2025 IEEE 29th International Conference on Intelligent Engineering Systems (INES) | 979-8-3315-9771-9/25/$31.00 ©2025 IEEE | DOI: 10.1109/INES67149.2025.11078212

# Attack Surface Mapping of Country-Wide Networks - a Technical Report

1st Ernő Rigó
*Institute for Computer Science and Control (SZTAKI)*
*Hungarian Research Network (HUN-REN)*
Budapest, Hungary
rigo.erno@sztaki.hun-ren.hu

2nd Zoltán Komáromi
*Institute for Computer Science and Control (SZTAKI)*
*Hungarian Research Network (HUN-REN)*
Budapest, Hungary
komaromi.zoltan@sztaki.hun-ren.hu

3rd Boldizsár Bencsáth
*Ukatemi Technologies Plc.*
Budapest, Hungary
boldizsar.bencsath@ukatemi.com

4th Gergő Ládi
*Ukatemi Technologies Plc.*
Budapest, Hungary
gergo.ladi@ukatemi.com

5th Ferenc Schulcz
*Ukatemi Technologies Plc.*
Budapest, Hungary
ferenc.schulcz@ukatemi.com

6th Annamária Riethné Nagy
*Institute for Computer Science and Control (SZTAKI)*
*Hungarian Research Network (HUN-REN)*
Budapest, Hungary
nagy.annamaria@sztaki.hun-ren.hu

7th Zoltán Aradi
*John von Neumann Faculty of Informatics*
*Óbuda University*
Budapest, Hungary
aradi.zoltan@uni-obuda.hu

***Abstract*—The escalating landscape of cyber threats necessitates a comprehensive approach to detecting compromised devices and services across wide-area networks, particularly for national security. This paper presents methodologies and results from a study aimed at enhancing the cybersecurity posture of Hungary's digital infrastructure, facilitated by the national Computer Security Incident Response Team (CSIRT). By employing active and passive attack surface detection, digital fingerprinting, and utilizing advanced data enrichment techniques from sources such as certificate transparency lists, we enhance the detection and analysis capabilities for compromised entities within the .hu domain and Hungarian IP address spaces. Our multi-faceted approach not only supports the early identification of security breaches but also enables proactive risk mitigation, contributing to a strengthened national cybersecurity framework.**

***Index Terms*—cybersecurity, vulnerability detection, data enrichment, compromised devices, CSIRT, certificate transparency, dark web intelligence, common platform enumeration, CPE, attack surface mapping**

## I. Introduction

The cybersecurity terrain is increasingly threatened by compromised devices and websites, essential in numerous high-profile internet threats. Advanced persistent threat (APT) actors exploit these for purposes such as evading traceability, temporary data storage, phishing, and distributing ransomware and cryptojacking malware. The availability of remotely controlled compromised devices or services, often as botnets, is central to spam, cryptocurrency mining, and distributed denial-of-service (DDoS) attacks. This project focuses on active and passive methods of wide area detection of compromised devices and services, supported by the Hungarian Computer Security Incident Response Team (CSIRT).

Building on the "Internet Survey Hungary" initiative, the project advances collection methodologies for IPv4/IPv6 and URI/URL-based service identification within the ".hu" ccTLD. The CSIRT's capability to scan the national IP range and ccTLD for compromised resources enhances situational awareness, enabling early detection and mitigation of threats like botnets and malware, preserving critical infrastructure. Additionally, detailed insights allow the CSIRT to issue informed advisories, initiate targeted security scans and strengthen national cyber resilience, reducing risks and further enhancing trust in the cybersecurity framework.

Independent development of attack surface mapping capabilities benefits a national CSIRT by providing tailored, comprehensive, and up-to-date insights into the specific vulnerabilities and threats pertinent to its national infrastructure, ensuring greater alignment with local regulatory and operational contexts. This independence allows for rapid customization and integration with existing security frameworks, facilitating a more dynamic and responsive defense posture. Relying on similar public services could be limiting due to potential misalignment with national security priorities, slower adaptability to emerging threats, and less control over data privacy and sovereignty, which are crucial for maintaining the integrity and confidentiality of national cybersecurity efforts.

