Analisis Keamanan Data Dalam Jaringan Terhadap Kegiatan Sniffing Menggunakan Serangan Man In The Midle Attack

Aditya Dyan Nugraha[1], Husaini[2], Anwar[3]

1 2 3 Jurusan Teknologi Informasi dan Komputer Politeknik Negeri Lhokseumawe
Jln. B.Aceh Medan Km.280 Buketrata 24301 INDONESIA

[1]aditya.dyan@hotmail.com

[2]husaini@pnl.ac.id

[3]anwar@pnl.ac.id

Abstrak— ***Man in the midle attack* (*MITM*) merupakan jenis serangan *hacking* yang tergolong ke dalam kategori *sniffing*, serangan *MITM* berjalan pada jaringan lokal yang dapat "menyadap" segala jenis kegiatan korban di *internet*. Serangan MITM sering terjadi pada jaringan *free-wifi*, karena pada jaringan *free-wifi* semua orang dapat saling terhubung dengan bebas. Serangan MITM dapat bekerja pada *website* yang menggunakan *port* 80 dan *port* 443, hanya saja pada website yang menggunakan *port* 443 harus di *bypass* ke *port* 80 terlebih dahulu agar serangan sukses dijalankan. Selama ini penyedia jaringan *free-wifi* tidak begitu memperhatikan tingkat keamanan pengguna layanannya, seringkali ditemukan sistem keamanan pada layanan *free-wifi* hanya sebatas memberikan *password* pada *access point*. Sistem keamanan pada penelitian ini menggunakan 2 teknik pengamanan, yaitu *iptables* dan *intrussion detection system* (*IDS*). Penggunaan *iptables* berguna untuk memblokir segala *request* yang mengarah ke *port* 80, sedangkan penggunaan *IDS* berguna untuk memonitoring jaringan dari jenis serangan *port scanning*, jika *port scanning* terdeteksi oleh *IDS*, maka *IDS* akan memberikan pesan notifikasi *telegram* kepada adminstrator jaringan.**
Kata Kunci— *MITM, free-wifi, port scanning, IDS, iptables*

Abstract— **Man in the midle attack (MITM) is a type of hacking attack that belongs to the sniffing category, MITM attacks run on local networks that can "sniff" all types of victim activities on the internet. MITM attacks often occur on free-wifi networks, because on the free-wifi network everyone can be connected freely. The MITM attack can work on websites that use port 80 and port 443, only on websites that use port 443 must be bypassed to port 80 first so that a successful attack is carried out. During this time free-wifi network providers did not pay much attention to the level of security of users of their services, often found a security system on free-wifi services only limited to providing passwords on the access point. The security system in this study uses 2 security techniques, namely iptables and intrussion detection system (IDS). The use of iptables is useful for blocking all requests leading to port 80, while the use of IDS is useful for monitoring the network from the type of port scanning attack, if the scanning port is detected by IDS, then the IDS will give the telegram notification message to the network administrator.**
Keywords— *MITM, free-wifi, port scanning, IDS, iptables*

I. PENDAHULUAN

Tingkat pertumbuhan penggunaan teknologi terus mengalami peningkatan secara signifikan, salah satunya yang mengalami peningkatan ialah penggunaan *internet*, saat ini sangat mudah sekali menemukan tempat – tempat yang menyediakan fasilitas jaringan *wi-fi* secara gratis, baik itu di warung kopi, rumah sakit, taman, sekolah, dan tempat – tempat umum lainnya.

Tentunya dengan bertebaran tempat – tempat tersebut memiliki dampak postif dan negatif. Salah satu dampak positif dengan adanya layanan *free wi-fi* ialah dapat menunjang mobilitas pengguna teknologi dalam melakukan berbagai kegiatannya. Namun tanpa disadari dampak negatif dari bertebarannya layanan *free wi-fi* terus menghantui para pengguna layanan *wi-fi* ditempat umum. Salah satu dampak negatif dari layanan *wi-fi* ditempat umum ialah tingginya tingkat kerentanan keamanan data terhadap kasus *hacking*, hal inilah yang dicoba untuk dimanfaatkan oleh segelintir oknum untuk meraup keuntungan secara pribadi.

