

“Research Paper on HESS: An Endpoint Security Tool”

1st Dr.Nilesh T.Gole
DEpt.Of Computer Science
&Engineering Vidarbha Insitute of
Technology, Nagpur
Email:n.gole@vitnagpur.edu.in

3rd Mr. Piyush Hedau
DEpt.Of Computer Science
&Engineering Vidarbha Insitute of
Technology, Nagpur

2nd Mr. Prathmesh Dhoble
DEpt.Of Computer Science
&Engineering
Vidarbha Insitute of Technology, Nagpur

4th Mr. SAIYED AMIR ALI
DEpt.Of Computer Science
&Engineering Vidarbha Insitute of
Technology.Nagpur

5th RUTUJA NAKHATE
DEpt.Of Computer Science
&Engineering. Vidarbha Insitute of
Technology.Nagpur

Abstract—

In the current rapidly evolving digital landscape, cybersecurity has shifted from being a luxury for large scale corporations to an absolute survival necessity for Micro, Small, and Medium Enterprises (MSMEs). These smaller organizations are frequently targeted by automated cyberthreats because they lack the high budget security infrastructure and specialized human resources required for continuous monitoring. This thesis presents the development of HESS (Host Endpoint Security Scanner), a centralized, agent based security scanning ecosystem designed to eliminate the common "visibility gaps" in distributed office networks. The core research addresses the inefficiency of manual security audits by introducing a Distributed System Architecture. In this framework, lightweight Python agents are deployed across multiple Windows endpoints to communicate with a central FastAPI based orchestration server. Unlike traditional scanners that focus solely on malware, HESS performs a multi dimensional audit of the host s security posture, including Windows Firewall configurations, critical Network port exposures (such as RDP and SMB), hardware level hardening (BitLocker, TPM, and Secure Boot), and Identity hygiene (blank passwords and administrative privilege c ounts). A key contribution of this project is the Automated Risk Scoring Engine, which translates complex, raw technical data into a simplified 0 100 Security Posture Score. This allows nontechnical administrators to immediately identify high risk assets w ithin their network. Furthermore, the system ensures data integrity through HMAC (Hash based Message Authentication Code) verification, preventing unauthorized or spoofed scan results.The research culminates in the automated generation of structured Excel and PDF reports that provide clear remediation steps, effectively bridging the compliance gap for regulations such as provide clear remediation steps, effectively bridging the compliance gap for regulations such as the DPDP Act 2023 and CERT In guidelines. Practical testing in a c ontrolled LAN environment demonstrates that HESS significantly reduces audit time while providing a production grade, scalable solution for enterprise level endpoint hardening A key contribution of this project is the Automated Risk Scoring Engine , which translates complex, raw technical data into a simplified 0 100 Security Posture Score. This allows nontechnical administrators to immediately identify high risk assets within their network. Furthermore, the system ensures data integrity through HMAC (Hash based Message Authentication Code) verification, preventing unauthorized or spoofed scan results.

1. INTRODUCTION

In the current era of rapid digital transformation, the security of endpoints, which are basically the laptops and desktops used by employees, has become the biggest headache for any organization.

Especially for Micro, Small, and Medium Enterprises (MSMEs) in India, the situation is quite dangerous. While these companies are moving all their data to cloud and using digital tools for GST or inventory, their basic computer security is often neglected. Most small offices think they are "too small to be a target," but the reality is that hackers use automated bots to scan the entire internet for weak spots. If one PC in a small office has a disabled firewall or an exposed RDP port, the entire business network can be encrypted by ransomware in minutes. The core p roblem is that maintaining security across multiple machines is a very slow and manual process. Usually, an IT admin has to physically go to every desk to check if BitLocker encryption is on or if someone is using a blank password. This "Manual Audit" is n ot only boring but also full of human errors. By the time the admin checks the last computer, the first one might already be compromised because the user changed the setting. There is a massive "Visibility Gap" where the management has no idea if their off ice is 10% safe or 90% safe.. HESS works on Distributed System Design. We have lightweight Python agents that sit on every client machine and a central FastAPI based server that acts as the brain. The system doesn't just look for viruses; it audit s the entire "Security Posture." It checks Firewall rules, open ports like SMB (445) and RDP (3389), hardware hardening like TPM and Secure Boot, and identity hygiene like admin account counts. The most important feature of HESS is the Automated Risk Scoring Engine. It takes all the raw technical data and converts it into a simple 0 100 score. If a PC has a critical hole, the score drops, and the admin gets an alert. To make it professional and audit ready, the system automatically generates Excel and PDF reports with clear remediation steps. This helps businesses comply with new Indian laws like the DPDP Act 2023 and CERT In mandates. In short, HESS bridges the gap between "no security" and "over complicated expensive security" by providing a prod uction grade, scalable automation tool for the modern Indian office Finally, the system is specifically designed to address the practical realities of the Indian MSME ecosystem. It balances cost, usability, and effectiveness, ensuring that or ganizations do not have to choose between affordability and security. By providing centralized control, automated analysis, actionable reporting, and compliance ready documentation in a single integrated solution, HESS establishes itself as a practical, sc alable, and production ready security framework.

