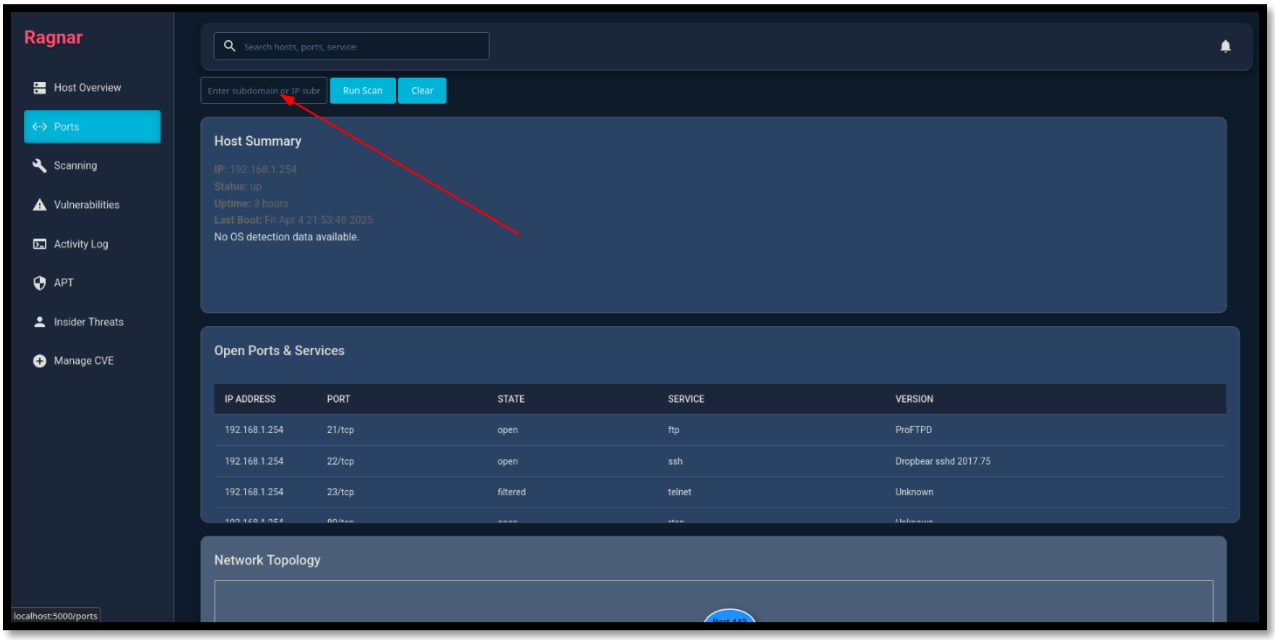
RAGNAR

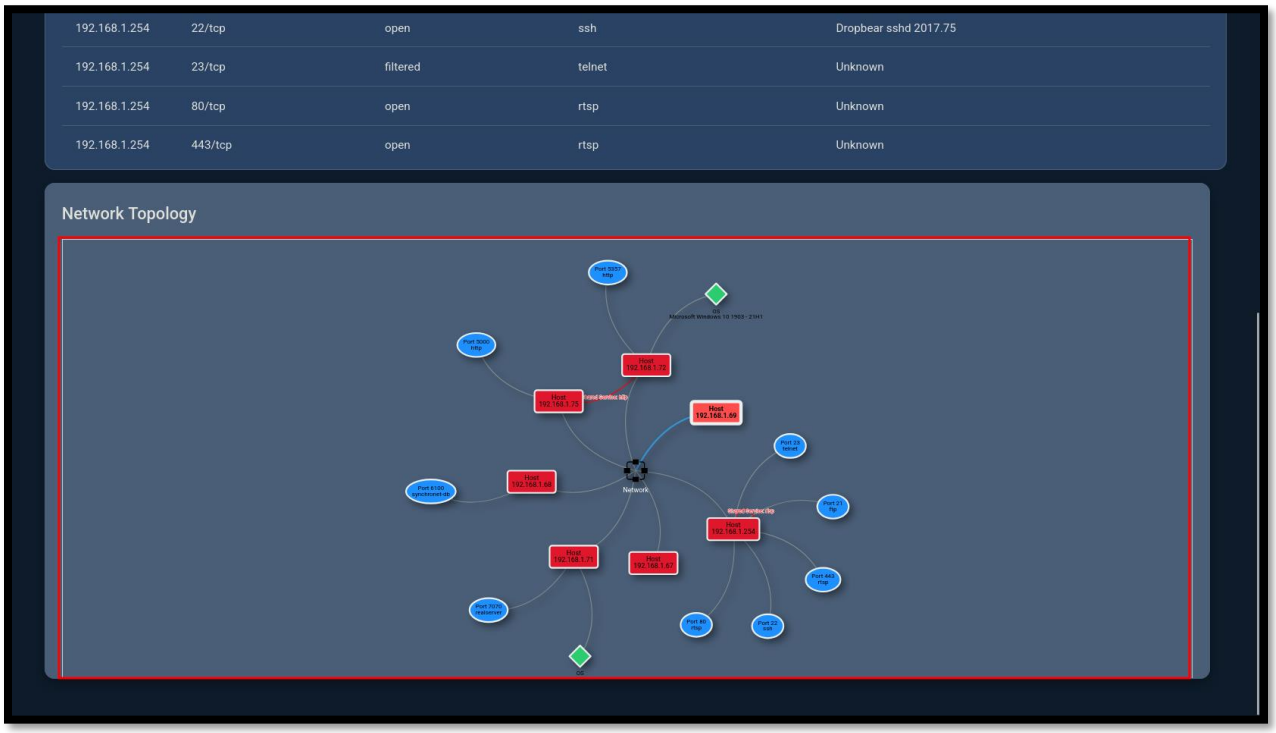
User Mannual

Prepared For: Islington Hacker-Thon 2025
