AUTO: Automated Domain Reconnaissance and Vulnerability Assessment Framework

Ravindra Chauhan[1], Jagannath Mohanty[2], Nikhil Ku. Gupta[3], Sonu[4], Priyansh Pal[5]
[1]*Guide, Department of Computer Science & Engineering RDEC, Ghaziabad*
[2,3,4,5]*Department of Computer Science & Engineering RDEC, Ghaziabad*

Abstract- The exponential growth of web applications, cloud-based services, and distributed enterprise infrastructures has significantly expanded the digital attack surface of organizations worldwide. As businesses increasingly rely on online platforms, domain ecosystems now consist of numerous subdomains, APIs, third-party integrations, and dynamically generated resources. This complexity introduces critical security challenges, making reconnaissance a fundamental phase in penetration testing and vulnerability assessment.

Traditional reconnaissance methodologies depend on multiple independent open-source tools for subdomain discovery, port scanning, vulnerability detection, and data collection. However, these tools often operate in isolation, requiring manual coordination, repetitive execution, and fragmented result analysis, which can lead to inefficiencies, inconsistent reporting, and overlooked security risks.

This paper presents AUTO (Automated Domain Reconnaissance Tool), an integrated and automated framework designed to streamline the entire reconnaissance lifecycle within a unified and structured environment. AUTO combines passive and active subdomain enumeration, historical URL extraction, live host detection, parameter discovery, JavaScript analysis, high-speed port scanning, and vulnerability assessment for XXE, SSRF, and CORS misconfigurations.

The framework integrates multiple open-source utilities into a sequential workflow pipeline that automates data aggregation, validation, and structured reporting. Additionally, AUTO incorporates visual reconnaissance through automated screenshot capture to enhance attack surface visibility.

By consolidating diverse reconnaissance processes into a single automation framework, AUTO reduces manual effort, minimizes human error, improves operational efficiency, and enhances coverage depth. Overall, AUTO transforms traditional reconnaissance into a scalable and intelligent cybersecurity solution.

Keywords- Domain Reconnaissance, Subdomain Enumeration, Vulnerability Assessment, Cybersecurity Automation, XXE, SSRF, CORS, Port Scanning, Open-Source Intelligence (OSINT), Security Testing.

I. INTRODUCTION

The rapid expansion of web technologies, cloud computing platforms, and distributed enterprise applications has significantly increased the digital footprint of modern organizations. Today's domain infrastructures consist of numerous subdomains, APIs, microservices, third-party integrations, and dynamically generated web resources. While this digital transformation improves scalability and accessibility, it simultaneously expands the potential attack surface, making organizations more vulnerable to cyber threats. As a result, reconnaissance has become one of the most critical phases in cybersecurity assessments and penetration testing. Reconnaissance refers to the systematic process of gathering information about a target domain or infrastructure to identify exposed assets, services, and potential vulnerabilities. It serves as the foundation for understanding the security posture of a system before launching further security testing or defensive measures. Traditionally, security professionals rely on multiple open-source tools to perform tasks such as subdomain enumeration, port scanning, URL extraction, vulnerability testing, and visual inspection. Although these tools are powerful individually, they operate independently and require manual coordination, scripting, and result consolidation. This fragmented workflow often leads to inefficiencies, redundant processing, inconsistent reporting formats, and the possibility of human oversight. Subdomain enumeration tools help identify hidden or forgotten assets associated with a primary domain. Port scanning utilities detect open services that may expose critical infrastructure components. Vulnerability

scanners identify weaknesses such as XML External Entity (XXE) injection, Server-Side Request Forgery (SSRF), and Cross-Origin Resource Sharing (CORS) misconfigurations. However, combining these tools into a coherent, automated pipeline remains a challenge for many security teams, especially in large-scale assessments. To address these limitations, this paper proposes AUTO (Automated Domain Reconnaissance Tool) — a comprehensive framework that integrates multiple reconnaissance and vulnerability assessment processes into a unified automation system. AUTO streamlines passive and active subdomain discovery, live host validation, historical URL extraction, parameter and JavaScript analysis, port scanning, vulnerability detection, and automated reporting within a structured workflow. By reducing manual intervention and standardizing output generation, the system enhances efficiency, scalability, and accuracy in domain reconnaissance. The primary objective of this research is to design and implement a scalable, automated reconnaissance framework that improves coverage depth while minimizing operational complexity. By transforming traditionally fragmented reconnaissance practices into a cohesive and repeatable workflow, AUTO aims to support security researchers, penetration testers, and organizations in proactively identifying potential attack vectors and strengthening their cybersecurity posture.

II. LITERATURE REVIEW

Review Domain reconnaissance and vulnerability assessment are essential phases in cybersecurity testing and penetration testing. Various tools such as subdomain discovery utilities, port scanners, and vulnerability detection frameworks have been developed to assist security professionals. However, most of these tools operate independently and require manual coordination. Researchers and cybersecurity professionals commonly use reconnaissance tools to discover hidden assets associated with a domain. These tools collect information from DNS records, search engines, APIs, and open-source intelligence sources to identify exposed infrastructure components. Despite their effectiveness, the lack of integration between these tools often leads to fragmented workflows and inefficient result analysis. Security professionals must manually combine outputs from different utilities and organize them for further testing. The proposed AUTO framework addresses this challenge by integrating multiple reconnaissance techniques and tools into a unified automated system. By combining subdomain discovery, URL extraction, port scanning, and vulnerability detection into a single pipeline, AUTO improves efficiency and simplifies the reconnaissance process.

