



Agent-less Windows System Vulnerability and Network Scanner for Security Assessment and Reporting

Satvik Dilip Barhate¹, Dr. Dinesh Puri²

MCA Student, Department of Computer Applications, SSBT's College of Engineering & Technology Jalgaon,

Maharashtra, India¹

Professor, Department of Computer Applications, SSBT's College of Engineering & Technology Jalgaon, Maharashtra,

India²

Abstract: Modern Windows endpoints and small enterprise networks expose multiple security-relevant services, software versions, configurations, and network paths. Conventional vulnerability assessment approaches may require endpoint agents, extensive deployment, or separate tools for network discovery and host-level inspection. This research presents CyberWolf, an agent-less Windows system vulnerability and network scanner designed to combine network discovery, service enumeration, structured scan-result processing, and rule-based security assessment in a lightweight workflow. The proposed approach uses Nmap for network discovery and XML output as a machine-readable data source, followed by parsing, normalization, security checks, finding prioritization, and report generation. The design is intended for controlled and authorized assessment of Windows hosts without installing a permanent software agent on each target. The research defines a repeatable assessment lifecycle, a normalized data model, example security rules, evaluation dimensions, limitations, and future extensions. The work is positioned as a defensive assessment framework for identifying network-exposed conditions and supporting remediation decisions.

Keywords: Windows Security, Vulnerability Assessment, Agent-less Scanning, Network Discovery, Nmap, CyberWolf, Security Automation, Vulnerability Management

I. INTRODUCTION

The increasing dependence on Windows workstations and servers has expanded the number of systems that must be inventoried, monitored, and assessed for security weaknesses. A typical environment may contain multiple hosts, open network ports, remote administration services, legacy protocols, and applications with different security requirements. Regular vulnerability assessment therefore depends on accurate asset discovery and repeatable security testing.

NIST SP 800-115 describes vulnerability scanning as a practical technique for identifying weaknesses and distinguishes network-based scanning from more detailed local or credentialed assessment [1]. Network-based scanning is useful for discovering reachable hosts, open ports, services, and other externally observable conditions. This distinction motivates an agent-less approach in which the assessment engine does not require a permanent software agent on every Windows endpoint.

CyberWolf follows a modular pipeline. It begins with an IP address, hostname, or approved network range; performs host and service discovery using Nmap; parses machine-readable XML results; normalizes the observations; applies security-oriented rules; and generates a structured report. Nmap is designed for network discovery and security auditing and provides output formats suitable for automation [2].

The objective is not to replace enterprise vulnerability-management platforms. Instead, the research studies a lightweight, transparent, and extensible method for combining network reconnaissance with Windows-focused security assessment. The framework is suitable for controlled laboratory environments, educational research, small networks, and future automation.

Research Objectives

- Design an agent-less workflow for discovering Windows hosts and exposed network services.
- Integrate network scanning with structured result parsing and security-rule evaluation.



- Reduce repetitive manual work involved in collecting scan results and preparing assessment reports.
- Provide a modular architecture that can be extended with Windows security checks and vulnerability intelligence.
- Define measurable evaluation criteria such as discovery coverage, processing time, finding accuracy, and reporting completeness.

Problem Statement

Manual vulnerability assessment of multiple Windows systems can be time-consuming because asset discovery, service enumeration, vulnerability interpretation, and reporting are often performed as separate activities. Installing and maintaining endpoint agents can also introduce deployment and management overhead. The research problem addressed in this work is how to construct a lightweight agent-less scanner that combines network discovery and automated security assessment while keeping the architecture understandable, extensible, and suitable for controlled environments.

Research Contributions

- A modular agent-less scanning architecture for Windows-oriented network assessment.
- A workflow that converts Nmap XML output into normalized records for automated analysis.
- A rule-based assessment layer for identifying security-relevant services, versions, configurations, and exposure conditions.
- A reporting model that associates findings with evidence, severity indicators, and remediation guidance rather than presenting raw scan output alone.

II. LITERATURE REVIEW

Security-testing guidance emphasizes that vulnerability assessment is a process involving planning, technical testing, analysis of findings, and mitigation [1]. Nmap documentation describes network discovery, port scanning, service detection, scripting, and machine-readable outputs, making it relevant to the discovery stage of an automated assessment workflow [2].

