Remik: Riset dan E-Jurnal Manajemen Informatika Komputer
Volume 8, Nomor 1, Januari 2024
http://doi.org/10.33395/remik.v8i1.13398
e-ISSN : 2541-1330
p-ISSN : 2541-1332

Optimasi Keamanan DNS: Eksplorasi Optimal dengan Implementasi DNS Security Extensions (DNSSEC)

[1]Fauzan Prasetyo Eka Putra, [2]Alief Badrit Tamam, [3]Reynal Widya Efendi, [4]Zaini Muim
[1,2,3,4]Universitas Madura
Pamekasan, Indonesia

[1]prasetyo@unira.ac.id , [2]aliefbadrittamam@gmail.com, [3]reynalwidya91@gmail.com, [4]mazmonim180@gmail.com

*Penulis Korespondensi
Diajukan : 14/01/2024
Diterima : 21/01/2024
Dipublikasi : 22/01/2024

ABSTRAK
Serangan Spoofing DNS merupakan ancaman serius terhadap keamanan dan integritas sistem, memungkinkan penyerang untuk mengalihkan pengguna ke situs web palsu atau menyebabkan pembaruan OS dan serangan malware. Penelitian ini menyajikan metodologi untuk mencegah pemalsuan domain dengan mengelola dan menganalisis DNS. Sistem Nama Domain (DNS) merupakan bagian kunci dari protokol Internet, namun keberlanjutan dan keakuratan DNS dapat dengan mudah diserang. Kecepatan perkembangan teknologi internet meningkatkan risiko keamanan, termasuk pencurian data. Masalah keamanan pada Perusahaan X, seperti kurangnya pengendalian hak akses pengguna, dapat mengancam keamanan dan menyebabkan penyalahgunaan. Spoofing DNS menyoroti metode serangan, tujuan, dan dampaknya terhadap keamanan pengguna internet. Metodologi penelitian ini mengadopsi pendekatan kualitatif untuk memahami perilaku pengguna dalam memanfaatkan komputer dan internet. Analisis lalu lintas jaringan, pemantauan aktivitas perangkat, dan deteksi serangan berbasis perilaku menjadi solusi pengawasan jaringan. Spoofing DNS dapat dideteksi dengan metode DHCP Spoofing dan IP Spoofing. Serangan umumnya menggunakan alat seperti Ettercap, yang dapat memblokir lalu lintas, mencuri kata sandi, dan mendukung protokol seperti SSH dan HTTPS. Implementasi DNS Security Extensions (DNSSEC) menjadi solusi untuk meningkatkan keamanan DNS dengan menambahkan tanda tangan digital. Namun, DNSSEC memiliki keterbatasan terhadap serangan komputer kuantum. langkah-langkah keamanan seperti implementasi DNSSEC menjadi kritis untuk melindungi sistem terhadap serangan Spoofing DNS yang semakin canggih. Penelitian ini diharapkan memberikan wawasan bagi pengembangan solusi keamanan yang lebih efektif dan efisien.

Kata Kunci : DNS, DNSSEC, Jaringan, Keamanan, Spoofing

I. 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 (Al Fikri & Djuniadi, 2021). Domain Name System/Sistem nama domain (DNS) adalah salah satu bagian inti dari rangkaian protokol TCP/IP dan protokol standar yang digunakan oleh Internet (Hussain et al., 2016). 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

Remik: Riset dan E-Jurnal Manajemen Informatika Komputer
Volume 8, Nomor 1, Januari 2024 e-ISSN : 2541-1330
http://doi.org/10.33395/remik.v8i1.13398 p-ISSN : 2541-1332

DNS (Gunawan et al., 2023).

Sistem nama domain terdiri dari nama-nama situs web yang dipetakan dengan protokol Internet, yang memfasilitasi penjelajahan dengan tidak mengharuskan pengguna untuk mengingat alamat notasi numerik. Sifat sistem ini, yang melibatkan transfer informasi dalam teks biasa, membuatnya rentan terhadap serangan keamanan (Hussain et al., 2016) . 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 (Mujiastuti & Prasetyo, 2021).

kami menyajikan metodologi untuk mencegah pemalsuan domain berdasarkan praktik-praktik yang baik dalam mengelola serta menganalisis DNS (Maroofi et al., 2021). 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 (Laksono & Nasution, 2020) . 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) (Maksutov et al., 2017) .

