Terbit online pada laman web jurnal : **http://jurnal.iaii.or.id**

JURNAL RESTI

(Rekayasa Sistem dan Teknologi Informasi)

Vol. 1 No. 3 (2017) 277 – 282 ISSN Media Elektronik : 2580-0760

Analisis Keamanan Lalu Lintas Paket Data Pada Ubuntu Menggunakan Metode *Attack Centric*

Feizil Afrizal[a], Rometdo Muzawi[b], Yoyon Efendi[c]
Teknik Informatika, STMIK Amik Riau, feizilafrizal@gmail.com
Manajemen Informatika, STMIK Amik Riau, rometdomuzawi@stmik-amik-riau.ac.id
Teknik Informatika, STMIK Amik Riau, yoyonefendi@stmik-amik-riau.ac.id

Abstract

Data traffic security in a network is very important, especially on a large scale such as companies, agencies and universities that have a lot of personal data. Effective data security is required, effective, flexible, not consuming enough time, big expense and have good advantages and shortcomings that are not too big so that data is not easy to be manipulated, analyzed, and attacked by irresponsible party. In the security analysis of data traffic on the ubuntu operating system is using Attack Centric method where each security attack will be analyzed its characteristics, after analyzing these characteristics then in the security mechanism for defense. This study aims to produce a system for analyzing, documenting attacks and how to handle it simply, in the hope that this analysis results, can reduce crime in the virtual world, to users who are not very proficient in cyberspace, and increase knowledge for users of the Internet network

Keywords : Data Security, Ubuntu 12.04.5 LTS, Centric Attack Method

Abstrak

Keamanan lalu lintas data di suatu jaringan sangatlah penting, apalagi berada pada skala yang cukup besar seperti perusahaan, instansi maupun perguruan tinggi yang memiliki banyak data bersifat pribadi. Diperlukan keamanan data yang efisien, efektif, fleksibelitas, tidak memakan waktu yang cukup banyak, pengeluaran biaya yang besar dan memiliki kelebihan yang baik serta kekurangan yang tidak terlalu besar supaya data tidak mudah di manipulasi, di analisis, dan di serang oleh pihak yang tidak bertanggung jawab. Pada analisis keamanan lau lintas data pada sistem operasi *ubuntu* ini menggunakan metode *Attack Centric* dimana setiap penyerangan keamanan akan dianalisis karakteristiknya, setelah menganalisis karakteristik tersebut barulah di teliti mekanisme keamanan untuk pertahannya. Penelitian ini bertujuan untuk menghasilkan sebuah sistem untuk menganalisis, mendokumentasi serangan dan cara penanganannya secara sederhana, di harapkan dengan adanya hasil analisis ini, dapat mengurangi kejahatan di dunia maya, terhadap *user* yang tidak terlalu mahir di dunia maya, dan menambah pengetahuan bagi pengguna jaringan internet.

Kata Kunci : *Keamanan Data, Ubuntu 12.04.5 LTS, Metode Attack Centric*

1. Pendahuluan

Dalam jaringan internet terdapat dua sisi yang berbeda dalam hal keamanan lalu lintas jaringan data, di satu sisi banyak usaha yang di lakukan untuk mempertahankan dan menjamin keamanan lalu lintas jaringan data, namun di sisi lain ada beberapa pihak tertentu yang bermaksud untuk melakukan pencurian data, dan perusakan lalu lintas jaringan data. Bentuk serangan tersebut antara lain dapat juga di sebut dengan, ARP (*Address Resolution Protocol*) *Poisoning* dan DNS(*Domain Name System*) *Spoofing*. Umumnya user biasa tidak akan mengenali apa dampak dari kedua penyerangan tersebut.

