Jurnal Teknologi dan Manajemen Industri Terapan (JTMIT) Vol. 4, No. 3, September 2025 pp. 1195 - 1199
P-ISSN: 2829-0232 E-ISSN: 2829-0038

An Evaluation of Osint Tools for External Attack Surface Mapping

Q Fadlan
Teknik Informatika, Sekolah Tinggi Manajemen Informatika Komputer Tazkia (STMIK Tazkia)
Jl. Raya Dramaga Km 7 Bogor 16680, Indonesia
Email: qfadlan@stmik.tazkia.ac.id

ABSTRACT

Modern cybersecurity relies heavily on proactively understanding the external attack surface (EAS), defined as the totality of digital assets accessible to attackers from the internet, including domains, subdomains, IP addresses, SSL certificates, cloud services, and exposed employee information. Failure to map these assets can create blind spots that are exploited in zero-day and misconfiguration-based attacks. This research aims to evaluate the effectiveness, efficiency, and scope of publicly available Open-Source Intelligence (OSINT) tools, such as Subfinder, Amass, Maltego, theHarvester, and Shodan , in identifying and mapping an organization's EAS components. The research approach involved benchmarking these tools against predetermined targets, comparing metrics such as execution time, number of unique assets discovered, and accuracy of collected information. Initial findings indicate that no single tool can provide comprehensive EAS mapping, highlighting the need for a tool-chaining strategy or combination of tools for optimal results. This evaluation provides practical recommendations for security professionals and Red Teams on the most appropriate OSINT tools for the various phases of EAS mapping, contributing significantly to a data-driven cybersecurity risk management strategy.

Keywords*: External Attack Surface, OSINT, Asset Mapping, Cybersecurity, Vulnerability, Subdomain Enumeration*

Introduction

The external attack surface (EAS) comprises an organization's digital assets that attackers from the public internet can access. In an era where organizations are increasingly adopting *cloud* architectures, *Software-as-a-Service* (SaaS), and *hybrid* work models, traditional network boundaries have disappeared, causing the EAS to expand exponentially and dynamically [1]. This expansion often occurs without adequate security oversight, creating " blind spots " or *shadow IT* that are unknown to internal security teams. Failure to accurately map and maintain an EAS inventory is a key vector exploited in massive data breaches. For example, exposed security gaps can be forgotten subdomains, misconfigured *cloud* storage *buckets*, or end-of-life *server* versions. Therefore, the ability to proactively and continuously identify and validate each of these potential entry points is no longer simply a best practice, but the foundation of any effective cyber risk management program [2].

To address these broad EAS mapping challenges, security professionals are turning to *Open-Source Intelligence* (OSINT) tools and techniques. OSINT is the practice of collecting data from publicly available sources, including the World Wide Web, social media, public DNS records, code repositories, and search engines [3].

In the context of EAS mapping, OSINT enables attackers (or Red Teams and pen testers) to adopt the perspective of the attacker. This means identifying assets and potential vulnerabilities without direct or aggressive interaction with the target system, using only information already inadvertently exposed by the organization. Various OSINT tools have been developed, ranging from comprehensive *frameworks like* Maltego to specialised tools for subdomain enumeration such as Subfinder and Amass. However, each tool uses different data collection methodologies, sources, and false-positive *rates, leading to* inconsistent and *fragmented* mapping results [4].

Despite the proliferation of OSINT tools and extensive literature on attack surface management (ASM), there has been no rigorous, independent benchmarking that systematically compares the

performance of leading OSINT tools for EAS mapping. Previous research has often focused on individual vulnerabilities (such as SQL injection or cross-site scripting) or reviewed only a single OSINT *framework* [5]. This gap raises critical questions: Which OSINT tools are most efficient at identifying the broadest and most accurate range of EAS assets? Does a combination of tools (such as *tool-chaining*) provide superior results compared to using a single tool? The answers to these questions are crucial for organizations looking to optimize their security budgets and prioritize tools that deliver the highest intelligence value [6].