## II. Related Work

The increasing reliance on digital infrastructure has heightened the need for effective cybersecurity measures, particularly in the context of internet-wide scanning and vulnerability assessment. This literature review synthesizes recent research into several subcategories as follows.

### *A. Vulnerability Scanning Techniques*

Vulnerability scanning is for identifying and mitigating security weaknesses. Recent studies emphasize the development and effectiveness of automated tools. Sllame et al. [1] integrate several open-source tools with AI-powered ImmuniWeb for a comprehensive assessment. Alazmi and Leon [2] systematically review web application vulnerability scanners, highlighting their role in web security. Nair et al. [3] introduce VSAT, enhancing assessment with a user-friendly interface and detailed reporting. Pour et al. [4] survey internet measurement techniques, discussing various scanning methodologies. Ecik [5] compares active and passive scanning, while Čerget et al. [6] review progress in identifying and mitigating cyber threats.

### *B. Wide Area Network (WAN) Attack Surface Mapping*

WAN attack surface mapping is focusing on vulnerabilities in extensive networks. Everson and Cheng [7] provide a comprehensive survey on tools and methodologies, emphasizing its importance for enhancing defenses. Roy et al. [8] offer a taxonomy of adversarial reconnaissance techniques, categorizing information gathering methods. Mayer et al. [9] discuss the landscape of internet-wide scanners for effective mapping, noting the need for better integration and usability. Pour et al. [10] survey measurement techniques for mapping, while Griffioen et al. [11] provide insights into a decade of internet scanning. Richter et al. [12] examine IPv6 scanning challenges, and Alian et al. [13] highlight automated vulnerability scanners' role in enhancing mapping efficiency.

### *C. Modelling and Enrichment of Cybersecurity Scan Data*

Data modeling and data management is offering a structured framework for organizing and interpreting data. Zhao et al. [14] present a graph model for street-level geolocation, improving spatial data representation. Pour et al. [10] discuss operational Cyber Threat Intelligence feeds for cybersecurity data enrichment. Effective data storage solutions focus on optimizing performance and cost, as explored by Leszczyna [15], who examines cybersecurity assessment methods to highlight critical data retention. Camargo et al. [16] show that scaled-down network telescopes enhance threat detection, demonstrating effective data storage and modeling's role in maintaining robust network traffic analysis.

## III. METHODOLOGY

This section describes our cybersecurity data management methodology that integrates domain-based identification, data normalization, and efficient processing. Our portable test environment ensures applicability and compliance with privacy and regulatory standards.

### *A. Target Identification*

Identifying compromised devices or services in a dynamic internet landscape is challenging due to the changing nature of IP addresses, especially in shared hosting environments where multiple services share a single IP. Web servers, for example, are often employ virtual hosting to operate different websites from one IP based on HTTP headers, particularly the domain name. Thus, relying solely on IP addresses can misidentify compromised services. Domain names offer the necessary granularity to accurately distinguish and detect threats among services using the same IP.

In the context of organizing and utilizing domain information efficiently, a comprehensive data model and storage strategy was developed. The model supports gathering domain data from various sources into a centralized repository that then be analyzed using different methods. The core data sources include continual data collection from Domain.hu regarding new and parked domains, data from the .hu zone files, self-collected TLS certificates, and data extracted from certificate transparency logs, alongside reputation databases (see Fig. 1). From these sources, 1 271 279 unique .hu TLD domain names were collected during the experimental phase of the project.

