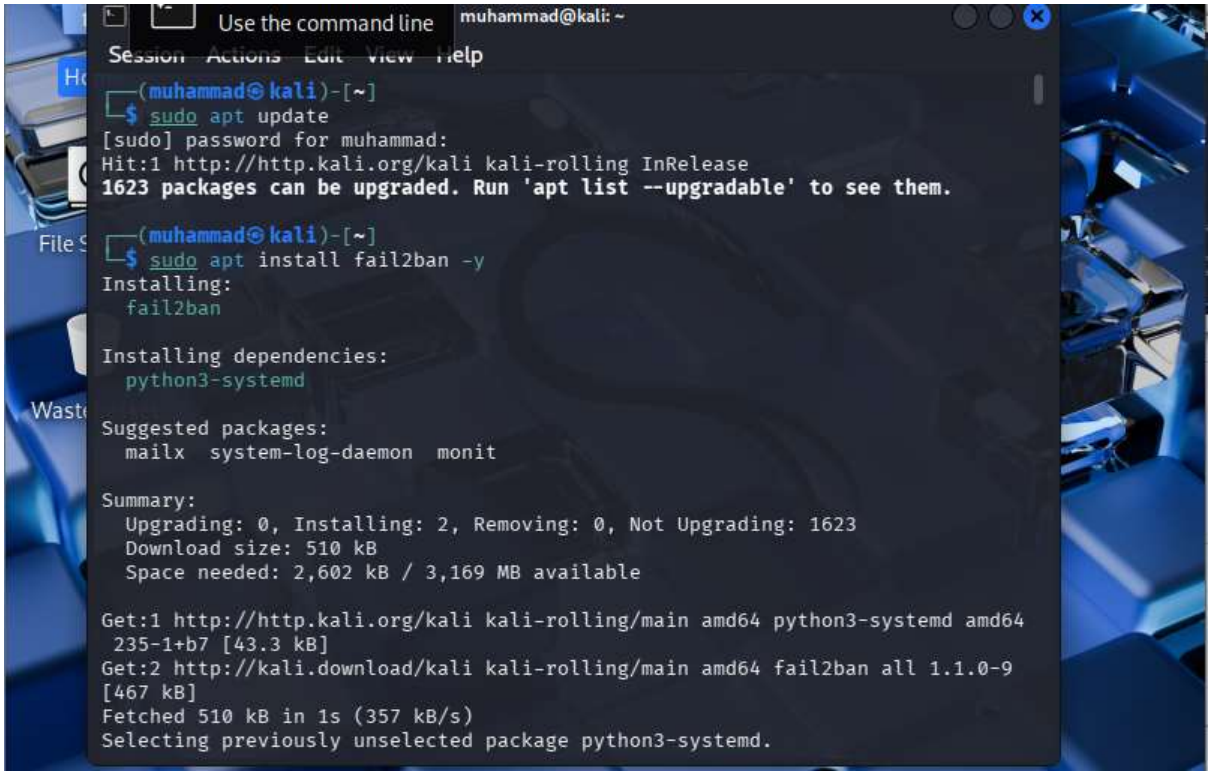
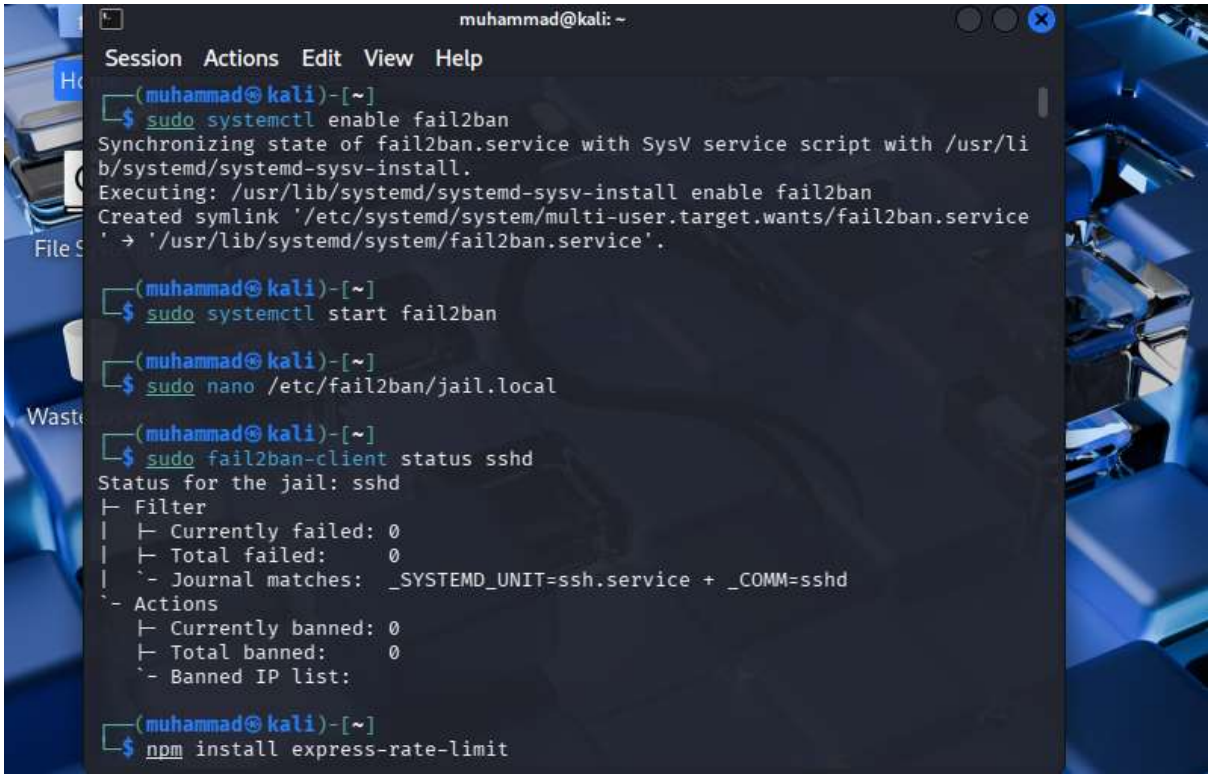
Name: Muhammad Bin Qasim