Pada dasarnya di dalam dunia maya siapa saja bisa terserang seperti di atas oleh sebab itu *administrator* jaringan ataupun *user* biasa harus dapat memahami karakteristik dalam penyerangan tersebut agar dapat menemukan solusi pertahanan yang nantinya dapat mempertahankan diri dari ancaman penyerang dalam pencurian data ataupun perusakan jaringan. Menuju dari permasalah yang telah di paparkan di atas maka peneliti sebagai penulis ingin mempermudah dalam permasalah tersebut dengan melakukan analisis

keamanan lalu lintas data pada sistem operasi ubuntu menggunakan metode *attack centric* yang akan menganalisis setiap karakteristik penyerangan keamanan dan akan di teliti mekanisme keamanan untuk tindakan pertahannya. Pada analisis tersebut akan menghasilkan sebuah sistem untuk mendokumentasi serangan dan cara penanganannya secara sederhana, di harapkan dengan adanya hasil analisis ini, dapat mengurangi kejahatan di dunia maya, terhadap *user* yang tidak terlalu mahir di dunia maya, dan menambah pengetahuan bagi pengguna jaringan internet.

2. Tinjauan Pustaka

2.1 Analisis Paket Data.

Menyatakan bahwa [1] analisis data adalah proses mencari dan menyusun data yang diperoleh dari hasil wawancara, catatan lapangan, dan bahan bahan lain secara sistematis sehingga mudah dipahami dan temuannya dapat diinformasikan kepada orang lain.

Sedangkan [2] Paket data adalah entitas dasar dari semua sistem komunikasi. Keamanan jaringan demikian berarti keamanan dari paket data. Sebuah paket data adalah blok yang paling dasar komunikasi yang melibatkan aliran *streamline* terbatas replika lainnya untuk mengirimkan informasi dari satu perangkat ke perangkat lainnya. Sebuah paket data yang terkandung dalam segmen data yang menimpan informasi lain seperti protokol yang digunakan, tujuan *hardware* alamat dan lain-lain. Singkatnya, identitas setiap paket yang datang dari sumber tidak bisa diandalkan dapat dideteksi dengan mempelajari isinya. Manajemen trafik data, pengukuran trafik jaringan komputer dan *sniffing* adalah beberapa produk dari *packet capture*, *packet capture* juga digunakan sebagai basis untuk berbagai macam sistem keamanan.

2.2 Keamanan Jaringan Komputer.

Tujuan utama dari keamanan sistem adalah memberikan jalur yang aman antar-entitas yang saling bertukar informasi dan untuk menyediakan perlindungan data [3]. Insiden keamanan jaringan komputer adalah suatu aktivitas yang berkaitan dengan jaringan komputer, di mana aktifitas tersebut memberikan implikasi terhadap keamanan.

2.3 Jenis Serangan terhadap Keamanan Komputer.

Pada dasarnya, menurut jenisnya, serangan terhadap suatu data dalam suatu jaringan dapat dikategorikan menjadi 2, yaitu :

a. Serangan Pasif *(Passive Attacks)* Serangan pasif adalah serangan pada sistem autentikasi yang tidak menyisipkan data pada aliran data (*data stream),* tetapi hanya mengamati atau memonitor pengiriman informasi ke tujuan. Informasi ini dapat digunakan di lain waktu oleh pihak yang tidak bertanggung jawab. Serangan pasif yang mengambil suatu unit data dan kemudian menggunakanya untuk memasuki ses autentikasi dengan berpura-pura menjadi user autentik/ asli disebut dengan *replay attack.* Beberapa informasiautentikasi seperti password atau data *biometric* yang dikirim melalui transmisi elektronik dapat direkam dan kemudian digunakan untuk memalsukan data yang sebenarnya. Serangan pasif ini sulit untuk dideteksi karena penyerang tidak melakukan perubahan data. Oleh sebab itu untuk mengatasi serangan pasif ini lebih ditekankan pada pencegahan daripada pendeteksiannya.

b. Serangan Aktif (*Active Attacks)* Serangan aktif adalah serangan yang mencoba memodifikasi data, mencoba mendapatkan autentikasi, atau mendapatkan autentikasi dengan mengirimkan paket-paket data yang salah ke data stream atau dengan memodifikasi paket-paket yang melewati data stream. Kebalikan dari serangan pasif, serangan aktif sulit untuk dicegah karena untuk melakukannya dibutuhkan perlindungan fisik untuk semua fasilitas komunikasi dan jalur-jalurnya setiap saat. Yang dapat dilakukan adalah mendeteksi dan memulihkan keadaan yang disebabkan oleh serangan ini.

