Cyber-Net-SecX
An Automated Framework For Network Vulnerability Assessment And Exploit Intelligence Integration

Harish R[1] , Harish S[2], Hariharan C[3], Eshwara K[4]
[1, 2, 3, 4] J.J.College of Engineering and Technology (JJCET), Tiruchirappalli,
Tamil Nadu, India

Abstract- *Network security has become a critical concern as modern organizations rely heavily on interconnected systems and digital infrastructure. Identifying vulnerabilities in network services is essential to prevent unauthorized access, data breaches, and system compromise. Traditional vulnerability assessment processes often require manual analysis using multiple tools, which can be time-consuming and prone to human error.This paper presents Cyber-Net-SecX, an automated framework designed to streamline the process of network vulnerability assessment. The proposed system integrates network reconnaissance, vulnerability intelligence extraction, exploit feasibility validation, and risk analysis into a single automated workflow. The framework utilizes Nmap for host discovery, port scanning, and service enumeration, while detected services are correlated with Common Vulnerabilities and Exposures (CVE)entries to identify potential security weaknesses. To determine exploit feasibility, the system connects to theMetasploit Framework usingRemote Procedure Call (RPC) and verifies the availability of relevant exploit modules. A CVSS-based risk analysis model is applied to evaluate vulnerability severity and classify risks.The implementation generates a structured multi-page security assessment report containing detected vulnerabilities, exploit intelligence, and risk severity visualization. Experimental testing in a controlled environment using a vulnerable virtual machine demonstrates that the automated framework significantly reduces manual analysis time while improving vulnerability detection efficiency. The results highlight the effectiveness of automated security assessment frameworks in supporting modern cybersecurity operations.*

Keywords: Cybersecurity, Vulnerability Assessment, Nmap, Metasploit, CVE Analysis

I. INTRODUCTION

In the modern digital era, organizations rely extensively on networked systems to support business operations, data storage, and communication. The rapid growth of internet-connected devices and services has significantly increased the attack surface of network infrastructures. As a result, cybersecurity has become a critical concern for institutions, enterprises, and individuals. Vulnerabilities present in network services, outdated software versions, and misconfigured systems can provide entry points for attackers to gain unauthorized access or disrupt essential services.

Vulnerability Assessment and Penetration Testing (VAPT) is widely used to identify security weaknesses in network environments. Security analysts commonly use tools such as Nmap for network discovery and service detection, and Metasploit for exploit research and validation. However, traditional vulnerability assessment processes often require security professionals to manually correlate scan results with vulnerability databases and exploit frameworks. This manual approach can be time-consuming and may lead to incomplete analysis or human error.

To address these challenges, automated security assessment frameworks are increasingly being developed to streamline vulnerability detection and analysis. Automation enables faster scanning, consistent analysis, and improved accuracy when identifying security weaknesses in network environments.

This research introduces Cyber-Net-SecX, an automated network vulnerability assessment framework designed to integrate reconnaissance, vulnerability intelligence extraction, exploit validation, and risk analysis into a unified system. The framework utilizes Nmap for network scanning and service enumeration, correlates detected services with Common Vulnerabilities and Exposures (CVE) databases, and validates exploit availability through Metasploit Remote Procedure Call (RPC) integration. Additionally, the system evaluates vulnerability severity using a CVSS-based risk scoring model and generates an automated security assessment report.

The primary objective of this research is to develop a system that reduces manual effort in vulnerability analysis while improving the efficiency and accuracy of cybersecurity assessments. By automating multiple phases of the vulnerability assessment process, Cyber-Net-SecX aims to assist cybersecurity professionals in identifying security risks more effectively and supporting proactive network defence strategies.

II. LITERATURE SURVEY

A. Network Scanning and Reconnaissance Tools

Network scanning is an essential step in vulnerability assessment. Tools such as Nmap (Network Mapper) are widely used for network discovery and security auditing. Nmap supports various scanning techniques including TCP SYN scanning, service version detection, and operating system fingerprinting. These capabilities help security analysts identify open ports and running services within a network. Network scanning tools provide the initial data required for detecting potential vulnerabilities in systems.

