JITEKH, Vol. 10, No. 2, Tahun 2022, 60-67

ISSN 2338-5677 Cetak
ISSN 2548-6646 Online

Analisis Keamanan Jaringan pada Jaringan *Wireless* dari Serangan *Man In The Middle Attack DNS Spoofing*

Teguh Pangestu[1], Risko Liza[2]
[1,2] Program Studi Teknik Informatika, Fakultas Teknik dan Komputer, Universitas Harapan Medan
Email: teguhcrack123@gmail.com, risko.liza@gmail.com

Abstrak

Saat ini pemanfaatan teknologi *wireless* (nirkabel) banyak digunakan pada institusi, perusahaan, persekolahan dan lain sebagainya. *Wireless* sangat berguna karena dapat mempermudah aktivitas kegiatan interaksi sesama manusia dalam mengirim data dan lain sebagainya. Namun tetapi, dengan adanya *wireless* tidak sepenuhnya aman dalam melakukan aktivitas interaksi sesama manusia dalam mengirim data dan lain sebagainya, salah satunya kegiatan *illegal man in the middle attack DNS spoofing*. Dengan adanya kegiatan *illegal* tersebut maka dibutuhkan sistem keamanan yang diharapkan dapat mencegah kegiatan *illegal man in the middle attack DNS spoofing*. hasil dari penyerangan yang di dapatkan berdasarkan 7 kali pengujian dengan menghitung *quality of service (QOS)* yaitu *packet loss* dengan hasil serangan 1 model 1 dengan *packet loss* 0,154%, serangan 2 model 1 dengan *packet loss* 0,234%, serangan 3 model 1 dengan *packet loss* 0.291%, serangan 1 model 2 dengan *packet loss* 0,173%, serangan 2 model 2 dengan *packet loss* 0,128%, serangan 3 model 2 dengan *packet loss* 0,028%, serangan 4 model 2 dengan *packet loss* 0,231%, yang dapat diartikan serangan ini dapat berjalan dengan baik. Dan hasil dengan memanfaatkan sistem keamanan *firewall* hanya dapat mencegah dengan memutus interaksi komunikasi antar penyerang dengan korban dan korban dengan penyerang.

Kata Kunci: Kali linux, ubuntu, man in the middle attack DNS spoofing, wireshark, firewall

Abstract

Currently the use of wireless technology (wireless) is widely used in institutions, companies, schools and so on. Wireless is very useful because it can facilitate human interaction activities in sending data and so on. However, the existence of wireless is not completely safe in carrying out human interaction activities in sending data and so on, one of which is the illegal man in the middle attack DNS spoofing activity. With these illegal activities, a security system is needed which is expected to prevent illegal man in the middle attack DNS spoofing activities. The results of the attack are obtained based on 7 tests by calculating the quality of service (QOS), namely packet loss with the results of attack 1 model 1 with packet loss 0.154%, attack 2 model 1 with packet loss 0.234%, attack 3 model 1 with packet loss 0.291%, attack 1 model 2 with packet loss 0.173%, attack 2 model 2 with packet loss 0.128%, attack 3 model 2 with packet loss 0.028%, attack 4 model 2 with packet loss 0.231%, which means this attack can run well. And the results by utilizing a firewall security system can only prevent it by cutting off communication interactions between the attacker and the victim and the victim and the attacker.

Keywords: Kali linux, ubuntu, man in the middle attack DNS spoofing, wireshark, firewall

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. Baik dalam mengirim data, mengirim pesan, dan lain sebagainya. 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. *Man in the middle attack* adalah serangan yang dilakukan oleh satu atau lebih penyerang, di mana penyerang mengirim dan memodifikasi pesan sementara dua pihak yang berwenang dalam komunikasi terus menerus. Dengan melakukan serangan ketika komunikasi sedang berlangsung [1].

DNS spoofing adalah adalah jenis serangan yang melibatkan penyediaan informasi alamat *IP* palsu dalam upaya untuk mengalihkan lalu lintas paket data dari tujuan yang dimaksudkan [2].

Kegiatan *illegal* ini timbul tentu akan sangat merugikan dari pengguna *wireless* tersebut, dimana

ISSN 2338-5677 Cetak
ISSN 2548-6646 Online

dampak kerugian dapat berupa kehilangan data, atau bocornya identitas rahasia dari pengguna jaringan *wireless* tersebut. *Wireless* merupakan kumpulan komputer yang terhubung dari satu komputer ke komputer lain, membentuk jaringan komputer. Jaringan ini menggunakan *media* udara/gelombang untuk mengirim data. Dalam sebuah jaringan, kecepatan dipengaruhi oleh faktor-faktor seperti perangkat yang anda gunakan dan perangkat yang menjadi *AP*, jarak dan ruang. Penelitian ini berusaha untuk mengetahui kinerja jaringan nirkabel *IEEE* 802.11n [3].