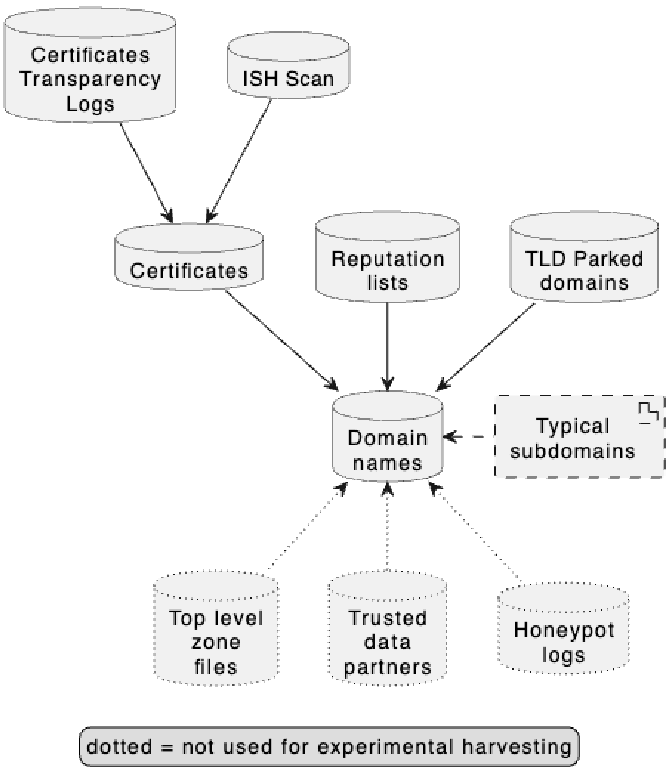


Fig. 1. Top-level domain sources

The data model accommodates CSV formats for processing into an OpenSearch database, facilitating structured ingestion and querying with fields like domain, (optional) owner, and precise harvest date. Records capture the latest modifications with fields such as *last.harvest.dns*, *last.harvest.cert*, and *last.harvest.reputation*, ensuring explicit documentation and date-referencing for optimal searchability. Designed for dynamic updates, the system achieves efficient data management by updating only when changes occur, thus minimizing redundancy. This approach prioritizes clarity and search optimization, allowing efficient aggregation of DNS, certificate, and reputation information for further research and application.

### *B. Data Normalization*

The data normalization process in this research aimed to address heterogeneity and enhance reliability, focusing on data from various vulnerability crawlers, including HTML content, DOM elements, CSS scripts or hashes, executable code (JavaScript and TypeScript). We have prioritized processing and storing attributes that serve as Indicators of Compromise (IoC), which, while not immediately indicating threats, reflect potential attack evidence. Our approach, by storing comprehensive data, enables temporal evaluations and correlates historical changes with potential compromises.

Several normalization tasks were primarily supported by hash comparisons, facilitating the detection of subtle content alterations and ensuring the integrity of IoC elements. The data model did not differentiate between sites within a broader domain but allowed filtering based on specific domains, supporting both consistency across multiple pages and localized focus. Although machine learning techniques were beyond the immediate scope, the structured database provided a foundation for future algorithmic applications.

Given the large volume and diversity of data attributes, the NoSQL database OpenSearch [17] was employed, selected for its open-source nature, extensive APIs, robust analytics, and adherence to industry standards, allowing quick searches and flexible analysis. The denormalized schema facilitated efficient storage and retrieval, optimizing structural queries related to each page as a primary entity. The normalization process transformed captured HTML content into structured fields using specialized data extraction libraries like BeautifulSoup, parsing data into categories such as server information, service characteristics, and web metadata. This breakdown into individual attributes ensured effective monitoring of changes for compromise signs.

### *C. ETL Workflow*

In the data collection, transformation, and loading (ETL) workflow designed for the project, several components and processes were implemented to efficiently handle data from collection to visualization. As illustrated by Fig. 2, specialized tools were used to emit structured data in formats such as CSV or JSON. These tools included all specific software and external data query services described in the following sections.

Following data collection, Python-based preparsers and enrichers functioned as the initial processing layer. These scripts were responsible for cleaning the raw data, normalizing it into consistent formats, and enriching it by incorporating additional computations or leveraging external datasets to enhance context. Python's versatility and ecosystem enabled the integration of libraries that performed complex data manipulation operations efficiently and flexibly.

