Penerapan *DNS Over HTTPS* dan *Arp Spoofing* Dalam Meningkatkan Keamanan Jaringan Cafe Kome Katamso

[1]Muhammad Fauzi Pulungan, [2]Wirda fitriani
[12]Program Prodi Sistem Komputer, Universitas Pembangunan Panca Budi, Medan, Indonesia
[1]Fauziipulungan21@gmail.com, [2] wirda@pancabudi.ac.id

Abstract - This research aims to improve computer network security in a cafe environment by implementing the DNS over HTTPS (DoH) method and overcoming the ARP Spoofing problem. In today's digital era, network security is a significant challenge, given risks such as data theft and intrusions that can harm users without their knowledge. Public internet networks, including those in cafe environments, are often the target of attacks that threaten data integrity, such as ARP Spoofing which manipulates ARP tables to damage network communications. This research focuses on the implementation of DoH, which encrypts DNS requests to protect user information from unauthorized interception and manipulation. DoH implementation aims to strengthen the security of DNS communications by securing data sent between computers and DNS servers, as well as reducing vulnerability to man in the middle (MITM) attacks and other spoofing. In addition, this research also evaluates and offers ARP Spoofing detection solutions to strengthen network protection from these attacks. The research method involves simulating the network topology at the Kome Katamso Medan cafe, using hardware such as a Compaq CQ40 Laptop and LAN Card, as well as software such as Ettercap-NG-0.7.3 for packet sniffing and Netstumbler for wifi monitoring. The results of the DoH implementation show a significant improvement in the security of communications between computers and DNS servers, as well as an increase in website access speed. Encryption implemented by DoH has proven effective in reducing vulnerability to MITM attacks and other spoofing, as well as ensuring that only users and DNS servers can access DNS information. This research also shows that implementing DoH and ARP Spoofing detection solutions significantly improves network security in cafe environments, providing additional protection against attacks that can compromise data integrity. These efforts are critical to creating a safer network environment for users in public spaces, making their internet experience more secure and efficient.

Keywords — ***DNS over HTTPS, ARP Spoofing, Network Security, Data Protection***

Abstrak— Penelitian ini bertujuan untuk meningkatkan keamanan jaringan komputer di lingkungan kafe dengan menerapkan metode DNS over HTTPS (DoH) dan mengatasi masalah ARP Spoofing. Di era digital saat ini, keamanan jaringan menjadi tantangan signifikan, mengingat risiko seperti pencurian data dan gangguan yang dapat merugikan pengguna tanpa sepengetahuan mereka. Jaringan internet publik, termasuk yang ada di lingkungan kafe, sering kali menjadi target serangan yang mengancam integritas data, seperti ARP Spoofing yang memanipulasi tabel ARP untuk merusak komunikasi jaringan. Penelitian ini berfokus pada penerapan DoH, yang mengenkripsi permintaan DNS untuk melindungi informasi pengguna dari penyadapan dan manipulasi pihak tidak berwenang. Implementasi DoH bertujuan untuk memperkuat keamanan komunikasi DNS dengan mengamankan data yang dikirimkan antara komputer dan server DNS, serta mengurangi kerentanan terhadap serangan man in the middle (MITM) dan spoofing lainnya. Selain itu, penelitian ini juga mengevaluasi dan menawarkan solusi deteksi ARP Spoofing untuk memperkuat perlindungan jaringan dari serangan tersebut. Metode penelitian melibatkan simulasi topologi jaringan di kafe Kome Katamso Medan, menggunakan perangkat keras seperti Laptop Compaq CQ40 dan LAN Card, serta perangkat lunak seperti Ettercap-NG-0.7.3 untuk sniffing paket dan Netstumbler untuk pemantauan wifi. Hasil implementasi DoH menunjukkan peningkatan signifikan dalam keamanan komunikasi antara komputer dan server DNS, serta peningkatan kecepatan akses situs web. Enkripsi yang diterapkan oleh DoH terbukti efektif dalam mengurangi kerentanan terhadap serangan MITM dan spoofing lainnya, serta memastikan bahwa hanya pengguna dan server DNS yang dapat mengakses informasi DNS. Penelitian ini juga menunjukkan bahwa penerapan DoH dan solusi deteksi ARP Spoofing secara signifikan meningkatkan keamanan jaringan di lingkungan kafe, memberikan perlindungan tambahan terhadap serangan yang dapat merusak integritas data. Upaya ini sangat penting untuk menciptakan lingkungan jaringan yang lebih aman bagi pengguna di ruang publik, menjadikan pengalaman internet mereka lebih aman dan efisien.

