Pemodelan Ringan Validasi *DNS-Spoofing* Attack Pada *Prototype 5G*

1st Muhammad Fadhilah.Rafii.Ramadhan
Fakultas Teknik Elektro
Universitas Telkom
Bandung, Indonesia
fadhilahrafii@student.telkomuniversity.ac.id

2nd Rendy Munadi
Fakultas Teknik Elektro
Universitas Telkom
Bandung, Indonesia
rendymunadi@telkomuniversity.ac.id

3rd Fardan
Fakultas Teknik Elektro
Universitas Telkom
Bandung, Indonesia
fardanext@telkomuniversity.ac.id

***Abstrak* — Kemunculan jaringan komunikasi 5G telah membawa peningkatan yang signifikan dalam hal kecepatan dan arsitektur jaringan dibandingkan dengan 4G. 5G memiliki kecepatan dua puluh kali lipat dan telah mengalami metamorfosis yang mendalam dari sistem terpusat menjadi sistem terdesentralisasi, dengan tujuan meminimalkan latensi lalu lintas. Namun terlepas dari langkah luar biasa ini, jaringan 5G berpotensi mengalami kerentanan keamanan yang tidak jauh berbeda dengan yang disaksikan dalam ranah 4G. Menurut penelitian, kelemahan keamanan dapat menyebabkan serangan spoofing, membuatnya mudah untuk melancarkan serangan yang mengubah tabel cache korban [2]. Network spoofing beroperasi ketika dua unit komputer pribadi (PC) bergabung dalam satu jaringan, yang masing-masing memiliki alamat MAC dan alamat IP yang unik, menurut penelitian (Hafizh, 2020). Ini memiliki dua alamat IP tetapi hanya satu alamat MAC karena penyerang mengubah alamat MAC [3]. Serangan DNS spoofing dapat terjadi pada jaringan 5G, sama seperti pada jaringan lainnya.**

***Kata kunci*— Kali linux, ARP Poisoning, DNS spoofing, 5G**

I. PENDAHULUAN

Komunikasi seluler 5G memiliki inovasi yang lebih maju dibandingkan dengan komunikasi seluler 4G secara umum. Mengutip dari jurnal (Security for 5G and Beyond) [1] perkembangan generasi kelima (5G) adalah suatu jaringan nirkabel untuk menghubungkan hampir semua aspek kehidupan melalui jaringan dengan kecepatan yang jauh lebih tinggi, dengan latensi sangat rendah dan konektivitas dimana-mana. Layanan 5G diklasifikasikan sebagai broadband seluler yang ditingkatkan di mana kecepatan menjadi elemen prioritas, diikuti oleh bandwith sebagai elemen kunci, dan juga meminimalkan waktu latensi yang dibutuhkan. Aspek ancaman keamanan 5G meningkat pesat karena peningkatan jenis layanan yang belum pernah terjadi sebelumnya dan jumlah penambahan perangkat. Oleh karena itu, solusi keamanan jika belum dikembangkan harus dipertimbangkan untuk menangani berbagai ancaman terhadap layanan yang berbeda, teknologi baru, dan lebih banyak data pengguna yang dapat diakses ke jaringan. Meskipun jaringan 5G memiliki kecepatan dan kapasitas yang lebih tinggi daripada pendahulunya, hal ini tidak membuatnya kebal terhadap serangan siber seperti serangan DNS spoofing.

II. KAJIAN TEORI

Serangan *DNS Spoofing* adalah jenis serangan dimana penyerang mencoba untuk mengalihkan lalu lintas data paket dari tujuan yang dituju dengan memberikan alamat IP palsu [2]. Serangan siber yang terjadi pada dunia maya ini memanipulasi *Domain Name System (DNS)* untuk mengalihkan lalu lintas ke situs web palsu yang berbahaya. Serangan ini memiliki risiko yang signifikan dalam aspek keamanan, karena merupakan bentuk serangan yang melibatkan penyerang yang menyamar sebagai pengguna atau sistem lain untuk mendapatkan akses informasi sensitif. Kegiatan ilegal ini sangat membahayakan pengguna nirkabel, dimana dampak kerugian dapat berupa hilangnya data dan penyerang juga dapat membocorkan identitas rahasia pengguna jaringan nirkabel.

