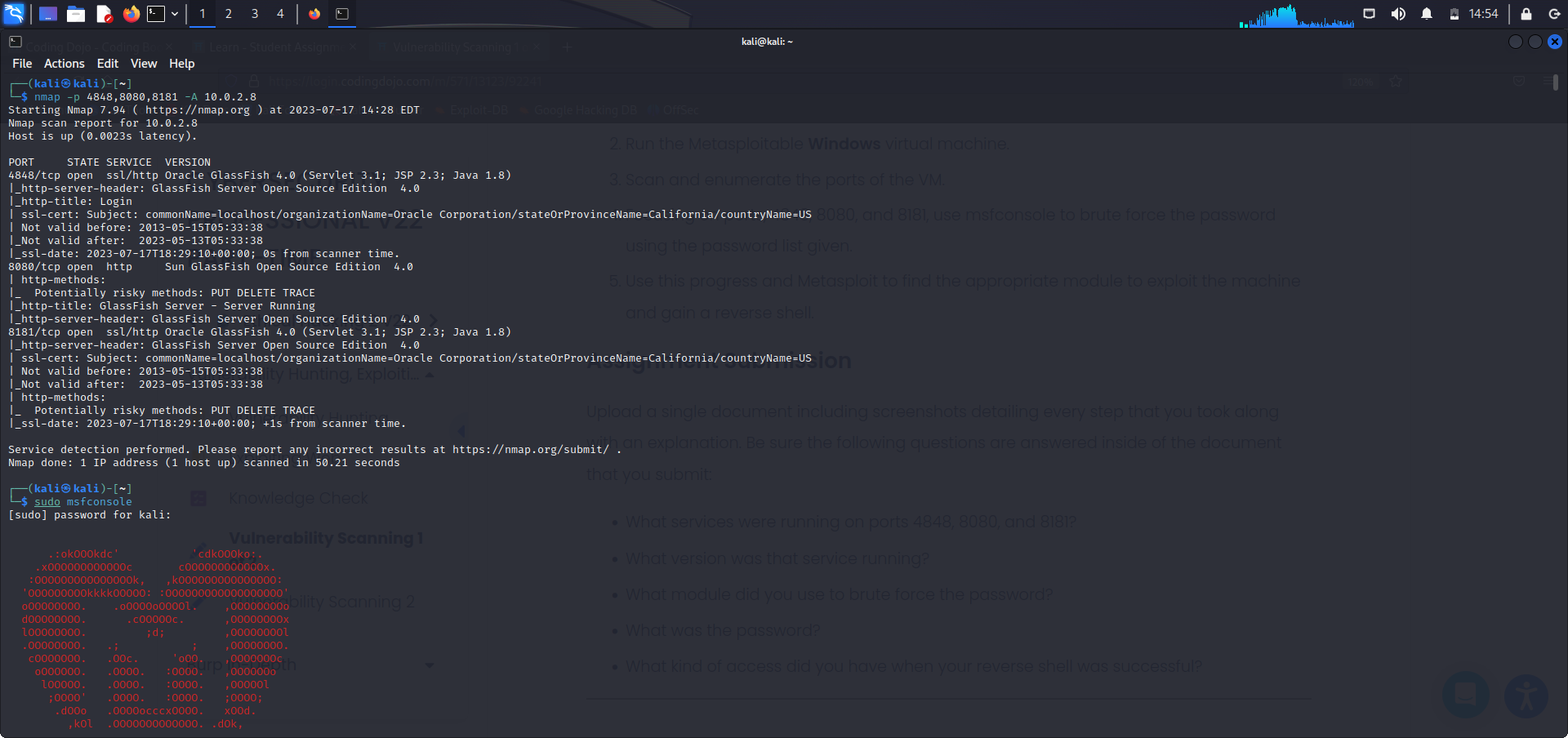
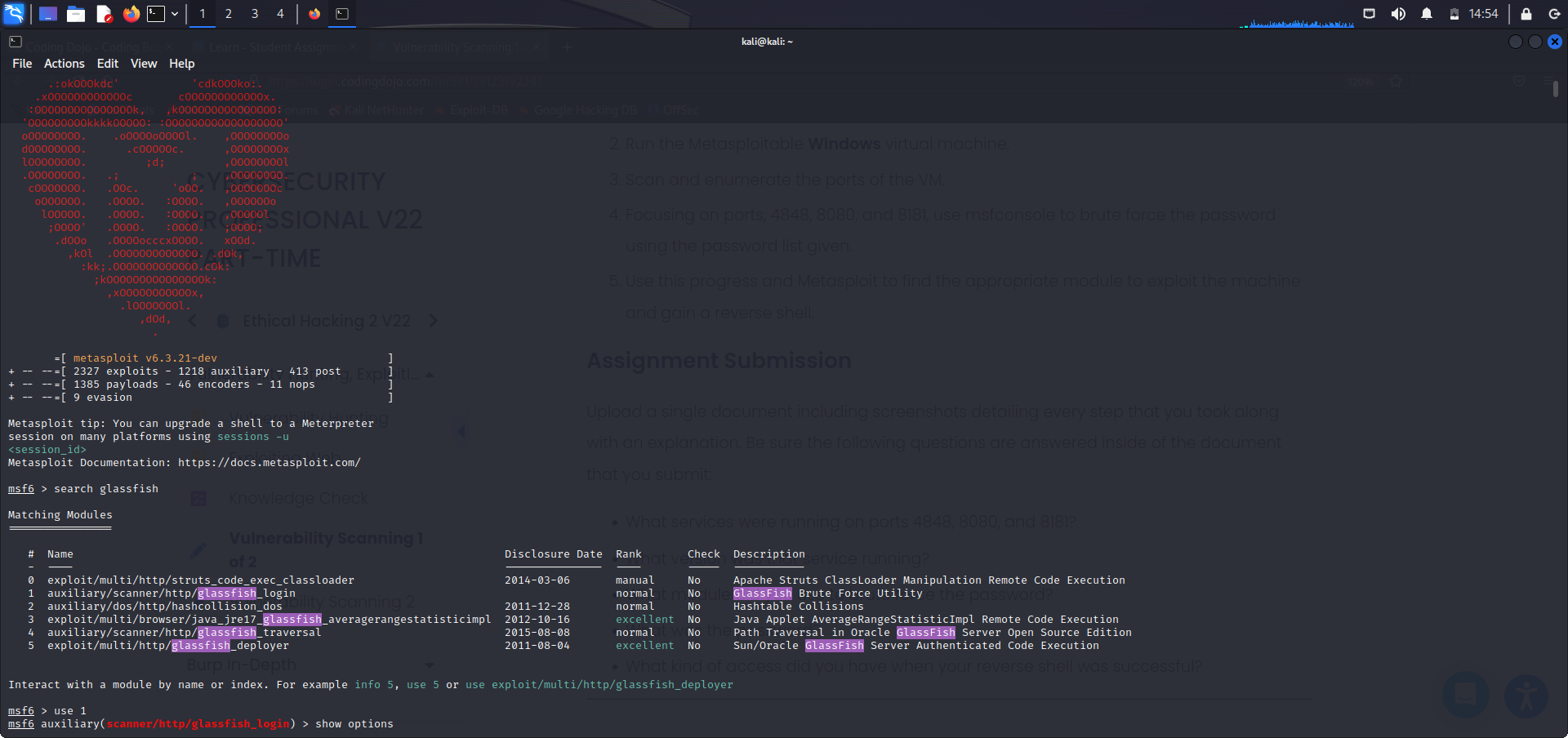
Vulnerability scanning

