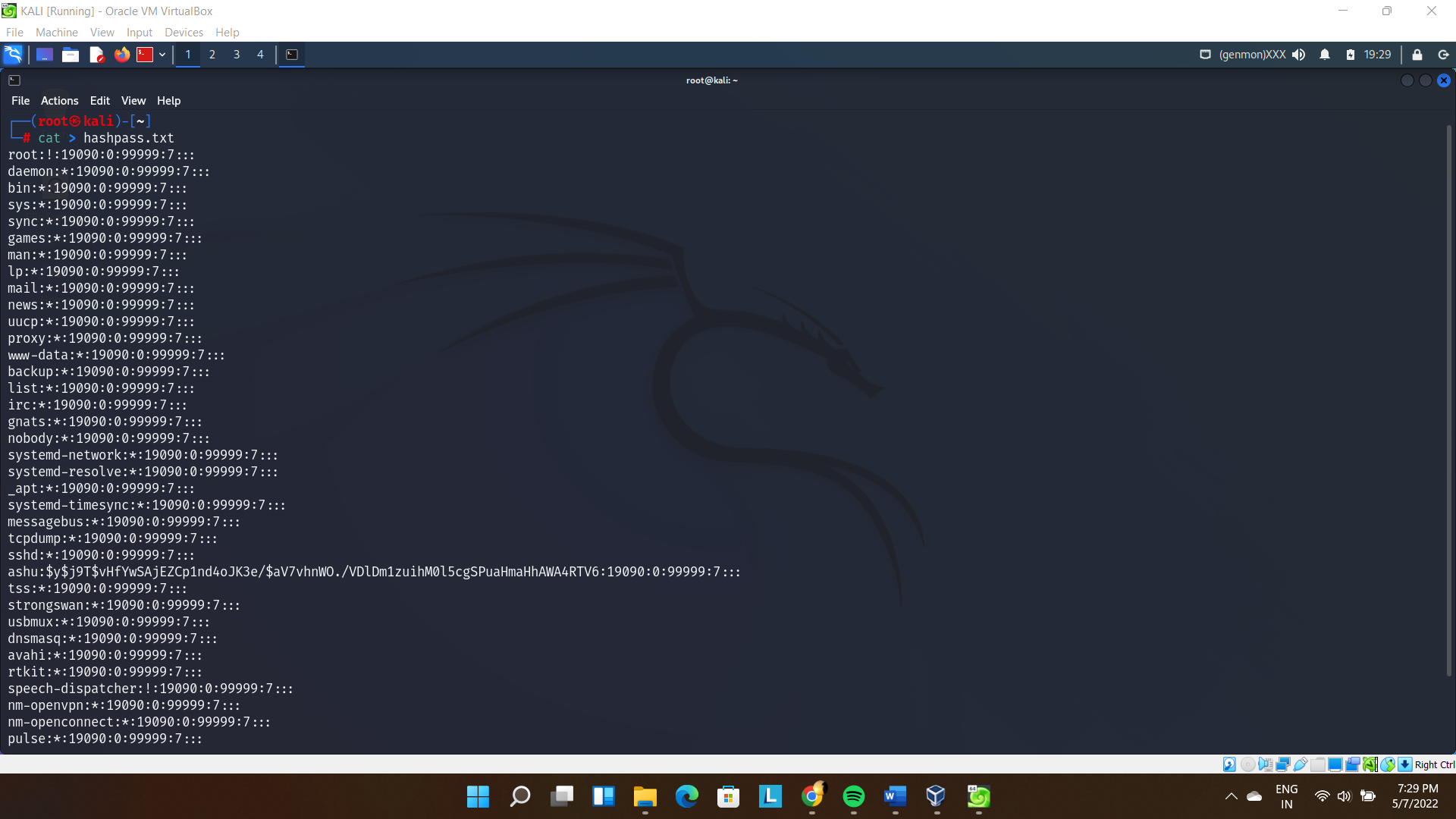


*Password Attacks using**John the ripper: -*