Maka dari permasalahan yang ada, dibutuhkan sistem keamanan yang dapat mencegah dari serangan kegiatan *illegal man in the middle attack* serta *DNS spoofing*. Sistem keamanan *firewall* yang dimana akan di coba dalam mengimplementasikan tahap pengujian untuk mengamankan serta mencegah apakah sistem keamanan *firewall* tersebut dapat mencegah atau sebaliknya. *Firewall* adalah sistem keamanan jaringan yang melindungi data anda dari pengguna yang tidak memiliki akses ke sana, *firewall* bertindak sebagai penyaring antara komputer *internal* dan komputer *external* [4].

Rumusan masalah disini adalah bagaimana cara menganalisa keamanan jaringan dari *serangan man in the middle attack DNS spoofing*, serta mencari solusi agar terhindar dari serangan tersebut, serta mencari bagaimana serangan tersebut dapat berjalan, serta mencari tahu bagaimana cara melakukan pencegahan, dan bagaimana cara dalam mengetahui perangkat yang kita gunakan dengan terhubung dengan jaringan *wireless* terkena dampak dari serangan tersebut. Dengan tujuan yang timbul dari rumusan masalah yaitu agar dapat mengetahui aspek-aspek persoalan yang ada pada rumusan masalah, yang dimana tujuan lain yaitu agar meningkatkan pengetahuan untuk permasalahan ini.

Maka berdasarkan permasalahan yang ada dan mencoba dengan percobaan untuk menyelesaikan permasalahan yang ada, tentu hasil yang diharapkan dan diinginkan akan dapat menjawab untuk menyelesaikan permasalahan tersebut dengan mencoba sistem keamanan *firewall* dalam mengamankan serta mencegah dari kegiatan jahat *illegal man in the middle attack DNS spoofing*. Dengan manfaat untuk menjadi acuan dalam pengembangan penelitian agar kedepannya lebih baik lagi. Bagi penulis untuk menambah wawasan dari segi keamanan jaringan. Dan bagi pengguna *wireless* agar dapat berinteraksi dengan terhubung jaringan *wireless* aman dalam beraktivitas. Penulis merangkum penelitian ini, dimana penulis melakukan uji coba dengan memanfaatkan *software virtualbox* sebagai *virtual* mesin untuk menjalankan sistem operasi *kali linux* sebagai penyerang dan sistem operasi *ubuntu* sebagai korban dalam tahap uji coba penelitian ini.

Kali linux merupakan sistem operasi *linux* berbasis *debian* yang dikembangkan oleh *offensive security*. Antarmuka pengguna *kali linux* memiliki antarmuka pengguna grafis *(GUI)* yang sederhana dan tidak mencolok [5]. *Ubuntu* merupakan salah satu distro *linux open source*, penggunaan *linux* di *server* menjadi sangat populer [6].

Penulis juga memanfaatkan *tools ettercap* untuk menyerang melalui sistem operasi *kali linux* dan juga memanfaatkan *tools tcpflow* untuk melihat data yang di*input* oleh korban. Pemanfaatan *software* atau *tools* untuk mengamankan perangkat ketika terjadi serangan, penulis memanfaatkan *software wireshark* untuk mendeteksi penyerang dan *firewall iptables* untuk memblokir hak akses penyerang yang dimana ini terjadi ketika terhubung dengan jaringan *wireless* yang sama antara penyerang dan korban.

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 protokol 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* [7].

Tcpflow berguna untuk mendeteksi serta melihat data ketika korban meng*input*kan data sensitif di saat terjadi serangan yang dilakukan penyerang.

Wireshark berguna untuk dapat menganalisa paket data secara *real time*. Artinya, aplikasi *wireshark* ini akan melakukannya pantau semua paket data masuk dan keluar melalui antarmuka yang ditentukan pengguna sejauh ini. *Wireshark* dapat menganalisis paket data *real time* berarti aplikasi *Wireshark* sedang berjalan pantau semua paket data masuk dan keluar menampilkannya melalui antarmuka yang telah ditentukan [8].

2. METODE PENELITIAN

2.1 Metodologi Penelitian

Dalam penelitian ini penulis menggunakan metode kualitatif, yang dimana penulis ingin mencoba meningkatkan keamanan dengan menggunakan sistem keamanan *firewall* disaat terjadi *serangan man in the middle attack DNS spoofing*. Adapun untuk mendukung penelitian ini hal yang dilakukan oleh penulis ada beberapa tahapan, yaitu:

1. Studi literatur.

ISSN 2338-5677 Cetak
ISSN 2548-6646 Online

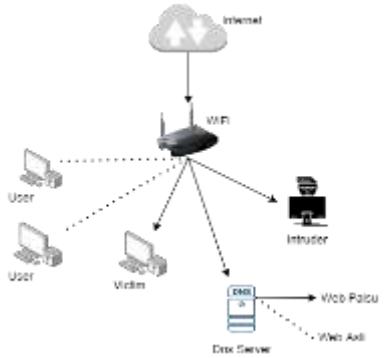
Mengumpulkan data-data pustaka untuk mendapatkan informasi-informasi yang dibutuhkan dalam mengerjakan penelitian.