A. Kali Linux

Keamanan Ofensif menciptakan Kali Linux, sistem operasi Linux dengan antarmuka pengguna grafis (GUI) langsung dan tidak mengganggu yang didasarkan pada Debian. [3]. Kali linux dirancang untuk pengujian penetrasi dan forensik lanjutan dengan menawarkan berbagai alat dan layanan yang memungkinkan pengguna melakukan tugas keamanan dengan mudah seperti pengujian penetrasi, penelitian keamanan, forensik komputer, penilaian pengujian kerentanan, dan penilaian kerentanan tim.

B. Ettercap

Fauzi dan Suartana (2017) menyatakan bahwa ettercap adalah program packet sniffer yang dapat digunakan untuk secara aktif menyadap protokol umum, membatasi lalu lintas jaringan LAN, dan mengaudit keamanan jaringan. Ini juga menganalisis protokol jaringan. Menempatkan antarmuka jaringan dalam mode promiscuous dan menggunakan peracunan ARP untuk mengkompromikan sistem target adalah bagaimana Ettercap melakukan serangan Man-in-the-Middle pada jaringan area lokal.

C. ARP Poisoning

Address Resolution Protocol (ARP) menerjemahkan alamat IP menjadi alamat Media Access Control (MAC) melalui mekanisme dalam mekanisme TCP/IP Suite. Metode serangan yang dikenal sebagai "keracunan ARP" pada jaringan komputer lokal melalui sarana kabel atau nirkabel memungkinkan peretas menemukan bingkai data di jaringan. dan mengubah lalu lintas jaringan bahkan

menghentikannya. Serangan ini memalsukan atau meracuni tabel ARP pada jaringan komputer bertujuan untuk membuat perangkat korban percaya bahwa alamat MAC dari router atau perangkat lainnya telah berubah atau terhubung dengan alamat MAC penyerang, dimana penyerang mengirimkan ARP palsu yang berisi informasi palsu tentang alamat MAC. Akibatnya perangkat korban akan mengirimkan lalu lintas jaringannya ke alamat MAC penyerang, yang memungkinkan penyerang untuk melakukan serangan Man in the middle dan memantau atau memanipulasi lalu lintas jaringan.

III. METODE

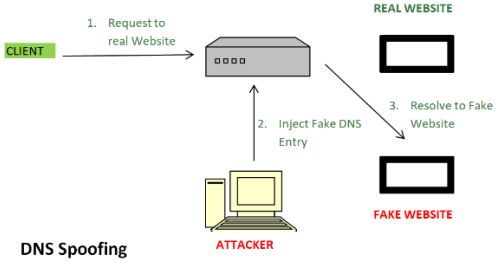
Dalam penelitian ini penulis menggunakan metode penyerangan *DNS Spoofing* menggunakan virtual machine kali linux dengan tools ettercap. Penulis ingin mengetahui dampak yang terjadi pada web browser seperti localhost webui open5gs, google, dan youtube jika diserang menggunakan metode serangan yang penulis sebutkan.

