Vol. 6 No. 1. Mei 2024
P-ISSN : 2714-5789 | E-ISSN : 2986-7959
Jurnal Sains dan Sistem Teknologi Informasi (SANDI)

ANALISIS KEAMANAN *WEBSITE* TERHADAP ERANGAN *PACKET SNIFFING* DI JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER FAKULTAS TEKNIK UNIVERSITAS NEGERI MAKASSAR

[1)]Suci Rahmahdany, [2)] Mustari Lamada, [3)] Hendra Jaya
[1]Program Studi Teknik Komputer, Universitas Negeri Makassar, [2]Program Studi Pendidikan Teknik Informatika dan Komputer,Universitas Negeri Makassar, [3]Jurusan Pendidikan Teknik Elektronika,Universitas Negeri Makassar
[1]**sucirahmahdany@gmail.com**, [2]mustarilamada@unm.ac.id, [3]hendra.jaya@unm.ac.id

ABSTRACT

The Department of Informatics and Computer Engineering has several websites specially made for JTIK students with their respective benefits, such as SIMPEL, SIM-TA, IDS (Integrated Data System), Sigmatik, and SIPI. This research aims to determine the level of vulnerability to packet sniffing attacks on websites at the Department of Information and Computer Engineering, Makassar State University. This research method uses a qualitative approach by testing sniffing attacks on several Users on the targeted website. The results of the analysis of packet sniffing attack trials show that there is a potential vulnerability to data theft attempts through sniffing attack methods on wireless networks on several websites studied. In this context, the SIMPEL, IDS, and SIMTA websites can be considered relatively safe websites. In test attacks against multiple Hotspots, Users, and devices, no information could be found other than confirmation that the website was encrypted using appropriate security protocols. In reverse, the Sigmatik and SIPI websites showed a higher level of vulnerability. Sensitive data such as Usernames and passwords used during the login process can be visible in test attacks. It happens because the Sigmatik and SIPI websites still use the insecure HTTP protocol, while the SIM-TA, SIMPEL and other websites have switched to the more secure TLS/SSL or HTTPS protocol. An important recommendation resulting from this research is the need to design a monitoring and detection system that can quickly recognize potential packet sniffing attacks. It is hoped that this research can become the basis for increasing awareness and efforts on website security in the academic environment and can be applied to a broader context in the digital world.

Keywords: *Website Security, Packet sniffing Attacks, Security Analysis*

ABSTRAK

Di Jurusan Teknik Informatika dan Komputer memiliki beberapa *website* yang dibuat khusus untuk mahasiswa JTIK dengan manfaatnya masing-masing seperti SIMPEL, SIM-TA, IDS (*Integrated Data System*), Sigmatik, dan SIPI. Penelitian ini bertujuan untuk mengetahui tingkat kerentanan terhadap serangan *packet sniffing* pada *website* yang berada di Jurusan Teknik Informatika dan Komputer Universitas Negeri Makassar. Metode penelitian ini menggunakan pendekatan kualitatif dengan melakukan uji coba serangan *sniffing* terhadap beberapa *User* pada *website* yang dituju. Hasil analisis uji coba serangan *packet sniffing* menunjukkan adanya potensi kerentanan terhadap upaya pecurian data melalui metode serangan *sniffing* pada jaringan nirkabel dibeberapa *website* yang diteliti. Dalam konteks ini, *website* SIMPEL, IDS, dan SIMTA dapat dianggap sebagai *website* yang relatif aman. Dalam uji coba serangan terhadap beberapa *Hotspot*, *User*, dan perangkat, tidak ada informasi yang dapat ditemukan selain konfirmasi bahwa *website-website* tersebut telah dienkripsi menggunakan protokol keamanan yang sesuai. Sebaliknya, *website* Sigmatik dan SIPI menunjukkan tingkat kerentanan yang lebih tinggi. Data sensitif seperti *Username* dan *password* yang digunakan selama proses *login* dapat terlihat dalam uji coba serangan. Hal ini terjadi karena *website* Sigmatik dan SIPI masih menggunakan protokol HTTP yang tidak aman, sedangkan *website* SIM-TA, SIMPEL, dan lainnya telah beralih ke protokol TLS/SSL atau HTTPS yang lebih aman. Rekomendasi penting yang dihasilkan dari penelitian ini adalah perlunya perancangan sistem pemantauan dan deteksi yang dapat dengan cepat mengenali potensi serangan *packet sniffing*. Penelitian ini diharapkan dapat menjadi dasar untuk meningkatkan kesadaran dan upaya keamanan *website* dilingkungan akademik dan dapat diterapkan pada konteks yang lebih luas di dunia digital.

