BAB I
PENDAHULUAN

1.1 Latar Belakang

Serangan *website phishing* dapat dicegah dengan memblokir alamat website atau domain yang di informasikan oleh *web browser*, atau dengan beberapa sistem yang sudah dikembangkan penyedia *web hosting*, seperti membaca duplikasi kode sumber dari suatu website resmi, atau pemanfaatan *machine learning* untuk melakukan identifikasi *phishing* melalui tampilan halaman website yang ditiru, ataupun sumber kode dengan berbagai metode perhitungan algoritma yang dikembangkan.

Serangan *website phishing* yang hanya berfokus pada halaman muka dan alamat domain memiliki potensi peningkatan serangan apabila dikombinasikan dengan sebuah class yang terdapat pada pengembangan aplikasi mobile. Class tersebut adalah WebView. Fungsi dari WebView pada aplikasi mobile yaitu menampilkan halaman sebuah website tanpa perlu menggunakan web browser. Pemanfaatkan WebView membuat *website phishing* memiliki potensi untuk bisa menyembunyikan alamat website atau domain dan protokol yang digunakan.

Namun metode terbaru *website phishing* yang dapat ditemukan, berupa teknik bernama BITB (Browes-in-the-Browser). Metode serangan ini melibatkan pembuatan jendela browser palsu didalam jendela aktif pada suatu web browser. Berdasarkan laporan dari *bleepingcomputer* Teknik ini digunakan untuk mendapatkan akun steam dengan cara *threat actor* membagikan link tautan *website phishing* yang memiliki konten tentang *event* penyelenggaraan kompetensi esport palsu [1].

Penelitian ini akan mencoba explorasi potensi jenis serangan baru website phishing dengan memanfaatkan WebView yang disediakan dalam bentuk aplikasi. Penelitian ini selanjutnya akan menyebut metode serangan ini dengan sebutan

serangan WeVPAM yang memiliki kepanjangan *WebView Phishing Application Mobile*.

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas, maka dibuat rumusan masalah yang akan diselesaikan dalam penelitian ini, yaitu: "Bagaimana cara kerja serangan WeVPAM untuk menyembunyikan alamat, domain dan protocol internet website phishing menggunakan WebView aplikasi mobile serta potensi ancamannya?"

1.3 Batasan Masalah

Untuk menghindari penyimpangan maupun pelebaran pokok masalah pada penelitian ini, maka peneliti memberikan batasan pembahasan pada:

a. Skenario generate website phishing
b. Penggunaan class WebView aplikasi mobile

1.4 Tujuan Penelitian

Tujuan dari penelitian ini, yaitu:

a. Membuktikan potensi metode serangan WeVPAM
b. Menjelaskan proses serangan WeVPAM sebagai bentuk serangan kombinasi

1.5 Manfaat Penelitian

Manfaat penelitian ini yaitu memberi informasi adanya sebuah potensi jenis serangan website phishing dengan metode kombinasi yang bisa digunakan untuk menyembunyikan alamat domain dari sebuah website phishing dan agar adanya peningkatan kesadaran, serta lebih lanjut agar terbentuk regulasi dalam penggunaan class WebView pada pemgembangan aplikasi mobile kedepannya.

1.6 Sistematika Penulisan

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 membuatan tugas akhir ini.

BAB III **METODOLOGI PENELITIAN**

Bab metodologi penelitian ini menjelaskan tentang pengertian dari metode dan alat yang digunakan untuk mendukung metode serangan WeVPAM.

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 akhir ini untuk pengembangan teknik selanjutnya.

DAFTAR PUSTAKA

Pada bagian ini akan dipaparkan tentang sumber-sumber yang digunakan dalam penulisan penelitian ini.