A. Metodologi Penelitian

1. Studi literatur
   Mengumpulkan bahan pustaka dalam rangka memperoleh pengetahuan yang diperlukan untuk penelitian.
2. Analisis
   Berdasarkan data yang dikumpulkan baik sebelum maupun sesudah penyerangan, analisis permasalahan yang muncul dalam penelitian.
3. Perancangan serangan
   Membuat serangan DNS Spoofing dan memahami cara kerjanya untuk memenuhi tujuannya
4. Implementasi dan Pengujian
   implementasi dan pengujian serangan untuk mencapai hasil yang diinginkan sehubungan dengan masalah penelitian.
5. Hasil analisis
   Temuan-temuan yang diperoleh dari pemeriksaan sistem penyerangan terbukti bermanfaat dalam mengatasi situasi yang berasal dari terjadinya masalah yang muncul dalam penelitian ini.
6. Kesimpulan
   Untuk menarik kesimpulan dan mengatasi masalah yang diangkat oleh penelitian, penulis merangkum temuan pengujian yang dikumpulkan melalui eksekusi serangan.

B. Rancangan Penelitian

1. Topologi Penyerangan DNS Spoofing



GAMBAR 1.
Topologi Serangan DNS Spoofing

2. Hardware dan Software

a. *Hardware* yang dibutuhkan yaitu :

1) Laptop DELL
2) Modem WiFi / WiFi yang terhubung

b. *Software* yang dibutuhkan dalam pengujian :

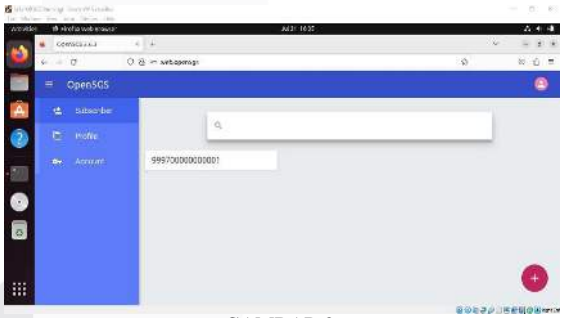
1) Sistem operasi : a. *Windows*
   b. *Kali linux*
   c. *Ubuntu 22.04 (jammy)*
2) Aplikasi : a. *Oracle VM Virtualbox*
   b. *Ettercap*
3) Penyerang : a. *Virtualbox*
   b. *Kali linux*
   c. *Ettercap*
4) Korban : *Web browser*

IV. HASIL DAN PEMBAHASAN

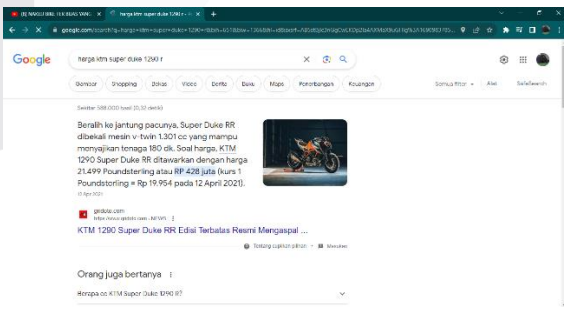
Bagian ini menyajikan deskripsi penulis tentang hasil serangan dan percakapan yang mengikutinya, yang diinformasikan oleh tinjauan literatur dan analisis masalah yang diidentifikasi.

A. Tampilan Web Sebelum Penyerangan

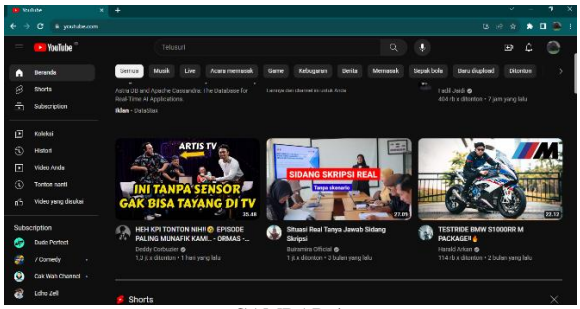
Penulis menjalankan sistem operasi mesin virtual Kali Linux pada laptop. Situs web asli dikirim ke halaman web palsu yang telah diubah oleh penyerang menggunakan IP di Kali Linux. Tampilan situs web dari Google, YouTube, dan Open5GS WebUI akan disediakan oleh penulis sebelum serangan DNS Spoofing.