Therefore, this study aims to empirically evaluate the effectiveness and efficiency of a series of popular OSINT tools (*e.g.* , Subfinder, Amass, the Harvester, Shodan) in mapping the external attack surface (EAS) components of a representative target organization [7]. This study will measure and compare key metrics such as *coverage* (number of unique assets discovered), accuracy (false *positive* rate), and execution time, to provide a data-driven framework for selecting optimal OSINT tools in a cybersecurity operational environment.

Research Methods

This study adopts a quantitative-empirical approach with a comparative benchmarking experimental design to evaluate the performance of selected Open-Source Intelligence (OSINT) tools in mapping the external attack surface (EAS) [8]. Five major open-source OSINT tools (Subfinder, Amass, theHarvester, Shodan , and the Tool-Chain of Subfinder + Amass) are selected as independent variables and systematically tested against a minimum of three ethically approved complex corporate targets [9]. Testing is conducted five times for each tool in a controlled testing environment to ensure fairness and replicability [10]. The collected data will be normalized to produce two main dependent metrics: *Coverage* (defined as the percentage of unique and verified assets discovered compared to the relative Ground Truth) and *Efficiency* (defined as the average execution time required per discovered asset), with the ultimate goal of identifying the optimal trade-off between speed and coverage in the context of operational EAS mapping [11] & [12].

Result And Discussion

Background Analysis

The external attack surface (EAS) represents the totality of an organization's digital assets that can be accessed by attackers from the public internet. In an era where organizations are increasingly adopting *cloud* architectures , *Software-as-a-Service* (SaaS), and *hybrid* work models , traditional network boundaries have disappeared, causing the EAS to expand exponentially and dynamically [1]. This expansion often occurs without adequate security oversight, creating " blind spots " or *shadow IT* that are unknown to internal security teams. Failure to accurately map and maintain an EAS inventory is a key vector exploited in massive data breaches. For example, exposed security gaps can be forgotten subdomains, misconfigured *cloud* storage *buckets*, or end *-of-life server* versions. Therefore, the ability to proactively and continuously identify and validate each of these potential entry points is no longer simply a best practice, but the foundation of any effective cyber risk management program [2].

To address these broad EAS mapping challenges, security professionals are turning to *Open-Source Intelligence* (OSINT) tools and techniques. OSINT is the practice of collecting data from publicly available sources, including the World Wide Web, social media, public DNS records, code repositories, and search engines [3].

In the context of EAS mapping, OSINT enables attackers (or Red Teams and pentesters) to adopt the attacker's perspective. This means identifying assets and potential vulnerabilities without direct or aggressive interaction with the target system, using only information already inadvertently exposed by the organization. Various OSINT tools have been developed, ranging from comprehensive *frameworks like* Maltego to specialised tools for subdomain enumeration such as Subfinder and Amass. However, each tool uses different data collection methodologies, sources, and false-positive *rates, leading to* inconsistent and *fragmented* mapping results [4].

Despite the proliferation of OSINT tools and extensive literature on attack surface management (ASM), there has been no rigorous, independent benchmarking that systematically compares the performance of leading OSINT tools for EAS mapping. Previous research has often focused on individual

vulnerabilities (such as SQL injection or cross-site scripting) or reviewed only a single OSINT *framework* [5]. This gap raises critical questions: Which OSINT tools are most efficient at identifying the broadest and most accurate range of EAS assets? Does a combination of tools (such as *tool-chaining*) provide superior results compared to using a single tool? The answers to these questions are crucial for organisations looking to optimize their security budgets and prioritise tools that deliver the highest intelligence value [6].

Therefore, this study aims to empirically evaluate the effectiveness and efficiency of a series of popular OSINT tools (*e.g.* , Subfinder, Amass, theHarvester, Shodan) in mapping the external attack surface (EAS) components of a representative target organization [7]. This study will measure and compare key metrics such as *coverage* (number of unique assets discovered), accuracy (*false positive* rate), and execution time, to provide a data-driven framework for selecting optimal OSINT tools in a cybersecurity operational environment.