Kata Kunci— DNS over HTTPS, ARP Spoofing, Keamanan Jaringan, Perlindungan Data.

I. Pendahuluan

Perkembangan Teknologi jaringan komputer telah mengalami perkembangan yang pesat, dan evolusinya tidak terlepas dari sejarah yang telah melatarbelakangi perkembangannya dari waktu ke waktu. Dalam kaitannya, komputer yang terhubung dapat menggunakan berbagai teknologi transmisi seperti media kabel, saluran telepon, gelombang radio, satelit, atau sinar inframerah [1]. Untuk mendukung fungsi jaringan, berbagai komponen peralatan dan perangkat keras jaringan komputer serta konfigurasi perlu diterapkan agar jaringan tersebut dapat digunakan secara efektif. Perkembangan jaringan komputer membawa berbagai keuntungan dalam mempermudah pekerjaan manusia. Namun, keberadaan teknologi ini juga membawa aspek negatif, seperti kejahatan komputer yang mencakup pencurian data dan interupsi komputer tanpa sepengetahuan pengguna [2]. Hal ini dapat menyebabkan kerugian bagi pemilik informasi, ketika informasi tersebut jatuh ke tangan pihak yang tidak berwenang.

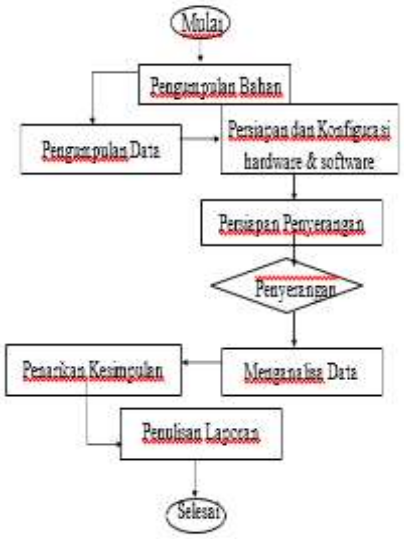
Secara umum, jaringan komputer internet yang bersifat publik dan global dianggap tidak aman. Saat data dikirimkan dari satu komputer ke komputer lainnya, data tersebut melewati beberapa komputer lain, memberikan peluang bagi pengguna internet lainnya untuk menyadap atau

mengubah data tersebut. Oleh karena itu, perlu dilakukan upaya untuk meningkatkan keamanan jaringan, terutama dalam menghadapi masalah seperti ARP Spoofing. ARP Spoofing, yang melibatkan manipulasi tabel ARP dalam jaringan, dapat membahayakan keamanan jaringan [3]. Oleh karena itu, penelitian ini bertujuan untuk meningkatkan keamanan jaringan di Café dengan menerapkan metode DNS over HTTPS (DoH) dan mengatasi masalah ARP Spoofing. ARP Spoofing dapat memalsukan MAC Address router atau proxy, mengecoh komputer intranet untuk melewati komputer penyerang, dan meneruskan akses router tersebut secara transparan [4].

Implementasi DoH menjadi fokus utama penelitian ini. DoH adalah metode enkripsi yang memastikan permintaan DNS dari perangkat klien ke server DNS tidak dapat disadap oleh pihak yang tidak berwenang. Dengan menerapkan DoH, Café dapat meningkatkan keamanan jaringan mereka dan melindungi informasi pelanggan dari potensi ancaman. Selain itu, penelitian ini juga mengevaluasi risiko ARP Spoofing dan memberikan solusi berupa penerapan teknologi deteksi ARP Spoofing untuk memberikan peringatan atau tindakan otomatis dalam menghadapi aktivitas mencurigakan dalam tabel ARP jaringan. Di lingkungan Cafe, akan diterapkan teknologi DNS over HTTPS (DoH) [5]. Ini penting karena DoH mengenkripsi permintaan DNS dari perangkat pelanggan ke server DNS, menjaga informasi DNS tetap rahasia dan aman dari penyadapan atau manipulasi oleh pihak yang tidak berwenang. Implementasi DoH bertujuan untuk meningkatkan keamanan jaringan Cafe dengan melindungi informasi sensitif pelanggan, seperti situs web yang dikunjungi, dari kemungkinan serangan atau pencurian data [6].

