**Name: Shangirne Kharbanda**

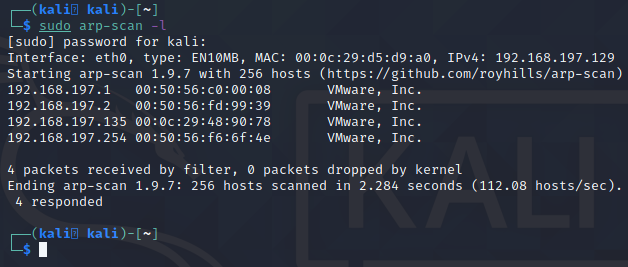
**Registration Number: 20BAI1154**

**LAB-8 ISM**

**HACK APACHE TOMCAT VIA MALICIOUS WAR UPLOAD**

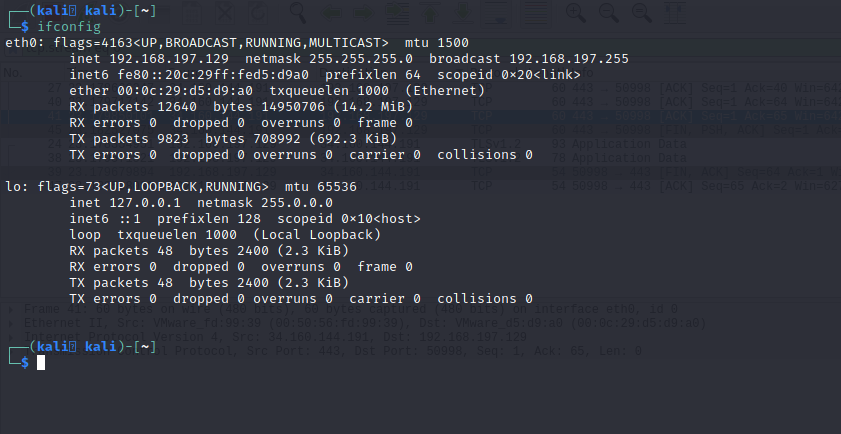
**1. AUTOMATIC ATTACK USING METASPLOIT**

We first check our IP of Metasploitable2 i.e. the target machine by running arpscan as shown below.

