VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

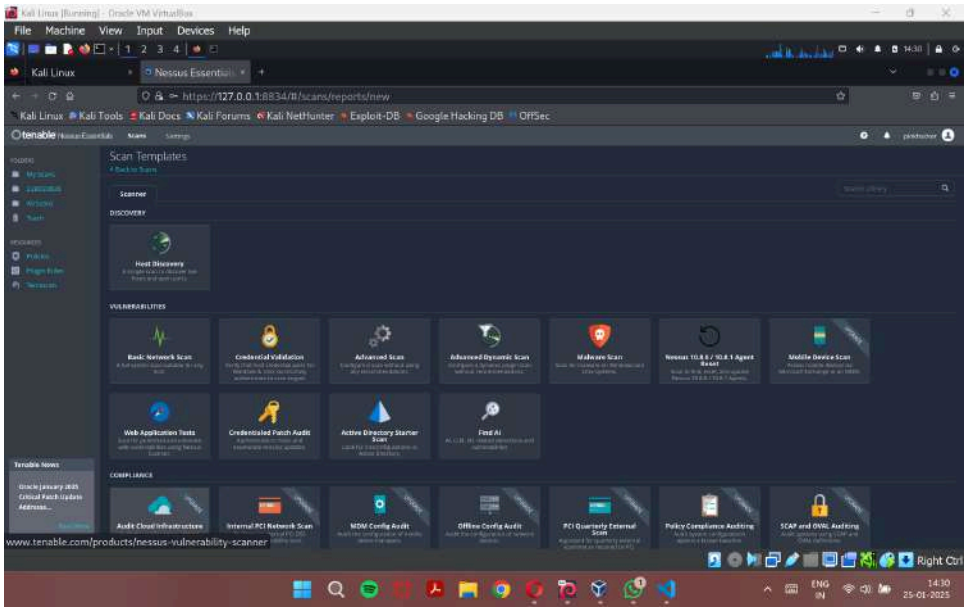
Nessus

NAME: DHEVATHA S P
REG NO.: 22BCE0826

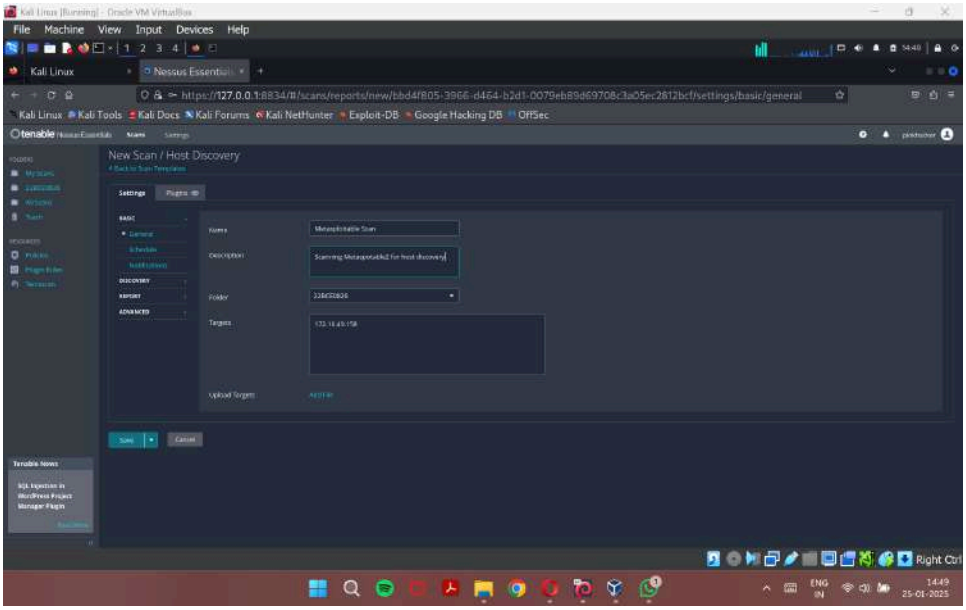
NAME OF FACULTY: DR. Satish C.J
COURSE TITLE : Penetration Testing and Vulnerability Analysis Lab
COURSE CODE: BCSE319P
LAB SLOT: L55+L56
SEMESTER: Winter Semester 2024-25
CLASS NO.: VL2024250505928

