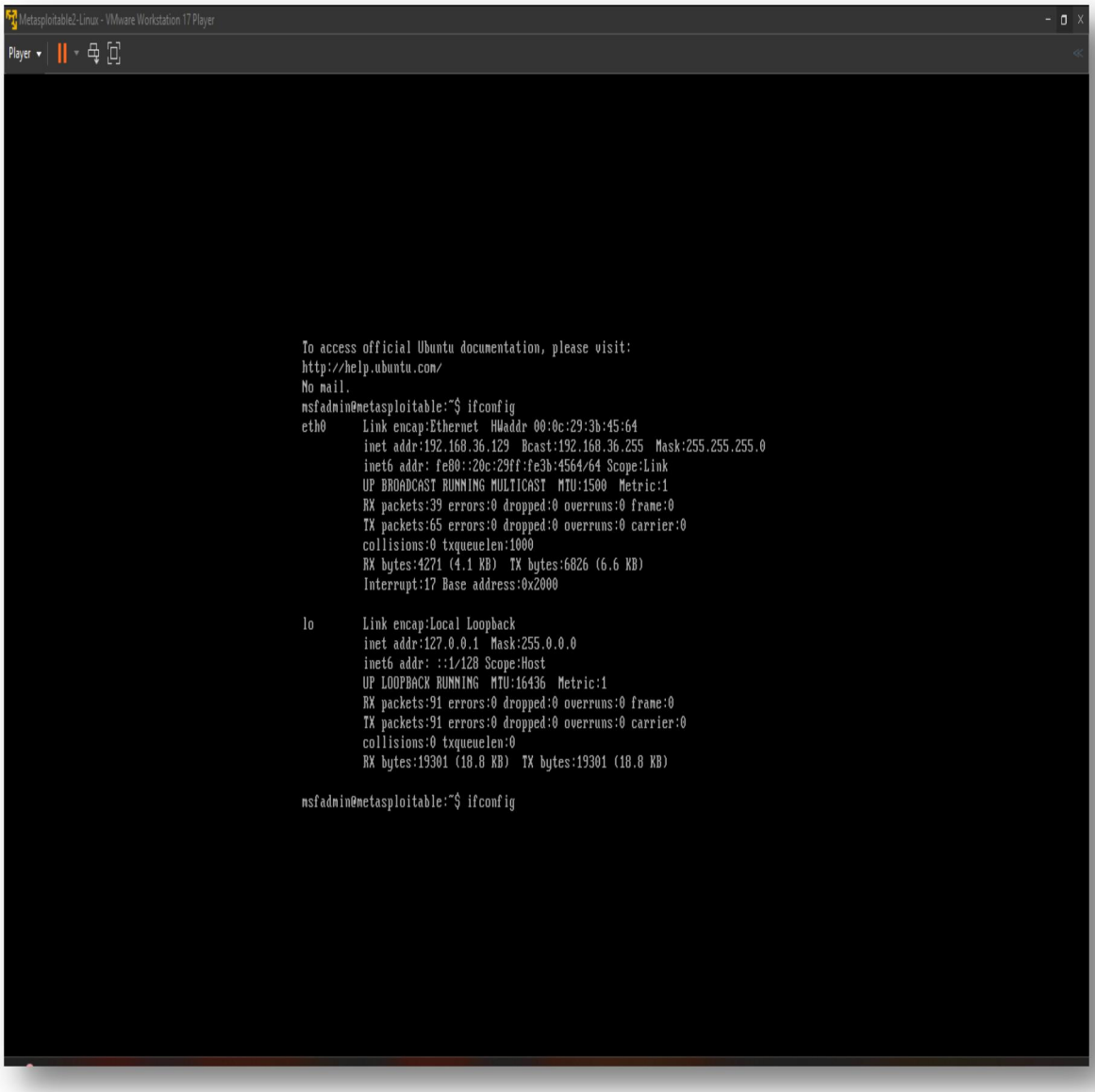