Man in the middle attack merupakan salah satu teknik *hacking* yang dilancarkan oleh seorang *hacker* untuk malakukan kegiatan *sniffing*, *spoofing*, *interception*, *modification*, *fabrication* pada suatu jaringan.

Dari permasalahan diatas, maka penulis bekeinginan untuk membuat tugas akhir dengan judul "Analisis Tingkat Keamanan Data Dalam Jaringan Terhadap Kegiatan Sniffing Menggunakan Serangan Man In The Midle Attack". Pada saat pengujian serangan, penulis akan menggunakan 3 tools yang berbeda, nantinya nama dari masing –masing tools akan penulis samarkan untuk mencegah pihak lain untuk melakukan tindakn hacking. Selanjutnya penulis akan mengimplementasikan sistem keamanan jaringan dengan menggunakan 2 teknik pengamanan, yaitu iptables dan intrusssion detection system (IDS).

Berdasarkan permasalahan yang telah diuraikan sebeleumnya, maka rumusan masalah yang dapat dirumuskan, yaiut:

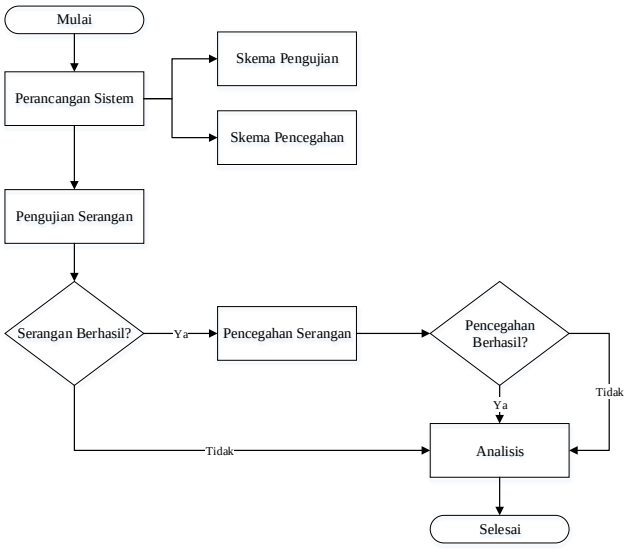
1) Bagaimana tingkat keberhasilan serangan MITM dengan menggunakan tools jenis A, B, dan C terhadap website yang menggunakan HTTP?
2) Bagaimana mengkonfigurasikan iptables dan IDS sebagai sistem keamanan access point?
3) Bagaimanan tingkat keberhasilan dalam mencegah kegiatan sniffing dengan menggunakan iptables dan IDS?

Adapun tujuan dari penelitian ini adalah untuk menguji tingkat keamanan website dengan menggunakan 3 jenis tools yang berbeda, serta untuk mengimplementasikan sistem keamanan pada jaringan access point dengan menggunkan iptables dan IDS.

II. METODOLOGI PENELITIAN

Tahapan Penelitian

Tahapan pengerjaan penelitian yang akan dilakukan, dapat dilihat pada gambar 1 di bawah ini:



Gambar 1. Tahapan Penelitian

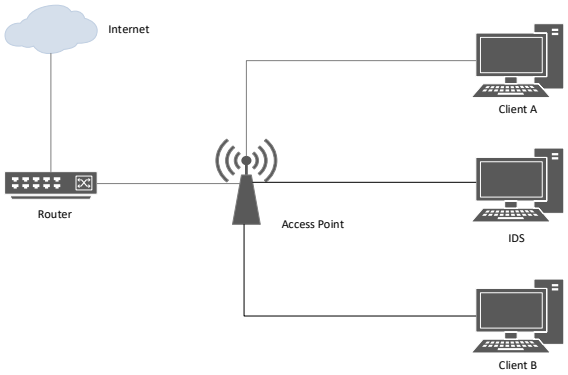
Pada gambar tahapan penelitian diatas, tahapan perancangan sistem dilakukan untuk menentukan kebutuhan peralatan/komponen baik itu perangkat lunak (software) maupun perangkat keras (hardware) yang hendak digunakan didalam penelitian. Selain itu agar peneliti dapat dengan mudah melakukan pengujian (penyerangan dan pencegahan) dengan mengacu terhadap skema yang telah dibuat.