B. Vulnerability Databases and CVE System

The Common Vulnerabilities and Exposures (CVE) system provides standardized identifiers for publicly disclosed security vulnerabilities. It is maintained by the MITRE Corporation and widely used in vulnerability assessment frameworks. The National Vulnerability Database (NVD) further enriches CVE entries with severity scores using the Common Vulnerability Scoring System (CVSS). These databases allow automated tools to correlate detected software versions with known vulnerabilities.

C. Exploit Frameworks for Vulnerability Validation

The Metasploit Framework is a widely used penetration testing platform that provides exploit modules for testing vulnerabilities. Security researchers use Metasploit to validate whether identified vulnerabilities can be exploited in real environments. Integration of exploit frameworks with vulnerability scanning tools improves the accuracy of vulnerability assessments and reduces false positives.

D. Automated Vulnerability Assessment Frameworks

Several automated frameworks have been proposed to improve the efficiency of vulnerability assessment processes. Automated systems combine network scanning, vulnerability intelligence extraction, and risk analysis to provide faster and more consistent results. However, many existing solutions rely on multiple independent tools. The proposed Cyber-Net-SecX system integrates reconnaissance, vulnerability detection, exploit validation, and risk scoring into a unified automated framework to enhance cybersecurity assessment efficiency.

III. SYSTEM DESIGN AND METHODOLOGY

A. System Architecture

The Cyber-Net-SecX framework is designed as an automated vulnerability assessment system that integrates network reconnaissance, vulnerability intelligence extraction, exploit validation, and risk analysis. The system follows a modular architecture in which each module performs a specific task within the vulnerability assessment workflow.

The overall workflow of the system is illustrated below:

Target System
↓
Network Reconnaissance
↓
Service Detection
↓
CVE Intelligence
↓
Metasploit RPC Exploit Check
↓
Risk Analysis (CVSS)
↓
Report Generation

This architecture enables the system to automate multiple stages of the vulnerability assessment process and provide structured security analysis results.

B. Hardware Requirements

The hardware requirements for implementing the Cyber-Net-SecX system are minimal and suitable for standard laboratory environments.

Processor: Intel Core i5 or higher
RAM: Minimum 8 GB
Storage: Minimum 100 GB free disk space
Network Interface: Ethernet or Wireless Network Adapter

C. Software Requirements

The system is implemented using open-source cybersecurity tools and software.

Operating System: Kali Linux
Programming Language: Python
Network Scanning Tool: Nmap
Exploit Framework: Metasploit
Libraries: Python-Nmap, ReportLab for report generation

These tools enable efficient integration of network scanning, vulnerability analysis, and automated reporting.

D. Implementation Methodology

The Cyber-Net-SecX system follows a multi-phase methodology for performing automated vulnerability assessment.

Phase 1: Target Identification

The user provides the target IP address and scanning parameters through the command-line interface. The system initializes the scanning process based on the provided input.

Phase 2: Network Reconnaissance

The system performs network scanning using Nmap to identify open ports, running services, and service versions.

Phase 3: Vulnerability Intelligence Analysis

Detected services are analysed and correlated with known vulnerabilities using CVE databases.

Phase 4: Exploit Validation

The system connects to the Metasploit Framework through RPC to determine whether exploits exist for the detected vulnerabilities.

Phase 5: Risk Assessment

A CVSS-based scoring mechanism evaluates the severity of identified vulnerabilities and categorizes them into different risk levels.

Phase 6: Report Generation

The final stage generates a structured security assessment report that includes vulnerability details, exploit intelligence, and risk severity analysis.

IV. RESULTS AND ANALYSIS

A. Experimental Setup

The Cyber-Net-SecX framework was tested in a controlled laboratory environment to evaluate its effectiveness in detecting network vulnerabilities. The testing environment consisted of two virtual machines connected within the same network.