Prepared By: Team Kernel Panic

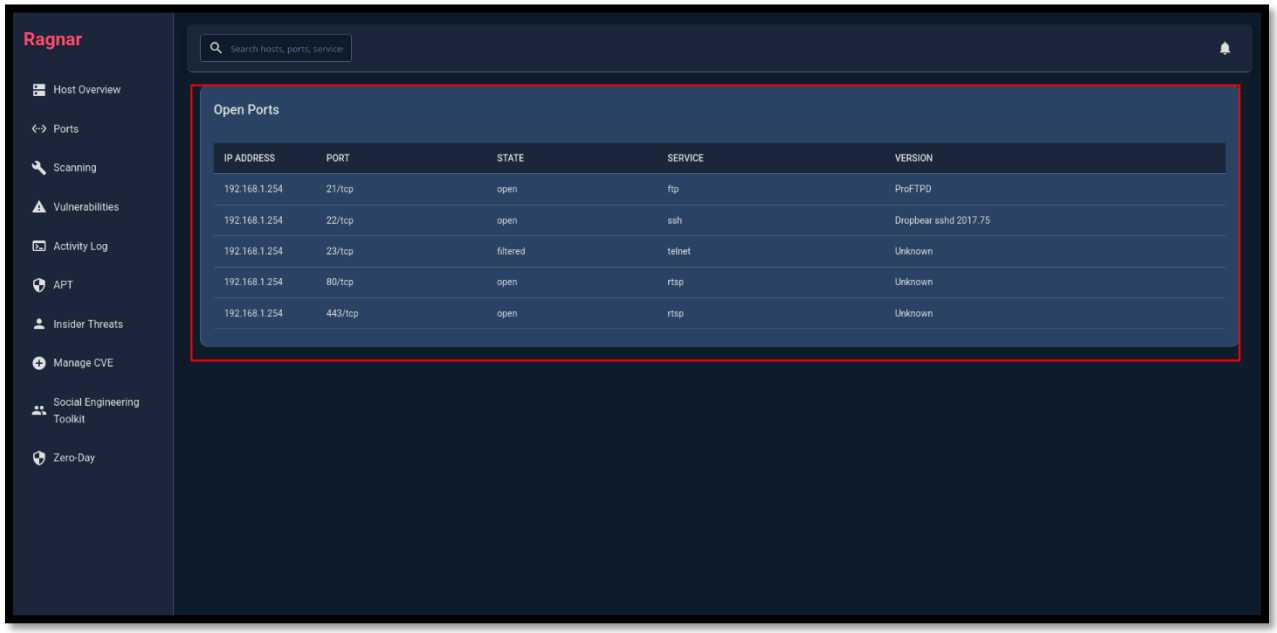
1. Enter the Ip address or CIDR range to scan the available assets of the network



