IMPLEMENTASI PENETRATION TESTING DAN WORDLIST GENERATOR DALAM PENGUJIAN KEAMANAN JARINGAN MENGGUNAKAN METODE DICTIONARY ATTACK

Adi Sunandar
Informatika, Universitas Singaperbangsa Karawang
Jl. HS.Ronggo Waluyo, Puseurjaya, Telukjambe Timur, Karawang, Jawa Barat 41361
2010631170041@student.unsika.ac.id

ABSTRAK

Keamanan kata sandi tentunya sudah bukan hal yang asing untuk sebagian besar pengguna internet yang sehari-harinya mengakses internet untuk berbagai kebutuhan. Tentunya kata sandi yang digunakan beragam mulai dari kata sandi yang kuat maupun kata sandi yang lemah, tidak sedikit para pengguna internet menggunakan kata sandi yang lemah sehingga mudah untuk dilakukan peretasan. Hal ini juga sering kali dijumpai pada jaringan yang ada di kantor ataupun gedung instansi pendidikan. Maka dari itu diperlukannya pengujian kata sandi yang dilakukan secara rutin untuk terus meningkatkan keamanan dari kata sandi yang digunakan tersebut. Salah satu cara untuk melakukan pengujian tersebut adalah menggunakan metode *penetration testing* yang biasa digunakan dalam menguji keamanan serta integritas suatu sistem. Dari hasil pengujian menggunakan metode *penetration testing* dan menggunakan *teknik dictionary attack* yang digabungkan dengan pembuatan *wordlist* secara otomatis menggunakan *wordlist generator*, didapatkan hasil berupa kata sandi yang digunakan oleh jaringan yang diuji coba dapat diketahui.

Kata kunci : *Penetration testing, keamanan jaringan, WiFi, dictionary attack*

1. PENDAHULUAN

Pada perkembangan jaringan yang semakin luas sekarang ini menjadi sangat penting untuk dapat memahami dan merencanakan sistem keamanan jaringan WLAN yang terhubung ke internet dengan cermat dan aman, sehingga aset atau sumber daya dalam jaringan dapat dilindungi secara efisien. Hal ini menjadi upaya dalam melakukan pertahanan terhadap beberapa jenis serangan yang sering dilakukan oleh hacker meliputi penggunaan *Brute Force Attack, Dictionary Attack, Packet Sniffer, Probe, Scan, ARP Spoofing / ARP Poisoning, Root Compromise, Account Compromise, dan Denial of Service (DoS)* [9].

Cara yang sering digunakan untuk melakukan pengujian terhadap jaringan yaitu *penetration testing* atau uji penetrasi. Metode ini adalah pendekatan di mana sistem yang digunakan diserang secara simulasi, dan sertifikat keamanan jaringan yang mumpuni sangat diperluan untuk mencegah upaya peretas atau penyusup yang dapat mengakibatkan kehilangan data dan aset sistem target. Orang yang melakukan metode ini disebut pentester [8].

Terdapat banyak cara untuk mengimplementasikan *Penetration Testing* pada jaringan yang digunakan, salah satu metode yang dapat digunakan adalah metode *Black Box* yang mana adalah jenis pengujian yang paling menyerupai situasi serangan luar dan sering disebut sebagai pengujian eksternal. Dalam jenis pengujian ini, penguji penetrasi akan melakukan tes dari lokasi yang jauh dengan hanya memiliki akses terbatas terhadap informasi yang tersedia [4].

Kemudian metode paling mudah dilakukan adalah dengan menggunakan teknik *Dictionary Attack* yang mana akan menggunakan *wordlist* yang telah disiapkan untuk mencoba menyerang dan menebak kata sandi dari sebuah jaringan yang dijadikan target oleh penyerang [3].