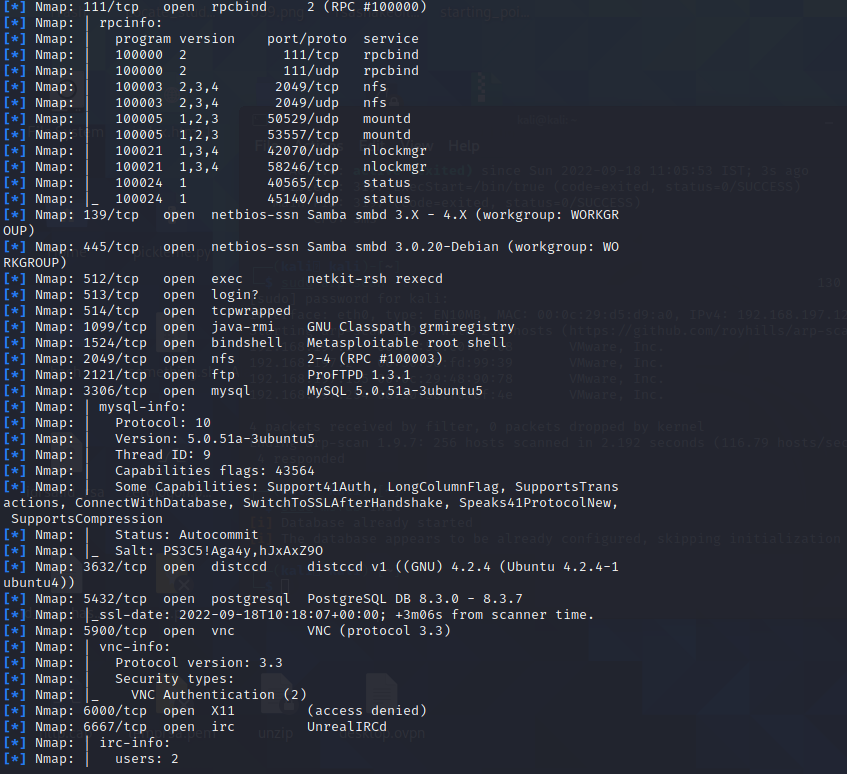


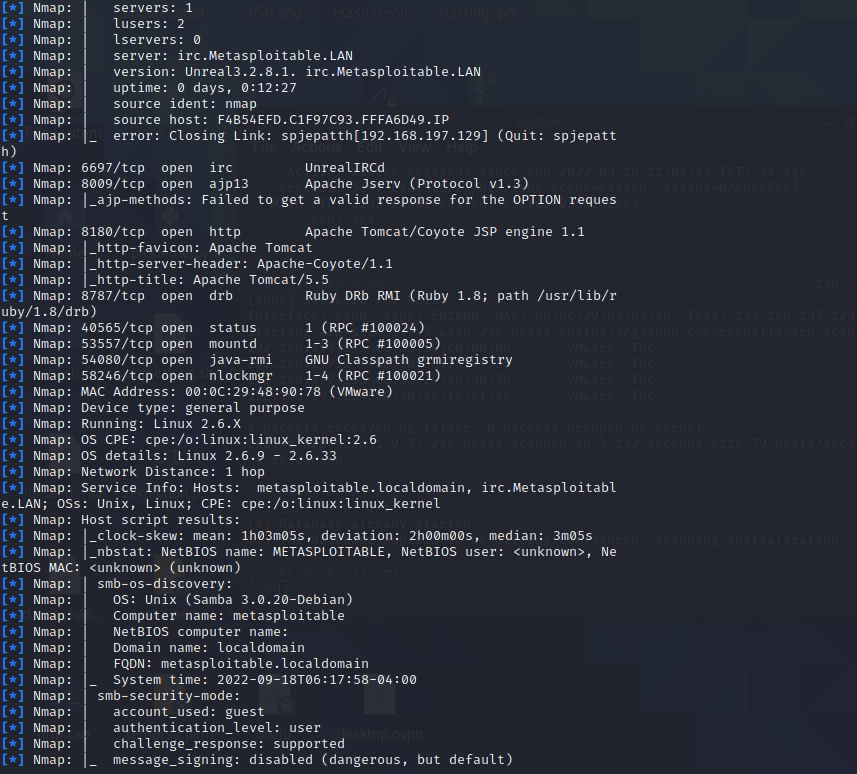
IP of Metasploitable2 is **192.168.197.135**

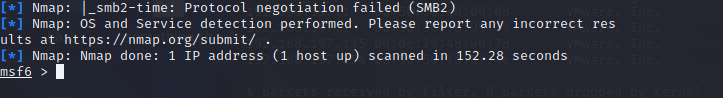
We will check IP of Kali by using ifconfig in Kali.



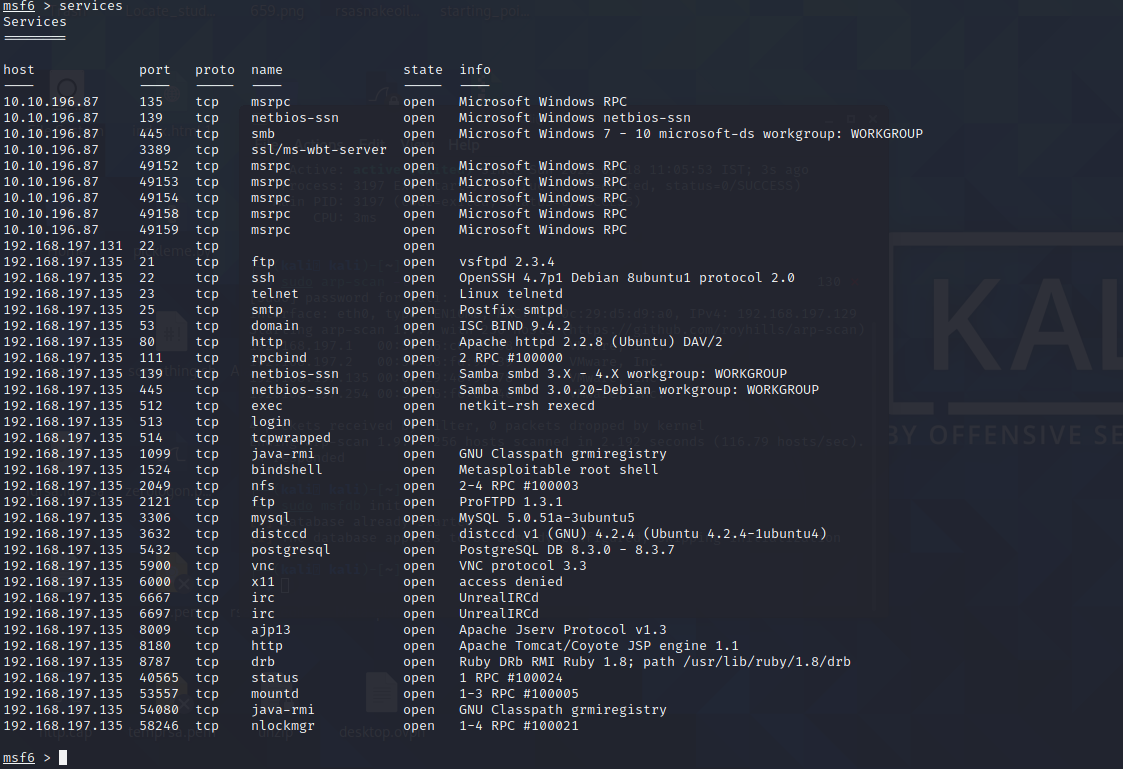
IP of Kali machine is **192.168.197.129**

Now we will start up msfconsole and run an Nmap scan on the machine in metasploit to see which ports and services are open