The cleansed and enriched data was then ingested into an OpenSearch time series database using Logstash, a robust data collection engine known for its flexibility and scalability. Logstash was configured to build pipelines for real-time data ingestion, enabling structured data from CSV or JSON files to be parsed, transformed, and loaded into OpenSearch. This integration facilitated the efficient management and retrieval of large volumes of time series data, typical in cybersecurity scenarios.

The OpenSearch platform enabled comprehensive data analysis and visualization through refined queries and dynamic dashboards, allowing analysts to monitor trends, detect anomalies, and derive insights into security threats with intuitive interfaces for tracking key metrics and decision-making. Additionally, the OpenSearch API facilitates seamless integration for external parties, like a national CSIRT, enabling efficient access, custom queries, and data extraction to enhance monitoring and alerting capabilities. This interoperability ensures the ETL pipeline enhances parallel efforts with broader national cybersecurity objectives.

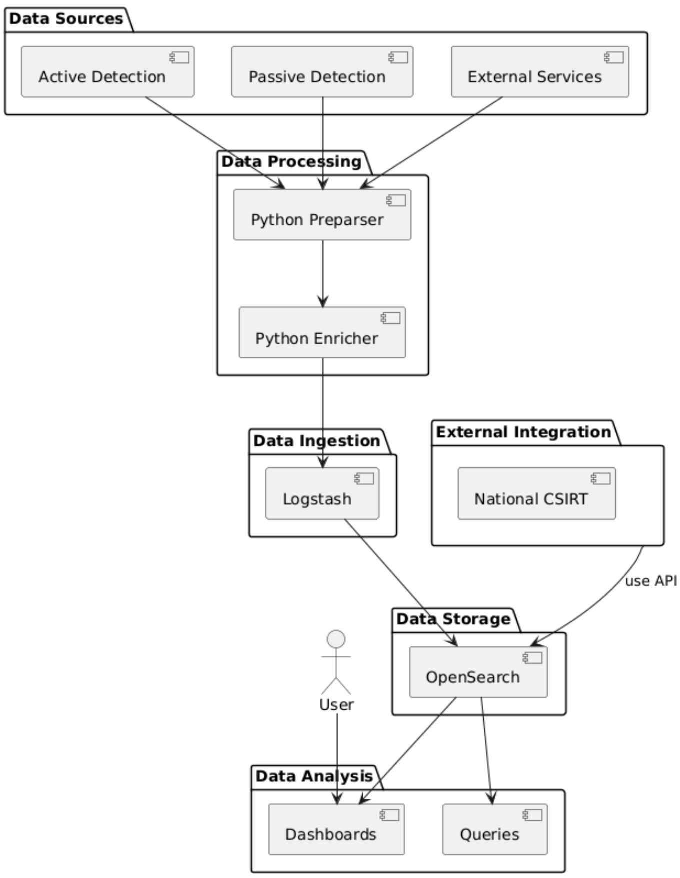


Fig. 2. ETL workflow

### D. Test Environment

In designing the research environment, which builds upon the Internet Survey Hungary (ISH) infrastructure, a methodological focus was placed on developing a proof of concept to demonstrate the practical applicability of theoretical concepts, particularly in the context of the Hungarian .hu domain space and IPv4 address range. This was done primarily to address the uncertainty factors related to the toolsets intended for use by the national CSIRT. The testbed was built to be repeatable and portable, leveraging containerization technologies such as Docker, alongside scale-out cloud platforms like OpenStack and Kubernetes, to ensure that the experiments could be replicated easily and deployed across various environments without significant reconfiguration.

The testbed focused on lightweight, scalable solutions for comprehensive anomaly detection tailored to specific project needs, necessitating custom-developed methods for effectiveness on smaller scales. The data architecture for compromised systems emphasized efficient data collection, structuring, and optimized search capabilities while maintaining high security and privacy standards. Designed to comply with legal requirements and industry best practices, the system incorporates robust security measures, ensuring data integrity and confidentiality.

