KESATRIA: Jurnal Penerapan Sistem Informasi (Komputer & Manajemen)
Terakreditasi Nomor 204/E/KPT/2022 | Vol. 4, No. 1, Januari (2023), pp. 224-233

Manajemen Pencegahan Serangan Jaringan Wireless Dari Serangan Man In The Middle Attack

Tengku Mohd Diansyah[1], Ilham Faisal[2], Dodi Siregar[3]
[1,2,3]Fakultas Teknik dan Komputer, Universitas Harapan Medan, Indonesia
Email: [1]Dian.10.22@gmail.com, [2]ilhamoppa11@gmail.com,
[3]dodi.stth@gmail.com

Abstract

Currently, wireless networks are very widely used to communicate because wireless networks are very fast and communicate without using cables, by using this wireless it turns out that there are weaknesses or security gaps due to irresponsible people illegally such as looking for backdoor gaps to infiltrate and attack aspects of authenticity. If a crime occurs, how to prevent the crime or attack. In this article, the possibility of an attack with the type of attack carried out is a man in the middle attack from this attack experiment will be carried out 5 times the attack experiment in this experiment the calculation of QoS (Quality of Service) is carried out, namely calculating how much packet loss and the results obtained in this attack experiment with the calculation of packet loss as much as 0.291% loss, attack 1 model 2 with packet loss 0.173%, attack 2 model 2 with packet loss which means this attack successfully attacks wireless communication. To prevent this attack activity, first know the technique of how the attack runs on a wireless network, using ettercap on linux times.

.

Keywords*: wireless attack; Person in the middle attack; QoS*

Abstrak

Saat ini jaringan wireless sangat banyak di gunakan untuk berkomunikasi di karenakan jaringan wireless sangat cepat dan berkomunikasi tanpa menggunakan kabel, dengan menggunakan wireless ini ternyata ada kelemahan atau celah keamanan di karenakan adanya orang yang tidak bertanggung jawab dalam illegal sperti mencari celah backdoor untuk menyusup dan menyerang aspek authenticity. Jika kegiatan kejahatan itu terjadi maka bagaimana cara mencegah kejahatan atau serangan tersebut. Pada artikel ini melakukan kemungkinan dalam penyerangan dengan jenis serangan yang di lakukan adalah serangan man in the middle attack dari percobaan penyerangan ini akan di lakukan sebanyak 5 kali percoban penyerangan dalam percobaan ini dilakukan perthitungan QoS (Quality of Service) yaitu menghitung berapa banyak paket loss dan hasil yang di dapat dalam percobaan penyerangan ini dengan menghitung paket loss nya sebanyak loss 0.291%, serangan 1 model 2 dengan packet loss 0,124%, serangan 2 model 2 dengan packet loss yang diartikan pada serangan ini berhasil untuk menyerang komunikasi wireless. Untuk mencegah daripada kegiatan penyerangan ini, terlebih dahulu untuk mengetahui teknik cara serangan itu berjalan pada jaringan wireless, dengan menggunakan ettercap pada kali linux.

Kata Kunci*: serangan wireless; Man in the middle attack; QoS*

1. Pendahuluan

Pemanfaatan *wireless* (nirkabel) pada era saat ini banyak digunakan pada institusi, perumahan, persekolahan, perusahaan dan lain sebagainya, yang dimana *wireless* berperan penting dalam membantu serta memudahkan interaksi antar manusia. Namun dengan adanya *wireless* (nirkabel) tidak seutuhnya aman dalam berinteraksi menggunakan *wireless* di tempat-tempat umum. Terdapat kegiatan-kegiatan *illegal* seperti *man in the middle attack, DNS spoofing*, dan lain sebagainya [1]. Dikarenakan Internet merupakan

