SNESTIK

Seminar Nasional Teknik Elektro, Sistem Informasi, dan Teknik Informatika

https://ejurnal.itats.ac.id/snestik dan https://snestik.itats.ac.id

Informasi Pelaksanaan :
SNESTIK III - Surabaya, 11 Maret 2023
Ruang Seminar Gedung A, Kampus Institut Teknologi Adhi Tama Surabaya

Informasi Artikel:
DOI : 10.31284/p.snestik.2023.4288

Prosiding ISSN 2775-5126

Fakultas Teknik Elektro dan Teknologi Informasi-Institut Teknologi Adhi Tama Surabaya
Gedung A-ITATS, Jl. Arief Rachman Hakim 100 Surabaya 60117 Telp. (031) 5945043
Email : snestik@itats.ac.id

Implementasi Domain Name Server (DNS) Spoofing pada Jaringan Nirkabel

Danang Haryo Sulaksono, Gusti Eka Yuliastuti, Citra Nurina Prabiantissa, I Kadek Agus Ariyasa

Institut Teknologi Adhi Tama Surabaya
e-mail: danang_h_s@itats.ac.id

ABSTRACT

The development of networks in this part of the world is very helpful in exchanging data between people in other places. However, in a wireless network, users must communicate with each other to be able to exchange data or information within a network where wireless networks can connect devices without using cables. The problem faced is in wireless networks for the lack of prevention on websites that have negative content. For that we need a way to divert the web with negative content with the web that has positive content. One solution to this problem is to use Domain Name Server (DNS) spoofing. DNS Spoofing is a Man In The Middle Attack (MITM) hacking method that can manipulate DNS packets in the DNS network itself by changing a domain address to be fake. Testing using QoS calculations. using four parameters. The first parameter is throughput, which produces a value of 9,589 bytes/s, which is a very good category for using DNS spoofing on wireless networks. The second is the delay test, and getting an average result of 0.0819334 ms is included in the very good category. In the third test, testing using jitter, getting a result of 0 ms, is included in the very good category. Fourth is testing with packet loss parameters resulting in 0% and entering into the very good category.

Keywords: *Domain Name Server (DNS) Spoofing, Hacking Man In The Middle Attack Method (MITM, QoS, Throughput, Delay, Jitter, Packet Loss*

ABSTRAK

Perkembangan jaringan di belahan dunia ini sangat membantu dalam pertukaran data antar manusia di lain tempat. Namun dalam suatu jaringan nirkabel user harus saling berkomunikasi untuk dapat bertukar data atau informasi dalam satu jaringan Dimana jaringan nirkabel dapat menghubungkan perangkat tanpa menggunakan kabel. Masalah yang dihadapi adalah pada jaringan nirkabel untuk kurangnya pencegahan pada web-web yang memiliki konten negatif. Untuk itu perlu suatu cara agar dapat mengalihkan web dengan konten negatif tersebut dengan web yang memiliki konten positif. Salah satu solusi untuk masalah tersebut adalah dengan menggunakan Domain Name Server (DNS) Spoofing. DNS Spoofing adalah sebuah metode hacking Man In The Middle Attack (MITM) yang dapat memanipulasi paket DNS yang ada dalam jaringan DNS itu sendiri dengan mengubah sebuah alamat domain menjadi palsu. Pengujian dengan menggunakan perhitungan QoS. menggunakan empat parameter. Parameter pertama adalah throughput, menghasilkan nilai 9.589 byte/s, masuk ke dalam kategori yang sangat bagus dalam menggunakan DNS Spoofing pada jaringan nirkabel. Kedua adalah pengujian delay, dan mendapatkan hasil rata-rata sebesar 0,0819334 ms masuk ke dalam golongan yang sangat baik. Pada pengujian ketiga, pengujian menggunakan jitter, mendapatkan hasil sebesar 0 ms, masuk ke dalam kategori yang sangat baik. Keempat adalah pengujian dengan parameter packet loss menghasilkan 0% dan masuk ke golongan sangat baik.

