**Implementation Of Web Application Firewall**

Objectives: This project is to implement a firewall(a guard) in a website that blocks and protect the attacks from potential attacks like SQLi, XSS, CRSF, etc. And send the logs to a SIEM for montoring and investigation.



Tools Used: Ubuntu VM(as Web Server & Attacker), Docker(as container), Splunk (for SIEM).

Project Overview: using file

Client → WAF (port 80) → web:5000 → db

│

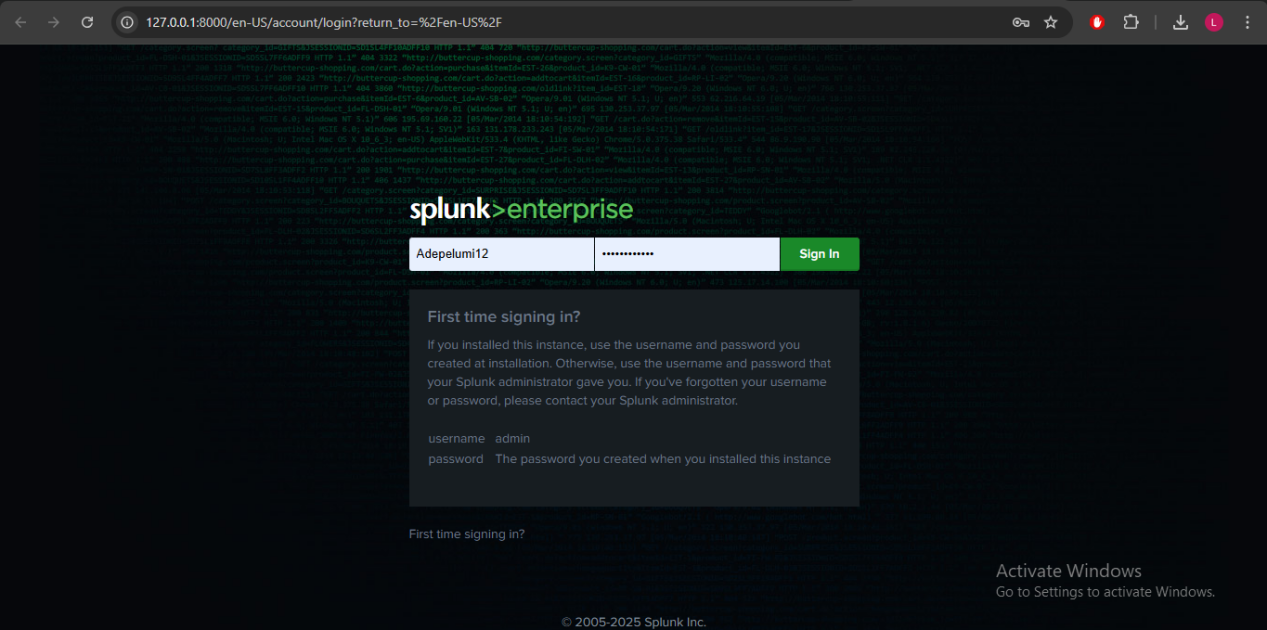
└─ writes JSON audit logs → /path/on/host/logs/modsecurity/audit.log