ISSN: 2720-992X

salah satu bentuk dari media komunikasi dan infomasi interaktif, adanya wujud internet yaitu dapat dilihat dari jaringan komputer yang telah terhubung di seluruh belahan dunia, internet ini dapat digunakan untuk berbagai hal misalanya digunakan untuk mengirim informasi antar komputer yang ada di seluruh dunia [2]. Penulis memperhatikan suatu kegiatan illegal, yang dapat dilakukan di jaringan *wirelless* dimana dalam aritkel ini penulis akan mengantisipasi atau mencegah dari kejahatan atau aktivitas illegal. Kegiatan illegal tersebut ialah spoofing yang terjadi pada domain name system (DNS). Man in the middle attack (MITM) suatu teknik jenis serangan yg dapat memposisikan dirinya pada antara percakapan yaitu dialog antara ke 2 belah pihak mirip model user serta website [3]. Konsep pada DNS spoofing yaitu teknik khusus yang dipergunakan untuk merogoh alih domain name system (DNS) sehingga domain dan IP address pada sebuah situs akan dialihkan di server pelaku. Oleh karena itu diperlukan penelitian yang dapat mengantisipasi juga mencegah serta meminimalisir upaya yang dilakukan dari agresi tersebut. Dalam hal ini adalah gangguan dari pihak-pihak yangtelah mengetahui kondisi keamanan dan kelemahan jaringan tersebut.Gangguan eksternal adalah gangguan yang memang berasal daripihak luar yang ingin mencoba atau dengan sengaja ingin menembus keamanan yang telah ada [4]. Pada penelitian sebelumnya yg dilakukan oleh Syaifuddin di jurnal tahun 2021 pada penelitian yang berjudul ("Analisis Address Resolution Protocol Poisoning Attack pada Router WLAN menggunakan Metode *Live Forensics*") yang meneliti tentang analisis agresi ARP poisoning yang terjadi di jaringan WLAN dengan menggunakan metode live forensics. Sebagai akibatnya analisa yang diterapkan bisa menjadi tolak ukur tindak pidana serta dapat menjadi tolak ukur untuk mencegah asal agresi tadi. Adapun penelitian tadi hanya mengahasilkan analisa dalam penyerangan tanpa adanya cara menerapkan bagaimana pencegahannya. Penelitian live forensics ini dilakukan pada dua kondisi, yaitu saat proses observasi jaringan (sebelum serangan) dan pada saat proses penyerangan, hal ini bertujuan untuk memudahkan dalam mengetahui perbedaan karakteristik data penelitian. Hasil dari penelitian ini dapat dijadikan bukti digital dalam melakukan laporan tindakan pidana serta dapat juga dijadikan tolak ukur dalam melakukan pengamanan jaringan [5].

2. Metodologi Penelitian

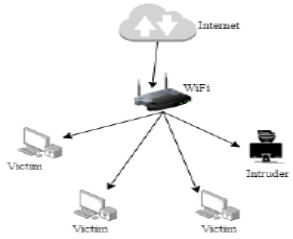
Adapun untuk mendukung penelitian ini hal yang dilakukan oleh penulis ada melakukan beberapa tahapan dimulai dari :

a) Pengumpulan data
   Mengumpulkan data-data pustaka untuk mendapatkan informasi-informasi yang dibutuhkan dalam
   mengerjakan penelitian.
b) Pemerikasaan
   Mecari masalah yang terjadi pada penelitian berdasarkan fenomena permasalahan yang ada. Serta melakukan pemeriksaan keamanan dengan menerapkan sistem keamanan, agar dapat mencegah dari kejahatan serangan yang akan di lakukan.
c) Analisis
   analisis sistem serangan dan keamanan tersebut, berguna dalam menangani kasus yang berdasarkan fenomena munculnya permasalahan yang ada pada penelitian ini, dan menghasilkan solusi dalam mengatasi permasalahan ini.
d) Laporan
   Pada tahap ini penulis menyimpulkan hasil daripada pengujian penelitian yang telah dilakukan implementasi serta uji coba. Sehingga mendapatkan hasil kesimpulan dalam menjawab permasalahan pada
   penelitian ini.

Gambar 1. Tahapan dalam Metode

2.1. Perancangan

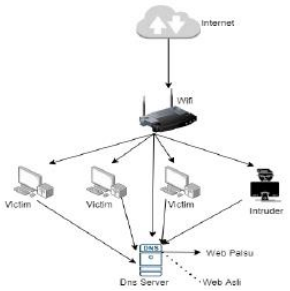
Selanjutnya merancang skema jaringan yang telah penulis kaji dalam penelitian atau riset ini, dengan terhubungnya user oleh perangkat atau *router wireless fidelity*. Maka penulis menyimpulkan terhubungnya dengan wireless tersebut dapat diartikan dengan terhubungnya oleh jaringan yang sama.