2. Analisis.
   Menganalisa masalah yang terjadi pada penelitian berdasarkan fenomena permasalahan yang ada. Serta menganalisa keamanan dengan menerapkan sistem keamanan, agar dapat mencegah dari kejahatan serangan.
3. Perancangan serangan dan perancangan sistem keamanan agar mencegah dari serangan *MITM DNS spoofing*. Merancang serangan yang berdasarkan fenomena untuk diketahui bagaimana cara serangan tersebut bekerja dalam menjalankan perannya. Dan juga merancang sistem keamanan yang nantinya akan di implementasikan kepada korban untuk mengantisispasi dan juga dapat mencegah dari serangan tersebut berdasarkan fenomena penelitian.
4. Implementasi dan Pengujian
   Implementasi serta pengujian serangan dan juga implementasi serta pengujian sistem keamanan, sehingga mendapatkan hasil yang sesuai untuk menyelesaikan permasalahan yang ada pada permasalahan penelitian ini.
5. Hasil analisis.
   Hasil dari 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.
6. Kesimpulan.
   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.

2.2 Rancangan Penelitian

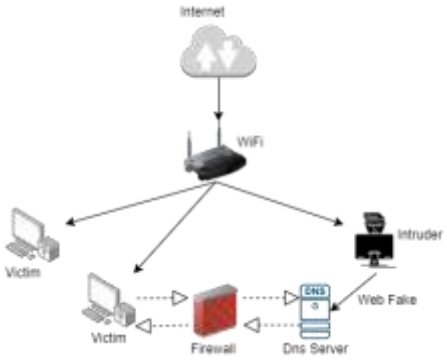
Adapun rancangan pada penelitian ini berlandaskan pada 2 aspek yaitu:

1. Dengan membangun topologi jaringan yang terhubung dengan jaringan *wireless* dan menyerang dengan memilih target



Gambar 1. Topologi Serangan Dengan Memilih Target

2. Dengan membangun topologi implementasi sistem keamanan *firewall*



Gambar 2. Topologi Implementasi Sistem Keamanan *Firewall Iptables*

2.3 Hardware dan Software

1. *Hardware* yang dibutuhkan yaitu :

- Laptop-ASUS dengan spesifikasi:

Processor : *Intel Core i5*-8265U
RAM : 4096MB
Hardisk : *SSD*
Bios : X330FA.305

- *Router Wireless* / *WiFi* Yang terhubung

2. *Software* yang dibutuhkan dalam pengujian :

Sistem operasi : *Windows* 11 (64-bit)
: *Kali Linux* (64-bit)
: *Ubuntu Desktop* 22.04 (64-bit)
Aplikasi : *Oracle* vm *VirtualBox*
: *Wireshark*
: *Ettercap-G*
: *Iptables*
: *TCPflow*
Penyerang: *VirtualBox*
: *Kali Linux*
: *Ettercap-G*
: *TCPflow*
Korban : *VirtualBox*
: *Ubuntu Desktop* 22.04
: *Wireshark*
: *Iptables*

ISSN 2338-5677 Cetak
ISSN 2548-6646 Online

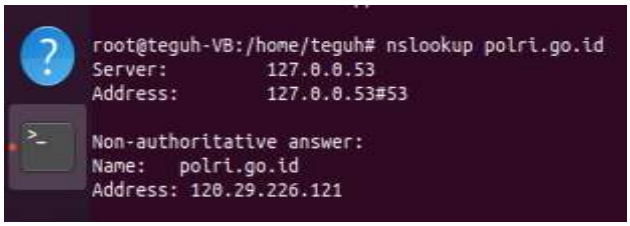
3. HASIL DAN PEMBAHASAN

Berdasarkan dari tahap pengumpulan data dengan studi literatur dan menganalisa permasalahan yang ada pada penelitian ini. Penulis akan menampilkan hasil dan juga pembahasan terkait dengan penelitian yang penulis lakukan ini.

3.1 Perangkat sebelum terjadi serangan

Penulis menggunakan perangkat *laptop* dengan menjalankan sistem operasi *ubuntu* untuk digunakan sebagai korban penyerangan. Penulis akan menampilkan tampilan perangkat dalam melakukan *browsing* sebelum terjadi serangan dengan target *website* yaitu *polri.go.id*. yang dimana penulis melakukan penyerangan dengan mengalihkan *website* asli menuju *website* palsu yang telah dimanipulasi oleh penyerang.