2. TINJAUAN PUSTAKA

2.1. Penelitian Terdahulu

Pada penelitian terdahulu yang dilakukan oleh Haeruddin dan Kurniadi dengan judul "Analisis Keamanan Jaringan WPA2-PSK Menggunakan Metode Penetration Testing (Studi Kasus: TP-Link Archer A6)" yang membahas tentang pengujian keamanan jaringan Wi-Fi menggunakan metode Penetration Testing pada router TP-Link Archer A6. Hasilnya menunjukkan bahwa jaringan dengan konfigurasi *default* rentan terhadap serangan. Dianjurkan untuk meningkatkan keamanan dengan mengkonfigurasi jaringan lebih aman [2].

Pada penelitian karya Ismail dan Pramudita dengan judul "Metode Penetration Testing pada Keamanan Jaringan Wireless Wardriving PT. Puma Makmur Aneka Engineering Bekasi" yang menjelaskan tentang *Penetration Testing* pada jaringan *wireless* PT. Puma Makmur Aneka Engineering, yang menemukan kerentanan seperti *WPA2 Cracking, DoS*, dan lainnya. Setelah perbaikan, tingkat kerentanan menurun, meskipun beberapa sulit diperbaiki sepenuhnya [5].

Pada penelitian karya Tri Yusnanto, Muhammad Abdul Muin, dan Sugeng Wahyudiono dengan judul "Analisa Infrastruktur Jaringan Wireless dan Local Area Network (WLAN) Menggunakan Wireshark Serta Metode Penetration Testing Kali Linux" yang menjelaskan tentang evaluasi keamanan jaringan nirkabel dengan metode *Penetration Testing* melibatkan empat tahapan. Temuan mencakup keberhasilan meretas enkripsi, autentikasi MAC, serangan DoS, dan MITM. Disarankan perbaikan pada

autentikasi, enkripsi, dan keamanan secara keseluruhan [10].

2.2. WLAN

Wireles Local Area Network (WLAN) atau biasa disebut juga sebagai *Wireless Fidelity* (Wi-Fi), merujuk pada teknologi yang memfasilitasi pertukaran data melalui gelombang radio tanpa perlu kabel. Berbagai perangkat elektronik seperti komputer, *smartphone*, tablet, dan lainnya dapat menggunakan teknologi ini. Wi-Fi populer di masyarakat karena keunggulan-keunggulan yang dimilikinya [7].

2.3. Serangan Jaringan Pada WLAN

Media transmisi nirkabel adalah gelombang radio yang dapat ditransmisikan ke berbagai area yang dapat dijangkau oleh gelombang tersebut. Namun, beberapa vendor telah menyediakan fitur yang memudahkan pengguna dan administrator jaringan untuk menggunakan teknologi ini, yang sering kali menyebabkan pengguna jaringan menggunakan konfigurasi default dari vendor. Oleh karena itu, *hacker* telah mengambil tindakan untuk menguji keamanannya. Ada beberapa jenis serangan yang biasanya dilakukan seperti *Brute Force Attack, Dictionary Attack, Packet Sniffer, Probe, Scan, ARP Spoofing / ARP Poisoning, Root Compromise, Account Compromise, dan Denial of Service (DoS)* [1].

2.4. *Penetration Testing*

Penetration testing adalah metode yang digunakan untuk mengevaluasi keamanan sistem komputer atau jaringan melalui simulasi peretasan. Proses ini melibatkan beberapa tahap, di antaranya perencanaan, pengumpulan informasi, analisis kerentanan, eksploitasi, dan pelaporan. Tahap perencanaan mencakup persiapan yang diperlukan seperti perizinan dan pencarian data, sementara pengumpulan informasi dilakukan untuk memperoleh data penting baik secara manual maupun menggunakan alat layanan *online*. Analisis kerentanan dilakukan untuk mengidentifikasi serangan yang mungkin terjadi dan mencari celah atau *port* yang dapat dimanfaatkan dalam serangan. Tahap eksploitasi melibatkan simulasi serangan untuk mendapatkan informasi sensitif seperti *username* dan *password*. Akhirnya, tahap pelaporan melibatkan penyusunan laporan yang menjelaskan hasil penetrasi dan menyarankan langkah-langkah korektif yang perlu diambil [6].

