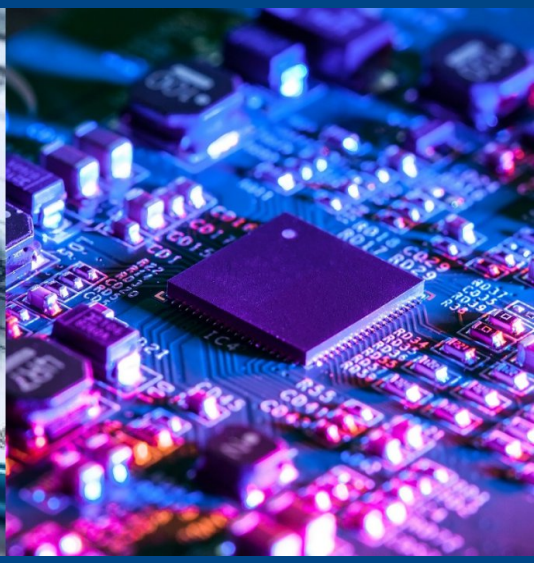
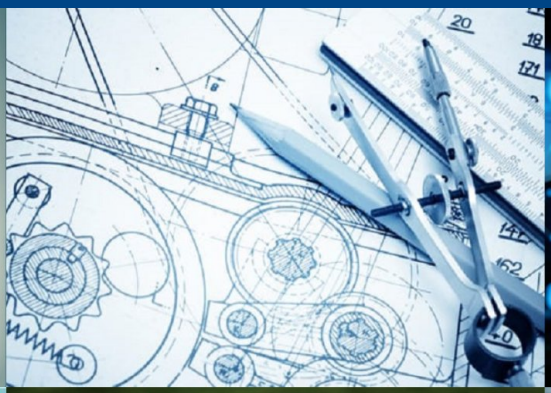
ISSN: 2582-7219

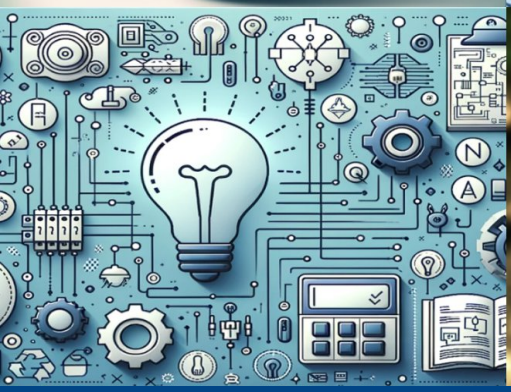




International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.206 **Volume 9, Issue 4, April 2026**

© 2026 IJMRSET | Volume 9, Issue 4, April 2026 | DOI:10.15680/IJMRSET.2026.0904322

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

SmartCyberAudit: AI-Based Cybersecurity Auditing and Threat Detection System

Khan Alfia Shamsul, Malik Reshma Shafaat, Qureshi Afifa Arif, Belim Hamzah Aslam, Prof. Junaid Mandviwala

Department of Artificial Intelligence & Data Science, Rizvi College of Engineering, Mumbai, Maharashtra, India

ABSTRACT: This paper presents SmartCyberAudit, an AI-based cybersecurity auditing and threat detection system designed to monitor computer systems, detect vulnerabilities, and provide automated protection mechanisms. The system integrates Machine Learning and Natural Language Processing techniques to identify anomalies and analyze system logs efficiently. Isolation Forest is used for anomaly detection, while TF-IDF and Naive Bayes are applied for intelligent log classification. The system evaluates overall system security using a risk scoring model and provides automated responses such as firewall activation and port blocking. The proposed solution is lightweight, cost-effective, and suitable for students, small organizations, and home users, offering an intelligent alternative to traditional security tools.