Vulnerability management also depends on remediation and prioritization. NIST SP 800-40 Rev. 4 describes patch management as identifying, prioritizing, acquiring, installing, and verifying patches and updates [3]. This supports the inclusion of remediation-oriented information in scanner reports rather than limiting output to technical detection data. Secure-configuration benchmarks provide another assessment source. CIS maintains consensus-based benchmarks for operating systems, including Microsoft Windows platforms [4], [5]. CISA's Known Exploited Vulnerabilities Catalog can provide an additional prioritization input when a detected product and version can be matched with confidence [6]. MITRE ATT&CK and CWE provide complementary security knowledge for interpreting exposed services and weaknesses [7], [11].

NIST CSF 2.0 and NIST SP 800-53 provide broader security and control perspectives that can help organize scanner findings and future configuration checks [8], [9]. CVSS provides a standardized framework for communicating vulnerability severity when a vulnerability is confirmed [10]. Microsoft security baselines and security documentation can further support Windows-specific hardening checks [13], [14].

Research Gap and Proposed Direction

The literature and security guidance indicate a recurring trade-off: network-based agent-less assessment has deployment advantages and broad visibility of network exposure, while local or credentialed assessment can provide deeper host-level information [1], [3]. The proposed CyberWolf framework therefore keeps an agent-less core while explicitly treating its visibility limitations as part of the research evaluation. The research direction is to connect discovery evidence to repeatable security rules and reporting without claiming that an exposed port alone proves a vulnerability.

Reference	Focus	Main Contribution	Relevance to CyberWolf
NIST SP 800-115 [1]	Security testing	Structured testing and assessment guidance	Supports assessment lifecycle
Nmap Guide [2]	Network discovery	Host, port, service and output capabilities	Core discovery engine
NIST SP 800-40 [3]	Patch management	Prioritization and verification	Supports remediation-oriented reporting
CIS Benchmarks [4], [5]	Configuration security	Windows hardening	Future configuration rules



		recommendations	
CISA KEV [6]	Vulnerability intelligence	Known exploited vulnerabilities	Prioritization input
MITRE ATT&CK [7]	Adversary techniques	Technique knowledge base	Context for exposed services
NIST CSF 2.0 [8]	Cybersecurity framework	Risk-management structure	Organizes findings
CVSS v4.0 [10]	Severity	Standardized severity concepts	Finding prioritization

III. RESEARCH METHODOLOGY

The proposed methodology follows a controlled security-assessment lifecycle: scope definition, target discovery, service enumeration, structured result collection, normalization, security-rule evaluation, finding prioritization, and report generation. The scanner is intended to be operated only against systems and networks for which the tester has explicit authorization.