2.5. *Dictionary Attack*

Dictionary Attack adalah teknik untuk mengakses komputer atau *server* yang dilindungi kata sandi dengan cara sistematis mencoba setiap kata dalam daftar kata-kata yang disimpan sebagai kata sandi. Serangan ini juga dapat digunakan untuk mencari kunci yang diperlukan untuk mendekripsi pesan atau dokumen yang dienkripsi [3].

2.6. Kali Linux

Kali linux merupakan sebuah program pengembangan tingkat lanjut untuk melakukan penetration testing yang dikeluarkan oleh Debian. Seluruh infrastuktur serta *tools* yang ada pada kali linux sudah direview dan dikemas kembali secara lebih baik sehingga mudah untuk digunakan [11].

2.7. Aircrack

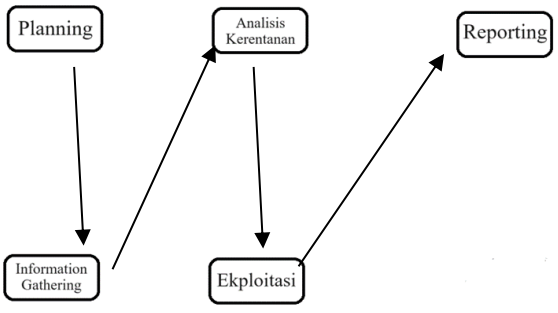
Merupakan sebuah tools yang memiliki beberapa kegunaan sehingga cukup popular untuk melakukan serangan terhadap jaringan wireless. Cara kerja dari tools ini adalah dengan melakukan decryption terhadap key atau hash yang didapatkan dari paket data yang sudah terekam dan tersimpan di dalam wordlist. Aircrack memiliki 4 utilitas utama yang saling berintegrasi satu sama lain, yaitu:

a. Airmon-ng yang berfungsi untuk memulai dan menghentikan mode monitoring pada driver jaringan yang digunakan.
b. Airodump-ng berfungsi sebagai alat untuk melakukan sniffing terhadap jaringan.
c. Aireplay-ng berfungsi sebagai alat untuk melakukan packet injection atau de-authentication terhadap jaringan tujuan.
d. Aircrack-ng berfungsi sebagai cracker yang akan melakukan decrypt terhadap hash password yang sudah di dapatkan

Keempat utilitas utama ini akan saling bersinergi dan terintegrasi satu sama lain untuk mendukung proses peretasan yang dilakukan [12].

3. METODE PENELITIAN

Medote Penelitian dalam melakukan penelitian ini, peneliti menggunakan prinsip *metode Penetration Testing*. Hal ini dikarenakan metode ini cukup sering digunakan dalam mencari kerentanan suatu sistem. Kemudian pada kali ini akan digunakan teknik *dictionary attack* yang akan menggunakan beberapa langkah. Langkah yang akan digunakan dalam melakukan metode *penetration testing* ini antara lain adalah:



Gambar 1. Alur *penetration testing*

Pada gambar 1 di atas dapat dilihat bahwa metode *penetration testing* yang digunakan terbagi menjadi beberapa langkah yaitu:

a. *Planning*
Perencanaan dalam melakukan penelitian kali ini adalah membuat *wordlist* yang akan digunakan dalam melakukan penelitian yang menggunakan 2 *tools* yang berfungsi sebagai *word generator* sehingga mempermudah proses pembuatan *wordlist*, kedua tools tersebut adalah *Common User Password Profiler (CUPP)* dan Mentalist.
b. Information Gathering
Mempersiapkan alat dan bahan yang akan digunakan dalam proses penelitian serta pengumpulan informasi yang diperlukan untuk mempermudah proses seperti *BSSID*, *Channel*, *SSID*, dan lain sebagainya menggunakan salah satu *tool* dari seri Aircrack-ng yaitu Airomon-ng.
c. Analisis Kerentanan
Melakukan Penangkapan terkait hash *password* yang diperlukan dalam penelitian untuk mendapatkan sandi dari jaringan Wi-Fi yang akan diuji coba menggunakan kombinasi 2 metode yaitu *Sniffing* dan *De-Authentication* menggunakan tools Airodump-ng dan Aireplay-ng.
d. Eksploitasi
Proses uji coba pembobolan kata sandi Wi-Fi dengan menggunakan metode *Brute Force Dictionary Attack* menggunakan tool Aircrack-ng dan menguji cobanya menggunakan *wordlist* yang sudah disiapkan dengan metode *social engineering* menggunakan *tools wordlist generator* CUPP dan Mentalist serta melakukan pengecekan terkait kekuatan sandi.
e. *Reporting*
Melakukan pencekan terhadap *wordlist* yang digunakan menggunakan *tool* Pipal untuk mengetahui kombinasi karakter yang digunakan untuk uji coba serta tingkat keamanan dari sandi jaringan yang sedang diuji coba.

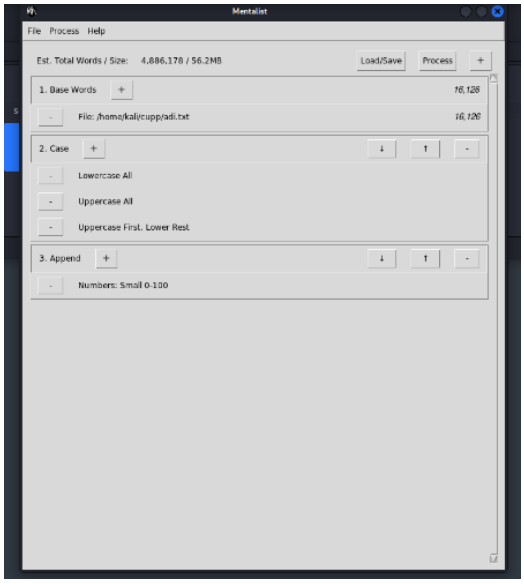
4. HASIL DAN PEMBAHASAN

4.1. *Planning*

Pada tahap *planning* ini akan dilakukan persiapan terkait alat dan bahan yang akan digunakan dalam melakukan *dictionary attack* pada jaringan Wi-Fi yang ada di unsika. Bahan yang diperlukan dalam penelitian kali ini adalah *wordlist* spesifik yang akan digunakan dalam uji coba dalam *dictionary attack*. Kemudian dalam membuat *wordlist* tersebut menggunakan 2 *tools* yang Bernama CUPP (*Common User Password Profiler*) dan Mentalist untuk membuat kumpulan *wordlist* berdasarkan beberapa kata dan aturan yang dimasukkan.

Gambar 2. Tampilan cup

Pada gambar 2 di atas dapat dilihat tampilan awal dari *tools* CUPP yang akan digunakan dengan memasukkan *syntax* yang sesuai. Kemudian setelahnya akan diminta untuk memasukkan beberapa informasi terkait nama, tanggal lahir, nama pasangan, nama anak, nama peliharaan, instansi serta kata - kata yang berhubungan dengan pemilik jaringan yang akan dicoba untuk dibobol. Kemudian secara otomatis *tools* CUPP akan melakukan *generate* otomatis kata yang sudah diinputkan dalam informasi diatas dan disimpan menjadi *file* dengan format *.txt.*

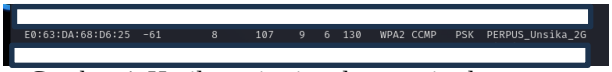


Gambar 3. Tampilan mentalist

Dan langkah yang terakhir dapat dilihat pada gambar 3 bahwa file *wordlist* yang dihasilkan oleh CUPP akan kita olah kembali dengan beberapa aturan baru seperti membuat seluruh kata menjadi *lowercase*, seluruh kata menjadi *uppercase*, setiap kata menerapkan prinsip *capitalize first letter*, serta menambahkan angka 0-100 pada setiap kata.

4.2. *Information Gathering*

Pada tahap *information gathering* ini proses dilakukan sebanyak 5 kali dan mendapatkan hasil yang serupa untuk setiap percobaannya. Sehingga pada tahap ini akan dilakukan proses pengumpulan informasi terkait jaringan yang akan diuji coba seperti nama jaringan (SSID), BSSID, *channel*, *encoder*, dan *encryption type*. Pada tahap ini akan menggunakan salah satu fungsi dari seri *tools* Aircrack-ng yaitu Airodump-ng.



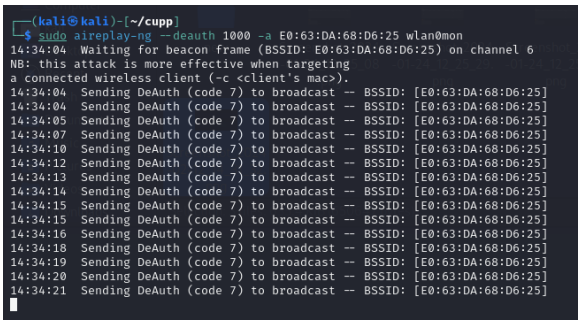
Gambar 4. Hasil monitoring dengan airodump-ng

Data – data penting untuk proses penelitian kali ini yang didapatkan dari hasil *monitoring* jaringan dan dilakukan menggunakan *tools* Airodump-ng dapat dilihat pada gambar 4 di atas. Pada gambar tersebut terlihat bahwa jaringan menggunakan *encoder* WPA2

dan memiliki tipe enkripsi PSK sehingga jaringan tersebut menggunakan sistem keamanan standar dari WPA2-PSK. Kemudian dapat dilihat pula *channel* dan BSSID dari jaringan tersebut.

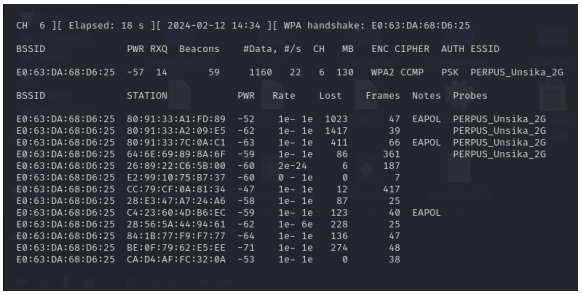
4.3. *Vulnerability Analysis*

Setelah berhasil menemukan informasi yang dibutuhkan, dapat dilanjutkan dengan melakukan *sniffing* jaringan untuk mendapatkan file *.cap* dari hasil *WPA Handshake* yang dilakukan antara *Access Point* dengan perangkat di sekitar. Pada kali ini dibantu oleh Wi-Fi Doogle TP-Link TL-WN722N versi 1 sebagai perantara antara kali linux dan *Access Point* Wi-Fi yang diuji coba. Kemudian dengan menggunakan 2 *tools* yaitu airodump-ng dan aireplay-ng dapat dilakukan *de-authentication* pada BSSID secara spesifik sekaligus melakukan *monitor* pada BSSID yang dijadikan *target* sehingga didapatkan *WPA-Handshake* yang disimpan dalam file dengan ekstensi *.cap*.



Gambar 5. Proses *de-authentication*

Pada gambar 5 di atas dapat dilihat bahwa menggunakan tool aireplay-ng dilakukan proses de-authentication sebanyak 1000 kali percobaam untuk BSSID E0:63:DA:68:D6:25 yang merupakan BSSID dari SSID PERPUS_Unsika_2G yang sebelumnya sudah di monitor



Gambar 6. Proses penangkapan *hash password*

Pada gambar 6 di atas dapat dilihat bahwa menggunakan tool airodump-ng dilakukan proses penangkapan hash password pada SSID PERPUS_Unsika_2G yang ditandai oleh adanya WPA handshake yang terjadi saat proses monitoring ini terjadi.

4.4. *Exploiting*

Kemudian setelah file *.cap* sudah didapatkan, maka dapat dilakukan peretasan pada *password* yang terkandung dalam file *.cap* yang sudah didapatkan tersebut menggunakan *tool* Aircrack.ng menggunakan metode *dictionary attack* yang menggunakan *wordlist* yang sudah dibuat sebelumnya menggunakan *tools Common User Password Profiler* (CUPP) dan *Mentalist*.

Gambar 7. Hasil eksploitasi dengan aircrack-ng

Pada gambar 7 di atas dapat dilihat bahwa *password* dari Wi-Fi dengan SSID PERPUS_Unsika_2G yang terenkripsi dengan WPA2-PSK telah berhasil ditemukan menggunakan Aircrack-ng. Diketahui bahwa *password* dari PERPUS_Unsika_2G adalah “unsika2023”

4.5. *Reporting*

Setelah tahap eksploitasi telah dilakukan menggunakan *tool* aircrack-ng yang telah dipaparkan pada *sub bab* sebelumnya, selanjutnya menggunakan pipal akan dilaporkan hasil statistik dari *wordlist* yang digunakan untuk melakukan eksploitasi sebelumnya.

Tabel 1. Hasil reporting dengan pipal

No	Jenis	Word 1
1	Lower Alphanumeric	6.263.227
2	Upper Alphanumeric	6.263.212
3	Mixed Alphanumeric	5.380.588
4	Lower Alphaspecialnumeric	4.488.339
5	Upper Alphaspecialnumeric	4.488.162
6	Mixed Alphaspecialnumeric	3.725.486
7	Numeric	53.227
8	Special Numeric	12.322

Berdasarkan data pada tabel diatas dapat dilihat bahwa persebaran set karakter pada *wordlist* yang digunakan cukup merata dengan kombinasi *Lower Alphanumeric* memiliki kombinasi sebanyak 6.263.227 jenis, kombinasi *Upper Alphanumeric* memiliki kombinasi sebanyak 6.263.212 jenis, *kombinasi Mixed Alphanumeric* memiliki kombinasi sebanyak 5.380.588 jenis, kombinasi *Lower Alphaspecialnumeric* memiliki kombinasi sebanyak 4.488.339 jenis, kombinasi *Upper Alphaspecialnumeric* memiliki kombinasi sebanyak 4.488.162 jenis, kombinasi *Mixed Alphaspecialnumeric* memiliki kombinasi sebanyak 3.725.486 jenis, kombinasi *Numeric* memiliki kombinasi sebanyak 53.227 jenis, dan kombinasi

Special Numeric memiliki kombinasi sebanyak 12.322 jenis.

5. KESIMPULAN DAN SARAN

Setelah dilakukan pengujian terhadap jaringan tersebut yang menggunakan enkripsi WPA2PSK diketahui bahwa kata sandi yang digunakan adalah "unsika2023" yang terdapat di dalam wordlist yang sudah dibuat menggunakan CUPP dan Mentalist. Hal ini dapat terjadi karena kombinasi dari kata sandi yang digunakan dapat tergolong sebagai kata sandi yang lemah yang menjadi celah untuk dieksploitasi oleh penyerang. Sehingga untuk meningkatkan keamanan dari kata sandi tersebut perlunya dilakukan perubahan pada kata sandi secara berkala ataupun menggunakan set kombinasi yang lebih beragam seperti penggunaan kombinasi dari *uppercase, lowercase, numeric* serta *special character*. Tetapi perlu dilakukan pengujian lebih lanjut lagi dengan menggunakan teknik yang lebih jauh seperti menggunakan teknik *Brute Force Attack* yang langsung menebak setiap kombinasi kata sandi tanpa perlu *wordlist* ataupun menggunakan teknik *Rainbow Table* yang menggunakan tabel berukuran besar untuk melakukan *decrypt* terhadap kata sandi.