Gambar 3. *Domain* Polri Sebelum Diserang



Gambar 4. Alamat *IP* Asli Domain Polri

3.2 Proses Penyerangan Dengan Memilih Target

Tahap uji coba yang penulis lakukan dengan aspek penyerangan yaitu penyerangan dengan memilih target. Adapun tahap proses pengujian serangan dengan memilih target yaitu sebagai berikut:

Gambar 5. *OS Kali Linux*

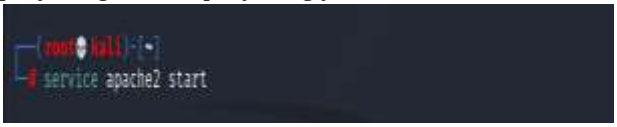
Tampilan sistem operasi *kali linux* yang telah terhubung dengan jaringan *wireless* kos yaitu *Wifi* Fermansio. Yang dimana, dengan terhubung nya *wireless Wifi* Firmansio, maka jaringan *wireless* tersebut yang digunakan untuk mengimplementasikan percobaan serangan.

Gambar 6. Alamat *IP* Penyerang

merupakan alamat *IP* penyerang yang didapat dengan meng*input*kan perintah *ifconfig* pada *terminal linux*, yang ber alamatkan 192.168.1.26. yang berguna untuk pengalihan alamat asli *website* yang akan diserang.

Gambar 7. Konfigurasi *DNS* Pada *Tools Ettercap*

Merupakan tampilan konfigurasi *domain* yang ingin di manipulasi oleh penyerang dengan menyimpannya pada *file ettercap* yaitu *file etter.dns*. Yang dimana situs *polri.go.id* merupakan situs asli daripada situs *website* polri yang ingin di manipulasi oleh penyerang. Dan mengalamatkan situs tersebut kepada alamat *IP* dari penyerang, *IP* dari penyerang yaitu 192.168.1.26.



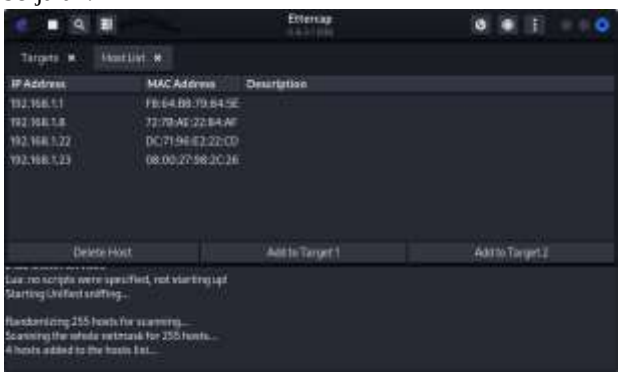
Gambar 8. Aktifasi *Apache2*

Merupakan tampilan aktifasi *apache2* untuk menjalankan perannya sebagai *web fake* untuk memanipulasi korban.

ISSN 2338-5677 Cetak
ISSN 2548-6646 Online

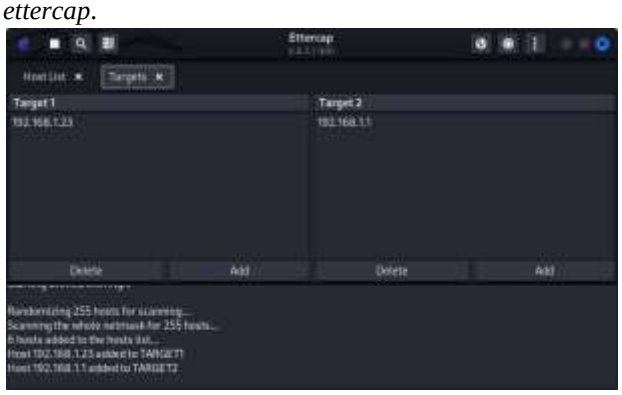
Gambar 9. Aktifasi Ettercap

Merupakan tampilan *tools ettercap* yang sudah aktif dan berjalan.



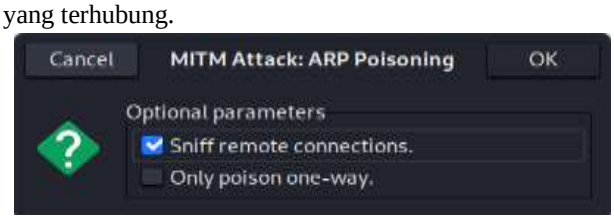
Gambar 10. Host Yang Ter*scanning*

Merupakan tampilan daripada *host-host* yang terhubung oleh jaringan setelah dilakukan *scanning* dengan *ettercap*.