Gambar 2. Rancangan Skema Network 1

Topologi jaringan atau skenario arsitektur jaringan yang akan penulis implementasikan pada uji coba penelitian ini. Dengan menghubungkan *attacker* dan sang korban pada jaringan wireless atau jaringan yang terhubung sama, dan dengan bentuk arsitektur jaringan seperti diatas, penulis dapat mengimplementasikan uji coba serangan man in the *middle attack* DNS spoofing dan penulis juga dapat mengimplementasikan pemantauan jaringan dan mencoba membentuk sistem keamanan *firewall* pada perangkat sistem yang terhubung oleh jaringan tersebut. Rancangan skema jaringan ketika terjadi serangan dilakukan untuk memberikan gambaran terhadap user yang menggunakan wireless, sebagai hak akses cepat dalam berinteraksi dengan menggunakan internet agar kemudian dapat mengetahui bagaimana serangan ini berjalan sesuai perannya yang dilakukan oleh penyerang untuk mendapatkan keinginan dari penyerang.

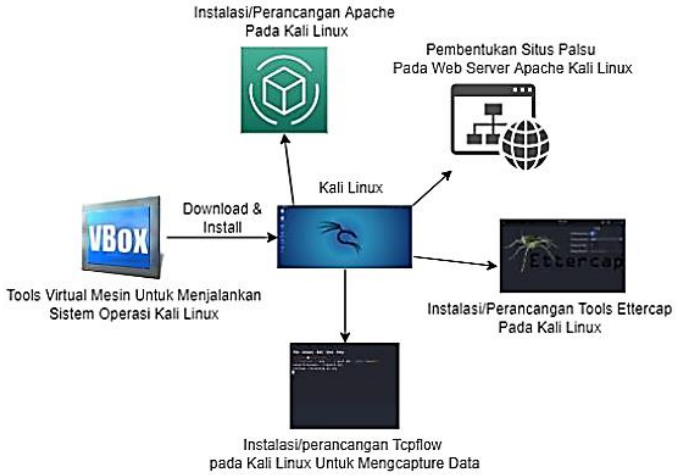
Pada tahap ini serangan dilakukan pada jaringan *wireless*, yang dimana pada satu jaringan *wireless* tersebut, akan terhubung beberapa *host* yang nantinya akan menjadi korban dari serangan *man in the middle attack* DNS *spoofing* ini. Oleh karena itu serangan ini dilakukan pada interaksi jaringan *wireless* yang terhubung juga oleh korban dengan satu jaringan yang sama pada jaringan *wireless.*



Gambar 3. Skema Serangan *Man in the middle attack*

Skema jaringan ketika terjadinya serangan telah penulis kaju untuk melakukan implentasi serangan terhadap jaringan wireless yang terhubung. Dengan jaringan yang terhubung pada satu jaringan *wireless* baik *attacker* maupun korban, yang kemudian menghasilkan kegiatan *illegal* tersebut, yang dilakukan oleh *attacker* kepada korban tersebut. Perancangan serangan membutuhkan tools yang mendukung dalam melancarkan

serangan. Agar dapat mengoptimalkan *serangan man in the middle attack DNS spoofing* dapat berjalan pada jaringan *wireless*.

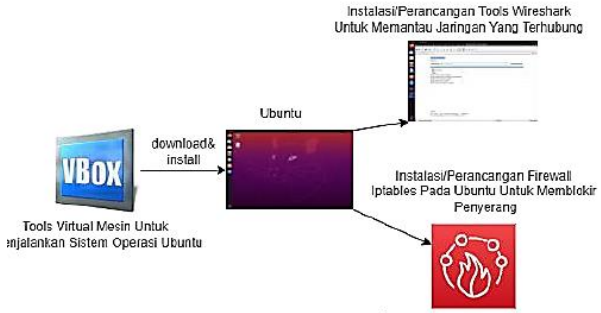


Gambar 4. Rancangan Serangan

Merupakan tampilan dari rancangan serangan. Perancangan serangan yang dapat dilakukan ketika terhubung oleh jaringan yang sama. Ketika sudah terhubung dengan jaringan yang sama maka dapat dilakukan teknik serangan *man in the middle attack DNS spoofing*. Dalam penelitian yang penulis angkat, penulis menggunakan virtualbox untuk menjalankan virtual mesin yang akan penulis gunakan dalam menguji coba riset pada penelitian yang penulis angkat, untuk menerapkan teknik serangan *man in the middle attack DNS spoofing*