Setelah tahapan perancangan sistem, kemudian dilanjutkan ke tahapan kedua, yakni pengujian serangan, pada tahapan ini peneliti melancarakan serangan man in the middle attack dengan beberapa skenario terhadap beberapa jenis atau kategori website yang telah ditentukan. Jika pengujian serangan tidak berhasil, maka peneliti akan melakukan analisis, namun, jika pengujian serangan berhasil, maka peneliti akan masuk ke tahapan ketiga.

Pada tahap ketiga ini, peneliti akan melakukan pencegahan terhadap serangan tersebut, jika pencegahan yang dilakukan berhasil / tidak berhasil, maka peneliti akan melakukan analisis.

Environment Pengujian

Environment (linkungan) pengujian disesuaikan berdasarkan desain arsitektur jaringan yang biasa digunakan di tempat – tempat umum, adapun desain arsitektur jaringan yang digunakan pada tempat – tempat umum dapat dilihat pada gambar 2.



Gambar 2. Arsitektur Jaringan

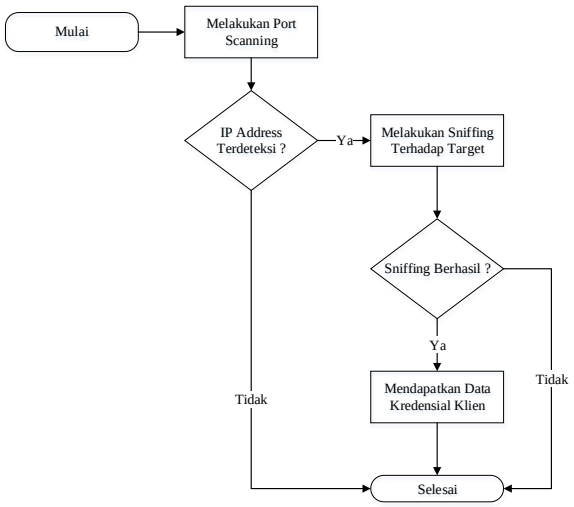
Pada gambar diatas menunjukkan arsitektur jaringan yang akan digunakan pada penelitian ini. Kedua klien akan terkoneksi dengan sebuah access point yang mana pada access point tersebut telah memiliki system hotspot yang akan mengatur autentikasi koneksi ke setiap klien. Access point tersebut terhubung langsung dengan router yang dihubungkan dengan internet, sehingga klien dapat berselancar di dunia maya.

Perancangan Sistem

Perancangan sistem pada penelitian ini disesuaikan dengan environment pengujian yang telah dijabarkan pada gambar 2. Nantinya beberapa sistem yang digunakan dalam pengujian ini menggunakan mesin virtual, guna untuk memperkecil anggaran yang akan dikeluarkan, walaupun menggunakan mesin virtual, kinerja dari sistem tersebut tetaplah sama dengan sistem yang sebenarnya.

Alur Pengujian Serangan

Alur pengujian serangan merupakan sebuah tahapan yang penulis lakukan dalam melakukan pengujian serangan, adapun tahapan – tahapannya dapat dilihat pada gambar 3 berikut.



Gambar 3. Diagram Alir Serangan

Skenario Pengujian

Pada penelitian kali ini, penulis menggunakan 4 jenis skenario pengujian, dimana skenario pengujian yang pertama ini akan menguji keamanan protokol HTTPS pada beberapa kategori situs web yang telah ditentukan dengan cara mengetikkan alamat situs web pada url box tanpa menggunakan protokol di komputer / laptop korban.

Selanjutnya pada skenario pengujian kedua ini tidak jauh berbeda dengan skenario pengujian yang pertama, hanya saja pada skenario pengujian yang kedua ini, korban akan mengetikkan alamat situs web pada url box dengan menggunakan protokol HTTPS.