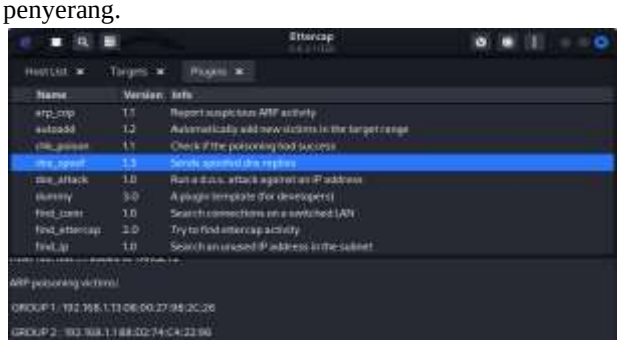
Gambar 11. Menentukan Target *Host*

Merupakan bentuk atau tampilan target yang telah penyerang pilih pada *host* yang terhubung. Pada gambar diatas, target 1 pada alamat *IP* 192.168.1.23 merupakan alamat *IP* dari pada korban, dalam hal ini sistem operasi *ubuntu* adalah target yang dipilih oleh penyerang sebagai korban. Dan pada gambar diatas, target 2 dengan alamat *IP* 192.168.1.1 merupakan alamat *gateway* pada jaringan yang terhubung.



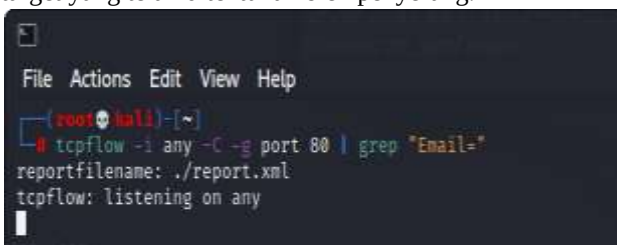
Gambar 12. Aktifasi *MITM ARP Poisoning*

Pada gambar diatas pelaku mengaktifkan fitur dari pada *ARP poisoning* agar dapat membajak, menangkap terjemahan dari *IP* logis yaitu *IP address* dan menterjemahkannya kepada *MAC address* dari pada penyerang.



Gambar 13. Aktifasi *DNS Spoofing*

Merupakan tahap dalam mengaktifkan fitur *dns_spoof* pada *ettercap*, sehingga serangan dapat berjalan kepada target yang telah ditentukan oleh penyerang.



Gambar 14. Aktifasi *Tools Tcpflow*

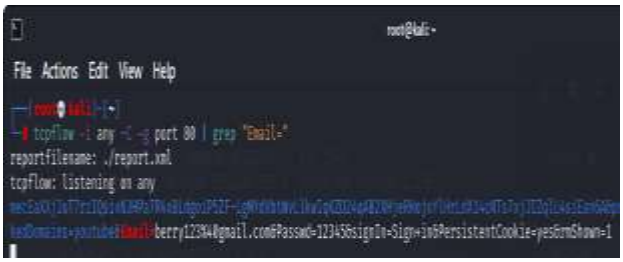
Merupakan tahap untuk mengaktifkan *tools tcpflow* dengan menginputkan perintah *tcpflow -i any -C -g port 80 | grep "Email="*. Maka *tcpflow* dapat berjalan dan aktif dengan melaksanakan perannya sebagai mengcapture data yang di*input*kan oleh korban.

Setelah melakukan tahap proses dari penyerangan dengan model pilihan pertama yaitu dengan memilih target. Penulis akan menampilkan hasil ketika telah terjadi serangan dengan menargetkan *website polri.go.id*. Adapun hasil yang di dapat ketika telah melakukan proses penyerangan dengan memilih target yaitu:

Gambar 15. *Domain* Polri Setelah Diserang

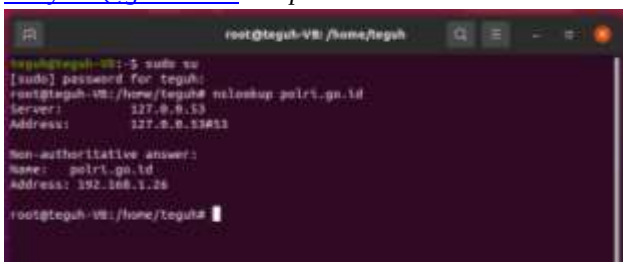
Merupakan tampilan *website polri.go.id* ketika terjadi serangan. Dengan mengubah tampilan *website* menuju halaman pada sistem penyerang.

ISSN 2338-5677 Cetak
ISSN 2548-6646 Online



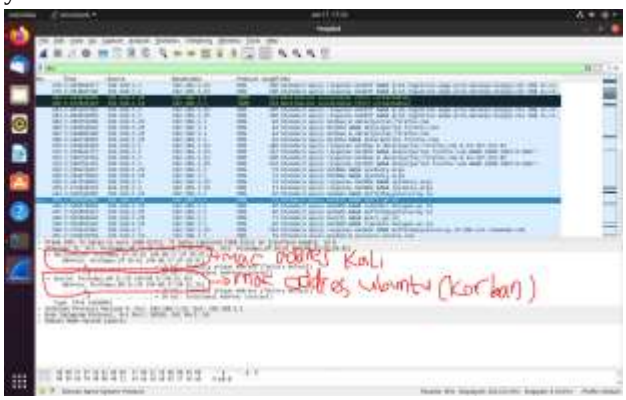
Gambar 16. Data Yang Didapat Dari *Tools Tcpflow*

Merupakan informasi data yang terlihat oleh penyerang ketika korban memasukkan informasi penting kedalam *web* palsu tersebut. Yaitu data yang didapat *email:* *berry123@gmail.com* dan *password*: 12345



Gambar 17. *IP Domain* Polri Setelah Diserang

Merupakan tampilan alamat dari *domain polri.go.id* ketika terjadi serangan. Yang dimana alamat dari *domain* polri tersebut mengarah pada alamat *IP* sistem penyerang yaitu 192.168.1.26.