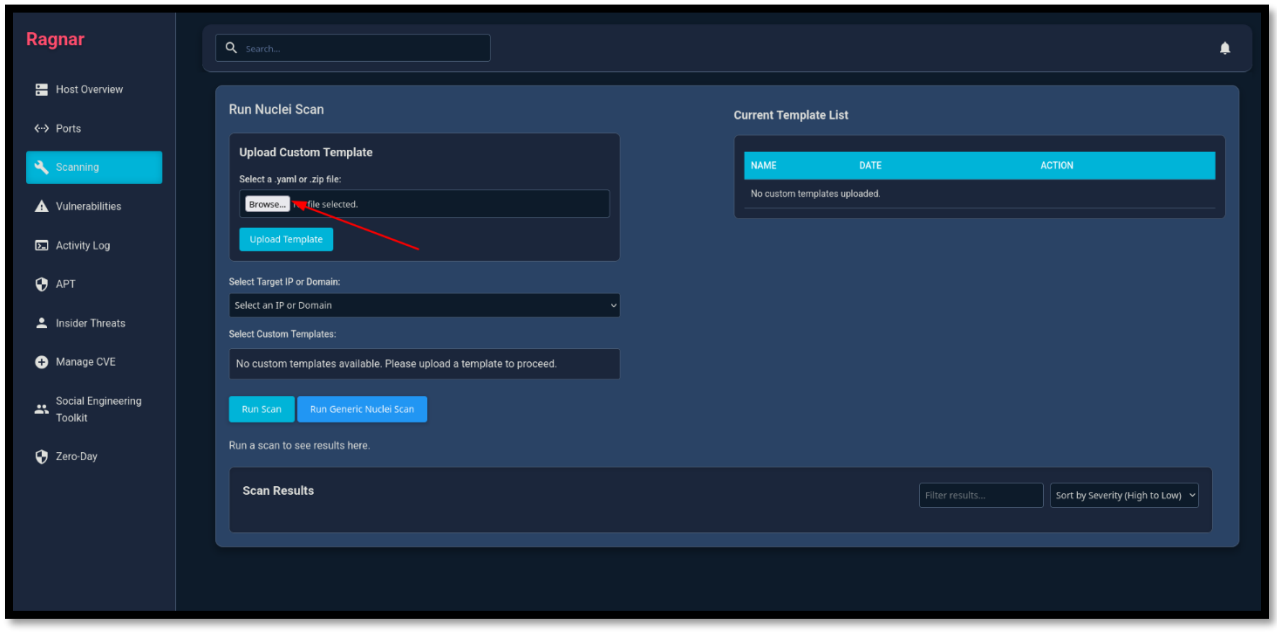
2. Scanned results can be visually analyzed from the graph and table in the next tab.



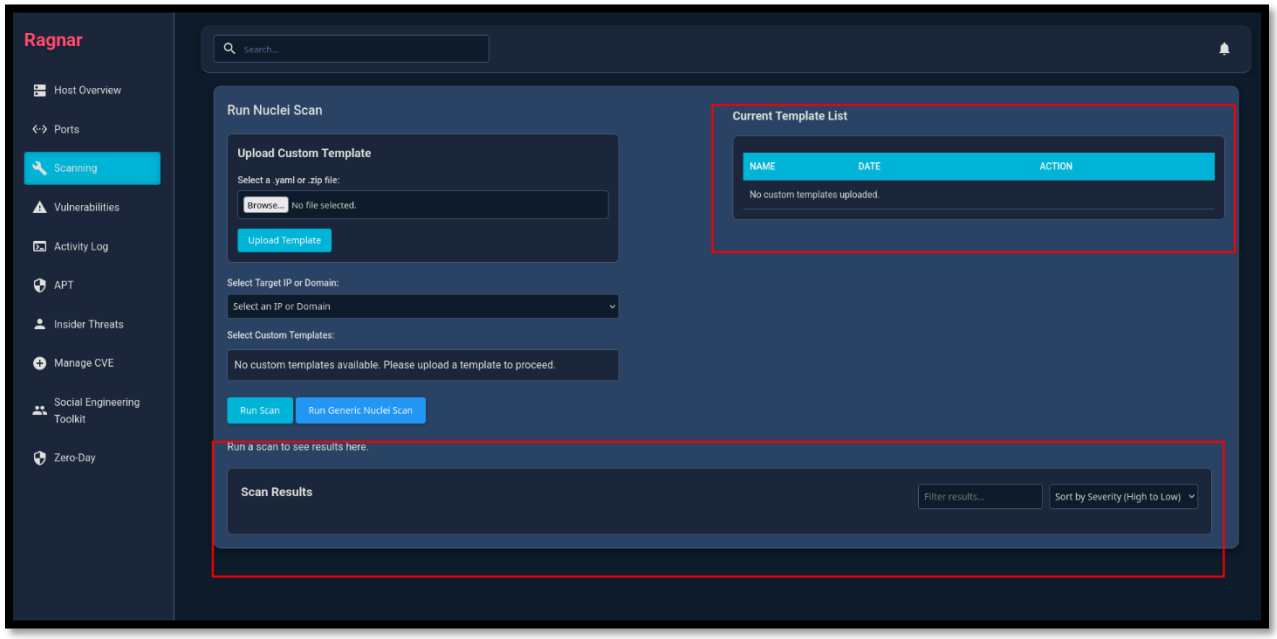
3. All the scanned ports and services can be viewed in the Ports tab of the scanned result



