Jurnal Rekayasa Sistem Informasi dan Teknologi
Volume 2, No 2 – November 2024
e-ISSN : 3025-888X

ANALISIS KEAMANAN JARINGAN WIRELESS MENGGUNAKAN METODE PENETRATION TESTING DI SMK BANGUN NEGERI HU'U

Nurfanis[1], Zaenudin[2], Muhamad Masjun Efendi[3]
[123]Program studi teknologi informasi, fakultas teknologi informasi dan komukasi
nurfanismulyana03@gmail.com, Zen3d.itb@gmail.com, creativepio@gmail.com

Received: 22-09- 2024	Revised: 10-10-2024	Approved: 20-11-2024

ABSTRAK

Perkembangan teknologi jaringan saat ini sangat berkebang pesat sehingga memungkinkan banyak orang yang menyalahgunakan teknologi itu sendiri. Contohnya wireless local area network (wlan). Jaringan wireless adalah salah satu teknologi media transmisi nirkabel yang sering digunakan oleh semua orang, penelitian ini menggunakan metode penetration testing yang bertujuan untuk menganalisis keamanan jaringan wireless yang sistem keamanannya menggunakan OPN dan WPA2, dalam menganalisis jaringan wireless menggunakan sistem operasi kali linux yang lebih spesifik dalam hal penetration testing. Hasil dari pengujian ini menunjukkan bahwa keamanan jaringan di SMK Bangun Negeri Hu'u, masih memiliki celah yang dapat memberikan peluang kepada hacker. Dibuktikan dengan dua jenis serangan yang dilakukan keduanya berhasil di keamanan OPN dan WPA2 yaitu serangan cracking the encryption dan attacking the infrastrukture.
***Kata kunci** : wifi, sandi, keamanan, OPN, dan WPA2*

ABSTRACT

The development of network technology is currently developing very rapidly, making it possible for many people to misuse the technology itself. For example, wireless local area network (WLAN). Wireless networks are one of the wireless transmission media technologies that are often used by everyone, this research uses the penetration testing method which aims to analyze the security of wireless networks whose security systems use OPN and WPA2, in analyzing wireless networks using the Kali Linux operating system which is more specific in penetration testing matters. The results of this test show that network security at Bangun Negeri Hu'u Vocational School still has gaps that could provide opportunities for hackers. This is proven by the two types of attacks that were carried out both successfully on OPN and WPA2 security, namely attacks cracking the encryption and attacking the infrastructure.
Keywords: wifi, password, security, OPN, and WPA2.

PENDAHULUAN

Keamanan jaringan sangat vatal bagi keamanan jaringan *computer.* Kelemahan – kelemahan yang terdapat pada jaringan *computer* jika tidak di lindungi dan di jaga dengan baik akan menyebabkan hak akses bagi siapa saja tanpa di ketahui, kerugian berupa kehilangan data yang tidak dapat di baca tidak dapat di gunakan oleh aplikasi atau pengguna, kerusakan *system server* yang mengakibatkan tidak tersedianya *fungsionalitas* layanan yang di sediakan, tidak maksimal dalam melayani *user* atau bahkan kehilangan aset-aset berharga *institusi* pada SMK bnagun negeri itu sendiri.

SMK bangun negeri hu'u merupakan salah satu Lembaga Pendidikan di kecamatan hu'u yang menggunakan *teknologi wireless* untuk keperluan belajar mengajar, salah satu mata pelajaran TIK (teknologi informasi dan komukasi) yang berlangsung di *Lab computer* sekolah.

Namun karena *system* keamanan jaringan *wireless* masih kurang , menyebabkan sering terjadinya pembobolan password wifi di sekolah, bukan hanya data sekolah tapi juga data pengguna tersebut, inilah yang sering kita kenal dengan sebutan *cyber crime .*
Di karenakan mudahnya di serang oleh *hecker* untuk melakukan aksinya melalui jaringan *wireless* lebih rentan di bandingkan jarigan kabel, maka di butuhkan sebuah

metode untuk melakukan uji coba jaringa *wireless*, apakah jaringan tersebut sudah sesuai dengan *standart* atau belum (adigunawan dan widadgo 2022).

LANDASAN TEORI

Jaringan computer adalah sebuah Kumpulan dari banyak perangkat,seperti *computer,hub,switch, router* atau peralatan jaringan lainnya yang terkoneksi media komukasi tertentu. Jaringan komputer sangat penting untuk mencari kerusakan jaringan dengan cepat dan sederhana.