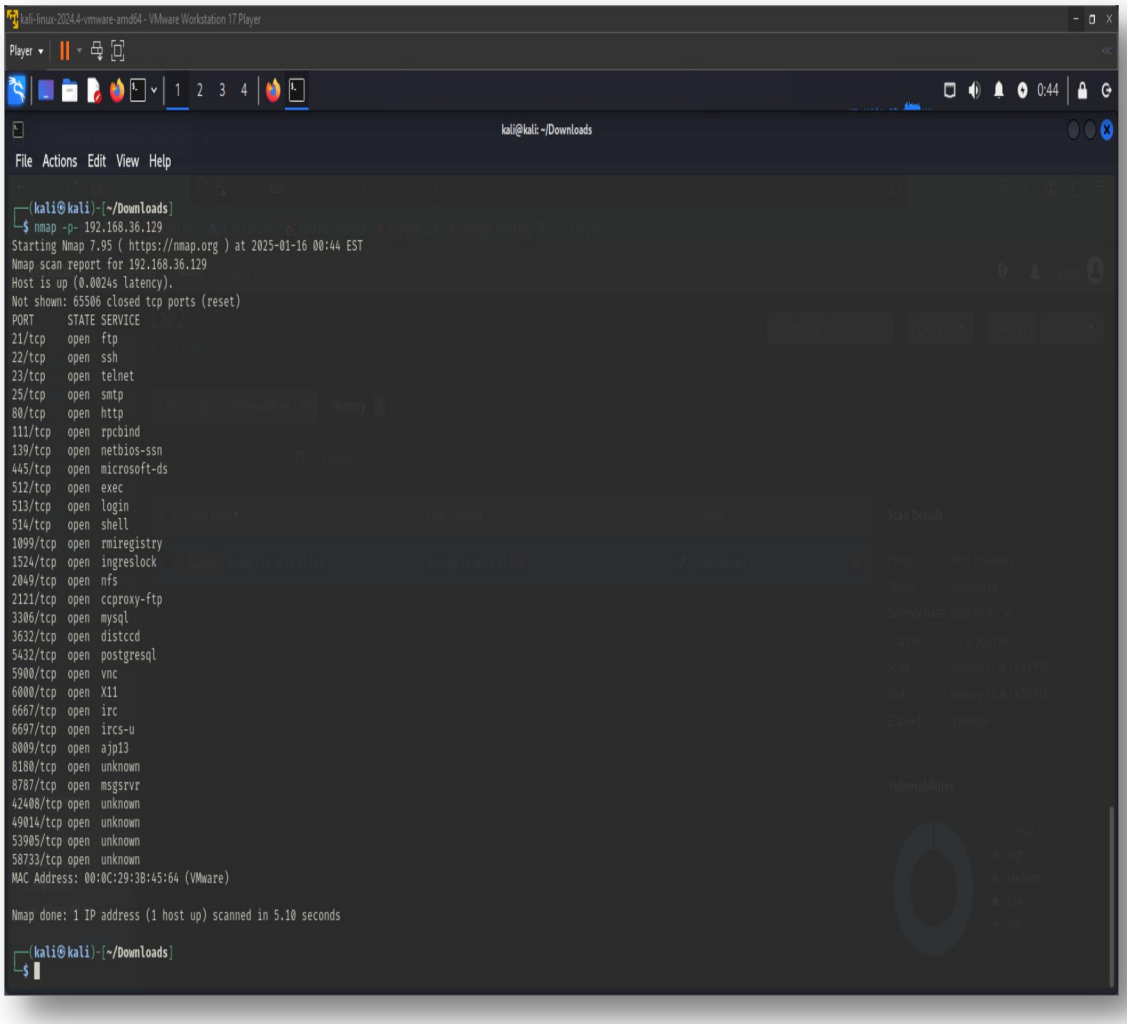
LAB-14