2.4 Metode *Attack Centric*

Metode yang diterapkan untuk melakukan penelitian ini adalah metode *Attack-Centric* [4]. Metode ini dilakukan dengan tiga langkah berikut:

1. Menganalisis apakah tujuan dari serangan tersebut contoh: untuk menganalisis jenis trafik dengan menangkap dan menganalisis paket-paket data yang ada pada trafik tersebut.
2. Menganalisis bagaimana sebuah serangan dapat terjadi contoh: menentukan titik di mana seorang penyerang harus mengawasi paket-paket yang melintas.
3. Menentukan mekanisme keamanan apa yang diperlukan untuk mencegah serangan tersebut. Contoh hasil pada metode ini adalah sebagai berikut: Jika sebuah serangan telah dianalisis adalah serangan yang bertujuan untuk menangkap dan menganalisis paket-paket data, maka mekanisme keamanan yang dibutuhkan untuk mencegah serangan tersebut adalah dengan melakukan mekanisme *anonymous connection* kepada semua *user* yang ada dalam jaringan. Hal ini akan mencegah seseorang untuk menentukan titik di mana dia harus mengawasi paket dikarenakan IP Address *user* yang ada dalam jaringan akan tersembunyi.

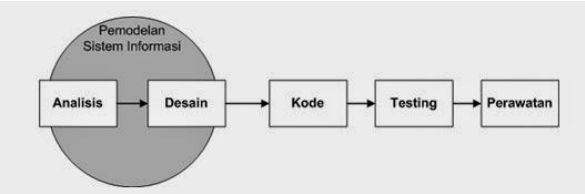
2.5 *Wireshark*

Wireshark adalah penganalisis paket gratis dan sumber terbuka.Perangkat ini digunakan untukpemecahan masalah jaringan, analisis,perangkat lunak dan pengembanganprotokol komunikasi, dan pendidikan. Awalnya bernama *Ethereal*, pada Mei 2006 proyek ini berganti nama menjadi *Wireshark* karena masalah merek dagang [3]

Wireshark merupakan salah satu network analysis tool, atau disebut juga dengan *protocol analysis* tool atau packet *sniffer* [5]. *Wireshark* dapat digunakan untuk troubleshooting jaringan, analisis, pengembangan *software* dan *protocol* serta untuk keperluan edukasi.*Wireshark* dikenal dengan nama *Ethereal*

3. Metodologi Penelitian

Perangkat lunak dikembangkan dengan menggunakan Metode yang tepat, pada objek dan aplikasi informasi mengenai *ARP Poisoning* dan *DNS Spoofing*, berdasarkan kebutuh yang ada maka digunakan menggunakan Metode Sekuensial Linier atau *Waterfall Development Model*, dimana metode ini memiliki 5 tahapan seperti gambar dibawah ini :



Gambar 1. Model Waterfall

1. Analisis

Pada proses ini dilakukan penganalisisan dan pengumupulan kebutuhan sistem yang meliputi informasi mengenail *ARP Poisoning* dan *DNS Spoofing*, juga berserta penanganannya hasil dari pengumpulan data tersebut nantinya akan di perlihatkan kepada *user* yang akan menggunakan aplikasi tersebut.

2. Desain

Pada tahap ini akan dipikirkan semua informasi yang berkaitan dengan *ARP Poisoning* dan *DNS Spoofing*, metode *attack centric netsh arpon* dan *firewall* agar nantinya dapat ditampilkan pada aplikasi yang akan memudahkan user dalam penggunaannya. Dalam tahap ini digunakan alat bantu seperti penggunaan *navifasi hirarki*, *use cas* diagram dan *sequence* diagram.