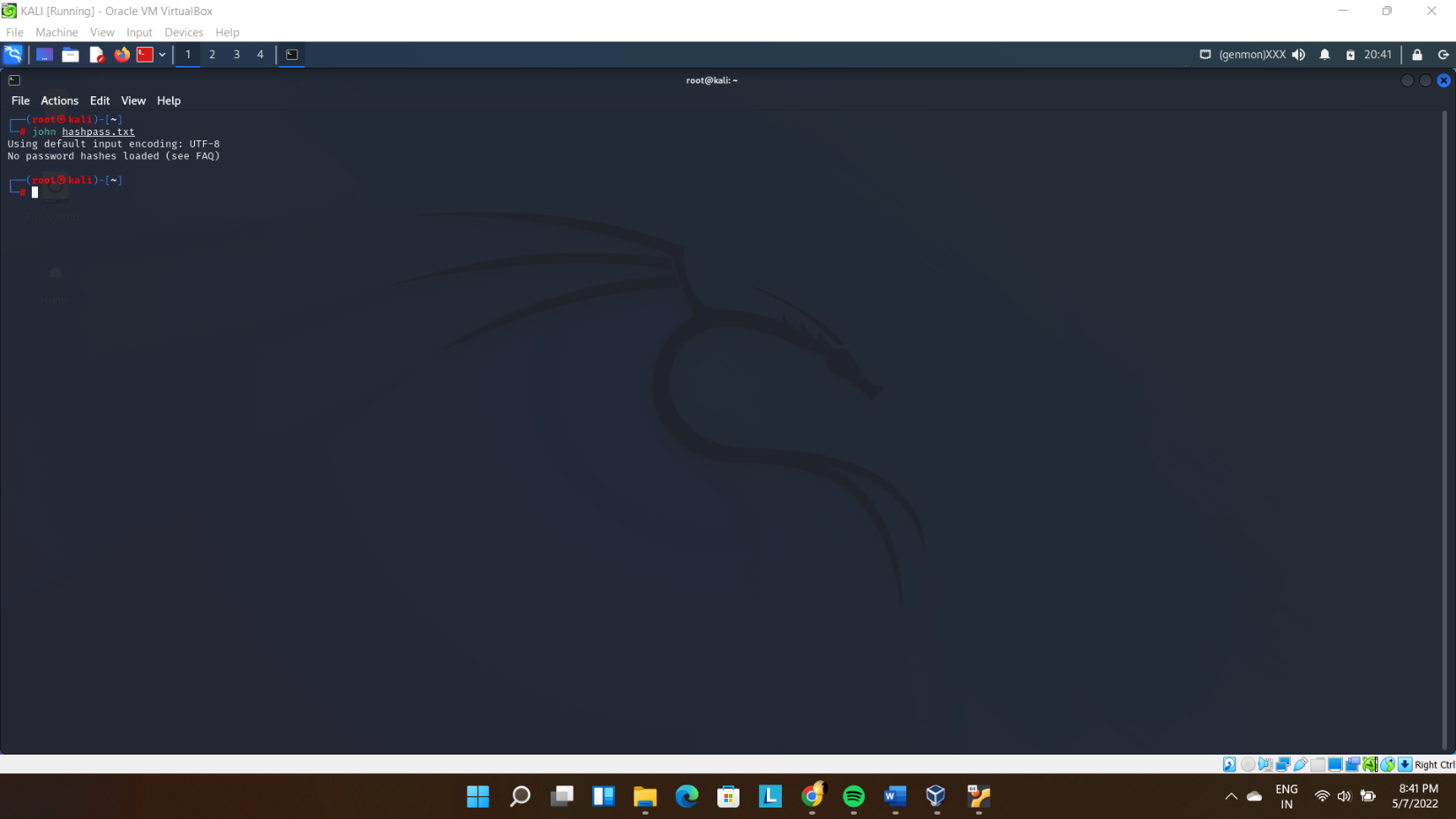
Starting with opening the file where hashes are stored:



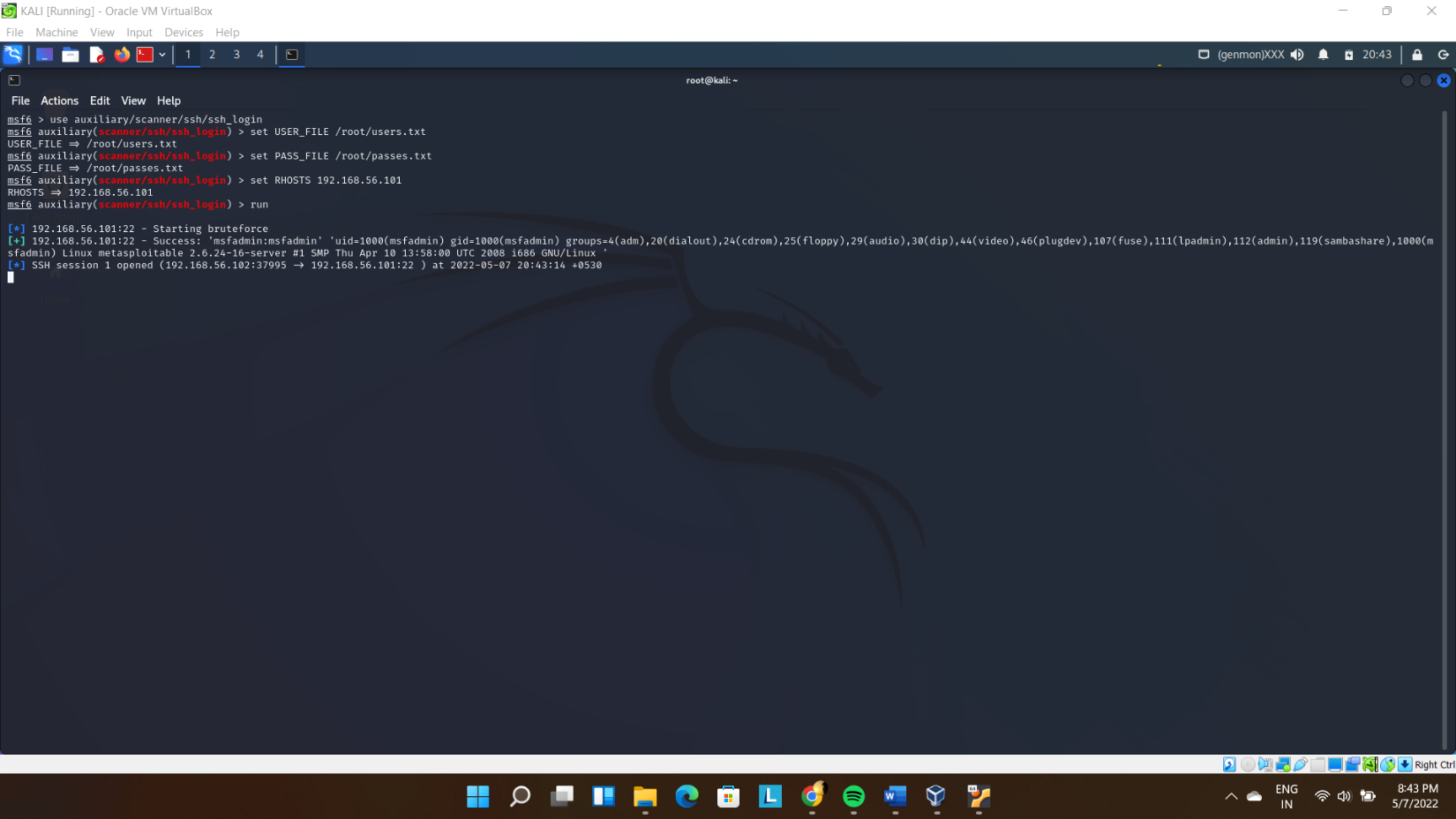
Creating and concatenating file for john to decrypt:

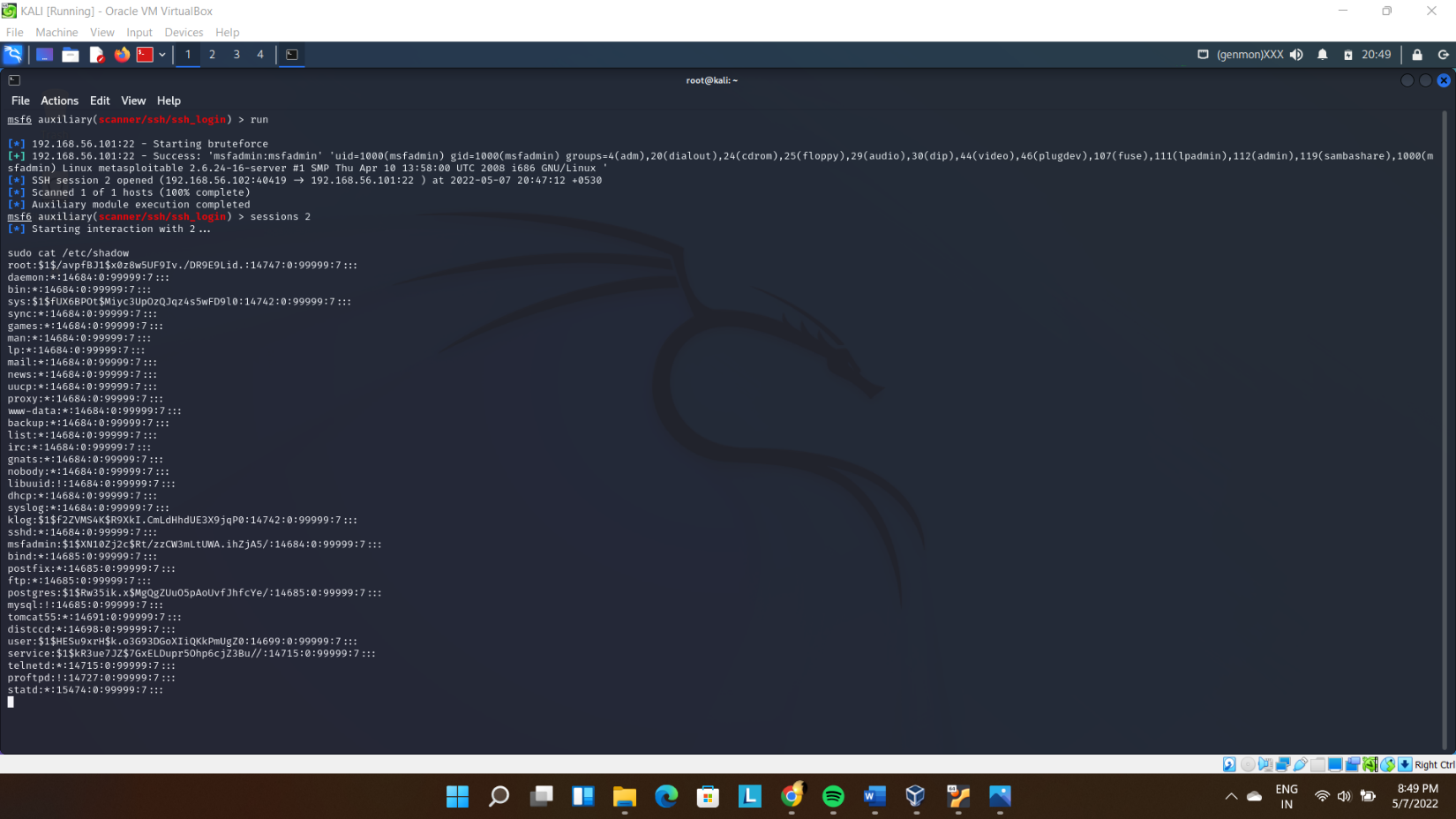


Executing this file with john showed this (as there are no default passwords in my kali installation):