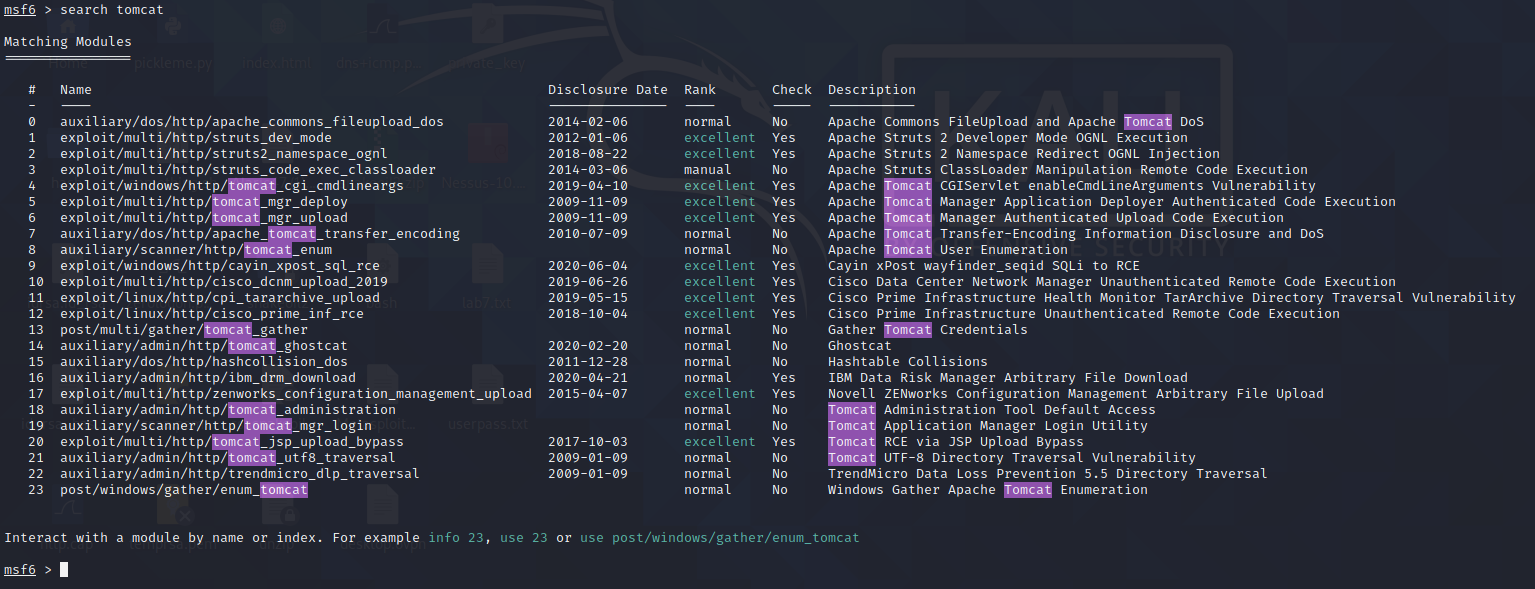




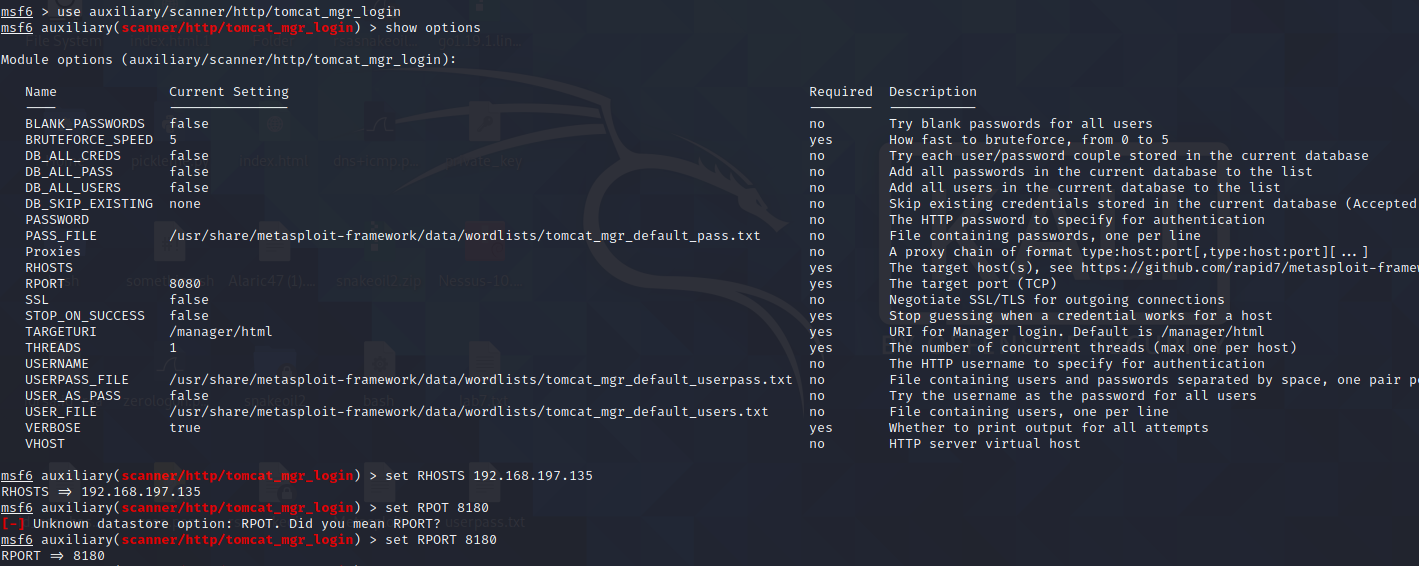
To see which services are open on the target machine, we simply type services in msfconsole as we have our nmap scan results now stored in the database.