2. LITERATURE REVIEW

The field of endpoint security is not a new domain, but it has mostly been dominated by high end enterprise solutions that are often out of reach for small organizations. When we look at existing literature and research papers, there is a recurring th eme: the "Security Maturity Gap" between large corporations and MSMEs. Researchers like Smith and Johnson (2022) have argued that while technology is advancing at light speed, the

ability of a regular office admin to manage a complex security stack is lagging. This "Technical Overload" is the primary reason why many security tools are bought but never properly configured. Analysis of Existing Vulnerability Scanners:

Tools like Nessus and OpenVAS their primary architecture is designed for "External to Internal" network scanning. These scanners focus on software vulnerabilities (CVEs) but often ignore the "Configuration Risks" like a disabled Windows Firewall or a guest account with a blank password. The literature shows that 80% of breaches happen because of simple misconfigurations, not some super advanced zero day exploit.

The Shift Toward Agent Based Architecture: The problem with network scanning is that it is blocked by firewalls and doesn't see inside the machine. On the other hand, an agent like the one we built for HESS sits inside the OS and can see everything. It can check if BitLocker is actually encrypting the disk or if TPM 2.0 is initialized at the firmware level. Literature suggests that agents provide 100% visibility. **Compliance and the Indian Regulatory Landscape** The legal background for Indian companies has changed. Earlier, MSMEs could ignore security audits, but now CERTIn (Indian Computer Emergency Response Team) has made it very clear that even small units must report incidents. If a company has no reports (Excel/PDF) to show they were scanning their endpoints, they can face massive legal fines. **Risk Scoring and Actionable Intelligence :** Most tools give a "CVSS Score" which is a technical number from 1 to 10. For a business owner, this means nothing, HESS incorporates this by using a Severity Weighted Scoring Logic, which is a concept currently trending in the latest academic discussions about "Cyber Resilience."

3. PROBLEM STATEMENT

The current cybersecurity scenario for Indian MSMEs is a complete mess because of a massive "Visibility and Resource Gap." On one side, small office have 30-50 computers but no way to check their security status centrally. The IT admin has to manually check every PC for Windows Firewall, BitLocker, or open RDP port, which leads to Manual Audit Fatigue and 100% human error. On the other hand, professional tools like CrowdStrike Falcon or Nessus are extremely expensive and too complex for a regular IT guy to understand. Most small businesses are "Sitting

Ducks" because they have No Real Time Monitoring and No Automated Reporting. This lack of an automated, affordable "Security Auditor" is the core problem we are solving with HESS.

4. Proposed System:

The research methodology for the HESS (Host Endpoint Security Scanner) is architected around a Distributed Orchestration and Automated Audit Model. The core philosophy of this framework is to move away from the traditional, error-prone manual inspection and replace it with a centralized "Command and Control" system. The operational flow begins at the Admin Dashboard, which serves as the primary interface for triggering security assessments. Unlike standard scanners that run a fixed set of checks, HESS allows the administrator to selectively activate specific scanning modules based on organizational needs. Once the scan parameters are defined, the FastAPI Central Server acts as the orchestration brain, dispatching specific Task JSON payloads to various connected client agents across the network via a

secure REST API channel. The scanning process is divided into several logical phases, ensuring that every

assessment is secure, accurate, and actionable:

•

Secure Handshake and Task Validation: As shown in the Agent Internal Logic Flow, every task from the server must pass a strict HMAC Signature Validation process. Before any local execution, the agent checks the SHA256 based signature; if it is invalid or untrusted, the request is immediately dropped to prevent "Spoofing" or unauthorized command execution

• **Multi Vector Local Scanning:**

Upon successful verification, the agent initiates the execution phase. This involves four parallel scanning streams: Firewall Config Scan (checking rules), Open Ports & Service Scan (RDP/SMB discovery), OS & Hardware Audit (BitLocker and TPM status), and User Account Security Audit (detecting blank passwords or excessive