GAMBAR 2.
Webui Open5gs Sebelum Penyerangan



GAMBAR 3.
Web Google Sebelum Penyerangan



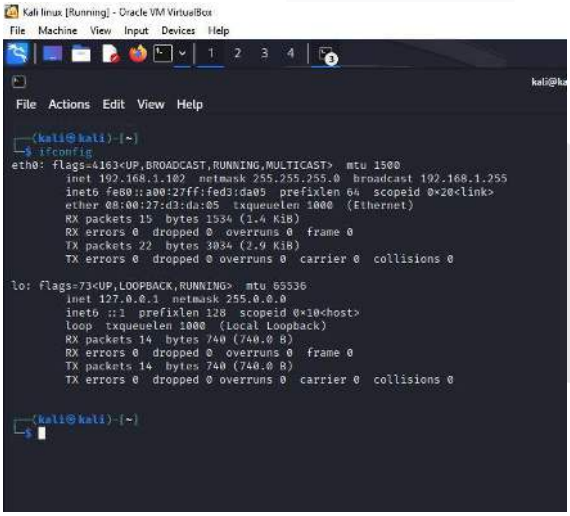
GAMBAR 4.
Youtube Sebelum Penyerangan

B. Proses Penyerangan

Bagian ini mencakup metode penulis untuk melakukan fase serangan percobaan, termasuk bagaimana mereka memilih target mana yang akan diserang. Berikut ini adalah tahapan prosedur pengujian serangan yang melibatkan pemilihan target:

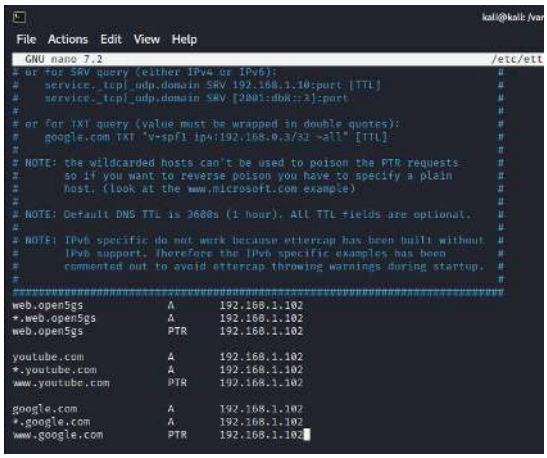
GAMBAR 5.
OS Kali Linux

tampilan sistem operasi Kali Linux setelah disambungkan dengan modem wifi Smartfren; percobaan serangan akan dilakukan melalui jaringan wifi.



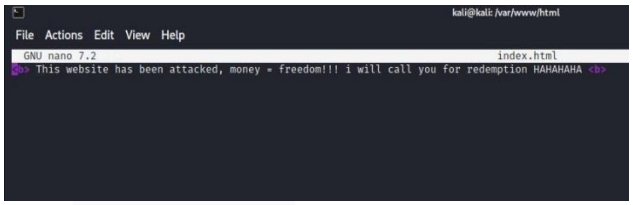
GAMBAR 6.
Alamat *IP kali Linux (penyerang)*

Anda dapat menggunakan terminal Kali Linux untuk mendapatkan alamat IP penyerang dengan menjalankan perintah ifconfig. Alamat IP yang dikumpulkan adalah 192.168.1.102, dan berfungsi sebagai pengalihan ke situs web yang dimaksudkan untuk diserang.