System Architecture

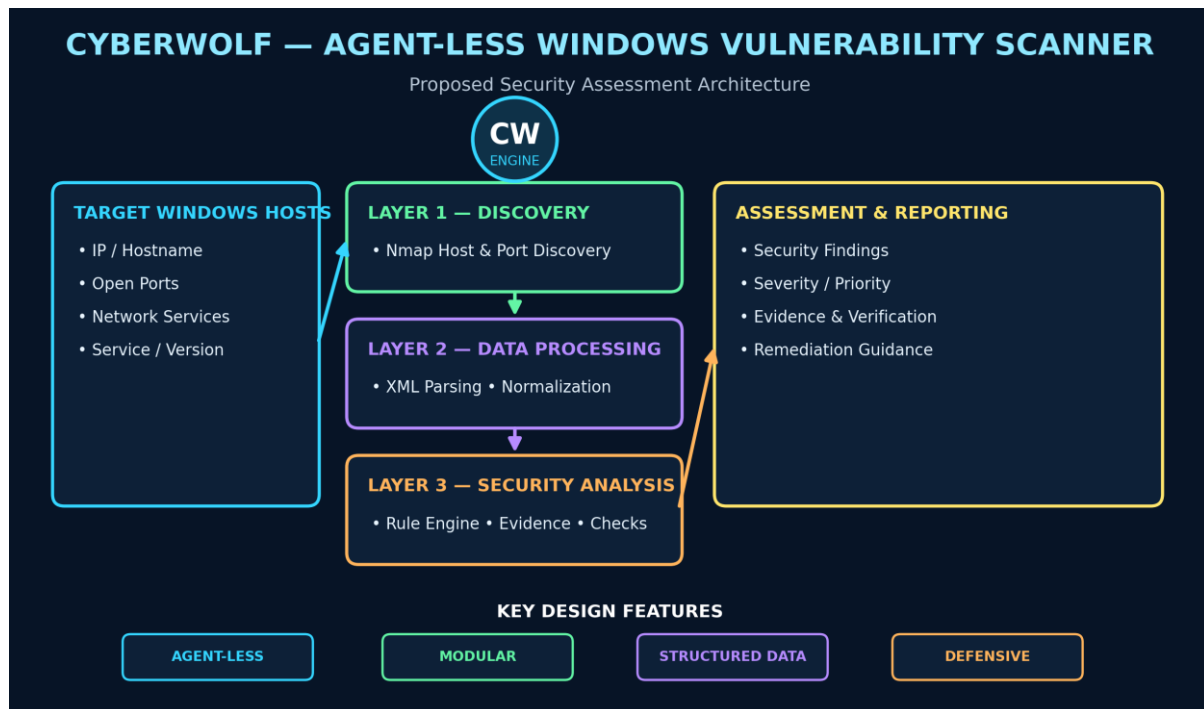


Fig. 1. Proposed CyberWolf agent-less assessment architecture.

The architecture contains five logical components. The target layer contains Windows hosts or a permitted network range. The discovery layer uses Nmap to identify live hosts, open ports, and service information. The scanner engine controls execution and stores scan artifacts. The parser and normalization layer converts XML output into structured records. Finally, the assessment and reporting layer evaluates rules and produces human-readable findings. This separation supports modular development because discovery mechanisms, parsing logic, and security checks can be extended independently.



Scanning Workflow

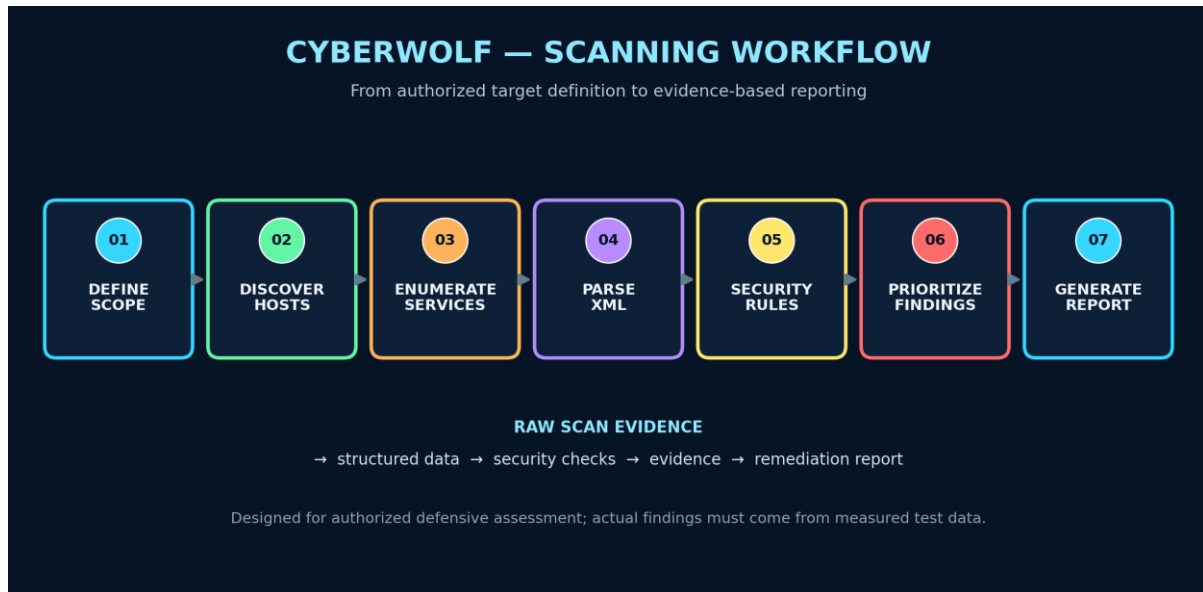


Fig. 2. End-to-end CyberWolf scanning and reporting workflow.