Nessus

1. Nessus set-up in Kali Linux. Select Host Discovery for scanning the Metasploitable2.

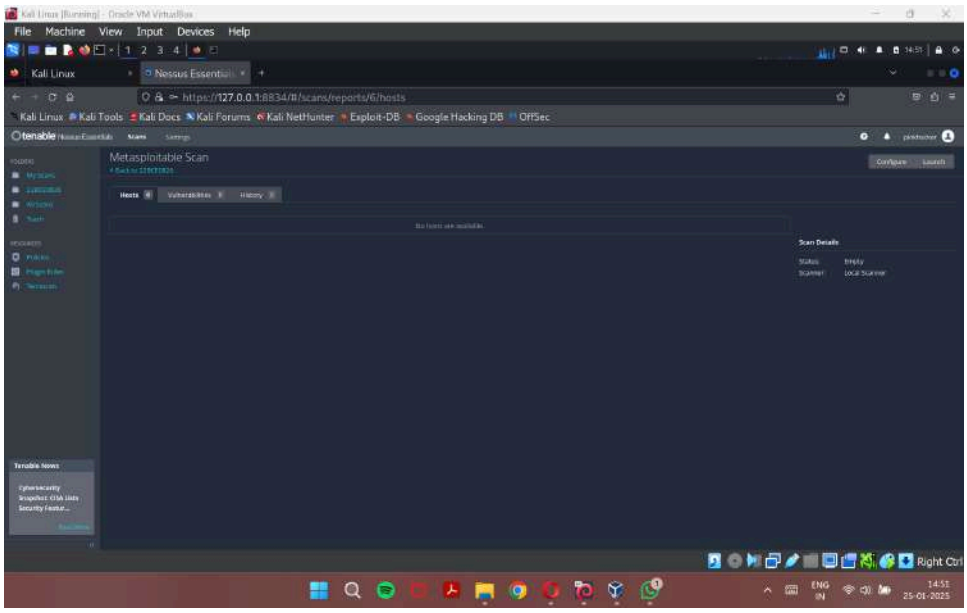


2. Filling up the details for vulnerabilities scan and save

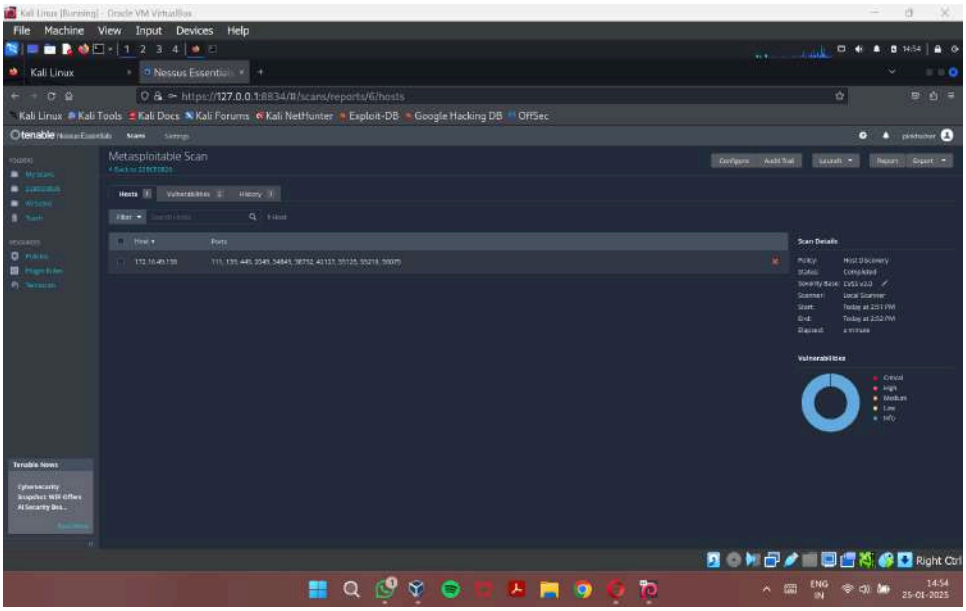