## IV. Results

### A. Non-intrusive Detection

Our study introduces a non-intrusive detection framework leveraging ZMap to effectively identify vulnerabilities and potential compromises within a network, specifically targeting the Hungarian IPv4 space. The solution was employed to map open TCP ports across the network. Subsequently, a custom detection script was designed to validate these findings by probing the identified hosts for specific vulnerabilities indicated by Common Vulnerabilities and Exposures (CVEs).

The methodology involves running ZMap to scan for open ports and using custom detection commands executed in parallel for efficiency. This approach focuses solely on TCP port-accessible vulnerabilities, excluding deeper forensic or network behavioral analyses, which fall outside the tool's current scope. The implementation required key dependencies including GNU parallel, zmap, ztee, and Bash scripting, with customizable parameters set within the scanning script for targeted IP and network interfaces (see Fig. 3).

Our approach excels in handling multiple hosts simultaneously. An experimental detection script was developed for scanning for malware via TCP port 7777, known for its ”xlogin:” banner indicating command-and-control communication. Results were logged into a structured output file for further processing. Performance tests demonstrated considerable speed, with the tool scanning the entire Hungarian IPv4 address space in around 3 minutes and 30 seconds, on a hardware with an Intel Core i7-6700 CPU with 66GB RAM and a 10 Gbps network adapter.

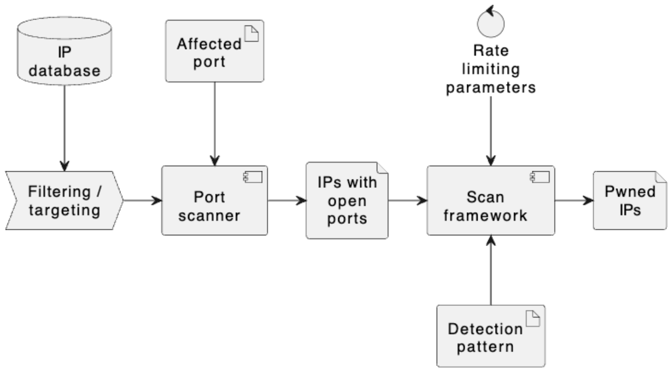


Fig. 3. Vulnerability detection schema

### B. Active Vulnerability Detection

*1) ZGrab2 Method:* The initial concept for detecting compromised hosts involved creating custom modules within the ZGrab2 framework. This approach aimed to leverage the ZMap/ZGrab2 ecosystem's power for high-speed network scanning and detection of malicious activity. The process required developing a custom ZGrab2 scanner module, which involved implementing the scanner logic in a new module written in Go and integrating it into the broader ZGrab2 toolkit.

Setting up the module involved configuring defaults, recompiling the ZGrab2 tool, and addressing complications from version control and environment setup. The detection logic targeted specific TCP ports for malware infection indicators, where compromised hosts might show identifiable signatures or open ports. In a later phase, this approach was abandoned for more efficient detection strategies, as custom ZGrab2 modules were complex and resource-intensive. Alternative methods provided better adaptability, speed, and ease of deployment, aligning more effectively with our project needs and priorities.

*2) NASL Method:* An active detection methodology was developed using the Nessus Attack Scripting Language (NASL) to identify vulnerabilities or compromised hosts across extensive network environments. Initially, the project explored using NASL for probing specific vulnerabilities through custom scripts, recognizing the flexibility and standardized approach that NASL scripts provide. This method was intended for application within a Dockerized setup of the Greenbone Vulnerability Manager, leveraging the openvas-nasl tool to execute NASL scripts for mass-detection purposes.

The performance of NASL scripts, in general, was not originally optimized to run single scripts across vast numbers of hosts, but rather the opposite. This architectural limitation posed challenges for our use case. During tests, the script portscan-http.nasl, which simply checks for open TCP ports 80 or 443, was utilized. In the first test, scanning 36,598 unique addresses, or approximately 0.5% of the Hungarian IPv4 space, took about 13 days. This delay was primarily due to time spent waiting for host responses, with many addresses lacking active web servers. In a second test, focused on IP addresses pre-identified by ZMap as having open ports, 120,953 unique addresses were scanned. This comprehensive test, accounting for every web server host in the Hungarian IPv4 network, took approximately one week to complete. These results highlighted the need for better-parallelized execution and optimized scanning strategies to enhance performance and efficacy in such large-scale network assessments.