II. Metode Penelitian

A. Metode

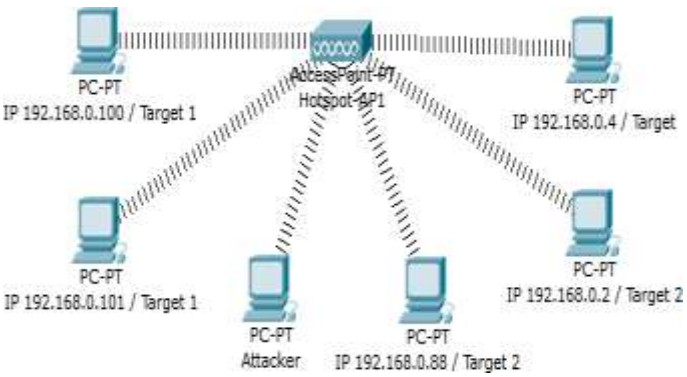


Gambar 1. Diagram Alir Penelitian.

Diagram alir penelitian dilakukan dalam beberapa tahapan. Menyiapkan literatur jurnal untuk menunjang penelitian. (2) Perizinan penelitian pihak cafe kome katamso medan,(3) Data-data yang ada, konfigurasi jaringan kabel LAN dan wifi yang terpasang di lingkup cafe kome katamso meliputi tempat, SSID, BSSID, enkripsi yang digunakan,di channel. (4) Menyiapkan hardware dan software yang dibutuhkan untuk menunjang pelaksanaan penelitian. (5) Percobaan penyerangan kepada jaringan kabel LAN dan wifi untuk mendapatkan informasi tentang keama-nannya. (6) Menarik kesimpulan untuk memutuskan sebuah saran yang bisa digunakan untuk mengamankan jaringan kabel LAN dan wifi melihat dari sisi pengguna [7].

B. Packet Sniffing

Percobaan ini bertujuan untuk mengumpulkan informasi penting seperti username, password, dan akses DNS, yang memungkinkan akses internet tidak sah. Hasilnya, penulis berhasil mendapatkan akses DNS serta username dan password email dari target, menunjukkan bahwa jaringan tidak aman karena informasi mudah dicuri.



Gambar 2. Tampilan simulasi penyerangan.

Gambar di atas menunjukkan skenario serangan di mana attacker membagi target menjadi dua kelompok: target 1 dan target 2. Jika target 1 tidak aktif, serangan berpindah ke target 2, dan sebaliknya, sehingga attacker dapat merekam semua aktivitas. Karena tidak ada aktivitas akses akun selama jam kerja, penulis melakukan dua skenario. Skenario pertama meliputi (1) Membuat akun dan password baru, (2) Mencoba login menggunakan komputer cafe , (3) Merekam aktivitas dengan software Ettercap [6].

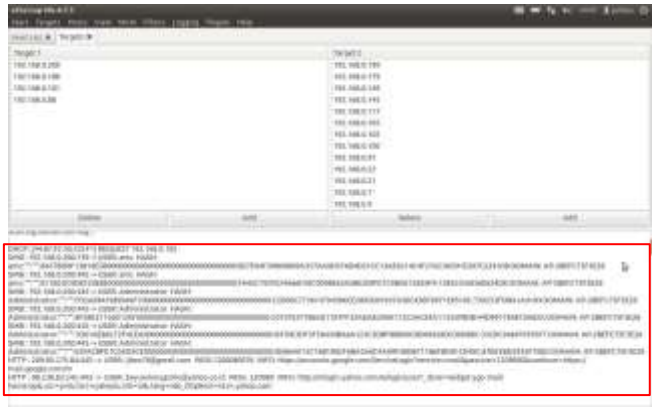
III. Hasil dan Pembahasan

Analisis keamanan jaringan perlu dilakukan untuk mengevaluasi seberapa aman sebuah jaringan kabel atau wireless. Keamanan tidak hanya bergantung pada hardware dan software, tetapi juga pada konfigurasi oleh pengguna dan desain jaringan. Di Cafe Kome Katamso Medan, keamanan jaringan masih perlu ditingkatkan, seperti penggunaan WiFi yang