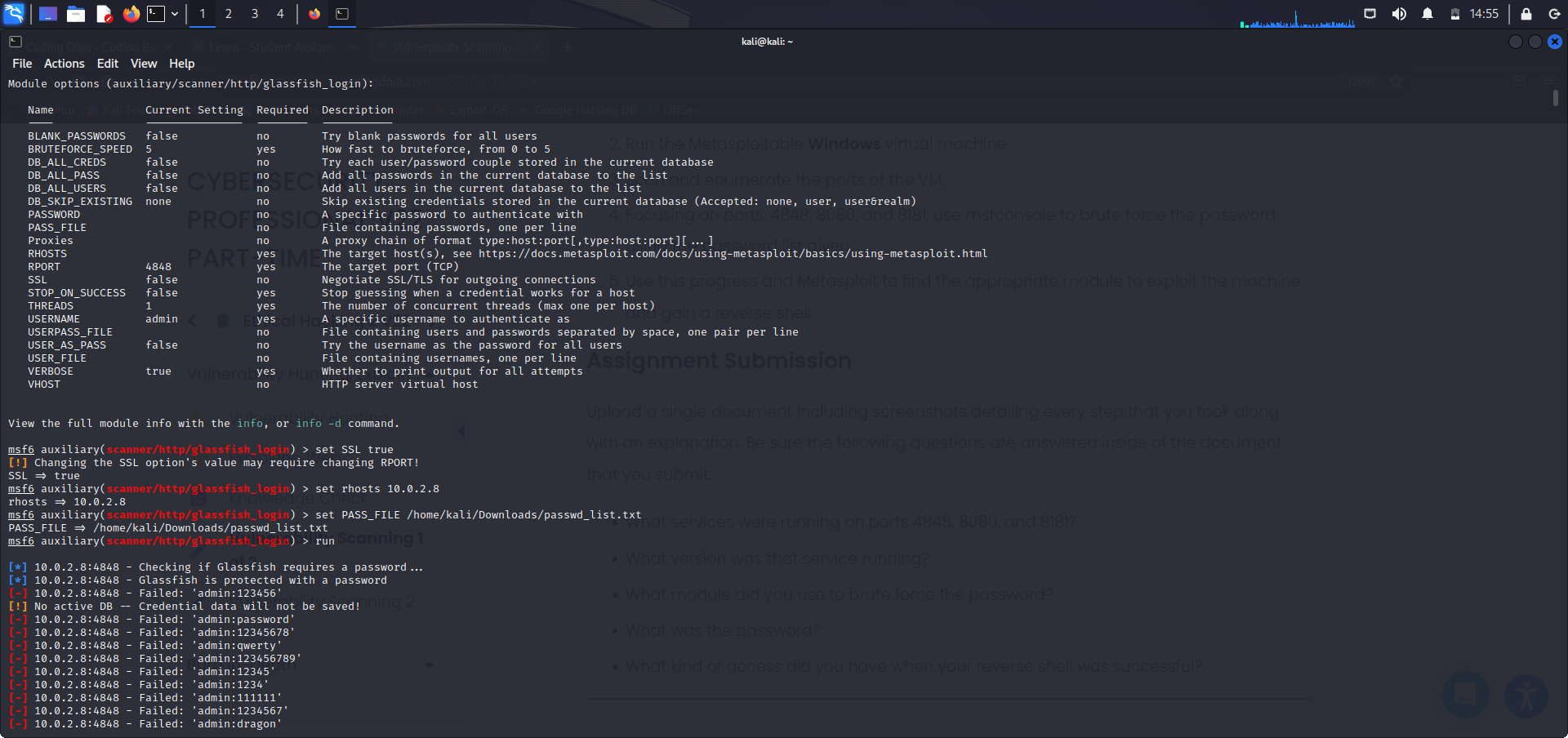
Spencer wise



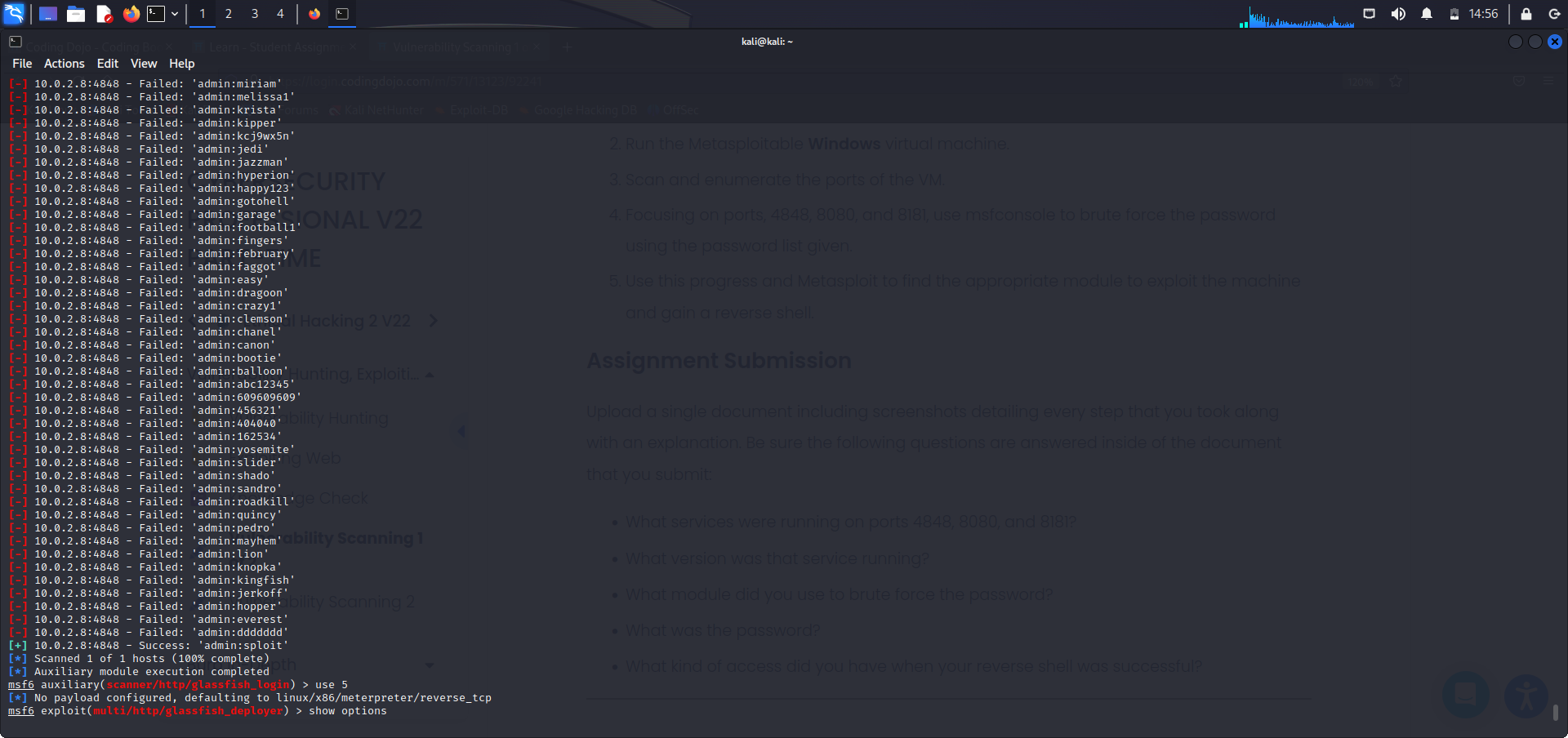
I did a port scan on ports 4848,8080,8181 on IP 10.0.2.8. Ports 4848/8181 service are ssl/http and version is oracle glassfish. 8080 service is http and its version is sun glassfish. My point of running a scan on these ports are to get the version of these ports to exploit them.