3. Kode

Pada tahapan pengkodeaan ini merupakan perancangan didesain ke bentuk yang dapat di mengerti oleh mesin, yaitu pada tahapan ini akan digunakan bahasa pemrograman php

4. Testing

Setelah proses pengkodeaan selesai, berikutnya akan dilanjutkan dnegan pengujian program perangkat lunak, yaitu bermaksud untuk memeriksa segala kemungkinan terjadinya kesalah dan memeriksa apakah hasil dari analisis yang telah di buat sesuai dengan hasil yang diinginkan.

5. Perawatan

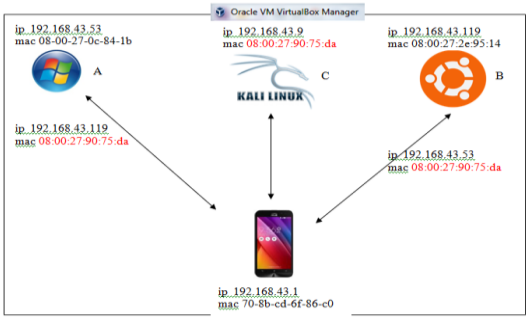
Proses pemeliharaan merupakan bagian paling terakhir dari pemodelan ini dan dilakukan setelah perangkat lunak dipergunakan. Kegiatan yang dilakukan pada proses pemeliharaan antara lain :

a. *Corrective Maintenance* : yaitu mengoreksi apabila terdapat kesalahan pada perangkat lunak, yang baru terdeteksi pada saat perangkat lunak dipergunakan.
b. *Adaptive Maintenance* : yaitu dilakukannya penyesuaian/perubahan sesuai dengan lingkungan yang baru, misalnya hardware, periperal, sistem operasi baru, atau sebagai tuntutan atas perkembangan sistem komputer, misalnya penambahan driver, dll.

4. Hasil dan Pembahasan

4.1 *Topologi Penyerangan ARP Poisoning*

Pada tahap ini akan ditampilkan langkah dari penggunaan ettercap dalam penyerangan beserta tabel arp ubuntu dan windows 7 Untuk dapat melakukan penyerangan arp poisoning terhadapat target di perlukan 3 komputer atau mesin virtual dan 1 buat Modem atau Hotspot untuk koneksi ke internet. Agar dapat mempermudah dalam tahap analisis berikut topologi dari penyerangan ARP Poisoning.



Gambar 2. Topologi Penyerangan ARP Poisoning

Pada Gambar 2 dapat di lihat proses terjadinya penyerangan ARP Poisoning di dalam jaringan, proses tersebut terjadi yakni ketika komputer A mengirimkan paket data ke komputer B di dalam jaringan, maka komputer C dapat mempoisoning paket tersebut agar nantinya paket ditujukan ke komputer C dahulu kemudian bari dilanjutkan kembali ketujuan asal yaitu komputer B, ARP Poisoning ini nantinya akan mengganti MAC Address komputer B dengan Mac

Address komputer C di tabel ARP komputer A, dan bigitu juga sebaliknya, MAC Address komputer A akan tergantikan dengan MAC Address komputer C di tabel ARP komputer B.

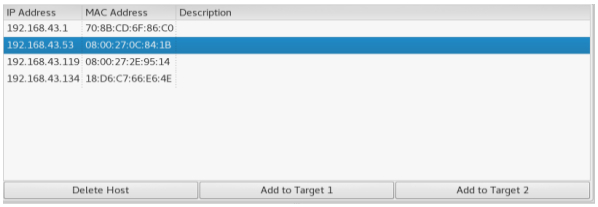
4.2 Penyerangan Arp Poisoning

Pada Gambar 3 terdapat aplikasi Ettercap yang dimana nantinya dengan aplikasi ini akan dilakukan penyerangan ARP Poisoning terhadap 2 komputer yang saling berkomunikasi.