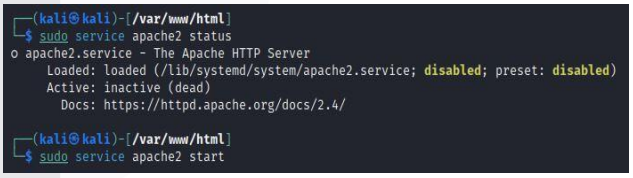
GAMBAR 7.
DNS Config Pada *Ettercap*

DNS config adalah tampilan konfigurasi domain yang akan dimanipulasi oleh penyerang. Domain yang akan diserang akan disimpan pada *Ettercap* menjadi *file etter.dns.* Situs web yang akan dimanipulasi oleh penyerang akan di alihkan ke *IP* penyerang yaitu 192.168.1.102



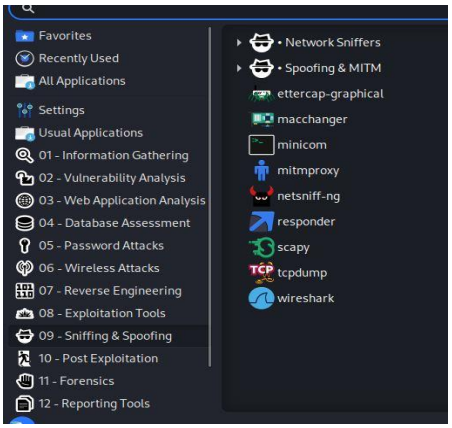
GAMBAR 8.
Directory Serangan

Directory serangan bersifat opsional, fungsi dari directory ini adalah memberikan tampilan kata-kata untuk web palsu. Perintah untuk directory ini adalah *sudo nano indeks.html.* Sehingga pada saat serangan berhasil dijalankan, kata-kata yang sudah dibuat akan muncul di web browser. Dalam kasus lain, kata-kata ini bisa tidak muncul sehingga hanya menunjukkan status bahwa jaringan hilang atau dialihkan.



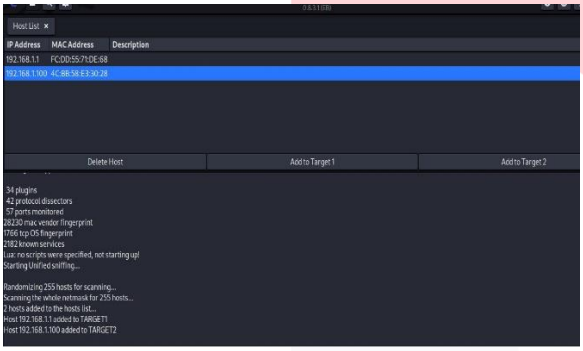
GAMBAR 9.
Mengaktifasi *Apache2*

Untuk menjalankan penyerangan DNS Spoofing pada kali linux dengan *Ettercap,* status apache perlu diaktifkan. *Apache2* berfungsi untuk menjalankan tugasnya sebagai web palsu untuk memanipulasi korban.

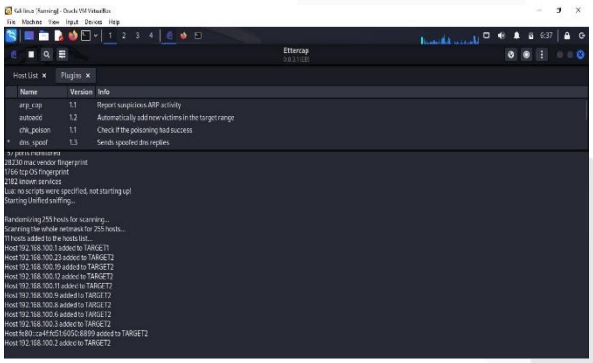


GAMBAR 10.
Aktifasi Ettercap

Untuk memulai penyerangan DNS Spoofing. Pelaku memilih penyerangan *sniffing & spoofing* dengan menggunakan *Ettercap-graphical.*



GAMBAR 11.
Host Terscanning
Host yang terhubung dengan jaringan modem *WiFi*, akan terscanning oleh *Ettercap.*

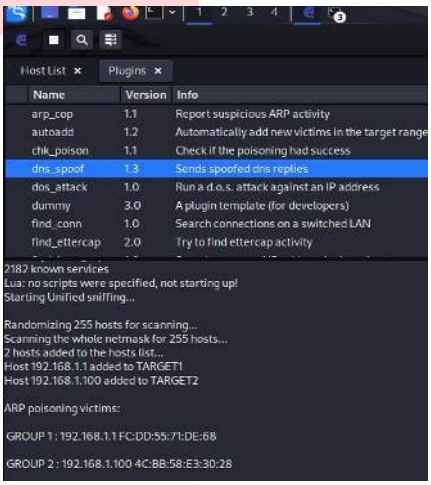


GAMBAR 12.
Menentukan Target Host

Pada *Gambar.11* dan *Gambar.12*, merupakan host target yang telah dipilih oleh penyerang. Alamat gateway jaringan terkait diidentifikasi oleh Target 1, yang memiliki alamat IP 192.168.1.1. Sebaliknya, pada target 2, alamat IP korban adalah 192.168.1.100.

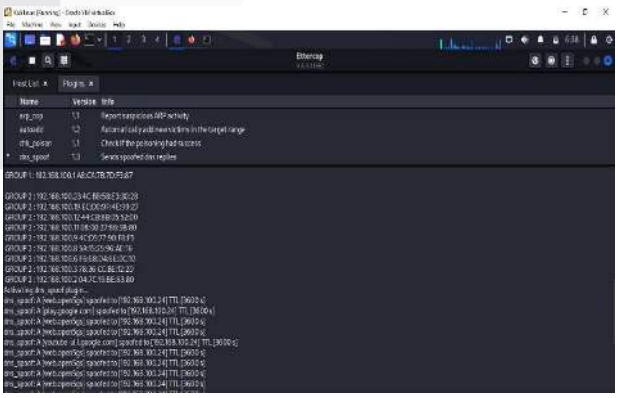
Gambar 13.
Aktifasi *ARP Poisoning*

Tujuan mengaktifkan *ARP Poisoning* adalah menjalankan tugasnya sebagai hijacking atau pembajak, menangkap terjemahan dari *IP address* dan mengirimkan lalu lintas jaringan korban ke alamat MAC penyerang.



GAMBAR 14.
Aktifasi DNS Spoofing

Tujuan mengaktifkan fitur *dns_spoof* pada *ettercap* adalah agar serangan dapat di penetrasikan atau di jalankan kepada target yang ditentukan oleh penyerang

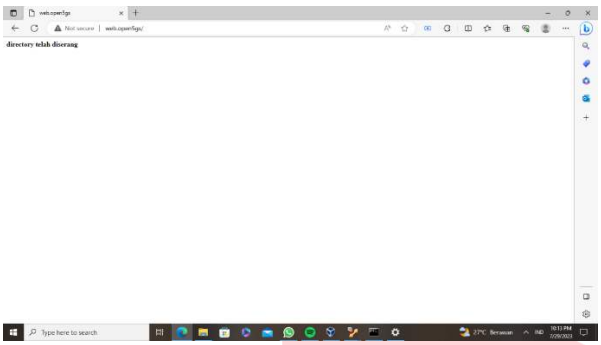


GAMBAR 15.
Web Berhasil di Spoofing

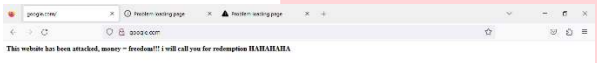
Ettercap menunjukkan status web yang di targetkan oleh penyerang, berhasil di spoofing. Artinya bahwa penyerang berhasil mengarahkan target ke fake web

C. Hasil Penyerangan

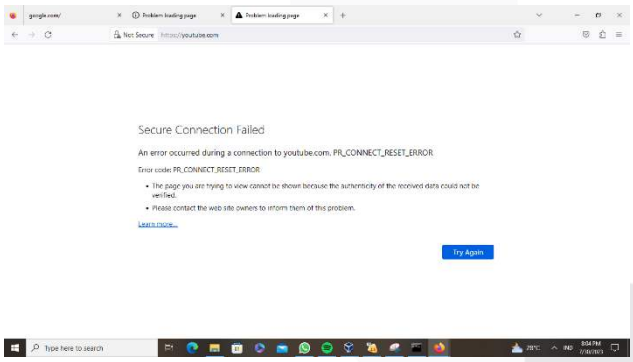
Penulis melakukan uji coba penyerangan sebanyak 3 kali percobaan. Berikut penulis tampilkan kondisi web setelah penyerangan DNS Spoofing berhasil dijalankan.



