BAB I
PENDAHULUAN

1.1 Latar Belakang

Serangan phishing telah menjadi ancaman yang signifikan untuk keamanan siber di Indonesia, seiring dengan penggunaan internet di Indonesia semakin meluas di masyarakat, dan kurangnya kesadaran akan keamanan informasi pribadi sehingga terjadi pencurian data pribadi. Serangan phishing adalah kejahatan siber yang menggunakan teknik pengelabuan untuk mendapatkan informasi yang sensitif, seperti kata sandi, data pribadi, dan informasi finansial [1].

Perkembangan serangan phishing saat ini menunjukan pertumbuhan yang cukup tinggi, dengan peningkatan kasus dari tahun 2022 hingga 2024. Pada tahun 2022, laporan aktivitas phishing yang bersumber dari Lanskap Keamanan Siber Indonesia BSSN mencatat aktivitas phishing sebanyak 33.305.209 trafik [1]. Pada tahun 2023, bersumber dari Lanskap Keamanan Siber Indonesia BSSN mencatat aktivitas phishing sebanyak 47.231.390 [2]. Pada tahun 2024, bersumber dari Lanskap Keamanan Siber Indonesia BSSN mencatat aktivitas phishing sebesar 26.771.610 [3].

Hal ini disebabkan oleh ketergantungan pada teknologi tanpa adanya pemahaman risiko, serta perkembangan taktik phishing yang semakin canggih. Sehingga, tingkat keberhasilan serangan phishing tetap tinggi. Meskipun ada upaya pencegahan seperti kampanye kesadaran dari berbagai lembaga, terdapat gap dalam evaluasi efektivitas metode pengujian kesadaran manusia melalui simulasi serangan. Gap ini menjadi indikasi kurangnya data tentang berapa persen pengguna yang tertipu dalam skenario simulasi.

Simulasi phishing merupakan pendekatan eksperimental yang efektif karena mampu mengukur respons nyata pengguna dalam situasi menyerupai kondisi serangan sebenarnya. Penelitian ini bertujuan mengisi gap tersebut, dengan mensimulasikan serangan phishing dalam lingkungan lab dan alat seperti SEToolkit

dan Zphisher [4]. Pendekatan ini relevan karena dapat memberikan wawasan langsung tentang kerentanan manusia. Dengan hasil penelitian ini diharapkan berkontribusi pada pengembangan strategi pendidikan yang efektif, mengurangi risiko serangan phishing di masa depan.

Pemilihan instagram dan WhatsApp didasarkan pada data SAFEnet yang mencatat keduanya sebagai platform paling banyak diserang di Indonesia, dengan tingkat kerentanan tinggi akibat interaksi cepat, kepercayaan antar pengguna, dan popularitas di kalangan usia muda. Instagram mendominasi insiden serangan digital dengan 68 kasus pada Q2 2025 (termasuk hacking dan doxing), sementara WhatsApp sering digunakan untuk ancaman dan phishing melalui pesan pribadi (53 kasus), menjadikannya target ideal untuk menguji respons nyata responden terhadap skenario serangan yang relevan dengan kebiasaan sehari-hari [5].

1.2 Rumusan Masalah

a. Bagaimana tingkat keberhasilan simulasi serangan phishing terhadap pengguna media sosial dalam lingkungan lab ?
b. Apa saja faktor yang mempengaruhi kerentanan pengguna media sosial terhadap simulasi serangan phishing ?

1.3 Batasan Masalah

a. Penelitian ini berfokus pada simulasi serangan phishing dalam lingkungan lab.
b. Fokus evaluasi efektivitas terbatas pada alat simulasi seperti SEToolkit dan Zphisher.
c. Fokus mengukur tingkat keberhasilan penipuan dan peningkatan kesadaran, tanpa membahas aspek teknis pertahanan siber lainnya seperti deteksi malware atau enkripsi data.
d. Penelitian dilakukan pada 20 pengguna aktif media sosial berusia 18 – 25 tahun.

1.4 Tujuan Penelitian

Tujuan yang akan dicapai oleh peneliti dalam penelitiannya adalah menghasilkan analisis efektivitas serangan phishing di era sekarang, dengan memvalidasi tingkat keberhasilan penipuan dengan menggunakan SEToolkit dan Zphisher terhadap pengguna media sosial dalam lingkungan lab.

1.5 Manfaat Penelitian

a. Penlitian ini diharapkan dapat berkontribusi pada pengembangan teori keamanan siber dengan memperluas tentang efektivitas serangan phishing di era digital saat ini.

b. Penelitian ini juga dapat memberikan rekomendasi praktis bagi platform media sosial dan penyedia layanan keamanan untuk meningkatkan keamanan dari segi sistem maupun user, seperti penambahan protokol anti phishing dan kampanye edukasi, sehingga bisa mengurangi risiko serangan nyata terhadap pengguna

1.6 Sistematika Penulisan

Sistematika penulisan ini berisikan garis besar atau gambaran umu yang menjelaskan alur dari penelitian ini sehingga dapat mempermudah pemahaman alur penelitian. Adapun garis besar isi skripsi ini adalah sebagai berikut :

BAB I PENDAHULUAN, tahapan ini merupakan bab awal yang menjelaskan tentang latar belakang, masalah penelitian, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA, berisi tinjauan pustaka, dasar-dasar teori yang digunakan dan memberikan pengertian beberapa teori antara lain; apa itu phishing, teknik phising (email phishing, spear phising, vishing, smishing, pharming), social engineering, SEToolkit, Zphisher, konsekuensi phishing, dan strategi pencegahan.

BAB III METODE PENELITIAN, bab ini terdapat tinjauan umum tentang aalur penelitian, prosedur, dan mekanisme metode analisis yang diterapkan pada penelitian.

BAB IV HASIL DAN PEMBAHASAN, bab ini menerangkan hasil yang memaparkan tingkat keberhasilan dan data demografis (perbedaan antara target yang sudah mempunyai ilmu keamanan jaringan dan tidak) dan membandingkan temuan dengan literatur terdahulu untuk menjawab tujuan penelitian.

BAB V PENUTUP, berisi Kesimpulan yang merupakan jawaban final atas rumusan masalah penelitian (terkait dengan tingkat keberhasilan serangan phishing pada pengguna media sosial serta menjelaskan faktor yang mempengaruhi kerentanan kesadaran pengguna media sosial terhadap phishing), serta memberikan saran strategi untuk melindungi dari serangan phishing.