*Grenze International Journal of Engineering and Technology, January Issue*

# Integrated Vulnerability and Asset Discovery Toolkit

S. Giridharan[1], M. Senthil Kumar[2], K. Madhura Nadh[3], C. Mahesh Kumar[4] and R. Ashwin[5]
[1-5]Department of Cyber Security, SRM Valliammai Engineering College, Tamilnadu, India
Email: giridharans.cys@srmvalliammai.ac.in, msen1982@gmail.com, kmadhuranadhzz@gmail.com, maheshmk8030@gmail.com, ashwinramesh9123@gmail.com

***Abstract*— Existing Organizations and individuals must make cybersecurity a top priority. As cyber threats continue to advance, organizations need to adopt proactive security strategies that merge vulnerability detection with asset discovery. This toolkit consolidates asset discovery, subdomain enumeration, endpoint mapping, and vulnerability scanning into one cohesive, scalable system. The swift rise of cyber threats calls for proactive and effective security practices that emphasize both vulnerability evaluation and asset identification. Nowadays, organizations confront an increasingly broad attack surface, with digital assets dispersed across various infrastructures, which heightens the risk of exploitation. By utilizing reNgine, a sophisticated reconnaissance and vulnerability scanning tool, our proposed system combines automated reconnaissance, vulnerability assessment, and continuous monitoring into a singular, scalable solution to enhance incident response times and encourage a proactive stance toward cybersecurity threats.**

***Keywords*— Vulnerability Discovery, Asset Discovery, Web Reconnaissance, reNigne, Threat Intelligence, Data Correlation.**

## I. INTRODUCTION

With the growing digitization of companies and organizations, prioritizing cybersecurity has become essential due to the increasingly advanced nature of cyber threats. The "Integrated Vulnerability And Asset Discovery Toolkit" aims to utilize various tools for subdomain enumeration, vulnerability evaluation, and asset identification to protect their digital presence. Nevertheless, the absence of integration among these tools often leads to overlapping workflows, inefficiencies, and disjointed security assessments. Conventional web reconnaissance involves utilizing numerous tools for subdomain discovery, port scanning service identification, directory fuzzing, and vulnerability evaluation. Security teams frequently encounter challenges with data correlation, as the outputs from different tools must be manually combined to produce valuable insights. In the situation, where false positives, overlapping results and disparate formats create further complexities in the ways of vulnerability management, it's a confusing and daunting task. The driving aim of this project is to build a centralized toolkit for discovery of vulnerability and asset capabilities to foster trust with multiple stakeholders, such as suppliers, distributors, and retailers. Block chain gives us data integrity but it does not assure you the predictive abilities needed for the inventory optimization.

The situation gets further complicated by the false positives, the overlapping results, and the different reporting format. The bigger picture of this project is to address the necessity for a central toolbox for vulnerability and asset discovery leveraging reNgine for automated security scanning and even more so, based on concrete system information for vulnerability scanning and asset discovering through multiple NPAs.

*Grenze ID: 01.GIJET.12.1.310*

It further improves efficiency, minimizes redundant activities, and overall strengthen an organization's security posture. Additionally, the interface will be a user friendly one from which users can easily generate Sigma rules and strip out the difficulty of defining as well as implementing detection strategies. This toolkit is built for scalability, which will allow ease of future improvements. To help deal with these issues, we present a completely automated and closed, centralized toolkit for vulnerability and/or asset discovery.
It includes reNgine, an advanced Open Source web reconnaissance and vulnerability scanning tool for full automation of the entire reconnaissance workflow so that security analysts have the tools at their disposal to proactively protect themselves from the cyber threats. With the Integrated Vulnerability and Asset Discovery Toolkit in place, their solution for automated enumeration of assets, subdomain discovery, vulnerability scanning, real-time notifications, and scalability in the cloud, is a holistic solution. With the inclusion of several cybersecurity tools, the toolkit expands the security evaluation, allowing the organization to adopt a strong and automated strategy to the threat finding and asset monitoring. It is an array of open source cybersecurity which allows it to play a part in simplifying reconnaissance, vulnerablility evaluation and asset identification. By integrating these two platforms businesses are better able to track inventory, make better decision and have a secure and intact supply chain platform to depend on for effective supply chain operation. This integrated solution has one of the greatest strengths in being able to change as business needs change. This an innovative and reactive [6] inventory management system that is able to witness sudden changes in consumer behavior, compliance laws, the breakage of global supply chains and so on. There is proposed strategy not only for the day to day inventory, but also for the long term flexibility by means of real time data analytics as well as security. Through the use of automated, data-driven decision making, organizations will increase accountability of their inventory management, reduce operational costs, and consequently increase productivity. It brings together all the popular open source security tools to aid in the process of Reconnaissance, Vulnerability Assessment and Asset Discovery. This combination ensures that a training approach that incorporates several methods to discover security vulnerabilities is facilitated. This toolkit achieves a strong and effective cybersecurity solution in that it unites multiple security instruments, automates vulnerability identification, and adopts a cloud based structure. It is such a valuable resource for penetration testers, security researchers, and organization that they immediately alert with their intelligence enhancement and intuitive interface. In this work, the literature survey is reviewed in Section II. Section III describes methodology and the functionality thereof. Results and discussions are discussed in Section IV. Finally, Section V concludes by suggesting and finding the main points.