terbuka (tanpa keamanan) dan banyak pegawai yang belum memahami keamanan jaringan komputer. Percobaan ini bertujuan untuk mengidentifikasi WiFi dengan informasi lengkap seperti SSID, alamat MAC, RSSI, vendor, channel, tipe jaringan, dan tingkat keamanan [8]. Tujuannya adalah untuk mempermudah penyerangan dengan mengakses jaringan WiFi yang ada. Hasil percobaan menunjukkan bahwa WiFi di area cafe tidak memiliki keamanan atau bersifat terbuka [9].

Gambar 3. Hasil penyerangan Packet Sniffing pada wifi.

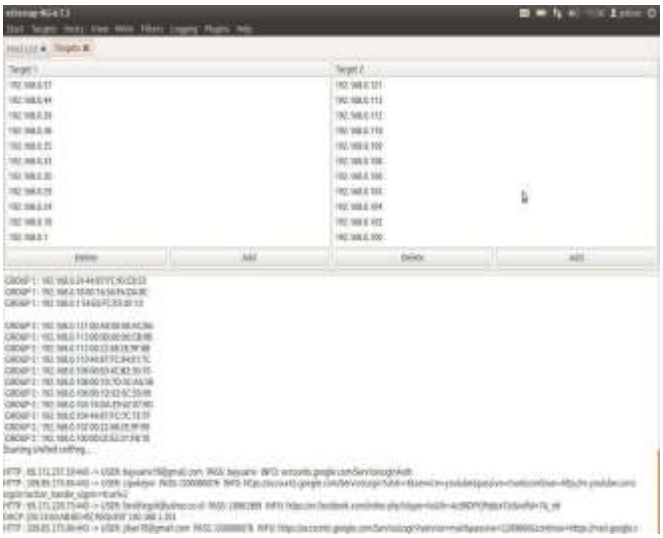
Gambar 3. Baris 1- 4 menunjukkan komunikasi otomatis antar komputer dalam satu jaringan (ACK). Baris terakhir menunjukkan bahwa salah satu komputer klien mengakses akun Gmail dengan username "bayuarie76@gmail.com" dan password "l200080076". Gambar 4. Di bawah ini menunjukkan bahwa baris 1-13 menampilkan file sharing antara server dan klien yang terenkripsi, sehingga tidak dapat dideskripsikan [10]. Baris 14 - 17 menunjukkan dua klien yang login ke akun gmail.



Gambar 4. Hasil penyerangan Packet Sniffing

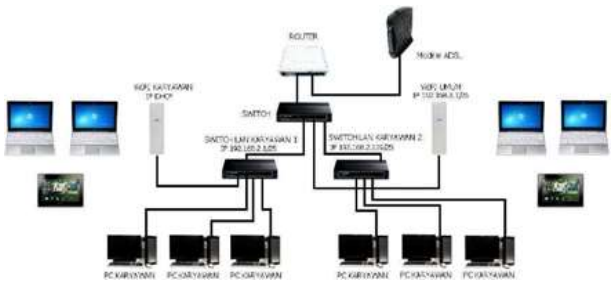
Gambar 5. Di bawah ini menunjukkan bahwa akun dengan password yang diubah dan beberapa akun acak dapat direkam.

Analisis mengungkapkan alasan mengapa WiFi di Cafe Kome Katamso Medan tidak dilindungi, menurut pihak pengelola Cafe Kome Katamso (1) WiFi di cafe disediakan untuk pengunjung dan pengguna layanan penerbangan agar dapat mengakses internet secara gratis sambil menunggu. (2) WiFi yang ada adalah utama dan mudah dikonfig-urasi jika diperlukan tambahan di masa depan. Secara umum, WiFi ini tidak dilindungi (seperti WEP, WPA, WPA2) karena ditujukan untuk fasilitas publik, bukan untuk keperluan komersial [11].