Kata Kunci: *Keamanan Website, Serangan Packet Sniffing, Analisis Keamanan*

Dokumen diterima pada 25-03-2024
Dipublikasikan pada 31-05-2024

I. PENDAHULUAN

Universitas Negeri Makassar adalah salah satu kampus yang memanfaatkan keberadaan *website* sebagai sumber data dan informasi untuk memudahkan mengakses informasi dan menyimpan semua data baik itu data pribadi, data mahasiswa, maupun data kampus yang bersifat tertutup. Di Jurusan Teknik Informatika dan Komputer memiliki beberapa *website* yang dibuat khusus untuk mahasiswa JTIK dengan manfaatnya masing-masing seperti SIMPEL, SIM-TA, IDS (Integrated Data System), Sigmatik, dan SIPI.

Keberadaan *website* ini sangat berguna bagi beberapa pihak. Namun, Monirruzman pada penelitiannya mengatakan bahwa tidak ada *website* yang dapat terhindar dari resiko kerentanan terhadap serangan siber. Salah satu serangan siber yang banyak terjadi didunia maya dan jarang diketahui oleh orang awam yaitu serangan packet *sniffing*.

Dengan dasar isu yang telah disebutkan, penulis merasa tertarik untuk menjalankan analisis keamanan *website* yang digunakan oleh mahasiswa, staff, serta dosen di Jurusan Teknik Informatika Fakultas Teknik Universitas Negeri Makassar. Uji coba keamanan ini dilakukan dengan tujuan untuk mengetahui tingkat kerentanan sistem keamanan *website* terhadap serangan *packet sniffing* dengan menggunakan beberapa aplikasi penganalisa jaringan seperti aplikasi *Wireshark* dan *Ettercap*. Sehingga, hasil yang diharapkan penulis yaitu dapat menggunakan *website* dengan keamanan privasi yang terjaga dari risiko serangan pemantauau paket data atau *packet sniffing* yang dapat mengancam keamanan harus data para pengguna *website* yang terhubung dijaringan nirkabel yang sama.

II. METODE PENELITIAN

A. Jenis Penelitian

Jenis penelitian ini ialah menggunakan metode eksperimental. Dimana penelitian eksperimental merupakan salah satu jenis penelitian yang mengkaji pengaruh suatu perlakuan terhadap objek untuk mengetahui akibat yang ditimbulkan (Arini, 2010). Objek yang akan diteliti akan diberikan suatu eksperimen berupa serangan *packet sniffing* menggunakan tools *Ettercap* kemudian dilakukan pengamatan terhadap kondisi-kondisi yang didapatkan dengan aplikasi *Wireshark* untuk dapat diketahui kerentanan terjadinya suatu serangan pada objek tersebut.

B. Waktu dan Tempat Penelitian

1. Waktu Penelitian

   Penelitian ini dilakukan dalam rentan waktu dari bulan Juni hingga bulan September tahun 2023.
2. Tempat Penelitian

   Penelitian dilaksanakan di Lab Jaringan Jurusan Teknik Informatika dan Komputer Fakultas Teknik Universitas Negeri Makassar.

C. Teknik Pengumpulan Data

Dalam penelitian ini, digunakan berbagai metode untuk mengumpulkan data sebagai berikut:

1. Studi literatur

   Pada tahap studi literatur, dilakukan analisis dengan cara mengumpulkan materi yang terkait dengan *website*, jaringan nirkabel/Wi-Fi, dan serangan *packet sniffing* yang bersumber dari beberapa jurnal, buku, hasil *browsing internet*, serta orang yang berpengetahuan mengenai hal tersebut.
2. Observasi

   Observasi dilakukan pada beberapa *website* yang sering digunakan mahasiswa di Fakultas Teknik Universitas Negeri Makassar diantaranya SIMPEL, SIM-TA, IDS, Sigmatik, dan SIPI.

D. Teknik Analisis Data

Peneliti menganalisis data yang diperoleh dari pengamatan dengan aplikasi *Wireshark* menggunakan pendekatan deskriptif kualitatif, dimana metode analisis ini dilakukan dengan cara membandingkan keamanan *website* dari situs yang diuji guna mencapai hasil yang akurat dari penelitian yang telah dilaksanakan.

E. Alat dan Bahan

Dibutuhkan beberapa instrumen untuk mendukung kelancaran proses penelitian ini yaitu sebagai berikut:

1. Perangkat Keras

   Dalam proses penelitian perangkat keras (hardware) yang digunakan yaitu:
   a) Laptop Asus VivoBook 14 X407MA Prosesor Intel inside RAM: 4GB
   b) Wireless Fidelity

2. Perangkat Lunak

   Dalam proses penelitian perangkat lunak (software) yang dibutuhkan yaitu:
   a) Sistem Operasi Kali Linux
   b) Aplikasi *Wireshark* (digunakan untuk serangan packet *sniffing*)

Dokumen diterima pada 25-03-2024
Dipublikasikan pada 31-05-2024

c) Aplikasi *Ettercap* (digunakan untuk serangan poisoning)
d) *website* JTIK (SIMPEL, SIM-TA, IDS Sigmatik, dan SIPI) .