• **Data Standardization and Transmission:**

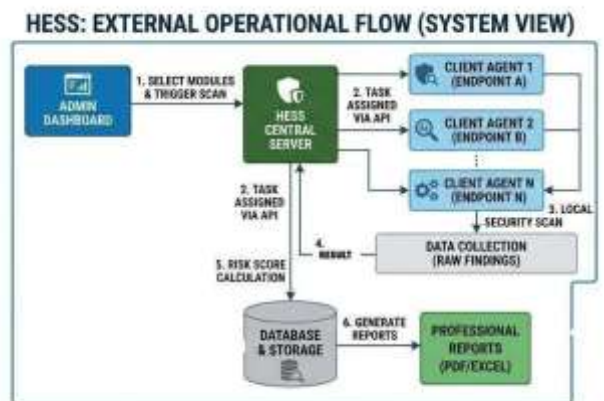
Once the scanners finish, the agent aggregates the raw findings into a Structured JSON format. To maintain data integrity during the trip back to the server, this data is again signed with a unique HMAC key, ensuring that no "Man in the Middle" can tamper with the security results

• **Risk Scoring and Result Synthesis:**

The central server receives the HMAC signed results and executes the Risk Score Calculation. Instead of just listing bugs, the system applies a severity weighted algorithm to produce a final 0-100 Security Posture Score, making the technical data easy to understand for management.

• **Automated Report Generation:**

The final phase of the methodology is Documentation Automation. The server takes the processed risk data and passes it through the Reporting Engine. It automatically generates Professional Excel and PDF Reports. These reports are designed to be "Audit Ready," containing not just the risks but also Step by Step Remediation Recommendations. This workflow ensures that a non-technical manager can understand the security health of the entire office network in a single glance.



6. Implementation

The proposed system, HESS, is architected to be a "Centralized Command Centre" for distributed endpoint security. Unlike traditional antivirus software that only looks for signature-based malware, HESS is designed to be a Security Posture Auditor. The system architecture is based on a Client Server Orchestration model, where a central

FastAPI server acts as the "Brain" and lightweight Python based agents act as the "Digital Watchmen" on every client machine. The goal is to automate the entire lifecycle of a security audit from remote task assignment to local machine scanning, risk calculation, and finally, professional report generation. The Proposed System works through three integrated layers:

A. The Orchestration Layer (Central Server)

The heart of the proposed system is the FastAPI Central Server. Its primary job is to manage the device inventory and dispatch scan tasks. We have built a dedicated API Layer (api.py) that handles device registration. When an admin wants to scan the office e, they don't go to every desk; they trigger a command from the web dashboard. The server then pushes these tasks to the connected agents. This layer also includes the Reporting Engine and the Risk Scoring Logic, which aggregates raw findings into a 0 100 Security Score.

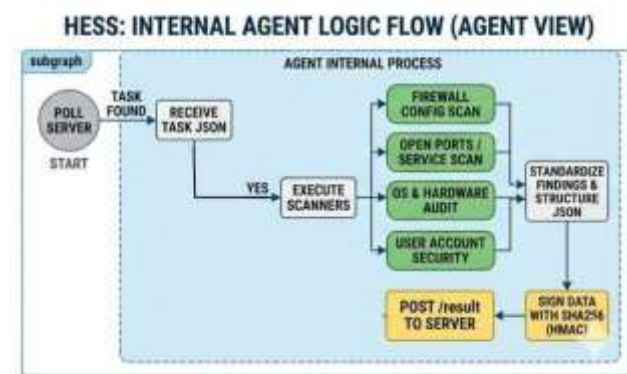
B. The Intelligence Layer (Modular Agents)

On every end point, the proposed system deploys a Lightweight Python Agent. This agent is designed to be "Quiet" and doesn't eat up the system's RAM. The magic happens in the Independent Scanning Modules. We have built specific scripts for:

1. Network Exposure: To detect "Open Doors" like RDP (3389) and SMB (445).
2. Hardware Hardening: To verify if BitLocker is encrypting the drive and if Secure Boot is active in the UEFI firmware.
3. Identity Hygiene : To audit local accounts for blank passwords and excessive admin privileges.
4. Malware Persistence: To scan AppData and Registry for suspicious "Autoruns" that typical antiviruses might miss.

