UJI COBA SERANGAN MAN IN THE MIDDLE PADA KEAMANAN SSL PROTOKOL HTTP

Henni Endah Wahanani [1)], Firza Prima Aditiawan[2)], Retno Mumpuni[3)]
Email : [1]henniendah.if@upnjatim.ac.id
[1,2,3] Program Studi Informatika, Fakultas Ilmu Komputer, UPN"Veteran" Jawa Timur

Abstrak

Aplikasi berbasis web bergantung pada protokol HTTP dan keamanan dalam transaksi mulai dari perbankan, *e-commerce*, dan pengadaan elektronik hingga yang berhubungan dengan data sensitif seperti transaksi keuangan atau informasi data pegawai. Hal ini dibutuhkan suatu keamanan dalam pengaksessannya, baik untuk *login* ataupun transaksi dalam website. Tujuan dari diciptakannya pengaman jaringan yaitu agar seluruh data atau informasi penting yang ada dalam *server* tidak terbocorkan oleh *public*. Penelitian ini mengusulkan pengujian serangan MITM (Man In The Middle) pada tingkat keamanan SSL dari protokol HTTP dengan teknik *sniffing* dengan 3 tools yang digunakan yaitu wiredshark, smartsniff dan bettercap . Berdasarkan hasil uji coba dengan 3 tools tersebut bahwa protokol HTTP dengan keamanan SSL sangat bagus terbukti saat melakukan aktifitas *login.* Pengujian melakukan aktifitas *sniffing* paket-paket data terinkripsi dengan baik sehingga sangat sulit untuk mengetahui *username* dan *password.*

Kata kunci: MITM, sniffing, HTTPS

1. PENDAHULUAN

Meningkatnya popularitas lalu lintas jaringan terenkripsi adalah pedang bermata dua. Di satu sisi, ia menyediakan mengamankan transmisi data, melindungi terhadap penyadapan, dan meningkatkan kepercayaan komunikasi pengguna. Di sisi lain, itu mempersulit pemantauan lalu lintas jaringan, termasuk klasifikasi lalu lintas dan identifikasi host. Saat ini, dapat melakukannya memantau, mengidentifikasi, dan mengklasifikasikan lalu lintas jaringan teks biasa, seperti HTTP, tetapi sulit untuk menganalisis komunikasi terenkripsi [1]. Aplikasi berbasis web bergantung pada protokol HTTP dan keamanan dalam transaksi mulai dari perbankan, e-commerce, dan pengadaan elektronik hingga yang berhubungan dengan data sensitif seperti informasi data pegawai. Pengguna mempercayai protokol ini untuk mencegah tampilan yang tidak sah atas informasi pribadi, keuangan, dan rahasia lain melalui Web.

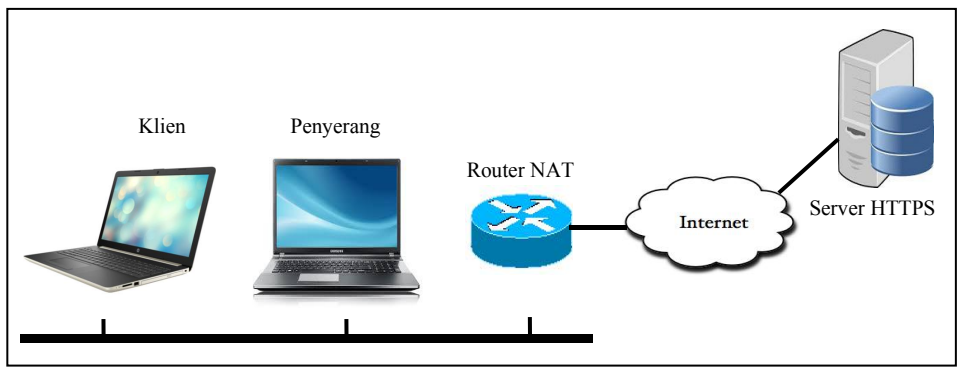
Segi pengamanan pada web browser maka dibutuhkan keamanan guna menghalau berbagai serangan. Netscape Communications memperkenalkan Secure Socket Layer (SSL) untuk komunikasi sensitif-keamanan pada tahun 1994. Internet Engineering Task Force (IETF) mengadopsinya pada tahun 1999 sebagai standar dikenal sebagai Transport Layer Security (TLS) [2] untuk mengamankan HTTP menjadi HTTPS. SSL berguna untuk mengenkripsi proses-proses autentifikasi yang terjadi pada web browser [3]. URL HTTPS menunjukkan bahwa browser akan mengunduh halaman Web menggunakan HTTP tetapi dengan *port default* yang berbeda (443) dan lapisan enkripsi / otentikasi TLS tambahan antara HTTP dan TCP. Akibatnya, kebanyakan orang mempertimbangkan data berbasis HTTPS untuk pertukaran data karena lebih aman, dan rata-rata pengguna cenderung mempercayai aplikasi web.