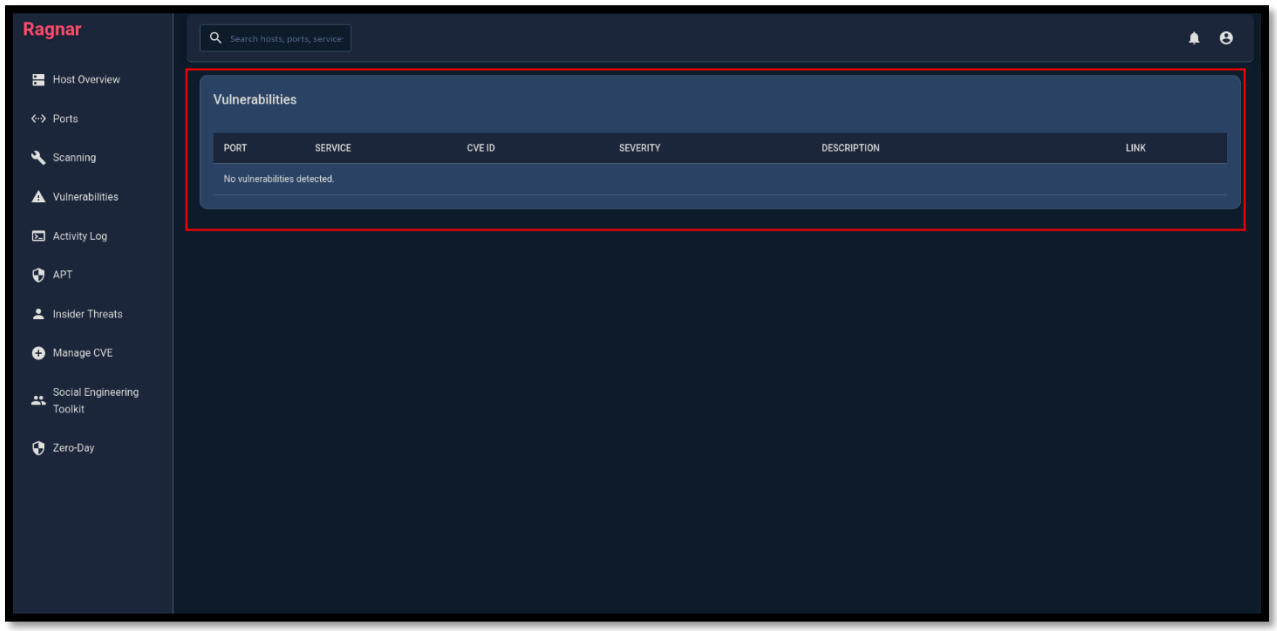
4. In the scanning section, we can load the nuclei templates in zip file and select which template to scan on the specified target.



5. The available templates are listed on the right side and after scanning with selected templates, the result is viewed in the bottom section.

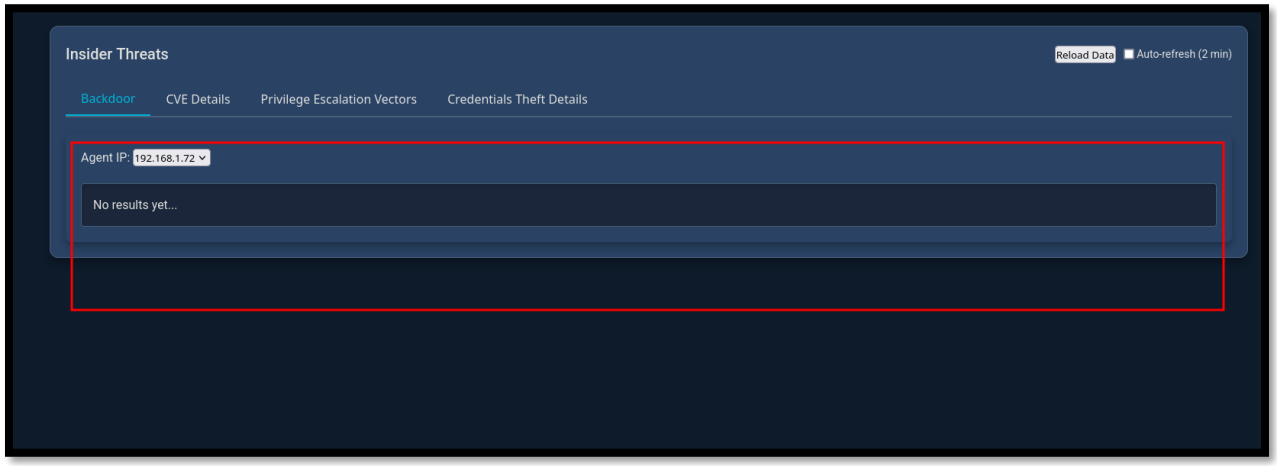


6.The vulnerabilities scanned by Nmap scripting engine is viewed in the vulnerability section.

