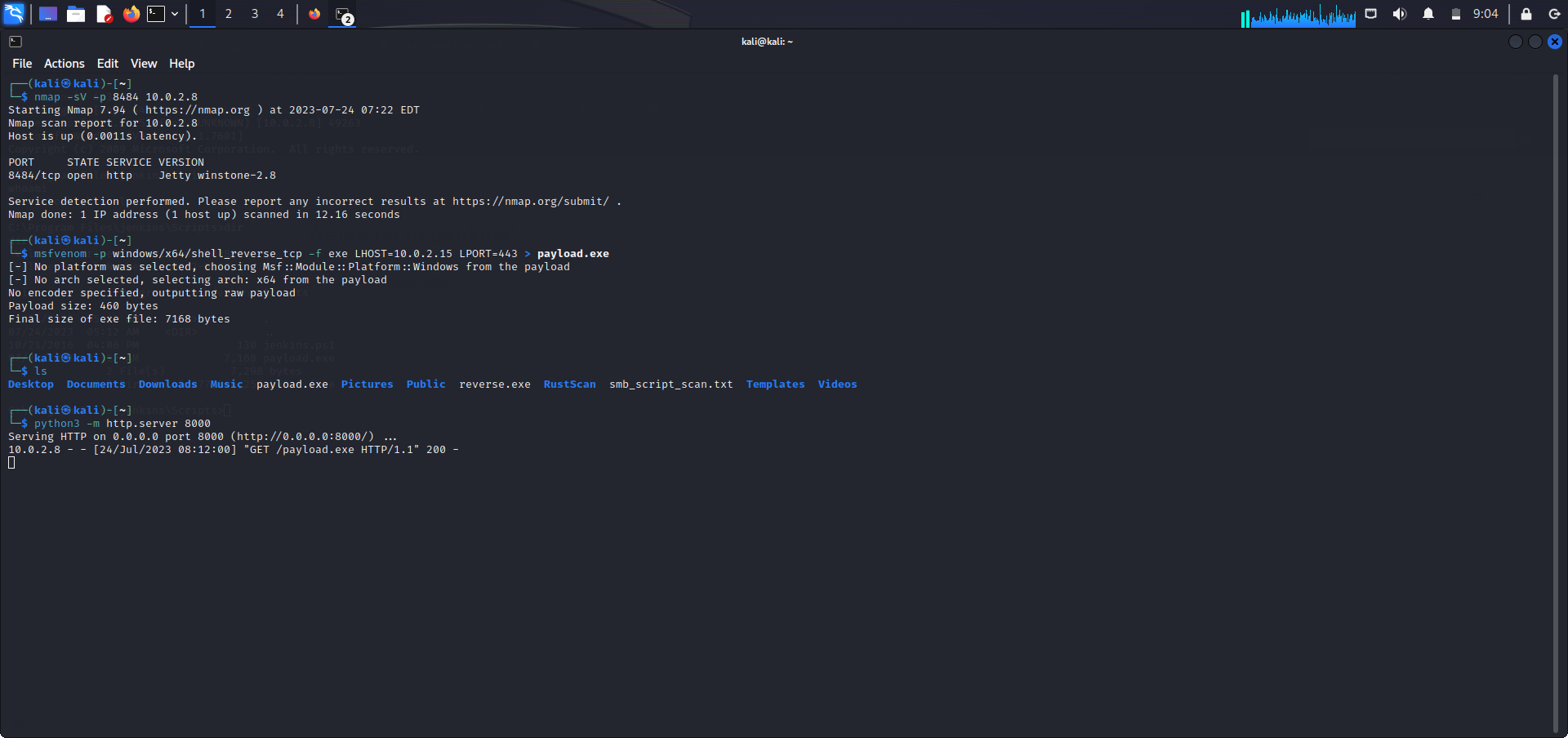
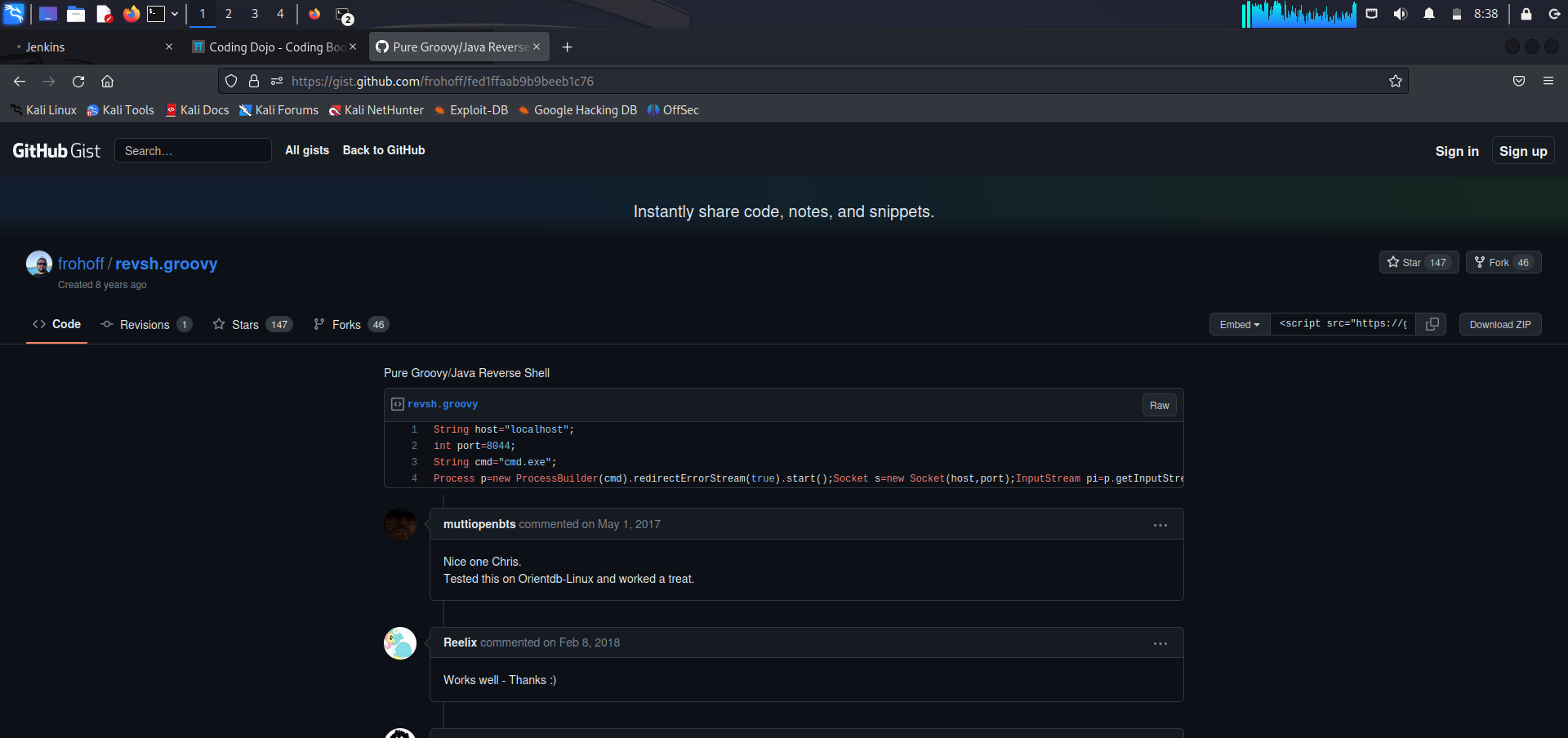
Vulnerability 2

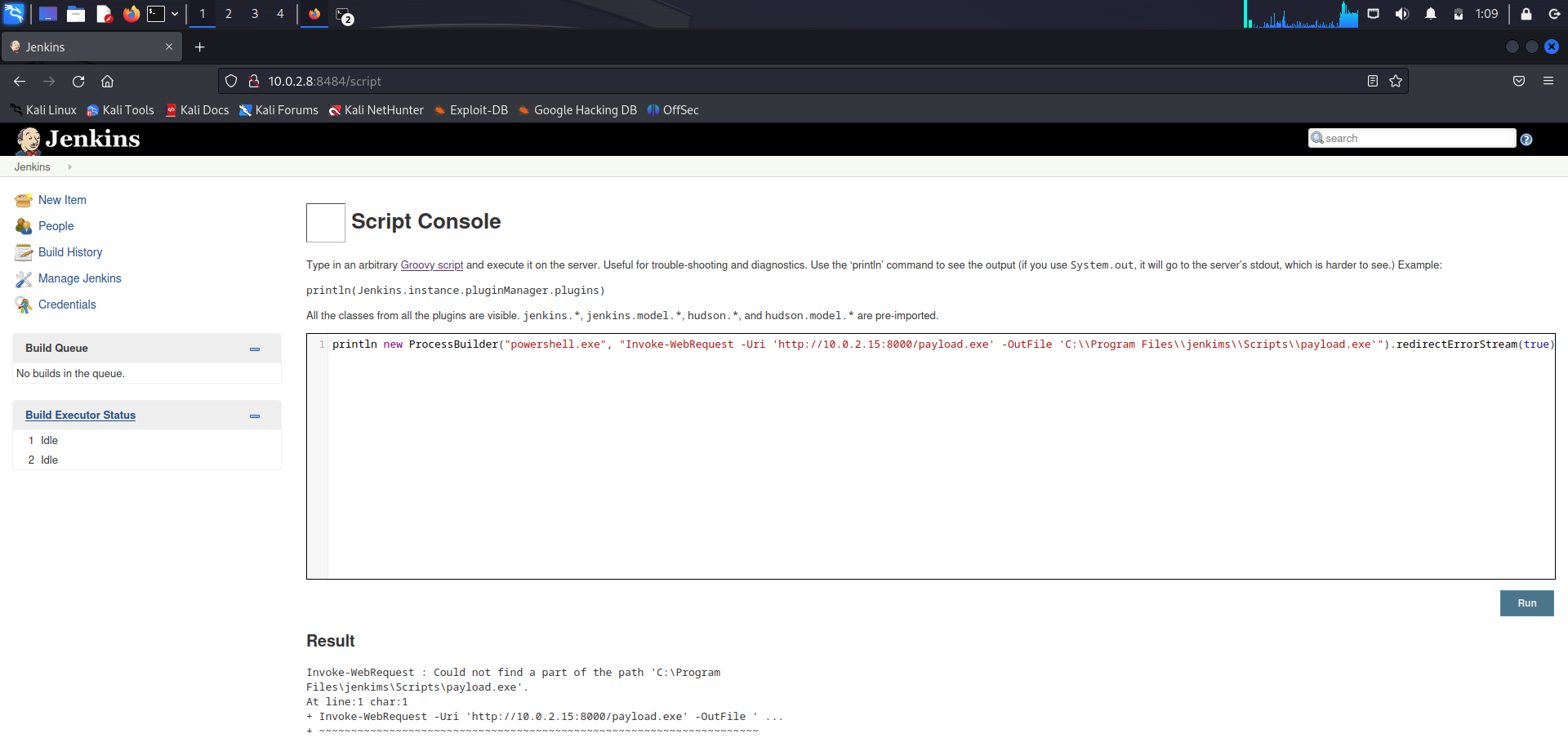
Spencer Wise