III. METHODOLOGY

The AUTO framework follows a structured pipeline to automate the reconnaissance and vulnerability assessment process.

1. Target Domain Input

The process begins when the user provides the target domain as input to the system. This domain becomes the starting point for the reconnaissance workflow.

2. Subdomain Enumeration

The framework performs both passive and active subdomain discovery techniques to identify all subdomains associated with the target domain.

3. Live Host Detection

After discovering subdomains, the system validates which hosts are active and accessible.

4. URL and Parameter Extraction

The framework collects historical URLs and parameters from archived web sources to identify potential entry points for testing.

5. JavaScript Analysis

JavaScript files are analyzed to discover hidden endpoints, API routes, and additional parameters that may expose vulnerabilities.

6. Port Scanning

High-speed port scanning is performed to identify open ports and the services running on them.

7. Vulnerability Testing

The system runs vulnerability detection modules to identify security issues such as XXE, SSRF, and CORS misconfigurations.

8. Automated Reporting

Finally, all collected information and detected vulnerabilities are compiled into structured reports to assist security researchers and penetration testers.

IV. IMPLEMENTATION

The AUTO framework is implemented as an automated pipeline that integrates multiple open-

source cybersecurity tools to perform domain reconnaissance and vulnerability assessment.

1. The system begins by accepting a target domain as input. After receiving the input, the framework performs automated subdomain enumeration to identify associated assets. The discovered subdomains are then validated to determine which hosts are active.
2. The system extracts historical URLs and parameters from archived web sources. JavaScript files are analyzed to discover hidden endpoints and API routes.
3. The framework then performs high-speed port scanning to identify open ports and running services. Finally, vulnerability testing modules are executed to detect issues such as XXE, SSRF, and CORS misconfigurations. All collected results are organized into structured reports to assist security researchers and penetration testers.

V. ADVANTAGES

1.Automation of tasks

AUTO automates many reconnaissance tasks, which reduces manual work for security researchers.

2. Time saving
   Since multiple tools run automatically in a single pipeline, the scanning process becomes faster.
3. Better attack surface discovery
   The system helps discover hidden subdomains, URLs, and endpoints that may contain vulnerabilities.
4. Improved efficiency
   By integrating multiple tools together, the framework improves the efficiency of security testing.
5. Organized results
   The system generates structured and organized reports, making it easier for security analysts to review the results.

VI. LIMITATIONS

1. Focus on web-based reconnaissance

The framework mainly focuses on domain and web application scanning and may not detect deeper system-level vulnerabilities.

2. Manual verification required

Some vulnerabilities detected by the system may require manual verification by security experts.

3. Performance depends on network speed

Slow internet connections can increase the scanning time.

4. Large targets require more time

Domains with a large number of subdomains and services may take longer to scan.

5. Limited advanced vulnerability detection

Some complex vulnerabilities may not be fully detected by automated tools.

VII. CONCLUSION

Reconnaissance plays a crucial role in identifying potential security weaknesses within modern web infrastructures. However, traditional reconnaissance processes rely on multiple independent tools, resulting in fragmented workflows and increased operational complexity.

This research presented AUTO (Automated Domain Reconnaissance Tool), an integrated framework that automates the domain reconnaissance and vulnerability assessment process. By combining subdomain discovery, URL extraction, parameter analysis, port scanning, and vulnerability detection into a single automated pipeline, AUTO simplifies the reconnaissance process and improves operational efficiency.

The framework reduces manual effort, enhances coverage depth, and generates structured output reports that assist security researchers and penetration testers in identifying potential vulnerabilities effectively. Overall, AUTO transforms traditional reconnaissance into a scalable and efficient security assessment solution.

VIII. FUTURE SCOPE

Future improvements to the AUTO framework may include the integration of machine learning techniques to enhance vulnerability detection accuracy.

- Another potential enhancement is the development of real-time monitoring capabilities, allowing the system to continuously scan domains and detect newly exposed assets.

- The framework may also be expanded to support cloud infrastructure reconnaissance and container security scanning.

ACKNOWLEDGEMENT

The authors would like to thank the faculty of R.D Engineering College for their support and guidance during this research.

Conflict of Interest
The authors declare no conflict of interest.

REFERENCES

[1] OWASP, *OWASP Top 10*, 2021
[2] Gordon Lyon, *Nmap Network Scanning*, 2009
[3] Project Discovery, *Subfinder Tool*, 2022
[4] OWASP Amass Project, 2021
[5] Project Discovery, *httpx Toolkit*, 2022
[6] Internet Archive, *Wayback Machine*, 2020
[7] C. Sullo, *Nikto Web Scanner*, 2019
[8] Stuttard & Pinto, *Web Application Hacker's Handbook*, 2011