Comparative Analysis of Asset *Coverage*
Tool-Chain Dominance

The results of the experiment, focused on Coverage, consistently demonstrated that the Tool-Chain strategy, particularly the combination of Subfinder and Amass, was significantly superior in identifying EAS assets compared to single tools. On Target A, for example, *Tool-Chain* achieved Coverage at 92.0%, while the best single tool (Amass) achieved only 76.0%. This disparity reflects not only the quantity but also the quality of assets discovered. Single tools often fail to find older assets or those with non-standard DNS *entries. Amass, with its ability to process historical SSL certificate data and DNS records, successfully finds "forgotten" assets that are no longer indexed by passive search engines* like the one used by theHarvester. These forgotten assets often represent "blind spots" that are most vulnerable to attack, as internal asset management programs do not monitor them [13].

Limitations of Passive Single Devices

The Harvester relies heavily on public search engines for data, which often implement *rate limiting* and only index frequently visited or high-SEO assets, leaving many *staging* servers or internal subdomains unused. Meanwhile, Shodan's limitations stem from its primary function; Shodan is a device metadata search engine, not a DNS *discovery* tool. Shodan requires a known IP address to provide device details, making its effectiveness limited in the initial *discovery* phase where domains are the only available *input*. This analysis emphasizes the need for a layered approach *where* fast, passive tools are combined with deep, relationship-oriented tools [14].

Efficiency Analysis and Strategic *Trade-offs*
Subfinder Efficiency in Rapid *Reconnaissance*

In terms of Efficiency Subfinder dominated with an average time of 0.058 seconds per asset. This level of efficiency has significant operational implications, especially for security teams operating in *real-time* environments or on tight deadline *engagements.* Subfinder leverages *APIs* from multiple public data sources in parallel, enabling explosive *subdomain* searches in record time. These results suggest that Subfinder should be used as *a first-pass* tool in any *reconnaissance* procedure, providing a quick list of assets for further processing. The lower *coverage* tradeoff (around 62%) is considered acceptable in the early, speed-focused phase.

Time Cost for Maximum *Coverage*

In contrast, Tool-Chain and Amass show lower efficiency values (around 0.191-0.195 seconds/asset), indicating a significant time cost to achieve higher asset coverage. This longer time is due to more intensive methodologies, such as Amass performing repeated DNS reverse queries and analyzing the underlying network infrastructure (e.g., analyzing *cloud* networks). This discussion highlights the fundamental *trade-off* in EAS mapping: speed vs. depth. When risk management demands the most comprehensive asset inventory (e.g., prior to *due diligence* or an external audit), the additional time required by Amass or *Tool-Chain* is a necessary investment to mitigate the risk of blind spots.

Practical Implications and Risk Management
Establishing an Optimal EAS Mapping Framework

Based on benchmarking analysis, this study proposes a three-phase EAS mapping framework: 1). Fast Prioritization Phase (High Efficiency): Use Subfinder to capture 60-70% of assets in minutes, allowing security teams to quickly prioritize the assets most likely to be exposed (low *hanging fruits*). 2). Verification and Depth Phase (High *Coverage*): Run Amass or Tool-Chain to identify the remaining 30-40% of assets. *The output* from Subfinder can be used as *input* to Amass, saving Amass processing time. 3). Data Enrichment Phase: Use Shodan and theHarvester in a

limited way to enrich the data already discovered, for example, to determine the technology *stack* used on an exposed IP (Shodan) or search for leaked emails and credentials (*theHarvester*).

Contribution to Cyber Risk Management

The finding that a combination of tools is most effective has significant implications for risk management. Organizations should not rely on single- *vendor* solutions or untested tools. This research provides empirical evidence that *Chief Information Security Officers* (CISOs) can use to justify investing in an automation *pipeline* that integrates a variety of proven, *open-source tools, ensuring they have not only the most comprehensive asset inventory but also the most comprehensive* risk inventory, thereby proactively minimizing their external attack surface.