- Scope definition: specify an individual host, an approved CIDR range, or a laboratory target.
- Host discovery: identify reachable systems and record basic network information.
- Service enumeration: determine exposed TCP/UDP services and, where supported, service/version information.
- Structured parsing: process Nmap XML output rather than relying on fragile screen-scraping.
- Security checks: compare collected evidence with predefined rules and vulnerability intelligence.
- Prioritization: associate each finding with evidence, severity indicators, affected asset, and recommended remediation.
- Reporting: generate a structured report that can be reviewed and repeated after remediation.

Data Model

Field	Purpose
Host IP	Identifies the assessed network endpoint.
Hostname	Stores discovered or resolved host identity when available.
Port / Protocol	Records exposed communication endpoints.
Service / Version	Captures discovered application or service information.
Evidence	Stores the scan observation supporting a finding.
Finding	Describes the security condition identified by a rule.
Severity	Provides a documented prioritization category.
Remediation	Provides a practical mitigation or verification step.

IV. ALGORITHMS AND SECURITY CHECKS

CyberWolf can be implemented as a rule-driven assessment engine. Each rule receives normalized scan data and returns either a finding or a non-match. This design avoids hard-coding every security condition into the scanning logic and makes the system easier to extend.

Algorithm 1: Agent-less Network Assessment

1. Accept target IP, hostname, or CIDR range.
2. Validate the target scope and launch discovery.
3. Execute Nmap with an appropriate scan profile for the authorized environment.
4. Save XML output as the raw evidence artifact.
5. Parse hosts, ports, protocols, services, and version fields.
6. Normalize the data into an internal representation.



- 7. Run enabled security rules against the normalized records.
- 8. Attach evidence and remediation guidance to matched findings.
- 9. Export a report and preserve scan metadata for repeat assessment.

Example Security Rules

Rule Category	Example Observation	Assessment Purpose
Exposed service	Unexpected remote-access or administrative service	Identify unnecessary network exposure.
Legacy protocol	Service associated with outdated or weak protocol usage	Flag candidates for protocol hardening.
Service version	Detected software/version with security relevance	Support vulnerability-intelligence matching.
Host discovery	Previously unknown live endpoint	Improve asset inventory visibility.
Configuration indicator	Security-relevant service or port pattern	Support hardening review.

An open port alone should not be treated as proof of a vulnerability. A detected service is evidence of exposure and should be correlated with version, configuration, authentication requirements, and vulnerability intelligence before a high-confidence vulnerability is reported. This principle reduces false positives and keeps the assessment evidence-based.

V. EXPERIMENTAL SETUP AND EVALUATION

The research can be evaluated in an isolated and authorized Windows laboratory containing one or more Windows hosts and a scanning workstation. The evaluation should use repeatable targets so that the scanner can be run before and after controlled configuration changes. A service may be deliberately enabled or disabled, a known test version may be installed, or a configuration may be changed to create a measurable test condition.

Evaluation Dimension	Metric	Purpose
Discovery	Hosts discovered / known hosts	Measure asset discovery coverage.
Service enumeration	Services identified correctly	Measure enumeration completeness.
Processing	Scan-to-report time	Measure automation efficiency.
Detection	True findings / false findings	Assess rule quality.
Reporting	Evidence completeness	Assess usefulness to analysts.
Repeatability	Consistency across repeated scans	Assess workflow stability.

Preliminary Implementation Observations

The CyberWolf implementation demonstrates the feasibility of an agent-less pipeline in which Nmap performs network discovery and its XML output is parsed programmatically. XML provides structured access to host, port, protocol, and service information and reduces dependence on terminal-output formatting. The approach is suitable for a lightweight command-line workflow and can be extended with additional checks.

No quantitative performance values are claimed in this paper without controlled measurements. Actual accuracy, runtime, and detection results should be calculated from the test environment and recorded with the Windows version, network topology, scan profile, and test date. This keeps measured evidence separate from design expectations.