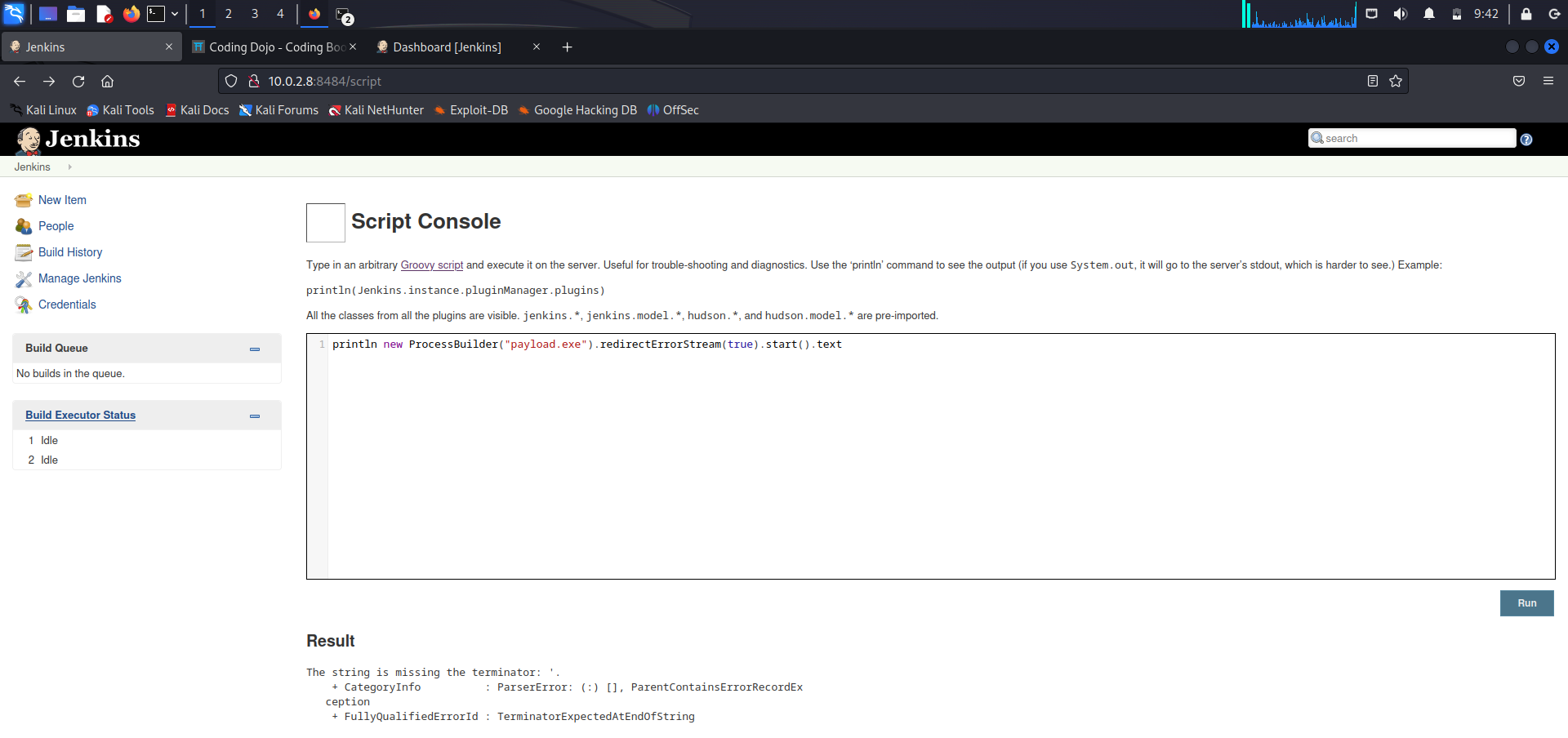
I started with a nmap of port 8484, target IP 10.0.2.8. This scan answered the first two questions of the project; that being the service(http) and version(Jetty Winstone-2.8) of port 8484. Created a payload through Metasploit and saved on my kali linux to be used in gaining a shell on my target machine. I also started python to ensure the payload is successful after I run the necessary executables.