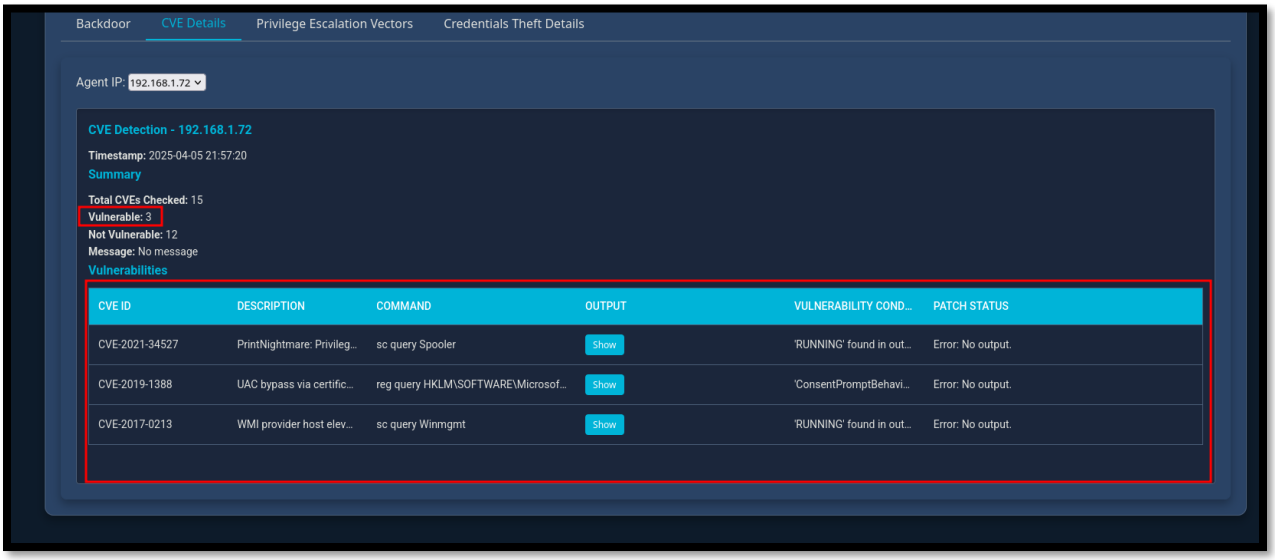


7. The activities logs are viewed in the Activity Log section.

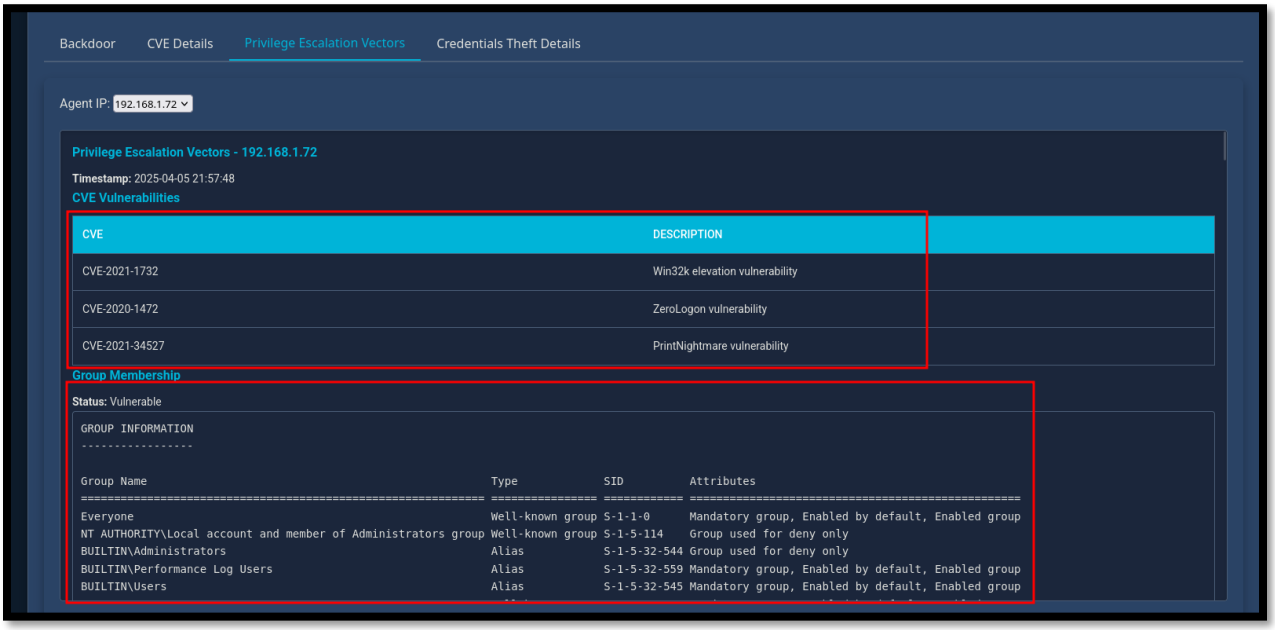
8. When the agent is run in the client's machine, it performs several scans and sends output to the server, in which the backdoor section is viewed as like in above figure.



