BAB V
KESIMPULAN DAN SARAN

5.1. Kesimpulan

Penelitian ini berhasil mengevaluasi efektivitas serangan *Man-in-the-Middle* (MITM) untuk menyadap kredensial *login* pada *website* SIAKAD UPN Veteran Jakarta melalui jaringan *wireless* di Fakultas Ilmu Komputer. Berdasarkan pengujian terhadap 25 responden yang menggunakan empat jenis *browser*, hasil penelitian menunjukkan bahwa serangan MITM memiliki tingkat keberhasilan yang berbeda pada setiap *browser*.

1. Penelitian ini menunjukkan bahwa serangan MITM dapat berhasil menyadap kredensial *login* pada *website* SIAKAD UPN Veteran Jakarta, terutama ketika protokol HTTPS yang seharusnya melindungi data diturunkan menjadi HTTP. Serangan ini dilakukan melalui tahapan sniffing, ARP *Poisoning*, dan penggunaan SSL Strip untuk mengalihkan lalu lintas HTTPS menjadi HTTP yang tidak terenkripsi. Serangan ini berhasil pada browser Google Chrome, Microsoft Edge, dan Opera dengan tingkat keberhasilan 100%, namun kurang berhasil pada Mozilla Firefox versi terbaru karena adanya mekanisme keamanan tambahan, seperti certificate pinning dan peringatan SSL/TLS. Ini menunjukkan bahwa efektivitas serangan MITM sangat bergantung pada jenis browser yang digunakan dan konfigurasi keamanan yang diterapkan pada browser tersebut.

2. Serangan MITM yang berhasil dapat menyebabkan kebocoran kredensial *login*, seperti username/email dan password, yang dikirim melalui lalu lintas HTTP yang tidak terenkripsi. Hal ini meningkatkan risiko penyalahgunaan data dan akses tidak sah ke sistem akademik, yang dapat merugikan privasi mahasiswa dan keamanan data di *website* SIAKAD. Potensi dampak ini menjelaskan mengapa pentingnya perlindungan terhadap komunikasi data menggunakan enkripsi yang kuat dan protokol HTTPS. Serangan *Man-in-the-Middle* (MITM) dapat menyebabkan berbagai dampak serius terhadap

keamanan data dan privasi mahasiswa, seperti pencurian data pribadi (NIM, email, dan kata sandi), manipulasi informasi akademik (mengubah nilai atau data mahasiswa), serta penyalahgunaan akun (akses ilegal ke akun SIAKAD untuk merubah data pribadi atau menyebarkan informasi yang tidak sah). Selain itu, serangan ini juga mengancam privasi mahasiswa dengan mengakses komunikasi sensitif yang seharusnya dilindungi.

3. Mengenai tingkat kerentanan *website* SIAKAD UPN Veteran Jakarta, berdasarkan pengujian keamanan menggunakan SSL Labs, *website* ini *me*ndapatkan grade B untuk konfigurasi SSL/TLS dan nilai F untuk konfigurasi Security Header. Hal ini menunjukkan bahwa *website* SIAKAD memiliki tingkat kerentanan yang cukup tinggi terhadap serangan MITM, terutama ketika menggunakan protokol HTTP atau konfigurasi keamanan yang tidak optimal. SSL/TLS adalah langkah pertama dalam melindungi komunikasi antara klien dan *server* melalui enkripsi dan otentikasi, sementara *header* keamanan adalah langkah tambahan yang dirancang untuk melindungi aplikasi *web* dari ancaman berbasis *browser* dan eksploitasi lapisan aplikasi. Keduanya saling melengkapi, di mana SSL/TLS bertugas melindungi data selama proses transmisi, sedangkan *header* keamanan memastikan data tersebut digunakan dan ditampilkan dengan aman di *browser*. Kombinasi keduanya sangat penting untuk mencapai tingkat keamanan *web* yang komprehensif.

Serangan *Man-in-the-Middle* (MITM) secara signifikan mengancam aspek *Confidentiality* (Kerahasiaan) dan *Integrity* (Integritas). Penyerang dapat mencegat, membaca, dan memanipulasi data sensitif seperti kredensial atau pesan pribadi, bahkan menyisipkan data palsu tanpa sepengetahuan korban. Sementara itu, dampak terhadap *Availability* (Ketersediaan) biasanya lebih jarang, tetapi dalam beberapa kasus, penyerang dapat mengganggu akses layanan dengan memutuskan atau memperlambat koneksi.

Secara keseluruhan, penelitian ini menekankan betapa pentingnya penerapan protokol HTTPS secara menyeluruh pada *website* SIAKAD UPN Veteran Jakarta.

HTTPS berfungsi untuk memastikan bahwa komunikasi antara pengguna dan *server* terlindungi dengan enkripsi yang kuat, sehingga data sensitif seperti kredensial *login*, nilai akademik, dan informasi pribadi mahasiswa tidak mudah disusupi oleh pihak yang tidak bertanggung jawab. Selain itu, penelitian ini juga menggarisbawahi perlunya peningkatan mekanisme keamanan lainnya, seperti konfigurasi SSL/TLS yang lebih kuat dan penerapan header keamanan yang tepat, guna mencegah serangan *Man-in-the-Middle* (MITM) yang dapat merusak privasi dan keamanan data pengguna. Dengan langkah-langkah tersebut, *website* SIAKAD diharapkan dapat lebih terlindungi dari ancaman potensial yang dapat merugikan mahasiswa dan pihak universitas secara keseluruhan.

5.2. Saran

Berdasarkan hasil penelitian, beberapa langkah penting yang dapat dilakukan untuk meningkatkan keamanan terhadap serangan *Man-in-the-Middle* (MITM) adalah selalu menggunakan *browser* versi terbaru untuk mendapatkan perlindungan keamanan terbaru, menghindari penggunaan jaringan Wi-Fi publik untuk mengakses data sensitif, terutama yang menggunakan protokol HTTP, memperhatikan indikator keamanan pada *browser*, seperti ikon gembok atau peringatan sertifikat, mengimplementasikan HTTPS secara menyeluruh pada semua halaman *website untuk* mengenkripsi lalu lintas data, memberikan edukasi kepada pengguna tentang risiko serangan siber dan langkah pencegahan yang dapat dilakukan. Selain itu, pengelola sistem juga diharapkan dapat meningkatkan versi TLS terbaru serta menerapkan *header* HSTS dan beberapa *header* lainnya untuk melindungi dari serangan penurunan HTTPS ke HTTP. Selain itu pengelola

Penelitian selanjutnya diharapkan dapat mengeksplorasi teknik serangan yang lebih kompleks, berfokus pada pengembangan atau evaluasi langkah-langkah pencegahan serangan *Man-in-the-Middle* (MITM) menggunakan teknologi terbaru seperti implementasi HTTPS dengan HSTS, firewall canggih, atau protokol keamanan tambahan. Selain itu, analisis komparatif berbagai *browser*, pengujian dengan alat lain seperti Bettercap, dan evaluasi kerentanan pada platform mobile

SIAKAD dapat menjadi fokus. Studi mengenai kesadaran pengguna terhadap risiko MITM, implementasi sertifikat SSL/TLS yang lebih kuat, serta pengujian pada skala lebih besar di lingkungan universitas lain juga disarankan untuk memperluas temuan penelitian. Pengujian pada jaringan yang lebih beragam dan situasi dunia nyata juga dapat memberikan wawasan lebih dalam tentang ancaman keamanan siber.