Kemudian, pada skenario ketiga ini, penulis akan menguji sistem keamanan / pencegahan serangan man in the middle attack dengan memblokir seluruh situs yang menggunakan protokol HTTP dengan menggunakan IP Tables.

Pada skenario pengujian yang keempat ini, penulis akan menerapkan dan menguji sistem keamanan / pencegahan serangan man in the middle attack dengan mengimplementasikan intrussion detection system (IDS) menggunakan snort pada jaringan wireless local area network. Nantinya ketika attacker melakukan port scanning ia langsung terdeteksi oleh snort, selanjutnya snort akan menyimpan log serangan tersebut kedalam database, kemudian snort akan mengirimkan notifikasi melalui telegram kepada network administrator untuk memberitahu bahwa telah terjadi port scanning yang dilakukan oleh salah satu pengguna terhadap jaringan wireless local area network.

III. HASIL DAN PEMBAHASAN

Pengujian Serangan Website

Pengujian serangan pada 6 jenis website yang dilakukan pada penelitian kali ini menggunakan 2 buah skenario, yaitu mengakses website dengan menggunakan protokol HTTPS dan mengakses website tanpa menggunakan protokol sama sekali. Pada pengujian ini juga, penulis menggunakan 3 jenis tools yang berbeda untuk mengetahui tingkat keefektifan masing – masing tools dalam melakukan serangan MITM. Pengujian ini bertujuan untuk mengetahui tingkat keamanan sebuah website dalam menjaga data – data penggunanya dari tindakan hacking serta untuk mengetahui website mana saja yang masih menggunakan port 80 (HTTP). Berikut ini hasil dari pengujian yang penulis ringkas kedalam tabel I.

Tabel I
Pengujian Website Tanpa Menggunakan Protokol (Tool A)

No	Kategori Website	URL Website	Tools A				Keterangan
			Username	Password	Beralih ke HTTPS	URL Berubah	
1	Email	outlook.com	Ya	Ya	Tidak	weboutlook.com	Berhasil
2		yahoo.com	Ya	Tidak	Tidak	webid.yahoo.com	Gagal
3	Internet Banking	klikbca.com	Ya	Ya	Tidak	webklikbca.com	Berhasil
4		ib.bankmandiri.coid	Ya	Ya	Ya	webib.bankmandiri.co.id	Berhasil
5	Online Shop	shopee.com	Ya	Terenkripsi	Tidak	webshopee.com	Berhasil
6		bukalapak.com	Ya	Ya	Tidak	webbukalapak.com	Berhasil
7	Portal Berita	detik.com	Ya	Ya	Tidak	webdetik.com	Berhasil
8		viva.com	Ya	Ya	Tidak	webviva.co.id	Berhasil
9	Sosial Media	facebook.com	Tidak	Tidak	Ya	Tidak berubah	Gagal
10		Instagram.com	Tidak	Tidak	Tidak	webinstagram.com	Gagal

Pengujian pada table 1 dilakukan dengan menggunakan tool A, dari pengujian tersebut dapat diketahui bahwa tidak semua website dapat di serang dengan menggunakan tool A. Penulis juga mendapatkan fakta bahwa dari keseluruhan website yang diserang hanya facebook.com yang tidak dapat diserang sepenuhnya, sementara yahoo.com dan instagram.com dapat di bypass protokol HTTPS-nya, hanya saja pada saat menguji website instagram.com, penulis mendapati bahwa website tidak menampilkan data apapun (baca: blank), khusus pada website yahoo.com pada session password, browser meminta untuk mengaktifkan cache browser, sehingga penulis hanya mendapatkan username saja. Berdasarkan data pada table I, maka penulis dapat menghitung nilai rata – rata keberhasilan yang diperoleh dari serangan menggunakan tool A.

$$RB = \frac{Jumlah\ Keberhasilan\ Serangan}{Jumlah\ Website}\ x\ 100\%$$

$$RB = \frac{7}{10}\ x\ 100\%$$

$$RB = 70\%$$

Dari perhitungan diatas, maka diperoleh persentase nilai rata – rata keberhasilan serangan menggunakan tool A terhadap 10 website pada tabel 1 ialah 70%.