Week 4: Advanced Threat Detection & Web Security Enhancements

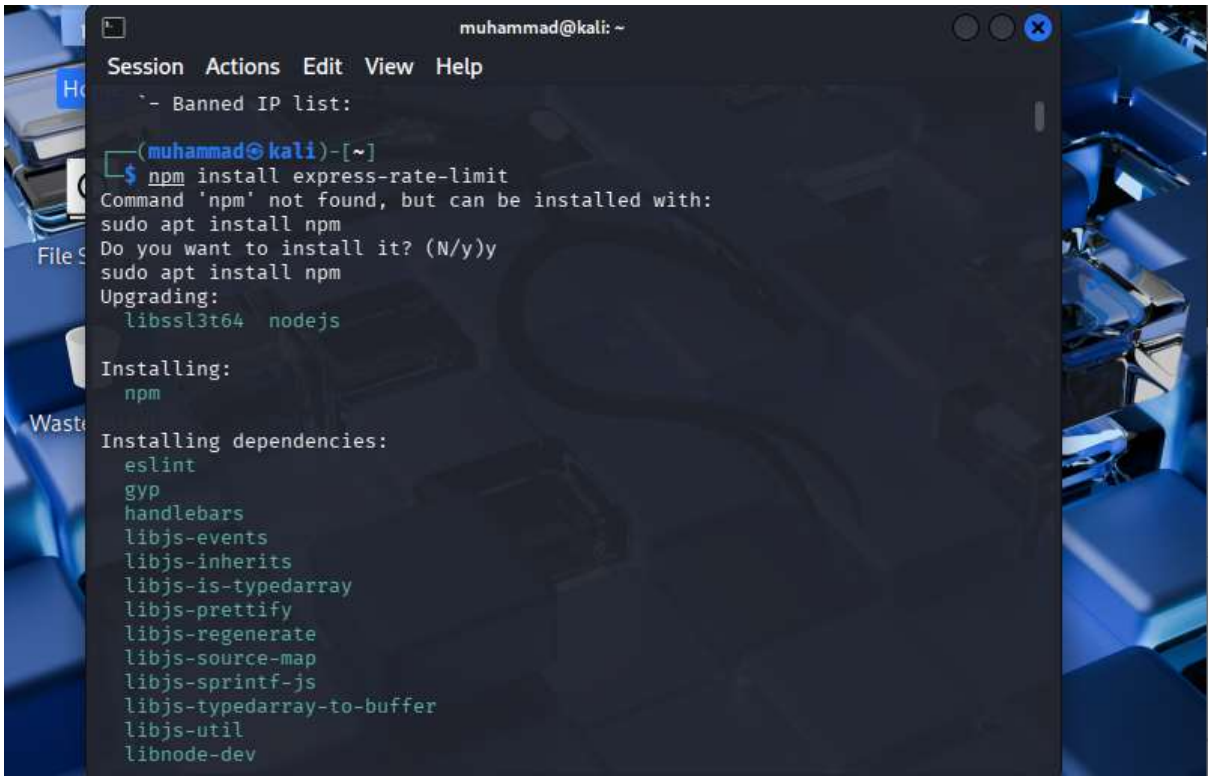
Installing Security Tools: I working on a Kali Linux terminal. First, update the system's package list to ensure everything is current. Then, install a program called fail2ban. This is a security tool designed to protect computers from brute-force login attacks. The terminal displays the successful download and installation process.



Configuring fail2ban: Turns on the fail2ban service and sets it to start automatically. Next, open its configuration file and check its current status to see if any malicious IP addresses have been blocked from accessing the system via SSH. At the bottom, they try to install a web package called express-rate-limit.