2.2. Skenario Pengujian

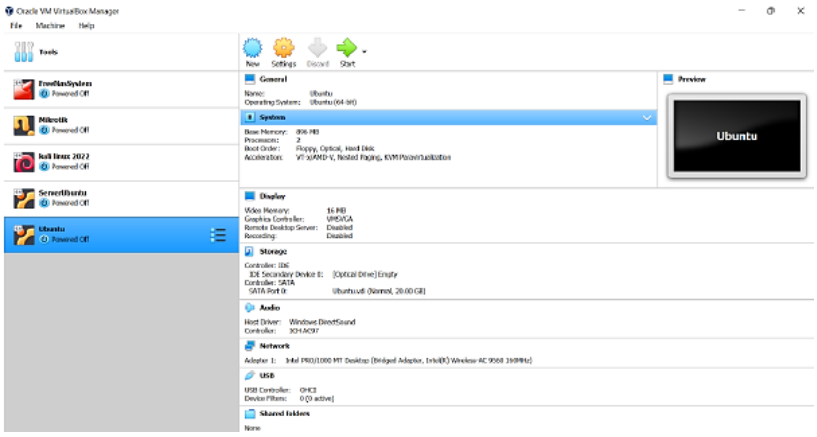
Perancangan keamanan membutuhkan *tools* yang mendukung dalam membentuk sistem keamanan. Agar dapat membentuk sistem keamanan pada perangkat yang terkena dampak serangan *man in the middle attack DNS spoofing* yang terjadi ketika terhubung pada jaringan *wireless*. Dan menggunakan Ettercap merupakan alat packet sniffer yang digunakan untuk menganalisis protokol jaringan dan memverifikasi keamanan jaringan. Ia juga memiliki kemampuan untuk memblokir lalu lintas jaringan LAN, mencuri kata sandi, dan secara aktif menguping protocol umum. Packet sniffing juga dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab untuk mencuri data sensitif dari pengguna yang saat ini terhubung dengan access point [6]. Berikut bentuk rancangan yang dibutuhkan dalam membangun sistem keamanan *firewall* pada perangkat yang akan menjadi korban.



Gambar 5. Skenario Pengujian serangan

Pada penelitian uji coba riset penelitian ini, penulis akan menggunakan peran dari pada *software virtualbox* sebagai virtual mesin, yang dimana akan digunakan dalam tahap menjalankan sistem operasi untuk menguji coba dan membentuk sistem keamanan di

dalam sistem operasi tersebut. Virtualbox sebelumnya telah diinstal pada sistem operasi utama windows yang digunakan penulis dalam melakukan tahap uji coba penelitian ini. Sebelum mendownload dan menginstal sistem operasi yang dijadikan bahan uji coba sistem yang digunakan oleh korban yang terkena serangan *man in the middle attack DNS spoofing*, dibutuhkan *software virtualbox* untuk menjalankan peran daripada sistem korban.