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 (Shulman & Waidner, 2014). Analisa kebutuhan sistem dilakukan untuk mengetahui apa saja yang diperlukan dalam merancang 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 (Fauzan Prasetyo Eka Putra, Selly Mellyana Dewi, Maugfiroh, 2023). karena Dengan perkembangan teknologi informasi, para penjahat menggunakan berbagai ruang cyber untuk meningkatkan kejahatan cyber (Dermawan et al., 2023) (Informasi et al., 2023).

II. STUDI LITERATUR

Karakteristik dan Metode Spoofing DNS

"Menurut penelitian yang dilakukan oleh Susanto dan Wibowo (2019), Spoofing DNS merupakan serangan yang signifikan di lingkungan jaringan Indonesia. Mereka mengidentifikasi metode serangan, termasuk cache poisoning, yang menjadi ancaman potensial terhadap integritas DNS."

Tujuan dan Dampak Spoofing DNS

"Studi yang dilakukan oleh Prasetyo dan Nugroho (2020) mengungkapkan bahwa Spoofing DNS memiliki dampak serius terhadap keamanan pengguna internet di Indonesia. Serangan ini dapat mengarahkan pengguna ke situs web palsu atau memberikan informasi palsu, meningkatkan risiko kerugian data pribadi."

Penggunaan Spoofing DNS dalam Pengalihan Aplikasi

"Implementasi Spoofing DNS untuk pengalihan aplikasi di lingkungan jaringan lokal Indonesia menjadi fokus penelitian, seperti yang dijelaskan oleh Setiawan dan Santoso (2018). Mereka mengidentifikasi bahwa serangan semacam ini dapat mempengaruhi integritas lalu lintas aplikasi di tingkat lokal."

Remik: Riset dan E-Jurnal Manajemen Informatika Komputer
Volume 8, Nomor 1, Januari 2024
http://doi.org/10.33395/remik.v8i1.13398
e-ISSN : 2541-1330
p-ISSN : 2541-1332

III. METODE

Tahapan penelitian

Perencanaan Penelitian:

Pada proses penelitian ini proses yang dilakukan meliputi penentuan tujuan penelitian, perumusan pertanyaan penelitian, menentukan metode penelitia, menetapkan sampel, mengidentifikasikan alat atau sumber penelitian yang diperlukan, membuat jadwal atau timeline

Perencanaan Research:

Dalam proses research merupakan pengumpulan data dimana kita akan mencari informasi dan sumber yang akan di tetapkan pada jurnal seperti IEEE, Google Scholar dan lain sebagainya, dan merencanakan strategi pencarian informasi.

Perbandingan Studi Literatur:

Perbandingan studi literatur adalah peninjauan literatur yang relevan dengan topik penelitian dan menganalisis temuan penelitian sebelumnya yang telah dilakukan dalam proses research, menilai kelebihan dan kekurangan studi literatur yang ada.

Penyesuaian Data:

Penyesuain data dimana disini kita melakukan pembersihan data dari potensi kesalahan dan mengcek kevalidan data, jika tidak sesuai maka kembali ke proses research jika sesuai akan dilanjutkan dalam proses analisis.

Analisis:

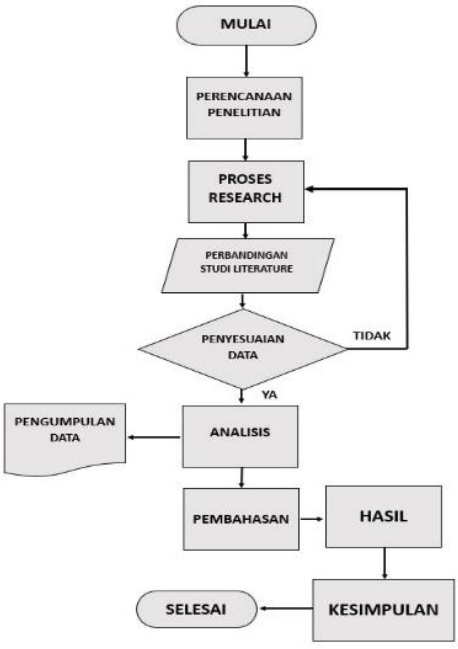
Pada proses analisis yakni penerapan metode analisis data yang sesuai dan menafsirkan hasil

Pengumpulan Data:

Pengumpulan data ini dilakukan agar data yang sudah disesuaikan dan di analisis dapat di survei dan dirancang sesuai rencana, dan dilakukan perekaman data secara sistematis.

Pembahasan dan Hasil:

Pembahasan merupakan poin utama untuk penentuan hasil dimana disini menyajikan hasil dari penelitian yang sudah terstruktur dan membahas temuan penelitian yang sesuai dengan pertanyaan penelitian dan menafsirkan arti temuan dan mengaitkannya dengan literatur yang ada, pengindetifikasian implikasi praktis dan teoritis serta menyajikan saran untuk penelitian lebih lanjut. Tahapan tersebut dapat dilihat di flowchart metode penelitian pada gambar 1.



Gambar. 1. Flowchart Metode Penelitian

Remik: Riset dan E-Jurnal Manajemen Informatika Komputer
Volume 8, Nomor 1, Januari 2024 e-ISSN : 2541-1330
http://doi.org/10.33395/remik.v8i1.13398 p-ISSN : 2541-1332

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.

IV. HASIL DAN PEMBAHASAN

DNS(Domain name system)

Dns ini bertujuan mengubah alamat IP menjadi sebuah domain atau nama yang akan memudahkan dalam melakukan pencarian sebuah domain (Bahtiar et al., 2021). 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 (Journal, 2023). Untuk mendemonstrasikan proses Spoofing DNS, contoh skenario berikut ini telah dibuat. Skenario ini menunjukkan bagaimana penyerang dapat mengarahkan korban ke situs web palsu Pertama Klien mengirimkan permintaan DNS ke server DNS, meminta alamat IP untuk nama domain, misalnya google.com. kedua Penyerang, sebagai perantara antara klien dan server DNS yang sebenarnya, mencegat permintaan ini. Selanjutnya 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, di mana penyerang dapat mencoba mencuri informasi sensitif seperti kata sandi atau kredensial login (Journal, 2023).

Spoofing DNS

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

e-ISSN : 2541-1330
p-ISSN : 2541-1332

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).

Pengalihan 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. 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. 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 (Wei & Heidemann, 2020).

Pengambilan Tindakan

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) (Alamsyah et al., 2020).Karena DNS dikirim tanpa dienkripsi, maka dienkripsi, spoofing dapat digunakan untuk menguping lalu lintas DNS untuk mengamati metadata komunikasi (Wei & Heidemann, 2020).

Untuk mendeteksi serangan seperti itu ada cara yang sangat sederhana yang diberikan yaitu, 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 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.

Penyerangan serta tools yang umum digunakan

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 (Pangestu et al., 2022). 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

e-ISSN : 2541-1330
p-ISSN : 2541-1332

menganalisis OS pola sidik jari dengan mengidentifikasi semua perintah yang dijalankan dalam sistem operasi tertentu dari korban di bawah pertimbangan (Majidha Fathima & Santhiyakumari, 2021).

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 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, 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 (Pingle et al., 2018). *Point-to-Point Tunneling Protocol (PPTP) suite* Attacker can perform MITM attack against PPTP tunnels (Pingle et al., 2018). 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 (Rizal et al., 2020) . 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 (Sutarti et al., 2018).

Penggunaan DNSSEC

Metode penelitian melibatkan studi kasus dengan implementasi DNSSEC (Muhammad Akbar et al., 2023), dari sisi keamanan tentunya ini sangat perlu menjadi perhatian dengan cara memaksimalkan fungsi keamanan yang ada (Andoro et al., 2022). Memilih sistem keamanan yang tepat akan mencegah kejadian yang tidak diinginkan seperti serangan atau akses tidak sah (Gani, 2014). 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 Ada solusi alternatif yang dapat ditawarkan yaitu menjalankan (Santoso, 2019) (Prasetyo, 2023). Domain Name System Security Extensions (DNSSEC) ini 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 (Triyana et al., 2017). Kerentanan disebabkan DNS tidak diinstall DNSSEC dan mode recursion yes Dengan mengaktifkan DNSSEC dan menonaktifkan mode recursive (Pohan, 2021). 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,

e-ISSN : 2541-1330
p-ISSN : 2541-1332

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. Salah satu keunggulan utama yang disediakan oleh sistem ini adalah (Baidawi, 2023). DNSSEC saat ini menggunakan tanda tangan digital yang bergantung pada 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 name.

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 public 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 memiliki KSK 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 kecil untuk mengangkut pesan DNS, terutama dengan adanya DNSSEC (Goertzen & Stebila, 2022).

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 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

e-ISSN : 2541-1330
p-ISSN : 2541-1332

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(Infomatika et al., 2023) Meskipun Demikian penting perlu diingat bahwa implementasi metode keamanan seperti DNSSEC merupakan langkah yang kritis untuk melindungi system terhadap serangan DNS Spoofing.