## II. LITERATURE SURVEY

[1] The system employs fault-tolerant control through adaptive model predictive control at the turbine level, along with a control reallocation mechanism at the farm level. Additionally, an Automatic Signal Correction (ASC) attack resilient strategy is proposed from the operator's perspective for network security improvement. The method is verified using an elaborate wind farm model affected by different fault and attack scenarios, demonstrating its ability to ensure safety and dependability of the system.
Towards Vulnerability assessment and Penetration Testing (VAPT) [2], an automated VAPT framework that exploits a multi agent system is proposed to maximize the vulnerability discovery as well as the carrying out of penetration tests. This includes monitoring ongoing threats for an ongoing threat analysis without requiring manual intervention and a thorough security evaluation. This framework is meant to enable the VAPT process to accurately simplify and streamline it for both the individual and for the company.
SCEVD (Semantic-enhanced Code Embedding for Vulnerability Detection) is presented by us [3], a use of graph pruning techniques that preserve the important information for higher detection accuracy. Experimental results demonstrate that semantic rich code representations can help increase vulnerability identifications by up to 12 percent compared to baseline trimming approaches, especially in high accuracy industries which include pharmaceuticals and perishable logistics and technology offers of automatic reporting solutions in the recent times. These solutions [10] provide stakeholders with verifiable records of transactions, allowing greater accountability a dispute.
[4] ContractWard is an Ethereum smart contract vulnerability detection technique that uses machine learning. It uses XGBoost and SMOTETomek for training and extracts bigram characteristics from operation codes. It has over 96% F1 scores after being evaluated on 49,502 contracts, guaranteeing great accuracy and effectiveness in spotting possible security threats in blockchain applications. such issues as standardization of data, aversion to sharing information, and complying with regulations present the adoption problem. Companies are exploring open-source platforms and collective frameworks to drive increased adoption and effortless integration with established supply chains.

## III. PROPOSED SYSTEM

The system we're proposing offers a smart way to find and manage security vulnerabilities. It automates the whole process of checking for weaknesses in your systems, so your team can focus on fixing problems instead of spending time searching for them. This automation cuts down on manual work and speeds things up. We've built in real-time monitoring, which means your assets are watched continuously. If something suspicious is detected, the system immediately sends alerts, reducing the window of opportunity for potential attack . The system smartly prioritizes threats by giving each a risk score based on factors like how easy it is to exploit the vulnerability, how critical the affected asset is to your operations, and the severity of the issue. This helps your team know what to tackle first. By combining automation, intelligent risk assessment, and flexible detection rules, this approach strengthens your organization's security. It ensures vulnerabilities are addressed quickly and efficiently, giving you peace of mind that your systems are protected against emerging threats. The real-time alerts mean you'll always be informed about potential dangers the moment they're detected prompt alerts about possible dangers. Users can also personalize their threat intelligence feeds, concentrating on topics like security patches, malware analysis, and new threats. Situational awareness and response effectiveness are improved by this tailored strategy. The technology optimizes resource usage while enhancing cybersecurity defenses by combining automation, intelligence-driven risk prioritization, real-time warnings, and configurable rule-based threat detection. Organizations can proactively manage vulnerabilities, minimize attack vectors, and uphold a strong security architecture with this all-inclusive solution.

