Jurnal Infomedia : Teknik Informatika, Multimedia, dan Jaringan
Volume 10, Number 2, Desember Tahun 2025
ISSN 2527-9858 (online), 2549-1180 (print)
Artikel Penelitian/Artikel Review

Implementasi Zero Trust Security Model Untuk Perlindungan Dns Dari Serangan Dns Spoofing Menggunakan Dns-Over-Https (Doh) Dan Ids.

M. Imam Faisal [1] **Alek Wijaya**[2] **Fatoni**[3] **Tamsir Ariyadi**[4]
[1] Teknik Informatika, Sains Teknologi, Universitas Bina Darma, mimamfsl10@gmail.com
[2] Teknik Informatika, Sains Teknologi, Universitas Bina Darma, alex_wj@binadarma.ac.id
[3] Teknik Informatika, Sains Teknologi, Universitas Bina Darma, fatoni@binadarma.ac.id
[4] Teknik Komputer, Sains Teknologi, Universitas Bina Darma, tamsirariyadi@binadarma.ac.id
*Corresponding Author: M. Imam Faisal, **mimamfsl10@gmail.com, 088287428282**

Abstrak
Penelitian ini dilatarbelakangi oleh meningkatnya ancaman terhadap keamanan jaringan, khususnya serangan Domain Name System (DNS) Spoofing yang memanfaatkan kelemahan pada proses resolusi DNS untuk mengarahkan pengguna ke tujuan berbahaya. Sistem DNS konvensional masih memiliki celah karena pertukaran data dilakukan tanpa enkripsi, sehingga rentan dimanipulasi. Oleh sebab itu, dibutuhkan pendekatan yang lebih adaptif dan berlapis. Salah satu strategi yang digunakan adalah Zero Trust Security Model (ZTSM) dengan prinsip "never trust, always verify," yang dalam penelitian ini diintegrasikan dengan DNS-over-HTTPS (DoH) dan Intrusion Detection System (IDS) Snort. Metode penelitian dilakukan melalui implementasi DoH menggunakan dnscrypt-proxy pada VPS berbasis Ubuntu, serta konfigurasi Snort sebagai IDS untuk memantau dan mendeteksi lalu lintas DNS mencurigakan. Simulasi serangan dilakukan menggunakan Kali Linux sebagai mesin penyerang dengan mengirimkan permintaan DNS ke domain uji secure.test. Hasil pengujian menunjukkan bahwa penggunaan DoH berhasil mengenkripsi komunikasi DNS, sehingga lalu lintas menjadi lebih aman. Di sisi lain, Snort mampu mendeteksi permintaan DNS yang tidak terenkripsi, meskipun efektivitasnya lebih terlihat pada protokol TCP dibandingkan UDP. Pada pengujian, deteksi Snort terhadap lalu lintas DNS melalui TCP mencapai 100%, sementara pada protokol UDP tingkat deteksi hanya 0%. Sebaliknya, ketika DoH aktif, seluruh permintaan DNS terenkripsi dengan tingkat deteksi 0% dan tidak terdeteksi 100%, yang menunjukkan bahwa IDS tidak dapat membaca payload DNS terenkripsi. Temuan ini mengindikasikan bahwa kombinasi Zero Trust Security Model, DoH, dan IDS dapat meningkatkan perlindungan DNS dari ancaman spoofing. Namun, optimalisasi lebih lanjut pada IDS masih diperlukan agar dapat memberikan deteksi yang konsisten pada semua jenis protokol komunikasi.

Keywords: *Domain Name System (DNS); Zero Trust Security Model; DNS Spoofing; DNS-over-HTTPS (DoH); Intrusion Detection System (IDS).*

Abstract
This research is motivated by the growing threats to network security, particularly Domain Name System (DNS) Spoofing attacks that exploit weaknesses in DNS resolution to redirect users to malicious destinations. Conventional DNS systems remain vulnerable because data exchange is carried out without encryption, making them prone to manipulation. Therefore, a more adaptive and layered approach is needed. One strategy employed is the Zero Trust Security Model (ZTSM) with the principle of "never trust, always verify," which in this study is integrated with DNS-over-HTTPS (DoH) and the Snort Intrusion Detection System (IDS). The research method was conducted by implementing DoH using dnscrypt-proxy on an Ubuntu-based VPS, along with configuring Snort as an IDS to monitor and detect suspicious DNS traffic. The attack simulation was carried out using Kali Linux as the attacking machine by sending DNS requests to the test domain secure.test. The results show that DoH successfully encrypted DNS communications, thereby securing the traffic. The experimental results indicate that Snort is capable of detecting unencrypted DNS requests, although its effectiveness is more pronounced in the TCP protocol compared to UDP. Specifically, the detection rate for DNS traffic over TCP reached 100%, while detection in the UDP protocol was recorded at only 0%. In contrast, when DoH was enabled, all DNS requests were encrypted, resulting in a detection rate of 0% and an undetected rate of 100%, thereby demonstrating that the IDS was unable to analyze the encrypted DNS payload. These findings suggest that the integration of the Zero Trust Security Model, DoH, and IDS can significantly enhance DNS protection against spoofing attacks. Nevertheless, further optimization of the IDS remains necessary to ensure consistent detection across different communication protocols.

Keywords: *Domain Name System (DNS); Zero Trust Security Model; DNS Spoofing; DNS-over-HTTPS (DoH); Intrusion Detection System (IDS).*

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan signifikan dalam kehidupan manusia. Hampir semua aspek aktivitas, baik pendidikan, bisnis, maupun pemerintahan, bergantung pada infrastruktur jaringan yang aman dan andal. Salah satu komponen fundamental dalam komunikasi internet adalah Domain Name System (DNS), yang berfungsi sebagai penerjemah nama domain menjadi alamat IP. Meskipun vital, DNS tradisional memiliki kelemahan mendasar karena proses resolusi dilakukan tanpa enkripsi, sehingga rentan dimanipulasi oleh pihak tidak berwenang. Kerentanan tersebut membuka peluang terjadinya serangan DNS Spoofing, yaitu upaya penyerang untuk mengarahkan permintaan DNS pengguna ke alamat IP palsu. Dampaknya dapat berupa pencurian data, penyebaran malware, maupun serangan man-in-the-middle.