Kata kunci: Domain Name Server (DNS) Spoofing, Metode Hacking Man In The Middle Attack (MITM, QoS, Throughput, Delay, Jitter, Packet Loss

PENDAHULUAN

Penyimpanan data-text dalam bentuk digital menjadi salah satu pilihan terbaik, karena tidak membutuhkan tempat penyimpanan yang besar. (Sulaksono, Danang H., 2016). Fasilitas penyebaran informasi pada era teknologi yang saat ini dapat dilakukan dengan cepat dan mudah melalui internet (Ainur, 2020). Dengan adanya data digital tersebut dapat memudahkan pertukaran data melalui jaringan. Perkembangan jaringan di belahan dunia ini sangat membantu dalam pertukaran data antar manusia di lain tempat. Namun dalam suatu jaringan nirkabel user harus saling berkomunikasi untuk dapat bertukar data atau informasi dalam satu jaringan. Dimana jaringan nirkabel dapat menghubungkan perangkat tanpa menggunakan kabel. Jaringan nirkabel menggunakan frekuensi yang sifatnya terbuka dibandingkan dengan menggunakan kabel. (Saskara, 2019).

Masalah yang dihadapi adalah pada jaringan nirkabel untuk kurangnya pencegahan pada web-web yang memiliki konten negatif. Hal ini perlu dilakukan agar user tidak dapat mengakses web-web yang terlarang karena memiliki konten negatif. Dimana web-web konten negatif ini seharusnya hanya dapat diakses dengan batas usia tertentu sehingga untuk dapat mengaksesnya pengguna wajib mencantumkan usianya terlebih dahulu. Untuk itu perlu suatu cara agar dapat mengalihkan web dengan konten negatif tersebut dengan web yang memiliki konten positif. (Sasmita, 2015).

Salah satu solusi untuk masalah tersebut adalah dengan menggunakan Domain Name Server (DNS) Spoofing. DNS Spoofing adalah sebuah metode hacking Man In The Middle Attack (MITM) yang dapat memanipulasi paket DNS yang ada dalam jaringan DNS itu sendiri dengan mengubah sebuah alamat domain menjadi palsu. Metode ini mengeksploitasi server yang vulnerable untuk memodifikasi data yang disimpannya yang nantinya akan digunakan oleh sistem yang menjadi target. Dengan adanya spoofing ini user dapat mengalihkan web yang memiliki konten negatif dengan web yang memiliki konten positif. (Hafizh, 2020).

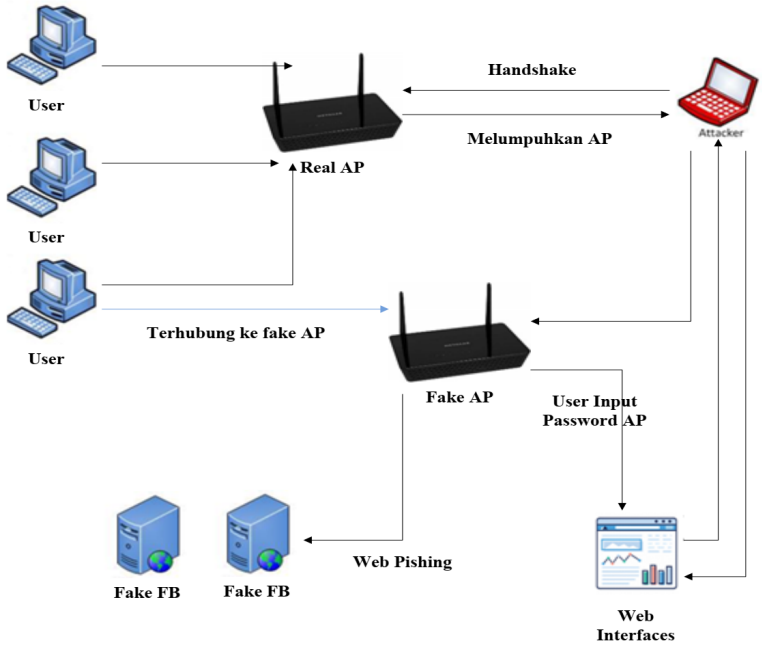
Pada penelitian yang dilakukan oleh (Ginting, 2019) menjelaskan bahwa celah keamanan dapat menyebabkan menyebabkan serangan spoofing sehingga mudah untuk melakukan serangan untuk memodifikasi cache table korban. Menurut penelitian (Hafizh, 2020) menjelaskan bahwa spoofing pada jaringan bekerja ketika dua unit personal computer (PC) terhubung dalam satu jaringan. Masing-masing PC memiliki IP address dan MAC address yang berbeda. Attacker memodifikasi MAC address, sehingga memiliki dua IP address namun hanya memiliki satu MAC address. Menurut (Suryana, 2016) menjelaskan bahwa email spoofing

merupakan kegiatan menipulasi data pada header email. Pengguna tidak akan bisa mengetahui perbedaan antara email spoofing dan email asli, sehingga pengguna tidak akan mengetahui ketika mana data yang asli dan bukan kecuali user menggunakan sistem keamanan untuk mengatasi email spoofing.