22BCE0826
Dhevatha S P

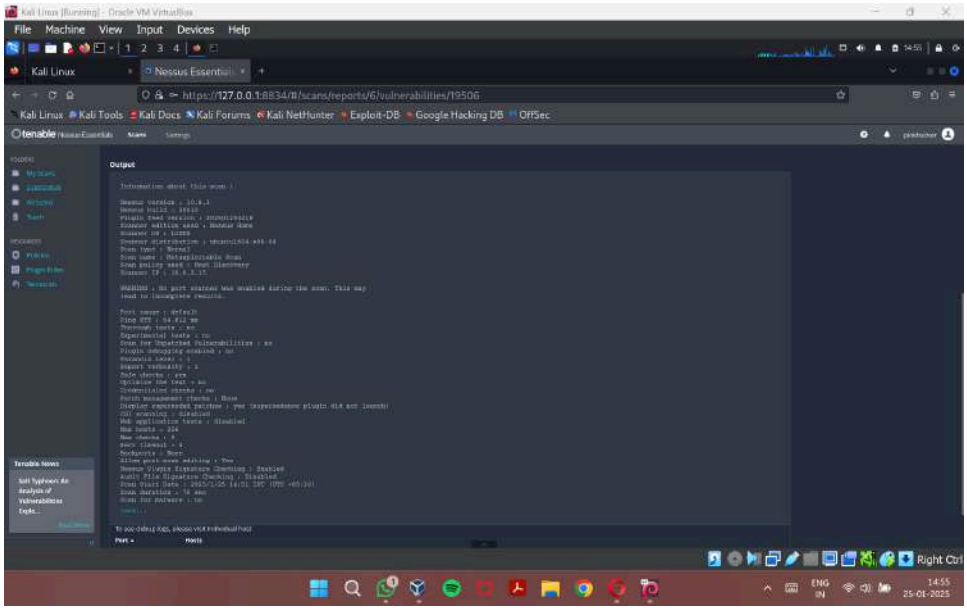
3. Launch the scan



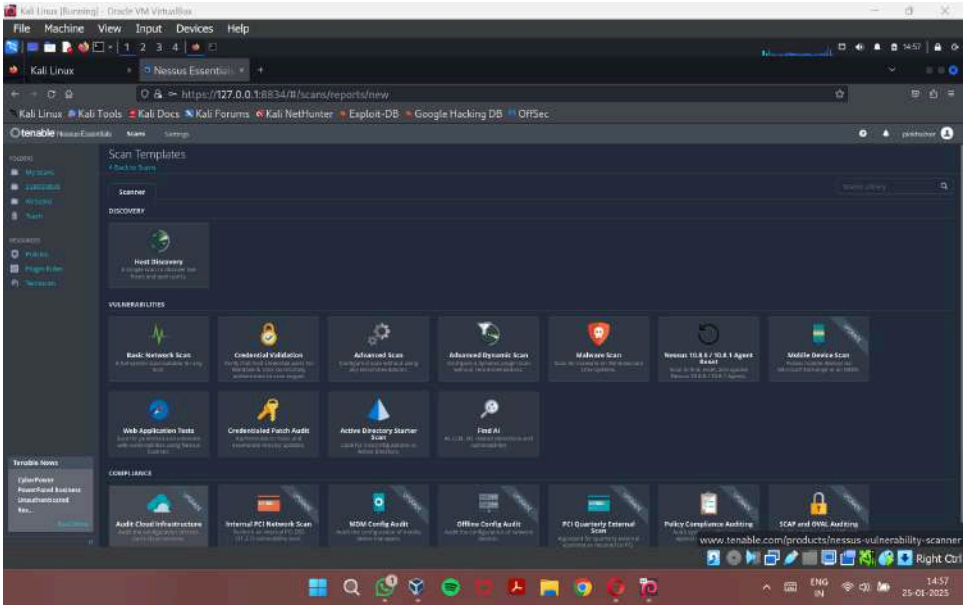
4. Scan results



5. Vulnerability results

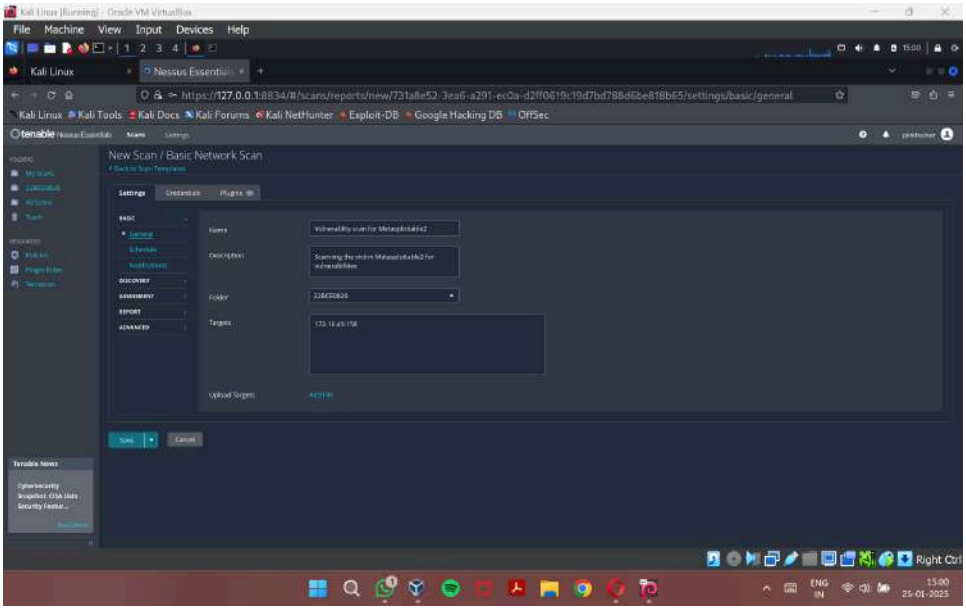


