project Development Phase
Model Performance Test

Date	10 November 2022
Team ID	PNT2022TMIDxxxxxx
Project Name	Project - xxx
Maximum Marks	10 Marks

Model Performance Testing:

Project team shall fill the following information when working for VAPT testing for a target .

S.No.	Parameter	Values	Screenshot
1.	Information gathering	Footprinting -Collected IP addresses, DNS information, and server details Recconicessines - Identified key technologies, open ports, and publicly available assets	
2.	Scanning the target	Scanning info -Network scan completed, identified active IPs and services Risk factors - Medium to High risks found on ports 22 (SSH), 80 (HTTP), and 443 (HTTPS)	
3.	Gaining access	Access process - Used brute-force on SSH and SQL injection vulnerability in web app Vulnerability found - SQL Injection, SSH misconfiguration	
4	Maintaining access - Automation (AI implementation)	AI tools used -	

		AI-enabled vulnerability scanner, automated penetration testing scripts Automation implemented - Scheduled vulnerability scanning, automated alert for privilege escalation attempts	
5	Covering Tracks & Report	Vulnerability risk factors - High-risk vulnerabilities documented (e.g., SQL injection, misconfigured access controls) VAPT report - Full VAPT report generated, including detailed findings, risk level, mitigation steps, and remediation timeline	