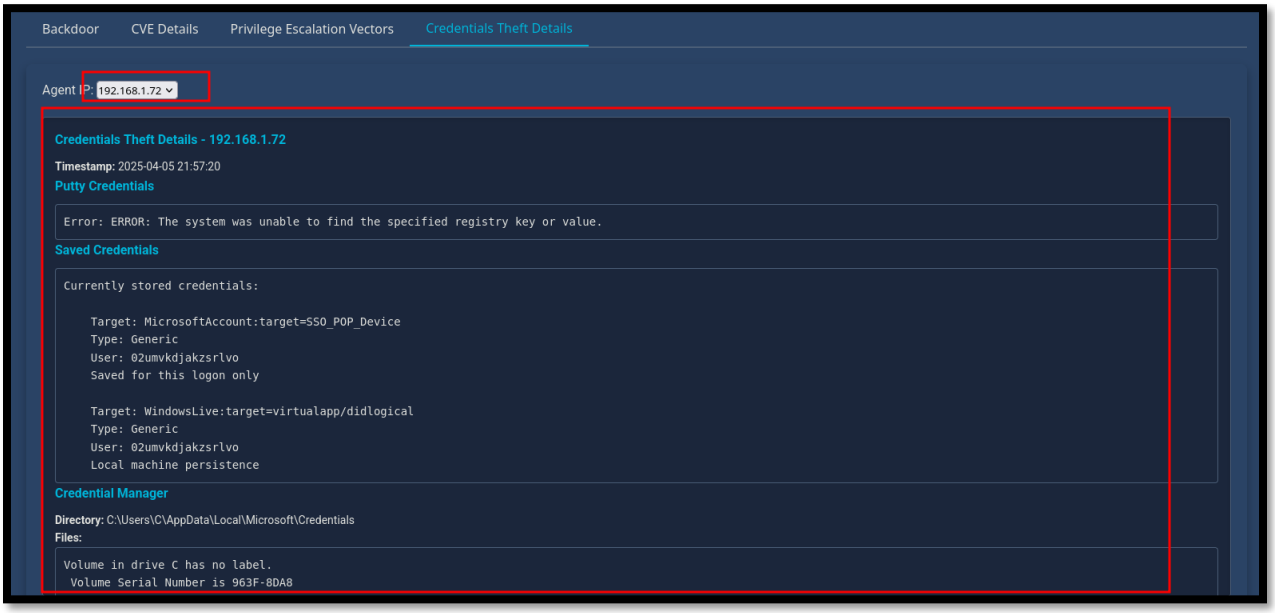
9. In this section, the CVE vulnerabilities that are found in the client's machine are displayed.



10. Here, various privilege escalation vectors and related P.E.s CVEs are scanned in the client's machine and displayed here.



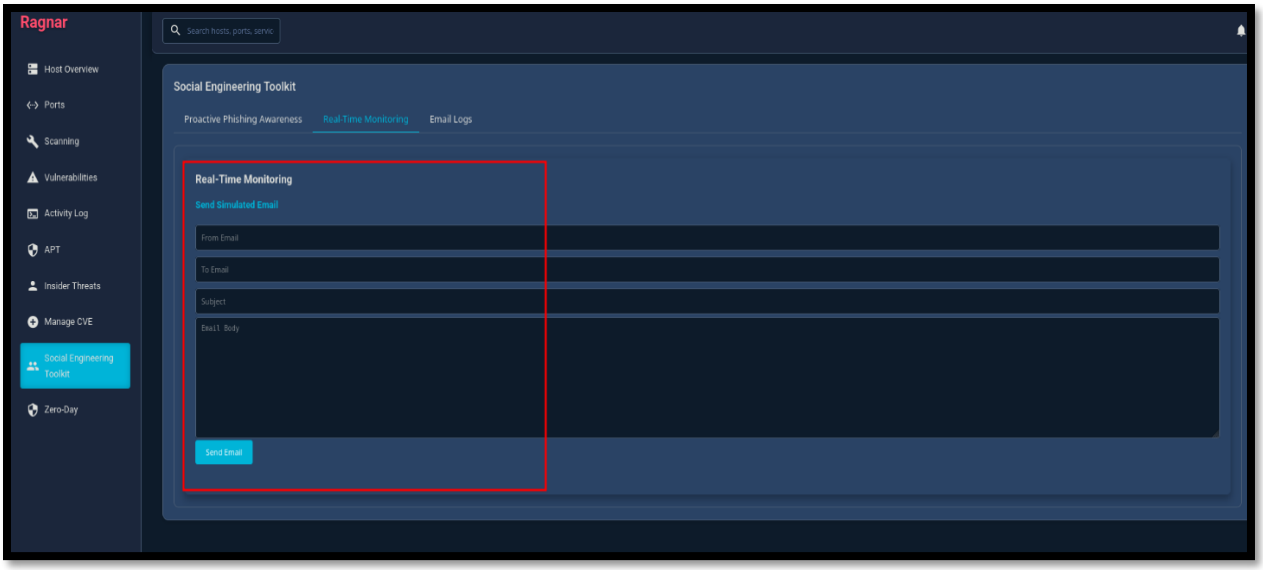
11. In client's machine, the saved credentials from several usual spots are scanned and displayed.