KEYWORDS: Cybersecurity, Artificial Intelligence, Anomaly Detection, Machine Learning, NLP, System Auditing

I. INTRODUCTION

Cybersecurity has become a critical concern due to the rapid increase in cyber threats such as malware, ransomware, phishing, and unauthorized access. Traditional security tools rely mainly on signature-based detection, making them ineffective against unknown or zero-day attacks.This project introduces SmartCyberAudit, an intelligent system that combines AI-based detection with system auditing to improve security. The system continuously monitors system parameters, detects suspicious behavior, and provides automated corrective actions. The aim is to develop a user-friendly and affordable cybersecurity solution that works efficiently on standard systems without requiring advanced technical expertise.

II. THEORY, METHODOLOGY, AND ALGORITHM

2.1 Theoretical Background

The system is based on three main concepts:

- **Anomaly Detection:** Identifies abnormal system behavior using Isolation Forest
- **Probabilistic Classification:** Uses Naive Bayes for log classification
- **Risk-Based Security Model:** Computes overall system risk score

These techniques allow intelligent detection of threats and vulnerabilities in real time.

2.2 Methodology

The system follows a structured pipeline:

1. **Data Collection:** CPU, RAM, processes, ports, logs
2. **Security Auditing:** Firewall, antivirus, updates, UAC
3. **AI Analysis:**
   - Isolation Forest for anomalies
   - NLP for log classification
4. **Risk Score Generation:** Combines all factors
5. **Automated Response:** Enables firewall, blocks ports
6. **Report Generation:** Generates final audit report

This modular approach ensures efficiency and scalability.

2.3 Algorithm Workflow

- Collect system metrics using monitoring tools

© 2026 IJMRSET | Volume 9, Issue 4, April 2026 | DOI:10.15680/IJMRSET.2026.0904322

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

- Perform security checks (firewall, antivirus, ports)
- Apply Isolation Forest to detect anomalies
- Analyze logs using TF-IDF and Naive Bayes
- Compute overall risk score
- Trigger automated protection if risk is high
- Generate audit report

III. LITERATURE REVIEW

Previous research in cybersecurity highlights the importance of AI and Machine Learning in threat detection.

- AI-based systems improve proactive threat detection
- Machine Learning models like Isolation Forest detect unknown attacks
- NLP techniques help interpret system logs efficiently

However, most existing systems focus on individual features and lack integration. SmartCyberAudit addresses this gap by combining auditing, AI detection, NLP analysis, and automated response into a single platform.