Scanning System: Kali Linux operating system
Target System : Metasploitable vulnerable virtual machine

The scanning system performed automated network reconnaissance, vulnerability detection, exploit validation, and risk analysis against the target machine.

B. CVE Intelligence Results

The Cyber-Net-SecX framework performs vulnerability intelligence analysis by correlating detected service versions with publicly available CVE databases. The system automatically identifies vulnerabilities associated with running services and retrieves their corresponding CVE identifiers and CVSS severity scores.

The analysis revealed several high and critical vulnerabilities associated with services running on the target system. For example, the FTP service running *vsftpd 2.3.4* was associated with *CVE-2011-2523*, which is categorized as a critical vulnerability with a high CVSS score. Similarly, multiple vulnerabilities were identified for the *OpenSSH* service and the *DNS service (ISC BIND).*

The detected vulnerabilities and their severity classifications are summarized in Table 1.

Table 1.CVE Intelligence Results

Port	Service	CVE ID	CVSS Score	Risk Level
1	FTP (vsftpd 2.3.4)	CVE-2011-2523	9.8	Critical
1	FTP	CVE-2021-3618	7.4	High
2	SSH (OpenSSH)	CVE-2023-38408	9.8	Critical
2	SSH	CVE-2016-1908	9.8	Critical
3	DNS (ISC BIND)	CVE-2008-0122	10.0	Critical
3	DNS	CVE-2020-8616	8.6	High

C. Exploit Intelligence using Metasploit RPC

To determine whether the detected vulnerabilities are exploitable, the Cyber-Net-SecX framework integrates with the *Metasploit Framework using Remote Procedure Call (RPC).* This module automatically queries the Metasploit exploit database and attempts to match detected services and versions with available exploit modules.

The exploit intelligence analysis revealed that ***the*** *FTP service running vsftpd 2.3.4* has a known exploit module available in the Metasploit framework. This exploit is commonly referenced as *exploit/unix/ftp/vsftpd_234_backdoor*, which allows unauthorized command execution on vulnerable systems.

For other detected services such as SSH, HTTP, and DNS, no matching exploit modules were identified due to version mismatches or lack of confirmed exploit signatures.

The exploit intelligence results aresummarized in Table 2.

Table 2. Metasploit RPC Exploit Intelligence Results

Port	Service	Exploit Module	Exploit Availability
1	FTP (vsftpd 2.3.4)	exploit/unix/ftp/vsftpd_234_backdoor	Available
2	SSH (OpenSSH)	No exploit matched	Not Available
3	Telnet	No exploit matched	Not Available
5	SMTP	No exploit matched	Not Available
0	HTTP (Apache)	No exploit matched	Not Available
3	DNS (ISC BIND)	No exploit matched	Not Available

D. Final Vulnerability Assessment

The final vulnerability assessment combines the results obtained from *CVE intelligence analysis and Metasploit exploit validation* to determine the overall severity of the detected vulnerabilities. The Cyber-Net-SecX framework evaluates each service based on the presence of known CVE entries, associated CVSS severity scores, and the availability of exploit modules in the Metasploit framework.

The analysis revealed that the *FTP service running vsftpd 2.3.4* presents the highest security risk because it is associated with multiple CVE-listed vulnerabilities and has a confirmed exploit module available in Metasploit. This vulnerability is categorized as *Critical severity*.

Similarly, services such as *SSH and DNS* were associated with multiple CVE entries with high CVSS scores, indicating potential security risks. However, no exploit modules were matched for these services during the exploit intelligence analysis. Therefore, they were classified as *High severity vulnerabilities.*

Other detected services did not have confirmed CVE entries or exploit modules and were therefore categorized as having *no significant vulnerabilities* within the scope of the automated assessment.

Table 3. Final Vulnerability Assessment Results

Port	Service	Assessment	Severity
1	FTP (vsftpd 2.3.4)	CVE-listed vulnerabilities + exploit available	Critical
2	SSH (OpenSSH)	CVE vulnerabilities detected	High
3	DNS (ISC BIND)	CVE vulnerabilities detected	High
3	Telnet	No CVE or exploit identified	N/A
5	SMTP	No CVE or exploit identified	N/A
0	HTTP (Apache)	No CVE or exploit identified	N/A

The final vulnerability assessment provides a clear overview of the security posture of the analysed system and helps administrators prioritize remediation efforts for critical vulnerabilities.