Gambar 18. Tampilan Protokol *DNS* Pada *Tools Wireshark*

Merupakan aliran transmisi pada alamat *gateway*, untuk mendapatkan alamat *IP domain* polri, telah dialihkan menuju alamat fisik dari penyerang yaitu 08:00:27:df:26:81. Alamat *IP* korban 192.168.1.23 yang ingin mengakses *domain* polri dikirim kepada alamat *gateway* 192.168.1.1, Untuk memberitahu kepada korban alamat *server* dari pada polri. Sehingga alamat *gateway* yang telah ter*duplicate* merespon alamat korban yang mengakses *domain* polri. Dan alamat *gateway* memberikan alamat aliran daripada *domain* polri menuju alamat *IP* penyerang. Maka tampilan dari pada situs polri akan terarahkan pada situs yang telah di bentuk pada *server web* di sistem penyerang.

3.3 Hasil Serangan Dengan Menghitung Packet Loss

Penulis melakukan uji coba serangan sebanyak 3 kali percobaan dan juga pengujian. Penulis menghitung *packet loss* berdasarkan statistik data *packet* pada *filtering* protokol *DNS* untuk mendapatkan hasil presentase pada *packet loss* ketika terjadi serangan. Dengan melihat dan mendapatkan data dari *software wireshark*.

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* serangan 1

Rumus untuk menghitung *packet loss* yaitu :
((*packet* yang dikirim – *packet* yang diterima) / *packet* yang dikirim x 100%)
= 954 – 730 / 954
= 224 / 954
= 0,234 x 100%
= 0,234 % *packet loss* serangan 2

Rumus untuk menghitung *packet loss* yaitu :
((*packet* yang dikirim – *packet* yang diterima) / *packet* yang dikirim x 100%)
= 192 – 136 / 192
= 56 / 192
= 0,291 x 100%
= 0,291 % *packet loss* serangan 3

Tabel 1. Tabel Hasil Kategori *Packet Loss* Percobaan Serangan

Percobaan Serangan	*Packet Loss*	Kategori
Serangan 1	0,154 %	Sangat Bagus
Serangan 2	0,234%	Sangat Bagus
Serangan 3	0,291%	Sangat Bagus

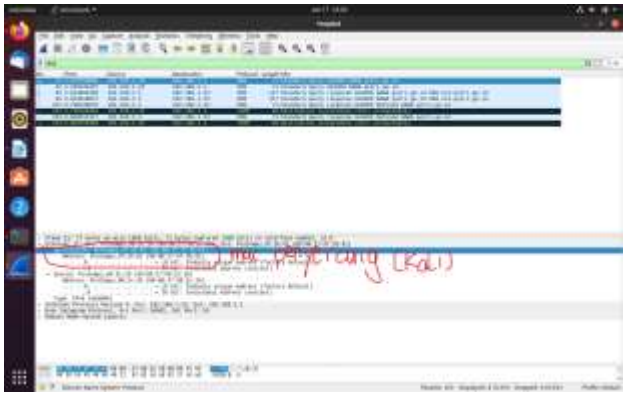
Tabel diatas merupakan hasil keseluruhan dari uji coba dalam menghitung *packet loss* ketika terjadi serangan, dan tercapture oleh aplikasi *wireshark*. Yang dimana berarti serangan tersebut melancarkan serangan dengan tidak terdapatnya *packet loss*. Yang berarti serangan tersebut berhasil dan lancar dalam menjalankan aksinya.

3.4 Proses Implementasi Sistem Keamanan Firewall Iptables

Berdasarkan analisa implementasi serangan yang terjadi dengan serangan memilih target yang penulis lakukan. Penulis melakukan percobaan implementasi sistem keamanan kepada *website polri.go.id*. Hasil percobaan

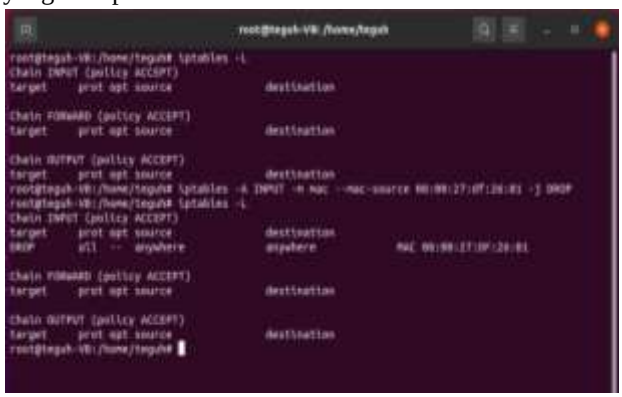
ISSN 2338-5677 Cetak
ISSN 2548-6646 Online

serangan yang dimana *website domain* polri menampilkan halaman palsu dari penyerang. Yaitu *domain polri.go.id.*