III. HASIL DAN PEMBAHASAN

3.1. Hasil

Dalam penelitian ini, peneliti menggunakan dua *Hotspot* sebagai parameter serta empat akun dan perangkat sebagai target untuk memperoleh hasil penelitian yang lebih valid. Oleh karena itu, hasil penelitian direalisasikan ke dalam Tabel 3.1. *Hotspot* Broadband_UNM dan Tabel 3.2 *Hotspot* Pribadi berikut.

TABEL 3.1
HOTSPOT BROADBAND UNM

Situs web yang diuji	Akun (target)	Hasil Penelitian	Keterangan
SIMPEL	*User* 1 (192.168.1.47)	Terenkripsi	Aman
	User 2 (192.168.1.74)	Terenkripsi	
	User 3 (192.168.1.27)	Terenkripsi	
	User 4 (192.168.1.63)	Terenkripsi	
IDS	*User* 1 (192.168.1.47)	Terenkripsi	Aman
	User 2 (192.168.1.74)	Terenkripsi	
	User 3 (192.168.1.27)	Terenkripsi	
	User 4 (192.168.1.63)	Terenkripsi	
SIM-TA	*User* 1 (192.168.1.47)	Terenkripsi	Aman
	User 2 (192.168.1.74)	Terenkripsi	
	User 3 (192.168.1.27)	Terenkripsi	
	User 4 (192.168.1.63)	Terenkripsi	
Sigmatik	*User* 1 (192.168.1.47)	*Username*, dan *password*	Rentan Terhadap Serangan *Packet Snifing*
	User 2 (192.168.1.74)	*Username*, dan *password*	
	User 3 (192.168.1.27)	*Username*, dan *password*	
	User 4 (192.168.1.63)	*Username*, dan *password*	
SIPI	*User* 1 (192.168.1.47)	*Username*, dan *password*	Rentan Terhadap Serangan *Snifing*
	User 2 (192.168.1.74)	*Username*, dan *password*	
	User 3 (192.168.1.27)	*Username*, dan *password*	
	User 4 (192.168.1.63)	*Username*, dan *password*	

Pada Tabel 3.1. *Hotspot* Broadband_UNM adalah hasil uji coba serangan *packet sniffing* menggunakan *Hotspot* yang digunakan secara umum di Jurusan Teknik Informatika dan Komputer yang dilindungi oleh keamanan *Wi-Fi protected access -pre shared key* (WPA2-Personal). Sehingga, pengguna yang mengetahui *password Hotspot* tersebut dapat terhubung. Dengan bantuan aplikasi *Ettercap* dapat menampilkan perangkat atau *User* yang sedang terhubung dengan *Hotspot* Broadband_UNM, dimana dengan adanya aplikasi ini peneliti dapat menentukan target perangkat yang akan diserang. Untuk itu, peneliti melakukan beberapa skenario uji coba pada *website* dengan menggunakan perangkat yang berbeda-beda.

TABEL 3.2.
HOTSPOT PRIBADI

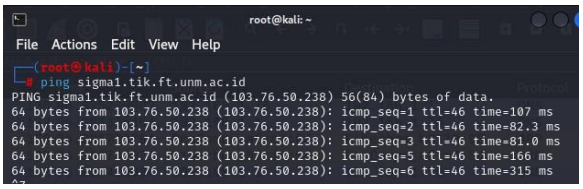
Situs web yang diuji	Akun (target)	Hasil Penelitian	Keterangan
SIMPEL	*User* 1 (192.168.45.207)	Terenkripsi	Aman
	User 2 (192.168.255.15)	Terenkripsi	
	User 3 (192.168.195.189)	Terenkripsi	
	User 4 (192.168.43.220)	Terenkripsi	
IDS	*User* 1 (192.168.45.207)	Terenkripsi	Aman
	User 2 (192.168.255.15)	Terenkripsi	
	User 3 (192.168.195.189)	Terenkripsi	
	User 4 (192.168.43.220)	Terenkripsi	
SIM-TA	*User* 1 (192.168.45.207)	Terenkripsi	Aman
	User 2 (192.168.255.15)	Terenkripsi	
	User 3 (192.168.195.189)	Terenkripsi	
	User 4 (192.168.43.220)	Terenkripsi	
Sigmatik	*User* 1 (192.168.45.207)	*Username*, dan *password*	Rentan Terhadap Serangan *Packet Snifing*
	User 2 (192.168.255.15)	*Username*, dan *password*	
	User 3 (192.168.195.189)	*Username*, dan *password*	
	User 4 (192.168.43.220)	*Username*, dan *password*	
SIPI	*User* 1 (192.168.45.207)	*Username*, dan *password*	Rentan Terhadap Serangan *Snifing*
	User 2 (192.168.255.15)	*Username*, dan *password*	
	User 3 (192.168.195.189)	*Username*, dan *password*	
	User 4 (192.168.43.220)	*Username*, dan *password*	