## IV. METHODOLOGY

The Integrated Cybersecurity Toolkit aims to expedite threat detection and analysis by combining automation, intelligence, and user customization. The first step in the development process is requirements gathering and design, which identifies the specific needs of security analysts. Core features like email analysis, domain monitoring, vulnerability scoring, real-time security news aggregation, custom rule generation, and an adjustable interface are defined in this phase. Several security features are put into place during the Module Development stage. To deliver the most recent threat intelligence, The Security Alerts Feed incorporates APIs from reliable sources such as TechCrunch Security and The Hacker News. The Domain Monitoring module analyzes dubious domains, extracts pertinent IP addresses, and takes screenshots for additional examination by leveraging services like URLScan.io and threat intelligence APIs. To enable analysts to design and modify Sigma rules for threat detection without requiring a great deal of programming knowledge, a Graphical User Interface (GUI) for Security Rules has been developed. Several fundamental components must be developed during the implementation phase. Open-source reconnaissance and vulnerability scanners are used to automate security assessments as part of the integration of cybersecurity tools. Vulnerability scanning and subdomain enumeration are used to find security flaws, exposed services, and configuration errors. The technology incorporates Telegram and Discord bots to provide real-time danger identification and immediate security alerts.

### *A. Integration of Multiple Tools*

The Integrated Vulnerability and Asset Discovery Toolkit is like a Swiss Army knife for cybersecurity. It brings together a bunch of open-source tools to automate the process of finding security holes and scanning for vulnerabilities. This means less manual work for your team and more accurate security checks. The toolkit can dig into online apps, networks, and cloud setups to find assets, spot misconfigurations, and flag vulnerabilities. It uses a mix of tools like Nmap, Subfinder, Amass, Naabu, and reNgine to scan for subdomains, open ports, services, and vulnerabilities. This multi-layered approach ensures a thorough check, reducing the need for repetitive tests. By automating these tasks, the toolkit keeps a constant watch on your security, helping businesses stay ahead of threats and keep their systems safe.The solution guarantees constant security monitoring by automating reconnaissance, allowing businesses to proactively identify and reduce threats.

### *B. Sub Domain Enumeration and Vulnerability Scanning*

Attackers often exploit forgotten or misconfigured subdomains to gain unauthorized access, making subdomain enumeration and vulnerability scanning crucial for security assessments. Our system leverages advanced tools like reNgine, Subfinder, and Amass to automate the discovery of subdomains and identify open ports. These tools work together to map the entire attack surface, uncovering both open and hidden subdomains that might host vulnerable services that are susceptible. The vulnerability scanning module then steps in, using scanners like Nuclei and OpenVAS to evaluate these subdomains for security flaws, including common vulnerabilities, outdated software, and misconfigurations. By automating this process, the system ensures a thorough check of

the organization's infrastructure, reducing the risk of missed security issues. It also allows for scheduled scans, enabling continuous monitoring of assets. The collected data is stored and analyzed to identify security patterns, helping firms prioritize high-risk vulnerabilities and address potential threats efficiently.

*C. Real Time Alert System*

When a vulnerability is detected, our real-time alerting module springs into action, instantly notifying users through Telegram and Discord bots. This ensures a swift response to security risks, unlike traditional systems that often suffer from delayed notifications, increasing the risk of exploitation. With our custom alert setups, security teams receive detailed notifications that include threat severity, impacted assets, and exploitability levels. These alerts come with comprehensive data, such as affected domains, vulnerability descriptions, and even repair suggestions, allowing security experts to take immediate action. By integrating real-time alerts with chat platforms, we've made it easier for security teams to discuss findings, assign tasks, and track remediation efforts all in one place, enhancing collaborative incident response.

*D. Third Party API Integration*

The Integrated Vulnerability and Asset Discovery Toolkit is like a Swiss Army knife for cybersecurity. It brings together a bunch of open-source tools to automate the process of finding security holes and scanning for vulnerabilities. This means less manual work for your team and more accurate security checks. The toolkit can dig into online apps, networks, and cloud setups to find assets, spot misconfigurations, and flag vulnerabilities. It uses a mix of tools like Nmap, Subfinder, Amass, Naabu, and reNgine to scan for subdomains, open ports, services, and vulnerabilities. This multi-layered approach ensures a thorough check, reducing the need for repetitive tests. By automating these tasks, the toolkit keeps a constant watch on your security, helping businesses stay ahead of threats and keep their systems safe.