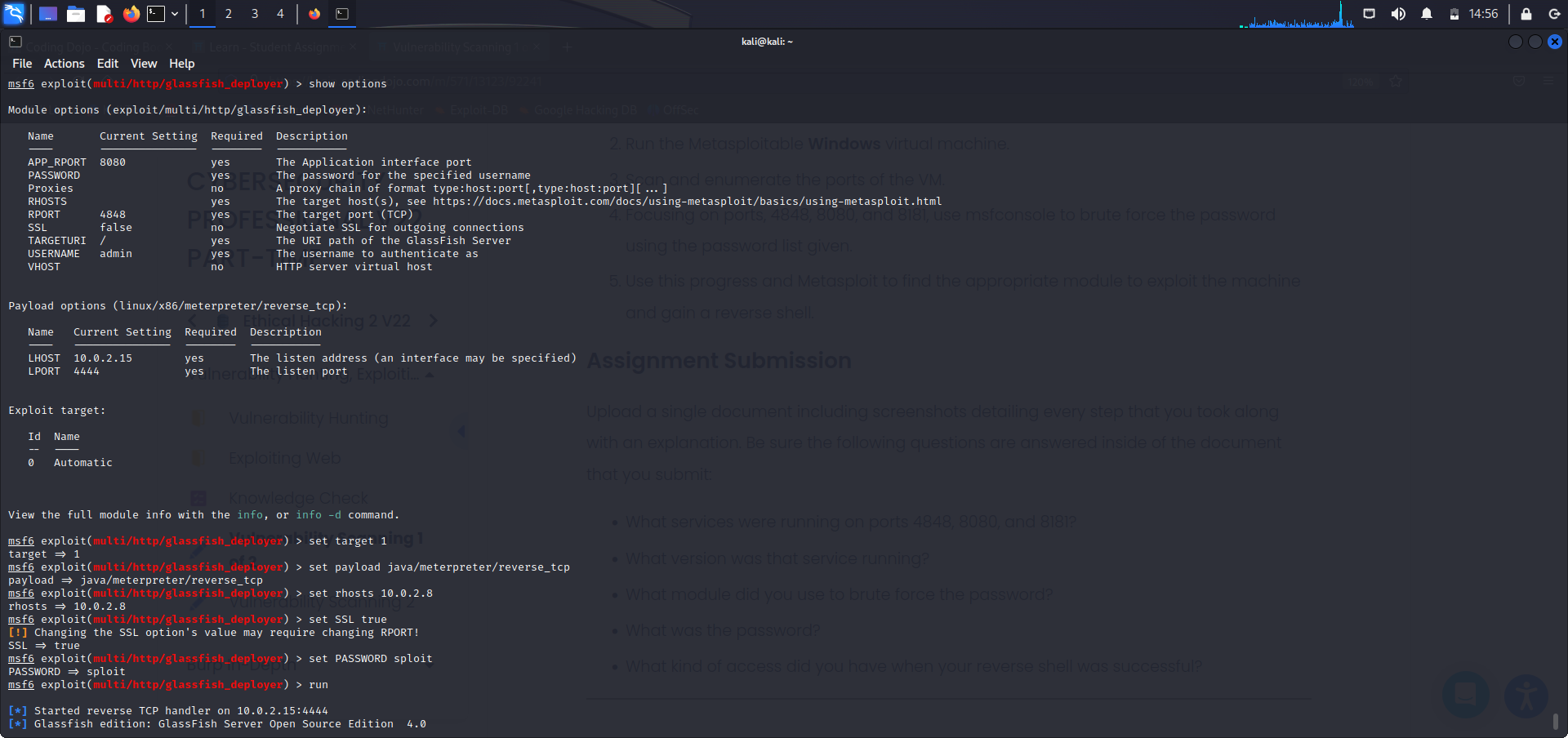
So now I have the version I open msfconsole (Metasploit) search the version in hopes of modules to use in my favor for gaining access to the system. I use module 1 for brute force utility (forced password cracker).