6. Start a new scan for vulnerabilities (choose Basic Network Scan)

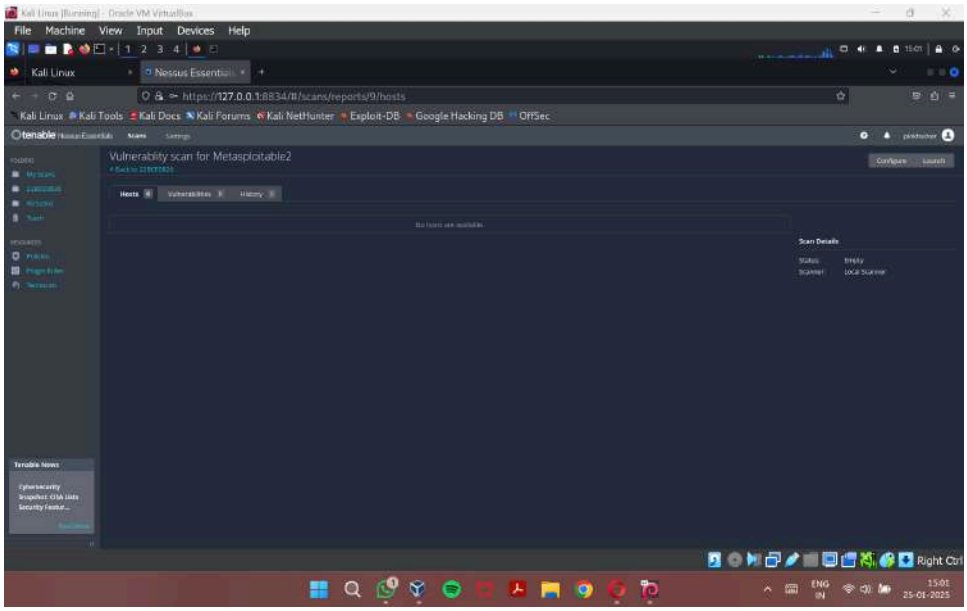


22BCE0826
Dhevatha S P

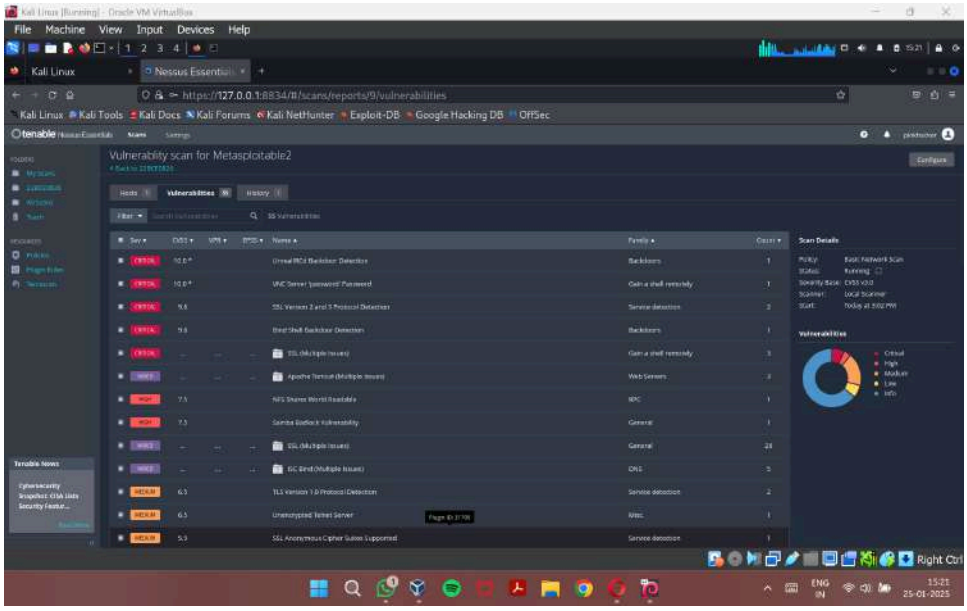
7. Fill as given and leave the rest of the fill ups as default and save