Ancaman ini semakin relevan karena banyak organisasi masih mengandalkan DNS standar tanpa mekanisme perlindungan tambahan. Model keamanan jaringan konvensional yang berbasis perimeter pun dianggap tidak lagi memadai, sebab mengasumsikan bahwa semua perangkat dalam jaringan internal dapat dipercaya. Padahal, serangan modern dapat berasal dari dalam maupun luar jaringan, serta mampu menembus perimeter tradisional. Oleh karena itu, paradigma baru keamanan informasi diperkenalkan melalui Zero Trust Security Model (ZTSM). Model ini pertama kali dikemukakan oleh Kindervag (2010) dengan prinsip never trust, always verify, yang menegaskan bahwa tidak ada entitas yang diberi kepercayaan secara implisit. Setiap permintaan akses harus diverifikasi terlebih dahulu, baik dari dalam maupun luar jaringan.

Dalam konteks perlindungan DNS, prinsip Zero Trust dapat diwujudkan melalui kombinasi dua teknologi utama, yaitu DNS-over-HTTPS (DoH) dan Intrusion Detection System (IDS). DoH mengenkripsi permintaan DNS ke dalam protokol HTTPS, sehingga menyulitkan pihak ketiga untuk menyadap atau memodifikasi paket DNS (Kintis, 2020). Sementara itu, IDS seperti Snort digunakan untuk memantau lalu lintas jaringan dan memberikan peringatan terhadap aktivitas mencurigakan. Integrasi DoH dan IDS diharapkan mampu menciptakan sistem DNS yang lebih tangguh terhadap manipulasi DNS.

Berdasarkan permasalahan tersebut, penelitian ini dilakukan dengan fokus pada pertanyaan utama: bagaimana celah keamanan DNS tradisional dapat dieksploitasi dalam serangan DNS Spoofing, bagaimana efektivitas kombinasi DoH dan IDS dalam mendeteksi serta mencegah serangan tersebut, serta sejauh mana penerapan Zero Trust dapat meningkatkan ketahanan DNS dalam skenario simulasi jaringan. Untuk menjawab pertanyaan ini, penelitian menggunakan pendekatan eksperimen melalui implementasi DoH menggunakan dnscrypt-proxy pada VPS Ubuntu, serta IDS Snort untuk mendeteksi lalu lintas DNS mencurigakan. Kali Linux digunakan sebagai perangkat penyerang yang mensimulasikan query DNS terhadap domain uji secure.test.

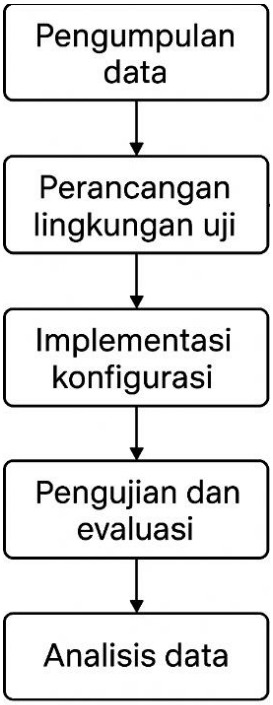
Tujuan dari penelitian ini adalah untuk mengevaluasi efektivitas integrasi Zero Trust Security Model dengan DoH dan IDS dalam melindungi DNS dari serangan DNS Spoofing. Secara khusus, penelitian ini berupaya mengidentifikasi kelemahan DNS tradisional, menguji efektivitas enkripsi DoH, serta menganalisis kemampuan IDS dalam mendeteksi permintaan DNS yang tidak terenkripsi. Selain itu, penelitian juga bertujuan memberikan gambaran nyata mengenai tantangan teknis yang mungkin muncul, seperti keterbatasan IDS dalam menganalisis lalu lintas terenkripsi atau kebutuhan optimasi rule deteksi.

Hasil penelitian diharapkan memberi manfaat baik secara teoretis maupun praktis. Secara akademik, penelitian ini memberikan kontribusi pada pengembangan ilmu keamanan jaringan dengan menyoroti penerapan Zero Trust pada level DNS. Secara praktis, hasil penelitian ini dapat menjadi acuan bagi administrator jaringan dalam merancang arsitektur yang lebih aman melalui integrasi DoH dan IDS. Selain itu, penelitian ini juga memberi kontribusi pada pengembangan keterampilan teknis, khususnya dalam penggunaan perangkat lunak terbuka seperti dnscrypt-proxy dan Snort, yang relevan untuk implementasi di lingkungan laboratorium maupun produksi. Lebih jauh lagi, penelitian ini dapat menjadi pijakan bagi studi lanjutan terkait keamanan DNS, pengembangan IDS berbasis kecerdasan buatan, atau perbandingan efektivitas berbagai protokol enkripsi DNS seperti DoH, DoT, dan DNSSEC.

METODE PENELITIAN

Metode penelitian merupakan kerangka penting dalam penyusunan karya ilmiah karena berfungsi sebagai panduan sistematis untuk memperoleh data, menganalisisnya, serta menarik kesimpulan yang valid. Menurut McLeod (2017), penelitian eksperimen merupakan salah satu metode yang paling relevan untuk menguji efektivitas sebuah sistem atau pendekatan baru dalam konteks teknologi informasi, karena memungkinkan peneliti untuk melakukan manipulasi terhadap variabel tertentu dan mengamati dampaknya secara langsung.