Gambar 3. Aplikasi Ettercap

4.3 Pemilihan Target Arp Poisoning

Pada Gambar 4 terdapat pemilihan target dari ARP poisoning yang akan dilakukan yaitu target 1 adalah windows 7 192.168.43.53 dengan MAC Address 08-00-27-0c-84-1b dan target 2 adalah ubuntu dengan ip address 192.168.43.119 dan mac address 08:00:27:2e:95:14.

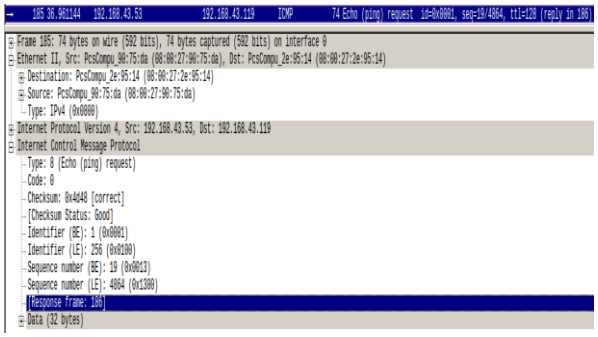


Gambar 4. Target ARP Poisoning Pada Ettercap

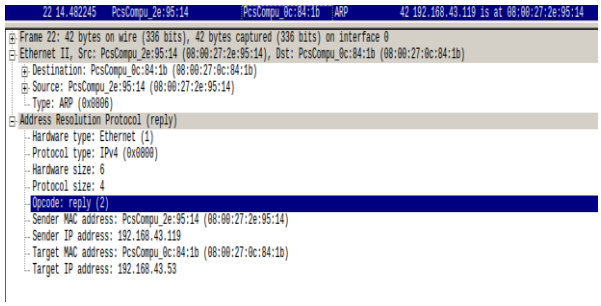
4.4 Analisis Paket Data Protocol ICMP Terkena Poisoning

Pada Gambar 5 dapat di lihat hasil penangkapan dari packet data protokol icmp yang telah terkena poisoning, pada frame 185 IP address windows 7 meminta ping kepada destination ubuntu dengan protokol ICMP, panjang packet bytes 74, TTL (Time To live) 128 dan dibalas damal response frame 186. Pada packet details di Ethernet II yaitu MAC address dengan sumber 08:00:27:90:75:da yang dimana sebenarnya MAC address tersebut merupakan MAC address dari penyerang yaitu kali linux yang dimana MAC address tersebut memiliki ip 192.168.43.9 menuju ke destination komputer B.

Pada frame 186 packet ICMP membalas pesan sebelumnya yang dikirim oleh komputer A. di packet list dapat di lihat pada source IP address komputer B membalas ke komputer komputer A dengan protocol ICMP panjang bytes 74, TTL (Time To live) 64 dan request frame 185. Di packet detail Ethernet II terdapat source MAC address 08:00:27:90:75:da menuju ke destination MAC address komputer B yang dimana MAC address tersebut merupakan MAC address kali linux.



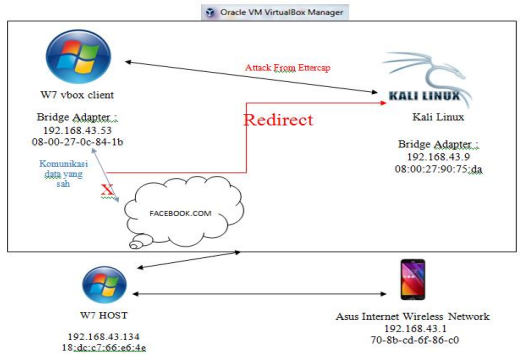
Gambar 5. Penangkapan Data ICMP Poisoning