IV. OUTPUTS

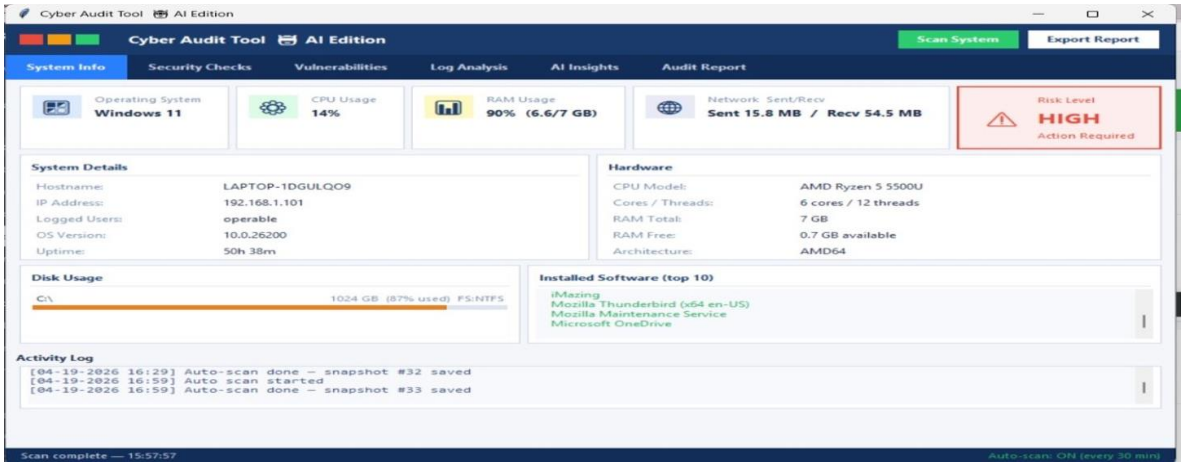


Figure 4.1: System Information Module Output

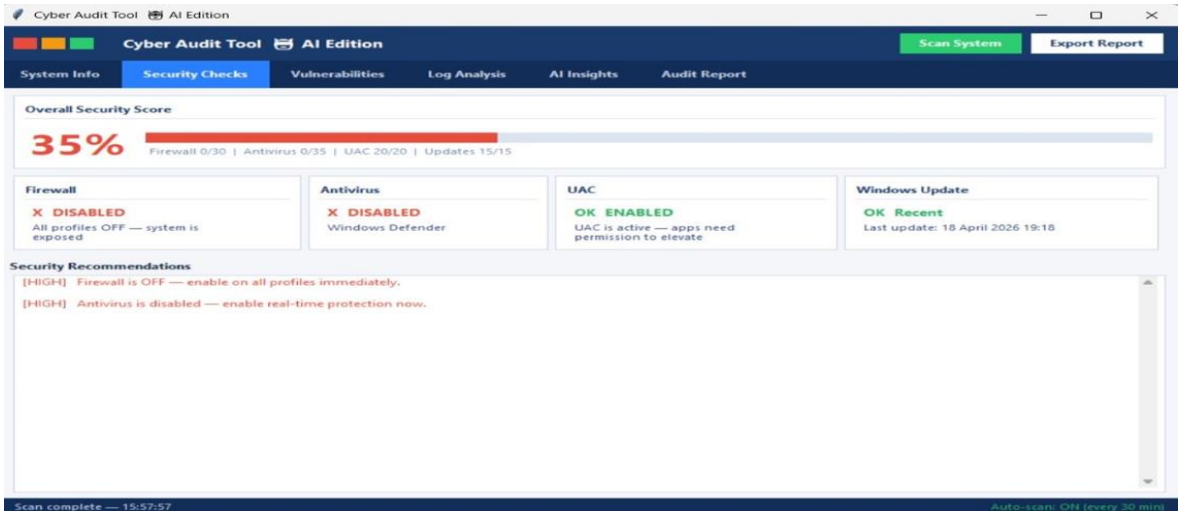


Figure 4.2: Security Checks Module Output

© 2026 IJMRSET | Volume 9, Issue 4, April 2026 | DOI:10.15680/IJMRSET.2026.0904322