Pada skenario uji coba menggunakan *Hotspot* pribadi yang dilindungi oleh keamanan *Wi-Fi protected access -pre shared key* (WPA2-Personal) dimana hasil uji coba serangan ditampilkan pada Tabel 3.2. *Hotspot* Pribadi, teridentifikasi hanya sedikit yang terkoneksi dalam jaringan. Sehingga, tidak semua orang dapat terhubung dalam *Hotspot* tersebut. Meskipun demikian, pengujian serangan *sniffing* baik menggunakan *Hotspot* Broadband_UNM atau *Hotspot* pribadi, tetap menunjukkan bahwa beberapa *website* masih memiliki kerentanan terhadap jenis serangan ini. Namun, menggunakan *Hotspot* Broadband_UNM menjadi peluang besar bagi *attacker* untuk melakukan serangan *sniffing* karena banyak teridentifikasi alamat IP, dan MAC address target pada aplikasi *Ettercap*.

Dokumen diterima pada 25-03-2024
Dipublikasikan pada 31-05-2024

Untuk memeriksa paket yang berasal dari *website* SIMPEL, SIM-TA, IDS, Sigmatik, dan SIPI, diperlukan langkah penyaringan (filtering) dari data yang sudah tercatat. Sebelum menerapkan filtering, peneliti perlu mengetahui alamat IP dari ke-5 *website* tersebut yang diperoleh dari DNS pada *website*. Ini bisa dilakukan dengan melakukan langkah-langkah berikut, membuka terminal dan memasukkan perintah "#ping (nama DNS *website*)", sebagai contoh "#ping sigma1.jtik.ft.unm.ac.id", kemudian klik "Enter" di- keyboard, dan alamat IP dari sigma1.tik.ft.unm.ac.id akan muncul seperti pada Gambar 3.1 IP Address *Website* Sigmatik berikut.

GAMBAR 3.1.
IP ADDRES WEBSITE SIGMATIK



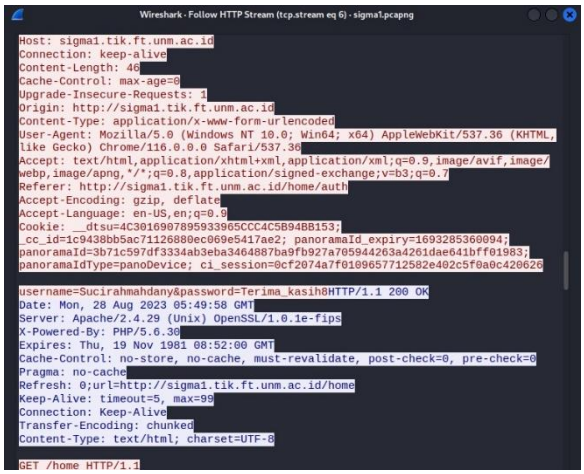
Pada Gambar 3.1 IP *Address* Sigmatik, menampilkan angka yang dilingkari dengan persegi panjang berwarna merah adalah IP address dari *website* Sigmatik, dan untuk lebih jelasnya dipaparkan pada Tabel 3.3. IP *Address Website* JTIK. Setelah mengetahui bahwa IP address dari *website-website* tersebut, Tahap selanjutnya adalah melakukan penyaringan paket berdasarkan IP Address menggunakan bilah filter yang terdapat di bawah ikon aplikasi *Wireshark*. Ini dapat dilakukan dengan memasukkan perintah "ip.addr==(IP Address *website*)". Sebagai contoh untuk *website* Sigmatik "ip.addr==103.76.50.238", akan menghasilkan tampilan paket-paket yang berkaitan dengan alamat IP tersebut.

TABEL 3.3.
IP ADDRESS WEBSITE JTIK

Website	DNS (*Domain Name System*)	IP *Address*
SIMPEL	simpel.jtik.ft.unm.ac.id	103.76.50.235
SIM-TA	simta.jtik.ft.unm.ac.id	103.76.50.235
IDS	ids.tik.ft.unm.ac.id	103.76.50.235
Sigmatik	sigma1.tik.ft.unm.ac.id	103.76.50.238
SIPI	Sipi.jtik.ft.unm.ac.id	103.76.50.235

Untuk melakukan analisis pada paket data yang menggunakan protokol HTTP seperti *website* Sigmatik dan SIPI, dapat dilakukan dengan meng-klik kanan paket data pada *listing packet* panel yang ingin dianalisis, setelah itu pilih "*Follow* HTTP *Stream*". Dalam Gambar 3.2. Isi *Packet Follow* HTTP *Stream website* Sigmatik, ditampilkan rincian paket data protokol HTTP yang membawa informasi "POST''.

GAMBAR 3.2.
ISI PACKET FOLLOW HTTP STREAM WEBSITE SIGMATIK



Dari Gambar 3.2. Isi *Packet Follow* HTTP *Stream website* Sigmatik menampilkan bahwa dalam rincian paket data protokol HTTP terdapat dua jenis warna teks yang berbeda. Teks dengan warna merah menunjukkan adanya permintaan HTTP (HTTP request), sementara teks yang berwarna biru menunjukkan tanggapan HTTP (HTTP *response*).