Gambar 6. Penangkapan Data ICMP Terkena Poisoning dari komputer B ke A

4.5 Topologi Penyerangan DNS Spoofing

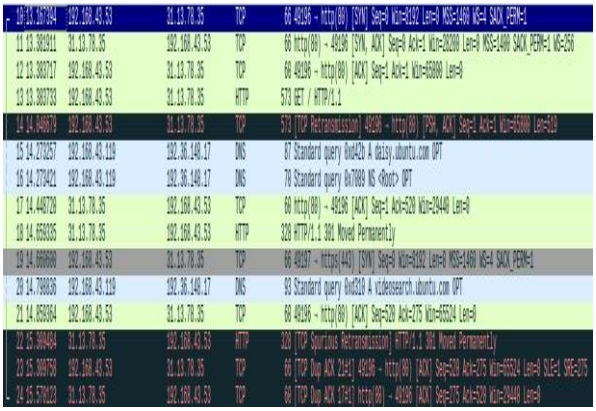
Untuk dapat melakukan penyerangan terhadap terhadap DNS spoofing diperlukan 1 mesin virtual dengan sistem operasi kali linux dan 1 mesin virtual dengan sistem operasi windows 7, beserta komputer host dan jaringan internet. DNS spoofing nantinya akan meredirect website facebook.com ke website palsu yang telah di buat oleh si penyerang, untuk mempermudah pemahaman lihat Gambar 7.



Gambar 7. Topologi Penyerangan ARP Poisoning

4.6 Analisis Paket Data DNS Spoofing

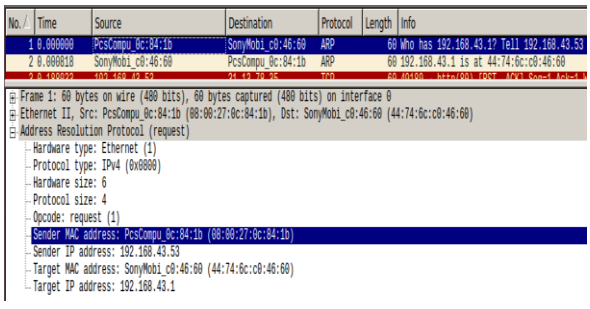
Pada tahap ini akan di tampilkan beberapa screenshoot hasil dari penyerangan DNS spoofing yang telah di jalankan. untuk lebih memahami bagaimana berjalannya DNS spoofing tersebut, terlihat pada Gambar 8 dari frame 10-14 17-19 21-24 merupakan proses berjalannya komunikasi antara komputer windows 7 dengan facebook.com, dengan menggunakan protocol TCP komputer client memulai pembentukan proses dari komunikasi yaitu dengan mengirimkan segmen TCP tanpa payload data, maka dari itu ukuran dari pengiriman begitu kecil, kemudian salah satu flag pada header TCP yaitu flag SYN di set menjadi 1 dengan panjang packet bytes 66 melalui port http dari 49196 port HTTP 80.



Gambar 8 Tampilan Akses Windows 7 Ke Facebook.com Sebelum DNS Spoofing Dijalankan

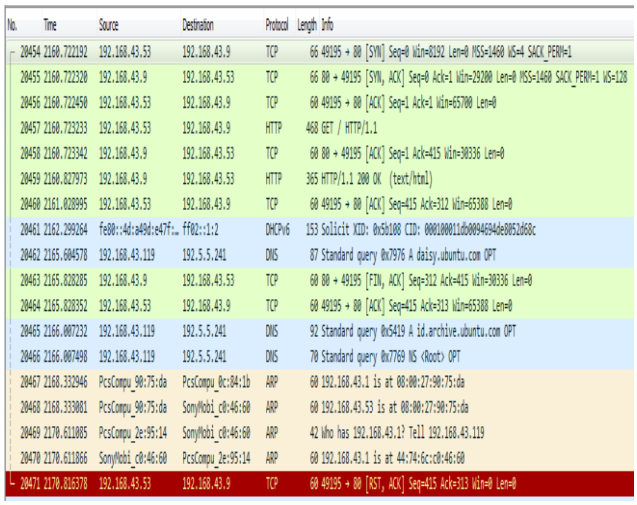
Pada Gambar . dapat di lihat yaitu terdapat proses pengenalan mac address terhadap modem yaitu pada frame 1 terdapat kolom Source MAC address dari 08:00:27:0c:84:1b (windows 7), yang menuju ke destination 44:74:6c:c0:46:60 (Mac sony xperia) dengan menggunakan protocol ARP yang berisikan informasi "siapa yang memiliki IP address 192.168.43.1?" yang mengatakan 192.168.43.53.

