RANCANG BANGUN *TOOLS ENUMERATION* CIPHERION DALAM ANALISIS KEAMANAN *WEBSITE* NINJA SHL DENGAN TEKNIK *PENETRATION TESTING*

SKRIPSI

Diajukan untuk memenuhi Sebagian dari persyaratan dalam memperoleh gelar Sarjana Teknik pada Program Studi Sistem Telekomunikasi

Oleh:
God Friend Hutagalung
2103445

PROGRAM STUDI SISTEM TELEKOMUNIKASI
KAMPUS UPI DI PURWAKARTA
UNIVERSITAS PENDIDIKAN INDONESIA
2025

LEMBAR HAK CIPTA

RANCANG BANGUN TOOLS ENUMERATION CIPHERION DALAM ANALISIS KEAMANAN WEBSITE NINJA SHL DENGAN TEKNIK PENETRATION TESTING

Oleh

God Friend Hutagalung

Sebuah skripsi yang diajukan untuk memenuhi salah satu syarat memperoleh gelar Sarjana Teknik pada Program Studi Sistem Telekomunikasi

Universitas Pendidikan Indonesia

Juli 2025

LEMBAR PENGESAHAN

RANCANG BANGUN *TOOLS ENUMERATION* CIPHERION DALAM ANALISIS KEAMANAN *WEBSITE* NINJA SHL DENGAN TEKNIK *PENETRATION TESTING*

God Friend Hutalung

2103445

Disetujui dan Disahkan Oleh Pembimbing:

Pembimbing I,

Galura Muhammad Suranegara, S.Pd., M.T.

NIP. 920190219920111101

Pembimbing II

Ahmad Fauzi, S.Si., M.T.

NIP. 920171219820915101

Mengetahui,

Ketua Program Studi

Sistem Telekomunikasi

Galura Muhammad Suranegara, S.Pd., M.T.

NIP. 920190219920111101

ABSTRAK

Keamanan informasi merupakan salah satu aspek yang sangat krusial dalam dunia digital yang semakin berkembang pesat. Seiring meningkatnya ketergantungan pada teknologi informasi, ancaman terhadap sistem dan data menjadi semakin kompleks dan beragam. Dalam konteks keamanan *web*, proses enumerasi sebagai bagian dari *penetration testing* berperan penting dalam mengidentifikasi *subdomain*, direktori tersembunyi, layanan berjalan, dan konfigurasi sistem yang dapat diakses publik, yang kemudian dapat menjadi celah potensial bagi serangan siber. Namun, metode manual dalam enumerasi kerap tidak efisien dan rentan terhadap kesalahan, sehingga diperlukan pendekatan otomatis yang lebih akurat dan cepat. Penelitian ini bertujuan untuk mengembangkan sebuah alat enumerasi otomatis bernama Cipherion, yang hanya berfokus pada aspek information gathering dan tidak melibatkan eksploitasi aktif terhadap sistem target. Cipherion dikembangkan menggunakan bahasa pemrograman *Python* dan diuji pada sistem operasi *Linux* dan *Windows*, dengan fitur identifikasi aset yang relevan seperti *subdomain*, direktori tersembunyi, layanan terbuka, dan konfigurasi publik berbasis protokol umum seperti *HTTP*, *HTTPS*, dan *FTP*. Pengujian dilakukan secara terkontrol pada *website* Ninja Shl sebagai simulasi target, tanpa melibatkan sistem produksi guna menjaga etika dan keamanan.

Kata Kunci: *Penetration Testing, Enumeration, Automated Tool, Keamanan Informasi, Cipherion.*

ABSTRACT

Information security is a critical aspect in today's rapidly evolving digital landscape. As dependence on information technology increases, threats to systems and data have become more complex and diverse. In the context of web security, enumeration plays a pivotal role in penetration testing by identifying subdomains, hidden directories, active services, and publicly accessible system configurations, all of which may serve as potential entry points for cyberattacks. However, manual enumeration methods tend to be inefficient and prone to human error, necessitating an automated approach that enhances both accuracy and speed. This research aims to develop an automated enumeration tool called Cipherion, designed specifically for the information gathering phase without engaging in active exploitation of the target system. Cipherion is developed using Python and tested on both Linux and Windows operating systems, featuring capabilities to identify assets such as subdomains, hidden directories, open services, and publicly accessible configurations using standard web protocols like HTTP, HTTPS, and FTP. The testing process is conducted in a controlled environment targeting the Ninja Shl website, ensuring ethical and secure analysis without involving live production systems.

Keywords: Penetration Testing, Enumeration, Automated Tool, Information Security, Cipherion..

.

