





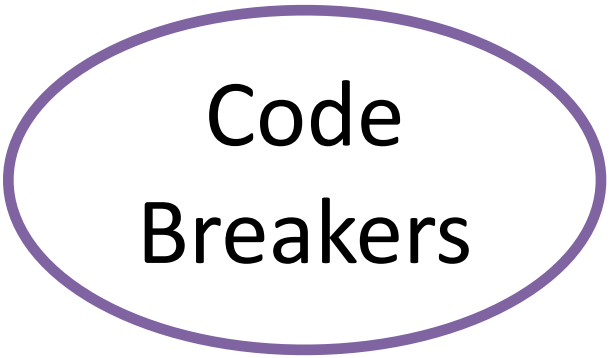


# **Detailed explanation of the proposed solution**

- 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- **Addresses Vulnerabilities:** Identifies outdated or misconfigured Windows systems to prevent security risks.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.

A thick purple oval border surrounds the text.

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.

THE CHINESE ARCH



## **Frameworks and Libraries:**

- **WinPEAS:** For system enumeration and vulnerability discovery.
- **Posh-Sysmon / Posh-SecMod:** For advanced Windows event logging and network scanning.
- **ExploitDB, CVEDetails:** For crawling and fetching relevant vulnerabilities and exploits.
- **TensorFlow/PyTorch:** For AI integration to detect anomalies and predict vulnerabilities.

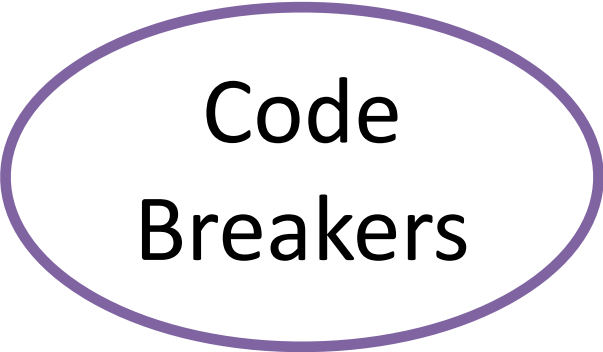
## **Tools:**

- **WMI (Windows Management Instrumentation):** For gathering system-level data.
- **SecurityPolicyDSC:** For checking compliance with Windows security policies.
- **WinCDP / LDWin:** For network scanning and mapping.





# **SMART INDIA HACKATHON 2024**



Code  
Breakers

**Methodology**  
**and process for**  
**implementation:**

***Technologies to be used:***

---



01

System & Network Enumeration:  
Use WMI and PowerShell to gather details on system configurations, software, user accounts, firewall rules, and network connections.

02

Vulnerability Detection:  
Compare collected data with databases like ExploitDB and CVEDetails to detect vulnerabilities.

03

AI-Powered Anomaly Detection:  
Implement AI to identify abnormal system and network behaviors that may indicate security issues.

04

Blockchain Logging:  
Record scan results on a blockchain, ensuring tamper-proof logs and secure, immutable data storage.

05

Report Generation:  
Generate detailed PDF/HTML reports with identified vulnerabilities, risk assessments, and remediation recommendations.