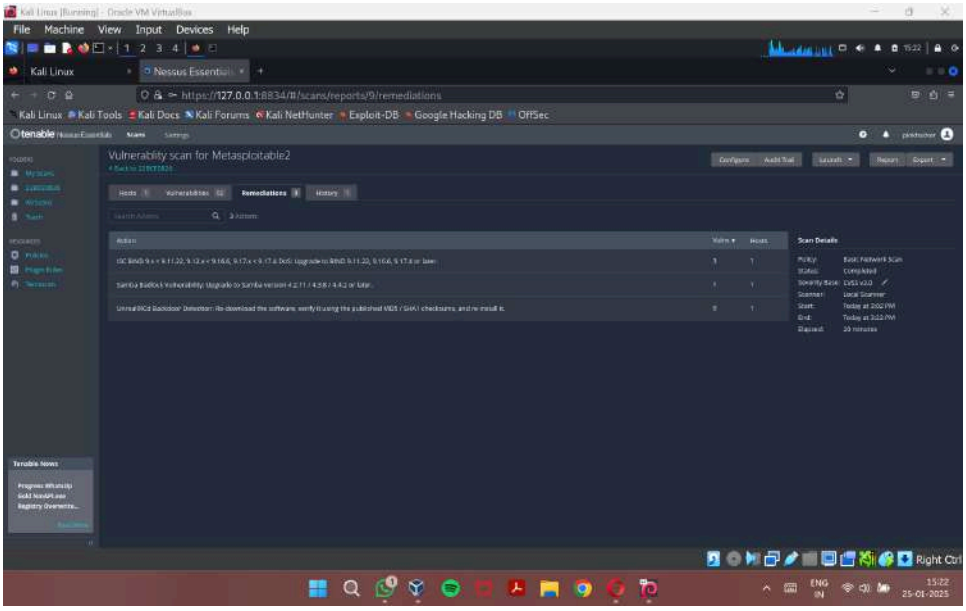
8. Launch the scan



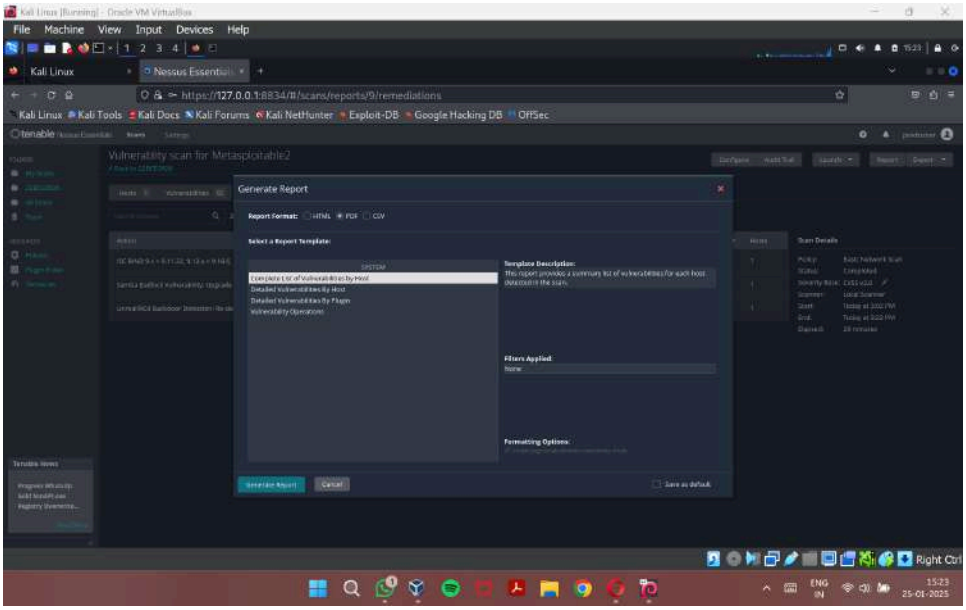
9. Vulnerabilities result and scores



10. Remediations



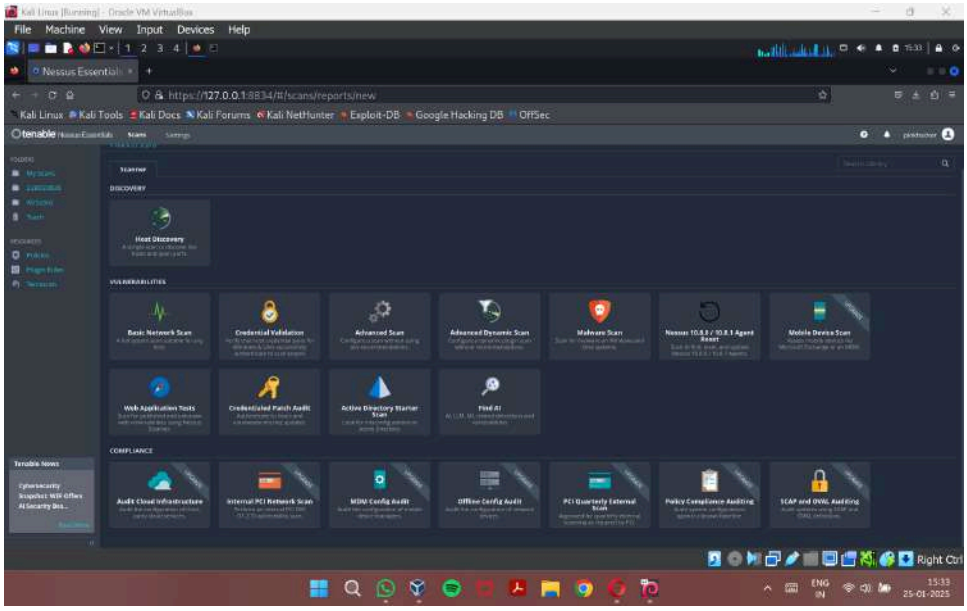