Gambar 19. Tampilan Protokol DNS Pada Wireshark

Merupakan tampilan *DNS* yang terkena serangan dan menemukan aliran alamat korban yang terduplikat dengan aliran alamat gateway yang ter arah pada alamat fisik penyerang. Alamat fisik penyerang yang di dapat dari sang korban yaitu dengan *MAC address* 08:00:27:df:26:81 yang tercapture oleh *wireshark.*

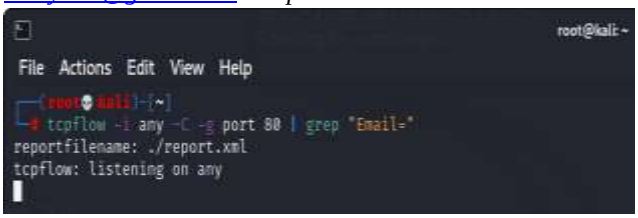


Gambar 20. Konfigurasi *Firewall Iptables*

Merupakan proses konfigurasi *firewall* yang dimana perintah dari gambar tersebut merupakan perintah untuk memblokir *MAC address* dari penyerang. Yang bertujuan agar tidak mendapatkan informasi penting dari korban dengan menerapkan kejahatan dari penyerang tersebut. Perintah *iptables -L* adalah perintah yang bertujuan untuk melihat isi dari pada konfigurasi sistem *firewall* tersebut. Perintah *iptables -A INPUT -m mac –mac-source 08:00:27:df:26:81 -j DROP*, merupakan perintah untuk menginputkan konfigurasi yang dimana *firewall* diminta untuk memutuskan aliran atau memblokir hak akses yang dialamatkan pada *MAC address* 08:00:27:df:26:81 yang merupakan alamat *MAC addres* dari penyerang.

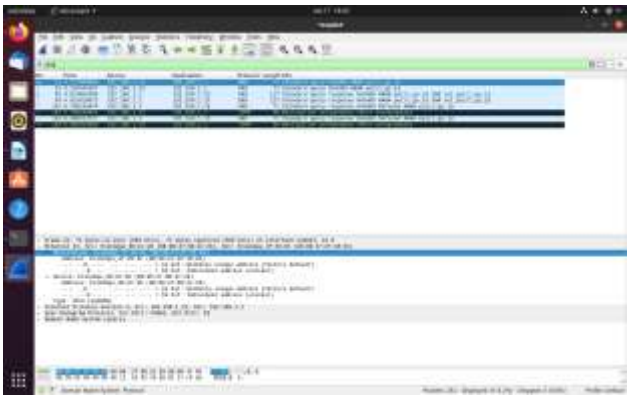
Gambar 21. *Domain* Polri Setelah Diamankan

Merupakan hasil tampilan setelah terbentuknya sistem keamanan yang telah di konfigurasi oleh penulis dengan sistem *firewall iptables*. Yang menghasilkan tampilan yang sama dengan tampilan saat terjadi serangan, tetapi aliran pengiriman data baik penyerang menuju korban dan korban menuju penyerang terputus. Sehingga penyerang tidak mendapatkan informasi yang diinginkan dari korban. Tampilan pada gambar diatas, korban mencoba menginputkan data dengan *username* : *berry123@gmail.com* dan *password* : 12345.



Gambar 22. Tampilan *Tcpflow*

Menunjukan hasil dari pada peran *firewall* dalam menjalankan tugasnya dengan memblokir hak akses dari pada penyerang, sehingga penyerang tidak mendapatkan hasil yang berupa informasi penting dari sang korban.



Gambar 23. Protokol *DNS* Pada *Wireshark*

Merupakan hasil tampilan daripada protokol *DNS* setelah dibentuk keamanan dengan *firewall iptables*. Menghasilkan bahwa *DNS* dalam keadaan normal, dengan *destination* atau tujuan aliran data masih tertuju pada *MAC address* penyerang, tetapi aliran data tidak terkoneksi atau terputus sehingga aliran data tidak dapat

ISSN 2338-5677 Cetak
ISSN 2548-6646 Online

berjalan dan terblokir aksesnya ketika dibentuknya sistem keamanan *firewall iptables.*

3.5 Hasil Analisa

Dengan melihat hasil dari beberapa percobaan dan juga melihat parameter dari dampak yang terjadi, dan penulis juga telah melakukan percobaan sistem keamanan dengan menggunakan *firewall iptables*. Dengan hasil daripada implementasi uji coba bentuk keamanan, penulis berhasil mencegah serangan *man in the middle attack DNS spoofing*, dan dibuktikan dengan hasil implementasi bentuk keamanan *firewall iptables,* yang dimana koneksi data terputus dan terblokir sehingga penyerang tidak mendapatkan data yang bersifat penting dari sang korban.