Penelitian ini menggunakan metode eksperimen, dengan mengimplementasikan pendekatan keamanan berbasis Zero Trust Security Model (ZTSM) melalui integrasi DNS-over-HTTPS (DoH) dan Intrusion Detection System (IDS) pada lingkungan jaringan virtual. Tujuan dari eksperimen ini adalah untuk menguji efektivitas kombinasi DoH dan IDS dalam mendeteksi serta memitigasi serangan DNS Spoofing. Secara umum, tahapan penelitian dibagi menjadi beberapa bagian: (1) pengumpulan data, (2) perancangan lingkungan uji, (3) implementasi konfigurasi, (4) pengujian dan evaluasi, serta (5) analisis data ditunjukkan pada gambar 1.



Gambar 1. Tahapan Penelitian

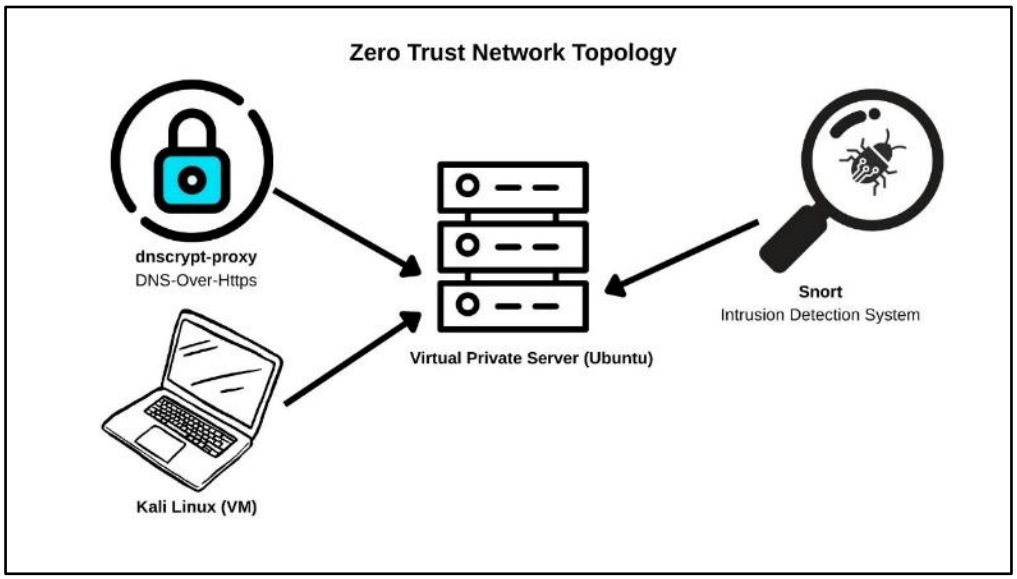
Pengumpulan Data

Tahap pertama adalah pengumpulan data berupa literatur dan studi terdahulu yang berkaitan dengan topik penelitian. Sumber data diambil dari jurnal internasional, standar keamanan seperti NIST SP 800-207 (Rose et al., 2020), serta dokumentasi perangkat lunak yang digunakan (dnscrypt-proxy dan Snort). Literatur yang dikaji meliputi:

- **Zero Trust Security Model (ZTSM)**: teori yang menolak adanya kepercayaan implisit pada jaringan, dengan prinsip *never trust, always verify*.
- **DNS Spoofing**: bentuk serangan yang mengeksploitasi kelemahan DNS tradisional tanpa enkripsi (Li, 2022).
- **DNS-over-HTTPS (DoH)**: teknologi enkripsi DNS yang meningkatkan privasi dan keamanan komunikasi (Kintis, 2020; Gonzalez, 2024).
- **Intrusion Detection System (IDS)**: sistem pemantauan jaringan yang mendeteksi pola lalu lintas mencurigakan (Bhuyan, 2019; Zhao, 2023).

Selain literatur, peneliti juga mengumpulkan data berupa contoh-contoh serangan spoofing, seperti **IP Spoofing, ARP Spoofing, MAC Spoofing, Email Spoofing, dan DNS Poisoning**. Contoh ini dijadikan acuan dalam merancang skenario uji serta menilai sejauh mana implementasi Zero Trust dapat memberikan perlindungan.

Perancangan Lingkungan Uji



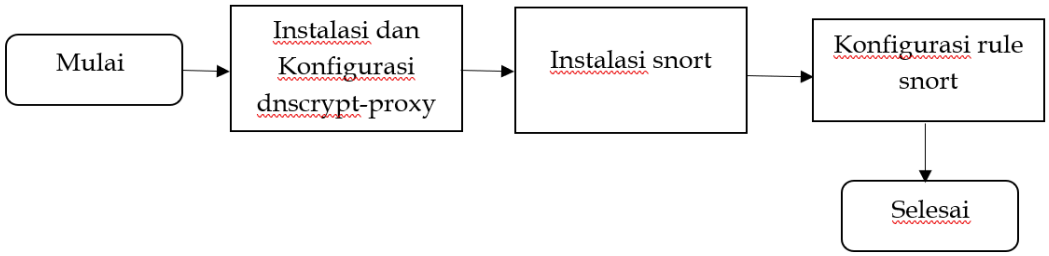
Gambar 2. Perancngan Penelitian

Lingkungan penelitian dirancang menggunakan dua sistem utama:

1. **VPS Ubuntu Server**
   - Menjalankan dnscrypt-proxy sebagai resolver DNS yang terenkripsi menggunakan DoH.
   - Menjalankan **Snort** sebagai IDS untuk memantau lalu lintas DNS.
   - Snort dikonfigurasi agar mendeteksi permintaan DNS yang mencurigakan melalui rule khusus.
2. **Kali Linux**
   - Berperan sebagai penyerang (*attacker*).
   - Digunakan untuk melakukan query DNS menggunakan perintah dig ke domain uji secure.test.
   - Mewakili skenario pengguna atau perangkat yang mencoba melakukan serangan manipulasi DNS.