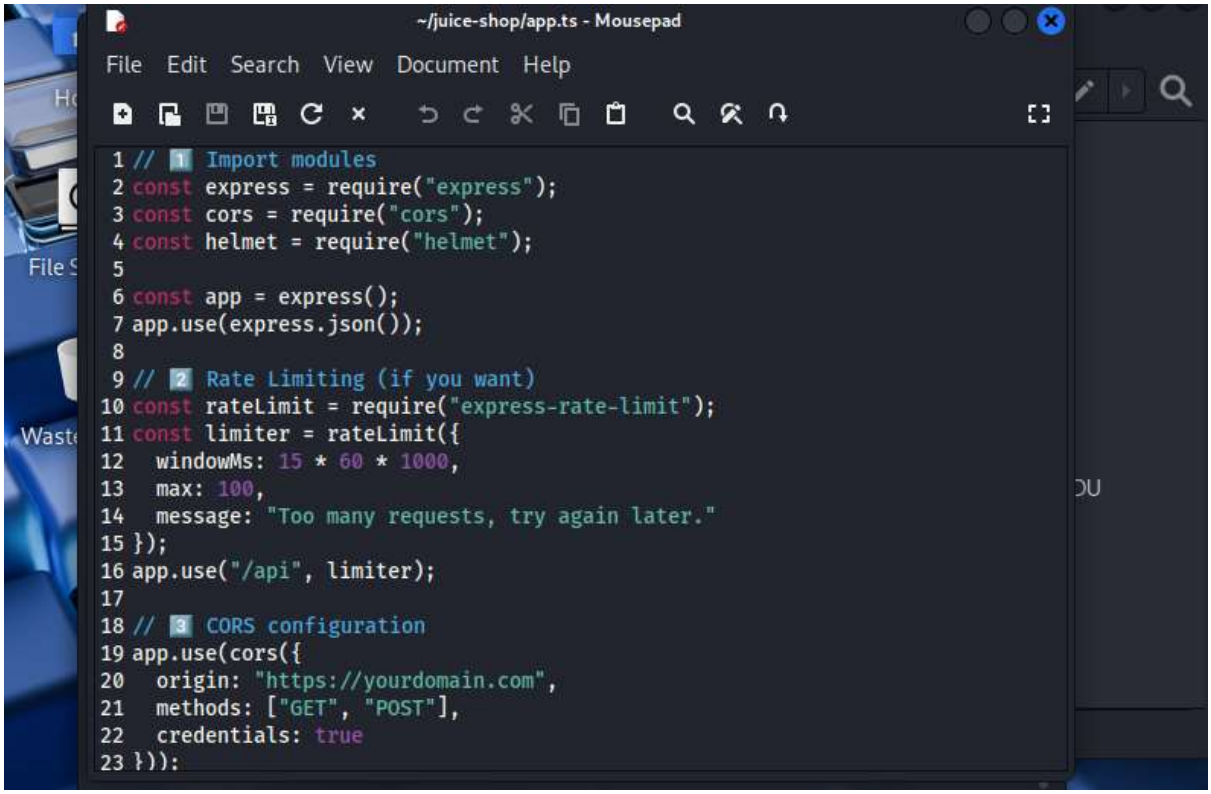


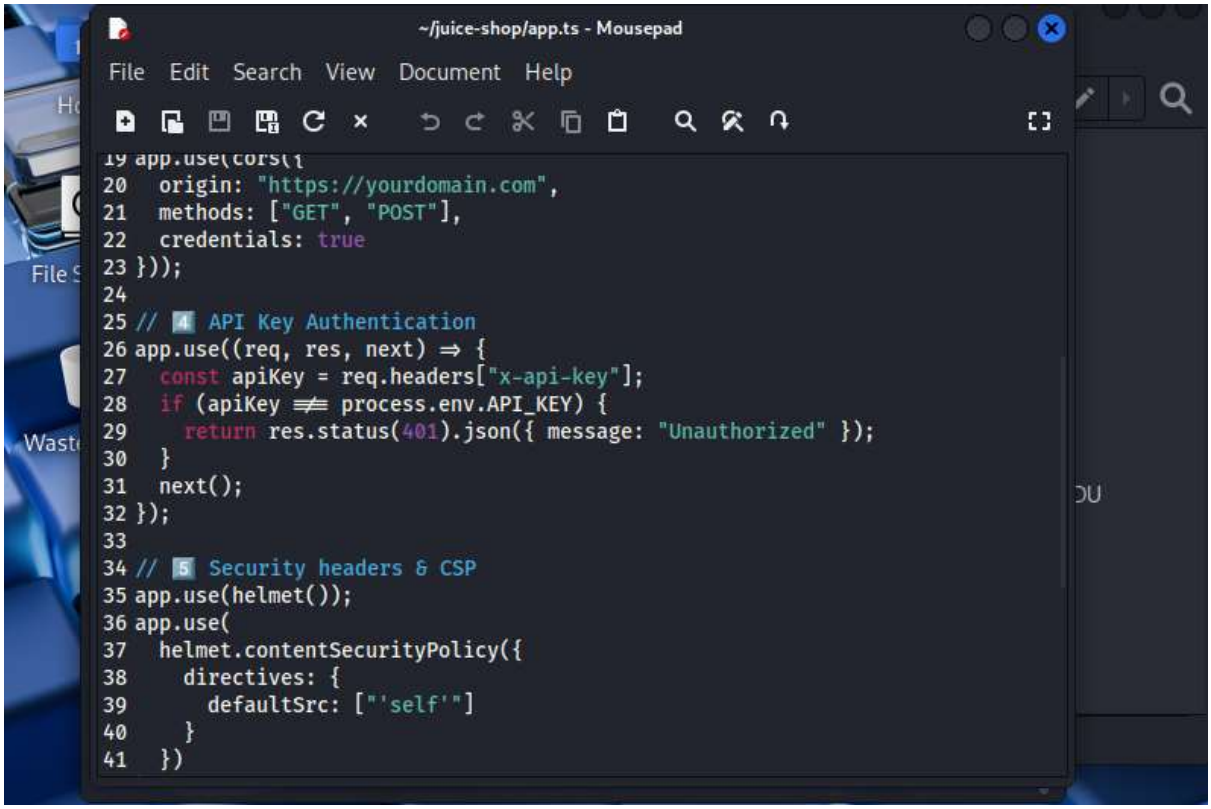
Installing Node Package Manager: Because the previous command failed, the system tells the user that npm (Node Package Manager) is not installed. Then types a command to install npm using the system's package manager. The screen shows a list of the required files being downloaded and set up. This tool is necessary for building JavaScript applications.