GAMBAR 16.
Webui Open5gs Setelah Penyerangan



GAMBAR 17.
Web Google Setelah Penyerangan



GAMBAR 18.
Youtube setelah penyerangan

V. KESIMPULAN

Dari hasil pengujian yang telah dilakukan bahwa *DNS Spoofing* termasuk serangan siber yang memanipulasi Domain Name System untuk mengarahkan lalu lintas ke situs web palsu dan juga memutus lalu lintas jaringan. Serangan ini dilakukan dengan cara memalsukan atau mengubah catatan DNS dengan mengarahkan pengguna ke alamat website yang salah. Serangan DNS Spoofing termasuk kategori serangan Man in the middle. Meskipun kecepatan dan kapasitas jaringan 5G lebih tinggi dibandingkan dengan jaringan sebelumnya, jaringan 5G tidak kebal terhadap serangan DNS spoofing. Serangan semacam ini masih mengeksploitasi kerentanan pada protokol DNS yang digunakan oleh jaringan, bukan tergantung pada jenis jaringan yang digunakan.

REFERENSI

[1] Ahmad, I., Shahabuddin, S., Kumar, T., Okwuibe, J., Gurtov, A., & Ylianttila, M. (2019). Security for 5G and beyond. IEEE Communications Surveys & Tutorials, 21(4), 3682-3722.

[2] V, C, Ginting, D. P. Kartikasari "Deteksi Serangan ARP Spoofing Berdasarkan Analisis Lalu Lintas Paket Protokol ARP". Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer. Vol. 3, No. 5. Hlm. 5049-5057. E-ISSN: 2548-964X, 2019.

[3] A. R. Taqwa, D. H. Sulaksono, "Implementasi Kriptografi Dengan Metode Elliptic Curve Cryptography (ECC) Untuk Aplikasi Chatting Berbasis Android", Jurnal Riset Inovasi Bidang Informatika dan Pendidikan Informatika (KERNEL). Vol. 1. No. 1, 2020

[4] Rianda. (2022). "Ketahui Pengertian DNS Spoofing dan Cara Pencegahannya". Internet : https://dewabiz.com/pengertian-dns-spoofing/, Nov. 5, 2022 [Aug. 15, 2023].

[5] Pangestu, T., & Liza, R. (2022, September 30). Analisis Keamanan Jaringan Pada Jaringan Wireless Dari Serangan Man In The Middle Attack DNS Spoofing. *JiTEKH*, *10*(2), 60-67

[6] N. Andiyani et al., "IMPLEMENTASI MAN IN THE MIDDLE ATTACK PADA ALGORITME BLAKE2S BERBASIS LoRa," vol. 6, no. 2, pp. 1–6, 2022

[7] Z. M. Subekti, H. Setiawan, Satria, W. M. Wijaya, A. Hafiz, and Warsudi, "PERANCANGAN INFRASTRUKTUR DOMAIN NAME SERVER LOKAL MENGGUNAKAN UBUNTU SERVER 16.04 PADA PT. XYZ," no. 2, p. 6, 2020

[8] randi candra kirana Yudi mulyanto, Herfandi, "ANALISIS KEAMANAN WIRELESS LOCAL AREA NETWORK (WLAN) TERHADAP SERANGAN BRUTE FORCE DENGAN METODE PENETRATION TESTING," vol. 4, no. 1, pp. 26–35, 2022.