AIM: Conduct Vulnerability assessments and penetration testing of mobile and IOT devices.

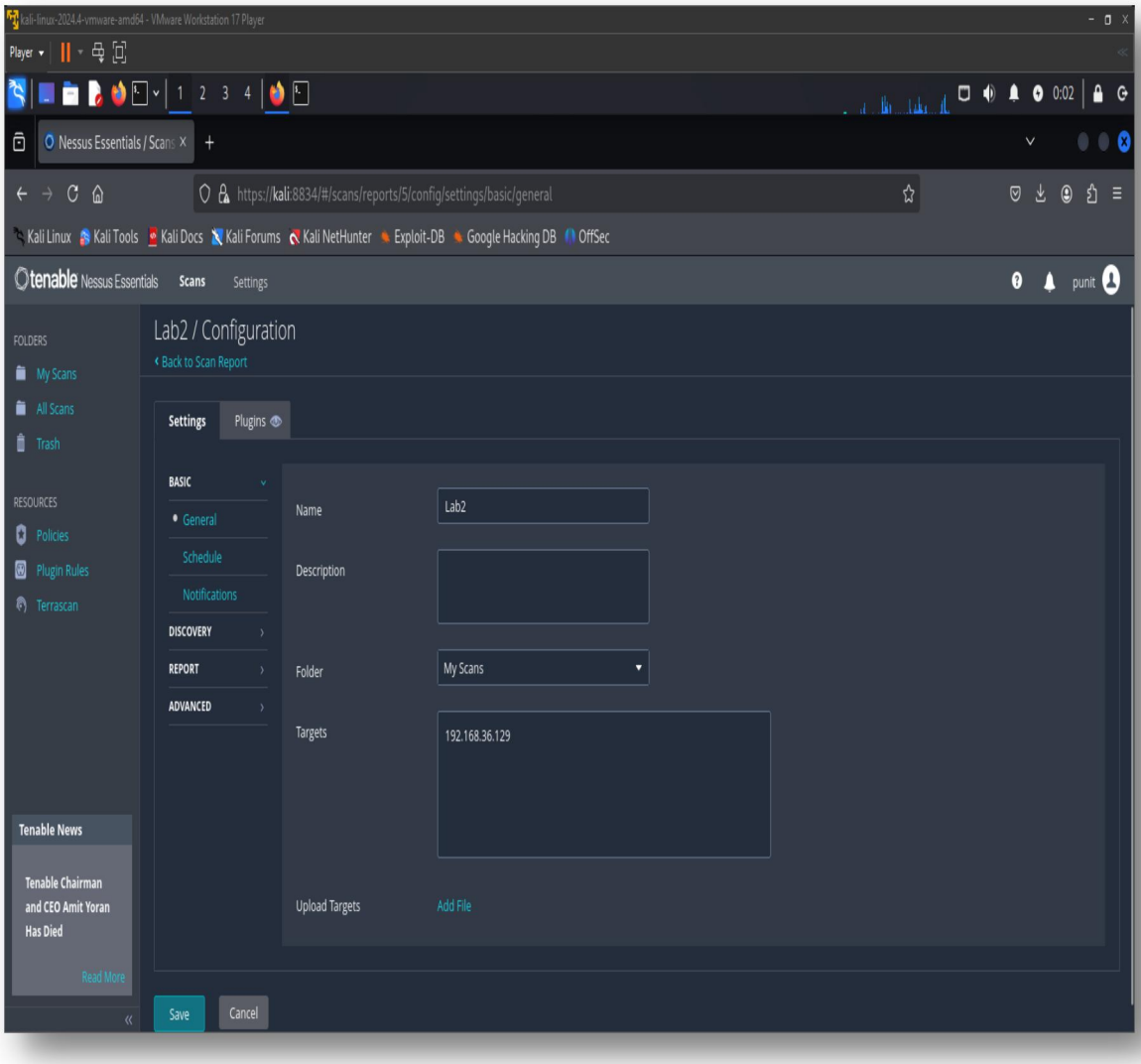
Step-1: Find your IP address in metasploitable and scan that IP address in Nessus to scan that IP address to find the vulnerabilities.