Topologi jaringan dirancang sedemikian rupa sehingga Kali Linux dapat mengakses domain secure.test melalui VPS Ubuntu. Pada VPS, Snort memonitor interface **loopback (lo)** untuk menangkap lalu lintas DNS, termasuk percobaan serangan spoofing. Lingkungan ini dipilih karena sesuai dengan prinsip **Zero Trust** yang mengutamakan segmentasi mikro dan pemantauan berlapis.

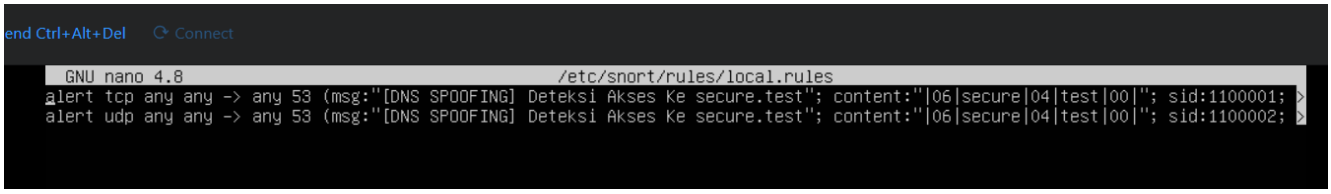
Implementasi Konfigurasi



Gambar 3. Tahapan Konfigurasi Penelitian

Tahap ini melibatkan penerapan teknis dari komponen-komponen sistem:

1. **Instalasi dan Konfigurasi dnscrypt-proxy**
   - Dnscrypt-proxy dipasang di VPS Ubuntu untuk mengenkripsi semua permintaan DNS dengan protokol HTTPS.
   - Konfigurasi file dnscrypt-proxy.toml dilakukan untuk memilih resolver yang mendukung DoH, memastikan seluruh permintaan DNS melewati jalur aman.
   - Pengujian awal dilakukan dengan perintah dig untuk memastikan tidak ada kebocoran DNS melalui port 53 tradisional.
2. **Instalasi dan Konfigurasi Snort**
   - Snort dipasang di VPS dan dijalankan pada interface lo.
   - Rule khusus ditambahkan untuk mendeteksi serangan DNS Spoofing, misalnya:



Pada gambar diatas rule yang tertulis adalah alert tcp any any -> any 53 (msg:"[DNS SPOOFING] Deteksi Akses Ke secure.test"; content:"|06|secure|04|test|00|"; sid:1000001; rev:1;) dan alert udp any any -> any 53 (msg:"[DNS SPOOFING] Deteksi Akses Ke secure.test"; content:"|06|secure|04|test|00|"; sid:1000001; rev:1;) digunakan untuk memantau permintaan DNS dan menghasilkan log saat lalu lintas mencurigakan terdeteksi.

HASIL DAN PEMBAHASAN

Setelah tahap implementasi konfigurasi selesai dilakukan, penelitian ini dilanjutkan dengan proses pengujian sistem untuk mengevaluasi efektivitas integrasi DNS-over-HTTPS (DoH) dan Intrusion Detection System (IDS) Snort dalam kerangka Zero Trust Security Model. Pengujian difokuskan pada kemampuan sistem dalam melindungi DNS dari serangan DNS Spoofing, baik dalam kondisi komunikasi terenkripsi maupun tidak terenkripsi. Proses pengujian dilakukan secara bertahap, dimulai dari aktivasi DoH untuk memastikan seluruh lalu lintas DNS telah dienkripsi, hingga simulasi serangan DNS Spoofing dengan menggunakan Kali Linux sebagai perangkat penyerang.

Pengujian ini dirancang untuk memberikan gambaran nyata mengenai bagaimana sistem bekerja dalam menghadapi skenario ancaman yang berbeda. Dengan menggunakan perintah dig terhadap domain uji secure.test, peneliti dapat memantau perilaku sistem ketika DoH aktif maupun nonaktif, sekaligus menilai kemampuan IDS Snort dalam mendeteksi lalu lintas DNS mencurigakan. Hasil pengujian kemudian dianalisis dengan memperhatikan perbedaan deteksi pada protokol Transmission Control Protocol (TCP) dan User Datagram Protocol (UDP), yang keduanya merupakan protokol utama dalam komunikasi DNS.

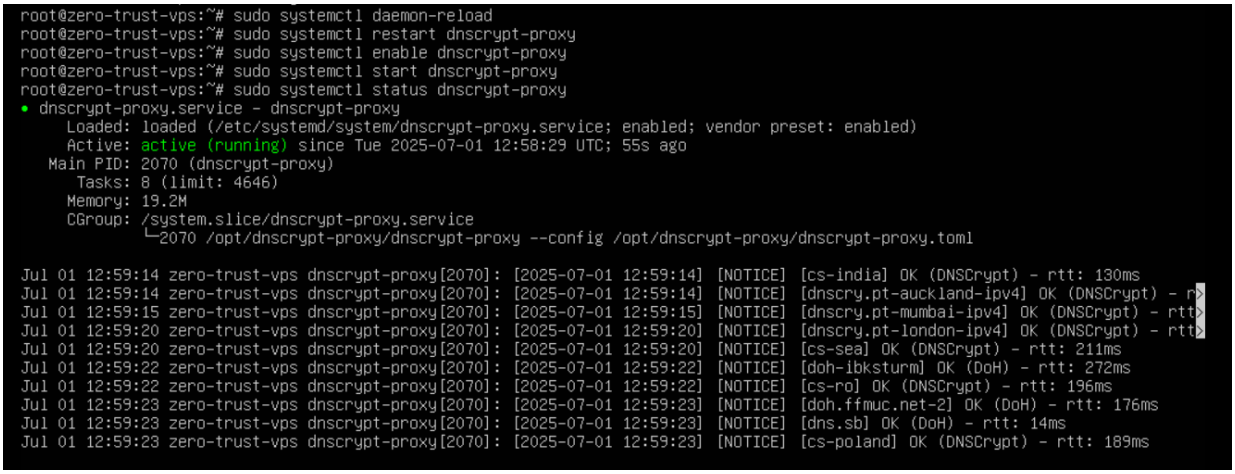
Pendekatan pengujian ini tidak hanya mengukur keberhasilan teknis dari implementasi DoH dan Snort, tetapi juga