Pada kolom packet detail, di bagian ARP request terdapat informasi pengirim MAC address yaitu 08:00:27:0c:84:1b dengan IP address 192.168.43.53 kepada target MAC address 44:74:6c:c0:46:60 dengan IP address 192.168.43.1



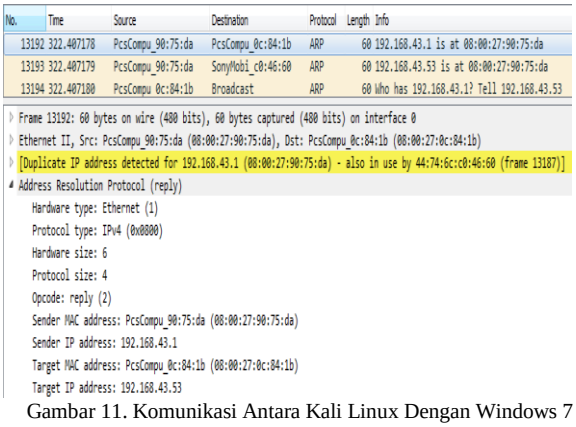
Gambar 9. Paket Data Wireshark windows 7 Belum Terkena Dns Spoofing

Dapat di lihat pada Gambar 10. Pada frame 20454-20460, 20463-20464, 20471 semua frame tersebut merupakan penangkapan paket data komunikasi antar komputer windows 7 dan kali linux ataupun sebaliknya, komunikasi berikut terjadi karna dns spoofing sudah di jalankan, maka dari itu semua akses ketika ip 192.168.43.53 (windows 7) melakukan akses ke facebook.com semuanya terarahkan ke 192.168.43.9 yaitu (kali linux)



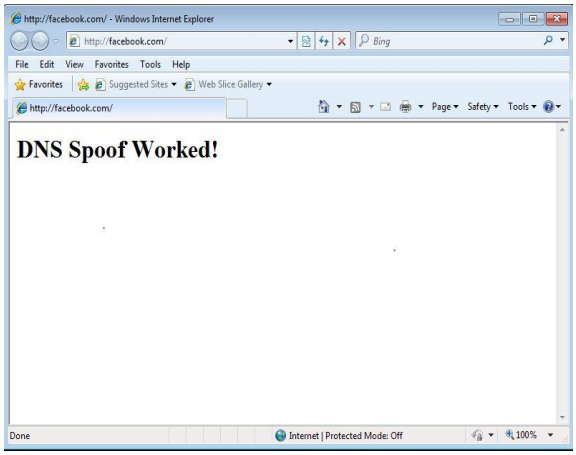
Gambar 10. Proses Akses Terhadap Facebook Di Wireshark Setelah Di Lakukan DNS Spoofing.