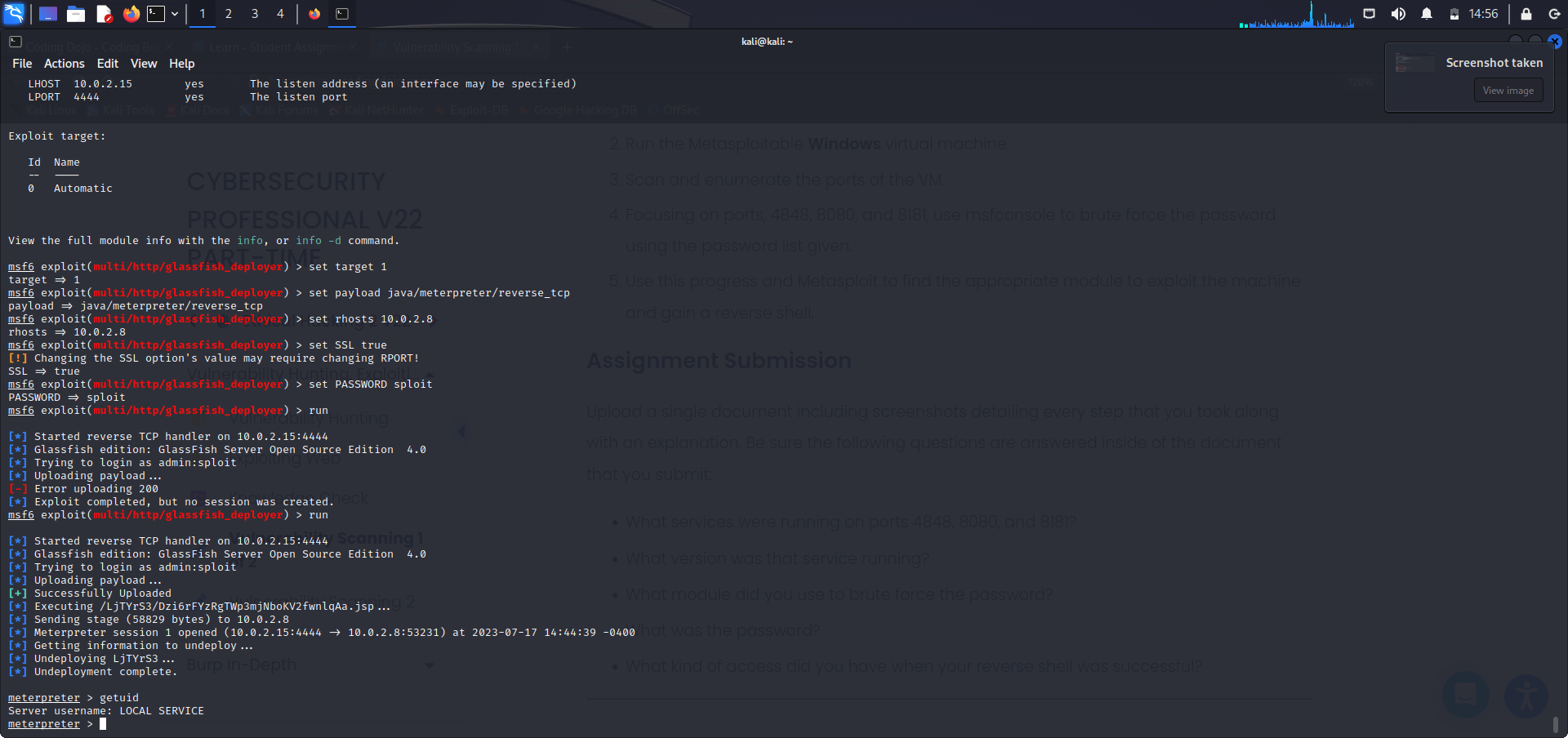
I change options of module 1 to fit the criteria of want I am seeking to executesuch as the “PASS\_FILE” (password list) to use. Rhosts or the IP address and run the module.



As you can see there was only one success ‘admin:sploit’. So now I have username and password.



Now that I have access to the system I can take it a step further by creating a shell (remote user). Again I search glassfish and find module 5 to my liking. I enter the necessary info to execute my shell such as the password I’d gotten from module one and target, rhost, lhost (me), and payload that would allow me to execute the shell. I hit run.



Now I have a reverse shell accessed through the username LOCAL SERVICE.