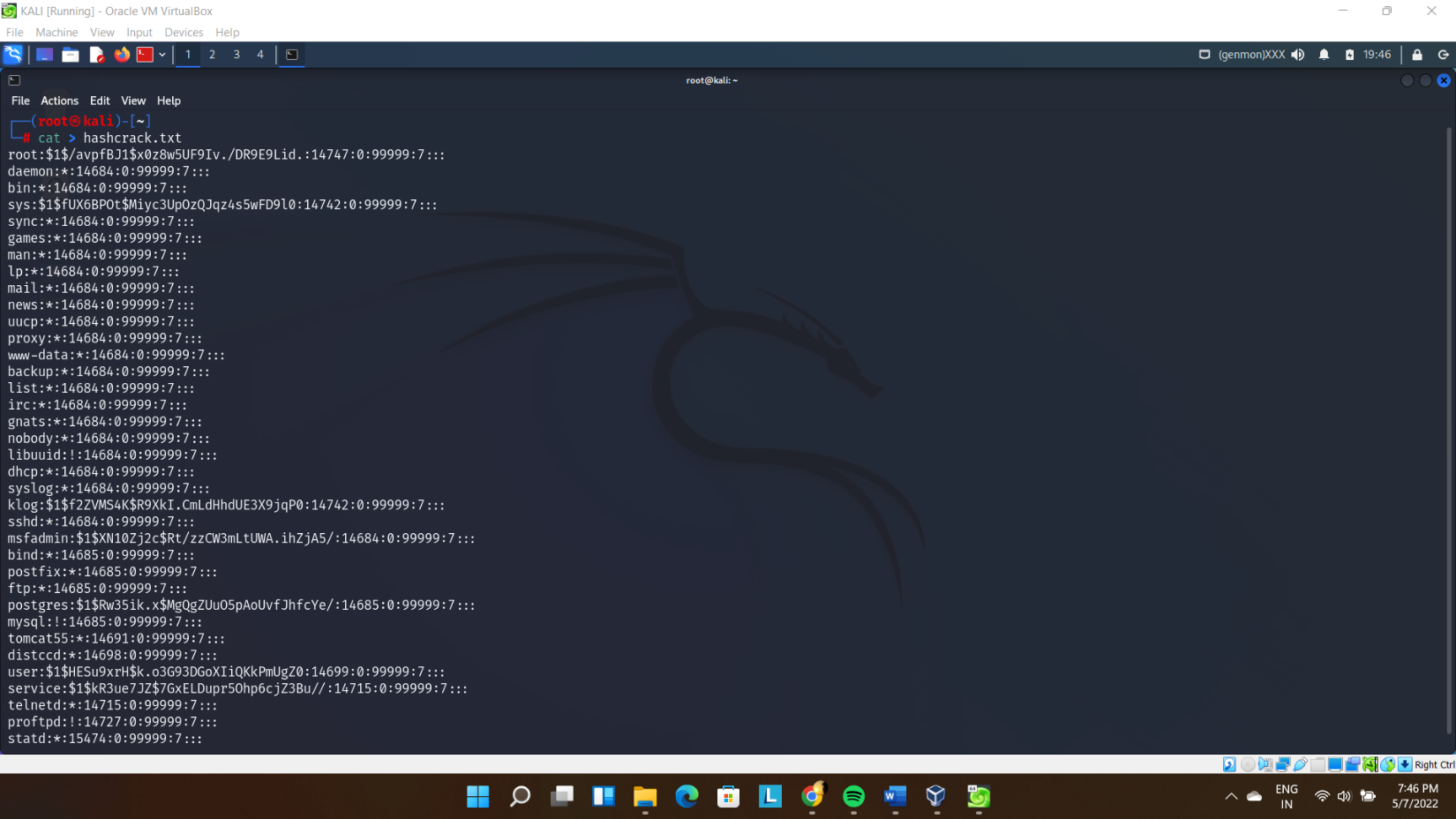


Therefore, I went ahead with doing the same with Metasploit Linux:

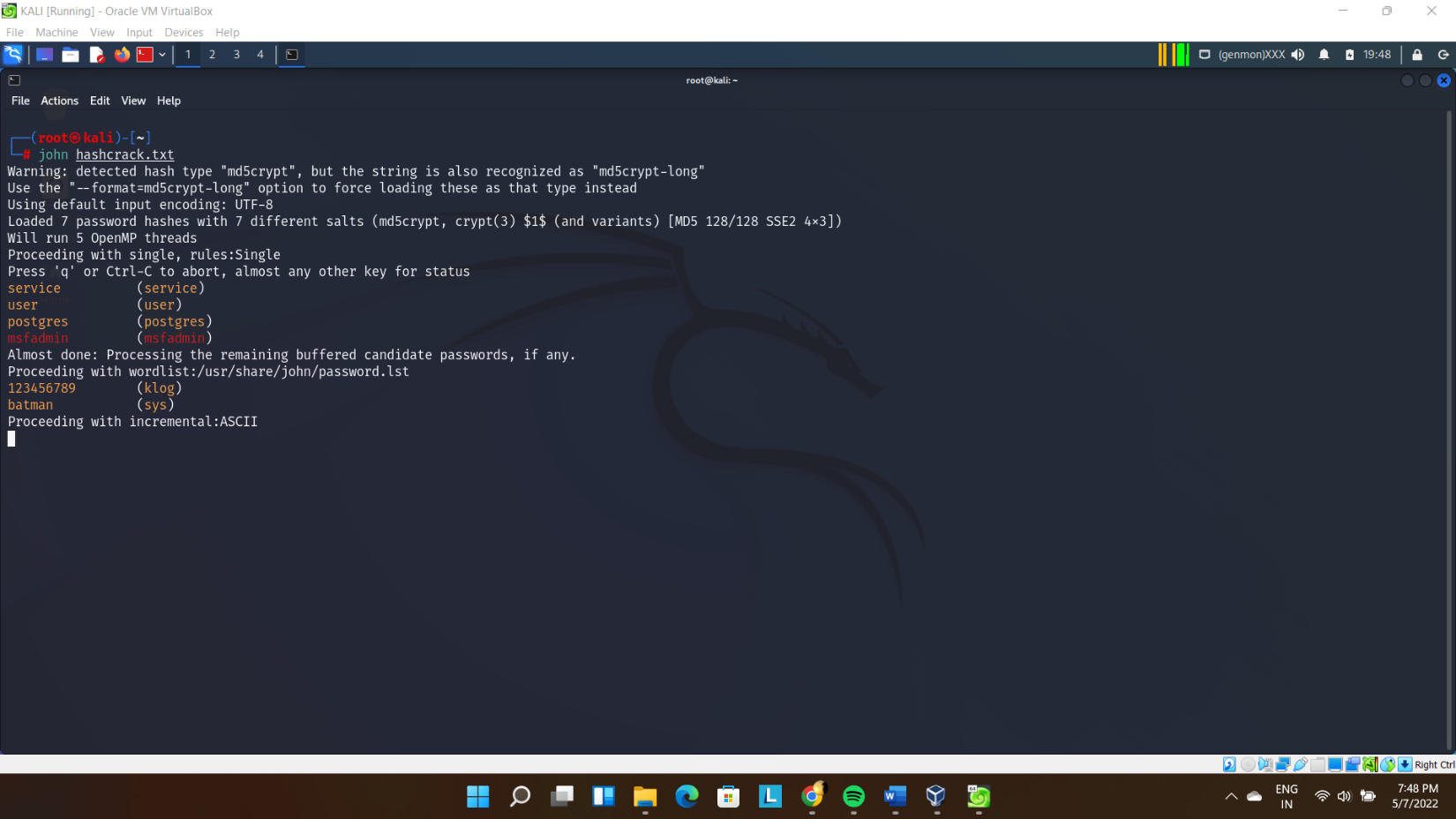




Creating and concatenating new file:

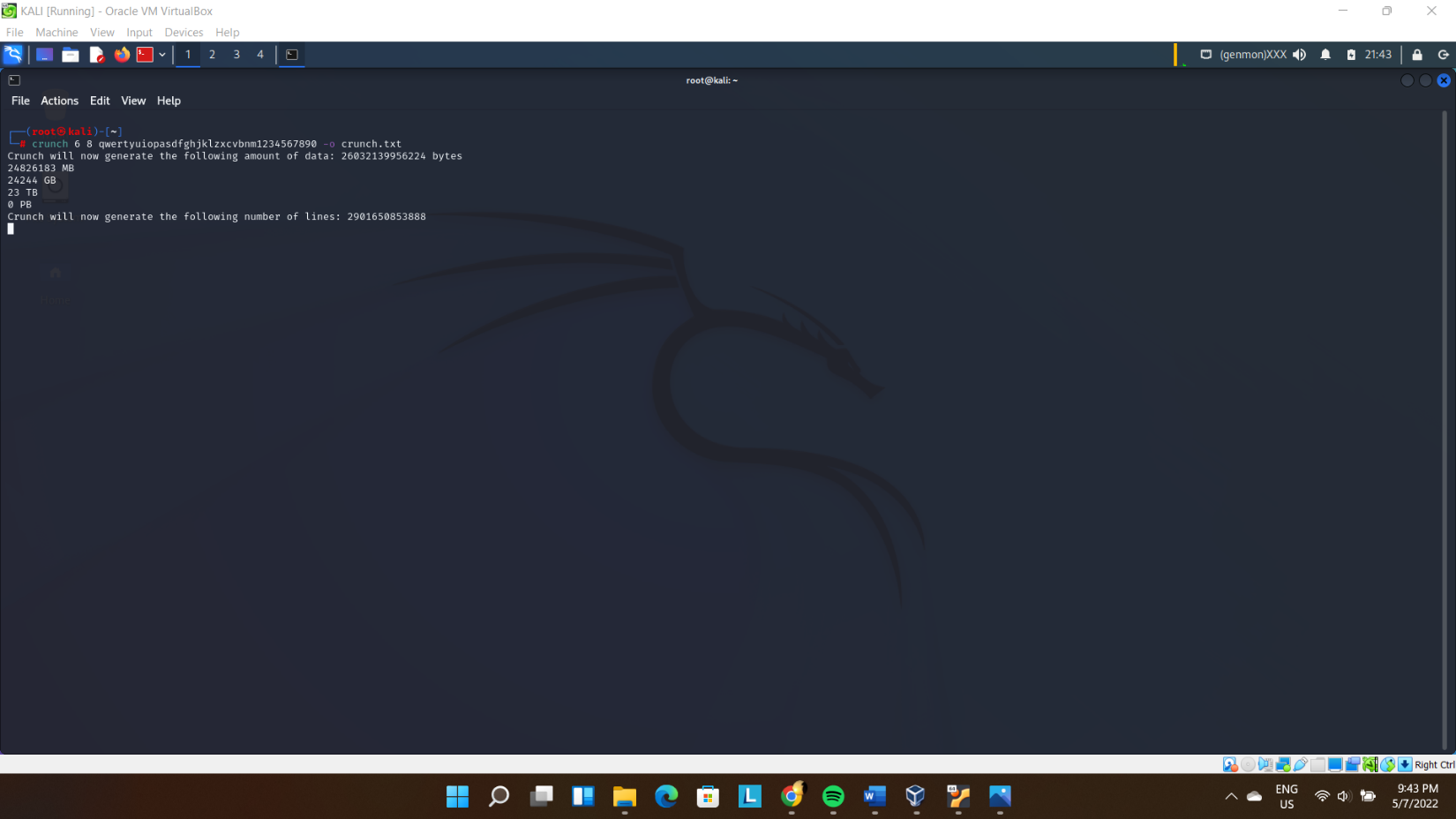


Finally, I got the following details:



*Password generating using Crunch: -*

Generating passwords:



Generating customized passwords:

