Just IT : Jurnal Sistem Informasi, Teknologi Informasi dan Komputer
Vol. 14, No. 2, Januari 2024, pp. 80-149
P-ISSN: 2089 – 0256, e-ISSN: 2598 – 3016

PERTAHANAN TINGKAT *SERVER* TERHADAP SERANGAN DNS SPOOFING DI JARINGAN MODERN

Fauzan Prasetyo*[1], Alief Badrit Tamam[2], Reynal Widya Efendi[3],M.Zaini Mun'im[4]
[1,2,3,4] Informatika, Fakultas Teknik ,Universitas Madura

prasetyo@unira.ac.id

Abstrak

Dalam era jaringan modern, pertahanan tingkat server terhadap serangan DNS spoofing menjadi krusial untuk menjaga integritas dan keamanan data. Artikel ini menyelidiki evolusi metode serangan DNS spoofing dan tantangan yang dihadapi dalam konteks jaringan saat ini. Kami menganalisis kerentanan server DNS terhadap manipulasi data, serta dampaknya terhadap pengguna dan organisasi. Sementara itu, fokus utama artikel ini adalah membahas strategi dan teknologi terkini untuk meningkatkan pertahanan tingkat server terhadap serangan DNS spoofing. Melalui kajian literatur dan penelitian terkini, artikel ini menguraikan implementasi DNS Security Extensions (DNSSEC), pemantauan lalu lintas DNS yang canggih, dan teknik enkripsi yang dapat mengurangi risiko serangan. Pembahasannya juga melibatkan pertimbangan praktis dalam menerapkan solusi ini di lingkungan jaringan yang kompleks. Dengan merinci perbandingan kelebihan dan kekurangan berbagai pendekatan, artikel ini bertujuan memberikan panduan praktis bagi profesional IT dalam memperkuat pertahanan server DNS dan memitigasi risiko serangan DNS spoofing di era digital saat ini.
Kata Kunci: *Jaringan Komputer, Dns, Keamanan Jaringan, Server, Spoofing*

Abstract

In the modern networking era, server-level defence against DNS spoofing attacks is crucial to maintain data integrity and security. This article investigates the evolution of DNS spoofing attack methods and the challenges faced in today's network context. We analyse the vulnerability of DNS servers to data manipulation, as well as the impact on users and organisations. Meanwhile, the main focus of this article is to discuss current strategies and technologies to improve server-level defences against DNS spoofing attacks. Through a review of recent literature and research, the article outlines the implementation of DNS Security Extensions (DNSSEC), advanced DNS traffic monitoring, and encryption techniques that can reduce the risk of attacks. The discussion also involves practical considerations in implementing these solutions in complex network environments. By detailing a comparison of the advantages and disadvantages of various approaches, this article aims to provide practical guidance for IT professionals in strengthening DNS server defences and mitigating the risk of DNS spoofing attacks in today's digital age.
Keywords: *Computer Network, Dns, Network Security, Server, Spoofing.*

1. PENDAHULUAN

Kerentanan ada di mana-mana, dari perangkat dan jalur data hingga aplikasi dan pengguna. memungkinkan orang

lain untuk mengakses data, mengubah isi, sampai menghapus data.[1] Domain Name System/Sistem nama domain (DNS) adalah salah satu bagian inti dari rangkaian protokol TCP/IP dan protokol standar yang digunakan oleh Internet[2] Server DNS digunakan untuk menerjemahkan alamat IP menjadi namadan sebaliknya untuk mengizinkan browser memasukkan alamat IP publik dan Memasukkan domain untuk mengakses Internet sangat penting saat mengakses server DNS[3] Sistem nama domain terdiri dari nama-nama situs web yang dipetakan dengan protokol Internet, yang memfasilitasi penjelajahan dengan tidak

p-ISSN 2089-0265
e-ISSN 2598-3016

mengharuskan pengguna untuk mengingat alamat notasi numerik. Sifat sistem ini, yang melibatkan transfer informasi dalam teks biasa, membuatnya rentan terhadap serangan keamanan.[2] Pesatnya perkembangan teknologi khususnya internet memudahkan pertukaran informasi dari dan ke berbagai tempat. Meskipun telah memiliki beragam jenis protokol keamanan, namun masih terdapat celah yang menembus keamanannya, yang berakibat pencurian data informasi penting.[4] kami menyajikan metodologi untuk mencegah pemalsuan domain berdasarkan praktik-praktik yang baik dalam mengelola serta menganalisis DNS[5] Banyaknya user yang berada pada Perusahaan X dan tidak adanya pengontrolan hak akses pada setiap user yang ada pada, Masalah ini dapat mengganggu keamanan dan penyalahgunaan.[6] Salah satu serangan yang mengganti alamat IP asli dengan alamat IP yang tidak valid untuk memverifikasi operasi yang benar dari sistem pendeteksi serangan DNS-spoofing (Malefactor).[7] Sistem Nama Domain atau DNS adalah salah satu infrastruktur dasar dari Internet di mana keandalan dan keakuratannya sangat penting dalam fungsi penjelajahan internet. Sayangnya, hal ini telah menjadi titik paling rentan di ruang cyber yang dapat diserang dengan mudah. Seperti yang telah disebutkan oleh Trusteer, fungsi utamanya adalah menerjemahkan nama host dan domain yang dapat dibaca manusia (seperti www.trusteer.com) ke dalam alamat IP (seperti 208.97.136.206) dan sebaliknya. Oleh karena itu, ketika komputer pengguna mencoba untuk terhubung ke situs web tertentu, DNS menerjemahkan nama domain situs web menjadi alamat IP numerik yang dapat dibaca computer[8] Pengawasan lalu lintas jaringan: Solusi pengawasan jaringan seperti analisis lalu lintas jaringan, pemantauan aktivitas perangkat, dan deteksi serangan berbasis perilaku memungkinkan identifikasi dan deteksi aktivitas yang mencurigakan atau serangan potensial.[9]

2. TINJAUAN PUSTAKA

2.1. DOMAIN NAME SYSTEM

Menurut (Jason Goertzen; D Stebila – 2022) sistem Nama Domain (DNS) adalah layanan yang sangat penting untuk Internet. DNS bertanggung jawab untuk menerjemahkan nama domain yang dapat dibaca manusia menjadi alamat IP yang dapat dimengerti mesin dan digunakan oleh miliaran perangkat setiap hari

2.2. DNS SPOOFING

Dalam Penelitian (Shanakan Anuradha Samarakoon – 2022) Spoofing DNS adalah serangan yang memungkinkan penyerang untuk mengalihkan lalu lintas yang ditujukan untuk satu domain situs web ke situs web lain, biasanya untuk tujuan jahat

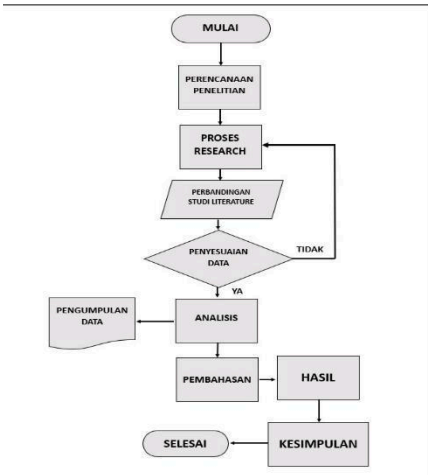
2.3. ETTERCAP

Ettercap adalah alat sniffing paket yang digunakan untuk menganalisis protokol jaringan dan memverifikasi keamanan jaringan. (T. Pangestu, R. Liza, P. Studi, T. Informatika, and U. H. Medan – 2022).

2.4. DNSSEC

Domain Name System Security Extensions (DNSSEC) : adalah sebuah suite spesifikasi yang dikembangkan oleh Internet Engineering Task Force (IETF) untuk meningkatkan keamanan dan integritas data yang dikirimkan melalui Domain Name System (DNS).Dalam Penelitian Oleh (Y. A. Pohan – 2021).

3. METODE PENELITIAN



p-ISSN 2089-0265
e-ISSN 2598-3016

Gambar. 1. Flowchart Metode Penelitian

Penelitian ini mengadopsi pendekatan penelitian kualitatif, sejalan dengan pandangan Sugiyono (2010) dan V. Wiratna Sujarweni (2014) yang mengklasifikasikan penelitian menjadi dua jenis, yaitu kualitatif dan kuantitatif. Menurut Strauss dan Corbin (V. Wiratna Sujarweni, 2014), penelitian kualitatif berfokus pada penemuan yang tidak dapat dicapai melalui prosedur statistik atau metode kuantitatif. Sementara itu, Bogdan dan Taylor (V. Wiratna Sujarweni, 2014) menjelaskan bahwa penelitian kualitatif menghasilkan data deskriptif berupa ucapan, tulisan, dan perilaku dari subjek yang diamati.

Dalam konteks penelitian ini, pilihan metode kualitatif dipilih karena tujuan utamanya adalah memahami perilaku mahasiswa dalam pemanfaatan komputer dan internet sebagai media pembelajaran Pemasaran Online. Metode kualitatif dianggap lebih sesuai untuk menggambarkan fenomena ini secara rinci.

Sumber data penelitian ini mencakup tiga elemen: tempat, aktor dan interaksi sinergis, sebagaimana diungkapkan oleh Spradley (Sugiyono, 2010). Penelitian ini tidak menggunakan istilah populasi, melainkan "social situation" yang melibatkan interaksi antara tempat, pelaku, dan aktivitas.

Sebagai pendukung, penelitian ini menggunakan analisis media online sperti IEEE, mandeley, dan google schoolar

Penting untuk mencatat bahwa perubahan metode penelitian menjadi penelitian IT dapat mengacu pada jurnal-jurnal terkait IT. Ini mencakup tinjauan literatur, pemilihan metode penelitian IT yang sesuai, dan pengembangan kerangka kerja berdasarkan literatur tersebut. Teknik pengumpulan data dan alat analisis harus disesuaikan dengan metode penelitian IT yang dipilih, dan validitas hasil penelitian harus tetap dijaga. Dengan pendekatan ini, penelitian IT dapat dilakukan dengan lebih kontekstual dan relevan

4. HASIL DAN PEMBAHASAN

Dns ini bertujuan mengubah alamat IP menjadi sebuah domain atau nama yang akan

memudahkan dala melakuan pencarian sebuah domain. [10] Spoofing DNS adalah teknik untuk mencegat permintaan peramban untuk sebuah situs web dan mengarahkan pengguna ke situs lain. Hal ini dapat dilakukan dengan mengubah alamat IP server DNS atau mengubah alamat IP server nama domain itu sendiri. Sebuah serangan spoofing DNS melibatkan penyerang yang menyamar sebagai server DNS dan mengirimkan respons ke Permintaan DNS yang berbeda dari yang dikirim oleh server yang sah. Penyerang dapat mengirim respons apa pun terhadap permintaan korban, termasuk alamat IP host palsu atau jenis informasi palsu. Ini dapat digunakan untuk memberikan informasi palsu tentang layanan dijaringan, atau untuk mengarahkan pengguna ke situs web palsu yang dirancang agar terlihat seperti situs web asli[11] Untuk mendemonstrasikan proses Spoofing DNS, contoh skenario berikut ini telah dibuat. Skenario ini menunjukkan bagaimana penyerang dapat mengarahkan korban ke situs web palsu

1. Klien mengirimkan permintaan DNS ke server DNS, meminta alamat IP untuk nama domain, misalnya google.com.
2. Penyerang, sebagai perantara antara klien dan server DNS yang sebenarnya, mencegat permintaan ini.
3. Alih-alih meneruskan Queri ke server DNS yang sebenarnya, penyerang mengirim respons DNS palsu DNS palsu dengan informasi palsu, seperti memberikan alamat IP palsu untuk nama domain google.com. Akibatnya, pengguna akan diarahkan ke situs web palsu atau infrastruktur tidak sah lainnya,

p-ISSN 2089-0265
e-ISSN 2598-3016

di mana penyerang dapat mencoba mencuri informasi sensitif seperti kata sandi atau kredensial login.[11]

Spoofing DNS terjadi ketika pengguna membuat permintaan DNS melalui resolver rekursif dan kueri itu dijawab oleh pihak ketiga (spoofer) yang bukan merupakan server resmi. Kami menyebut respons yang berpotensi diubah sebagai spoofing. Kami mendeteksi spoofers yang terang-terangan spoofers yang jelas tentang identitas mereka. Tujuan dari Spoofer Pihak ketiga dapat memalsukan DNS untuk tujuan jinak atau jahat/berbahaya.
Pengalihan web untuk portal tawanan: Penggunaan yang paling banyak dilakukan
penggunaan yang paling umum dari spoofing DNS adalah untuk mengarahkan pengguna ke portal captive
sehingga mereka dapat mengautentikasi ke jaringan publik. Banyak basestation wifi institusional mencegat semua permintaan DNS ke
menyalurkan pengguna ke halaman login berbasis web (portal). Setelah setelah pengguna melakukan autentikasi, lalu lintas DNS di masa depan biasanya lewat.
Mengalihkan aplikasi: Spoofing DNS dapat digunakan untuk mengalihkan lalu lintas jaringan ke server alternatif. Jika digunakan untuk mengalihkan lalu lintas web atau pembaruan OS, spoofing seperti itu bisa berbahaya bagian dari penyuntikan malware atau eksploitasi. Atau, bisa juga untuk mengurangi lalu lintas jaringan eksternal.
Respons yang lebih cepat: Beberapa ISP mencegat lalu lintas DNS untuk memaksa lalu lintas DNS melalui resolver rekursif mereka sendiri. Pengalihan ini pengalihan ini mungkin bertujuan untuk mempercepat respons, atau
mengurangi trafik eksternal (kasus khusus pengalihan aplikasi aplikasi, atau menerapkan pemfilteran konten lokal (dijelaskan lokal (dijelaskan selanjutnya).
Pemfilteran dan Penyensoran Jaringan: Spoofing DNS adalah sebuah metode yang populer untuk mengimplementasikan penyaringan jaringan, yang memungkinkan ISP untuk memblokir tujuan untuk menegakkan hukum lokal (atau kebijakan organisasi).
atau kebijakan organisasi, ketika dilakukan di dalam perusahaan). DNS spoofing telah digunakan untuk mengontrol pornografi , untuk Sensor politik , dan untuk menerapkan kebijakan lainnya. Spoofing untuk penyaringan jaringan dapat dianggap sebagai teknik yang menguntungkan atau penyensoran yang berbahaya, tergantung pada sudut pandang seseorang tentang kebijakan tersebut. Spoofing untuk penyaringan lalu lintas dapat dideteksi dengan validasi DNSSEC, jika digunakan.[12] Strategi yang dapat diambil dalam mengamankan DNS: Syarat dari keamanan adalah prevention (pencegahan),
yaitu memperkecil peluang penembusan oleh pemakai yang tak diotorisasi. Observation (observasi) yaitu identifikasi dan otentifikasi. Response (respon) yaitu upaya pengamanan data baik fisik maupun maya (software).[13]
Penyadapan: Karena DNS dikirim tanpa dienkripsi, maka dienkripsi, spoofing dapat digunakan untuk menguping lalu lintas DNS untuk mengamati metadata komunikasi.[12]
Deteksi pemalsuan DNS
Untuk mendeteksi serangan seperti itu ada cara yang sangat cara sederhana yang diberikan sebagai berikut:
DHCP SPOOFING :
Protokol DHCP menyediakan jaringan parameter pengaturan dari host baru. parameter ini termasuk subnet mask, DNS Server, default gateway, lease time, dan alamat IP.
Ini menyediakan arsitektur client-server untuk bertukar paket data antara DHCP server dan host. DHCP memiliki standar

p-ISSN 2089-0265
e-ISSN 2598-3016

keamanan yang luar biasa dan memainkan peran penting dalam manajemen jaringan.

Setiap pesan DHCP dikirim dalam bentuk teks yang tidak dimodifikasi teks yang tidak dimodifikasi, dan tidak ada sumber pesan DHCP

otentikasi. Hal ini tidak menjamin DHCP server yang tepercaya DHCP server dan komunikasi dengan klien yang sebenarnya.

Penyerang melakukan serangan DoS pada DHCP server , atau meluncurkan serangan DHCP starvation attack. ini mengarah pada alokasi kumpulan IP andrress Pool yang disediakan oleh DHCP server, sehingga yang perangkat baru tidak dapat memperoleh alamat IP.

PENIPUAN IP (IP SPOOFING) :

Dari satu pengguna/pengirim ke titik akhir tergantung pada alamat IP dari header paket. Ini menjelaskan struktur paket data yang digunakan untuk enkapsulasi data yang seharusnya dibawa. Sementara dengan menggunakan titik akhir dan informasi sumber, lebih lanjut mendefinisikan pengalamatan mekanisme pengalamatan untuk mengklasifikasikan datagram. Dalam sebuah IP serangan spoofing, musuh jahat menangkap komunikasi antara pihak-pihak yang sebenarnya. Penyerang tersebut mengatur aliran komunikasi dan memiliki kemampuan eliminasi dari informasi yang dikirim oleh peserta yang asli tanpa informasi dari titik akhir yang sebenarnya.[14] Biasanya tools ettercap dimanfaatkan atau digunakan untuk menyerang melalui sistem operasi kali linux dan juga Menggunakan tools tcpflow untuk melihat data yang diinput oleh korban. Penerapan software atau tools untuk mengamankan perangkat ketika terjadi serangan.

Ettercap adalah alat sniffing paket yang digunakan untuk menganalisis protokol jaringan dan memverifikasi keamanan jaringan. Ia juga memiliki kemampuan untuk mencegat lalu lintas LAN, mencuri kata sandi, dan secara aktif mendengarkan protokol umum. Packet sniffing juga dapat digunakan oleh pihak yang tidak bertanggung jawab untuk mencuri data sensitif dari pengguna yang saat ini terhubung dengan access point.[15] Ettercap menganalisis serangan keracunan ARP dengan memeriksa paket dari sumber ke tujuan dan korban keracunan. Melalui pengamatan tersebut, jika ada

lonjakan tiba-tiba dalam pemanfaatan tautan atau generasi yang mencurigakan paket di jalur tertentu, lalu lintas tertentu dapat diisolasi dan diperiksa untuk lalu lintas palsu atau malware serangan. Pekerjaan ini dapat diperluas untuk menganalisis OS pola sidik jari dengan mengidentifikasi semua perintah yang dijalankan dalam sistem operasi tertentu dari korban di bawah pertimbangan.[16]

Ettercap juga memiliki fitur lain yang dapat dimanfaatkan oleh penyerang

keuntungan dari . Fitur-fitur tersebut antara lain:

Injeksi Karakter: Penyerang dapat menyisipkan sembarang karakter sembarang ke dalam koneksi langsung di kedua arah. Dia dapat meniru perintah yang dikirim dari klien atau balasan yang dikirim dari server.

Penyaringan paket: Penyerang dapat menyaring muatan TCP atau UDP dari paket dalam koneksi langsung dengan mencari ASCII atau string atau string heksadesimal, dan menggantinya dengan string miliknya, atau denganhanya menghapus paket yang disaring.

Pengumpulan kata sandi otomatis (untuk sebagian besar protokol jaringan yang umum): Dissector Block aktif secara otomatis mengambil dan mengekstrak informasi yang relevan dari banyak protocol termasuk TELNET, FTP, POP3, RLOGIN, SSH1, ICQ, SMB, MySQL, HTTP, NNTP, X11, NAPSTER, IRC, RIP, BGP, SOCKS 5, IMAP 4, VNC,

p-ISSN 2089-0265
e-ISSN 2598-3016

LDAP, NFS, dan SNMP.

Secure Shell (SSH) Support : Penyerang dapat mendeteksi nama pengguna, kata sandi, dan data koneksi SSH1.

Hyper Text Transfer Protocol Secure (HTTPS) support: Penyerang dapat membajak sesi SSL HTTP, selama penggunamenerima sertifikat palsu. [17]

Point-to-Point Tunneling Protocol (PPTP) suite: Attacker can perform MITM attack against PPTP tunnels. [17]

Poin-poin di atas menjadi dasar untuk menjamin hak akses terhadap sistem yang sedang dibangun, oleh karena itu diperlukan suatu metode implementasi untuk menjamin keamanan penggunanya.[18] Dengan mudahnya pengaksesan terhadap informasi tersebut menyebabkan timbulnya masalah baru yaitu informasi atau data-data penting dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab untuk mendapatkan keuntungan sendiri[19] Dari sisi keamanan tentunya ini sangat perlu menjadi perhatian dengan cara memaksimalkan fungsi keamanan yang ada[20] Memilih sistem keamanan yang tepat akan mencegah kejadian yang tidak diinginkan seperti serangan atau akses tidak sah. [21] Penanggulangan Untuk Serangan – Serangan tersebut dengan Menggunakan Metode sebagai berikut : Aspek keamanan didefinisikan dalam lima poin, yaitu: Kerahasiaan, persyaratan bahwa informasi (data) hanya boleh diakses oleh pihak yang berwenang, Integritas, persyaratan bahwa informasi hanya dapat diubah oleh orang yang berwenang, Ketersediaan, persyaratan bahwa informasi (data) hanya dapat diakses oleh pihak yang berwenang. informasi dapat diakses. kepada pihak yang berkepentingan dengan segala otorisasi, Otentikasi, Mengharuskan pengirim informasi dapat diidentifikasi dengan benar dan terdapat jaminan bahwa identitas yang diperoleh tidak palsu, Non-repudiation, Mengharuskan baik pengirim maupun penerima informasi informasi Nomorbisa menolak mengirim atau menerima pesan

[22] Ada solusi alternatif yang dapat ditawarkanyaitu menjalankan[23]

Domain Name System Security Extensions (DNSSEC) : adalah sebuah suite spesifikasi yang dikembangkan oleh Internet Engineering Task Force (IETF) untuk meningkatkan keamanan dan integritas data yang dikirimkan melalui Domain Name System (DNS). DNS merupakan protokol kunci yang digunakan untuk menerjemahkan nama domain menjadi alamat IP yang sesuai. DNSSEC bertujuan untuk mengatasi potensi masalah keamanan terkait dengan DNS, seperti cache poisoning, man-in-the-middle attacks, dan penggantian data DNS yang tidak sah[24] Kerentanan disebabkan DNS tidak diinstall DNSSEC dan mode recursion yes Dengan mengaktifkan DNSSEC dan menonaktifkan mode recursive[25] Dengan ini dapat mengurangi kerentanan terhadap serangan Pada DNS dalam serangan DNS Spoofing. Pertama-tama kita akan melihat ke dalam waktu permintaan DNS apakah pengirim, penerima, atau kedua belah pihak memulai pratinjau. Setelah itu, kita akan melihat lebih jauh dari mana query berasal, dari pengguna atau media sosial atau penyedia. Setelah kita memiliki pemahaman tentang semua aliran pesan kami akan menganalisis kerentananya dari sudut pandang DNSSEC dan mengevaluasi risiko keamanannya. [26]

DNSSEC memastikan bahwa pesan DNS yang diterima memang berasal dari server yang diberi wewenang untuk merespons terhadap kueri, dan bahwa pesan tersebut belum dimodifikasi dalam transit.[27]

Salah satu keunggulan utama yang disediakan oleh sistem ini adalah [28] DNSSEC saat ini menggunakan tanda tangan digital yang bergantung pada

p-ISSN 2089-0265
e-ISSN 2598-3016

asumsi keamanan tradisional seperti anjak piutang dan diskrit logaritma, yang tidak akan tahan terhadap serangan komputer kuantum yang relevan secara kriptografis. Untuk membantu menjelaskan bagaimana translasi DNS dilakukan, kita akan mengandaikan ada klien yang menginginkan alamat IP misalnya.com. Klien biasanya akan mengirim sebuah ke resolver caching untuk menangani sisa terjemahan atas nama klien. Dengan mengasumsikan bahwa resolver tidak memiliki jawaban untuk kueri example.com, maka akan meminta server nama root untuk server nama yang bertanggung jawab atas nama domain .com. Setelah resolver menerima balasan dari server nama root, maka resolver akan menanyakan nama yang bertanggung jawab atas .com untuk server nama yang bertanggung jawab atas example.com. Terakhir, setelah resolver mengetahui server nama yang bertanggung jawab untuk example.com, maka akan menanyakan server-server tersebut untuk mendapatkan alamat IP yang terkait dengan example.com, dan akhirnya menerima dan meneruskan respons ke klien. Tanggapan respons untuk setiap kueri perantara dapat di-cache mengurangi waktu resolusi dan mengurangi beban pada server nama.

DNSSEC menambahkan tanda tangan digital ke DNS untuk menjaga
integritas data. Label catatan sumber daya tidak harus unik, sehingga semua catatan sumber daya dengan tipe tertentu dan label tertentu dikelompokkan bersama sebagai RRSet. RRSet ini kemudian ditandatangani oleh algoritme tanda tangan digital yang ditentukan, dan tanda tangan disimpan di dalam catatan sumber daya RRSIG. Kunci publik dipublikasikan ke zona di dalam DNSKEY
catatan sumber daya. Umumnya ada dua jenis pasangan kunci
dihasilkan: Kunci Penandatanganan Zona (ZSK), dan Kunci Penandatanganan Kunci
(KSK). ZSK bertanggung jawab untuk menandatangani dan memverifikasi
catatan sumber daya di zona tersebut, dan KSK bertanggung jawab untuk menandatangani ZSK dan memungkinkan rantai
kepercayaan dapat dibangun. Karena kueri dibuat dari server root ke anak-anaknya, dan anak-anaknya, yang akhirnya mencapai server
name server yang sesuai untuk menjawab kueri, sebuah rantai kepercayaan dibangun. Setiap zona yang ditanyakan harus memiliki intisari dari publik
KSK publik yang digunakan disimpan dalam catatan penandatangan delegasi (DS) di zona zona induknya, jika tidak, ZSK publik yang ditransmisikanpublik yang ditransmisikan oleh server nama tidak dapat dipercaya.Satu zona yang tidak mempublikasikan catatan DS adalah zona root, karena kurangnyainduk. KSK publik dari zona root harus diambil out-of-band dari DNS; sebagian besar sistem operasi modern memilikiKSK publik zona akar sudah terinstal sebelumnya, sehingga menghilangkan kebutuhanbagi pengguna untuk mengambil dan mengonfigurasi kunci itu sendiri.

DNS seperti yang ditentukan sebelumnya hanya memungkinkan untuk pesan DNS
paling banyak 512 byte melalui UDP, yang dengan cepat menjadi terlalu keciluntuk mengangkut pesan DNS, terutama dengan adanya DNSSEC.[27]

HASIL :

Spoofing DNS adalah teknik yang digunakan untuk mencegat permintaan peramban terhadap suatu situs web dan mengarahkan pengguna ke situs lain. Serangan ini dapat dilakukan dengan mengubah alamat IP server DNS atau mengubah alamat IP server nama domain itu sendiri. Dalam serangan Spoofing

p-ISSN 2089-0265
e-ISSN 2598-3016

DNS, penyerang menyamar sebagai server DNS dan mengirim respons palsu ke permintaan DNS korban. Respons tersebut dapat berisi informasi palsu, seperti alamat IP host palsu atau informasi palsu lainnya. Spoofing DNS dapat digunakan untuk mengarahkan pengguna ke situs web palsu atau untuk memberikan informasi palsu tentang layanan di jaringan. Namun Skenario yang dilakukan biasanya, yang pertama yaitu Klien mengirimkan permintaan DNS ke server DNS untuk mendapatkan alamat IP suatu nama domain, misalnya, google.com, Setelah itu Penyerangm sebagai perantara, mencegat permintaan tersebut, Lalu Penyerang mengirimkan respons DNS palsu kepada klien, memberikan informasi palsu seperti alamat IP palsu untuk google.com dan sebagai hasilnya, Pengguna diarahkan ke situs web palsu atau infrastruktur tidak sah lainnya.

DNS Spoofing ini dilakukan penyerang untuk melakukan Pengalihan Web untuk portal tawanan, Serta Mengalihkan aplikasi untuk menyebabkan pembaruan OS atau serangan malware, dan Memberikan respons yang lebih cepat dengan menyaring lalu lintas DNS. Spoofing DNS dapat digunakan untuk menerapkan penyaringan jaringan, yang memungkinkan ISP untuk memblokir tujuan tertentu sesuai dengan kebijakan atau hukum local.

DNS Spoofing dapat di deteksi dengan menggunakan metode DHCP Spoofing dan juga dapat menggunakan IP SPOOFING.

Biasanya Penyerang menggunakan Metode Ettercap untuk Serangan DNS Spoofing dengan menganalisis protocol jarinan, memblokir lalu lintas, dan mencuri kata sandi, Penyerang juga dapat memanfaatkan Teknik pengumpulan kata sandi otomatis dan mendukung protocol seperti SSH dan HTTPS.

Serangan tersebut dapat ditanggulangi Dengan menggunakan Metode DNSSEC Karena DNSSEC (Domain Name System Security Extensions) dapat digunakan untuk meningkatkan keamanan DNS dengan menambahkan tanda tangan digital untuk menjaga integritas data Dan kunci Penandatangan Zona (ZSK) dan Kunci pendatanganan Kunci (KSK) digunakan untuk Menandatangani catatan sumber daya di zona dan membangun rantai kepercayaan. DNSSE dapat membantu melindungi terhadap serangan seperti cache poisoning, Man-In-The-Middle attacks, dan penggantian data DNS yang tidak sah. Dibalik itu semua DNSSEC juga memiliki keterbatasan yaitu tidak tahan terhadap serangan komputer kuantum yang relevan secara kriptografis. Dengan adanya ekstensi ini dapat memberikan layanan yang lebih mudah, dalam manangani permasalahan[29] Meskipun Demikian penting perlu diingat bahwa implementasi metode keamanan seperti DNSSEC merupakan langkah yang kritis untuk melindungi system terhadap serangan DNS Spoofing.