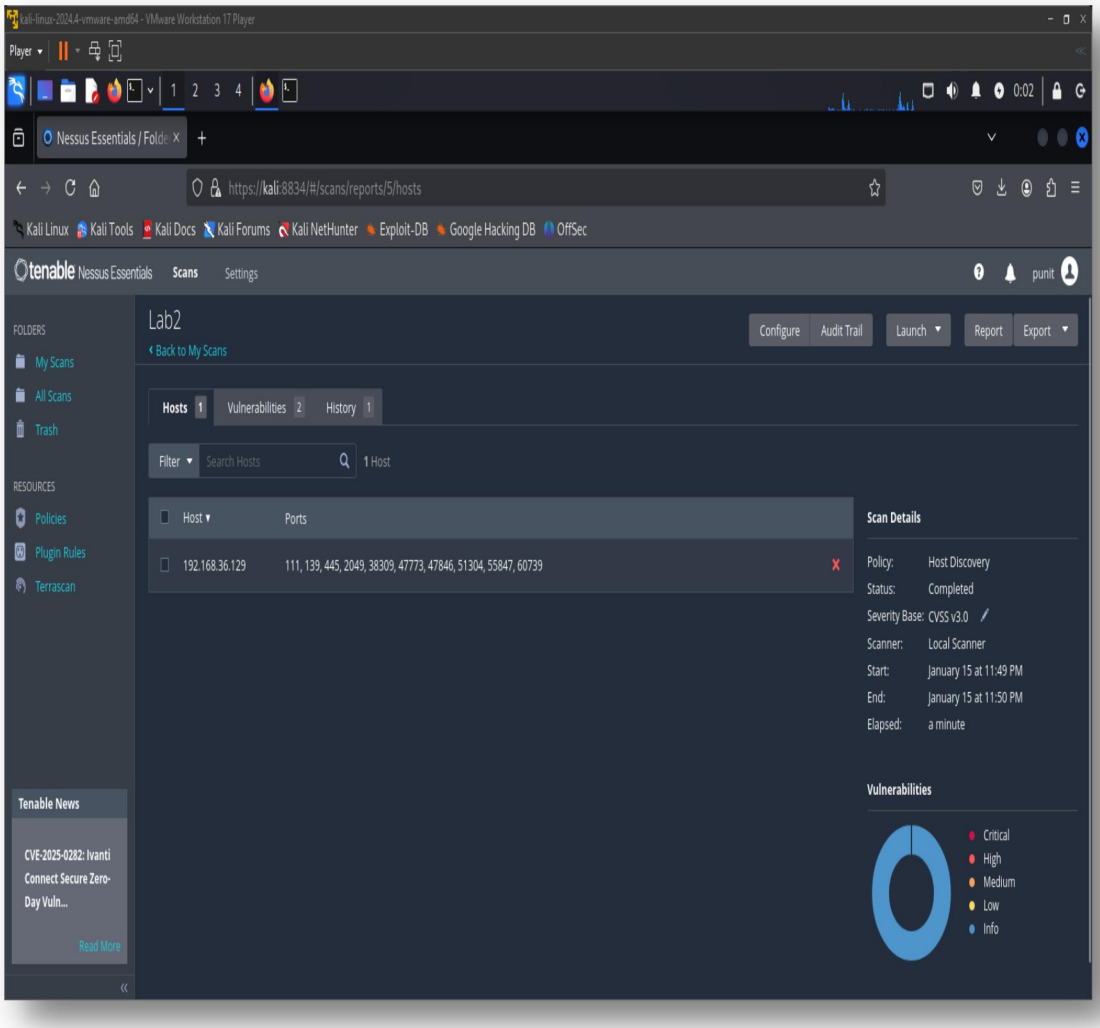
Step-2: Scan Target IP of metasploitable Using Nmap to see the open ports.



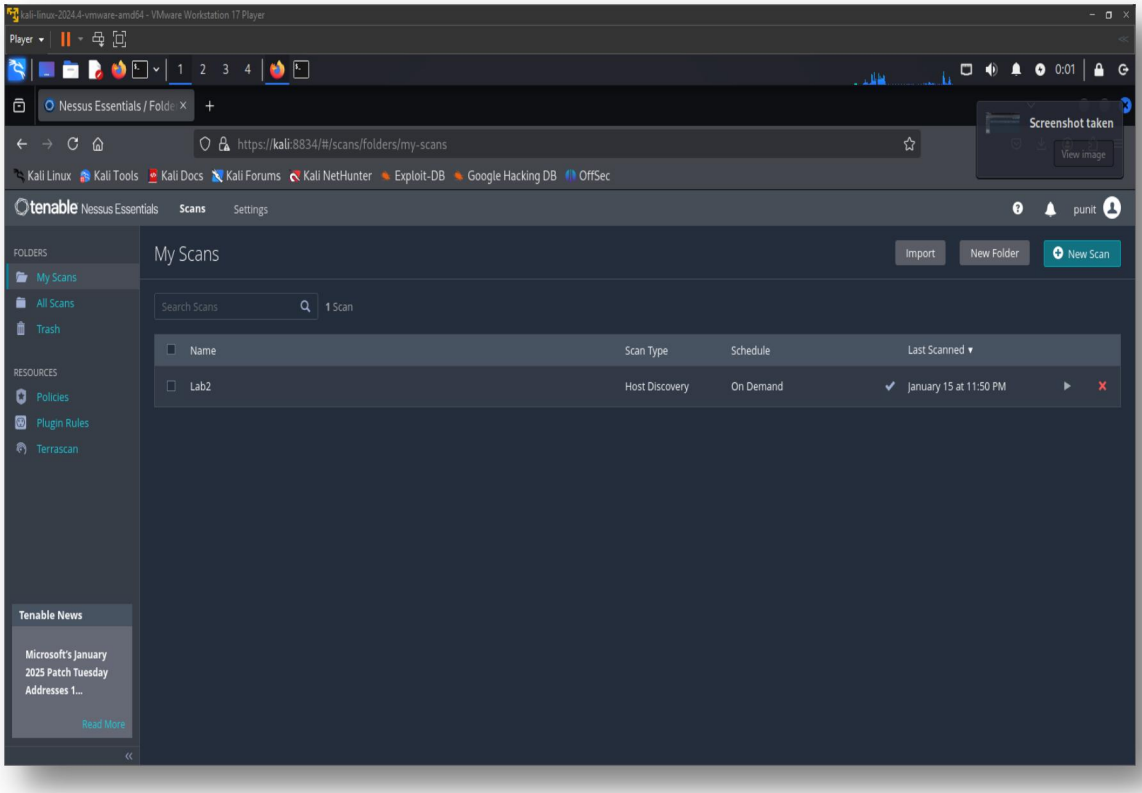
Step-3: In Nessus Go to Host Discovery and enter the target IP that you want to scan and launch to find Vulnerabilities.

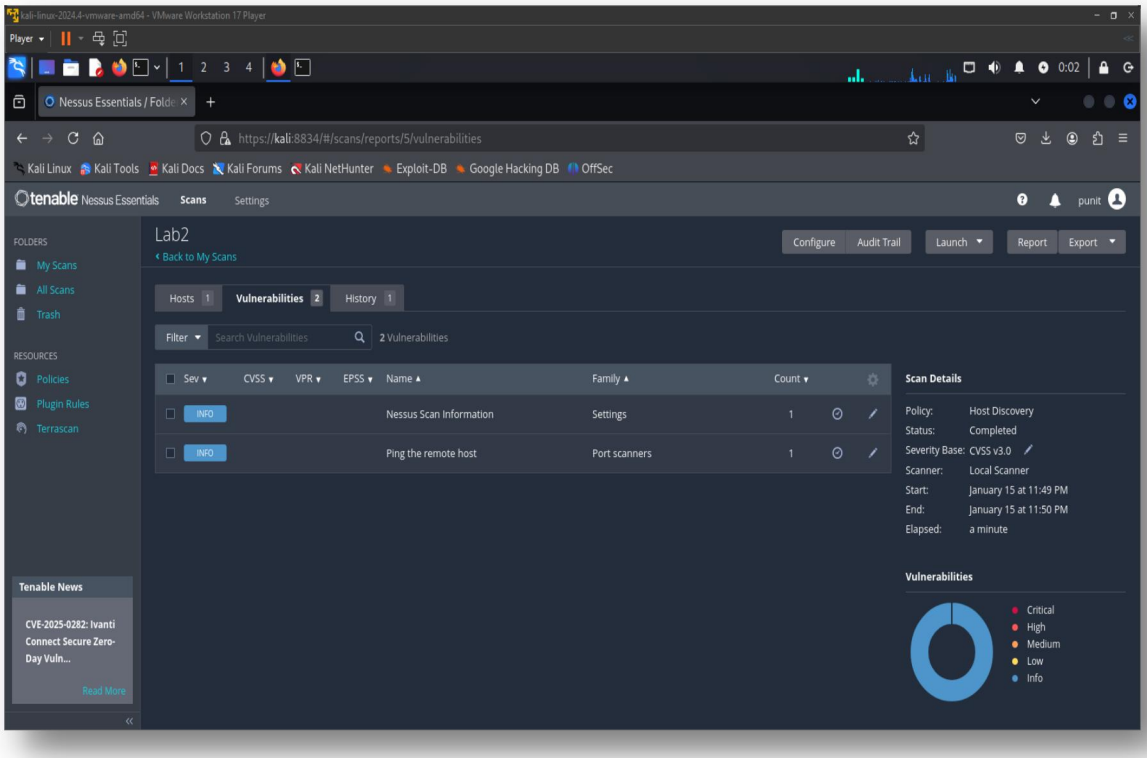


Step-4: After that it will start to scan and after the completion it will show the vulnerabilities that have in the target IP or hosts.