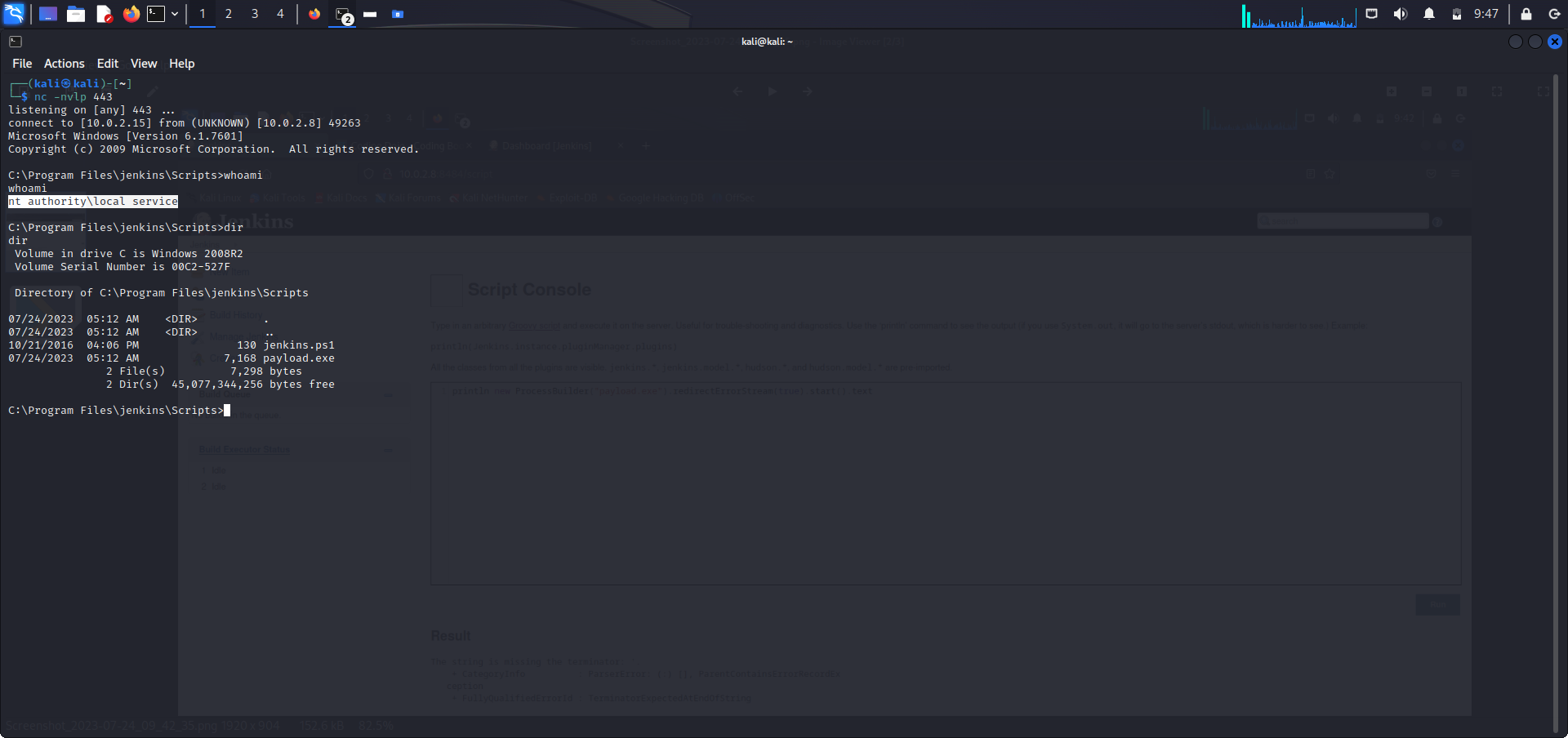
Researched vulnerabilities of Jetty…and came to GitHub for a reverse shell script that I input into Jenkins which is <http://10.0.2.8:8484/script> to get desired shell.



Well the previous script was giving me fits so I found another that was easy going to run with no hitches. This script basically is instructing IP 10.0.2.8 to ‘GET’ the payload from 10.0.2.15(kali machine) that I created earlier and saved on the machine.



Then used this script to execute the payload. That I got from GitHub.



Using the netcat command I started listening for any traffic on port 443(which is the port that information from 10.0.2.8 will come back to on my kali machine 10.0.2.15. after executing the payload it is confirmed that I am connected to target machine through my kali machine. The user is highlighted with the who am I prompt.