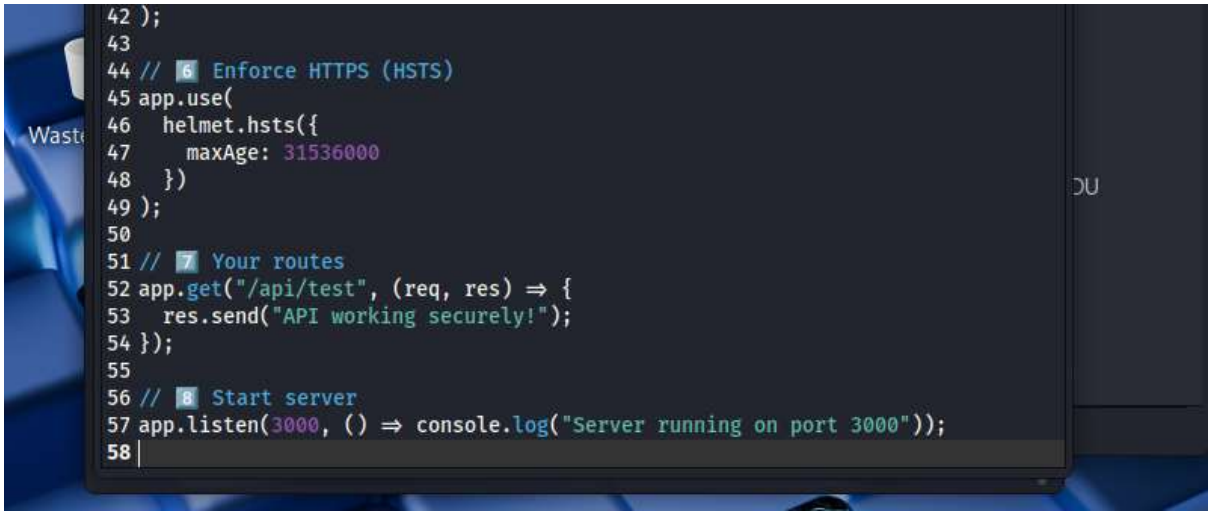


Installing Project Dependencies: Navigated into a folder named juice-shop and typed the command npm install. This command tells the system to download all the extra code files needed to run this specific web project. The terminal shows a list of orange warning messages, which simply indicate that some of the packages being downloaded are outdated.

Writing Web Server Code: This shows a text editor open to a file named app.ts. The code is written in JavaScript/TypeScript for a web server. It starts by bringing in helpful tools like Express, CORS, and Helmet. It also contains a section that sets up "rate limiting," which prevents a single user from crashing the server by sending too many requests too quickly.







Setting an Environment Variable In this last screenshot, goes back to the terminal inside the juice-shop folder. Type an export command to create a temporary system variable named API_KEY and set its value to "MBQ". This secret key is exactly what the code in Image 6 will be looking for to allow access to the web app.

Github Link:

https://github.com/MBQ17/Week-4-Advanced-Threat-Detection-Web-Security-Enhancements