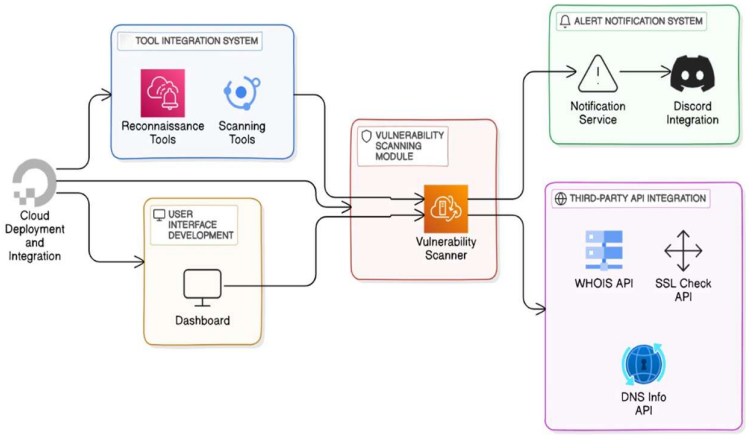


Fig. 1: Architecture Diagram

Figure 1 shows how we've put together a bunch of cybersecurity tools in our Integrated Vulnerability and Asset Discovery Toolkit. It's like a well-organized toolbox for security automation. Key parts include scanning for vulnerabilities, finding subdomains, sending real-time alerts, hooking up with third-party APIs, having a user-friendly GUI, and being able to scale up on the cloud. All these pieces work together to make finding threats and assessing risks smoother and more effective, giving you a cybersecurity setup that really delivers.

*E. Graphical User Interface*

To make cybersecurity easier and more accessible, we've designed a user-friendly graphical user interface (GUI) for our toolkit. This interactive dashboard lets users manage scans, tweak security settings, and check out threat intel without needing to be tech wizards. You can create reports, customize security alerts, schedule automatic scans, and assess vulnerabilities all from one place. One standout feature is the Sigma rule generation tool, which lets security teams craft and put into action custom detection rules tailored to their specific needs. The GUI also comes with interactive visualizations like heatmaps, graphs, and charts that help analysts quickly spot security trends and high-risk assets. This centralized control panel brings together GUI, cloud scalability, real-time alerts, subdomain enumeration, vulnerability assessment, and third-party API interaction, making automated risk assessment a breeze for both seasoned cybersecurity pros and those just starting out in the field.

*F. Scaling Tool to Cloud Interface*

We've put our solution on the cloud to make sure it's always up and running, performs well, and can grow as needed. This means companies can do big security checks without worrying about their hardware holding them back. Cloud deployment lets us process threats and vulnerabilities in different situations all at the same time. The system can adjust its resources on the fly to keep up with demand for real-time threat detection. Plus, storing data in the cloud keeps logs, security reports, and scan results safe with access controls and encryption. The cloud's flexibility also means the system can handle lots of traffic, making it a good fit for large-scale security operations. With real-time processing, constant monitoring, and automatic updates, our cloud-based module keeps the security toolkit working well, quickly, and ready to adapt to new cybersecurity challenges.

## V. Result and Discussion

The Integrated Vulnerability and Asset Discovery Toolkit is like a superhero team for cybersecurity. By bringing together multiple security features into one framework, it supercharges cybersecurity automation, risk prioritization, and real-time threat monitoring.

Fig. 2: Tool Analytics

Unlike regular vulnerability scanners that work in isolation, this toolkit combines vulnerability detection, asset discovery, and real-time threat intelligence to give you a holistic view of your security landscape. One standout feature is the real-time alerting mechanism, which uses Telegram and Discord bots to quickly notify security professionals. This means you can tackle threats as soon as they pop up, keeping your systems safe and sound.
By minimizing the response time to vulnerabilities, this feature shortens the window of opportunity for attackers to launch an attack. Furthermore, the GUI for creating Sigma rules streamlines the design of unique detection rules, increasing the adaptability and user-friendliness of security. However, a key challenge encountered during implementation was optimizing cloud-based scalability to support large-scale security assessments. Deploying the system on cloud infrastructure resolved performance bottlenecks, allowing faster and more efficient vulnerability scanning and analysis

**V. RESULTS & STATISTICAL INSIGHTS**

| Metric | Value | Insight |
|---|---|---|
| CVEs reported (Jan–Jul 2024) | 22,254 (+30% vs 2023) | Sharp rise reflects expanding attack surface blog.qualys.com +10 |
| Weaponized CVEs | 0.91% (~204) | Exploitation of older CVEs ↑10% YoY |
| Total CVEs full-year 2024 | 40,009 (+38% vs 2023) | Averaging ~108 CVEs/day |
| Critical/High severity CVEs (2024) | 19,100 (~47.7%) | Nearly half are high-impact |
| Weaponized vs published CVEs | 3,945 of 40,187 (~9.8%) | Most exploits target older flaws |
| Time to exploit (avg) | ~42 days | Exploits generally follow disclosure swiftly |
| Avg MTTR (critical) | ~65 days | Against exploit window of ~42 days; leaves systems exposed |

Fig 3

All things considered, the toolkit effectively fills in automated gaps in vulnerability management, increasing the effectiveness, scalability, and actionability of security assessments. Deep packet inspection, behavioral anomaly detection, and AI-driven threat intelligence analysis are possible future developments that could strengthen proactive threat mitigation and cybersecurity defense capabilities.

