BAB V
PENUTUP

5.1 Kesimpulan

Simulasi serangan phishing yang dilakukan secara terstruktur menggunakan alat SEToolkit dan Zphisher, dikombinasikan dengan sesi edukasi singkat, terbukti efektif meniru karakteristik serangan phishing nyata dalam lingkungan laboratorium yang terkontrol. Hasil simulasi berhasil menangkap kredensial login dan alamat IP dari sebagian besar responden, yang menggambarkan tingkat kerentanan pengguna media sosial terhadap login palsu yang dirancang secara meyakinkan. Temuan ini mengonfirmasi rumusan masalah pertama mengenai tingkat keberhasilan serangan phishing terhadap pengguna medai sosial dalam skenario simulasi lab.

Analisis faktor kerentanan menunjukkan bahwa pengetahuan awal rendah tentang phishing, kebiasaan penggunaan media sosial tanpa verifikasi, dan minimnya pemanfaatan fitur keamanan seperti autentikasi dua faktor berkontribusi signifikan terhadap keberhasilan simulasi. Responden dengan karakteristik tersebut lebih mudah terjebak, namun setelah mengalami simulasi, banyak yang terdorong mengubah perilaku dan meningkatkan konfigurasi keamanan akun.

Temuan ini konsisten dengan landasan teori Bab II tentang peran faktor psikologis, perilaku, dan emosional dalam kerentanan social engineering, serta secara empiris menjawab rumusan masalah kedua mengenai faktor-faktor yang mempengaruhi kerentanan pengguna media sosial terhadap serangan phishing.

Secara keseluruhan, penelitian ini menyimpulkan bahwa simulasi serangan phishing dapat berfungsi ganda sebagai instrumen pengukuran sekaligus intervensi edukatif yang efektif untuk meningkatkan kesadaran keamanan siber pengguna media sosial, dengan tetap mempertimbangkan faktor-faktor kerentanan individu yang telah diidentifikasi

5.2 Saran

Berdasarkan hasil penelitian dan keterbatasan yang ditemui, beberapa saran yang dapat diajukan sebagai berikut:

a. Penelitian selanjutnya disarankan untuk melibatkan jumlah responden yang lebih besar dan latar belakang yang lebih beragam, misalnya pegawai kantor, pelajar SMA, atau kelompok usia diatas 25 tahun, sehingga generalisasi temuan terkait efektivitas simulasi phishing dan pola kerentanan dapat diperkuat di berbagai konteks pengguna.

b. Selama proses penelitian, keterbatasan yang muncul antara lain keterbatasan waktu pelaksanaan, lingkungan simulasi yang berbasis lab, serta ketergantungan pada self-report kuesioner untuk mengukur aspek perilaku. Oleh karena itu, penelitian dimasa depan dapat mempertimbangkan pengamatan perilkau yang lebih naturalistik di luar lab dengan mempertimbangkan etika penelitian yang ketat, penambahan instrumen pengukuran lain, serta penembangan skenario yang lebih mendekati kondisi serangan di dunia nyata.

c. Penelitian lanjutan dapat mengembangkan sesi edukasi dengan menambahkan phishing quiz interaktif yang mengintegrasikan elemen gamifikasi, seperti poin reward dan leaderboard, untuk meningkatkan engagement responden dalam mengenali pola phishing secara real-time. Selain itu, pengembangan aplikasi mobile phishing simulator dengan fitur obfuscation URL (seperti dynamic domain generation atau URL shortener yang disamarkan) akan lebih mendekati skenario serangan nyata di lingkungan mobile-first, sehingga simulasi menjadi lebih realistis dan efektif dalam membangun kewaspadaan pengguna media sosial terhadap ancaman phishing yang terus berevolusi.

Saran-saran tersebut diharapkan dapat menjadi masukan bagi peneliti lain, institusi pendidikan, dan praktisi keamanan siber dalam merancang program edukasi dan penelitian lanjutan terkait mitigasi serangan phishing di media sosial.