My first step was to execute an nmap with the target ports to be able to identify what type of services are running in order to know what type of exploit it could use. Realize that it is a GlassFish I look for the option in msfconsole I look for the appropriate exploit I put the necessary parameters I assigned the password file with which I wanted to do the brute force attack after obtaining the password look for another exploit to gain shell Access now with the information obtained in the previous steps

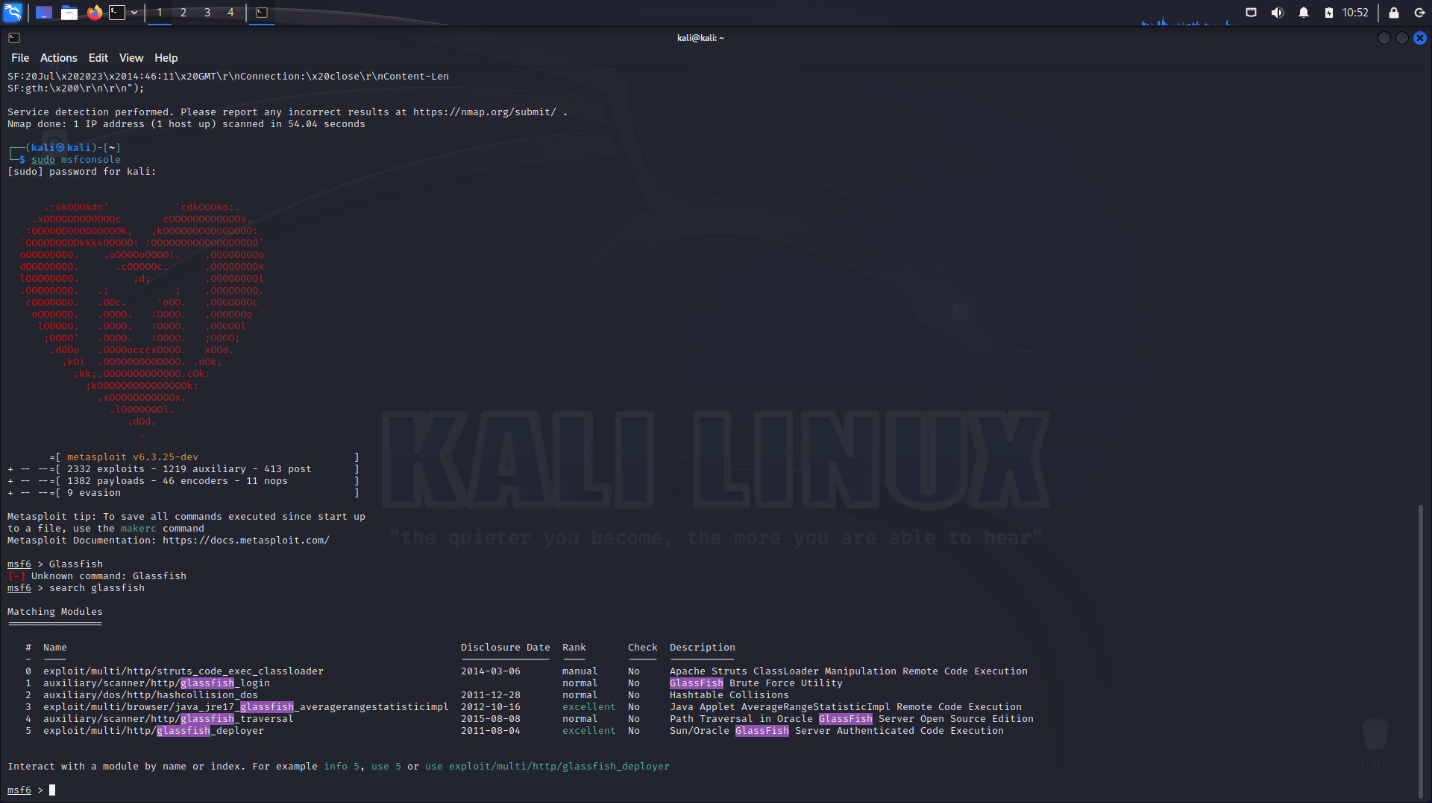
* What services were running on ports 4848, 8080, and 8181?