bertujuan untuk menilai sejauh mana prinsip Zero Trust dapat diterapkan dalam konteks keamanan DNS. Prinsip never trust, always verify diuji secara praktis dengan menempatkan setiap query DNS dalam kondisi yang membutuhkan verifikasi tambahan, baik melalui enkripsi maupun monitoring oleh IDS. Dengan demikian, hasil penelitian ini diharapkan dapat menjawab pertanyaan penelitian terkait efektivitas enkripsi DoH, keterbatasan IDS dalam lalu lintas terenkripsi, serta tantangan teknis dalam penerapan Zero Trust pada sistem DNS.

Selain itu, pengujian dilakukan dengan mempertimbangkan kondisi nyata di lapangan, di mana sebagian besar komunikasi DNS masih menggunakan protokol UDP, sementara DoH hadir sebagai solusi modern untuk melindungi privasi dan keamanan pengguna. Oleh karena itu, evaluasi keberhasilan IDS dalam mendeteksi query DNS berbasis TCP maupun UDP menjadi penting, karena dapat memberikan gambaran praktis mengenai kelemahan dan keunggulan sistem yang dibangun. Dari hasil pengujian inilah pembahasan akan diarahkan untuk menganalisis kelebihan, kekurangan, serta implikasi yang muncul dalam penerapan Zero Trust pada perlindungan DNS.

Hasil Penelitian

Penelitian ini menghasilkan implementasi sistem keamanan DNS berbasis Zero Trust Security Model (ZTSM) dengan mengintegrasikan DNS-over-HTTPS (DoH) melalui aplikasi dnscrypt-proxy dan Intrusion Detection System (IDS) Snort. Lingkungan penelitian terdiri dari dua perangkat: VPS Ubuntu Server sebagai server target yang dilengkapi DoH dan IDS, serta Kali Linux sebagai penyerang yang melakukan query DNS terhadap domain uji secure.test.



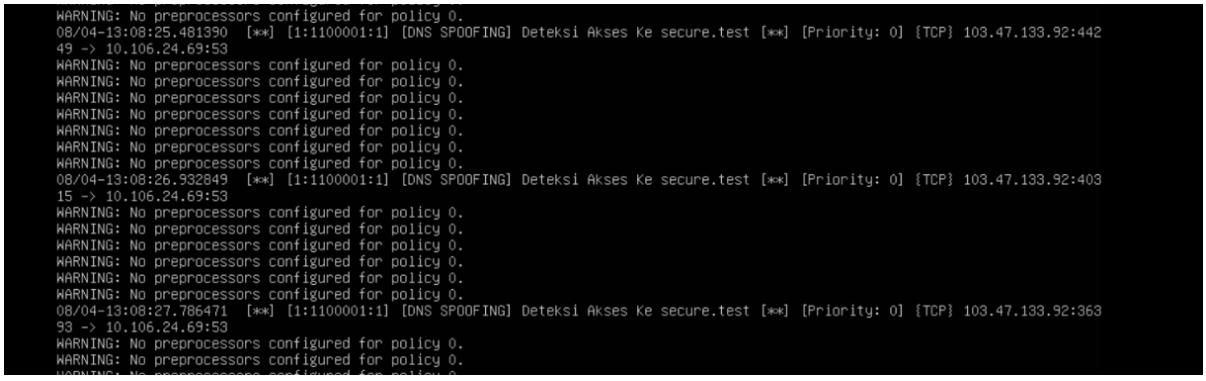
Dalam kondisi DoH aktif, hasil pengujian menunjukkan bahwa setiap permintaan DNS yang dikirim dari Kali Linux berhasil dijawab dengan benar oleh VPS. Namun, lalu lintas DNS tidak lagi terbaca pada port standar 53 karena telah dibungkus dalam protokol HTTPS (port 443). Dengan kondisi ini, Snort tidak menampilkan peringatan (alert) meskipun query dilakukan berulang kali. Hal ini mengindikasikan bahwa DoH bekerja sesuai fungsinya, yakni mengenkripsi resolusi DNS sehingga payload tidak dapat dianalisis atau dimanipulasi oleh pihak ketiga, termasuk IDS berbasis tanda tangan.

Tabel 1. Kondisi Jaringan Pengujian

Kondisi Jaringan	Protokol	Perintah Uji	Hasil Snort	Keterangan
DoH dinonaktifkan (DNS lewat port 53)	TCP	dig +tcp secure.test	Terdeteksi	Snort memicu alert, berhasil membaca pola string payload DNS. Rule khusus berfungsi efektif untuk mendeteksi potensi DNS Spoofing.
DoH dinonaktifkan (DNS lewat port 53)	UDP	dig secure.test	Tidak terdeteksi	Snort tidak memicu alert. Rule khusus belum menangkap pola payload DNS pada protokol UDP.

Ketika DoH dinonaktifkan, kondisi jaringan berubah. Query DNS kembali berjalan tanpa enkripsi melalui port 53. Pada kondisi ini, pengujian dilakukan dengan dua cara: menggunakan protokol TCP dan menggunakan protokol UDP. Hasil pengujian menunjukkan bahwa untuk protokol TCP, Snort berhasil mendeteksi adanya aktivitas mencurigakan. Setiap kali dilakukan query dig +tcp secure.test, Snort memicu peringatan yang menampilkan pesan adanya potensi serangan DNS Spoofing. Hal ini menandakan bahwa rule khusus yang dipasang pada Snort mampu bekerja secara efektif dalam membaca pola string pada payload DNS yang ditransmisikan menggunakan TCP.