Serangan Man In The Middle (MITM) mengeksploitasi fakta bahwa Server HTTPS mengirim sertifikat dengan kunci publiknya ke Web browser. Jika sertifikat ini tidak dapat dipercaya, seluruh jalur komunikasi akan rentan terhadap pencurian data. Serangan semacam itu menggantikan sertifikat asli yang mengautentikasi server HTTPS dengan sertifikat yang dimodifikasi. Serangan berhasil jika pengguna lalai memeriksa

sertifikat ketika *browser* mengirim pemberitahuan peringatan. Ini terjadi terlalu sering — terutama di antara pengguna yang sering menemukan sertifikat yang ditandatangani sendiri ketika mengakses situs intranet [4]. Serangan MITM biasanya menargetkan individu, dan, serangan sering tetap tidak ditemukan dan tidak tercatat dalam statistik. Saat ekonomis operator diserang, serangan sering tetap disembunyikan kepada publik untuk menjaga citra perusahaan [5]. Hanya dalam serangan skala besar, itu terungkap sejauh mana kerusakan yang ditimbulkan.

Salah satu cara pertama adalah serangan lokal melalui koneksi Ethernet atau Wifi. Seorang penyerang dengan akses ke jaringan lokal dapat melakukan serangan terhadap perangkat pintar pada dua cara umum yaitu *polling cloud* (internet) dan koneksi langsung. Dalam kasus pertama, dalam *polling cloud*, perangkat pintar selalu berkomunikasi dengan *cloud*. Perangkat pintar menggunakan metode ini ketika ingin terus memeriksa server *cloud* apakah ada versi *firmware* baru yang tersedia. Jika ya, itu mengunggah statusnya. Untuk menargetkan aplikasi seperti itu, penyerang dapat melakukan serangan MITM. Mereka dapat mengarahkan lalu lintas jaringan menggunakan ARP atau dengan memodifikasi pengaturan DNS. Untuk mencegat penyerang *traffic* HTTPS dapat menggunakan sertifikat yang ditandatangani sendiri atau beberapa alat seperti SSLstrip. Ketika koneksi dilakukan melalui HTTPS, beberapa perangkat pintar tidak memverifikasi apakah sertifikat tersebut dipercaya atau tidak. [6] "tidak satu pun dari perangkat yang diuji melakukan otentikasi SSL bersama, di mana kedua belah pihak mengotentikasi satu sama lain, bukan hanya server yang mengotentikasi dengan klien. Sebagian besar perangkat sepenuhnya mengabaikan daftar pencabutan sertifikat, yang memungkinkan penyerang menggunakan kunci yang diperoleh melalui pelanggaran data tanpa masalah".

Pada gambar 1 menunjukkan di mana pengguna di klien ingin melakukan transaksi aman di server menggunakan HTTPS. Klien dan server bertukar data jaringan, sedangkan penyerang bertindak sebagai *gateway* untuk aliran lalu lintas. Penyerang (yaitu, "MITM") memotong lalu lintas dari sumber dan meneruskannya ke tujuan, sehingga memperoleh kemampuan untuk mengubah pesan dan menyisipkan pesan baru tanpa salah satu pihak menyadarinya.