Konten dari paket data yang berlabel "POST" berisi berbagai jenis informasi, termasuk data rahasia seperti *Username* dan *password*. Selain itu, dalam rincian paket data tersebut, peneliti dapat menganalisis beberapa informasi seperti pada Tabel 3.4. Hasil Identifikasi paket data *Website* Sigmatik berikut.

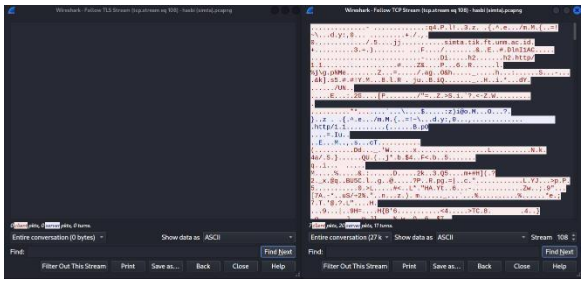
Dokumen diterima pada 25-03-2024
Dipublikasikan pada 31-05-2024

TABEL 3.4.
HASIL IDENTIFIKASI PAKET DATA WEBSITE SIGMATIK

Website	Informasi	Hasil Analisis	Keterangan
Sigmatik	POST	-	Memberitahukan bahwa *client* melakukan sebuah permintaan dengan menggunakan isi pesan untuk mengirim data ke *server web*.
	Host	sipi.jtik.ft.unm.ac.id	Menunjukkan bahwa *client* sedang terkoneksi dengan sipi.jtik.ft.unm.ac.id
	Connection	*Keep-alive*	Suatu parameter yang menentukan batas waktu maksimal saat koneksi terputus dan jumlah permintaan maksimum.
	Content-Type:	application/x-www-form-urlenconded; charset=UTF-8.	*Client* mengirimkan data melalui *Form Uniform Resource Locator* (URL)
	User-Agent:	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, *Like Gecko*) Chrome/116.0.0.0 Safari/537.36.	Menyatakan kemungkinan *Web Browser* yang sedang digunakan oleh *client*.
	Accept-Encoding	gzip,deflate	Menunjukkan metode kompresi yang digunakan oleh *client* yaitu gzip atau *deflate*.
	Accept-Language	en-US, en ; q=0.9	Menunjukkan Bahasa yang diterima oleh server adalah Bahasa Inggris
	HTTP/1.1 200 OK.	-	Menyatakan permintaan telah berhasil dieksekusi.
	Date	Mon, 28 Aug 2023 05:49:58 GMT	Menunjukkan waktu ketika server mengirimkan data tersebut.
	Server	*Apache*	Jenis server yang digunakan yaitu *Apache*.

Sedangkan untuk melakukan analisis pada paket data yang memiliki lapisan keamanan seperti *website* SIMPEL, SIM-TA, dan IDS, dapat dilakukan dengan klik kanan paket data pada panel daftar paket yang ingin dianalisis, setelah itu pilih "*Follow* TLS *Stream*". Gambar 3.3. Isi Paket Data Follow TLS Stream dan TCP Stream *Website* SIM-TA dibawah ini adalah contoh tampilan rincian paket data protokol TLS yang membawa informasi "*Application Data''*.

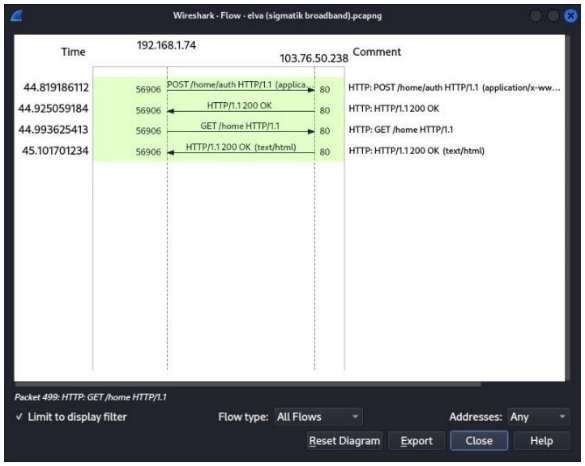
GAMBAR 3.3
ISI PAKET DATA FOLLOW TLS STREAM DAN TC STREAM WEBSITE SIM-TA



Dalam Gambar 3.3 Isi Paket Data Follow TLS Stream dan TCP Stream *Website* SIM-TA, menampilkan "Follow TLS Stream" dan "Follow TCP Stream" dari data yang telah dipilih. Dari rincian data protokol TLS tersebut, tidak ada informasi yang dapat ditemukan. Oleh karena itu, peneliti menganalisis paket data yang sama dengan cara mengklik kanan pada paket data yang akan dianalisis. dan memilih "Follow TCP Stream". Namun, hasilnya peneliti tidak dapat dengan mudah menganalisis informasi karena yang dikirim telah melalui proses enkripsi.