Namun, hasil berbeda diperoleh pada pengujian menggunakan protokol UDP. Query DNS tetap dapat dijalankan menggunakan perintah standar dig secure.test, dan server memberikan respon normal. Akan tetapi, Snort tidak memicu alert meskipun rule khusus untuk UDP telah dipasang. Artinya, IDS gagal mengenali lalu lintas DNS berbasis UDP, padahal mayoritas komunikasi DNS di dunia nyata memanfaatkan UDP sebagai protokol utama. Kondisi ini memperlihatkan adanya keterbatasan IDS berbasis signature dalam memantau lalu lintas jaringan yang kompleks, terutama pada protokol tertentu.



Tabel 1. Kondisi Jaringan Pengujian

Temuan Penelitian	Deskripsi	Implikasi
Efektivitas DoH	Payload DNS berhasil disembunyikan melalui enkripsi DoH sehingga tidak dapat dibaca atau dimanipulasi.	DoH memberikan perlindungan kuat terhadap serangan manipulasi DNS.
Deteksi Snort pada TCP	Snort berhasil mendeteksi query DNS mencurigakan ketika DoH tidak digunakan dengan protokol TCP.	IDS memberikan lapisan deteksi tambahan untuk lalu lintas DNS berbasis TCP.
Keterbatasan Snort pada UDP	Snort gagal mendeteksi query DNS melalui protokol UDP meskipun lalu lintas tidak terenkripsi.	Efektivitas IDS terbatas, perlu penguatan rule khusus untuk UDP.

Secara keseluruhan, hasil penelitian menunjukkan tiga temuan penting. Pertama, DoH terbukti efektif menyembunyikan payload DNS sehingga lalu lintas terenkripsi tidak dapat dibaca atau dimanipulasi. Kedua, IDS Snort mampu mendeteksi query DNS mencurigakan pada protokol TCP ketika DoH tidak digunakan, sehingga dapat memberikan lapisan deteksi tambahan. Ketiga, IDS gagal mendeteksi query DNS pada protokol UDP meskipun lalu lintas tidak terenkripsi, yang berarti efektivitas IDS terbatas pada protokol tertentu.

Pembahasan

Hasil penelitian memberikan gambaran nyata mengenai peran DoH dan IDS dalam kerangka Zero Trust Security Model. Pada kondisi DoH aktif, komunikasi DNS terenkripsi sepenuhnya, sehingga serangan DNS Spoofing tidak mungkin dilakukan karena paket DNS tidak dapat diubah selama proses transmisi. Temuan ini konsisten dengan penelitian Kintis (2020) yang menyatakan bahwa DoH meningkatkan keamanan resolusi DNS dengan menyediakan kerahasiaan (confidentiality) dan integritas (integrity) komunikasi. Gonzalez (2024) juga menegaskan bahwa DoH memperkuat privasi pengguna karena query DNS tidak lagi dapat diakses oleh pihak ketiga di jalur transmisi. Dalam kerangka Zero Trust, kondisi ini mewakili prinsip dasar assume breach, di mana enkripsi memastikan bahwa komunikasi tetap aman meskipun jalur transmisi diasumsikan tidak dapat dipercaya.

Sementara itu, IDS Snort memperlihatkan kinerjanya pada komunikasi tidak terenkripsi. Ketika DoH nonaktif dan query DNS dilakukan melalui protokol TCP, IDS dapat mengenali pola string domain secure.test dan memberikan peringatan. Temuan ini sesuai dengan teori Bhuyan (2019) bahwa IDS berbasis tanda tangan mampu mendeteksi serangan dengan cepat apabila pola serangan sudah diketahui sebelumnya. Dengan demikian, Snort tetap relevan sebagai alat deteksi intrusi yang dapat berfungsi sebagai lapisan pertahanan tambahan.

Namun, kelemahan nyata terlihat ketika komunikasi dilakukan melalui protokol UDP. IDS gagal mendeteksi query DNS meskipun rule untuk UDP telah ditambahkan. Temuan ini menunjukkan keterbatasan IDS signature-based yang sejalan dengan pandangan Lu (2019) bahwa IDS jenis ini tidak fleksibel dalam menghadapi variasi serangan baru maupun protokol tertentu. Fakta bahwa mayoritas lalu lintas DNS di internet menggunakan UDP memperlihatkan bahwa kelemahan ini sangat signifikan, dan menjadi salah satu faktor yang harus diperhatikan dalam pengembangan sistem deteksi ke depan.

Dari perspektif Zero Trust Security Model, kombinasi DoH dan IDS dapat dipandang sebagai mekanisme yang saling melengkapi. DoH bertindak sebagai lapisan preventif dengan mengenkripsi komunikasi DNS, sementara IDS berfungsi sebagai lapisan deteksi yang memberikan peringatan ketika terjadi aktivitas mencurigakan pada komunikasi yang tidak terlindungi. Prinsip never trust, always verify tercermin dalam cara kerja kedua komponen ini, di mana sistem tidak serta merta mempercayai lalu lintas jaringan, tetapi tetap melakukan verifikasi dan monitoring.