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR PUSTAKA

Abdollahi, A. (2025). *A Beginner's Guide To Web Application Penetration Testing*.

Alhamed, M., & Rahman, M. M. H. (2023). A Systematic Literature Review on Penetration Testing in Networks: Future Research Directions. *Applied Sciences*, *13*(12), 6986. https://doi.org/10.3390/app13126986

Bakaletz, R. (2022). *A Machine Learning Approach for Reconnaissance Detection to Enhance Network Security*.

Barman, F., Alkaabi, N., Almenhali, H., Alshedi, M., & Ikuesan, R. (2023). A Methodical Framework for Conducting Reconnaissance and Enumeration in the Ethical Hacking Lifecycle. *European Conference on Cyber Warfare and Security*, *22*(1), 54–64. https://doi.org/10.34190/eccws.22.1.1438

Bhadola, S. (2022). *Network Enumeration Best Practices*. *9*(2).

Castagnaro, A., Conti, M., & Pajola, L. (2024). *Offensive AI: Enhancing Directory Brute-forcing Attack with the Use of Language Models* (No. arXiv:2404.14138). arXiv. https://doi.org/10.48550/arXiv.2404.14138

Chu, G. (2021). *Automation of Penetration Testing*.

Cochran, K. A. (2024). *Cybersecurity Essentials: Practical Tools for Today's Digital Defenders*. Apress. https://doi.org/10.1007/979-8-8688-0432-8

Fadhli, M. (2024). *Comprehensive Analysis of Penetration Testing Frameworks and Tools: Trends, Challenges, and Opportunities*. *4*.

Jain, N. (2025). *Application of deep reinforcement learning for real-time demand response in smart grids. International Research Journal of Modernization in Engineering Technology and Science,*

Jabr, I., Salman, Y., Shqair, M., & Hawash, A. (2025). Penetration Testing and Attack Automation Simulation: Deep Reinforcement Learning Approach. *An-Najah University Journal for Research - A (Natural Sciences)*, *39*(1), 7–14. https://doi.org/10.35552/anujr.a.39.1.2231

Jaspher Kathrine, G. (2020). COMPARATIVE ANALYSIS OF SUBDOMAIN ENUMERATION TOOLS AND STATIC CODE ANALYSIS. *JOURNAL OF MECHANICS OF CONTINUA AND MATHEMATICAL SCIENCES*, *15*(6). https://doi.org/10.26782/jmcms.2020.06.00013

Kak, A. (2020). *Lecture 23: Port and Vulnerability Scanning, Packet Sniffing, Intrusion Detection, and Penetration Testing*.

Kumar Csa, A. (2025). Ethical Hacking and Penetration Testing. *International Scientific Journal of Engineering and Management*, *04*(04), 1–9. https://doi.org/10.55041/isjem02790

Kumar, R., Rachamalla, D., & Vatti, P. R. (2025). *Zero-Trust Architectures: Decoding the Future of Enterprise Cyber Resilience*.

Lim, P.-C., Chieng, G.-W. A., Ling, H.-C., & Jali, N. (2024). OWASP A03 Injection Vulnerability in Web Application Development. *Journal of Advanced Research in Applied Sciences and Engineering Technology*, 107–116. https://doi.org/10.37934/araset.57.1.107116

Liu, D., Wang, W., & Xu, P. (2024). *D-DSE: Distinct Dynamic Searchable Encryption Resisting Volume Leakage in Encrypted Databases*.

Mansoori, B. (2022). *WordPress Penetration Testing using WPScan & Metasploit*.

Malasri S (2025) *Multitools Based on Ethical Hacking*. *8*(3).

Osazuwa, O. M. C. (2023). *Confidentiality, Integrity, and Availability in Network Systems: A Review of Related Literature*. *8*(12).

Rifqi Azis & Setiadi Yazid. (2022). PENGUJIAN KERENTANAN WEBSITE WORDPRESS DENGAN MENGGUNAKAN PENETRATION TESTING UNTUK MENGHASILKAN WEBSITE YANG AMAN. *Jurnal RESTIKOM : Riset Teknik Informatika dan Komputer*, *3*(3), 93–105. https://doi.org/10.52005/restikom.v3i3.87

Samonas, S., & Coss, D. (2024). *THE CIA STRIKES BACK: REDEFINING CONFIDENTIALITY, INTEGRITY AND AVAILABILITY IN SECURITY*.

Silka Gonzalez (2020).*The Complete Guide to Penetration Testing*.

Zhang, W., Xing, J., & Li, X. (2025). *Penetration Testing for System Security: Methods and Practical Approaches* (No. arXiv:2505.19174). arXiv. https://doi.org/10.48550/arXiv.2505.19174