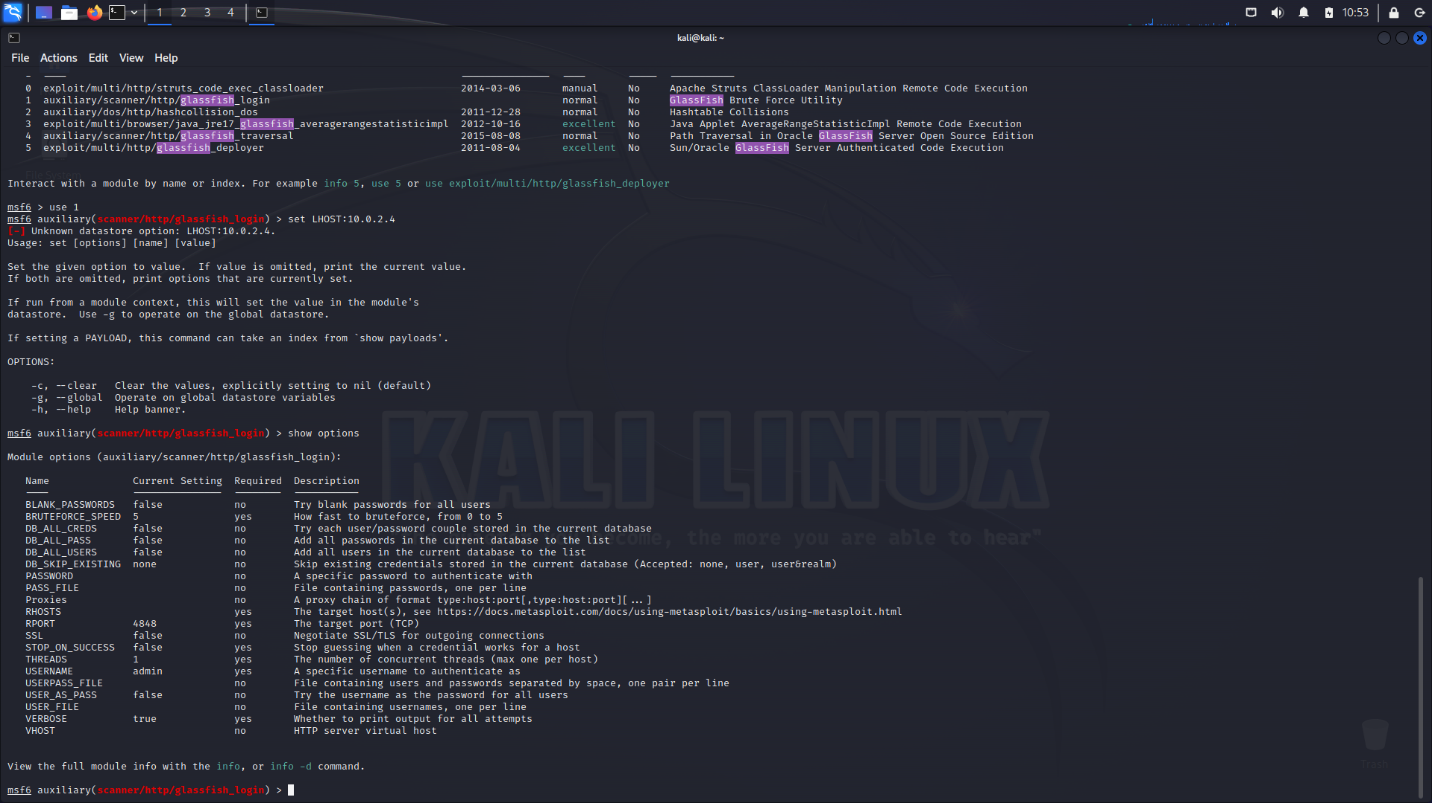


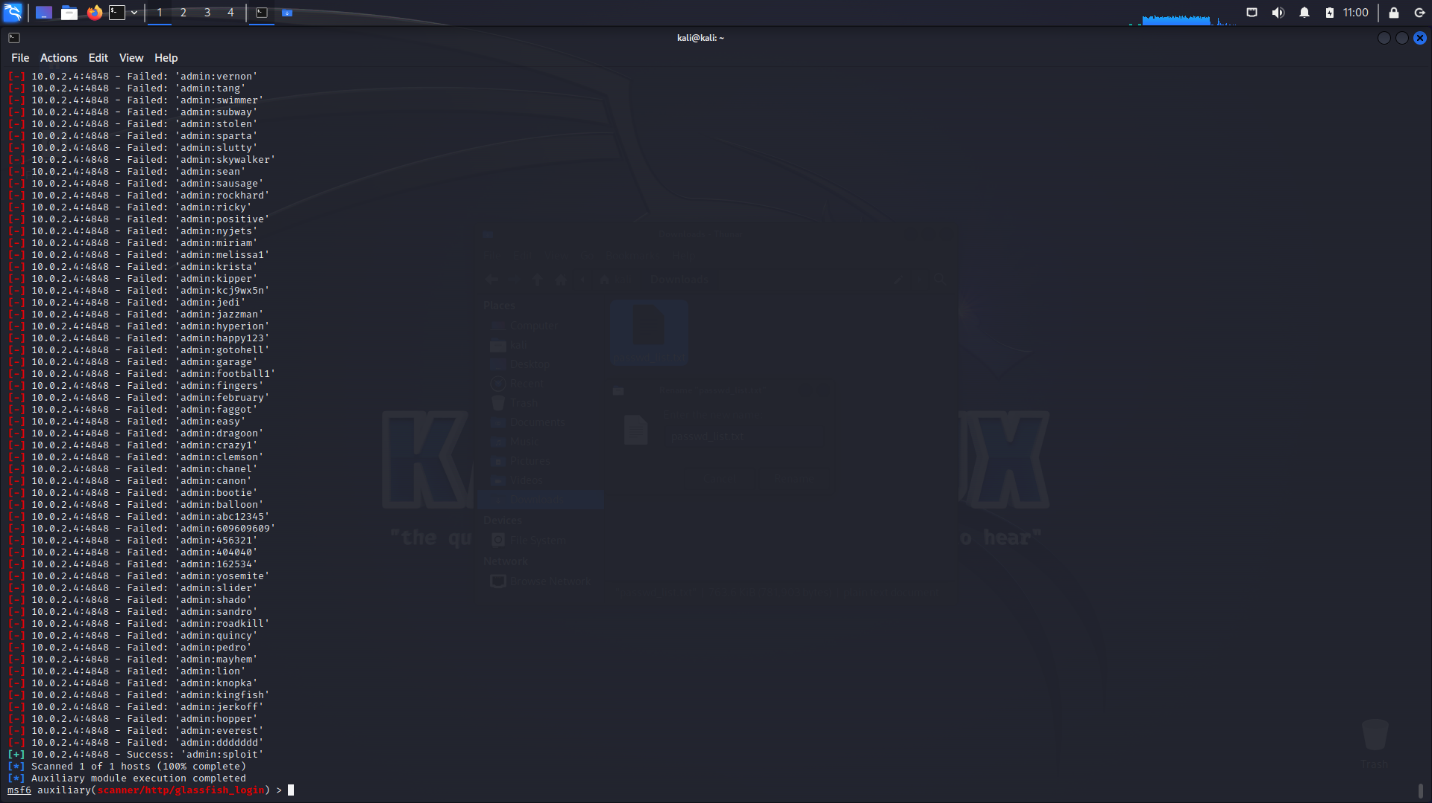
* What version was that service running?

Oracle Glassfish 4.0 (servlet 3.1: JSP 2.3: Java 1.8)

* What module did you use to brute force the password?





* What was the password?
* What kind of access did you have when your reverse shell was successful?

CMD admin acces