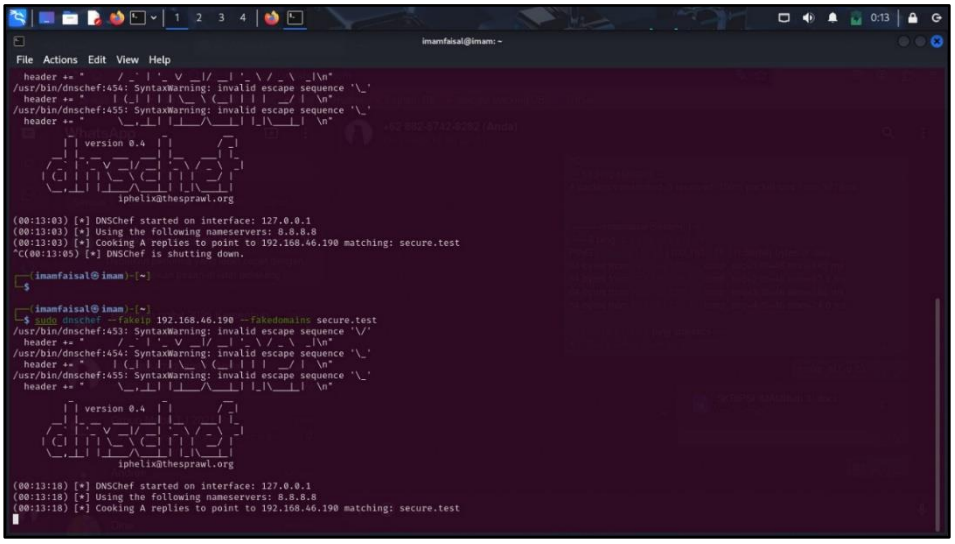
Meski demikian, hasil penelitian ini juga memperlihatkan adanya trade-off antara privasi dan monitoring. Enkripsi DoH memberikan perlindungan tinggi, namun pada saat yang sama membatasi kemampuan IDS dalam memantau isi komunikasi. Sebaliknya, ketika komunikasi tidak terenkripsi, IDS dapat melakukan deteksi, tetapi lalu lintas DNS kembali terbuka terhadap risiko manipulasi. Trade-off ini menegaskan bahwa tidak ada satu solusi tunggal yang mampu menjawab seluruh permasalahan keamanan jaringan. Pendekatan Zero Trust menjadi relevan karena menekankan keamanan berlapis (defense in depth) dan verifikasi berkelanjutan.

Implikasi praktis dari penelitian ini adalah bahwa organisasi sebaiknya menerapkan DoH sebagai standar keamanan DNS untuk memastikan privasi dan integritas resolusi. Namun, penggunaan IDS tetap diperlukan untuk memberikan lapisan deteksi tambahan, khususnya pada lalu lintas yang tidak terenkripsi. Agar lebih efektif, IDS perlu ditingkatkan dengan metode berbasis anomaly detection atau machine learning (Zhao, 2023), sehingga sistem mampu mengenali pola lalu lintas abnormal tanpa harus mengandalkan tanda tangan yang eksplisit. Selain itu, integrasi IDS dengan sistem Security Information and Event Management (SIEM) atau pemanfaatan teknik TLS fingerprinting dapat menjadi alternatif solusi untuk meningkatkan visibilitas pada lalu lintas terenkripsi.

Untuk mendukung pemahaman terhadap skenario DNS Spoofing, ditambahkan juga contoh visualisasi sebelum diserang seperti gambar dibawah ini, dan sesudah dari serangan menggunakan tool dnschef. Meskipun serangan ini tidak dapat dijalankan secara langsung dalam VPS karena keterbatasan hak akses dan konflik port, tool ini digunakan pada

sistem lokal untuk memperlihatkan bagaimana domain secure.test dapat diarahkan ke IP palsu.

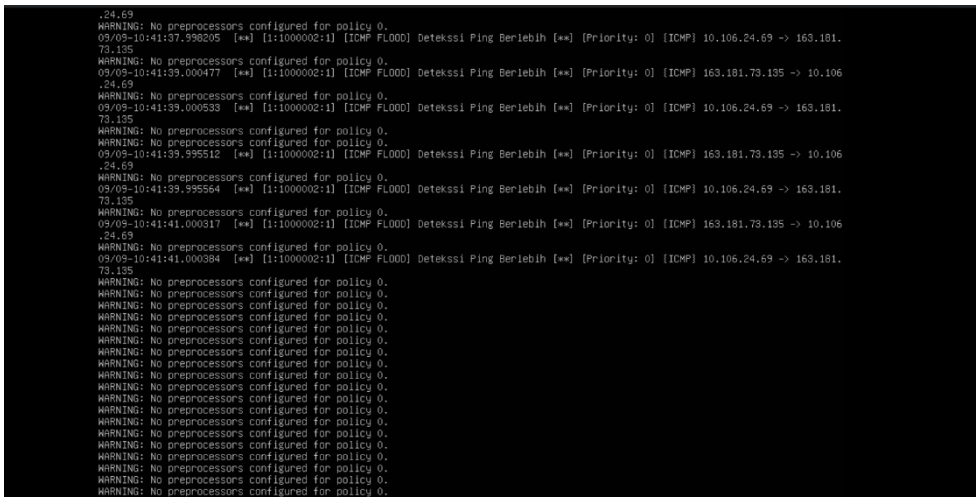
Dalam simulasi pada gambar berikut, saat pengguna mengakses secure.test melalui browser, halaman yang muncul bukanlah konten sebenarnya, melainkan tampilan palsu yang disiapkan oleh dnschef.



Visualisasi pada gambar dibawah ini menegaskan bahwa tanpa penerapan enkripsi DNS dan sistem deteksi intrusi, lalu lintas DNS sangat rentan dimanipulasi. Oleh karena itu, integrasi DoH dan IDS dalam kerangka Zero Trust terbukti mampu memberikan perlindungan yang lebih kuat dan adaptif dalam menghadapi ancaman DNS Spoofing, meskipun implementasinya tetap membutuhkan penyempurnaan terutama dalam hal deteksi protokol UDP dan segmentasi jaringan.

Sebagai pengujian tambahan, dilakukan simulasi serangan berupa ICMP Flood dengan tujuan untuk menguji kemampuan Snort dalam mendeteksi lalu lintas ICMP berlebihan. Rule Snort yang digunakan yakni “alert icmp any any -> any any (msg:"[ICMP FLOOD] Deteksi Ping Berlebih"; sid:1000002; rev:1;)”.