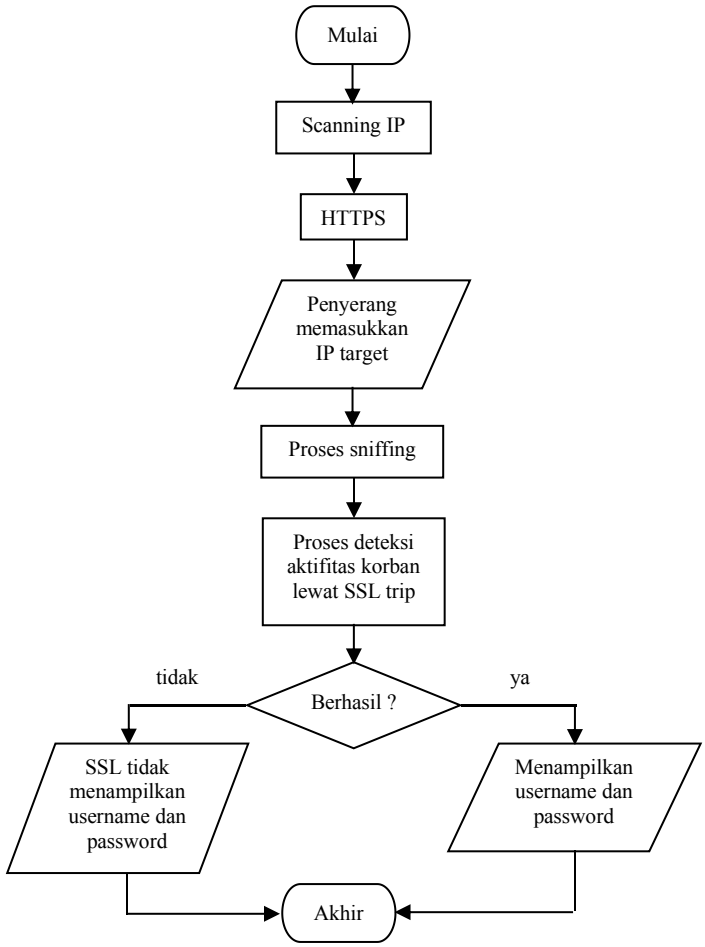


Gambar 1. Model Serangan MITM

Didalam penelitian ini akan dilakukan pengujian tingkat keamanan SSL dari protokol HTTP. Tujuan pengujian ini dilakukan untuk mengetahui tingkat keamanan SSL dalam melindungi data dan proses komunikasi data dengan server. Untuk pengujian ini akan digunakan metode penyerangan MITM. Serangan MITM yang digunakan teknik *sniffing*. Metode ini berguna untuk mencari kelebihan dan kekurangan dari sebuah keamanan website mulai dari keamanan dari paket-paket data pada website dan sistem komunikasi yang dilakukan website dengan web server.

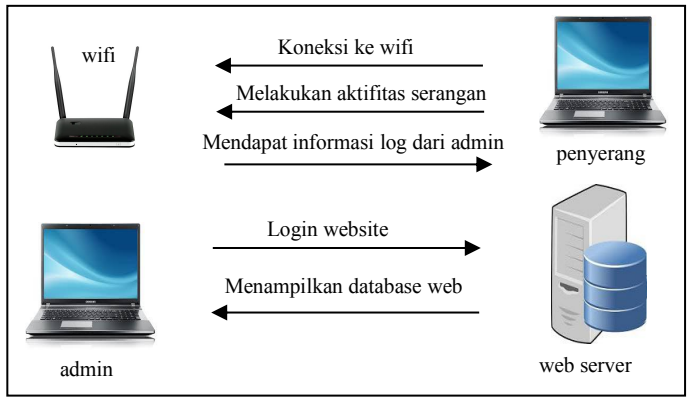
2. METODOLOGI

Pada gambar 2, penyerang melakukan IP *scanning* dengan menggunakan teknik untuk mengetahui IP dari target. Langkah selanjutnya memasukkan IP target dengan metode *sniffing* yang digunakan untuk mengetahui aktifitas target. Proses selanjutnya yaitu proses SSL trip ,dalam proses ini berfungsi menampilkan aktifitas target yaitu aktifitas login.



Gambar 2. Alur serangan MITM

Pada gambar 3, Metode MITM ini terfokus kepada teknik *sniffing* dengan mendeteksi paket-paket data dan mengetahui *username* dan ,*password*. Analisa akan dilakukan pada protokol HTTPS melalui beberapa kali pengujian. Penyerang menghubungkan dengan jaringan *wifi*, dimana *wifi* tersebut juga telah terhubung dengan admin. Dalam hal ini penyerang akan melakukan *scanning IP* yang berguna untuk mendeteksi aktifitas dari admin. Aktifitas yang dimaksud adalah ada nya aktifitas yang berhubungan dengan web server. Pengujian ini akan dilakukan mengunakan *tool* yang selanjutnya akan dibandingkan. Dalam penelitian ini *tools* yang dibandingkan yaitu *wiredshark, bettercap* dan *smartsniff*.



Gambar 3. Skenario pengujian serangan MITM

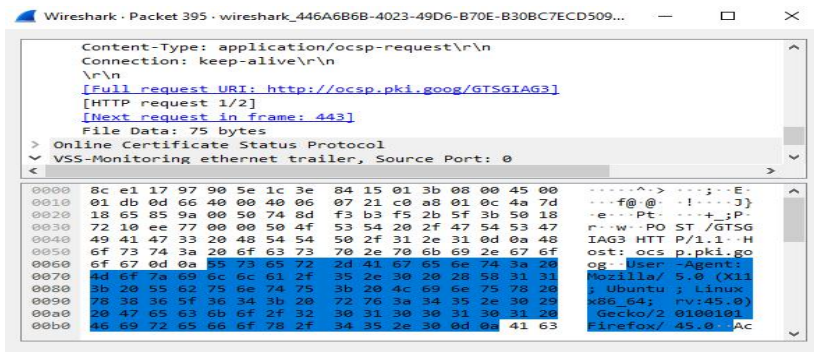
3. HASIL DAN PEMBAHASAN

Pembahasan mengenai implementasi sistem serta hasil pengujian akan dijelaskan juga proses pengujian dengan menggunakan tools dan juga akan ditampilkan daftar tabel pengujian berhasil dan gagal dalam pengujian HTTPS tersebut.