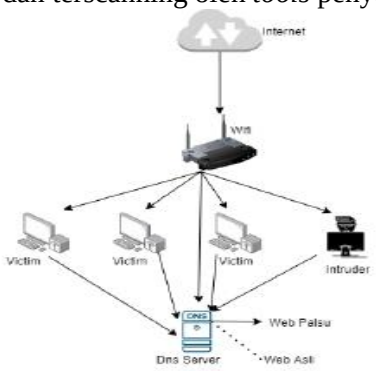


Gambar 6. Virtual Box

Menunjukkan bagaimana tampilan awal menu *software virtualbox* yang akan digunakan sebagai virtual mesin pada sistem operasi ubuntu. Untuk membangun sistem keamanan pada jaringan yang akan diimplementasikan oleh penulis. Sebelumnya penulis telah menginstal sistem operasi ubuntu pada situs resmi https://ubuntu.com/ dengan versi ubuntu desktop 22.04 . Sistem operasi ubuntu yang telah terhubung pada jaringan wireless yang sama atau telah terhubung dengan jaringan yang sama dengan *attacker*, sehingga *host* dari sistem ubuntu yang terhubung, akan dapat terscanning oleh *attacker* dan mengakibatkan terjadinya kejahatan [7] serangan *man in the middle attack DNS spoofing.* Dalam menjalankan untuk mengantisipasi dan mencegah daripada serangan yang terjadi, dibutuhkan hak akses untuk memantau kegiatan yang terjadi pada jaringan yang terhubung. Dengan adanya hak akses atau metode dalam melihat traffic interaksi komunikasi terhadap jaringan, itu dapat memudahkan penulis dalam menjalankan peran sistem operasi ubuntu yang menjadi korban, untuk melihat apa yang terjadi kepada host yang terhubung dan terkena serangan kejahatan tersebut.

3. Hasil Dan Pembahasan

Model serangan yang kedua yaitu dengan cara menyerang dengan jaringan yang terhubung dengan satu jaringan yang sama. Dan menyerang seluruh *host* yang terhubung dengan jaringan yang sama dan terscanning oleh *tools* penyerang yaitu *tools ettercap*.



Gambar 7. Serangan pada host yang terhubung

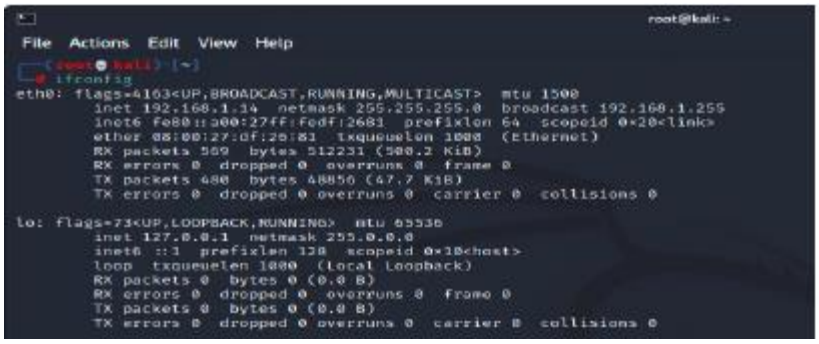
Pada gambar 7, merupakan bentuk topologi serangan dengan menyerang seluruh host yang terhubung dengan jaringan wireless. Penulis membentuk serangan ini dengan menerapkan peran dari pada attacker agar dapat banyak mengambil informasi kepada pengguna yang ingin mengakses situs, dan bertepatan situs yang ingin pengguna atau user tuju telah dimanipulasi oleh sang attacker, dengan cara yang jahat tanpa diketahui oleh sang korban atau pengguna

3.1. Pengujian Model Serangan

Pada model serangan yang pertama, yaitu implementasi model serangan dengan memilih target. Penulis menerapkan tiga kali percobaan serangan dengan terhubung pada jaringan *wireless* atau perangkat *router wireless* yang berbeda, dan juga *domain* yang berbeda yaitu *domain siaunhar.harapan.ac.id*, *domain polri.go.id*, dan *domain google.com*. Penulis melakukan percobaan serangan di waktu yang berbeda, dan tempat yang berbeda.

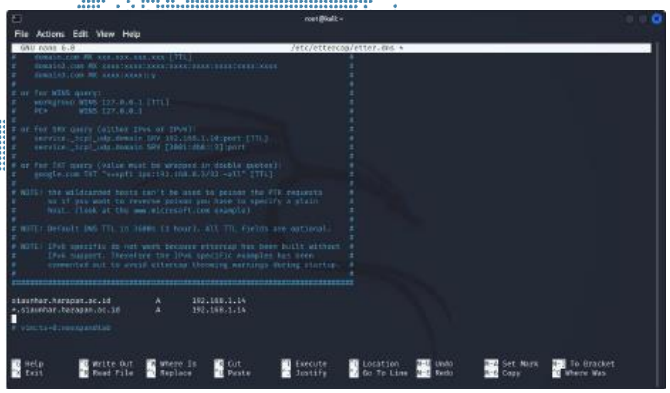
Gambar 8. Tampilan Kali Linux

Untuk tahap percobaan serangan, terlebih dahulu untuk melihat alamat *ip address* penyerang yang berguna untuk dilakukan konfigurasi *DNS* pada *tools ettercap*. *Open terminal linux* untuk mendapatkan alamat *IP* penyerang, dengan menginputkan perintah *ifconfig*.