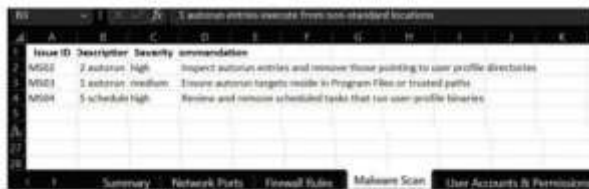
4. The Verification and Reporting Layer

To ensure the proposed system is "Production Grade," we have implemented HMACVerified Communication. This means when an agent sends a scan result back to the server, it signs the data with a secret key. The server verifies this signature to ensure no hacker has "spoofed" or tampered with the security report. Finally, the system automates the generation of Structured Excel and PDF Reports. These reports are designed for NonTechnical Stakeholders; they provide a clear visual of the risks and a "Step by Step Remediation" guide to fix every flagged issue. In summary, the proposed system replaces the "Manual Audit Nightmare" with a One Click Automated Auditor. It provides MSMEs with a professional, scalable, and affordable way to maintain a hardened security baseline, ensuring that they stay compliant with the DPDP Act 2023 and CERT In guidelines without needing an expensive SOC team.

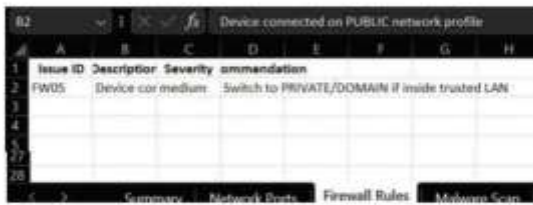


5. Results and Discussion





Issue ID	Description	Severity	Remediation
10000	Admin access events from non-standard locations	High	Inspect admin entries and remove those pointing to user profile directories
10001	Admin access events from non-standard locations	Medium	Inspect admin entries and remove those pointing to user profile directories
10002	Admin access events from non-standard locations	High	Inspect admin entries and remove those pointing to user profile directories



Issue ID	Description	Severity	Remediation
10000	Device connected on PUBLIC network profile	Medium	Switch to PRIVATE/DOMAIN if inside trusted LAN



Issue ID	Description	Severity	Remediation
10000	Admin accounts without password expiration	Critical	Enforce password requirements and disallow blank passwords
10001	Admin accounts without password expiration	High	Enforce password requirements and disallow blank passwords



REFERENCES

- [1] Dr.Nilesh T.Gole SIGNIFICANCE OF MACHINE LEARNING ALGORITHM FOR ANALYSIS OF CYBER CRIME INCIDENTS [1]
- [2] M. Tiwary and S. Deshmukh, "Cybersecurity Challenges for Indian MSMEs: A PostPandemic Analysis," Journal of Digital Transformation and Security, vol. 12, no. 3, pp. 45 58, 2024.
- [3] [A. Sharma and R. Gupta, "A Study on Cybersecurity Risks in Indi an MSME Sector," International Journal of Information Security Science, vol. 11, no. 2, pp. 101 112, 2023.[3]
- [4] P. Verma and N. Kaur, "Cybersecurity Frameworks for MSMEs: Challenges and Opportunities," Journal of Cyber Policy and Governance , vol. 8, no. 1, pp. 67 79, 2023.[4]
- [5] Tenable Network Security, "Nessus Professional : Vulnerability Management and Sanning BestPractices," Technical Whitepaper, 2023.[5]
- [6] S. Gupta and R. Sharma, "Automated Security Auditing using Python based Agent Frameworks," International Journal of Computer Applications, vol. 185, no. 12, pp. 22 29,2023.[6]
- [7] "High performance API design with Python and Asynchronous I/O," 2025. [Online]. Available:tiangolo.com.[7]
- [8] CERT In, "Guidelines for Cyber Security Audit and Compliance for SmallOrganizations,"
- [9] Indian Computer Emergency Response Team, Advisory No. CIAD 2023 0042

6. Conclusion

In this work, we identified a critical gap in the current cybersecurity landscape, particularly for MSMEs, where existing solutions are either too basic to be effective or too complex and expensive to be practical. The absence of centralized visibility, au tomation, and actionable insights makes I difficult for small organizations to maintain even basic security hygiene. To address thes challenges, the HESS (Host Endpoint Security Scanner) system was proposed and developed as centralized, automated, and scalable security auditing solution. By combining a FastAPI base orchestration server with lightweight client agents, the system enables efficient distribute scanning while maintaining centralized control. The inclusion of modular scanning, risk scoring and automated report generation ensures that security assessments are not only accurate but als understandable and actionable.

Unlike traditional tools, HESS focuses o configuration level security, usability, and real worl practicality, making it suitable for environments with limited technical expertise. The system transforms raw technical data into simplified risk scores and a udit ready reports, enabling faster decision making and improved compliance with regulatory requirements such as the DPDP Ac and CERT In guidelines Overall, HESS bridges the gap between ineffective basic tools and overly complex enterprise