BAB I
PENDAHULUAN

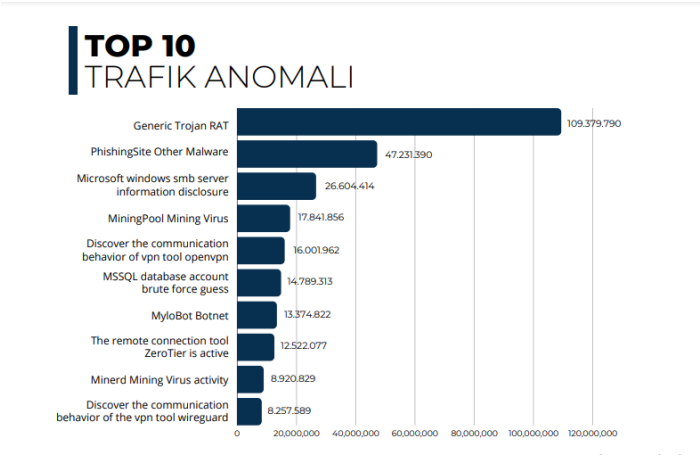
1.1 Latar Belakang

Di era digital yang semakin berkembang pesat, keamanan informasi telah menjadi salah satu aspek krusial yang mempengaruhi berbagai kehidupan, baik bagi individu, organisasi maupun negara. Teknologi informasi dan komunikasi yang semakin terhubung telah membawa perubahan signifikan dalam cara manusia berinteraksi dan menjalankan aktivitas sehari-hari. Namun, kemajuan teknologi ini juga membuka pintu bagi ancaman siber yang semakin kompleks dan beragam. Menurut Laksana & Mulyani (2023) teknologi-teknologi canggih seperti kecerdasan buatan, Internet of Things (IoT), dan blockchain, yang seharusnya membawa kemajuan positif, justru dapat dimanfaatkan oleh pelaku kejahatan siber untuk mengembangkan serangan yang lebih sulit dideteksi. Serangan ini, jika tidak diimbangi dengan pengembangan strategi keamanan yang efektif, akan terus berkembang dan menjadi ancaman yang lebih besar. Serangan siber dapat menyebabkan kerugian finansial yang besar, merusak reputasi, mencuri informasi sensitif, dan bahkan mengancam keamanan nasional.

Di Indonesia, situasi ini semakin memprihatinkan. Laporan dari Badan Siber dan Sandi Negara (BSSN) pada tahun 2023 menunjukkan peningkatan signifikan dalam jumlah insiden siber selama lima tahun terakhir. Pada tahun 2023 saja, tercatat sebanyak 403.990.813 anomali trafik yang mengindikasikan aktivitas siber mencurigakan. Anomali ini tidak hanya berdampak pada performa perangkat dan jaringan, tetapi juga dapat menyebabkan pencurian data sensitif, perusakan reputasi, dan penurunan kepercayaan publik terhadap organisasi. Grafik anomali periode Januari – Desember 3023 ditunjukan pada gambar 1.1.

Gambar 1.1 Grafik Anomali Periode Januari - Desember 2023

Pada lanskap keamanan siber Indonesia tahun 2023 juga terdapat top 10 trafik anomali yang dapat dilihat pada gambar 1.2 berikut:



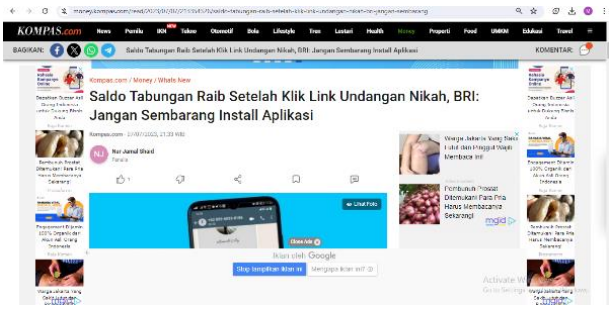
Gambar 1.2 Top 10 Trafik Anomali Selama Tahun 2023

Pada Gambar 1.2 salah satu jenis serangan siber yang semakin sering terjadi di Indonesia adalah *phishing* dengan jumlah sebanyak 47.231.390 anomali. Salah satu kasus phising yang terjadi di Indonesia dapat dilihat pada gambar 1.3.

Gambar 1.3 Kasus Phising Pembobolan Bank BRI

Sumber: Kompas.com

Dilansir dari Kompas.com kasus phising yang terjadi di Indonesia adalah kasus pembobolan Bank BRI di Sumatera Barat pada tahun 2022, pada kasus ini korban menerima pesan melalui WhatsApp terkait perubahan biaya transfer dan korban mengklik tautan yang dilampirkan pada pesan WhatsApp tersebut kemudian korban mengisi formulir yang berisikan username dan password-nya. Akibatnya, korban mengalami kerugian sebesar 1,1 miliar rupiah. Kasus lain phishing lainnya yang terjadi di Indonesia dapat dilihat pada Gambar 1.4. berikut:



Gambar 1.4 Kasus Phishing Hilangnya Saldo Nasabah

Sumber: Kompas.com

Pada Gambar 1.4 dilansir dari kompas.com kasus phising lainnya yang terjadi di Indonesia adalah seorang nasabah di Kota Malang, Jawa Timur kehilangan saldo di rekeningnya hingga Rp 1,4 miliar, setelah membuka sebuah undangan pernikahan berformat aplikasi (APK) di WhatsApp.