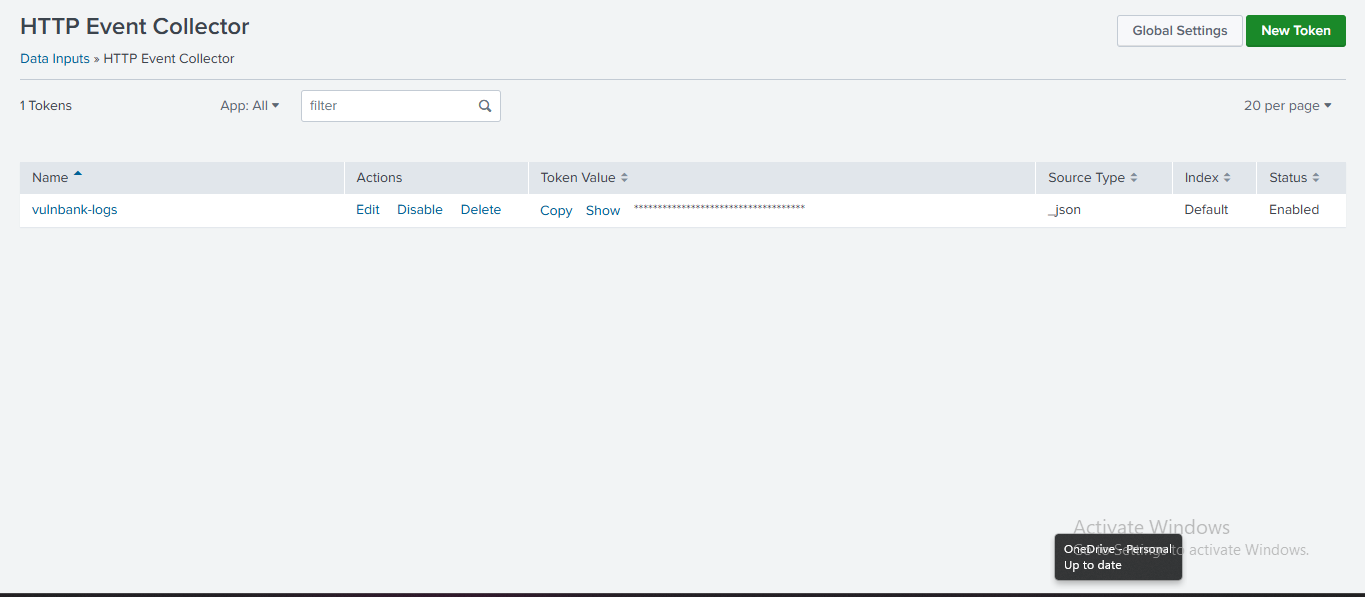
│

└─ Splunk UF monitors & forwards → Splunk

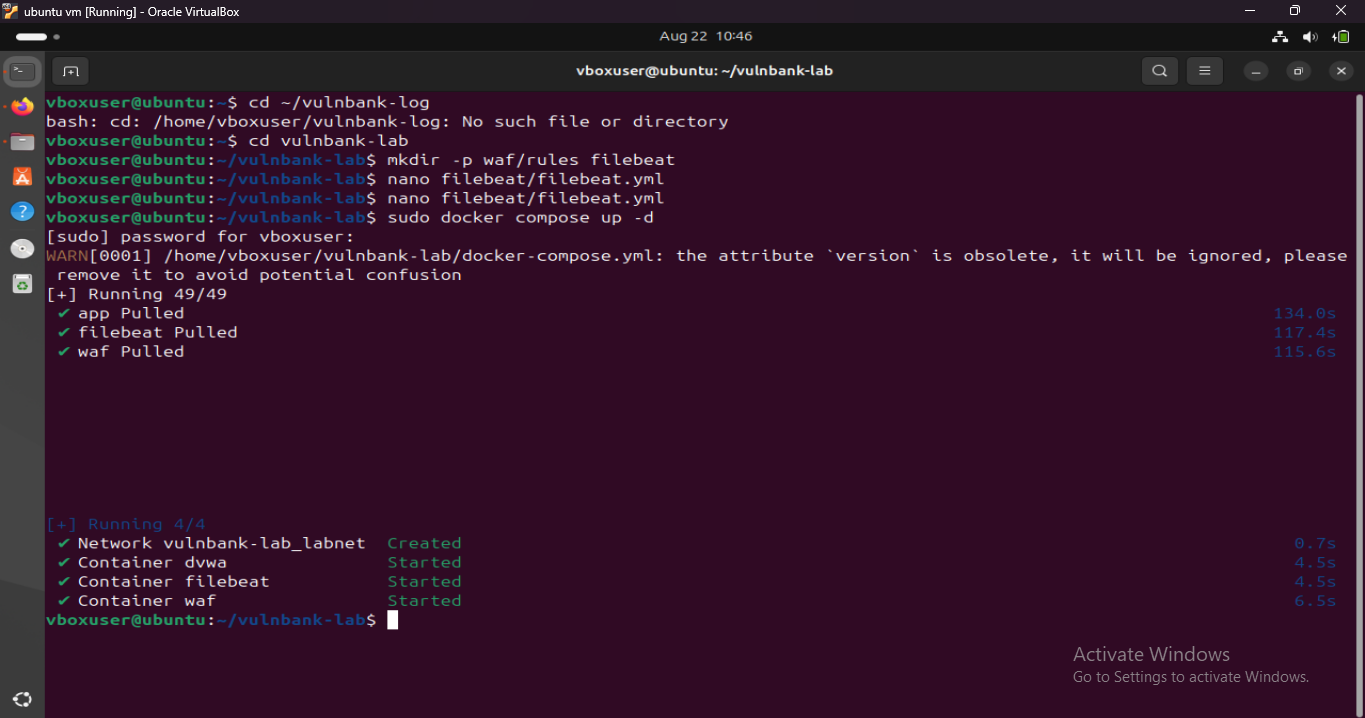
Steps:

1. Install Splunk on host machine, setup Http Event Collector token, name it the webapp name, set index to main or default, set source type to JSON & status to Enabled. Install Docker in the ubuntu VM.





2.)Make a folder for the project, and change directory, copy the docker-compose.yml file on vulnbank.org github(I will upload mine; it is already edited), create a filebeat.yml file(I will put mine in github) filebeat converts logs to JSON format so it could read in SIEM. Run docker compose u -d to start the docker container.



All containers has started.

3.)