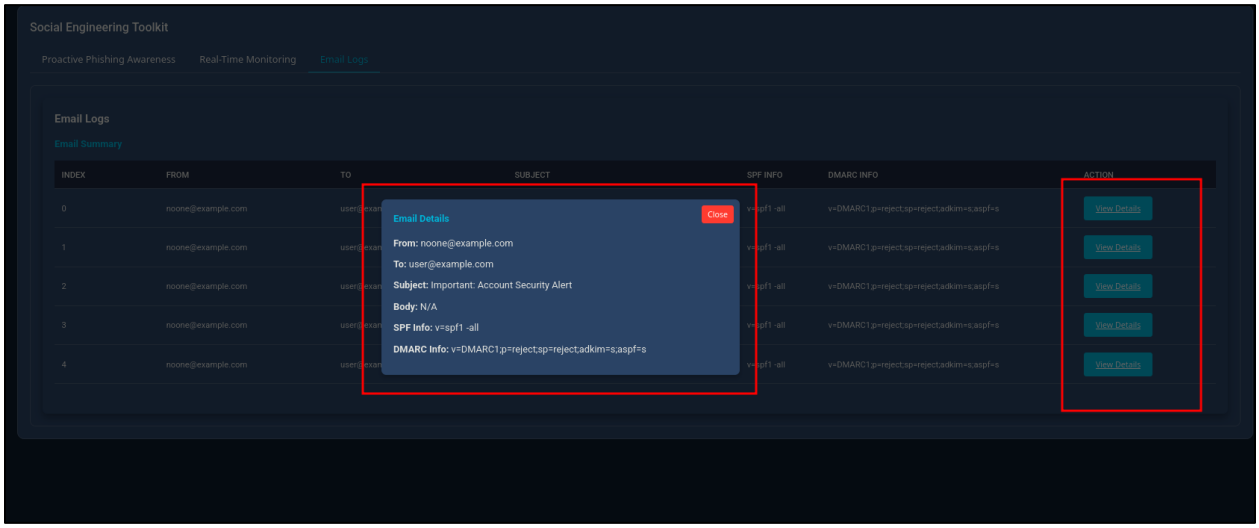
12. As previously mentioned, the templates for CVEs scan can be changed and updated by user and is updated in agent from server URL. It can be updated from the section here.

13. We can run a proactive phishing awareness program where we send fake phishing email to company's employees as per his/her email address. Then when he/she clicks the link, he/she is redirected to awareness video and his/her details are recorded in the server's log. In this way, we can identify the weakest link in the organization which is human factor and can implement several awareness programs to mitigate those types of threats.