CyberWolf — Security Assessment Report Concept

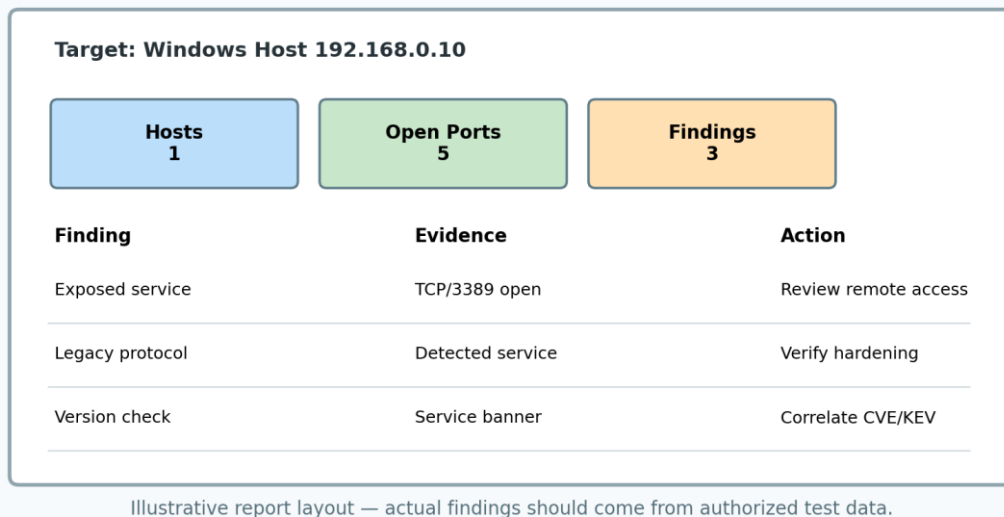


Fig. 3. Illustrative vulnerability-assessment report layout.

VI. RESULTS AND DISCUSSION

The expected research outcome is a repeatable assessment workflow that transforms raw network-scan data into structured security findings. The strongest evidence should come from controlled experiments comparing known test conditions with scanner output. Such experiments can measure whether a deliberately exposed service, changed configuration, or known test version is identified as expected.

The separation between discovery and assessment is important. Discovery tools are optimized to collect observations, whereas a vulnerability-management workflow must interpret those observations. By keeping the two layers separate, CyberWolf can incorporate additional data sources such as current vulnerability catalogs or configuration benchmarks without changing its basic scanning mechanism.

False positives are another important consideration. Service banners can be incomplete, modified, or ambiguous. Version matching should therefore use multiple evidence fields when available and should communicate evidence or confidence rather than treating every version match as a confirmed vulnerability. CISA KEV can support prioritization when a product/version match is reliable, while CIS Windows Benchmarks can support configuration-oriented checks [4]–[6].

The framework is suitable for educational and small-network use because its components can be inspected individually. In larger enterprise environments, additional capabilities such as credentialed assessment, asset management, centralized scheduling, authenticated configuration checks, and integration with patch-management systems would be required.

VII. SECURITY, ETHICS, AND SCOPE

CyberWolf is intended for defensive security assessment. Scanning should be performed only on systems and networks for which the operator has explicit authorization. Aggressive scan settings can generate network traffic or trigger security controls, so test profiles should be selected according to the environment and approved rules of engagement.

Raw scan results should be treated as security-sensitive information because reports may contain IP addresses, hostnames, service banners, and configuration observations. Appropriate access controls and retention practices should therefore be applied to stored scan artifacts.



VIII. LIMITATIONS AND FUTURE WORK

- Agent-less scanning cannot provide the same host-level visibility as local or credentialed assessment.
- Service/version detection may be incomplete or inaccurate when banners are suppressed or altered.
- Vulnerability matching requires current and trustworthy vulnerability intelligence and careful version correlation.
- The present research design does not claim enterprise-scale performance without measured testing.
- Future work can add authenticated Windows checks through controlled administrative interfaces while keeping the core agent-less mode.
- Future versions can integrate CVE/KEV intelligence, CIS Windows configuration checks, severity scoring, historical comparison, scheduled scanning, and HTML/PDF reporting.
- A future experimental study can compare discovery coverage and processing time against selected open-source scanners using the same controlled test network.

IX. CONCLUSION

This research presented **CyberWolf**, an agent-less Windows system vulnerability and network scanner developed to simplify the process of network discovery, service enumeration, security assessment, and vulnerability reporting. The proposed framework combines Nmap-based network scanning with XML result parsing, data normalization, rule-based security checks, finding prioritization, and report generation. This modular approach makes the assessment process more systematic and reduces the need for repetitive manual analysis.

