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:


SQL

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.

FEASIBILITY AND VIABILITY

Potential challenges and risks

- Restricted permissions on machines may limit the tool's ability to scan all areas of the system.
- AI-powered anomaly detection could flag non-critical issues, leading to unnecessary alerts.
- Scanning may consume significant system resources on low-end devices, impacting performance.
- Accessing and scanning sensitive system data could raise potential privacy and compliance issues.
- Relying on outdated databases may result in missing recent vulnerabilities or false security assessments.
- Storing scan logs on blockchain without proper encryption could expose sensitive system information.

Strategies for overcoming these challenges

- **False Positives**: Regularly refine AI models using real-world data and feedback to minimize incorrect alerts.
- **Performance**: Schedule scans during system idle times or run in small batches to reduce resource impact on low-end systems.
- **Privacy Concerns**: Ensure read-only operations with encryption and data masking to safeguard sensitive information.
- **Outdated Vulnerability Data**: Automate updates from trusted sources to keep vulnerability data current and relevant.
- **Blockchain Data Security**: Implement encryption for blockchain-stored logs to ensure tamper-proof records while protecting sensitive data.

SMART INDIA HACKATHON 2024

Code Breakers

Analysis of the feasibility of the idea

- ***Technological***:

➢ The solution leverages proven tools like WMI, PowerShell, and vulnerability databases (e.g., ExploitDB).

➢ AI/ML for anomaly detection is supported by existing libraries, making real-time vulnerability assessments achievable.

➢ Additionally, blockchain technology ensures secure and immutable logging of scan results, preventing tampering or unauthorized modifications.

- ***Operational***:

➢ The agent-less design simplifies deployment across Windows 10/11, reducing overhead and eliminating the need for additional software.

➢ The solution integrates smoothly with AV/EDR systems and scales easily for both individual and enterprise use.

➢ Blockchain enhances security by ensuring tamper-proof logs, adding an extra layer of trust and data integrity.