### C. Defacement Detection

Our primary activities in defacement detection is utilizing web crawling to identify content changes indicative of defacement or black hat SEO activities. The aim is to identify a potential detection solution. This involves constructing an archive-like service that can thoroughly compare and analyze website contents using automated tools to detect anomalies and deviations from the norm.

The deface detection tool identifies potentially compromised websites through web crawling and heuristic analysis, featuring a Python-implemented crawler script and a signature collection process that acquires SHA-256 hashes of compromised content from sources like Zone-H. While practical, the tool can be enhanced; it currently focuses on specific HTML tags, potentially missing some defacement cues, especially those using unconventional coding or media elements. Future improvements could include integrating multi-modal hashing techniques like TLSH and neural network models to boost detection accuracy, reduce false positives, and cover a wider array of defacement tactics, thereby increasing reliability and operational success.

### D. Detection with Honeypots

The evaluation of compromised device detection, conducted through HunCERT's deployment of a distributed honeypot system across Hungarian IP space, provided insights into regional malicious activity. These honeypots, integrating HunCERT Probe data, non-intrusively collected traffic patterns indicating potential compromises, focusing on identifying sources of malicious activities, such as URL interactions deploying harmful payloads. The most prominent outcome was the development of a framework autonomously searching for malicious patterns in honeypot data, capable of detecting known signatures and issuing alerts. This methodology leverages historical data, continuously enhanced by normalized patterns from reliable sources like security forums, threat databases, and research publications, integrating fresh intelligence on emerging threats.

## V. Data Enrichment

In WAN-scale compromised device identification, data enrichment enhances collected raw data with reputation and ground truth sources, enabling more precise endpoint identification. This section discusses our primary efforts in this field.

### A. Certificate Transparency Database

Data enrichment through certificate transparency lists can enhance security posture by using our tool, which efficiently crawls the *crt.sh* database to retrieve certificates associated with Hungarian domains. This capability helps construct a comprehensive digital certificate view and enrich domain lists and compromised service catalogs. By querying domains and subdomains, the tool captures valuable metadata, offering insights into domain relationships and certificate validity spans.

Running the tool with different configurations, such as excluding or including expired certificates and choosing between metadata-only or full data, affects performance metrics significantly. Processing ten domains for metadata without expired certificates takes about 47 seconds, while including them extends this to 1-2 minutes. Full data retrieval takes 4-5 minutes for non-expired searches and up to 45 minutes when expired certificates are included. However, inherent latency in the source platform can cause service errors, disrupting download continuity and necessitating retries or additional handling mechanisms.

### B. Dark Web and Community Data Sources

Data enrichment through dark web sources enhances our framework by expanding datasets on data breaches and compromised elements, leveraging insights from breach lists and vulnerability reports. This integration, using intelligence from sources like Shadowserver and APIs such as Shodan and Censys, provides early indicators of undisclosed breaches, improving threat detection and network security by highlighting risks associated with specific domains or IP addresses. Public reputation lists, like those from AdGuard, further aid cybersecurity by categorizing domains by reputation. Integrating these with dark web data and scan results uncovers discrepancies in compromised elements.

However, sourcing data from the dark web and community sources poses challenges due to potential legal and ethical issues, and the uncertainty of data accuracy can lead to false positives. This requires sophisticated data filtering and strict adherence to regulations. Collaborating with cybersecurity experts, such as those at Censys, ensures compliance and effective data utilization, providing structured and legitimate access to these resources.

### C. Vulnerability Databases

Data enrichment using public Common Platform Enumeration (CPE) information enhances IT security and operational efficiency by analyzing technologies on publicly accessible websites. Tools like Wappalyzer perform technology analysis through regex-based rules to identify technologies via HTML source code, HTTP headers, and JavaScript/CSS files, inferring additional technologies like linking WordPress with PHP.