Tabel II
Pengujian Website Tanpa Menggunakan Protokol (Tool B)

No	Kategori Website	URL Website	Tools B				Keterangan
			Username	Password	Beralih ke HTTPS	URL Berubah	
1	Email	outlook.com	Ya	Ya	Tidak	Tidak berubah	Berhasil
2		yahoo.com	Tidak	Tidak	Ya	Tidak berubah	Gagal
3	Internet Banking	klikbca.com	Ya	Ya	Tidak	Tidak berubah	Berhasil
4		ib.bankmandiri.coid	Ya	Ya	Tidak	Tidak berubah	Berhasil
5	Online Shop	shopee.com	Ya	Terenkripsi	Tidak	Tidak berubah	Berhasil
6		tokopedia.com	Ya	Ya	Tidak	Tidak berubah	Berhasil
7	Portal Berita	detik.com	Ya	Ya	Tidak	Tidak berubah	Berhasil
8		viva.com	Ya	Ya	Tidak	Tidak berubah	Berhasil
9	Sosial Media	facebook.com	Tidak	Tidak	Ya	Tidak berubah	Gagal
10		instagram.com	Ya	Ya	Tidak	Tidak berubah	Berhasil

Pada tabel II penulis melakukan penyerangan dengan menggunakan tool B. Dari hasil tabel 2 terjadi beberapa perubahan data jika dibandingkan dengan serangan menggunakan tool A. Website yang mengalami perubahan ialah instagram.com. Dimana pada website instagram.com

yang pada pengujian pertama penulis mendapati bahwa website tidak menampilkan data apapun, namun pada pengujian ini website dapat menampilkan form login. Dari tabel II diatas dapat dihitung persentase keberhasilan serangan menggunakan tool B, yaitu:

$$RB = \frac{Jumlah\ Keberhasilan\ Serangan}{Jumlah\ Website}\ x\ 100\%$$

$$RB = \frac{8}{10}\ x\ 100\%$$

$$RB = 80\%$$

Persentase nilai rata – rata keberhasilan serangan menggunakan tool B lebih tinggi dibandingkan dengan menggunakan tool A, yaitu 80%.

Selanjutnya penulis melanjutkan pengujian serangan menggunakan tool C, dari pengujian tersebut, penulis mendapatkan hasil yang dapat dilihat pada tabel 3 berikut.

Tabel III
Pengujian Website Tanpa Menggunakan Protokol (Tool C)

No	Kategori Website	URL Website	Tools C				Keterangan
			Username	Password	Beralih ke HTTPS	URL Berubah	
1	Email	outlook.com	Tidak	Tidak	Tidak	wwwww.oulook.com	Gagal
2		yahoo.com	Tidak	Tidak	Tidak	Tidak berubah	Gagal
3	Internet Banking	klikbca.com	Ya	Ya	Tidak	wwwww.klikbca.com	Berhasil
4		ib.bankmandiri.coid	Tidak	Tidak	Tidak	wwwww.ib.bankmandiri.coid	Gagal
5	Online Shop	shopee.com	Ya	Terenkripsi	Tidak	wwwww.shopee.com	Berhasil
6		tokopedia.com	Ya	Ya	Tidak	wwwww.tokopedia.com	Berhasil
7	Portal Berita	detik.com	Ya	Ya	Tidak	wwwww.detik.com	Berhasil
8		viva.com	Ya	Ya	Tidak	wwwww.viva.co.id	Berhasil
9	Sosial Media	facebook.com	Tidak	Tidak	Ya	Tidak berubah	Gagal
10		instagram.com	Ya	Ya	Tidak	wwwww.instagram.com	Berhasil