Rule ini berfungsi untuk memberikan peringatan apabila terdapat trafik ICMP yang masuk atau keluar secara intensif, yang biasanya menjadi indikasi dari serangan Denial of Service (DoS) berbasis ping. Serangan kemudian dijalankan dari Kali Linux menggunakan perintah “ping -f -s 65500 (target_ip)”. Perintah ini mengirimkan paket ICMP dengan ukuran sangat besar secara terus-menerus ke alamat IP server target yang dipasang Snort.



Berdasarkan gambar diatas, Snort berhasil memunculkan alert dengan pesan "[ICMP FLOOD] Deteksi Ping Berlebih", yang menandakan bahwa lalu lintas ICMP berlebihan berhasil dikenali. Alert yang muncul menunjukkan adanya komunikasi ICMP dari alamat sumber 10.106.24.69 menuju alamat tujuan 163.181.73.135 dan sebaliknya.

Dengan demikian, pembahasan ini menegaskan bahwa penerapan Zero Trust melalui integrasi DoH dan IDS memang mampu meningkatkan ketahanan DNS terhadap serangan spoofing, meskipun efektivitas IDS masih terbatas. Penelitian ini membuktikan bahwa kombinasi mekanisme preventif dan deteksi tetap lebih kuat dibandingkan hanya mengandalkan satu lapisan keamanan saja, dan membuka peluang penelitian lanjutan untuk mengoptimalkan monitoring pada protokol UDP maupun komunikasi terenkripsi.

KESIMPULAN

Berdasarkan hasil kajian teori, implementasi sistem, serta analisis data yang dilakukan, dapat disimpulkan bahwa pendekatan Zero Trust Security Model (ZTSM) efektif dalam meningkatkan keamanan sistem Domain Name System (DNS) terhadap serangan DNS Spoofing. Integrasi antara DNS-over-HTTPS (DoH) dan Intrusion Detection System (IDS) Snort memberikan perlindungan berlapis yang dapat mendeteksi dan memitigasi ancaman terhadap komunikasi DNS secara lebih adaptif dan kontekstual.

Berdasarkan hasil pengujian, ketika DoH aktif melalui dnscrypt-proxy, seluruh permintaan DNS berhasil dienkripsi dan tidak dapat dibaca dalam bentuk plaintext. Pada kondisi ini, sistem IDS tidak mendeteksi adanya lalu lintas mencurigakan, dengan nilai deteksi sebesar 0% dan tidak terdeteksi sebesar 100%, yang menunjukkan bahwa komunikasi DNS telah sepenuhnya diamankan. Sebaliknya, saat dnscrypt-proxy dinonaktifkan, lalu lintas DNS kembali menggunakan protokol biasa. Pada protokol TCP, Snort mampu mendeteksi seluruh permintaan DNS sebagai anomali dengan tingkat keberhasilan deteksi mencapai 100%, tanpa adanya permintaan yang lolos dari pemantauan (0% tidak terdeteksi). Namun, pada protokol UDP, Snort tidak berhasil memicu peringatan sehingga tingkat deteksi hanya 0%, sementara lalu lintas yang tidak terdeteksi mencapai 100%. Hal ini mengindikasikan bahwa efektivitas IDS Snort dalam mendeteksi lalu lintas DNS plaintext masih terbatas, terutama pada protokol UDP, sehingga diperlukan penguatan rule dan aspek pemantauan untuk meningkatkan cakupan deteksi pada berbagai variasi protokol.

Selain itu, simulasi konseptual menggunakan dnschef sebagai ilustrasi serangan DNS Spoofing membuktikan bahwa tanpa enkripsi dan pemantauan aktif, pengguna dapat dengan mudah diarahkan ke situs palsu. Hal ini memperkuat urgensi penerapan prinsip "never trust, always verify" dalam arsitektur keamanan DNS.

Dengan demikian, implementasi ZTSM melalui kombinasi DoH dan IDS dapat menjadi solusi strategis untuk mengurangi risiko manipulasi DNS. Namun, keberhasilannya bergantung pada konfigurasi yang tepat, monitoring menyeluruh, serta evaluasi berkelanjutan terhadap potensi celah yang masih tersisa dalam sistem.

REFERENSI

Kindervag, J. (2010). No More Chewy Centers: Introducing the Zero Trust Model of Information Security. Forrester Research.

Kintis, K., Antonakakis, M., & Dagon, D. (2020). Evaluating the Efficacy of DNS-over-HTTPS for Secure DNS Resolution. Journal of Cybersecurity, 6(2), 45-58.Galley. K. E. (Ed.). (2004). *Global climate change and wildlife in North America.* Bethesda, MD: Wildlife Society.

McLeod, S. (2017). Experimental Method. Simply Psychology. Retrieved from https://www.simplypsychology.org/experimental-method.html

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture (NIST Special Publication 800-207). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207

Li, Y. (2022). Enhancing DNS Security Against Spoofing Attacks Using Encrypted Protocols. Journal of Network and Computer Applications, 200, 103300.

Gonzalez, R., Patel, S., & Lee, T. (2024). *Enhancing DNS Security with DNS-over-HTTPS: Performance and Privacy Considerations*. *IEEE Transactions on Network and Service Management*.

Bhuyan, M. H., Bhattacharyya, D. K., & Kalita, J. K. (2019). Network Anomaly Detection: Methods, Systems and Tools. Springer.

Zhao, X., Liu, Y., & Chen, W. (2023). Machine Learning-based IDS for DNS Spoofing Detection. IEEE Transactions on Dependable and Secure Computing.

Yao, H., Gao, P., Zhang, P., Wang, J., Jiang, C., & Lu, L. (2019). Hybrid Intrusion Detection System for Edge-Based IIoT Relying on Machine-Learning-Aided Detection. IEEE Network, 33(5), 75-81. https://doi.org/10.1109/MNET.001.1800479.