Shodan complements this by scanning open ports and HTTP(S) data to identify server parameters and exposure to vulnerabilities through headers like X-Powered-By and Strict-Transport-Security. This approach provides a comprehensive technology landscape overview, revealing security exposures from outdated or misconfigured components. Integrating CPE information standardizes software and hardware identification, supporting asset management and vulnerability assessments by mapping technologies to known vulnerabilities, facilitating proactive risk management.

## VI. Conclusion and Future Work

Our research targets to further enhance Hungary's cybersecurity framework, benefiting the national Computer Security Incident Response Team (CSIRT) with comprehensive tools and enriched datasets from significant data sources. These resources enable detailed threat analyses, providing insights into compromised devices and services, allowing the CSIRT to identify vulnerabilities and respond swiftly, enhancing situational awareness and operational efficacy. This approach strengthens cyber resilience and establishes a trustworthy national cybersecurity framework, supporting sustainable socioeconomic growth by safeguarding digital infrastructure.

Looking forward, several directions for further improvement and research are evident. Integrating machine learning and artificial intelligence to enhance predictive analysis capabilities can improve threat detection accuracy and responsiveness but also can lead to explainability issues and false positives. Expanding data enrichment processes by incorporating even more diverse threat intelligence sources, including real-time IoT feeds, could serve as a key to building a comprehensive threat detection ecosystem. Additionally, enhancing the scalability and efficiency of detection tools by leveraging advanced cloud computing and distributed techniques remains a critical focus. By pursuing these strategies, we can continue to advance security measures, adapt to evolving threats, and reinforce cybersecurity infrastructure at both national and international levels.

## Acknowledgment

Project no. NKFIH-3568-1/2022 has been implemented with the support provided by the Ministry of Culture and Innovation of Hungary from the National Research, Development and Innovation Fund, financed under the 2022-2.1.1-NL funding scheme. The authors express their gratitude for computational resources provided by the HUN-REN Cloud [18].

## References

[1] A. M. Sllame, T. E. Tomia, and R. M. Rahuma, "A Holistic Approach for Cyber Security Vulnerability Assessment Based on Open Source Tools: Nikto, Acunitx, ZAP, Nessus and Enhanced with AI-Powered Tool ImmuniWeb," in *2024 IEEE 4th International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering (MI-STA)*. Tripoli, Libya: IEEE, May 2024, pp. 68–75. [Online]. Available: https://ieeexplore.ieee.org/document/10599685/

[2] S. Alazmi and D. C. De Leon, "A Systematic Literature Review on the Characteristics and Effectiveness of Web Application Vulnerability Scanners," *IEEE Access*, vol. 10, pp. 33 200–33 219, 2022. [Online]. Available: https://ieeexplore.ieee.org/document/9739725/

[3] A. Nair, A. Anil, A. R. Pallivathuckal, D. Daiju, and J. John, "Vulnerability Scanning and Analysis Tool (VSAT)," in *2023 9th International Conference on Smart Computing and Communications (ICSCC)*. Kochi, Kerala, India: IEEE, Aug. 2023, pp. 338–343. [Online]. Available: https://ieeexplore.ieee.org/document/10335065/

[4] M. S. Pour, D. Watson, and E. Bou-Harb, "Sanitizing the IoT Cyber Security Posture: An Operational CTI Feed Backed up by Internet Measurements," in *2021 51st Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*. Taipei, Taiwan: IEEE, Jun. 2021, pp. 497–506. [Online]. Available: https://ieeexplore.ieee.org/document/9505129/

[5] H. Ecik, "Comparison of Active Vulnerability Scanning vs. Passive Vulnerability Detection," in *2021 International Conference on Information Security and Cryptology (ISCTURKEY)*. Ankara, Turkey: IEEE, Dec. 2021, pp. 87–92. [Online]. Available: https://ieeexplore.ieee.org/document/9654331/

[6] M. Čerget' and J. Hudec, "Cyber-Security Threats Origins and their Analysis," *Acta Polytechnica Hungarica*, vol. 20, no. 9, 2023.