Berdasarkan hal yang telah diuraikan di atas, maka pada penelitian ini diusulkan Implementasi Domain Name Server Spoofing pada jaringan nirkabel untuk mengalihkan web dengan konten negatif pada web dengan konten positif.

METODE

Analisis dan perancangan sistem ini untuk mengimplementasikan Domain Name Server Spoofing pada jaringan nirkabel. Dimana hal ini berguna untuk menghubungkan dan mempermudah pengambilan data dari user lain dalam satu jaringan. Analisis sistem meliputi analisis kebutuhan sistem dan analisis fasilitas dalam perencanaan sistem yang dibuat.

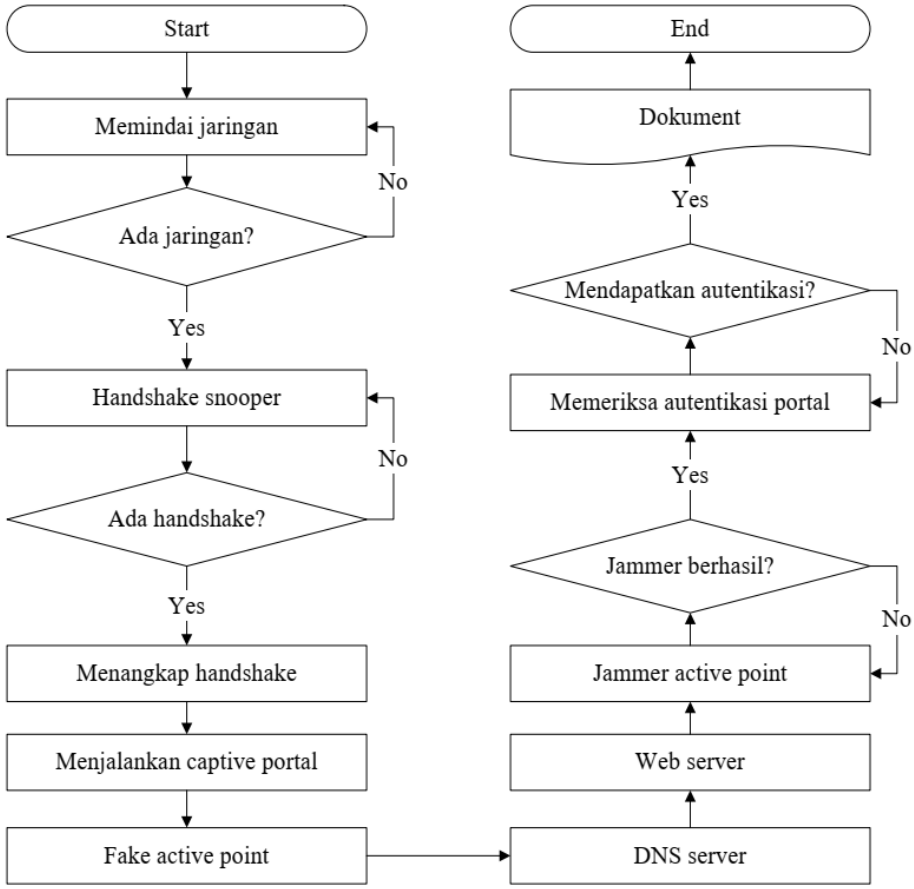


Gambar 1 Skema Perancangan Sistem Spoofing

Gambar 1 diatas menjelaskan tentang skema rancangan Sistem pengambilan data user lain dalam jaringan nirkabel. Dimana attacker melakukan pemindaian jaringan nirkabel yang tersedia pada suatu Access Point untuk mendapatkan handshake dari user. Setelah itu attacker melumpuhkan Access Point dengan teknik Deauthentication serta menyebabkan user tidak dapat terhubung ke

Access Point. Setelah melumpuhkan Access Point, attacker membuat Fake Access Point dan Web Interfaces.User secara otomatis terhubung ke Fake Access point dan di Runder ke Web Interfaces untuk dimintai Password. Sistem ini juga terintegrasi dengan web Phising.