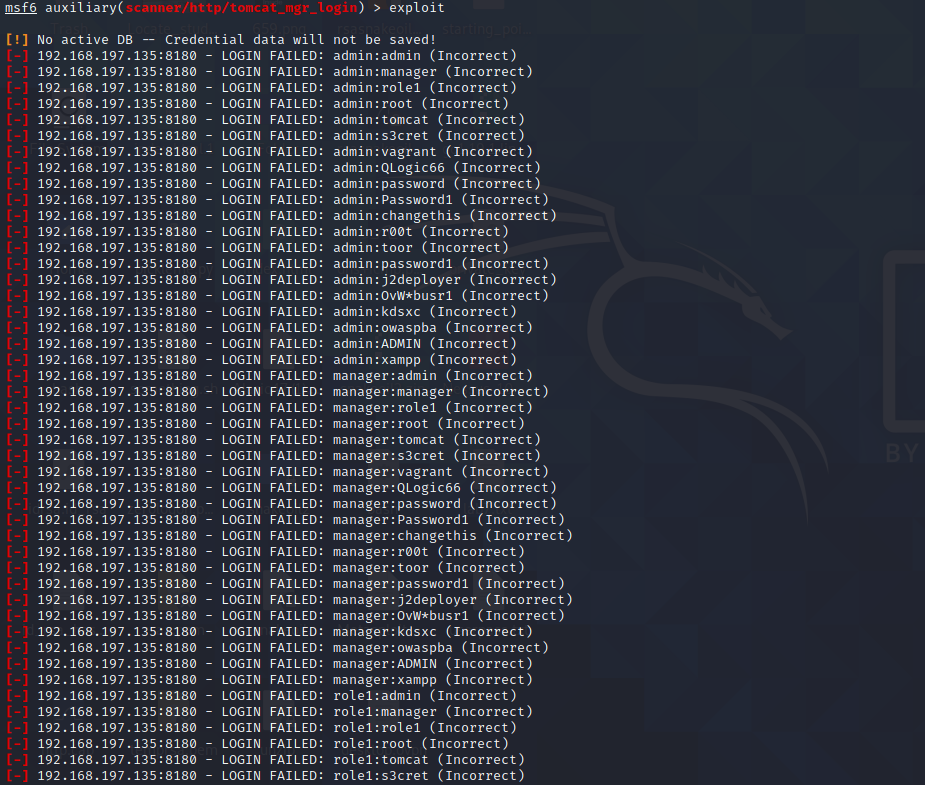
We will search tomcat in metasploit

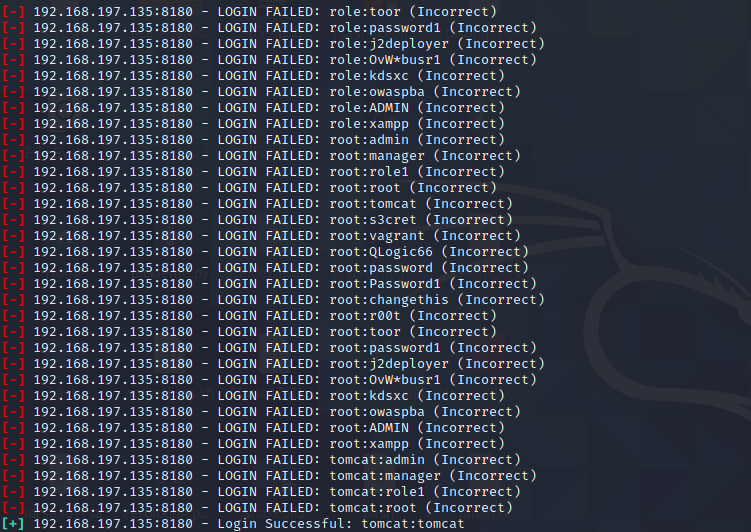


We will use the module **auxiliary/scanner/http/tomcat\_mgr\_login.**

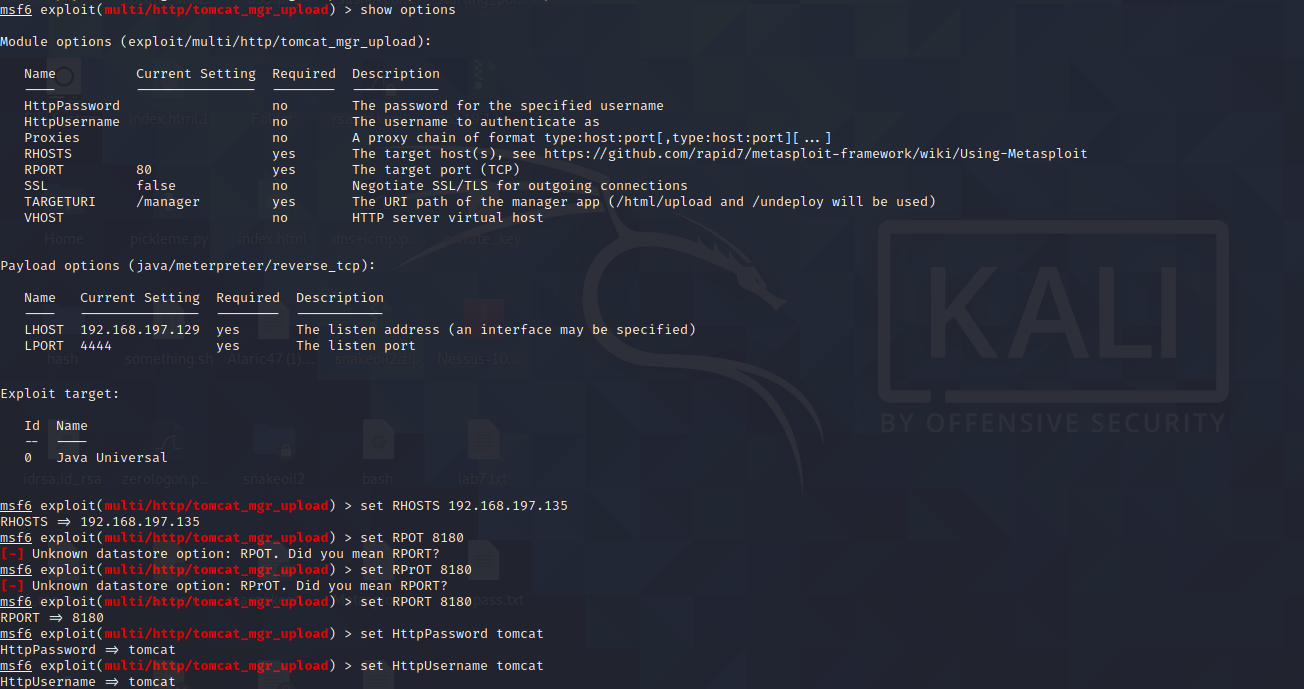