Kombinasi teknologi kabel dan *nirkabel* juga dapat di gunakan untuk membuat jaringan komputer. Perangkat jaringan berkomukasi memalui media transmisi kabel atau *nirkabel* jaringan dapat bersifat *private* atau *public.* Jaringan *private* biasanya mengharuskan pengguna memasukkan *kredesial* untuk mengakses jaringan, biasanya ini di sediakan secara manual oleh *administrator* jaringan, atau langsung di peroleh oleh pengguna melalui kata sandi atau *kredensial* lainyan. Jaringan publik seperti internet tidak membatasi akses (Hasibuan & Elhanafi, 2022)

jenis jaringa komputer berdasarkan media transmisi

a) Jaringan kabel
   Adalah jaringan yang digunakan dari satu komputer ke komputer lainnya, diperlukan kabel jaringan. Kabel jaringan mengirimkan informasi dalam bentuk sinyal elektronik atau komputer berjaringan.(Spanning et al., 2020)
b) Jaringan nirkabel
   Jaringan nirkabel adalah sebuah jaringan yang menggunakan gelombang radio sebagai media transmisi dan dipancarkan.

Kali Linux

Kali linux merupakan operation system berbasis *linux debian* yang di kembangkan oleh *offensive security. User interface* dari *kali linux* memiliki tampilan *graphical user interface (GUI)* yang sederhana dan tidak terlalu mencolok, *kali linux,* selain terdapat di PC, juga dapat di intalasi dan diinstalasi pada sistem *android* yang disebut *kali nethunter* yang memiliki fungsi dan fitur yang sama.

Fitur-fitur dari *kali linux* adalah sebagai berikut:

a) *Tools penetration testing >300*
b) *Free licensed*
c) Mengikuti *FHS complaint*
d) *Support* perangkat *wireless*
e) *IDE* yang aman
f) *Support* dengan banyak bahasa

Aircrack

Aircrack-ng adalah rangkaian aplikasi yang dapat digunakan untuk mengevaluasi dan mengukur tingkat keamanan jaringan wifi. *Aircrack* bekerja pada jaringan wifi yang mendukung mode pemantauan dan dapat mendeteksi lalu lintas jaringan dari 80211a, 802.11b dan 802.11g. Fungsi dari *aircrack* ini adalah pemantauan, menyerang, pengujian dan *cracking.*(Chandra & Azis, 2021)

Hashchat

Hashchat adalah alat peretas kata sandi dengan *hash MD5,* lalu didukung oleh *wordlist* yang besar.

Mancchanger

Macchanger adalah salah satu dari banyak aplikasi pengganti *MAC Address* yang umum digunakan. Penggunaan *macchanger* hanya bersifat sementara, karena *MAC Address* akan Kembali normal setelah komputer di *restart.*(No et al., 2023)

DDos Attack

DDoS Attack adalah serangan yang sangat popular digunakan oleh peretas. Selain memiliki beberapa jenis, *DDoS* juga memiliki konsep yang sangat sederhana, meskipun *trafik server* berjalan dengan beban tinggi, hingga tidak dapat lagi menampung koneksi dari pengguna lain *(overload).*

Brute Force Attack

Salah satu kelemahan yang diketahui dalam *WPA2-PSK* adalah ketika *clien* terhubung ke titik akses di mana proses jabat tangan terjadi. Dengan mendapatkan paket jabat tangan, peretas dapat melakukan *brute force*

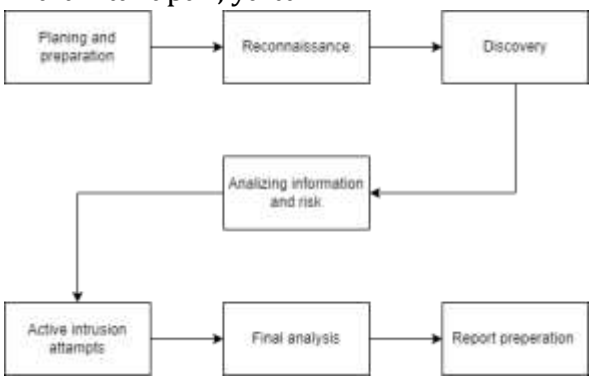
METODOLOGI PENELITIAN

Jenis Penelitian

Jenis penelitian yang digunakan dalam penelitian ini adalah penelitian kualitatif. Alasan pemilihan metode penelitian kualitatif adalah karena penelitian kualitatif bersifat deskriptif, sering menggunakan analisis, dan membuat proses penafsirannya lebih terlihat. Penelitian kualitatif adalah penelitian yang berbasis penelitian yang informasi dan kesimpulannya diperoleh dari hasil interaksi langsung antara peneliti, objek penelitian, dan populasi tempat penelitian dilakukan.

Metode kualitatif memperlakukan partisipan sebagai subjek bukan objek sehingga partisipan menganggap dirinya berharga karena informasi dari mereka sangat bermanfaat.