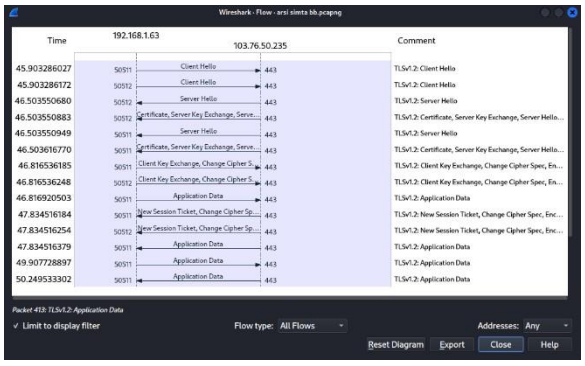
Pemeriksaan proses komunikasi data yang terjadi ketika korban mengakses *website* Sigmatik dan SIPI, dengan mengklik "Statistic" dimenu bar dan memilih "Flow Graph''.

GAMBAR 3.4
PROSES KOMUNIKASI DATA DATA CLIENT DAN SERVER PADA PROTOKOL HTTP



dan Server pada Protokol HTTP, menampilkan proses pertukaran data antara klien dengan *User* 2 IP address 192.168.1.47 dan server yaitu sigma1.tik.ft.unm.ac.id dengan IP address 103.76.50 238.

GAMBAR 3.5.
PROSES KOMUNIKASI DATA DATA CLIENT DAN SERVER PADA PROTOKOL HTTPS



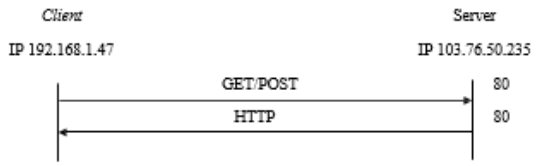
Pada Gambar 4.27 Proses Komunikasi Data *Client* dan Server pada Protokol HTTPS, menampilkan proses pertukaran data antara klien dengan *User* 4 IP address 192.168.1.63 dan server yaitu simta.tik.ft.ac.id dengan IP address 103.76.50.235 dan melalui gateway 192.168.1.1.

3.2. Pembahasan

Hasil dari pengujian serangan *packet sniffing* dalam penelitian ini mengindikasikan bahwa beberapa *website* di Jurusan Teknik Informatika dan Komputer UNM memiliki potensi kerentanan terhadap upaya pencurian data dengan menggunakan metode serangan *sniffing* pada jaringan nirkabel. Pada *website* SIMPEL, IDS, dan SIMTA dapat diklasifikasikan sebagai *website* yang aman, karena dalam pengujiannya dalam menyerang beberapa User dan perangkat, *website* tersebut tidak dapat ditemukan informasi apapun, selain informasi bahwa *website-website* tersebut terenkripsi. Berbeda halnya dengan *website* Sigmatik, dan SIPI, peneliti dapat melihat data penting User seperti Username dan password pada saat melakukan aktivitas login. Hal tersebut disebabkan karena beberapa *website* seperti Sigmatik, dan SIPI masih menggunakan protokol HTTP, sedangkan *website* SIM-TA, SIMPEL, dan menggunakan protocol TLS atau HTTPS. Perbedaan utamanya terletak pada cara kerjanya.

Dilihat dari Gambar 4.26 Proses Komunikasi data *Client* dan Server pada Protokol HTTP, secara simpelnya, proses komunikasi data pada *website* yang menggunakan protokol HTTP seperti Sigmatik, dan SIPI dijelaskan dalam Gambar 4.28 Proses Komunikasi Data *Website* Sigmatik dan SIPI berikut.

GAMBAR 3.4.
IP ADDRES WEBSITE SIGMATIK



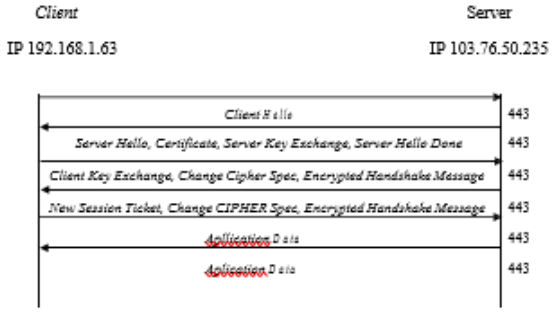
Dalam Gambar 4.28 Proses Komunikasi Data *Website* Sigmatik dan SIPI, Menggambarkan proses pertukaran data antara klien dan server *website* Sigmatik, dan SIPI secara sederhana. Terlihat bahwa ketika *client* meminta data dari web server terdapat dua pilihan yang tersedia yakni menggunakan metode GET atau menggunakan metode POST.