Gambar 9. Tampilan Alamat IP penyerang

Pada gambar 9, merupakan alamat *IP* penyerang yang didapat dengan menginputkan perintah *ifconfig* pada *terminal linux*, yang ber alamatkan 192.168.1.14. Setelah mendapatkan alamat *IP address* penyerang, selanjutnya melakukan tahap konfigurasi *DNS* pada *file etter.dns tools ettercap* yang berguna untuk pengalihan *IP domain* yang akan di targetkan. Untuk menuju *file* konfigurasi *DNS*, maka terlebih dahulu menginputkan perintah pada *terminal linux nano /etc/ettercap/etter.dns*.

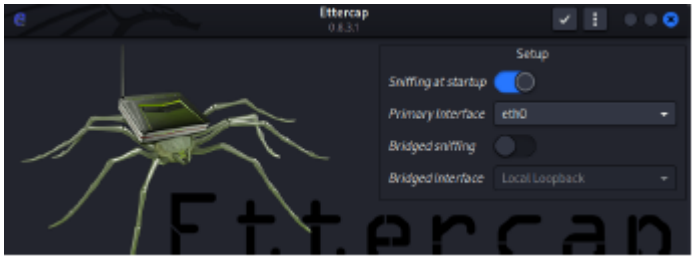


Gambar 10. Konfigurasi domain

Pada gambar 10, merupakan tampilan konfigurasi *domain* yang ingin di manipulasi oleh penyerang dengan menyimpannya pada *file ettercap* yaitu *file etter.dns*. Yang dimana situs *siaunhar.harapan.ac.id* merupakan situs asli daripada situs *website* kampus Universitas Harapan Medan yang ingin di manipulasi oleh penyerang. Dan mengalamatkan situs tersebut kepada alamat *IP* dari penyerang, *IP* dari penyerang yaitu 192.168.1.14. Setelah dilakukan konfigurasi oleh penyerang. Penyerang menyimpan *file* tersebut pada *file etter.dns* dengan menekan tombol *ctrl+x* lalu tekan tombol *enter* dan tekan *enter* untuk menyimpan *file* tersebut. Setelah selesai menyimpan *file* konfigurasi pada *tools ettercap* yang digunakan pelaku. Kemudian aktifkan *server apache* pada sistem pelaku, agar alamat yang terkonfigurasi pada *file ettercap* sebelumnya akan mengarah pada situs palsu yang telah di konfigurasi oleh pelaku sebelumnya. Mengaktifkan *apache server* dengan menginputkan perintah pada *terminal kali linux service apache2 start*. Setelah mengaktifkannya maka *server* tersebut dapat aktif dan berjalan pada sistem pelaku.

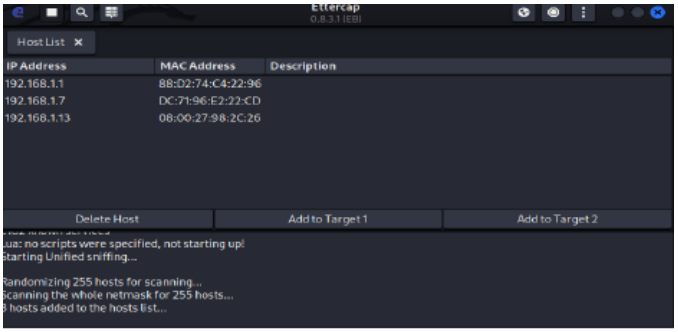
Gambar 11. Starting Apcahe

Tahap selanjutnya dengan mengaktifkan *tools ettercap* pada *kali linux*, agar dapat melaksankan perannya dalam menjalankan serangan *man in the middle attack DNS spoofing*. Perintah untuk menjalankannya yaitu dengan menginputkan perintah pada *terminal kali linux ettercap -G*, maka *tools ettercap* dapat aktif dan berjalan.