## VI. CONCLUSION

By combining vulnerability scanning, subdomain enumeration, real-time alerting, and third-party information into a single, effective system, the Integrated Vulnerability and Asset Discovery Toolkit offers a complete, automated, and scalable cybersecurity solution. The technology guarantees quicker and more accurate threat detection, improves automation, and decreases human labor by combining several security operations into a single framework. Traditional vulnerability management frequently necessitates a great deal of human involvement, which causes delays in the detection and mitigation of security threats. But by automating these procedures, this toolset frees up security professionals to concentrate on remediation rather than vulnerability detection by hand learning techniques with blockchain technology created a robust and intelligent inventory management solution. Security operations are greatly enhanced by the key features, which include cloud-based scalability, a customized GUI for rule authoring, and real-time security warnings. By using Telegram and Discord bots, the real-time alerting system makes sure security analysts are informed of threats instantly, enabling quicker incident response and shorter attack windows. Furthermore, companies can improve flexibility and agility by customizing security rules to fit their unique threat landscape with the help of the configurable Sigma rule-based detection system. Because cloud infrastructure deployment guarantees high availability, scalability, and quick processing, the toolkit may be used for cybersecurity requirements at both the small and enterprise levels. Demonstrated faster threat detection, reduced false positives, and improved resource optimization compared to traditional security tools. The integration of third-party threat intelligence APIs further enhances detection accuracy by cross-referencing vulnerabilities with global security databases. This not only improves security posture but also enables proactive threat mitigation, helping organizations identify and remediate vulnerabilities before they can be exploited. In order to further improve security intelligence, future developments will concentrate on deep packet inspection, enhanced behavioral analytics, and AI-driven automation. Increasing interoperability with more enterprise solutions and cybersecurity frameworks will improve flexibility and guarantee smooth integration with current security infrastructures.The significance of automation and intelligence-driven cybersecurity solutions in contemporary security operations is demonstrated by this study. With its strong, scalable, and proactive approach to real-time vulnerability management, the suggested toolkit gives businesses increased visibility, increased productivity, and better defense against new online threats.

## ACKNOWLEDGMENT

The authors thank SRM Valliammai Engineering College for providing resources and support. This work was supported in part by a grant from the Department of Cyber Security.

## REFERENCES

[1] O. Raut, A. Sultanpure, A. Naik and S. Bhadgaonkar, “ScanXpert – Framework for Web Reconnaissance and Vulnerability Enumeration,” Int. Res. J. Mod. Eng. Tech. Sci., vol. 7, no. 5, May 2025.
[2] A. Verma, A. K. Singh, D. Shukla et al., “Xploitguard: Automated Vulnerability Scanning Tool,” SSRN, Apr. 2025.
[3] S. Jai Balaji and A. Karmel, “Detecting Vulnerabilities Using Open Source Intelligence,” in Hybrid Intelligent Systems (LNNS), vol. 420, pp. 530–540, Mar. 2022.
[4] Z. Li, D. Zou, S. Xu et al., “VulDeePecker: A Deep Learning Based System for Vulnerability Detection,” arXiv preprint arXiv:1801.01681, Jan. 2018.
[5] S. Gvozdenovic, J. Becker, J. Mikulskis and D. Starobinski, “IoT Scan: Network Reconnaissance for the Internet of Things,” arXiv preprint arXiv:2204.02538, Apr. 2022.
[6] S. Marksteiner, H. Lernbeiß and B. Jandl Scherf, “An Iterative and Toolchain Based Approach to Automate Scanning and Mapping Computer Networks,” arXiv preprint arXiv:1710.01026, Oct. 2017.
[7] Z. Li, D. Zou, S. Xu, Z. Chen, Y. Zhu and H. Jin, “VulDeeLocator: A Deep Learning based Fine grained Vulnerability Detector,” arXiv preprint arXiv:2001.02350, Jan. 2020.
[8] “Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning,” G. F. Lyon, Insecure.Com LLC, 2009. (Tool reference)
[9] “reNgine: Automated Web Reconnaissance Framework for Web Applications,” GitHub Repository, 2023. (Tool reference)
[10] S. Roy, N. Sharmin, J. C. Acosta, C. Kiekintveld and A. Laszka, “Survey and Taxonomy of Adversarial Reconnaissance Techniques,” arXiv preprint arXiv:2105.04749, May 2021.
[11] R. Valenza, G. Costa and A. Armando, “Never Trust Your Victim: Weaponizing Vulnerabilities in Security Scanners,” arXiv preprint arXiv:2006.09769, Jun. 2020.