Dan adapun solusi lain yang ditawarkan oleh penulis agar dapat terhindar dari serangan tersebut yaitu dengan berhati-hati dalam mengakses situs yang tidak dipercaya. Dan untuk mengetahui situs yang dapat dipercaya dapat diketahui dengan melihat *(SSL) secure sockets layer* pada situs yang ingin kita akses. *SSL* berguna untuk mengamankan situs *website* dari serangan yang tidak diketahui oleh pengguna, maka dari itu penulis memberikan solusi untuk dapat terhindar dari serangan tersebut dengan melihat *SSL* pada suatu situs *website* yang ingin dituju. Agar dapat melihat *SSL* yaitu, *SSL* dapat dilihat pada lambang gembok yang terkunci pada sisi kiri situs *web* yang ingin diakses yang menandakan situs tersebut dapat dipercaya dan aman. Sehingga dengan adanya lambang tersebut, merupakan tanda situs tersebut terpercaya dan aman untuk diakses.

4. KESIMPULAN

Berdasarkan hasil dan pembahasan pada penelitian yang penulis lakukan. Penulis menyimpulkan bahwa dengan menggunakan *software wireshark* dapat menganalisa keamanan jaringan dari serangan *man in the middle attack DNS spoofing*, kemudian dengan berjalannya percobaan serta pengujian yang dilakukan, mendapatkan solusi dengan melihat *SSL* agar terhindar dari serangan tersebut, dengan berjalannya proses penelitian ini menghasilkan cara untuk mengetahui teknik serangan ini berjalan melancarkan aksinya dengan memanfaatkan *tools ettercap* dan didukung *OS kali linux*, dengan berjalannya percobaan serta pengujian pada penelitian ini menghasilkan bahwa sistem keamanan *firewall iptables* dapat mencegah serta memblokir penyerang ketika terkena dampak serangan *man in the middle attack DNS spoofing,* dengan berjalannya peroses pengujian yang telah dilakukan menghasilkan bahwa *software wireshark* dapat mengetahui alamat *MAC address* penyerang.

5. DAFTAR PUSTAKA

[1] N. Andiyani *et al.*, “IMPLEMENTASI MAN IN THE MIDDLE ATTACK PADA ALGORITME BLAKE2S BERBASIS LoRa,” vol. 6, no. 2, pp. 1–6, 2022.

[2] randi candra kirana Yudi mulyanto, Herfandi, “ANALISIS KEAMANAN WIRELESS LOCAL AREA NETWORK (WLAN) TERHADAP SERANGAN BRUTE FORCE DENGAN METODE PENETRATION TESTING,” vol. 4, no. 1, pp. 26–35, 2022.

[3] D. Qadri, T. Y. Arif, and A. Azmi, “Analisis Tingkat Kinerja Jaringan Wireless Ieee 802.11N Menggunakan Mikrotik,” *J. Komputer, Inf. Teknol. dan Elektro*, vol. 6, no. 2, pp. 21–26, 2021, doi: 10.24815/kitektro.v6i2.21848.

[4] G. H. A. Kusuma, “… Skema Sistem Keamanan Jaringan Web Server menggunakan Web Application Firewall dan Fortigate untuk Mencegah Kebocoran Data di Masa Pandemi Covid-19,” *J. Informatics Adv. …*, vol. 2, no. 2, pp. 1–4, 2021, [Online]. Available: http://journal.univpancasila.ac.id/index.php/jiac/article/view/3259

[5] M. A. Adiguna and B. W. Widagdo, “Analisis Keamanan Jaringan WPA2-PSK Menggunakan Metode Penetration Testing (Studi Kasus : Router Tp-Link Mercusys Mw302r),” *J. SISKOM-KB (Sistem Komput. dan Kecerdasan Buatan)*, vol. 5, no. 2, pp. 1–8, 2022, doi: 10.47970/siskom-kb.v5i2.268.

[6] Z. M. Subekti, H. Setiawan, Satria, W. M. Wijaya, A. Hafiz, and Warsudi, “PERANCANGAN INFRASTRUKTUR DOMAIN NAME SERVER LOKAL MENGGUNAKAN UBUNTU SERVER 16.04 PADA PT. XYZ,” no. 2, p. 6, 2020.

[7] 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.

[8] T. M. Diansyah, “Analisa Pencegahan Aktivitas Ilegal Didalam Jaringan Menggunakan Wireshark,” *J. TIMES*, vol. IV, no. 2, pp. 20–23, 2015, [Online]. Available: http://ejournal.stmik-time.ac.id/index.php/jurnalTIMES/article/view/229