

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Sebagai seseorang yang ahli dibidang kewanan informasi (pentester) atau bug hunter, sebagian besar waktu yang mereka gunakan adalah melakukan pengumpulan informasi sebanyak mungkin mengenai target (information gathering/reconnaissance). Pentester dan bug hunter harus melakukan pengintaian ekstensif untuk menemukan aset menarik seperti server, teknologi dan aplikasi web dari sebuah domain atau subdomain. Mencari dan mengumpulkan subdomain dari domain utama merupakan bagian terpenting dari fase reconnaissance dalam kegiatan penilaian keamanan informasi, terutama pada kegiatan black-box penetration testing dan bug hunting. Pengumpulan informasi tersebut dapat dijadikan sebagai target dalam pengujian untuk mencari kemungkinan bahwa salah satu subdomain memiliki kaitan dengan domain utama dan menemukan aplikasi tersembunyi yang berjalan di subdomain, sehingga dapat meningkatkan peluang dalam menemukan kerentanan.

Dalam melakukan pengumpulan informasi dapat dibagi menjadi dua, yaitu active reconnaissance dan passive reconnaissance. Active Reconnaissance adalah pengumpulan data dengan cara bertatap muka langsung atau berhubungan langsung dengan target/sasaran, sedangkan passive reconnaissance adalah menggunakan media informasi yang sudah

tersedia seperti berita, internet, dan sebagainya [1]. Pada proses ini dapat dilakukan secara manual dan otomatis, penulis menggabungkan proses tersebut menjadi semi-otomatis, sehingga kegiatan yang dilakukan secara berulang saat proses pengumpulan informasi menjadi lebih efektif dan efisien.

1.2 Rumusan Masalah dan Hipotesis (hipotesis opsional)

Berdasarkan latar belakang diatas, dapat dirumuskan sebuah perumusan masalah yaitu:

Bagaimana cara mempermudah kegiatan dalam pengumpulan informasi secara efektif, efisien dan otomatis dalam kegiatan penilaian keamanan informasi, terutama pada kegiatan black-box penetration testing dan bug hunting?

1. Bagaimana metode yang digunakan dalam pengumpulan informasi sehingga bisa lebih efisien dan efektif?
2. Apa saja sumber daya atau situs pihak ketiga yang akan digunakan dalam melakukan pengumpulan informasi?

1.3 Batasan Masalah

Berdasarkan masalah diatas, maka batasan masalah dari laporan ini adalah

- a. Membahas pembuatan alat yang digunakan untuk mengumpulkan informasi sebanyak mungkin terkait target tertentu secara efektif, efisien dan otomatis
- b. Melengkapi tools yang diperlukan pentester yang mengikuti kaidah The

National Institute of Standards and Technology (NIST) dan/atau Information Systems Security Assessment Framework (ISSAF).

- c. Alat pengumpulan informasi otomatis yang dibuat hanya tersedia di platform linux dan window dengan ketentuan menggunakan Subsistem Windows untuk Linux (WSL)
- d. Melakukan komparasi terhadap alat pengumpulan informasi yang telah ada di projek open source dan komersil
- e. Membahas langkah langkah dan konsep bagaimana alat ini bekerja disaat melakukan pengumpulan informasi secara otomatis efisien dan efektif.

1.4 Tujuan Penelitian

Tujuan yang ingin diraih dalam penelitian ini adalah:

- a. Membuat aplikasi untuk mendukung tahapan pengumpulan informasi (reconnaissance) yang mana memudahkan peneliti, analis keamanan siber, penetration tester dan bug hunter.
- b. Melengkapi tools yang diperlukan pentester yang mengikuti kaidah The National Institute of Standards and Technology (NIST) dan/atau Information Systems Security Assessment Framework (ISSAF).
- c. Memperkenalkan Sudomy sebagai salah satu tools yang bisa digunakan dalam pengumpulan subdomain dan analisa secara otomatis terhadap informasi yang didapatkan.

1.5 Sistematika Penulisan

Berikut merupakan rincian dari sistematika penulisan laporan sebagai berikut:

BAB I PENDAHULUAN

Bab ini berisi mengenai uraian latar belakang, perumusan masalah, batasan masalah, maksud dan tujuan, manfaat penelitian dan metode penelitian.

BAB II LANDASAN TEORI

Menguraikan teori – teori yang relevan yang mendasari pembahasan pemecah masalah yang berhubungan guna mendukung dalam membuat tugas akhir ini.

BAB III METODOLOGI PENELITIAN

Bab metodologi penelitian ini menjelaskan tentang pengertian dari metode dan alat yang digunakan untuk mengembangkan suatu sistem.

BAB IV HASIL DAN PEMBAHASAN

Membahas tentang implementasi dan hasil dari sistem yang dibangun, serta pelaksanaan uji coba dan evaluasi dari hasil uji coba.

BAB V PENUTUP

Berisi bahasan terkait kesimpulan dan saran mengenai tugas