Tantangan utama dalam upaya pencegahan phishing adalah kurangnya kesadaran dan edukasi di kalangan pengguna internet. Banyak pengguna yang belum memahami bagaimana serangan phishing bekerja dan langkah-langkah apa yang perlu diambil untuk melindungi diri mereka. Untuk itu, diperlukan metode edukasi yang efektif dalam meningkatkan kesadaran dan pemahaman tentang phishing. Salah satu pendekatan yang dapat digunakan adalah pengembangan *game* edukasi. Penelitian oleh Alkhalil et al. (2021) menunjukkan bahwa pendidikan dan simulasi phishing dapat secara signifikan mengurangi risiko serangan phishing dengan meningkatkan kesadaran dan pemahaman pengguna. Dari latar belakang

ini, peneliti bertujuan untuk merancang *game* edukasi terkait serangan phishing yang dapat mensimulasikan serangan phishing dan memberikan pengetahuan praktis tentang cara mengidentifikasi dan menghindari serangan tersebut.

1.2 Rumusan dan Batasan Masalah

Berdasarkan latar belakang yang telah dijelaskan terdapat beberapa rumusan masalah yang dapat dirinci, sebagai berikut:

1. Bagaimana hasil analisis *decompile* terhadap aplikasi *phising*?
2. Bagaimana hasil perancangan *game PhisTrap* berdasarkan hasil *decompile*?

Berdasarkan pada rumusan masalah, perlu dijelaskan batasan masalah agar penelitian tetap terfokus dan sesuai dengan rencana, memastikan pencapaian tujuan penelitian. Oleh karena itu, berikut merupakan batasan masalah dari penelitian ini:

1. Penelitian ini hanya akan melakukan *decompile* serangan *phising* yang umum digunakan, seperti *phising* melalui pesan WhatsApp dengan lampiran berbahaya, dan menganalisis teknik-teknik yang dapat disimulasikan dalam *game*.
2. Perancangan *game PhisTrap* dirancang hanya sampai proses pengujian beta dan *game PhisTrap* dirancang hanya untuk *platform Android* saja dan hanya akan diuji pada dua orang *tester* untuk mendapatkan umpan balik awal.

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah yang sudah dijabarkan diatas, terdapat tujuan penelitian sebagai berikut:

1. Untuk mengetahui bagaimana teknik, pola, dan mekanisme yang digunakan dalam serangan phishing melalui proses *decompile* aplikasi *phising*.
2. Untuk mengetahui hasil perancangan *game PhisTrap* yang didasarkan pada temuan dari *decompile* pada aplikasi *phising*.

1.4 Manfaat Penelitian

Hasil dari penelitian ini diharapkan dapat memberikan manfaat secara praktis maupun teoritis. Secara teoritis, penelitian ini diharapkan dapat menambah

literatur mengenai pemanfaatan *game* edukasi terutama untuk mensimulasikan serangan *phishing* dan memberikan pengetahuan praktis tentang cara mengidentifikasi dan menghindari serangan tersebut. Secara praktis, penelitian ini diharapkan menjadi salah satu pilihan solusi untuk mengedukasi dan meningkatkan kesadaran tentang *phising* dan mengurangi resiko serangan *phising*.

1.5 Struktur Organisasi Skripsi

Struktur organisasi dalam penelitian skripsi ini mengikuti Pedoman Penelitian Karya Ilmiah UPI Tahun Akademik 2021. Berikut struktur organisasi skripsi berdasarkan Pedoman Penelitian Karya Ilmiah UPI Tahun Akademik

1. Bab I: Pendahuluan, bab ini menjadi bab perkenalan yang mencakup latar belakang penelitian, rumusan masalah penelitian, tujuan penelitian, manfaat/signifikansi penelitian serta organisasi skripsi.
2. Bab II: Kajian Pustaka, bab ini meberikan konteks yang jelas terhadap topik atau permasalahan yang diangkat dalam penelitian, berisikan teori yang sedang dikaji dan kedudukan masalah penelitian dalam bidang ilmu yang diteliti. Topik yang dibahas meliputi keamanan siber, *phishing, computer based learning*, *game*, dan hasil-hasil penelitian yang relevan.
3. Bab III: Metode Penelitian, bab ini merinci pada metode penelitian yang digunakan, termasuk jenis penelitian, prosedur penelitian, subjek penelitian, instrumen penelitian, dan teknik analisis data.
4. Bab IV: Temuan dan Pembahasan, bab ini memaparkan temuan-temuan dari penelitian serta membahas hasil perancangan produk dan hasil uji yang diperoleh dari pengolahan data.
5. Bab V: Simpulan, Implikasi, dan Rekomendasi, bab ini memberikan kesimpulan berupa rangkuman dari keseluruhan penelitian yang telah dilakukan, serta implikasi dan rekomendasi yang dihasilkan dari penelitian ini.