Hasil dari pengujian pada tabel 3 mengalami perubahan yang cukup signifikan, dimana pada dua pengujian sebelumnya, yaitu pada website outlook.com, ib.bankmadiri.co.id penulis berhasil mendapatkan data kredensial pengguna, namun pada pengujian dengan menggunakan tool C ini penulis tidak berhasil mendapatkan data kredensial pengguna. Dari data pada tabel 3 maka penulis dapat mencari nilai persentase dari pengujian dengan menggunakan tool C ini.

$$RB = \frac{Jumlah\ Keberhasilan\ Serangan}{Jumlah\ Website}\ x\ 100\%$$

$$RB = \frac{6}{10}\ x\ 100\%$$

$$RB = 60\%$$

Dari perhitungan diatas, maka dapat diketahui bahwa nilai persentase keberhasilan dari menggunakan tool C terhadap 10 website yang diuji diatas ialah 60%.

Pengujian Tools Serangan

Seperti yang dapat dilihat pada tabel 1, 2, dan 3, masing – masing *tools* memiliki tingkat persentase keberhasilan yang berbeda – beda, oleh karena itu, pada sub – subbab ini, penulis akan meneliti *tools* yang mana saja yang dapat digunakan untuk melakukan serangan *MITM* berdasarkan keefetifitasannya. Berikut hasil perbandingan tools serangan yang dapat dilihat pada tabel 4.

Tabel IV
Perbandingan Tools Serangan

No.	Tools Serangan	Persentase Keberhasilan	Perubahan URL	Kesulitan Membaca Hasil Serangan
1.	A	70%	web	Sedang
2.	B	80%	Tidak ada	Sulit
3.	C	60%	wwwww	Mudah

Dari tabel 4 diatas dapat di analisa bahwa, tools yang memiliki tingkat keberhasilan yang tertinggi ialah tool B, sedangkan tools A memiliki tingkat keberhasilan sebesar 70% dan tools C memiliki persentase keberhasilan sebesar 60%. Jika dilihat dari perubahan URL yang terjadi, maka, penggunaan tools B dapat menjadi salah satu opsi yang baik untuk melakukan serangan MITM, dikarenakan pada saat penggunaan tools C, URL tidak berubah sama sekali, sehingga dapat "mengakali" korban. Akan tetapi jika dilihat dari tingkat kesulitan saat membaca data hasil serangan, maka tools C merupakan tools yang sangat user friendly jika dibandingkan dengan tools A dan B.

Berdasarkan hasil analisa diatas, maka penulis dapat menyimpulkan bahwa penggunaan tools B cukup efektif dalam melakukan serangan MITM, akan tetapi untuk menjalankan tools B diperlukan pengetahuan yang cukup mumpuni, dikarenakan pada saat menjalankan tools B, diperlukan untuk melakukan konfigurasi terlebih dahulu agar tools dapat mem-bypass protokol HTTPS.

Sedangkan penggunaan tools C sangat cocok bagi pembaca yang baru mengenal teknik hacking, karena dengan menggunakan tools C, pembaca tidak memerlukan untuk mengkonfigurasi dan mengingat command line yang cukup panjang, akan tetapi tingkat keberhasilan dari tools ini berada pada posisi terendah dari dua tools lainnya.

Sementara itu, penggunaan tools A menjadi opsi alternatif bagi pembaca, karena tools A ini memiliki kemampuan yang cukup seimbang, baik itu dari segi keberhasilannya, kemudahan penggunaannya, dan kesulitan membaca hasil serangannya.

Hasil Pengujian Keamanan

Pada pengujian keamanan, penulis mengkombinasikan 2 metode dalam mengamankan data pengguna jaringan WLAN. Metode yang pertama ialah dengan menggunakan IDS untuk memonitor serangan dan metode yang kedua ialah menerapkan IP Tables untuk memblokir situs HTTP. Dari pengujian tersebut maka penulis mendapatkan hasil, yang hasil tersebut penulis rangkum ke dalam tabel 5 berikut.