Pada saat *client* melakukan permintaan dengan menentukan parameter dibagian Uniform Resource Locator (URL), maka metode permintaan HTTP yang digunakan adalah GET. Contohnya adalah URL yang ada pada halaman web. Disisi lain, jika *client* melakukan permintaan dengan mengirimkan data ke server web melalui badan pesan, metode permintaan mengirimkan respon HTTP ke *client* yang berisi data yang diminta dalam bentuk teks biasa.

Situasi berbeda terjadi pada *website* SIM-TA, SIMPEL, dan IDS. Ketika target mengakses *website* tersebut melalui browser, browser tersebut sebagai *client* akan meminta data dari server. Namun, server tidak mengirimkan data yang diminta secara langsung. Hal ini terjadi karena klien dan server akan melakukan komunikasi awal untuk memverifikasi identitasnya terlebih dahulu. Lalu dilakukan perundingan mengenai kode privasi sebelum komunikasi data dilakukan. Oleh karena itu, ketika proses dalam *sniffing* dilakukan, data yang melalui kompter attacker tidak dapat dengan mudah terbaca dalam aplikasi Wireshark, seperti yang tampak dalam Gambar 3.4 Isi Paket Data Follow TLS Stream dan TCP Stream *Website* SIM-TA.

Dalam Gambar 3.5 Proses Komunikasi Data *Client* dan Server pada Protokol HTTPS, secara simpelnya, proses komunikasi data pada *website* yang menggunakan protokol HTTPS pada *website* SIM-TA, SIMPEL, dan IDS digambarkan seperti berikut.

GAMBAR 3.5.
PROSES KOMUNIKASI DATA PROTOKOL HTTPS PADA WEBSITE KE SIM-TA



Gambar 3.5 Proses Komunikasi Data Protokol HTTPS Pada *Website* SIM-TA, menggambarkan proses komunikasi yang sederhana antara *client* dengan server *website* SIM-TA. Pada gambar tersebut terlihat *Client* mengirimkan permintaan "*Client* Hello" kepada server. Kemudian, Server membalas dengan mengirimkan pesan "Server Hello" kepada *client* dan mengikutsertakan kunci publik server untuk HTTP yang digunakan adalah POST. Contohnya adalah saat mengisi formulir Username dan password pada halaman web. Setelah itu, server akan melaksanakan pertukaran kunci publik dengan *client*. Selain itu, server juga mengirimkan sertifikatnya kepada *client* sebagai

Dokumen diterima pada 25-03-2024
Dipublikasikan pada 31-05-2024

bagian dari proses otentikasi. Setelah itu, server membalas pesan dengan "Server hello done". Apabila sertifikat tersebut telah diterbitkan oleh salah satu otoritas sertifikasi atau CA (Certification Authority) yang terpercaya dan terdaftar dalam daftar CA yang diakui oleh web browser, maka *client* dapat menverifikasi public key server. Selanjutnya, ketika *client* mengirimkan pemberitahuan "Change Cipher Spec" kepada server untuk menandakan bahwa *client* akan memulai penggunaan public key untuk melakukan enkripsi pesan. Setelah itu, server memulai sesi baru dengan mengirimkan notifikasi "Change Cipher Spec" ke *client* menunjukkan bahwa server akan memulai menggunakan tiket sesi yang mencakup semua pesan yang telah dibahas sebelumnya dan akan mengenkripsinya dengan *secret key* yang hanya diketahui oleh server. Selanjutnya, *client* dan server kemudian bisa bertukar data aplikasi melalui saluran yang aman yang telah dibuat oleh keduanya.

Setelah menyelesaikan transmisi data, jika *client* ingin meminta data tambahan dari server, *client* akan mengirim pesan "*Client* Hello" dengan menggunakan ID sesi dari sesi sebelumnya. Kemudian, server akan memeriksa *session cache* untuk mencocokkan ID sesi tersebut. Jika ada kesamaan yang ditemukan, server dapat melanjutkan sesi dan mengirim pesan "Server Hello". Setelah itu, *client* dan server akan melakukan pertukaran pesan "Change Cipher Spec". Dengan langkah-langkah ini, *client* dan server bisa mengirim data aplikasi melalui saluran yang aman yang telah ditetapkan sebelumnya

a. Solusi Untuk Mencegah Serangan Packet *Sniffing*

Penulis telah menyusun beberapa saran yang dapat dijadikan sebagai langkah yang dapat diambil untuk meningkatkan tingkat keamanan *website* terhadap jenis serangan *packet sniffing* pada kedua platform ini.