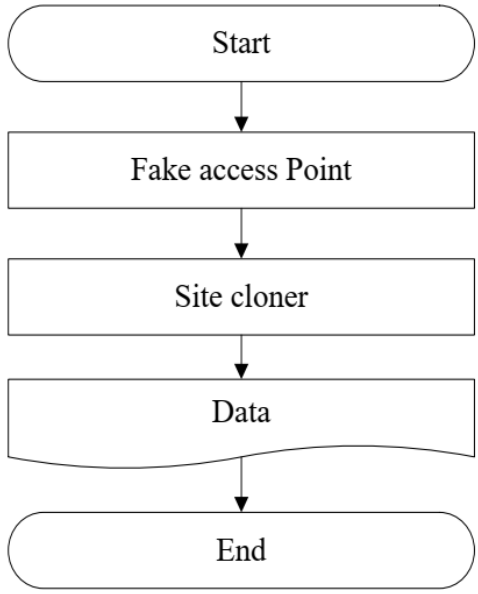
DNS spoofing merupakan teknik untuk memasukkan atau meracuni cache pada suatu server DNS dengan data atau informasi yang salah. Metode ini mengeksploitasi server yang vulnerable untuk memodifikasi data yang disimpannya yang nantinya akan digunakan oleh sistem yang menjadi target.



Gambar 2 Flowchart Sistem DNS Spoofing

Gambar 2 merupakan alur dari pembuatan sistem spoofing, dimana alur pertama yang dilakukan adalah melakukan pemindaian jaringan nirkabel target setelah itu Luncurkan serangan Handshake Snooper Untuk mendapat handshake (diperlukan untuk verifikasi kata sandi). Luncurkan serangan Captive Portal untuk Menimbulkan Fake AP meniru Access Point yang asli. Memunculkan server DNS dan mengarahkan semua permintaan ke host penyerang yang menjalankan portal captive. Memunculkan server web, melayani portal target yang meminta pengguna untuk kunci WPA / WPA2 mereka. Menimbulkan jammer untuk menonaktifkan semua client dari AP asli dan memikat mereka ke AP palsu. Semua upaya otentikasi di captive portal diperiksa terhadap file handshake yang ditangkap sebelumnya. Serangan akan secara otomatis berakhir setelah kunci yang benar telah dikirimkan. Kuncinya akan dicatat dan klien akan diizinkan untuk menyambung kembali ke titik akses target.

Gambar 3 menjelaskan tentang alur Web Phising dimana attacker membuat Fake Access Point untuk mendapatkan user yang akan ditipu. Setelah mendapatkan bidikan user, attacker membuat web palsu dengan tampilan dan nama domain semirip mungkin dari website aslinya. Dengan berbekal nama domain dan tampilan yang mirip, web phising akan bekerja mengumpulkan user untuk login menggunakan informasi asli. Kemudian data-data yang dimasukkan tersebut secara otomatis akan tersimpan di database untuk digunakan login ke website asli oleh pelaku penyebar web phising.



Gambar 3. Alur Web Phising

HASIL DAN PEMBAHASAN

Sistem yang diuji pada implementasi DNS spoofing dalam jaringan nirkabel mempunyai empat parameter QoS. Parameter tersebut adalah throughput, jitter, delay dan packet loss. waktu yang digunakan untuk pengambilan data adalah kurang dari 50 detik. Software yang digunakan untuk pengujian ini adalah wireshark. Untuk mendapatkan kategori kelayakan pengujian QoS, penelitian ini menggunakan standar Tiphon.

Measurement	Captured	Displayed	marked
Packets	42	42(100%)	-
Time span, s	33.580	33.580	-
Average pps	1.2	1.3	-
Average packet size, B	322	322	-
Bytes	13507	13507(100%)	0
Average bytes/s	402	402	-
Average bytes/s	3217	3217	-