5. KESIMPULAN

Hasil penelitian ini diharapkan dapat memberikan wawasan yang berharga bagi pengembangan[30]Untuk menghadapi ancaman Spoofing DNS, penting untuk dipahami bahwa serangan ini memiliki potensi bahaya yang serius terhadap integritas dan keamanan sistem. Spoofing DNS memungkinkan penyerang untuk mengalihkan pengguna ke situs web palsu, hal yang disebabkan Spoofing DNS ini yaitu pembaruan OS atau serangan malware, serta menyaring lalu lintas DNS untuk berbagai tujuan. Untuk melawan ancaman ini, metode keamanan seperti DNSSEC ini dibutuhkan, DNSSEC dapat meningkatkan keamanan DNS dengan menambahkan tanda tangan

digital untuk menjaga integritas data, walaupun Implemetasi ini tidak tahan terhadap serangan komputer kuantum yang relevan secara kriptografis. Meskipun demikian, langkah-langkah keamanan seperti implementasi DNSSEC tetap merupakan langkah kritis untuk melindungi sistem terhadap serangan DNS Spoofing yang semakin canggih dan merugikan.

[1] K. Al Fikri and Djuniadi, "Keamanan Jaringan Menggunakan Switch Port Security," *InfoTekJar J. Nas. Inform. dan Teknol. Jar.*, vol. 5, no. 2, pp. 302–307, 2021, [Online]. Available: http://bit.ly/InfoTekJar

[2] M. A. Hussain, H. Jin, Z. A. Hussien, Z. A. Abduljabbar, S. H. Abbdal, and A. Ibrahim, "DNS Protection against Spoofing and Poisoning Attacks," *Proc. - 2016 3rd Int. Conf. Inf. Sci. Control Eng. ICISCE 2016*, pp. 1308–1312, 2016, doi: 10.1109/ICISCE.2016.279.

[3] A. Gunawan, R. Rahmah, and A. Iskandar, "Rancang Bangun Jaringan Hotspot Menggunakan LINUX ClearOS Dengan Konsep Security Gateway," *JTIM J. Teknol. Inf. dan Multimed.*, vol. 4, no. 4, pp. 272–280, 2023, doi: 10.35746/jtim.v4i4.251.

[4] R. Mujiastuti and I. Prasetyo, "Membangun Sistem Keamanan Jaringan Berbasis VPN yang Terintegrasi dengan DNS Filtering PIHOLE," *J. Tek. Inform.*, no. November 2021, pp. 1–10, 2021, [Online]. Available: www.google.com

[5] S. Maroofi, M. Korczynski, A. Holzel, and A. Duda, "Adoption of Email Anti-Spoofing Schemes: A Large Scale Analysis," *IEEE Trans. Netw. Serv. Manag.*, vol. 18, no. 3, pp. 3184–3196, 2021, doi: 10.1109/TNSM.2021.3065422.

[6] A. T. Laksono and M. A. H. Nasution, "Implementasi Keamanan Jaringan Komputer Local Area Network Menggunakan Access Control List pada Perusahaan X," *J. Sist. Komput. dan Inform.*, vol. 1, no. 2, p. 83, 2020, doi: 10.30865/json.v1i2.1920.

[7] A. A. Maksutov, I. A. Cherepanov, and M. S. Alekseev, "Detection and prevention of DNS spoofing attacks," in *Proceedings - 2017 Siberian Symposium on Data Science and Engineering, SSDSE 2017*, 2017. doi: 10.1109/SSDSE.2017.8071970.

[8] H. Shulman and M. Waidner, "Towards forensic analysis of attacks with DNSSEC," *Proc. - IEEE Symp. Secur. Priv.*, vol. 2014-Janua, pp. 69–76, 2014, doi: 10.1109/SPW.2014.20.

[9] A. H. Fauzan Prasetyo Eka Putra, Selly Mellyana Dewi, Maugfiroh, "Privasi dan Keamanan Penerapan IoT Dalam Kehidupan Sehari-Hari : Tantangan dan Implikasi," *J. Sistim Inf. dan Teknol.*, vol. 5, no. 2, pp. 26–32, 2023, doi: 10.37034/jsisfotek.v5i1.232.

[10] D. Bahtiar *et al.*, "Pengenalan Dasar Instalasi Jaringan Komputer Menggunakan Mikrotik," *J. Kreat. Mhs. Inform.*, vol. Volume 2 N, p. Page 507-518, 2021.

[11] W. D. Journal, "SECURITY OF THE DNSSEC PROTOCOL AND ITS IMPACT ON ONLINE PRIVACY," vol. 1, no. 5, 2023.

[12] L. Wei and J. Heidemann, *Whac-A-Mole: Six Years of DNS*

Spoofing, vol. 1, no. 1. Association for Computing Machinery, 2020. [Online]. Available: http://arxiv.org/abs/2011.12978

[13] H. Alamsyah, R. -, and A. Al Akbar, "Analisa Keamanan Jaringan Menggunakan Network Intrusion Detection and Prevention System," *JOINTECS (Journal Inf. Technol. Comput. Sci.*, vol. 5, no. 1, p. 17, 2020, doi: 10.31328/jointecs.v5i1.1240.