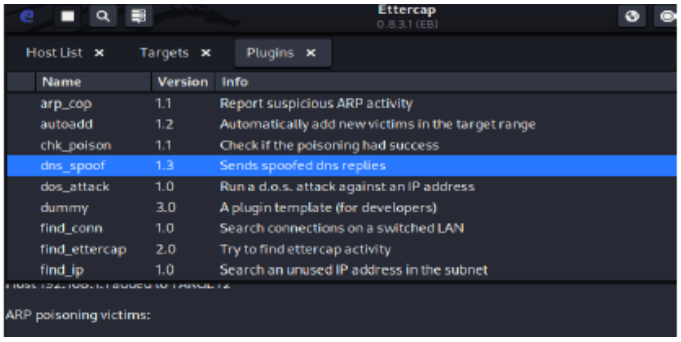
Gambar 12. Tools Etercap

Tampilan *tools ettercap* yang sudah aktif dan berjalan. Setelah berjalan maka pilih fitur *sniffing* pada *ettercap* dengan menekan tombol fitur centang pada *ettercap*. fitur *sniffing* pada *ettercap* berguna untuk dapat melihat lalu lintas data yang terhubung pada jaringan. Setelah masuk dalam fitur *sniffing* pada *ettercap* maka pelaku memilih fitur selanjutnya yaitu melihat *host* yang terhubung pada jaringan tersebut. Agar dapat melihat *host* yang terhubung, pelaku memlih fitur pengaturan yang dilambangkan titik 3 diujung sebelah kanan. Dan memilih fitur *scan for host* pada *ettercap*.



Gambar 13. Scanning Host yang terhubung

Berikutnya aktifkan *dns_spoof* pada *ettercap*, yang berguna untuk mengaktifkan aliran alamat situs yang akan diakses oleh korban, yaitu situs *siaunhar.harapan.ac.id*. Maka dengan diaktifkannya fitur tersebut akan mengalihkan tampilan *web* asli atau situs asli dari pada tampilan *siaunhar.harapan.ac.id* menuju tampilan *web* atau situs palsu yang sebelumnya telah di konfigurasi oleh pelaku.



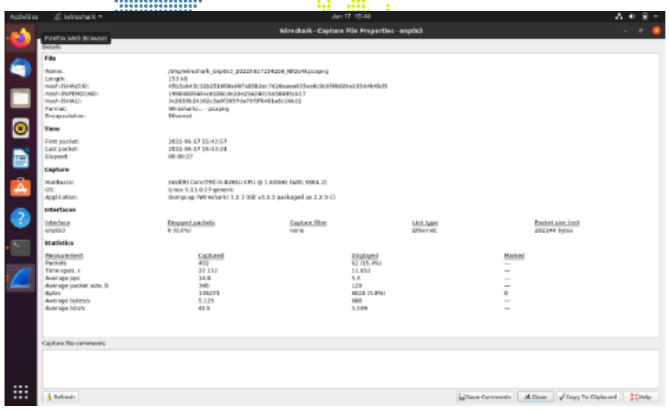
Gambar 14. DNS Spoofing aktif

Merupakan tahap dalam mengaktifkan fitur *dns_spoof* pada *ettercap*, Sehingga serangan dapat berjalan kepada target yang telah ditentukan oleh penyerang. Kemudian aktifkan *tools tcpflow* agar dapat menerima data atau pesan yang diinputkan oleh korban, sehingga penyerang mendapatkan apa yang diinginkan dari sang korban. Dalam hal ini *username* dan *password* merupakan data yang diinginkan oleh penyerang.

3.2. Hasil Serangan Dengan Menghitung Packet Loss

Setelah penulis melakukan beberapa kali percobaan dengan menguji serangan dan mendapatkan hasil serangan dibuktikan dengan menghitung *packet loss* yang telah tercapture oleh *software wireshark*, sehingga mendapatkan bukti kalau serangan itu berhasil berjalan. Berikut kategori degradasi pada perhitungan *packet loss*. merupakan nilai presentase kategori dalam menghitung *packet loss* yang tercapture pada aplikasi *wireshark*. Kategori sangat bagus yang berarti tidak ada *packet loss* yang terjadi, dan jika jelek yang berarti *packet* tersebut banyak terjadi *loss* atau tidak terkirim kepada tujuannya. Hasil Serangan Dengan Menghitung Packet Loss berdasarkan statistik data *packet* pada

filtering protokol *DNS* untuk mendapatkan hasil presentase pada *packet loss* ketika terjadi serangan. Dengan menghitung dari *software wireshark*.