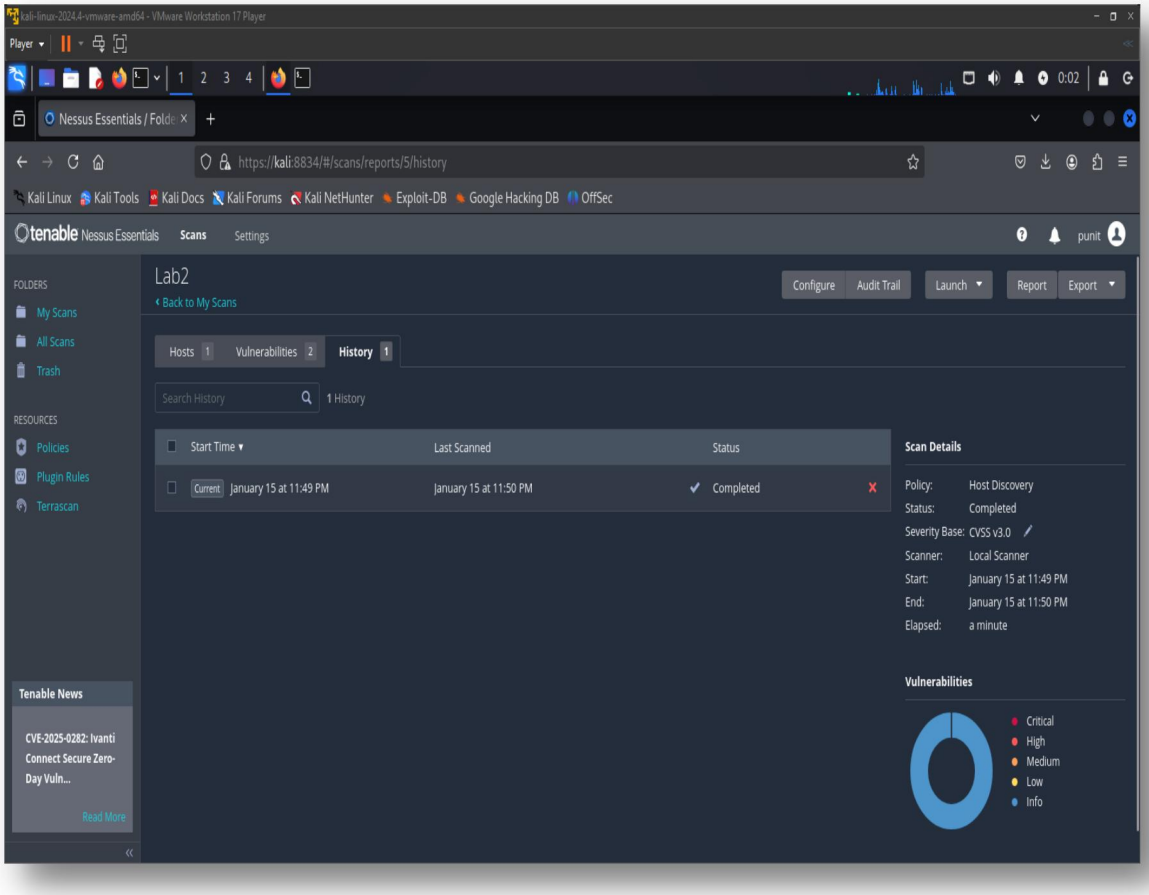


Step-5: Now you are able to see the vulnerabilities that are scanned on that host or target IP and you are able to see the info of that vulnerabilities.





➔ Also You are able to see the History that you scanned.



Conclusion:-

Conducting vulnerability assessments and penetration testing on mobile and IoT devices is essential to identifying and mitigating security risks in today's interconnected world. These assessments help uncover vulnerabilities in device firmware, applications, network communications, and access controls that could be exploited by attackers. By proactively testing and analyzing potential attack surfaces, organizations can strengthen their overall security posture, ensure compliance with industry standards, and protect sensitive user data. As mobile and IoT ecosystems continue to evolve, regular testing and adaptive security measures remain critical to safeguarding both users and infrastructure.