BAB I
PENDAHULUAN

1.1 Latar Belakang

Keamanan informasi merupakan aspek fundamental dalam menjaga integritas, kerahasiaan, dan ketersediaan sistem digital yang semakin kompleks. Seiring meningkatnya ketergantungan terhadap teknologi informasi, ancaman terhadap sistem dan data menjadi semakin beragam dan canggih. Serangan *cyber* yang menyasar aplikasi web sering kali memanfaatkan celah keamanan yang tidak terdeteksi, sehingga diperlukan pendekatan sistematis untuk mengidentifikasi dan mengevaluasi potensi kerentanan. Salah satu metode yang digunakan adalah *penetration testing*.Menurut (Cochran, 2024), *penetration testing* merupakan strategi penting dalam mengidentifikasi kelemahan sistem sebelum dimanfaatkan oleh pihak yang tidak bertanggung jawab.

Dalam tahapan awal *penetration testing*, proses *enumeration* menjadi krusial karena berfungsi untuk mengumpulkan informasi sebanyak mungkin mengenai target, seperti *subdomain*, direktori tersembunyi, layanan aktif, dan konfigurasi sistem yang dapat diakses publik. Oleh karena itu, penelitian ini mengembangkan Cipherion, sebuah *tools* enumerasi otomatis berbasis *Python* yang menggabungkan berbagai teknik seperti *subdomain discovery*, *port scanning*, *directory brute-forcing*, dan *service detection*. Cipherion dirancang dengan pendekatan *command-line interface (CLI)* agar dapat digunakan secara fleksibel dalam berbagai skenario pengujian keamanan web.Menurut (Chu, 2021) penggunaan *CLI* dalam pengembangan *tools* keamanan memberikan efisiensi dan kontrol yang lebih tinggi bagi pengguna teknis dalam lingkungan pengujian. .

Pengujian dilakukan dalam lingkungan simulasi menggunakan website Ninja SHL sebagai target, dengan pendekatan *black-box testing* yang mengacu pada standar *OWASP Testing Guide*. *Tools* ini tidak melakukan eksploitasi aktif, melainkan hanya berfokus pada tahap *information gathering* untuk mendukung proses audit keamanan secara etis dan legal. Hasil pengujian menunjukkan bahwa Cipherion mampu mengotomatisasi proses enumerasi secara efisien dan

menghasilkan output yang relevan untuk tahap analisis kerentanan lebih lanjut (Barman dkk, 2023).

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dipaparkan di atas, maka dapat ditentukan rumusan masalah dalam penelitian ini adalah:

1. Bagaimana rancang bangun *tools* enumerasi otomatis Cipherion untuk mengidentifikasi aset digital pada *website* Ninja SHL?
2. Bagaimana analisis hasil pengujian fungsionalitas *tools* Cipherion Ninja SHL dalam proses pengujian keamanan sistem informasi menggunakan metode *Black-box testing*?
3. Bagaimana analisis hasil pengujian usabilitas *tools* Cipherion Ninja SHL dalam mendukung proses penetration testing menggunakan instrumen *System Usability Scale (SUS)*?

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah yang sudah dijelaskan, terdapat beberapa ruang lingkup sebagai berikut:

1. Merancang dan membangun *tools* enumerasi otomatis bernama Cipherion yang mampu mengidentifikasi berbagai aset digital seperti *subdomain*, direktori tersembunyi, layanan terbuka, serta konfigurasi publik dalam konteks analisis keamanan *website* Ninja SHL.
2. Melakukan analisis hasil pengujian fungsionalitas *tools* Cipherion Ninja SHL dalam proses pengujian keamanan sistem informasi menggunakan instrumen *Black-box Testing*.
3. Melakukan analisis hasil pengujian usabilitas *tools* Cipherion Ninja SHL dalam mendukung proses *penetration testing* menggunakan instrumen *System Usability Scale (SUS).*

1.4 Ruang Lingkup Penelitian

Berdasarkan rumusan masalah yang sudah dijelaskan, terdapat beberapa batasan masalah sebagai berikut:

1. Fokus pengembangan *tools* enumerasi Cipherion yang dirancang untuk melakukan identifikasi aset digital meliputi *subdomain*, direktori tersembunyi, layanan terbuka, dan konfigurasi yang dapat diakses publik
2. Evaluasi performa Cipherion dilakukan berdasarkan hasil pengujian aktual yang mencakup akurasi temuan, jumlah aset yang terdeteksi, dan eksekusi modul secara menyeluruh.
3. Penelitian tidak mencakup analisis eksploitasi kerentanan, *bypass* otentikasi, atau tahap *exploit*, dan sepenuhnya berfokus *pada information gathering* untuk mendukung tahap awal *penetration testing*.

1.5 Manfaat Penelitian

1.5.1 Secara Teoritis

Penelitian ini memberikan kontribusi terhadap pengembangan metode enumerasi otomatis dalam analisis keamanan aplikasi *web*, khususnya pada tahap *reconnaissance* dan *scanning* dalam *penetration testing*. Integrasi berbagai teknik seperti *subdomain discovery*, *port scanning*, dan *directory brute-forcing* melalui *tools* Cipherion memperkuat pendekatan modular dalam audit keamanan berbasis *black-box*. Hasil penelitian ini dapat menjadi referensi bagi pengembangan *tools* keamanan siber yang lebih terstruktur dan *extensible*, serta mendukung studi lebih lanjut dalam bidang *ethical hacking*, *web security analysis*, dan otomasi proses pengujian kerentanan sistem.

1.5.2 Secara Praktis

Secara praktis, manfaat penulisan ini adalah sebagai berikut:

1. Bagi penulis, penelitian ini menjadi pengalaman langsung dalam merancang dan mengintegrasikan beragam teknik enumerasi seperti *subdomain discovery*, *port scanning*, dan *directory brute-forcing* ke dalam *tools* keamanan berbasis *Python*, serta menerapkannya dalam simulasi *penetration testing* yang sesuai dengan standar *OWASP*.

2. Bagi masyarakat, penelitian ini diharapkan mendukung peningkatan kesadaran dan pemahaman tentang proses pengujian keamanan aplikasi *web*, khususnya dalam hal identifikasi aset digital yang rentan, sehingga membantu mencegah risiko kebocoran data dan serangan *cyber*.
3. Bagi universitas, hasil penelitian ini dapat menjadi referensi praktis dalam bidang *ethical hacking* dan otomasi *penetration testing*, serta mendorong pengembangan *tools* keamanan *cyber* yang bersifat *open-source* dan relevan untuk kebutuhan akademik maupun profesional.