Gambar 5. Hasil penyerangan Packet Sniffing jaringan baru

Setelah penelitian, penulis merekomendasikan beberapa solusi untuk meningkatkan keamanan jaringan di Cafe Kome Katamso, antara lain: 1. Pisahkan jaringan WiFi/LAN cafe dari WiFi fasilitas pengguna layanan untuk mencegah serangan Packet Sniffing. Solusi teknisnya termasuk mengatur subnetting seperti IP 192.168.2.1/25 untuk LAN karyawan1, IP 192.168.2.129/25 untuk LAN karyawan2, dan IP 192.168.3.1/26 untuk WiFi umum [12].



Gambar 6. Perbedaan jaringan internet untuk cafe dan umum.

Gambar 6. Diatas menunjukkan bahwa memisahkan IP jaringan mencegah serangan Packet Sniffing masuk ke jaringan lain karena serangan ini beroperasi di layer 2. Metode

lain adalah binding IP dan MAC Address untuk melawan ARP Spoofing dengan mendaftarkan setiap pengguna di gateway, sehingga paket dikirim dengan benar [13]. Selain itu, gunakan enkripsi WPA2-PSK dan Radius untuk mengamankan WiFi cafe, membatasi jangkauan sinyal dan memastikan hanya karyawan yang mengetahui aksesnya. Solusi Alternative Untuk Mencegah Serangan Packet Sniffing Bagi Pengguna Linux (Sebagai Client dan Server) [14].

Untuk mencegah ARP Spoofing, ubah ARP table dari dynamic menjadi static dan pastikan static ARP table diterapkan pada client dan gateway [15]. Gunakan ArpOn untuk melawan spoofing dengan langkah-langkah berikut (1) Instal ArpOn dengan perintah: $ sudo apt-get install arpon, (2) Konfigurasi ArpOn dengan mengedit file /etc/default/arpon, (3) simpan file dengan CTRL + O dan keluar CTRL + X, (4) Restart Arpon dengan $ sudo / ets, (5) jalankan Arpon dengan perintah $ audo arpon [16].

IV. Kesimpulan

Berdasarkan hasil penelitian, dapat disimpulkan sebagai berikut:

1. Penulis berhasil mengimplementasikan DNS Over HTTPS (DoH) pada router MikroTik.

2. Setelah konfigurasi DoH berhasil, penulis melakukan pengujian dan DoH berfungsi dengan baik.

3. DNS Over HTTPS mengenkripsi seluruh komunikasi antara komputer dan server DNS, sehingga meningkatkan keamanan dan mengurangi risiko serangan man-in-the-middle (MITM) serta spoofing lainnya.

4. Keuntungan utama dari DNS Over HTTPS adalah tingkat keamanan yang tinggi. Hanya pengguna dan server DNS yang dapat melihat tujuan akses, yang efektif untuk menghindari serangan berbasis DNS.

5. Selain meningkatkan keamanan, DNS Over HTTPS juga dapat mempercepat akses ke beberapa situs web dan menggantikan DNS dari ISP.

V. Daftar Pustaka

[1] M. Pederson, N. Fitria, R. Elinda Sari, and Z. Yanti, "Implementasi DNS Server pada Sistem Operasi Ubuntu Menggunakan VirtualBox," *J. Netw. Comput.*, vol. 2, no. 2, pp. 52–62, 2023, [Online]. Available: https://jurnal.netplg.com/.

[2] S. Anwar, S. A. Karimah, and ..., "Deteksi ARP Spoofing pada Jaringan Wireless Menggunakan Metode String Matching dengan Algoritma Boyer Moore dan Brute Force," *eProceedings …*, vol. 10, no. 3, pp. 3450–3454, 2023, [Online]. Available: https://openlibrarypublications.telkomuniversity.ac.id/index.php/engineering/article/view/20614.

[3] A. Arini, M. Luthfi Arsalan, and H. Teja Sukmana, "Keamanan Jaringan Wi-Fi Terhadap Serangan Packet Sniffing Menggunakan Firewall Rule (Studi Kasus : Pt. Akurat.Co)," *Cyber Secur. dan Forensik Digit.*, vol. 6, no. 2, pp. 30–38, 2024, doi: 10.14421/csecurity.2023.6.2.4075.