Gambar 15. Stastik data Protokol DNS

Merupakan data dari protokol *DNS* yang tercapture dengan *tools wireshark* ketika terjadinya serangan. Rumus untuk menghitung *packet loss* yaitu :
((*packet* yang dikirim – *packet* yang diterima) / *packet* yang dikirim x 100%)
= 402 – 340 / 402
= 62 / 402
= 0,154 x 100%
= 0,154 % *packet loss* yang terjadi pada protokol *DNS* pada percobaan serangan dengan model serangan yang pertama. Hasil *capturing* statistik pada protokol *DNS.*

Tabel 1. Hasil kategori Packet Loss dan Percobaan Serangan

Percobaan Serangan	*Packet Loss*	Kategori
Serangan 1 Model 1	0,154 %	Sangat Bagus
Serangan 2 Model 1	0,234%	Sangat Bagus

Merupakan hasil keseluruhan dari uji coba dalam menghitung *packet loss* ketika terjadi serangan, dan tercapture oleh aplikasi *wireshark*. Yang dimana berarti serangan tersebut melancarkan serangan dengan tidak terdapatnya *packet loss*. Yang berarti serangan tersebut berhasil dan lancar dalam menjalankan aksinya. Tetapi pada hasil percobaan serangan dengan target *google.com, facebook.com, dan detik.com* tidak berhasil dengan menampilkan halaman palsu. Sehingga dapat diartikan bahwa serangan dengan menargetkan *domain google.com, detik.com,* dan *facebook.com* dapat berjalan tetapi tidak dengan menampilkan halaman palsu dikarenakan tingkat keamanan pada *domain* tersebut dapat mencegah serangan *man in the middle attack DNS spoofing*.

4. Kesimpulan

Dengan berjalannya beberapa kali percobaan dan pengujian serangan yang telah dilakukan oleh penulis, menghasilkan solusi dengan melihat keamanan pada website atau SSL (secure sockets layer) yang diperingati oleh keamanan pada website tersebut agar dapat terhindar dari serangan man in the middle attack DNS spoofing. pengujian serangan yang telah dilakukan oleh penulis, menghasilkan solusi dengan melihat keamanan pada website atau SSL (secure sockets layer) yang diperingati oleh keamanan pada website tersebut agar dapat terhindar dari serangan man in the middle attack DNS spoofing.

Daftar Pustaka

[1] T. Pangestu and R. Liza, "Analisis Keamanan Jaringan pada Jaringan Wireless dari Serangan Man In The Middle Attack DNS Spoofing," Jitekh, vol. 10, no. 2, pp. 60–67, 2022.

[2] M. F. Ardiansyah, T. M. Diansyah, and R. Liza, "Penggunaan Set top box Bekas untuk Dimanfaatkan sebagai Cloud Server," 2022.

[3] T. M. Diansyah, I. Faisal, A. Perdana, B. O. Sembiring, and T. H. Sinaga, "Analysis of Using Firewall and Single Honeypot in Training Attack on Wireless Network," J. Phys. Conf. Ser., vol. 930, no. 1, 2017, doi: 10.1088/1742-6596/930/1/012038.

[4] "Analisa Pencegahan Aktivitas Ilegal Didalam Jaringan Menggunakan Wireshark," Jun. 2015, [Online]. Available: http://ejournal.stmik-time.ac.id/index.php/jurnalTIMES/article/view/229

[5] S. Syaifuddin, D. Regata Akbi, and A. Gholib Tammami, "Analisis Address Resolution Protocol Poisoning Attack Pada Router Wlan Menggunakan Metode Live Forensics," J. Komput. Terap., vol. 7, no. Vol. 7 No. 1 (2021), pp. 62–73, 2021, doi: 10.35143/jkt.v7i1.4575.

[6] A. Rizal Fauzi and I. Made Suartana, "Monitoring Jaringan Wireless Terhadap Serangan Packet Sniffing Dengan Menggunakan Ids," J. Manaj. Inform., vol. 8, no. 2, p. 7, 2018.

[7] W. Zaenal Mutaqin Subekti, Hendra Setiawan, Satria, Widia Murni Wijaya,Aliy Hafiz, "Perancangan Infrastruktur Domain Name Server Lokal Menggunakan Ubuntu Server 16.04 Pada PT. Xyz," no. 2, p. 6, 2021.