E. Performance Metrics

The performance of the Cyber-Net-SecX framework was evaluated by measuring the time required to complete each stage of the automated vulnerability assessment process. The system was tested in a controlled laboratory environment where Kali Linux acted as the scanning system and the Metasploitable virtual machine served as the target system.

The framework performs multiple automated operations including host discovery, port scanning, service enumeration, CVE intelligence extraction, exploit validation using Metasploit RPC, and final report generation. The total

time required for completing the full vulnerability assessment depends primarily on the number of ports scanned and the number of services detected.

Port scanning consumes the largest portion of the total scanning time. When scanning a limited number of common ports (for example, top 100 or 1000 ports), the scanning process completes quickly. However, performing a full port scan of all *65,535 ports* increases the scanning time significantly due to the large number of probes and response checks required.

Table 4. Performance Metrics of Cyber-Net-SecX

Process Stage	Description	Performance Observation
Host Discovery	Identifying active hosts in the network	Completed within a few seconds
Port Scanning	Detecting open ports and services	Time depends on number of ports scanned
Service Enumeration	Identifying service versions	Increases with number of open services
CVE Intelligence Analysis	Mapping detected services to CVE database	Completed quickly
Exploit Intelligence (Metasploit RPC)	Matching services with exploit modules	Completed within a few seconds
Report Generation	Generating final vulnerability assessment report	Completed quickly

The evaluation results demonstrate that Cyber-Net-SecX provides an efficient automated approach for vulnerability assessment by minimizing manual analysis and enabling rapid correlation of reconnaissance data with vulnerability intelligence and exploit frameworks.

F. False Positive Analysis

During automated vulnerability assessments, there is a possibility that some detected vulnerabilities may not accurately represent exploitable security weaknesses. These cases are commonly referred to as *false positives*, where a vulnerability scanner reports a potential vulnerability based on service version identification or banner analysis, even though the system may already be patched or configured securely.

In the Cyber-Net-SecX framework, vulnerability detection primarily relies on *service and version identification combined with CVE intelligence mapping*. Since the system correlates detected software versions with publicly available vulnerability databases, there is a possibility that certain vulnerabilities may be reported even if security patches have been applied without updating the service banner information.

For example, some services may display older version identifiers while the underlying system has been patched by the system administrator. In such cases, the system may flag vulnerabilities associated with that version even though the actual risk is mitigated.

To reduce false positives, the framework integrates *exploit intelligence validation through Metasploit RPC,* which attempts to match vulnerabilities with available exploit modules. This additional validation step helps distinguish between theoretical vulnerabilities and those with confirmed exploit availability.

Future improvements to the Cyber-Net-SecX framework may include integrating *patch management data, configuration analysis, and behavioural validation techniques* to further reduce false positive results and improve the accuracy of vulnerability detection.

V. DISCUSSION

A. Advantages of Automated Assessment

The Cyber-Net-SecX framework demonstrates several advantages compared to traditional manual vulnerability assessment methods. Automated scanning enables security analysts to quickly identify open ports, running services, and potential vulnerabilities within a network environment. By integrating reconnaissance tools, vulnerability intelligence databases, and exploit frameworks into a unified system, the framework significantly reduces the time and effort required for vulnerability analysis.

Automation also improves consistency and repeatability in security assessments. Manual testing may overlook certain services or vulnerabilities due to human error, whereas automated frameworks perform systematic scans across multiple ports and services. Additionally, the integration of CVE intelligence analysis and Metasploit exploit validation allows the system to distinguish between theoretical vulnerabilities and those with confirmed exploit availability, improving the reliability of vulnerability assessment results.