Throughput adalah kecepatan (rate) transfer data efektif, yang diukur dalam bps. Throughput merupakan jumlah total kedatangan paket yang sukses yang diamati pada destination selama interval waktu tertentu dibagi oleh durasi interval waktu tersebut. Throughput dapat dihitung dengan cara perhitungan sebagai berikut:

$$Throughput = \frac{322\ byte}{33.580\ s} = 9.589\ byte/s$$

Delay adalah waktu tunda saat paket dikirim yang diakibatkan oleh proses transmisi dari satu titik ke titik lain yang menjadi tujuannya. Delay diperoleh dari selisih waktu kirim antara satu paket TCP dengan paket lainnya. Waktu delay ada empat nilai, yaitu 0,101568000 s, 0,101568000 s, 0,016659000 s, 0,016659000 s, 0,000058000 s, dan 0,000058000 s. Berikut ini adalah perhitungan delay : 0,101568000

$$Rata - rata\ delay\ 1{,}2 = \frac{0{,}101568000}{42} = 0{,}0024182\ s$$
$$= 0{,}24182 ms$$

$$Rata - rata\ delay\ 3{,}4 = \frac{0{,}016659000}{42} = 0{,}000039664\ s$$
$$= 0{,}0039664\ ms$$

$$Rata - rata\ delay\ 5{,}6 = \frac{0{,}000058000}{42} = 0{,}000000138\ s$$
$$= 0{,}0000138\ ms$$

$$Rata - rata\ delay\ 1-8 = \frac{0{,}24182 + 0{,}24182 + 0{,}0039664 + 0{,}0039664 + 0{,}0000138 + 0{,}0000138}{6}$$

$$= \frac{0{,}4916004}{6} = 0{,}0819334$$

KESIMPULAN

Pengujian DNS spoofing dilakukan dengan menggunakan empat parameter QoS dan standar dari Tiphon. Parameter pertama adalah throughput, menghasilkan nilai 9.589 byte/s, masuk ke dalam kategori yang sangat bagus dalam menggunakan DNS Spoofing pada jaringan nirkabel. Kedua adalah pengujian delay, dan mendapatkan hasil rata-rata sebesar 0,0819334 ms masuk ke dalam golongan yang sangat baik. Pada pengujian ketiga, pengujian menggunakan jitter, mendapatkan hasil sebesar 0 ms, masuk ke dalam kategori yang sangat baik. Keempat adalah pengujian dengan parameter packet loss menghasilkan 0% dan masuk ke golongan sangat baik.

DAFTAR PUSTAKA

[1] A. R. Taqwa, D. H. Sulaksono, “Implementasi Kriptografi Dengan Metode Elliptic Curve Cryptography (ECC) Untuk Aplikasi Chatting Berbasis Android”, Jurnal Riset Inovasi Bidang Informatika dan Pendidikan Informatika (KERNEL). Vol. 1. No. 1, 2020.

[2] Anshori, I. Fardian, “Implementasi Socket TCP/IP Untuk Mengirim Dan Memasukkan File Text Kedalam Database”, Jurnal RESPONSIF. Vol. 1. No. 1. E-ISSN: 2685-6964, 2019.

[3] D. Irawan, “Mencuri Informasi Penting Dengan Mengambil Alih Akun Facebbok Dengan Metode Phising”, Jurnal Ilmu Komputer & Informatika. Vol. 1. No. 1, 2020.

[4] A. Ginanjar, N. Widiyasono, R. Gunawan, “Analisis Serangan Web Phising Pada Layanan E-Commerce Dengan Metode Network Forensic. Process”, JUTEI Edisi. Vol. 2. No. 2. ISSN: 2579-3675, 2018.

[5] V, C, Ginting, D. P. Kartikasari “Deteksi Serangan ARP Spoofing Berdasarkan Analisis Lalu Lintas Paket Protokol ARP”. Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer. Vol. 3, No. 5. Hlm. 5049-5057. E-ISSN: 2548-964X, 2019.

[6] [6] G. Saskara, I. A. Jude, I. P. Oktap. P. H. Putra, “Keamanan Jaringan Komputer Nirkabel Dengan Captive Potal Dan WPA/WPA2 Di Politeknik Ganesha Guru”, Jurnal Pendidikan Teknologi dan Kejuruan. Vol. 16, No. 2. P-ISSN: 0216-3241, E-ISSN: 2541-0652, 2019.

[7] F. Suhaila, “Analisis Jaringan LAN di SMK 5 TELKOM Banda Aceh”, Fakultas Tarbiyah dan Keguruan. Universitas Islam Negeri Ar-Raniry. Darusalam Banda Aceh, 2019.

[8] A. N. Syahrudin T. Kurniawan, “Input Dan Output Pada Bahasa Pemrograman Python (Studi Kasus: STMIK Sumedang”, Jurnal Dasar Pemrograman Python STMIK, 2018.