[7] D. Everson and L. Cheng, "A Survey on Network Attack Surface Mapping," *Digital Threats: Research and Practice*, vol. 5, no. 2, pp. 1–25, Jun. 2024. [Online]. Available: https://dl.acm.org/doi/10.1145/3640019

[8] S. Roy, N. Sharmin, J. C. Acosta, C. Kiekintveld, and A. Laszka, "Survey and Taxonomy of Adversarial Reconnaissance Techniques," *ACM Computing Surveys*, vol. 55, no. 6, pp. 1–38, Jul. 2023. [Online]. Available: https://dl.acm.org/doi/10.1145/3538704

[9] J. Mayer, M. Schramm, L. Bechtel, N. Lohmiller, S. Kaniewski, M. Menth, and T. Heer, "I Know Who You Scanned Last Summer: Mapping the Landscape of Internet-Wide Scanners," in *2024 IFIP Networking Conference (IFIP Networking)*. Thessaloniki, Greece: IEEE, Jun. 2024, pp. 222–230. [Online]. Available: https://ieeexplore.ieee.org/document/10619808/

[10] M. Safaei Pour, C. Nader, K. Friday, and E. Bou-Harb, "A Comprehensive Survey of Recent Internet Measurement Techniques for Cyber Security," *Computers & Security*, vol. 128, p. 103123, May 2023. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0167404823000330

[11] H. Griffioen, G. Koursiounis, G. Smaragdakis, and C. Doerr, "Have you SYN me? Characterizing Ten Years of Internet Scanning," in *Proceedings of the 2024 ACM on Internet Measurement Conference*. Madrid Spain: ACM, Nov. 2024, pp. 149–164. [Online]. Available: https://dl.acm.org/doi/10.1145/3646547.3688409

[12] L. Zhao, S. Kobayashi, and K. Fukuda, "Exploring the Discovery Process of Fresh IPv6 Prefixes: An Analysis of Scanning Behavior in Darknet and Honeynet," in *Passive and Active Measurement*, P. Richter, V. Bajpai, and E. Carisimo, Eds. Cham: Springer Nature Switzerland, 2024, vol. 14537, pp. 95–111, series Title: Lecture Notes in Computer Science.

[13] A. A. Alian, B. Sobhy, M. Nasser, and L. Hani, "Backslash map: An Automated Vulnerability Scanner," in *2023 Eleventh International Conference on Intelligent Computing and Information Systems (ICICIS)*. Cairo, Egypt: IEEE, Nov. 2023, pp. 476–482. [Online]. Available: https://ieeexplore.ieee.org/document/10391153/

[14] B. Zhao, S. Ji, W.-H. Lee, C. Lin, H. Weng, J. Wu, P. Zhou, L. Fang, and R. Beyah, "A Large-Scale Empirical Study on the Vulnerability of Deployed IoT Devices," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 3, pp. 1826–1840, May 2022. [Online]. Available: https://ieeexplore.ieee.org/document/9259111/

[15] R. Leszczyna, "Review of cybersecurity assessment methods: Applicability perspective," *Computers & Security*, vol. 108, p. 102376, Sep. 2021. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0167404821002005

[16] A. V. C. Camargo, L. M. Bertholdo, and L. Z. Granville, "Less is More? Exploring the Impact of Scaled-Down Network Telescopes on Security and Research," in *Anais do XLII Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC 2024)*. Brasil: Sociedade Brasileira de Computação, May 2024, pp. 1050–1063. [Online]. Available: https://sol.sbc.org.br/index.php/sbrc/article/view/29854

[17] "OpenSearch." [Online]. Available: https://opensearch.org/

[18] Mihály Héder, Ernő Rigó, Dóra Medgyesi, Róbert Lovas, Szabolcs Tenczer, Ferenc Török, Attila Farkas, Márk Emődi, József Kadlecsik, György Mező, Pintér Ádám, and Péter Kacsuk, "The Past, Present and Future of the ELKH Cloud," *Információs Társadalom (Information Society)*, vol. XXII, no. 2, 2022.