



THE PAGE

STARTING IN 2024

- **Problem Statement ID – 1684**
- **Problem Statement Title- Agent-less
Windows System Vulnerability and Network
Scanner**
- **Theme- Blockchain & Cybersecurity**
- **PS Category- Software**
- **Team ID-**
- **Team Name (Registered on portal)**



SMART INDIA HACKATHON 2024



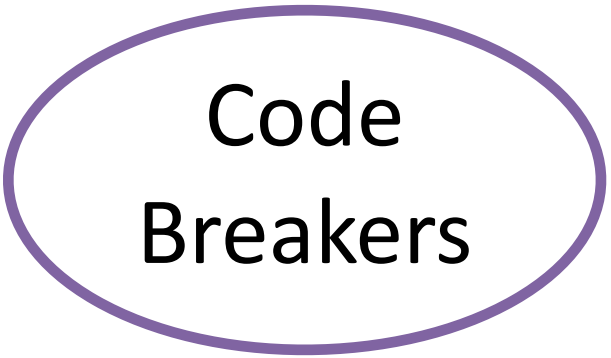
Agent-WindowSystemVulnerabilityandNetworkScanner

Detailed explanation of the proposed solution

- Our solution is an agent-less vulnerability and network scanner for Windows OS, using **blockchain, cybersecurity**, and **AI/ML** technologies.
- It leverages native tools like WMI and PowerShell to perform system and network-level vulnerability assessments by analyzing configurations, user accounts, firewall rules, and open ports.
- It integrates with threat intelligence databases like ExploitDB and CVE to identify known vulnerabilities and provide remediation steps.
- Using blockchain for secure logging ensures tamper-proof records, while AI/ML models perform anomaly detection and risk prediction to improve detection accuracy.
- The findings are compiled into a comprehensive PDF/HTML report with mitigation strategies, offering a smart, secure, and innovative solution for system security.

How it addresses the problem

- **Addresses Vulnerabilities:** Identifies outdated or misconfigured Windows systems to prevent security risks.
- **Agent-less Deployment:** No installation needed, reducing complexity and minimizing attack surfaces.
- **Proactive Security:** Maps system and network vulnerabilities to help users secure their systems.
- **Automated Reporting:** Ensures continuous monitoring and quick remediation of vulnerabilities.



Code
Breakers



SMART INDIA HACKATHON 2024

Innovation and uniqueness of the solution

- **Agent-less Approach:** Operates without requiring an agent, reducing system overhead and integrating seamlessly with native tools like PowerShell and WMI.
- **Blockchain Integration:** Ensures tamper-proof, immutable logging of scans, enhancing data integrity in cybersecurity.
- **AV/EDR Friendly:** Complements existing AV and EDR tools, working alongside them for comprehensive security coverage.
- **AI/ML and Threat Intelligence:** Uses AI/ML for anomaly detection and integrates threat intelligence for real-time vulnerability identification and patching.
- **Comprehensive Scanning:** Provides system and network assessments with automated reports for easy remediation.