1. Pengguna *Website*
   a) Menerapkan keamanan enkripsi WPA2-PSK pada *hotspot* untuk meningkatkan keamanan. Dengan menerapkan keamanan tersebut, hanya penguna yang memiliki akses yang dapat mengakses jaringan. Sehingga, serangan *sniffing* oleh pihak yang tidak berwenang dapat cegah.
   b) Menghindari pengaksesan akun atau mengirim data sensitif saat menggunakan jaringan *hotspot* umum atau *hotspot* yang kata sandinya banyak yang tahu. Hal ini dapat menjadi peluang lebih besar untuk menjadi target serangan *sniffing*.
2. Pengembang Situs Web

Melakukan penerapan sertifikat SSL pada *website* Sigmatik dan SIPI. Dengan mengaktifkan sertifikat SSL, informasi yang bersifat rahasia akan tetap terlindungi saat dikirim melalui internet karena akan diubah menjadi format terenkripsi. Akibatnya, hanya penerima pesan yang memiliki kunci dekripsi yang dapat membaca isi pesan tersebut setelah melewati proses enkripsi. Tindakan ini menjadi sangat penting karena pada saat data dikirimkan melalui perjalanan ke beberapa komputer sebelum mencapai server tujuan. Jika tidak ada enkripsi dengan sertifikat SSL, perangkat lain yang berada di antara komputer pengguna dan server dapat mengakses data sensitif seperti nama pengguna dan kata sandi.

IV. KESIMPULAN

Dari temuan yang diungkapkan dalam penelitian ini, dapat diambil kesimpulan sebagai berikut:

1. Tingkat keamanan *website* di Jurusan Teknik Informatika dan Komputer masih memerlukan peningkatan pada *website* Sigmatik, dan SIPI. Hal ini terbukti karena *website* tersebut rentan terhadap serangan *packet sniffing*yang memiliki kemampuan untuk merekam dan menampilkan informasi sensitif seperti *Username* dan *password* saat proses *login* dilakukan menggunakan aplikasi *Wireshark*. Pada *website* Sigmatik, dan SIPI belum menerapkan sertifikat SSL seperti *website* SIMPEL, SIM-TA, dan IDS. Oleh karena itu, sangat rentan terhadap serangan packet *sniffing*, meskipun jika *User* menggunakan versi terbaru dari *browser*.
2. Hasil identifikasi dari serangan *packet sniffing* pada *website* di Jurusan Teknik Informatika dan Komputer yaitu mendapatkan informasi berupa jenis koneksi dan protokol yang digunakan, jenis pesan seperti POST dan GET, jenis *port*, *host* atau server, jenis *browser* yang digunakan, Bahasa, jenis server yang digunakan, serta yang paling penting informasi data sensitif seperti *Username* dan *password User*.

V. SARAN

Berdasarkan uraian dari kesimpulan, maka kelemahan yang telah diidentifikasi dapat dijadikan sebagai pengalaman dan referensi untuk kedepannya. Untuk itu, rekomendasi dari penulis untuk penelitian selanjutnya yaitu dapat merancang sistem pemantauan dan deteksi yang dapat dengan cepat mengenali potensi serangan packet *sniffing*, sehingga langkah-langkah untuk menangani masalah tersebut dapat segera ditindak lanjuti, seperti implementasi Intrusion Prevention System (IPS) yang dirancang untuk mendeteksi serangan, serta dapat mengambil tindakan pencegahan untuk memblokir serangan tersebut secara otomatis.

Dokumen diterima pada 25-03-2024
Dipublikasikan pada 31-05-2024

DAFTAR PUSTAKA

[1] Lamada, M. S., Miru, A. S., & Amalia, R.-. (2020). Pengujian Aplikasi Sistem Monitoring Perkuliahan Menggunakan Standar ISO 25010. Jurnal MediaTIK, 3(3). https://doi.org/10.26858/jmtik.v3i3.15172

[2] Arini, N. E. (2010). Bahan Ajar: Materi Psikologi Eksperimen.(bab 3. Jwnis penelitian)

[3] Kurniawan, T. A. (2020). Analisa Keamanan Jaringan Wi-Fi Terhadap Serangan Packet *Sniffing*. Jurnal Ilmiah Fakultas Teknik LIMIT'S, 16(2), 11-15

[4] Siahan, A. P U. (2018). Pelanggaran Cybercriem dan kekuatan yurisdiksi di Indonesia. Jurnal Teknik dan Informatika, 5(1), 6-9.

[5] Syahab, A. S., Ujianto, E. I. H., & Rianto, R. (2023). Penggunaan Wireshark Dan Nessus Untuk Analisis Ssl/Tls Pada Keamanan Data Pengguna *Website*. Jika (Jurnal Informatika) 7(2) 183 https://doi.org/10.31000/jika.v7i2.7566

[6] Syaifuddin, M., Andika, B., & Ginting, R. I. (2017). Analisis Celah Keamanan protocol TCP/IP. Jurnal ilmiah SAINTIKOM, 16 (2), 130-135.

[7] Wati, E. S., & Apriansyah, D. (2019). Sistem Keamanan Jaringan Wireless Menggunakan Peap Mas Chap. Jurnal ONESISMIK, 1(1), 1-9.

Dokumen diterima pada 25-03-2024
Dipublikasikan pada 31-05-2024