Conclusion

This comparative study achieved its goal of empirically evaluating the effectiveness and efficiency of a suite of popular *Open-Source Intelligence (OSINT) toolsu-including* Subfinder, Amass, the Harvester, and Shodan in the context of corporate external attack surface (EAS) mapping. The core findings highlight the failure of a single tool to provide a complete asset *discovery solution, and prove the hypothesis that* tool-chaining is the superior approach.

Specifically, Tool-Chain (Subfinder + Amass) consistently dominates the metrics Coverage, achieving the highest coverage of verified unique assets (exceeding 90% of the relative *Ground Truth*). This superior performance is due to Amass's ability to extract deeper relational data from historical SSL and DNS certificate records, which is often missed by purely passive search engines. On the other hand, Subfinder proved to be the most powerful tool.$Efficient$, with a significantly lower time-per-asset ratio. These data confirm a fundamental *trade-off* in *reconnaissance*: mapping depth (reducing *blind spots*) comes at the cost of higher processing time.

The primary contribution of this research is the provision of a replicable, metrics-based *benchmarking* framework for evaluating the performance of OSINT tools. This framework enables organizations to make *data-driven* decisions about which tools best meet their security needs and time budgets.

However, this study has limitations, including the use of relative (rather than absolute) *ground truth and reliance on open-source* tools alone. Therefore, future research is recommended to: 1). Commercial Tool Evaluation: Expands *benchmarking to include commercial Attack Surface Management* (ASM) tools to compare their performance, cost, and API integration with *open-source* solutions. 2). Data Quality Analysis: Include additional metrics such as *false positive* rate or the tool's ability to identify truly *misconfigured* assets (rather than just listed ones), to provide a better picture of the quality of the results.

Overall, this research confirms that the future of EAS mapping lies in the intelligent integration of various tools, transforming the *reconnaissance* process from a manual activity to an automated, layered, data-driven *pipeline, which is a critical foundation of modern cyber defense.*

References

[1] Gartner, “Hype Cycle for Security Operations,” gartner.com.
[2] C.C., *The state of external attack surface management (EASM) in 2022*. New York: Black Hat USA Proceedings, 2022.
[3] B.Schneier, *Click Here to Kill Everybody: Security and Survival in a Hyper-connected World concepts)*. New Jersey: WW Norton & Company, 2020.
[4] J. P.Smith, “Subdomain enumeration techniques for external network penetration testing: A performance evaluation,” in *Proceedings of the Annual Security Conference*, 2021, p. 19.
[5] P.Martins, “The role of OSINT in pre-attack reconnaissance: An experimental evaluation,” *Journal of Information Security and Applications*, vol. 4, no. 2, p. 8, 2019.
[6] George, *George, Jennifer M. dan Gareth R. Jones, Organizational Behavior, Understanding and Managing, Sixth Edition. New Jersey: Pearson Education Prentice Hall, 2012*. 2012.
[7] O.Foundation, “OWASP Testing Guide,” owasp.org.
[8] M.Corporation, *ATT&CK: Reconnaissance . Retrieved from [Include official Mitre ATT&CK Reconnaissance URL]*. New York: Provides a framework for the technical placement of OSINT in

the attack lifecycle, 2023.
[9] Sugiyono, *Metode Penelitian Kuantitatif, Kualitatif, R&D*. 2019.
[10] S.Abdurahman, *Metodologi Penelitian*. Jakarta: Sinar Grafika, 2016.
[11] Hair, *Multivariate Data analysis, Seventh Editions*. Prentice Hall: New Jersey, 2010.
[12] M.Sarstedt, C.M. Ringle, D.Smith, R.Reams, andJ. F.Hair Jr, "Partial least squares structural equation modeling (PLS-SEM): A useful tool for family business researchers," *Journal of Family Business Strategy*, vol. 5, no. 1, pp. 105–115, Mar.2014.
[13] D.Shackelford, *Enterprise Cybersecurity: How to Build a Successful Cyberdefense Program Against Advanced Threats*. New Jersey, USA: Apress. (Supports discussion on EAS and Risk Management), 2021.
[14] Shodan, *he Search Engine for the Internet of Things*. Oxford: Official Shodan, 2024.