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

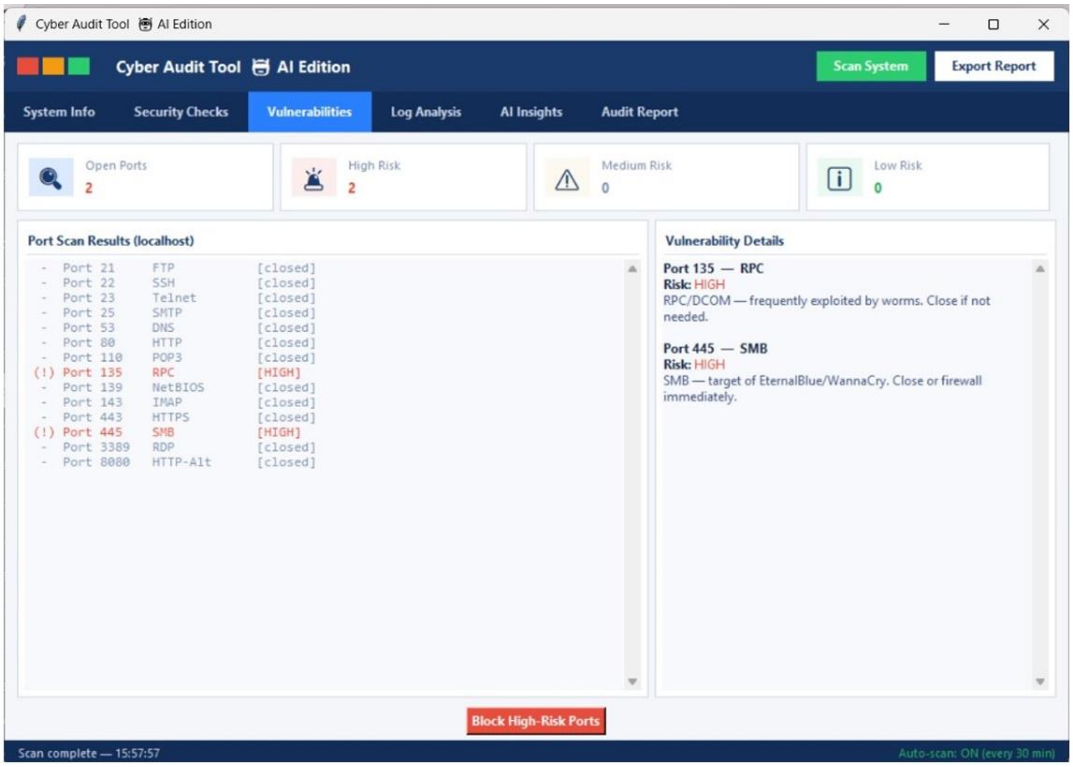


Figure 4.3: Vulnerability Scanning Module Output

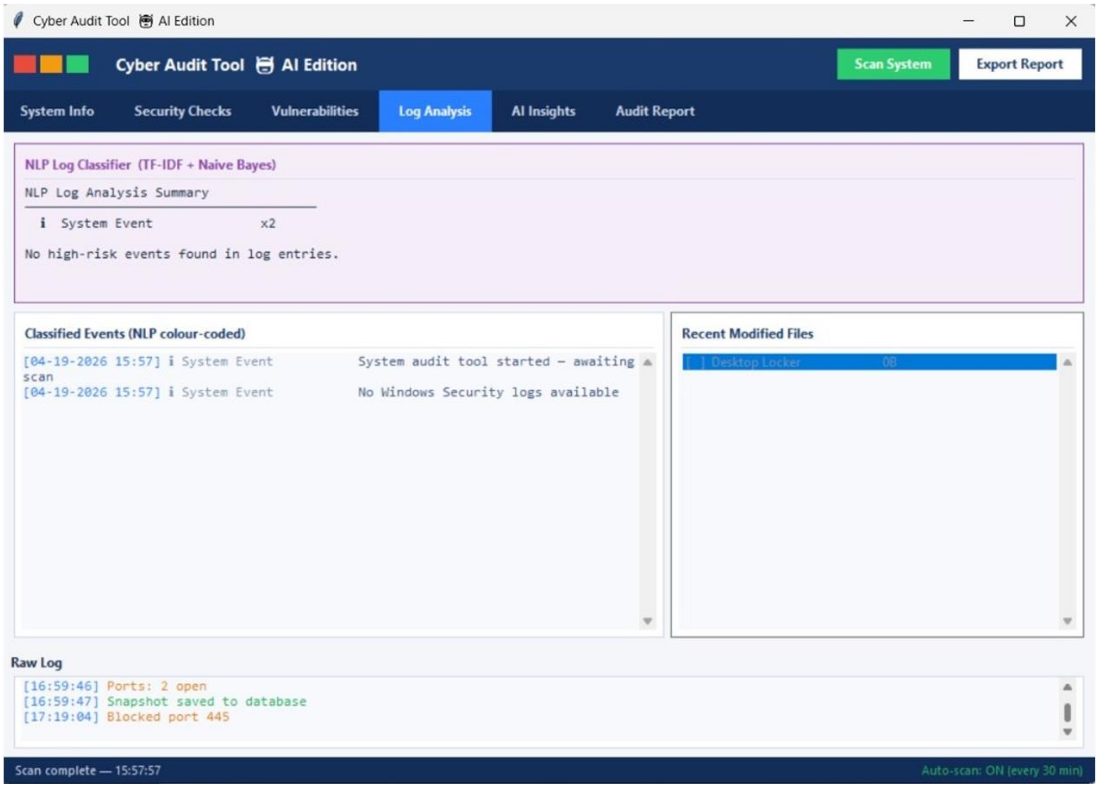


Figure 4.4: NLP-Based Log Analysis Module Output

© 2026 IJMRSET | Volume 9, Issue 4, April 2026 | DOI:10.15680/IJMRSET.2026.0904322

