BAB 1
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi yang semakin pesat, dapat menimbulkan permasalahan bagi teknologi itu sendiri, hal tersebut menjadikan internet sebagai salah satu media yang dimanfaatkan untuk pencurian data organisasi, individu maupun pemerintah.

Analisis Malware adalah proses memahami perilaku dan tujuan file atau URL yang mencurigakan. Output dari analisis malware membantu dalam mendeteksi dan mitigasi potensi ancaman. Analisis dapat dilakukan dengan cara Analisis Statis dan Analisis Dinamis. Analisis statis memeriksa file untuk mencari tanda–tanda niat jahat, berfungsi untuk mengidentifikasi infrastruktur, perpustakaan atau file paket berbahaya. Analisis Dinamis mengeksekusi kode berbahaya yang dicurigai di lingkungan aman.

Email *Phising* adalah salah satu kejahatan siber dengan tindakan mengelabuhi seseorang atau organisasi tertentu melalui email demi mendapatkan informasi penting dan rahasia. Aksi *Phising* termasuk dalam salah satu aksi kejahatan siber (*cyber crime).*

Pada tahap analisis data barang bukti berupa informasi yang didapat dari *tools* talos intelligent, virus total, dan any run. Website tersebut akan mengunakan sejumlah alat deteksi virus untuk menggolongkan IP address, domain atau file tergolong dalam *malicious*, sedangkan talos digambarkan sebagai automaton (semacam robot) yang terbuat dari perunggu, sedangkan any run adalah sebuah alat pemindai analisis malware.

1.2 Tujuan

Adapun tujuan dari proyek akhir ini adalah merealisasikan analisis *Malware* dengan metode dinamik menggunakan *Sandbox.*

1.3 Rumusan Masalah

Rumusan masalah dalam pembuatan proyek akhir:

1. Bagaimana cara mendeteksi ancaman *malware*?
2. Bagaimana cara penggunaan metode analisis *malware*?
3. Bagaimana cara installasi software?

1.4 Batasan Masalah

Pada tugas akhir ini penulis membatasi permasalahan sebagai berikut:

1. Jenis – jenis malware yang di analisis: *Adware, Botnet, Bug, Ransomware, Rootkit, Spyware, Trojan horse, virus, worm, laucher, information-stelling Malware, Downloader, Backdoor, Spam-Sending, Scareware.*
2. Pengujian dan Analisis pada Sandbox.
3. Analisis Menggunakan *MITTRE ATT&CK* Framework.