We will now run the exploit

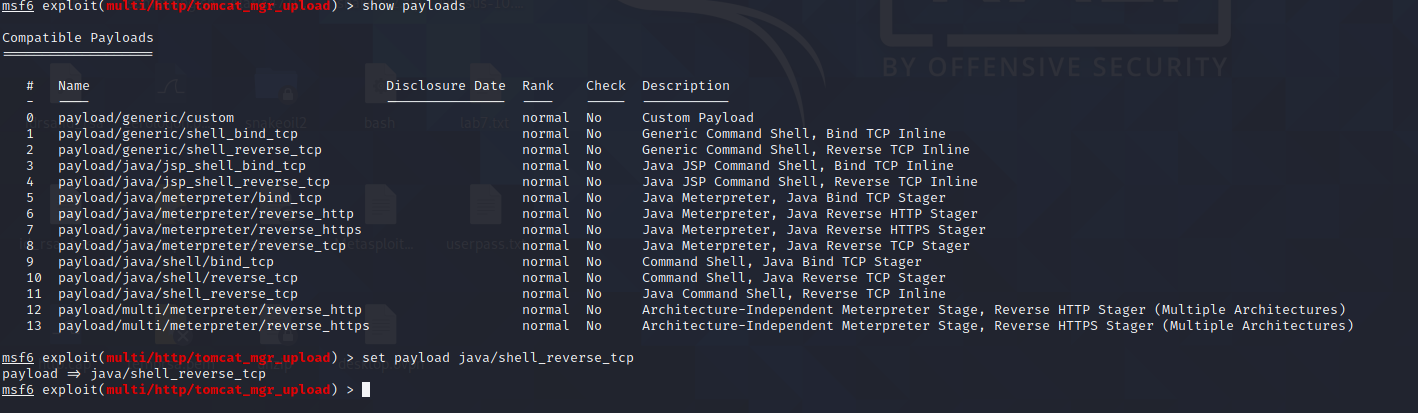




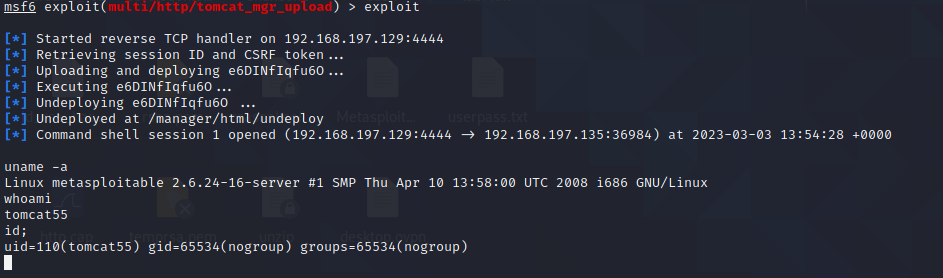
Now we will use module **exploit/multi/http/tomcat\_mgr\_upload and configure it.**

****

Setting payload:

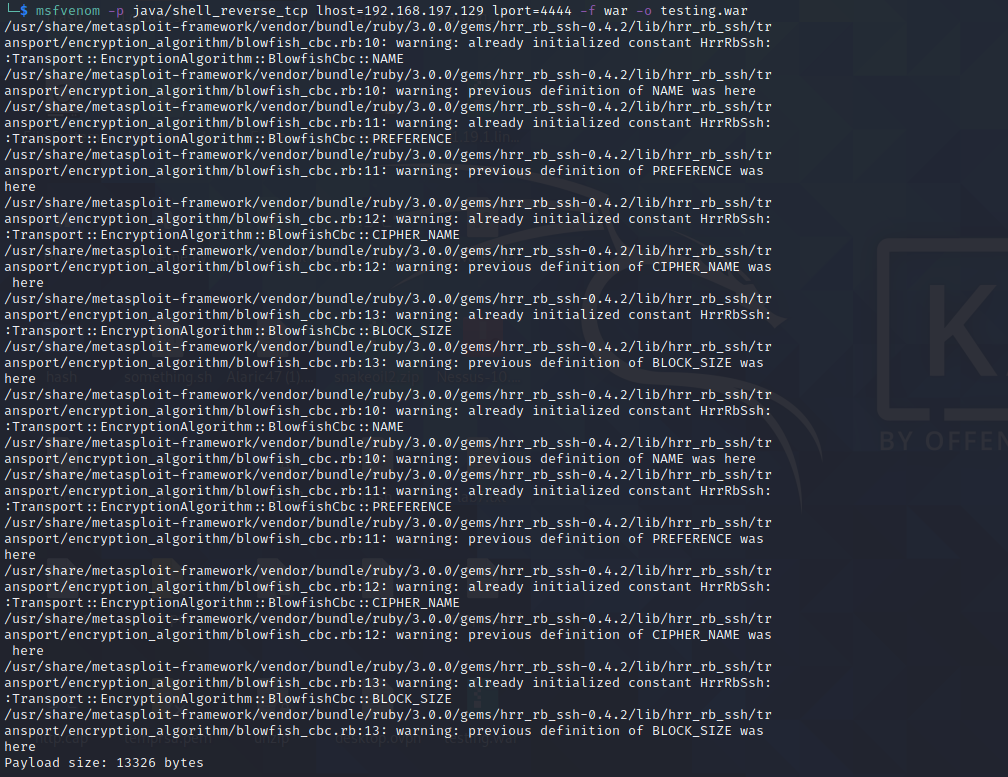


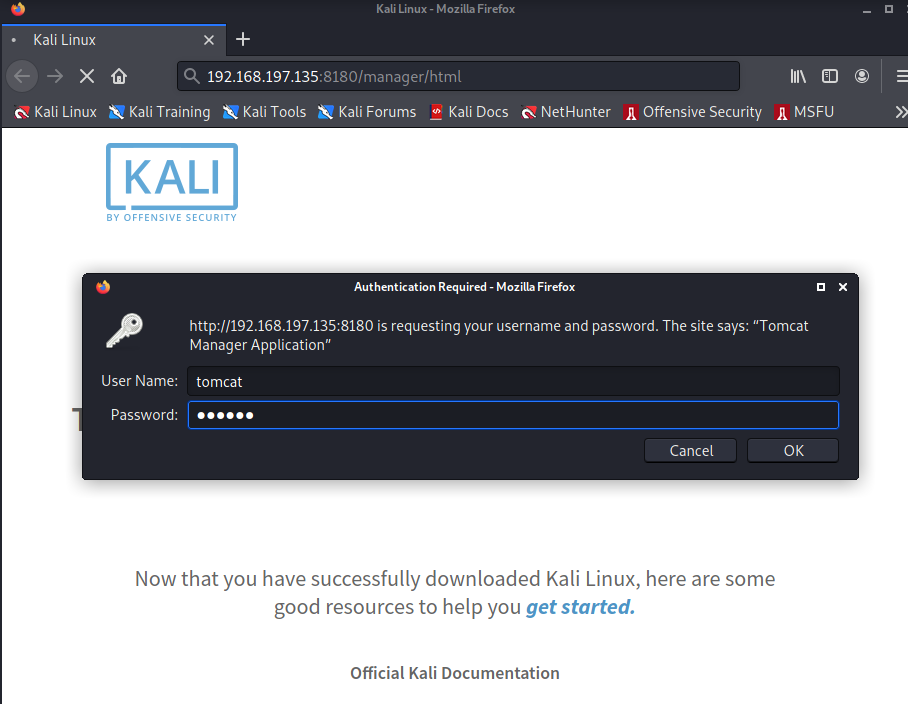
Running the exploit, a shell is opened and we have now breached into the server as shown below:

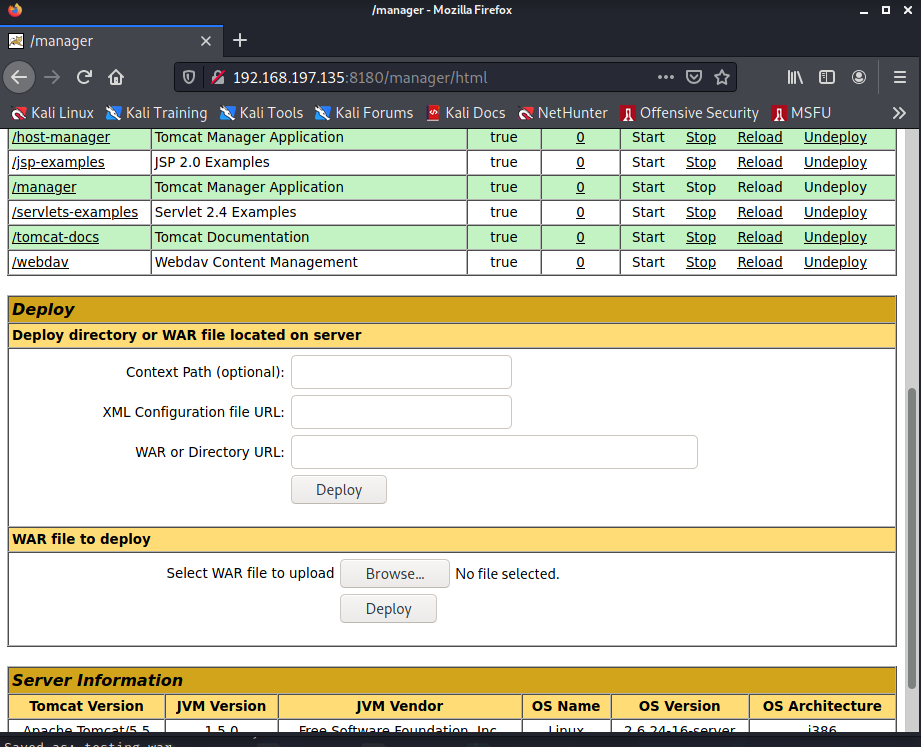


**2. MANUAL ATTACK WITH MSFVENOM**

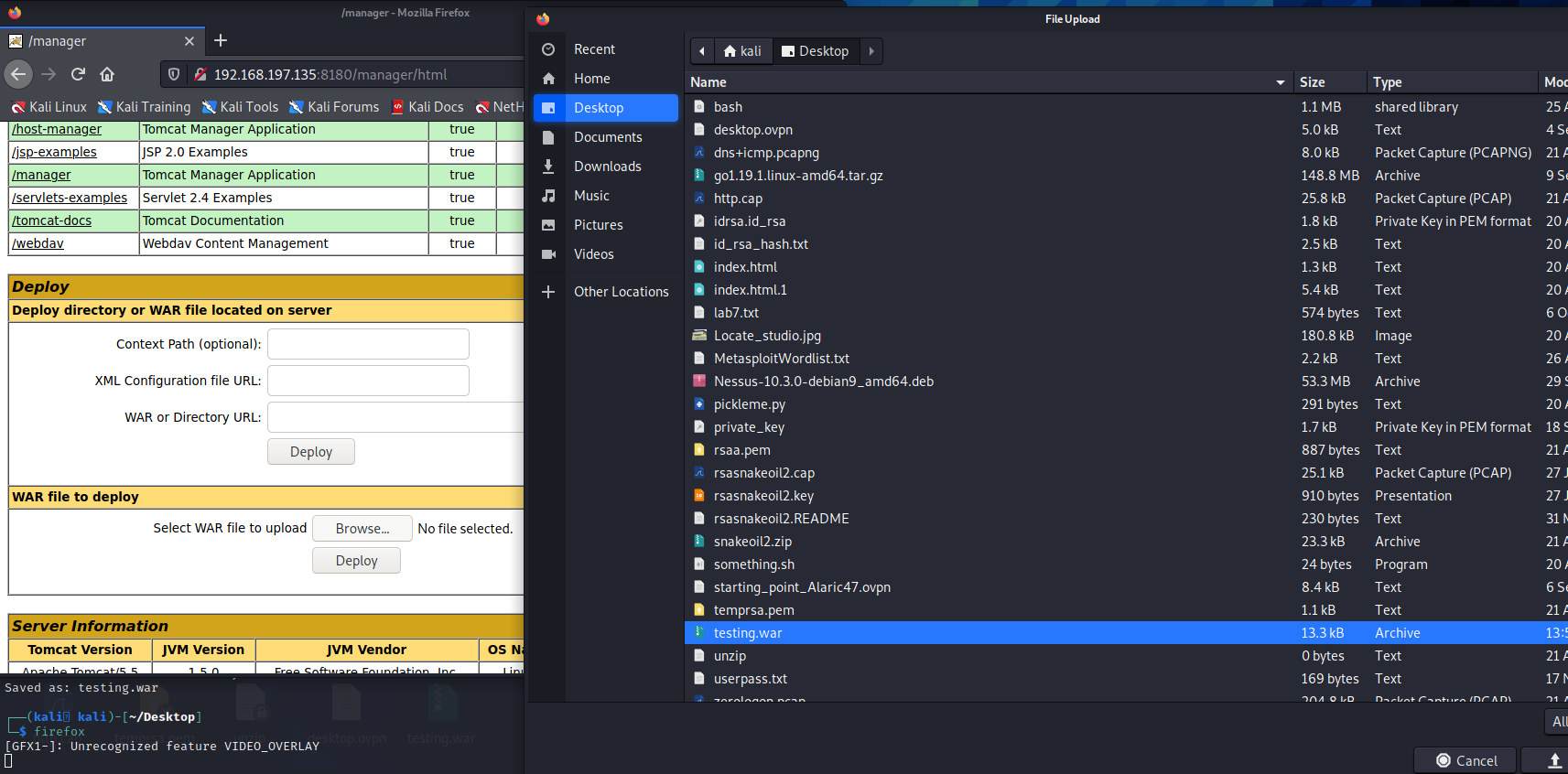
**Creating the payload:**



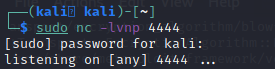
Now we will go to firefox and type in the address and authenticate with our username and password that we know is tomcat and tomcat:



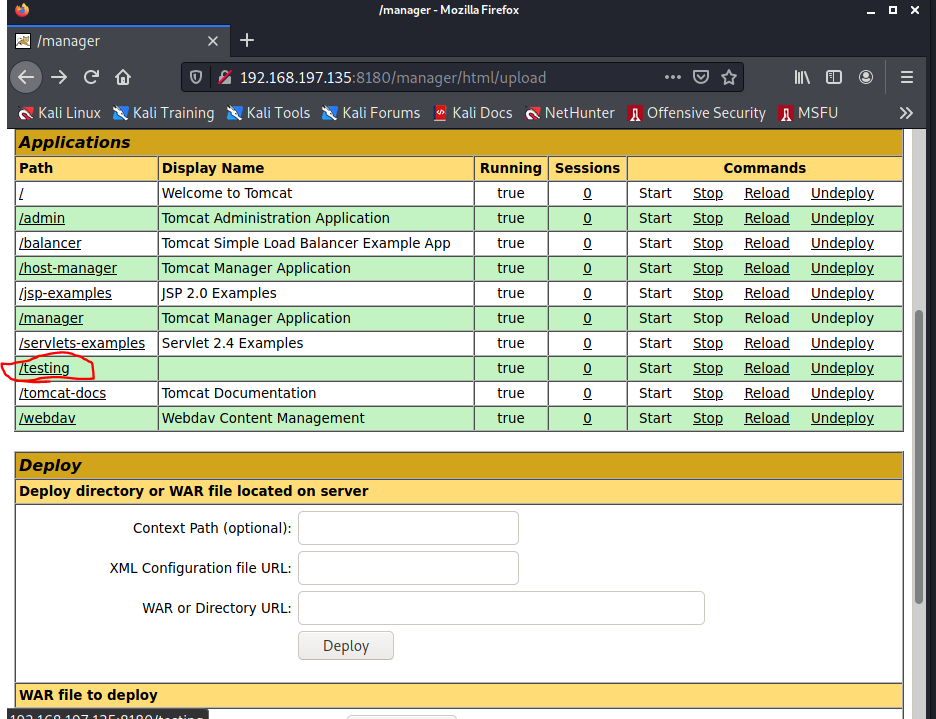
We will browser and deploy the testing.war payload on the Apache tomcat server.



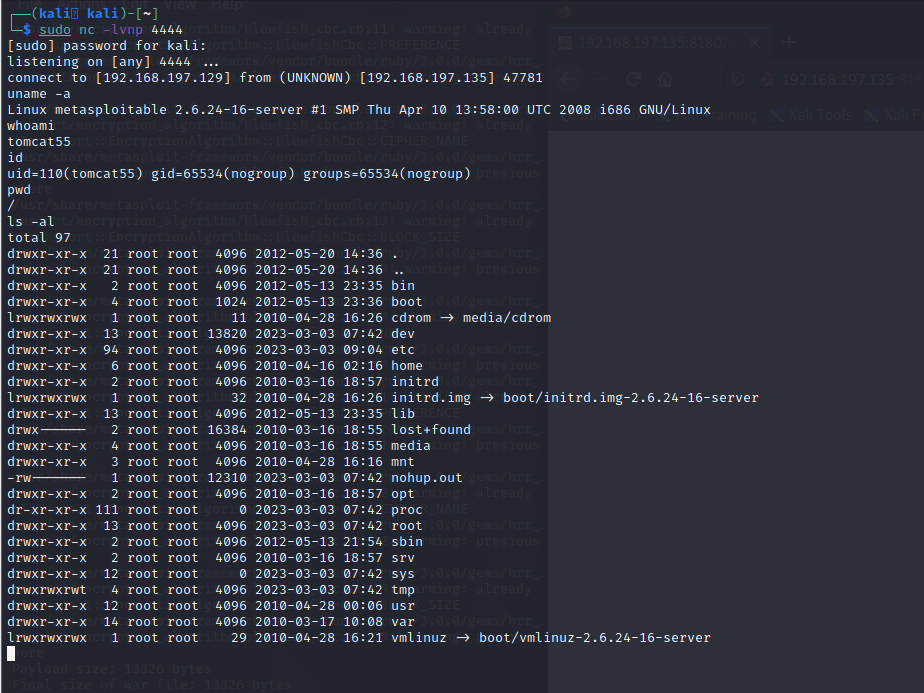
We will open up a netcat listener first.



After uploading and deploying the file, we will now find the file in the apache tomcat server and click on it.



After clicking on it, we should get a shell back into our netcat listener setup on port 4444.



And as shown in the screenshot, we get a shell back to our netcat listener and we are running commands on the server.

**Thus , we have successfully breached into the Apache Tomcat server manually by creating a payload using msfvenom and then deploying it into the server itself.**