11. Generating report



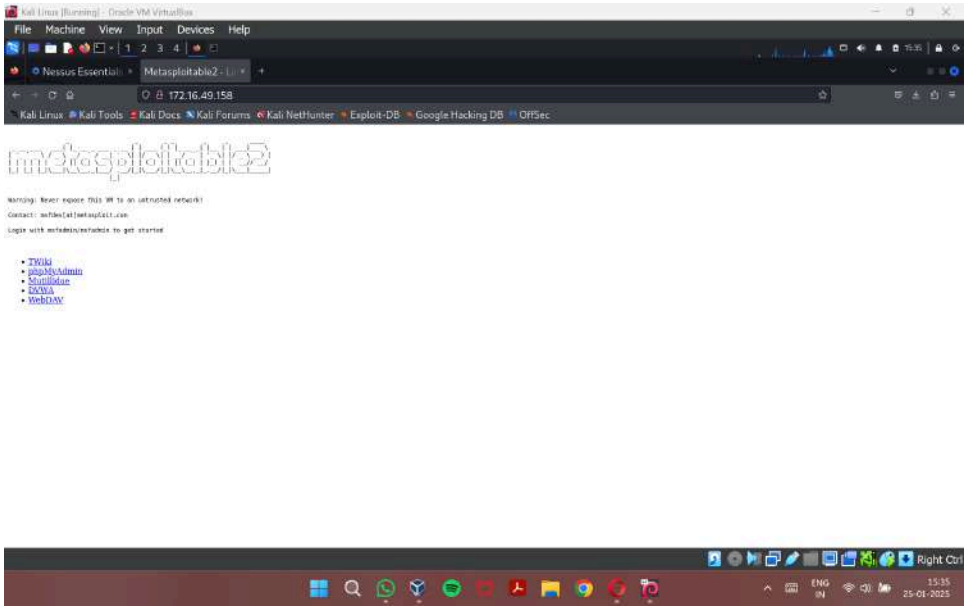
12. Vulnerability Scan Report:

https://drive.google.com/file/d/1BLhM2Kqy1e7la-CsBJEALWN-dPGpwg4A/view?usp=sharing

13.Next scan, scanning website. Choose Web Application Tests

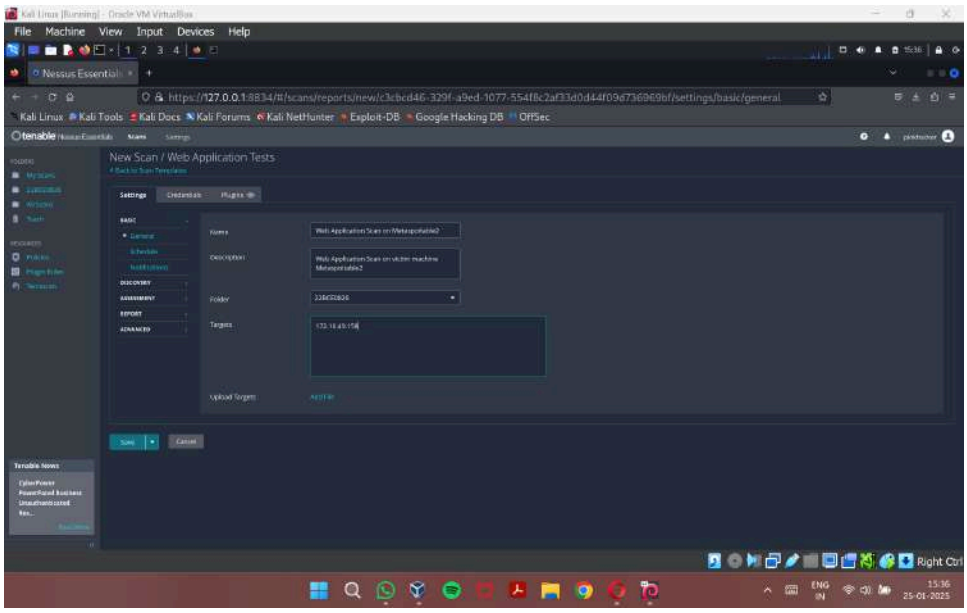


14.The Metasploitable2 web application running in 172.16.49.158

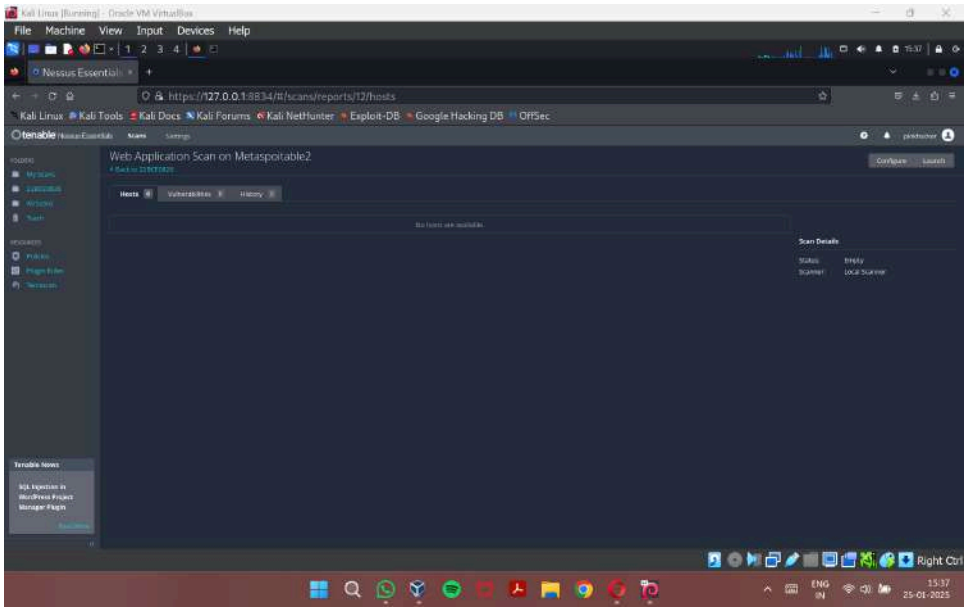


22BCE0826
Dhevatha S P

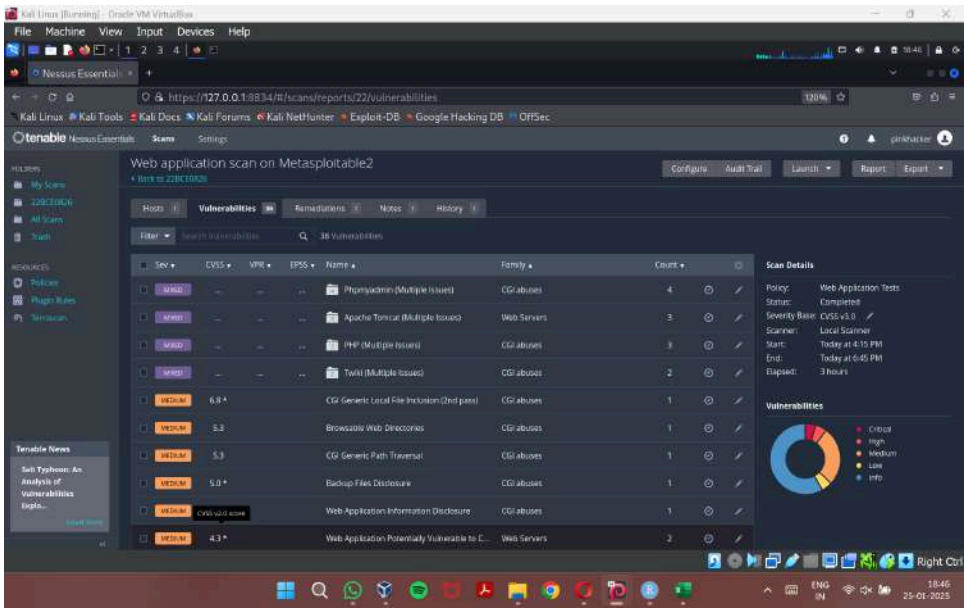
15.Fill as below and leave rest as it is