Dapat di lihat pada No. 13192 *source mac address* 08:00:27:90:75:da (kali linux) mengirimkan packet bytes dengan panjang packet 60 ke destination mac address 08:00:27:0c:84:1b (windows 7) dengan informasi 192.168.43.1 berada di 08:00:27:90:75:da (kali linux), pada gambar sebelumnya dapat di lihat bahwa mac address 08:00:27:90:75:da (kali linux) merupakan ip address 192.168.43.9 bukan ip address 192.168.43.1 yang sebenarnya dimiliki oleh gateway pada lalu lintas ini dapat di simpulkan bahwa pada tabel arp 08:00:27:0c:84:1b (windows 7) sekarang sudah terdaftar bahwa 192.168.43.1 dengan mac address 08:00:27:90:75:da (kali linux), untuk lebih jelasnya dapat dilihat pada Gambar 11.



Gambar 11. Komunikasi Antara Kali Linux Dengan Windows 7 Ketika DNS Spoofing

Pada Gambar 12 dapat di lihat bahwa DNS spoofing telah berhasil di lakukan, disebabkan user berhasil di arahkan kepada website palsu yang telah di buat sebelumnya di kali linux.



Gambar 12. Halaman Facebook.com Setelah Dilakukan DNS Spoofing

5. Kesimpulan

5.1 Simpulan

1) Aplikasi informasi sederhana yang ditujukan untuk keamanan lalu lintas data pada pengguna yang masih awam di warnet, agar dapat melindungi diri dari pencurian data pribadi dan hal yang tidak di inginkan lainnya.
2) Penelitian ini juga dapat berguna bagi admin jaringan internet yang ingin mengetahui bagaimana tahapan penyerangan dari arp *poisoning* dan dns *spoofing* terjadi.
3) Dari aplikasi *Wireshark* dihasilkan hasil aktivitas penyerangan arp *poisoning* dan dns *spoofing* yang terjadi pada sistem dan hal ini memudahkan bagi admin menganalisis pola serangan dan jenis serangan apa saja yang terjadi..

5.2 Saran

Berdasarkan penelitian, analisis, pembahasan dan uji coba pada Implementasi Analisis keamanan lalu lintas data pada sistem operasi ubuntu menggunakan metode *attack centric*, maka dari itu penulis memberikan saran sebagai berikut:

1) Aplikasi akan berjalan dengan baik apabila mengikuti petunjuk penggunaan aplikasi.
2) Aplikasi Analisis keamanan lalu lintas data pada sistem operasi ubuntu menggunakan metode *attack centric*, masih jauh dari kata sempurna di karenakan kejahatan criminal di dunia maya tidak hanya akan dilakukan dalam dua mode penyerangan, oleh karna itu dapat diharapkan Aplikasi Analisis keamanan lalu lintas data pada sistem operasi ubuntu menggunakan metode *attack centric* dapat terus berkembang untuk penyesuaian kebutuhan yang ada.
3) Pengembangan bisa lebih kepada spesifikasi tutorial ataupun pada penambahan fitur untuk penanganan yang lebih cepat.

6. Daftar Rujukan

[1] E. M. Putra *et al.*, "Analisis Kemanan Jaringan Internet (Wifi) Dari Serangan Packet Data Sniffing Di Universitas MuhammadiyahPalembanG," pp. 1–11.

[2] M. A. A. Gobel, Suyoto, and T. Suselo, "Analisis Dan Pengembangan Sistem Peringatan Keamanan Jaringan Komputer Menggunakan Sms Gateway Dan Paket Filter," *Semin. Nas. Teknol. Inf. dan Komun. 2014 (SENTIKA 2014)*, vol. 2014, no. Sentika, pp. 382–388, 2014.

[3] Z. A. Pribadi, "Analisis dan Implementasi Firewall dengan Metode Stateful Multilayer Inspection Pada Mikrotik Router OS," 2013.

[4] B. Nugraha, "Analisis Teknik-Teknik Keamanan Pada Cloud Computing dan NEBULA (Future Cloud): Survey Paper," *Teknosi*, vol. 2, no. 2, pp. 35–42, 2016.

[5] R. Rosnelly and R. Pulungan, "Membandingkan Analisis Traffic antara WireShark dan NMap," *Pros. Konf. Nas. Sist. Inf. 2011*, pp. 936–947, 2011.