Tabel V
Pengujian Keamanan

No	Metode Keamanan	Deteksi Port Scanning	Blokir Protokol HTTP	Mencegah Pencurian Data
1.	IDS	Ya	Tidak	Ya/Tidak
2.	IP Tables	Tidak	Ya	Ya

Dari tabel 5 dapat di analisa bahwa penggunaan IDS hanya sebatas monitoring saja, sehingga untuk melakukan tindakan preventif, maka di perlukan sumber daya manusia (baca: administrator jaringan) yang dapat dengan cepat melakukan tindakan pencegahan.

Penggunaan IP Tables pada jaringan WLAN cukup membantu dalam mencegah tindakan sniffing (baca: serangan MITM) dari oknum yang tidak bertanggung jawab, hanya saja penggunaan IP Tables dalam memblokir request yang mengarah ke port 80 sehingga dapat merugikan pengguna jaringan WLAN, walaupun saat ini hampir semua website sudah beralih menggunakan port 443 (baca: HTTPS). Namun hingga saat ini masih ada juga website yang masih belum bermigrasi menggunakan protokol HTTPS.

IV. KESIMPULAN

Berdasarkan hasil dari penelitian pada bab sebelumnya (baca: BAB III) terhadap serangan MITM pada 5 kategori website dan sistem keamanannya, maka dapat disimpulkan sebagai berikut:

1. Serangan MITM dapat dijalankan dengan berbagai macam tools serangan, seperti tools A, tools B, dan tools C.
2. Serangan dengan menggunakan tools B memiliki persentase keberhasilan yang lebih tinggi, yaitu 80% dibandingkan dengan penggunaan tools lainnya.
3. Penggunaan tools B untuk melakukan sniffing memiliki persentase sebesar 70%, sementara itu penggunaan tools C memiliki persentase keberhasilan sebesar 60%.
4. Penggunaan tools B tidak akan merubah URL dari website yang dikunjungi korban, sehingga korban tidak curiga jika dia sedang di serang.
5. Hasil serangan tools C lebih mudah di baca, jika dibandingkan dengan tools A dan tools B.
6. Mengetikkan protokol HTTPS pada URL box pada saat hendak mengakses website akan mencegah dari serangan MITM.
7. Penggunaan Ip Tables dapat mencegah dari serangan MITM. Akan tetapi akan menyulitkan pengguna jaringan untuk mengakses website yang masih menggunakan protokol HTTP.

REFERENSI

[1] Ahmad Zainuddin, L. A. (2014). ANALISIS SISTEM KEAMANAN HOTSPOT DENGAN MENGGUNAKAN HONEYPOT DAN IDS DI KAMPUS STMIK PPKIA PRADNYA PARAMITA MALANG. *Jurnal Teknologi Informasi*, 107-109.

[2] Muhammad Sabri Ahmad, I. R. (2017). Investigasi Live Forensik Dari Sisi Pengguna Untuk Menganalisa Serangan Man In The Middle Attack Berbasis Evil Twin. *ILKOM Jurnal Ilmiah*, 1-8.

[3] Muhammad Taufiq Muslih, B. E. (2013). PENGEMBANGAN APLIKASI SMS GATEWAY UNTUK INFORMASI PENDAFTARAN PESERTA DIDIK BARU DI SMAN 1 JEPARA. *Indonesian Jurnal on Networking and Security (IJNS)*, 50-51.

[4] Radhika.P, R. S. (2017). Defending Man In The Middle Attacks. *International Research Journal of Engineering and Technology (IRJET)* , 579-585.

[5] Ridlo, M. R. (2016). *Snort Sebagai Intrusion Detection System dan Notifikasi Melalui Telegram.* Dipetik Juni 4, 2018, dari Universitas Islam Indonesia: https://dspace.uii.ac.id/handle/123456789/2702

[6] Tulika Shubh, S. S. (2016). Man-In-The-Middle-Attack Prevention Using HTTPS and SSL . *International Journal of Computer Science and Mobile Computing*, 569-579 .

[7] Ery Setiyawan Jullev Atmadji, B. M. (2017). Pemanfaatan IPTables Sebagai Intrusion Detection System (IDS) dan Intrusion Prevention System (IPS) Pada Linux Server. *TEKNIKA*, 21.