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

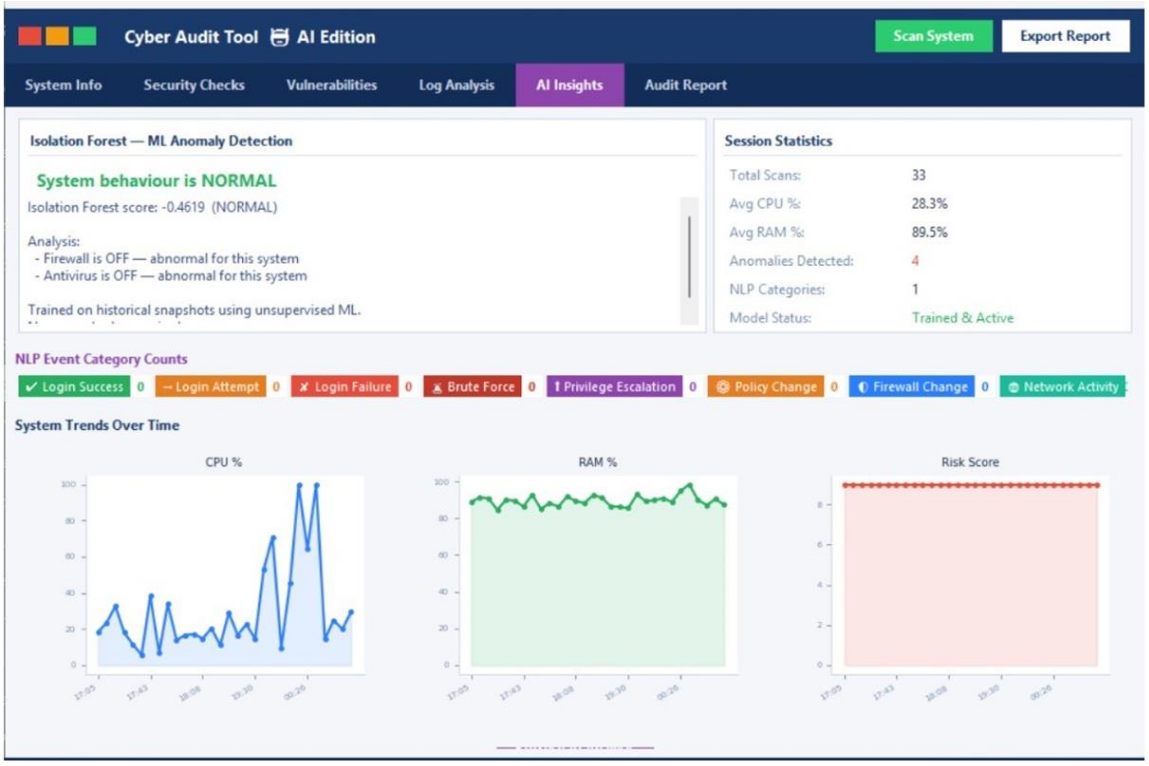


Figure 4.5: AI Risk Score and Threat Prediction Output

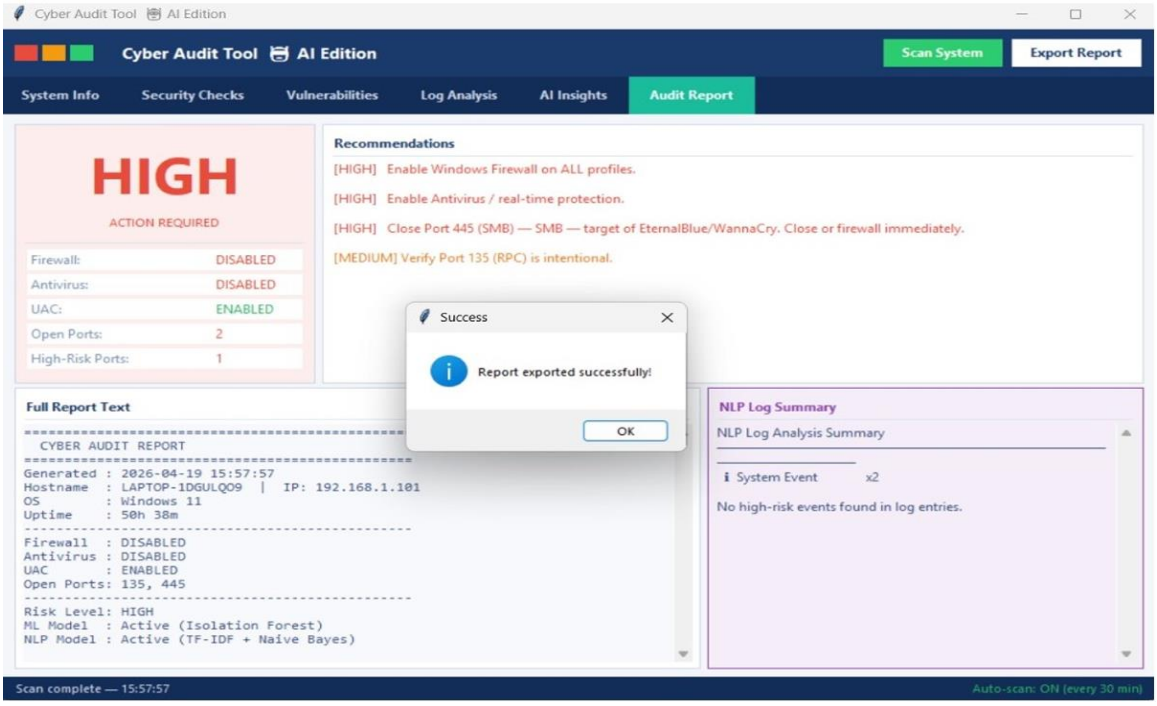


Figure 4.6: Generated Audit Report Output

© 2026 IJMRSET | Volume 9, Issue 4, April 2026 | DOI:10.15680/IJMRSET.2026.0904322

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

V. RESULTS AND DISCUSSION

The system was tested under various conditions including normal usage, high CPU load, disabled firewall, and open ports.

- Successfully detected anomalies such as high CPU usage and suspicious processes
- Identified risky ports like Port 445 and flagged vulnerabilities
- Risk score increased when threats were introduced
- Automated response reduced system risk effectively

The system performed efficiently with low memory usage and fast execution time.

Limitations:

- Works mainly on Windows systems
- Requires administrator privileges
- Not suitable for large enterprise environments

Overall, the system provides a strong and practical cybersecurity solution.

VI. CONCLUSIONS

- SmartCyberAudit successfully integrates AI with cybersecurity auditing
- The system detects anomalies using Machine Learning techniques
- NLP-based log analysis improves threat understanding
- Automated response reduces manual effort
- The system is lightweight and cost-effective
- Future improvements include cloud integration and mobile support

REFERENCES

[1] Dong & Kotenko, Cybersecurity in AI Era, 2025
[2] Sharma & Patel, AI in Cybersecurity, IEEE, 2025
[3] Liu et al., Isolation Forest, IEEE, 2008
[4] Russell & Norvig, Artificial Intelligence, 2021
[5] Stallings, Network Security Essentials, 2017
[6] Bird et al., NLP with Python, 2009
[7] Scikit-learn Documentation
[8] Python Documentation
[9] Microsoft Security Documentation

Appendix I – Model Architecture

- Python, Tkinter, Scikit-learn
- Isolation Forest for anomaly detection
- TF-IDF + Naive Bayes for log analysis

Appendix II – Dataset Summary

- Low Risk: 0–30
- Medium Risk: 31–60
- High Risk: 61–100

Appendix III – Sample Command

```
netsh advfirewall firewall add rule name="Block445" dir=in action=block protocol=TCP localport=445
```

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com