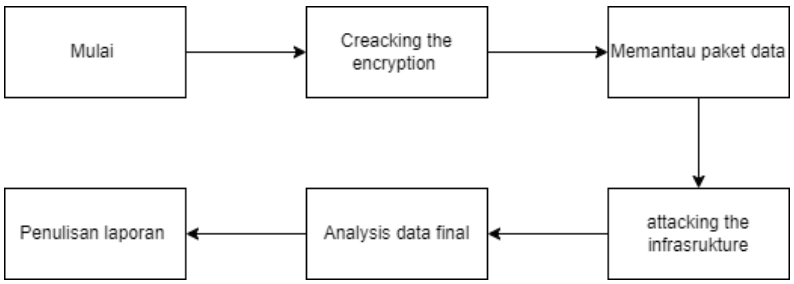
Pentesting (PenetrationTesting) adalah metode eksekusi evaluasi keamanan sistem dan jaringan komputer. Penilaian tersebut diselesaikan dengan melakukan simulasi serangan *(attack).* Kegiatan ini biasa disebut sebagai *"ethical hacking".* Metode *pentesting* memiliki alur tahapan, yaitu:



Gambar 1 diagram alur penetration testing

Tahapan Penelitian

Tahapan penelitian merupakan proses atau gambaran proyek yang akan penulis kerjakan. Penulis mengumpulkan informasi berdasarkan jurnal yang ditemukannya, sehingga mendapatkan informasi yang benar untuk memudahkan penulis dalam melakukan penelitian.Diagram di bawah menunjukkan tahapan penyelidikan.



Gambar 2 Diagram Tahapan Penelitian

HASIL PENGUJIAN

Tahap implementasi merupakan salah satu tahap penerapan agar dapat berfungsi sesuai dengan kebutuhan dan perancangan sebelumnya. Selain itu juga pada implementasi ini akan dijelaskan bagaimana ini akan bekerja. Adapun *hardware* yang digunakan antara lain *PC* yang berfungsi sebagai tempat instalasi *Kali Linux.* Sedangkan *software* yang digunakan adalah *Aircrack-ng* dan *DDoS* untuk melakukan serangan pengujian.

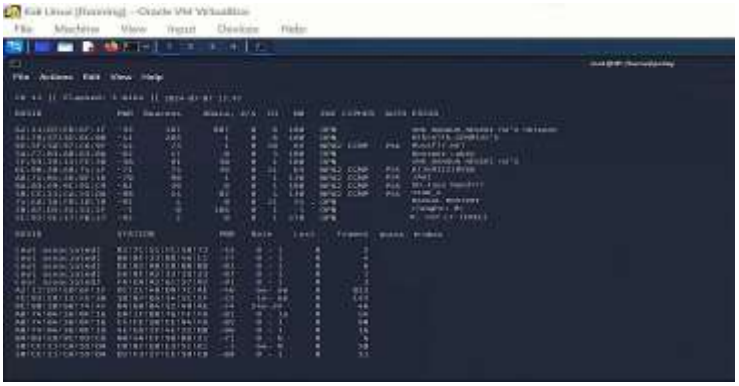
Tabel 1 hasil pengujian

Jenis serangan	Informasi yang dibutuhkan	Status keamanan OPN	Status keamanan WPA2-PSK
Cracking the encryption	*Channel* yang digunakan dan *BSSID* dari *access point.*	Berhasil	Berhasil
Attacking The Infrastructure	*Attacker* harus berada dalam jangkauan jaringan *Wireless*, *MAC Address* dari perangkat *Tester*.	Berhasil	Berhasil

Hasil dari pengujian *Cracking The Encryption* pada tabel 1 diatas adalah terdapat informasi mengenai *channel* yang digunakan dan *BSSID dari access point serta enkripsi* yang digunakan atau keamanan.

Keamanan *OPN*

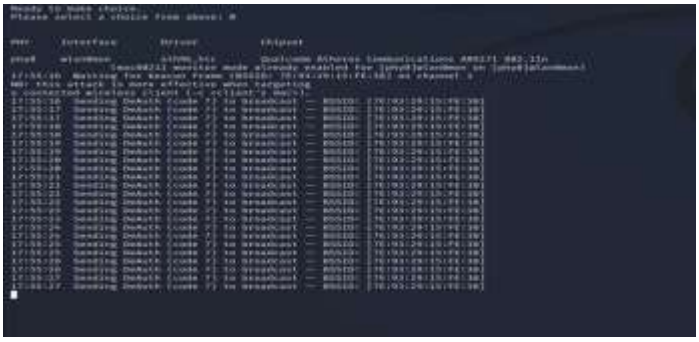
Tahapan pertama yang dilakukan adalah *scanning (Cracking The Encryption)* jaringan *wireless* yang ada disekitarnya, dimana tujuan dari serangan ini adalah untuk mengetahui apakah semu *Access Point* dilindungi dengan sistem keamanan enkripsi seperti *WEP, WPA* ataupun *WPA2,*