DAFTAR PUSTAKA

[1] Azmi, A., Y., F., AG, J., G., Wahyudi, E., 2022. Analisis Network Security Padalayananwifi Indihome Terhadap Serangandenial of Service (Dos). JURNAL LITEK: Jurnal Listrik Telekomunikasi Elektronika, 19(1), pp.8-12.

[2] Haeruddin, Kurniadi, A., 2021. Analisis Keamanan Jaringan WPA2-PSK Menggunakan Metode Penetration Testing (Studi Kasus: TP-Link Archer A6). Conference on Management, Business, Innovation, Education and Social Science (COMBINES), 1(1), pp.508-515.

[3] Halawa, B., F., Suwardi, A., Toro, R., Syahputri, R., 2020. Analisis Kelemahan Sistem Authentication Pengguna Pada Wireless IEEE 802.11i. Prosiding Seminar Nasional SMIPT 2020 Sinergitas Multidisiplin Ilmu Pengetahuan dan Teknologi, 3(1), pp.291-301.

[4] Hasibuan, M., Elhanafi, A. M., 2022. Penetration Testing Sistem Jaringan Komputer Menggunakan Kali Linux Untuk Mengetahui Kerentanan Keamanan Server dengan Metode Black Box (Studi Kasus Web Server Diva Karaoke.co.id). Sudo Jurnal Teknik Informatika, 1(4), pp.171-177.

[5] Ismail, R. W., Pramudita, R., 2020. Metode Penetration Testing pada Keamanan Jaringan Wireless Wardriving PT. Puma Makmur Aneka Engineering Bekasi. Jurnal Mahasiswa Bina Insani, 5(1), pp.53-62.

[6] Mulyanto, Y., Fari, A. A., 2022. Analisis Keamanan Login Router Mikrotik dari Serangan Bruteforce Menggunakan Metode Penetration Testing (Studi Kasus SMK NEGERI 2 SUMBAWA). JINTEKS (Jurnal Informatika Teknologi dan Sains), 4(3), pp.143-155.

[7] Nurdiana, F. R., Gunawan, I., Viollita, R. C., Faizal, M. A., Nurcahyadi, D., 2021. Analisis Keamanan Jaringan WIfi Menggunakan Wireshark. JES (Jurnal Elektor Smart), 1(1), pp.10-13.

[8] Rusdi, M. I., Prasti, D., 2019. Penetration Testing Pada Jaringan Wifi Menggunakan Kali Linux. Seminar Nasional Teknologi Informasi dan Komunikasi (SEMANTIK) 2019, 2(1), pp.260-269.

[9] Santoso, N. A., Ainurohman, M., Kurniawan, R. D., 2022. Penerapan Metode Penetration Testing Pada Keamanan Jaringan Nirkabel. Jurnal Responsif, 4(2), pp.162-167.

[10] Yusnanto, T., Muin, M., A., Wahyudiono, S., 2022. Analisa Infrastruktur Jaringan Wireless dan Local Area Network (WLAN) Menggunakan Wireshark Serta Metode Penetration Testing Kali Linux. Journal on Education, 4(4), pp.1470-1476.

[11] Dayan, R., Muhyidin, Y., Singasatia, D., 2023. Analisis Keamanan Jaringan Pada Wireless Local Area Network Terhadap Serangan Brute Force Menggunakan Metode Penetration Testing. JATI (Jurnal Mahasiswa Teknik Informatika), 7(3), pp.2051-2056.

[12] Fauzan, M. F., Irawan, A. S. Y., 2021. Wireless Attack : Menggunakan Tools Aircrack Pada Kali Linux Untuk Melakukan WPA Attack. Jurnal LENTERA (Kajian Keagamaan, Keilmuan dan Teknologi). 20(1), pp.63-74.