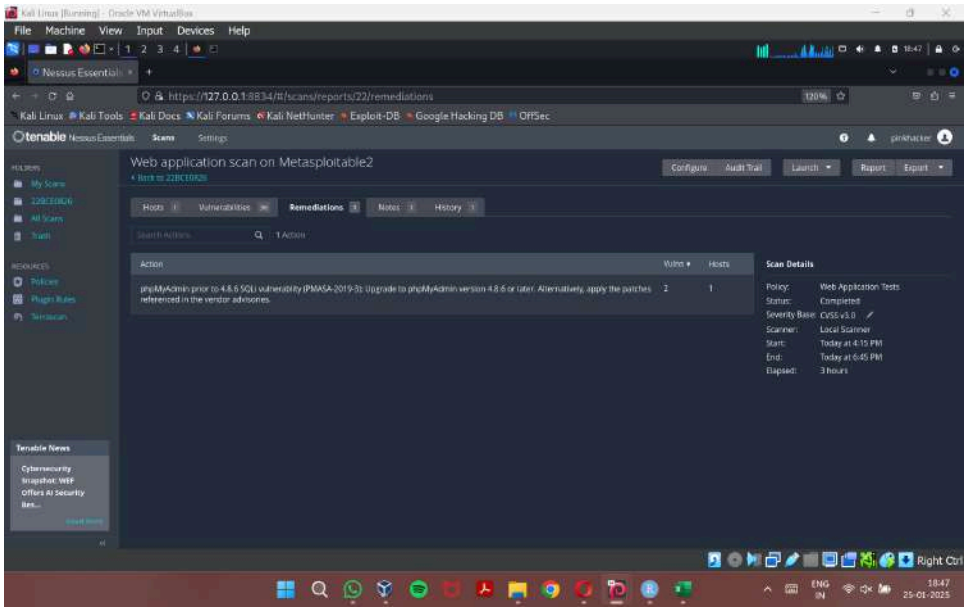
16.Launch the scan



17. Vulnerabilities results



18.Remediations for the Apache TomCat vulnerability



19.Vulnerability Report :
https://drive.google.com/file/d/1TnWvbcrwUyl5qa84y0HnwdyCFTof0Dbh/view?usp=sharing

22BCE0826
Dhevatha S P