V. KESIMPULAN

Hasil penelitian ini diharapkan dapat memberikan wawasan yang berharga bagi pengembangan 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.

VI. REFERENSI

Al Fikri, K., & Djuniadi. (2021). Keamanan Jaringan Menggunakan Switch Port Security. *InfoTekJar : Jurnal Nasional Informatika Dan Teknologi Jaringan*, *5*(2), 302–307. http://bit.ly/InfoTekJar

Alamsyah, H., -, R., & Al Akbar, A. (2020). Analisa Keamanan Jaringan Menggunakan Network Intrusion Detection and Prevention System. *JOINTECS (Journal of Information Technology and Computer Science)*, *5*(1), 17. https://doi.org/10.31328/jointecs.v5i1.1240

Andoro, I. F. B., Agung Budijanto, H., & Aidjili, M. (2022). Analisa Keamanan Jaringan Dengan Mikrotik. *RISTEK : Jurnal Riset, Inovasi Dan Teknologi Kabupaten Batang*, *6*(2), 35–39. https://doi.org/10.55686/ristek.v6i2.111

Bahtiar, D., Febrianto, W. J., Maulana, A., Saputra, S., Darmawan, W., Remis, Tafonao, P., Julianto, R., Zai, R., & Djutalov, R. (2021). Pengenalan Dasar Instalasi Jaringan Komputer Menggunakan Mikrotik. *Jurnal Kreativitas Mahasiswa Informatika*, *Volume 2 N*, Page 507-518.

Baidawi, A. (2023). JARINGAN SENSOR NIRKABEL DAN IoT UNTUK KOTA PINTAR PAMEKASAN. *Jurnal Sistem Informasi Kaputama (JSIK)*, *7*(2), 104–110. https://doi.org/10.59697/jsik.v7i2.108

Dermawan, I., Baidawi, A., Iksan, & Mellyana Dewi, S. (2023). Serangan Cyber dan Kesiapan Keamanan Cyber Terhadap Bank Indonesia. *Jurnal Informasi Dan Teknologi*, *5*(3), 20–25. https://doi.org/10.60083/jidt.v5i3.364

Fauzan Prasetyo Eka Putra, Selly Mellyana Dewi, Maugfiroh, A. H. (2023). Privasi dan Keamanan Penerapan IoT Dalam Kehidupan Sehari-Hari : Tantangan dan Implikasi. *Jurnal Sistim Informasi Dan Teknologi*, *5*(2), 26–32. https://doi.org/10.37034/jsisfotek.v5i1.232

Gani, A. G. (2014). Konfigurasi Sistem Keamanan Jaringan. *Jurnal Sistem Informasi Universitas Suryadarma*, *6*(1), 134–149. https://doi.org/10.35968/jsi.v6i1.280

Goertzen, J., & Stebila, D. (2022). *Post-Quantum Signatures in DNSSEC via Request-Based Fragmentation*. http://arxiv.org/abs/2211.14196

Gunawan, A., Rahmah, R., & Iskandar, A. (2023). Rancang Bangun Jaringan Hotspot Menggunakan LINUX ClearOS Dengan Konsep Security Gateway. *JTIM : Jurnal Teknologi Informasi Dan Multimedia*, *4*(4), 272–280. https://doi.org/10.35746/jtim.v4i4.251

Hussain, M. A., Jin, H., Hussien, Z. A., Abduljabbar, Z. A., Abbdal, S. H., & Ibrahim, A. (2016). DNS Protection against Spoofing and Poisoning Attacks. *Proceedings - 2016 3rd International Conference on Information Science and Control Engineering, ICISCE 2016*, 1308–1312. https://doi.org/10.1109/ICISCE.2016.279

Infomatika, P., Teknik, F., Madura, U., Km, J. P., & Timur, P. J. (2023). *APLIKASI PENGOLAHAN DATA MAHASISWA KKN*. *8*(2), 24–29.

Informasi, J., Mar, Y., & Ratnasari, N. (2023). *Penerapan Media Pembelajaran Untuk Anak Penderita Autisme Menggunakan Teknologi Augmented Reality*. *5*(4), 39–52. https://doi.org/10.60083/jidt.v5i4.413

Journal, W. D. (2023). *SECURITY OF THE DNSSEC PROTOCOL AND ITS IMPACT ON ONLINE PRIVACY*. *1*(5).

Laksono, A. T., & Nasution, M. A. H. (2020). Implementasi Keamanan Jaringan Komputer Local Area Network Menggunakan Access Control List pada Perusahaan X. *Jurnal Sistem Komputer Dan Informatika (JSON)*, *1*(2), 83. https://doi.org/10.30865/json.v1i2.1920

Majidha Fathima, K. M., & Santhiyakumari, N. (2021). A Survey on Network Packet Inspection and ARP Poisoning Using Wireshark and Ettercap. *Proceedings - International Conference on Artificial Intelligence and Smart Systems, ICAIS 2021*, 1136–1141.

https://doi.org/10.1109/ICAIS50930.2021.9395852

Maksutov, A. A., Cherepanov, I. A., & Alekseev, M. S. (2017). Detection and prevention of DNS spoofing attacks. *Proceedings - 2017 Siberian Symposium on Data Science and Engineering, SSDSE 2017*. https://doi.org/10.1109/SSDSE.2017.8071970

Maroofi, S., Korczynski, M., Holzel, A., & Duda, A. (2021). Adoption of Email Anti-Spoofing Schemes: A Large Scale Analysis. *IEEE Transactions on Network and Service Management*, *18*(3), 3184–3196. https://doi.org/10.1109/TNSM.2021.3065422

Muhammad Akbar, N., Prasetyo Eka Putra, F., Zulfana Imam, K., & Umar Mansyur, M. (2023). Analisis Kinerja dan Interopabilitas STB Sebagai Server Penilaian Akhir Tahun. *Jurnal Informasi Dan Teknologi*, *5*(2), 91–96. https://doi.org/10.37034/jidt.v5i2.365

Mujiastuti, R., & Prasetyo, I. (2021). Membangun Sistem Keamanan Jaringan Berbasis VPN yang Terintegrasi dengan DNS Filtering PIHOLE. *Jurnal Teknik Informatika*, *November 2021*, 1–10. www.google.com

Pangestu, T., Liza, R., Studi, P., Informatika, T., & Medan, U. H. (2022). *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*. *10*(2), 60–67.

Pingle, B., Mairaj, A., & Javaid, A. Y. (2018). Real-World Man-in-the-Middle (MITM) Attack Implementation Using Open Source Tools for Instructional Use. *IEEE International Conference on Electro Information Technology*, *2018-May*, 192–197. https://doi.org/10.1109/EIT.2018.8500082

Pohan, Y. A. (2021). Meningkatkan Keamanan Webserver Aplikasi Pelaporan Pajak Daerah Menggunakan Metode Penetration Testing Execution Standar. *Jurnal Sistim Informasi Dan Teknologi*, *3*, 1–6. https://doi.org/10.37034/jsisfotek.v3i1.36

Prasetyo, F. (2023). Penggunaan Stb Sebagai Media E-Learning Berbasis Moodle. *Jurnal Informatika*, *23*(1), 35–42. https://doi.org/10.30873/ji.v23i1.3523

Rizal, R., Ruuhwan, R., & Nugraha, K. A. (2020). Implementasi Keamanan Jaringan Menggunakan Metode Port Blocking dan Port Knocking Pada Mikrotik RB-941. *Jurnal ICT : Information Communication & Technology*, *19*(1), 1–8. https://doi.org/10.36054/jict-ikmi.v19i1.119

Santoso, J. D. (2019). Keamanan Jaringan Nirkabel Menggunakan Wireless Intrusion Detection System. *Infos*, *1*(3), 44–50.

Shulman, H., & Waidner, M. (2014). Towards forensic analysis of attacks with DNSSEC. *Proceedings - IEEE Symposium on Security and Privacy*, *2014-Janua*, 69–76. https://doi.org/10.1109/SPW.2014.20

Sutarti, Pancaro, A. P., & Saputra, F. I. (2018). Implementasi IDS (Intrusion Detection System) Pada Sistem Keamanan Jaringan SMAN 1 Cikeusal. *Jurnal PROSISKO*, *5*(1), 1–8.

Triyana, N., Eka, A., Program,), Pendidikan, S., Informasi, T., Pgri, S., Jalan, T., Sujadi, M., & Nomor, T. (2017). *Analisis Dns Amplification Attack*. *1*(1), 17–22.

Wei, L., & Heidemann, J. (2020). Whac-A-Mole: Six Years of DNS Spoofing. In *Proceedings of ACM Conference (Conference'17)* (Vol. 1, Issue 1). Association for Computing Machinery. http://arxiv.org/abs/2011.12978