[14] D. Javeed and U. MohammedBadamasi, "Man in the Middle Attacks: Analysis, Motivation and Prevention," *Int. J. Comput. Networks Commun. Secur.*, vol. 8, no. 7, pp. 52–58, 2020, doi: 10.47277/ijcncs/8(7)1.

[15] T. Pangestu, R. Liza, P. Studi, T. Informatika, and U. H. Medan, "ISSN 2338-5677 Cetak ISSN 2548-6646 Online Analisis Keamanan Jaringan pada Jaringan Wireless dari Serangan Man In The Middle Attack DNS Spoofing ISSN 2338-5677 Cetak ISSN 2548-6646 Online," vol. 10, no. 2, pp. 60–67, 2022.

[16] K. M. Majidha Fathima and N. Santhiyakumari, "A Survey on Network Packet Inspection and ARP Poisoning Using Wireshark and Ettercap," *Proc. - Int. Conf. Artif. Intell. Smart Syst. ICAIS 2021*, pp. 1136–1141, 2021, doi: 10.1109/ICAIS50930.2021.9395852.

[17] B. Pingle, A. Mairaj, and A. Y. Javaid, "Real-World Man-in-the-Middle (MITM) Attack Implementation Using Open Source Tools for Instructional Use," *IEEE Int. Conf. Electro Inf. Technol.*, vol. 2018-May, pp. 192–197, 2018, doi: 10.1109/EIT.2018.8500082.

[18] R. Rizal, R. Ruuhwan, and K. A. Nugraha, "Implementasi Keamanan Jaringan Menggunakan Metode Port Blocking dan Port Knocking Pada Mikrotik RB-941," *J. ICT Inf. Commun. Technol.*, vol. 19, no. 1, pp. 1–8, 2020, doi: 10.36054/jict-ikmi.v19i1.119.

[19] Sutarti, A. P. Pancaro, and F. I. Saputra, "Implementasi IDS (Intrusion Detection System) Pada Sistem Keamanan Jaringan SMAN 1 Cikeusal," *J. PROSISKO*, vol. 5, no. 1, pp. 1–8, 2018.

[20] I. F. B. Andoro, H. Agung Budijanto, and M. Aidjili, "Analisa Keamanan Jaringan Dengan Mikrotik," *RISTEK J. Riset, Inov. dan Teknol. Kabupaten Batang*, vol. 6, no. 2, pp. 35–39, 2022, doi: 10.55686/ristek.v6i2.111.

[21] A. G. Gani, "Konfigurasi Sistem Keamanan Jaringan," *J. Sist. Inf. Univ. Suryadarma*, vol. 6, no. 1, pp. 134–149, 2014, doi: 10.35968/jsi.v6i1.280.

[22] J. D. Santoso, "Keamanan Jaringan Nirkabel Menggunakan Wireless Intrusion Detection System," *Infos*, vol. 1, no. 3, pp. 44–50, 2019.

[23] F. Prasetyo, "Penggunaan Stb Sebagai Media E-Learning Berbasis Moodle," *J. Inform.*, vol. 23, no. 1, pp. 35–42, 2023, doi: 10.30873/ji.v23i1.3523.

[24] N. Triyana *et al.*, "Analisis Dns Amplification Attack," vol. 1, no. 1, pp. 17–22, 2017.

[25] Y. A. Pohan, "Meningkatkan Keamanan Webserver Aplikasi Pelaporan Pajak Daerah Menggunakan Metode Penetration Testing Execution Standar," *J. Sistim Inf. dan Teknol.*, vol. 3, pp. 1–6, 2021, doi: 10.37034/jsisfotek.v3i1.36.

[26] R. Kreuger, "Review of social media traffic at the DNS resolvers and their security," vol. 1, no. 1.

[27] J. Goertzen and D. Stebila, "Post-Quantum Signatures in DNSSEC via Request-Based Fragmentation," Nov. 2022, [Online]. Available: http://arxiv.org/abs/2211.14196

[28] A. Baidawi, "JARINGAN SENSOR NIRKABEL DAN IoT UNTUK KOTA PINTAR PAMEKASAN," *J. Sist. Inf. Kaputama*, vol. 7, no. 2, pp. 104–110, 2023, doi: 10.59697/jsik.v7i2.108.

[29] P. Infomatika, F. Teknik, U. Madura, J. P. Km, and P. J. Timur, "APLIKASI PENGOLAHAN DATA MAHASISWA KKN," vol. 8, no. 2, pp. 24–29, 2023.

[30] N. Muhammad Akbar, F. Prasetyo Eka Putra, K. Zulfana Imam, and M. Umar Mansyur, "Analisis Kinerja dan Interopabilitas STB Sebagai Server Penilaian Akhir Tahun," *J. Inf. dan Teknol.*, vol. 5, no. 2, pp. 91–96, 2023, doi: 10.37034/jidt.v5i2.365.