The agent-less architecture provides a practical advantage because it does not require a permanent software agent to be installed on every target Windows system. CyberWolf can collect information about reachable hosts, open ports, protocols, services, and available version information through network-based assessment. The structured XML output also provides a suitable format for automated processing and allows the collected information to be converted into meaningful security findings.

The research emphasizes that **network exposure does not automatically indicate a confirmed vulnerability**. Detected services and versions should be evaluated using reliable evidence, configuration information, and appropriate vulnerability intelligence. This approach helps reduce false positives and provides security analysts with more useful and understandable assessment reports.

Although CyberWolf has limitations compared with credentialed or enterprise-level vulnerability assessment platforms, its modular design provides a useful foundation for further development. Future work can include integration with **CVE and CISA KEV intelligence, CIS Windows security benchmarks, authenticated Windows checks, historical scan comparison, scheduled scanning, confidence scoring, and advanced HTML/PDF reporting.**

Overall, CyberWolf demonstrates a practical approach to **agent-less Windows vulnerability assessment and network security automation**. The proposed framework can support cybersecurity learning, controlled security assessments, and future research focused on improving automated vulnerability detection, analysis, and reporting.

The framework also provides a clear separation between network discovery and vulnerability analysis, making the overall process easier to manage and improve. The use of structured scan data allows security findings to be stored and analyzed consistently across different assessments. CyberWolf can help reduce the time required for manual collection and interpretation of network security information. It can also provide a foundation for comparing security conditions before and after remediation. The modular design allows new security rules and assessment techniques to be added without redesigning the complete system. With further testing and validation, the framework can be improved for broader Windows-based network environments. The proposed approach demonstrates the potential of combining network scanning and automated security analysis in a lightweight solution. Therefore, CyberWolf provides a useful foundation for continued research in automated vulnerability assessment and cybersecurity automation.

REFERENCES

- [1] K. Scarfone, M. Souppaya, A. Cody, and A. Orebaugh, "Technical Guide to Information Security Testing and Assessment," NIST Special Publication 800-115, National Institute of Standards and Technology, 2008.
- [2] G. Lyon, "Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning," Nmap Project.



- [3] M. Souppaya and K. Scarfone, "Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology," NIST Special Publication 800-40 Rev. 4, National Institute of Standards and Technology, 2022.
- [4] Center for Internet Security, "CIS Microsoft Windows 11 Enterprise Benchmark," CIS Benchmarks.
- [5] Center for Internet Security, "CIS Microsoft Windows Server Benchmark," CIS Benchmarks.
- [6] Cybersecurity and Infrastructure Security Agency, "Known Exploited Vulnerabilities Catalog," CISA.
- [7] MITRE, "MITRE ATT&CK Enterprise," MITRE Corporation.
- [8] National Institute of Standards and Technology, "Cybersecurity Framework (CSF) 2.0," NIST, 2024.
- [9] National Institute of Standards and Technology, "Security and Privacy Controls for Information Systems and Organizations," NIST Special Publication 800-53 Rev. 5.
- [10] FIRST, "Common Vulnerability Scoring System Version 4.0," FIRST.Org, Inc., 2023.
- [11] MITRE, "Common Weakness Enumeration (CWE)," MITRE Corporation.
- [12] OWASP Foundation, "Web Security Testing Guide," OWASP Foundation.
- [13] Microsoft, "Windows Security Baselines," Microsoft Learn.
- [14] Microsoft, "Security Compliance Toolkit," Microsoft Learn.
- [15] Nmap Project, "Nmap Reference Guide," Nmap Documentation.
- [16] Center for Internet Security, "CIS Controls v8," Center for Internet Security.
- [17] National Institute of Standards and Technology, "Guide for Conducting Risk Assessments," NIST Special Publication 800-30 Rev. 1.
- [18] National Institute of Standards and Technology, "Computer Security Incident Handling Guide," NIST Special Publication 800-61 Rev. 2.
- [19] National Institute of Standards and Technology, "Security and Privacy Controls for Information Systems and Organizations," NIST Special Publication 800-53 Rev. 5.