3.1 Pengujian MITM

Skenario pengujian serangan MITM sesuai dengan metodologi penelitian dengan tools *wiredshark,bettercap* dan *smartsniff* pada protokol HTTPS di aktifitas *login*.

1. Pengujian serangan mengunakan wiredshark dengan melakukan aktifitas *login.* Hasil bisa dilihat pada gambar 4.

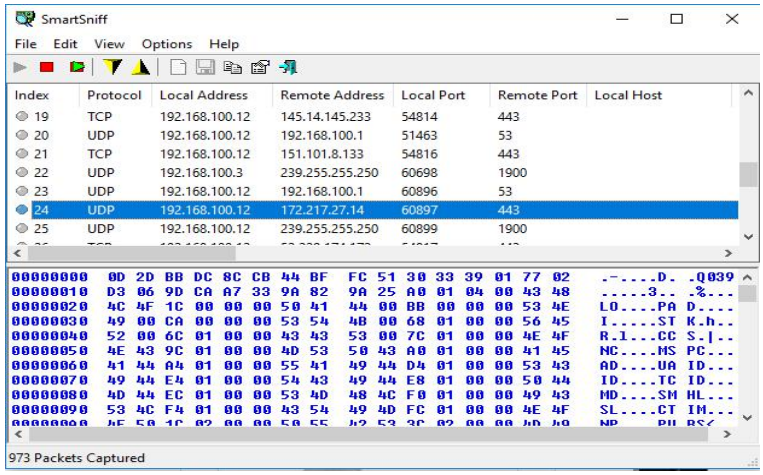


Gambar 4. Hasil pengujian HTTPS dengan wiredshark

2. Pengujian serangan mengunakan bettercap. Hasil bisa dilihat pada gambar 5

Gambar 5. Hasil pengujian HTTPS dengan menggunakan bettercap

3. Pengujian serangan mengunakan smartsniff. Hasil bisa dilihat pada gambar 6.



Gambar 6. Hasil pengujian HTTPS dengan menggunakan smartsniff

3.2 Daftar Tabel Pengujian

Pada daftar tabel 1 menampilkan hasil pengujian yang berupa perbandingan dari beberapa kali pengujian dengan menggunakan berbagai *tools*.

Tabel 1 Pengujian HTTPS

Tools	Pengujian HTTPS	Kekurangan
Wiredshark	3 kali gagal	Tidak dapat mendeteksi aktifitas protokol HTTPS
Bettercap	2 kali berhasil 1 kali gagal	Tidak didukung dengan SSL trip
SmartSniff	3 kali berhasil	Tidak mendukung *sniffing password* ,hanya bersifat monitoring satu PC dan tidak mendukung MITM.

4. KESIMPULAN DAN SARAN

Berdasarkan uji coba serangan MITM untuk menguji keamanan SSL pada protokol HTTP, tingkat keamanan dari HTTP terjamin dengan adanya SSL. Aktifitas komunikasi antar pengguna ataupun admin dengan *webserver* terjaga dengan baik melalui enkripsi data. Serangan MITM dengan teknik *sniffing* menggunakan *tools wiredshark*, *smartsniff*, *bettercap* pada HTTPS sangat sulit untuk mengetahui *username* dan *password*. Penelitian ini dapat di kembangkan dengan uji coba menggunakan metode MITM yang lain seperti *ARP Poisioning*, *Drifnet* dan sebagainya.

5. DAFTAR RUJUKAN

[1] Husák, M., Čermák, M., Jirsík, T., & Čeleda, P. 2016. *HTTPS traffic analysis and client identification using passive SSL/TLS fingerprinting.* EURASIP Journal on Information Security.

[2] T. Dierks and C. Allen, 1999. *The TLS Protocol*, IETF RFC 2246. www.ietf.org/rfc/rfc2246.txt.

[3] Arshad Mohammad and Ali Hussain Md. 2016. *Secure Framework To Mitigate Man In The Middle Atack Over SSL Protocol*. Indian Journal Of Science And Technology, Vol. 9

[4] Callegati, F., Cerroni, W., & Ramilli, M. 2009. *Man-in-the-Middle Attack to the HTTPS Protocol.* IEEE Security & Privacy Magazine, 7(1), 78–81.

[5] Cekerevac, Z.,Dvorak, Z., Prigoda, L., & Cekerevac, P. 2017. Internet of things and the man in the middle attacks security and economic risks. Journal MESTE, 5(2), 15-25.

[6] Barcena, M. B., & Wueest, C. 2015. *Insecurity in the Internet of Things.* https://www.symantec.com/content/en/us/enterprise/fact_sheets/b-insecurity-in-the-internet-of-things-ds.pdf