ABSTRAK

Pada tahun 2021, sekitar 85% komunikasi di dalam internet dilindungi menggunakan enkripsi. Dalam hal ini, *DNS (Domain Name System)* memiliki peran penting sebagai sistem yang menerjemahkan nama domain menjadi alamat IP yang dapat diakses oleh perangkat dan aplikasi. Namun *DNS* memiliki masalah potensi keamanan dan privasi yang perlu diatasi, salah satunya adalah *DNS Leak*. *DNS Leak* terjadi ketika permintaan *DNS* dikirim melalui jalur yang tidak dienkripsi, sehingga dapat diintip oleh pihak-pihak yang tidak berwenang. Data yang diintip ini dapat berupa alamat IP dan nama domain yang diakses oleh pengguna. Salah satu cara untuk menanggulangi kerentanan *DNS Leak* adalah menerapkannya protokol *DNS Over HTTPS (DoH)*. *DNS Over HTTPS* memastikan bahwa semua permintaan DNS dienkripsi dalam lalu lintas HTTPS. Sehingga data yang melewati jalur komunikasi lalu lintas data menjadi tidak dapat dibaca oleh *sniffer*. Penelitian ini mengimplementasikan *DoH* dan disimulasikan menggunakan layanan Bind9 yang berfungsi sebagai *recursive DNS Server* dan dikonfigurasi menggunakan *SSL* dari *let's encrypt* yang berfungsi menjalakan tugas *HTTPS* untuk mengenkripsi data yang lewat pada jalur komunikasi data. Dengan menerapkan *DoH*, penelitian ini menunjukkan bahwa semua permintaan *DNS* melalui jalur *HTTPS* menjadi terenkripsi. Sehingga alamat IP dan nama domain yang dituju oleh pengguna tidak dapat dibaca menggunakan aplikasi *packet sniffer* seperti *TCPdump* atau *wireshark*. Hal ini menunjukkan bahwa *DoH* dapat menanggulangi *DNS Leak*.

Kata Kunci: DNS, DNS Leak, HTTPS, SSL dan DNS Over HTTPS

ABSTRACT

By 2021, around 85% of communications on the internet are protected using encryption. In this case, DNS (Domain Name System) has an important role as a system that translates domain names into IP addresses that can be accessed by devices and applications. However, DNS has potential security and privacy issues that need to be addressed, one of which is DNS Leak. DNS Leak occurs when DNS requests are sent over an unencrypted path, so they can be snooped on by unauthorized parties. This snooped data can be in the form of IP addresses and domain names accessed by users. One way to overcome the DNS Leak vulnerability is to implement the DNS Over HTTPS (DoH) protocol. DNS Over HTTPS ensures that all DNS requests are encrypted in HTTPS traffic. So that data that passes through the data traffic communication lines becomes unreadable by the sniffer. This research implements DoH and is simulated using the Bind9 service which functions as a recursive DNS Server and is configured to use SSL from let's encrypt which functions to carry out HTTPS tasks to encrypt data passing on data communication lines. By implementing DoH, this research shows that all DNS requests over HTTPS paths become encrypted. So that the IP address and domain name intended by the user cannot be read using packet sniffer applications such as TCPdump or wireshark. This shows that DoH can overcome DNS Leak.

Keywords: DNS, DNS Leak, HTTPS, SSL and DNS Over HTTPS