BAB I PENDAHULUAN

I.1 Latar Belakang

Seiring dengan perkembangan teknologi komputer, metodologi peretasan turut berkembang. Berdasarkan data dari Badan Siber dan Sandi Negara (BSSN, 2022), total anomali lalu lintas internet di Indonesia mencapai 976 juta serangan. Meski jumlah tersebut menurun 40% dari tahun 2021 dengan 1,6 miliar serangan, jumlah tersebut masih lebih tinggi apabila dibandingkan dengan tahun 2019 dengan 290 juta serangan, dan tahun 2020 dengan temuan 495 juta serangan.

Berdasarkan Pasal 15 ayat (1) UU No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, pemilik sistem harus menyelenggarakan Sistem Elektronik secara andal dan aman serta bertanggung jawab atas sistem tersebut. Pemilik sistem elektronik harus bertanggungjawab terhadap kerahasiaan, integritas, dan ketersediaan (*Confidentiality, Integrity, Availability)* dari operasi dan data penggunanya.

Sedangkan berdasarkan Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik Pasal 24 ayat (1), (2), (3), pemilik sistem elektronik tidak hanya harus menjalankan prosedur pengamanan sistem elektronik, pemilik sistem juga harus menyediakan sistem pencegahan dan penanggulangan terhadap ancaman dan serangan, serta melaporkan ke pihak yang berwajib apabila terjadi kegagalan atau gangguan sistem yang serius akibat terjadinya serangan dari pihak luar. Oleh karena itu, kebocoran data yang terjadi pada sistem harus ditanggapi dengan segera.

Tidak ada sistem yang seratus persen aman dari penyerangan. Berdasarkan saran dari Badan Siber dan Sandi Negara (BSSN), pengumpulan, dokumentasi, dan pencatatan informasi kebocoran data perlu dilakukan dalam 24 jam pertama sejak insiden terjadi serta bekerja sama dengan tim hukum. Meski begitu, banyak tantangan untuk aktivitas forensik digital yang dapat menghambat jalannya penyelidikan, seperti kehilangan, kerusakan, atau modifikasi dari barang bukti digital, penyembunyian data di barang bukti, serta kurangnya kerja sama dengan badan hukum atau kurangnya pemahaman hukum mengenai keamanan sistem elektronik di Indonesia. Oleh karena itu, *framework* yang dapat digunakan untuk menghubungkan tim teknis dan legal dapat dimanfaatkan untuk mempercepat tanggapan.

Tugas Akhir ini dilakukan dengan tujuan memberikan simulasi penggunaan *framework.* Simulasi yang akan dilakukan adalah penggunaan *framework* dalam melakukan pengujian dan

analisis forensik digital, serta memberikan rekomendasi perangkat lunak forensik digital yang dapat digunakan dalam analisis forensik digital menggunakan *framework*.

Pada Tugas Akhir ini, dilakukan serangan terhadap sistem operasi rentan berbasis Linux dengan mengikuti *walkthrough* untuk kemudian dilakukan forensik digital terhadap sistem operasi tersebut. Hasil dari serangan dan forensik digital akan dianalisis, dan dibandingkan tiga perangkat lunak forensik yang digunakan pada forensik digital ini. Selain itu, dilakukan perbandingan hasil temuan barang bukti digital dengan serangan yang dilakukan untuk mendapatkan informasi prioritas barang bukti digital untuk dianalisis.

I.2 Rumusan Masalah

1. Bagaimana cara untuk melakukan forensik digital pada perangkat berdasarkan *framework*?
2. Apa perbedaan hasil antara program forensik digital dan log sistem yang digunakan dalam pengujian forensik ini?

I.3 Tujuan

1. Membandingkan perbedaan hasil antara program forensic digital dalam kemampuannya untuk melakukan forensik sistem.
2. Membandingkan perbedaan hasil antara log sistem yang digunakan dalam pengujian forensik untuk mendapatkan log yang diprioritaskan untuk diperiksa.

I.4 Manfaat

Dengan dibuatnya Tugas Akhir ini, diharapkan dapat memberikan manfaat:

1. Dapat memberikan rekomendasi perangkat lunak forensik digital.
2. Dapat memberikan rekomendasi log sistem yang diprioritaskan untuk dianalisis

I.5 Batasan Masalah

1. Eksperimen ini hanya dibatasi pada sisi sistem. Tugas Akhir ini tidak membahas bagian aplikasi dan tiap kerentanannya.
2. Tugas Akhir ini hanya dilakukan pada sisi tim forensik.
3. Tugas Akhir ini dilakukan sebagai simulasi. Tugas Akhir ini tidak melakukan pengujian pada jaringan fisik.

4. Simulasi serangan pada Tugas Akhir ini dilakukan berdasarkan *walkthrough* yang tersedia di internet, berjudul Typhoon: 1.02 Vulnhub Walkthrough - Yucel Can Kircaali (yckircaali.com).
5. Tugas Akhir ini hanya melakukan forensik pada *vulnerable machine.* Tugas Akhir ini tidak membahas *data recovery* pada mesin virtual ini.

I.6 Sistematika Penulisan

Sistematika penulisan terbagi menjadi beberapa bab, dapat dijabarkan sebagai berikut :

1. BAB I – Pendahuluan, bab ini berisi penjelasan latar belakang, rumusan masalah, tujuan penelitian, batasan penelitian dan manfaat penelitian tentang desain dan analisis sistem forensik digital pada *server* Typhoon dengan *framework* FORZA, pada bab ini juga terdapat sistematika penulisan.
2. BAB II – Landasan Teori, bab ini berisi penjelasan kajian literatur pendukung untuk penelitian ini.
3. BAB III – Metodologi Penelitian, bab ini berisi penjelasan tahapan yang dilakukan untuk mendapatkan hasil dari penelitian dengan model konseptual dan sistematika penelitian.
4. BAB IV – Perancangan Sistem, bab ini berisi penjelasan sistem yang digunakan.
5. BAB V – Simulasi dan Analisis Pengujian, bab ini berisi eksperimen dan analisis dari hasil eksperimen yang sudah didapatkan.
6. BAB VI – Kesimpulan dan Saran, bab ini berisi kesimpulan dari hasil penelitian berdasarkan pengujian dan analisis data yang menjawab tujuan awal dari penelitian.