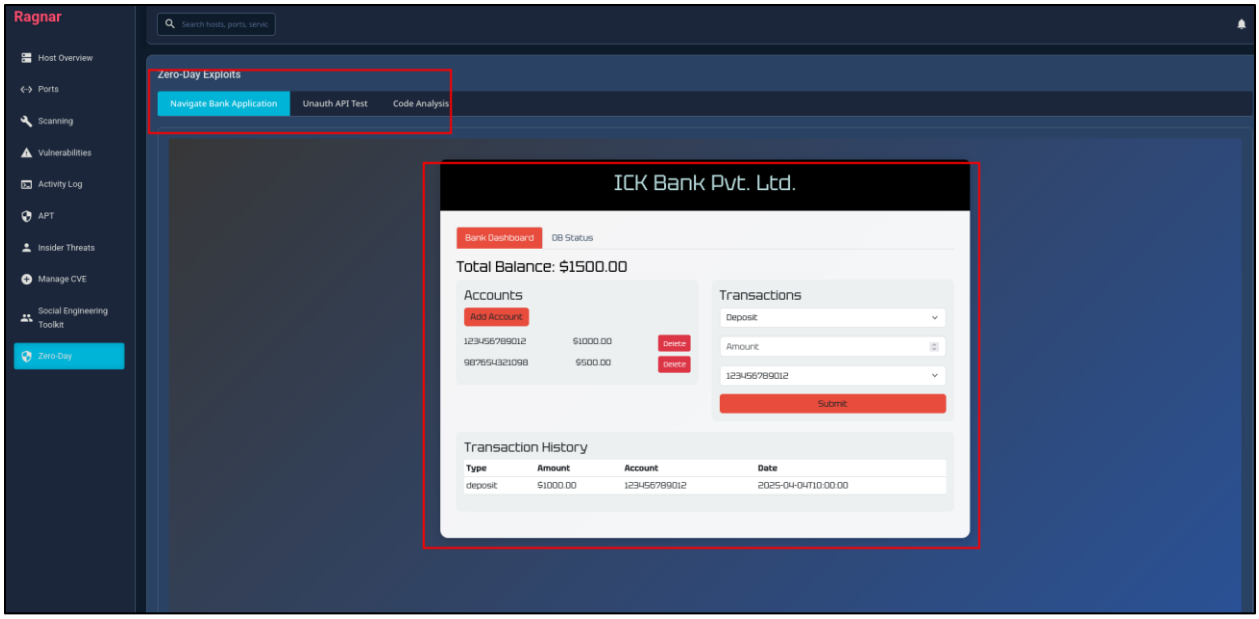
14. We can simulate phishing detection using ML. For that, first we need to send an example malicious mail, and it is shown to be detected and flagged by the analysis logic of hugging face's model.



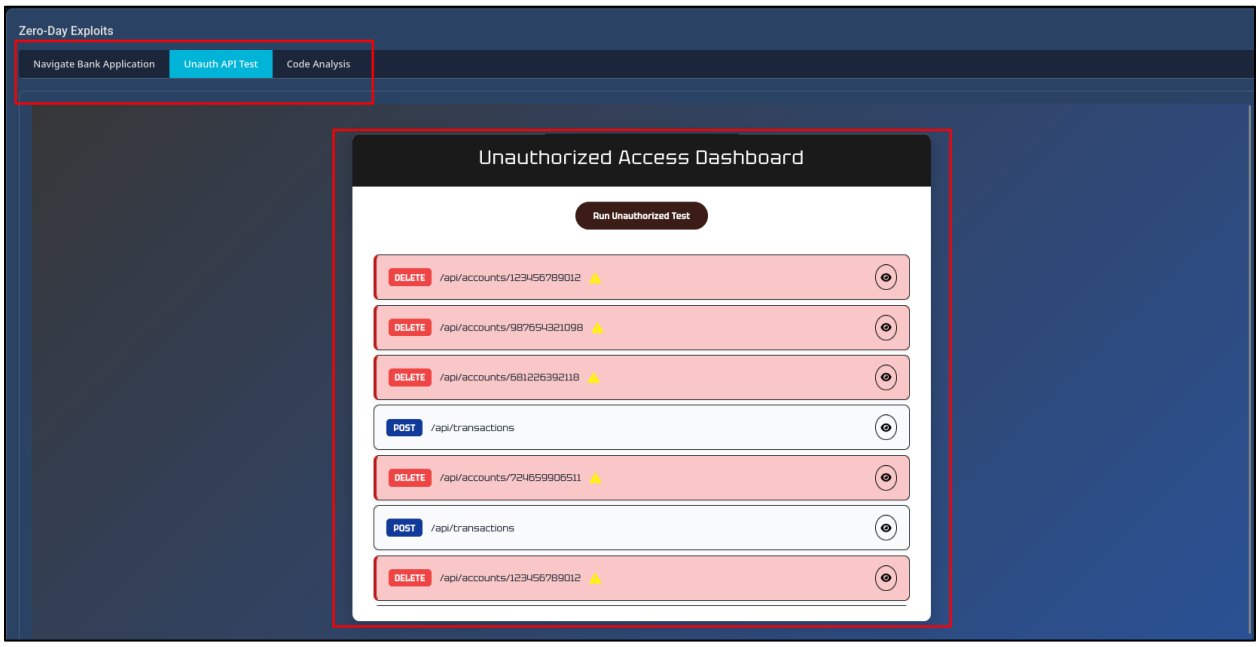
15. In the email logs section, the flagged email can be seen.



16. We can also identify zero-day vulnerability to some extent as per the logic applied in our framework. For test scenario, a bank application's several API endpoints are navigated and recorded in log.



17. Then we can automate the unauthorized access test using single button click according to previously saved API logs.



18. In this framework, static code analysis is also implemented where some used vulnerable functions are flagged and shown as report structure in the UI. For that,

we can just give git repository and if commit hash changed, then it is scanned to identify possible vulnerabilities.