[4] K. Zonggonau and H. Sajati, "Membangun Sistem Keamanan Arp Spoofing Memanfaatkan Arpwatch Dan Addons Firefox," *Compiler*, vol. 4, no. 1, pp. 49–58, 2015, doi: 10.28989/compiler.v4i1.87.

[5] Y. Winawang, "Implementasi Keamanan Jalur Internet Menggunakan IP Tunneling pada OpenVPN Access Server dengan Protokol OpenVPN dan Protokol DNS Over HTTPS," *J. Syntax Admiration*, vol. 2, no. 4, pp. 712–730, 2021, doi: 10.46799/jsa.v2i4.207.

[6] A. Tedyyana and R. Kurniati, "Membuat Web Server Menggunakan Dinamic Domain Name System Pada IP Dinamis," *J. Teknol. Inf. Komun. Digit. Zo.*, vol. 7, no. 1, pp. 1–10, 2016.

[7] L. O. Sari, E. Safrianti, and D. Wahyuningtias, "Analisis Keamanan Jaringan Berbasis Point to Point Protocol Over Ethernet (PPPoE) Menggunakan Mikrotik," *MALCOM Indones. J. Mach. Learn. Comput. Sci.*, vol. 4, no. 3, pp. 943–954, 2024, doi: 10.57152/malcom.v4i3.1301.

[8] A. A. Zabar and F. Novianto, "Keamanan Http Dan Https Berbasis Web Menggunakan Sistem Operasi Kali Linux," *Komputa J. Ilm. Komput. dan Inform.*, vol. 4, no. 2, pp. 69–74, 2015, doi: 10.34010/komputa.v4i2.2427.

[9] O. Abdurahman and T. Umi Kalsum, "Penerapan PI HOLE DNS Server Sebagai ADS-Blocker Dan Sistem Filtering Website Pada Jaringan Hotspot," *J. Media Infotama*, vol. 18, no. 2, p. 341139, 2022.

[10] R. A. Ramadhan, A. T. Tira, and M. R. Fadhilah, "Network Forensic: Analysis of Client Attack and Quality of Service Measurement by ARP Poisoning using Network Forensic Generic Process (NFGP) Model," *Sistemasi*, vol. 13, no. 2, p. 713, 2024, doi: 10.32520/stmsi.v13i2.3804.

[11] F. Firmansyah and R. A. Purnama, "Filtering Domain Name Server (DNS) untuk Membangun Internet Sehat Menggunakan Routerboard Mikrotik," *JUITA J. Inform.*, vol. 7, no. 1, p. 43, 2019, doi: 10.30595/juita.v7i1.4164.

[12] G. Prakoso and A. Khamas Heikmakhtiar, "Analisis Keamanan Jaringan: ARP Spoofing dan DNS Spoofing dengan Metode National Institute of Standards and Technology," *J. Educ.*, vol. 06, no. 02, pp. 12895–12902, 2024.

[13] M. N. Hafizh, I. Riadi, and A. Fadlil, "Forensik Jaringan Terhadap Serangan ARP Spoofing menggunakan Metode Live Forensic," *J. Telekomun. dan Komput.*, vol. 10, no. 2, p. 111, 2020, doi: 10.22441/incomtech.v10i2.8757.

[14] A. Ariyanto and Asmunin, "Deteksi Paet Sniffing Pada Wirelles Menggunakan ARP Watch," *J. Manaj. Inform.*,

vol. 8, no. 2, pp. 178–181, 2018, [Online]. Available: https://jurnalmahasiswa.unesa.ac.id/index.php/jurnal-manajemen-informatika/article/view/25232.

[15] M. I. Susanto, A. Hasad, and M. A. Bakri, "Sistem Proteksi Jaringan Wlan Terhadap Serangan Wireless Hacking," *RJEC (Journal Electr. Electron.*, vol. 7, no. 1, pp. 25–34, 2019, [Online]. Available: https://jurnal.unismabekasi.ac.id/index.php/jrec/article/download/1762/1489.

[16] D. Novianto, "Implementasi DNS Forwarding Untuk Optimasi Resolving DNS Website Menggunakan Router Berbasis Linux," *Konf. Nas. Sist. Inf.*, pp. 1096–1101, 2018.