B. Limitations and Challenges

Despite its advantages, the Cyber-Net-SecX framework has certain limitations. The vulnerability detection mechanism relies heavily on service and version identification, which may occasionally lead to false positives when service banners do not accurately reflect the actual patch status of the system. Some systems may display outdated version information even though the vulnerabilities have already been patched.

Another challenge is the increased scanning time when performing comprehensive port scans across large port ranges. Scanning all available ports may increase network traffic and affect system performance in large-scale network environments. Additionally, some services may restrict version detection or block scanning attempts, limiting the accuracy of vulnerability identification.

C. Ethical and Legal Considerations

Vulnerability assessment activities must be conducted within appropriate ethical and legal boundaries. Unauthorized network scanning or penetration testing may violate organizational security policies or cybersecurity laws. Therefore, it is essential that automated security assessment frameworks such as Cyber-Net-SecX are used only in authorized environments or controlled laboratory settings.

The experiments performed in this research were conducted within a controlled testing environment using a vulnerable virtual machine specifically designed for cybersecurity research. Security professionals must always obtain proper authorization before performing vulnerability assessments on real-world systems to ensure compliance with ethical standards and legal regulations.

VI. CONCLUSION

This research presented *Cyber-Net-SecX,* an automated framework designed to streamline the process of network vulnerability assessment by integrating reconnaissance, vulnerability intelligence extraction, exploit validation, and risk analysis into a unified system. The framework utilizes Nmap for network scanning, correlates detected services with publicly available CVE databases, and verifies exploit feasibility using Metasploit RPC integration.

The experimental results demonstrated that Cyber-Net-SecX can effectively identify exposed services, detect known vulnerabilities, and evaluate associated risk levels within a network environment. By automating multiple stages of the vulnerability assessment process, the system significantly reduces manual effort while improving the efficiency and consistency of security analysis.

The integration of CVE intelligence and exploit validation provides a comprehensive understanding of potential security risks, enabling administrators to prioritize remediation efforts more effectively. Future enhancements may include integration with real-time vulnerability databases, improved false positive reduction techniques, and advanced risk prioritization mechanisms.

Overall, Cyber-Net-SecX demonstrates the potential of automated vulnerability assessment frameworks in supporting proactive cybersecurity management and strengthening network security posture.

VII. ACKNOWLEDGMENT

The authors would like to express sincere gratitude to our guide, *Mrs. P. Suganya* and Professor*Dr. M. P. Revathi*, *Department of Computer Science and Engineering – Cyber Security, J.J. College of Engineering and Technology (JJCET), Tiruchirappalli,* for her continuous guidance and support throughout the development of this research work. Special thanks are extended to the project supervisor and faculty mentors for their valuable suggestions, encouragement, and technical guidance during the completion of this study.

The authors also acknowledge the open-source cybersecurity community for providing essential tools and frameworks such as *Nmap* and *Metasploit*, which played a significant role in the implementation of the Cyber-Net-SecX framework. Finally, appreciation is extended to colleagues and peers for their constructive feedback and support during the testing and evaluation phases of the project.

REFERENCES

[1] G. Lyon, *Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning*. Available: https://nmap.org/book/

[2] Rapid7, "*Metasploit Framework Documentation*," 2023. Available: https://www.metasploit.com

[3] MITRE Corporation, "*Common Vulnerabilities and Exposures (CVE)*," 2023. Available: https://cve.mitre.org

[4] National Institute of Standards and Technology (NIST), "National Vulnerability Database (NVD)." Available: https://nvd.nist.gov

[5] P. Mell, K. Scarfone, and S. Romanosky, "*A Complete Guide to the Common Vulnerability Scoring System*

(CVSS)," *IEEE Security & Privacy*, vol. 4, no. 6, pp. 85–89, 2006.

[6] D. Kennedy, J. O'Gorman, D. Kearns, and M. Aharoni, *Metasploit: The Penetration Tester's Guide*. San Francisco, CA, USA: No Starch Press, 2011.

[7] Open Web Application Security Project (OWASP), "*OWASP Top 10 Web Application Security Risks*," OWASP Foundation, 2021. Available: https://owasp.org