Gambar 1 *scanning* informasi jaringan

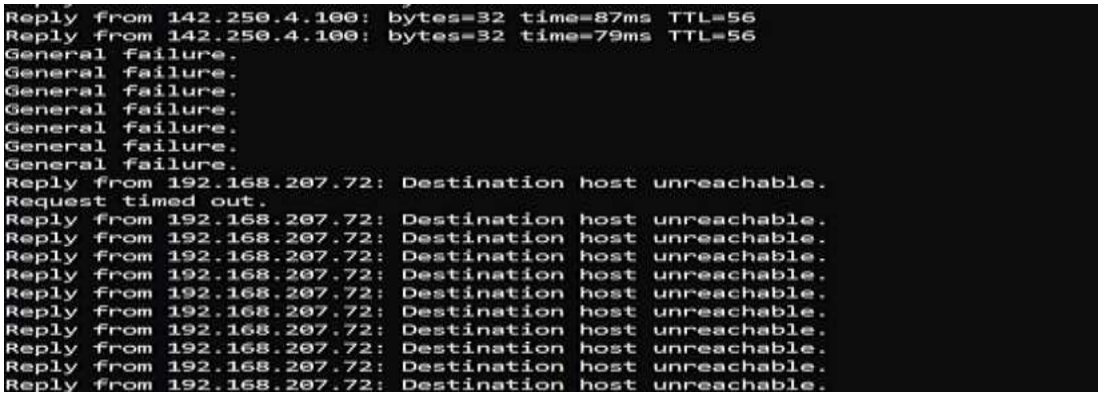
Pada gambar 2 Ketika akan menjalankan serangan, peneliti menjalankan *script* yang sudah dibuat terlebih dahulu, bisa kita lihat perintah yang di gunakan yaitu *sudo python3 wifidos.py* dimana ini digunakan untuk menjalankan script yang sudah kita buat terlebih dahulu, jadi disana terdapat *wlan0* yang nomornya 0. Pada tahap selanjutnya memilih *wlan0* ini dilakukan untuk mempermudah penyerengan.

Gambar 3 memilih jaringan yang akan di serang



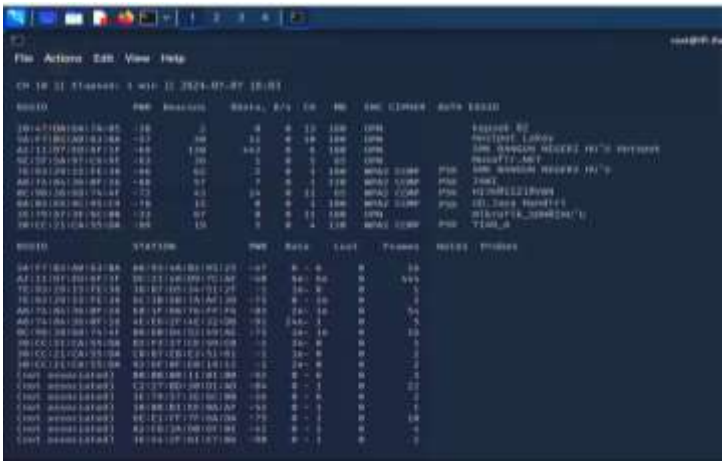
Gambar 4 serangan sedang berlangsung

Pada proses penyerangan terhadap *wireless* yang dituju, selanjutnya, terdapat gangguan atau putus koneksi pada koneksi *PC tester* dan untuk memasikan koneksi sampai benar-benar terputus, ini memerlukan waktu untuk bisa memutuskan koneksi pada *PC tester.*



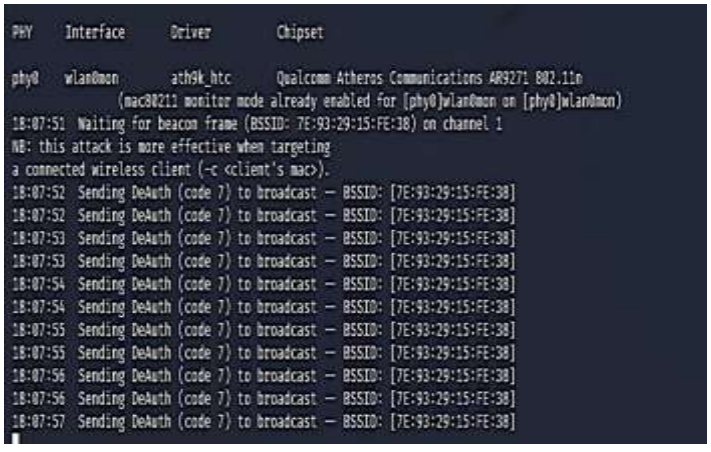
Gambar 5 dampak serangat *Ddos Attack*

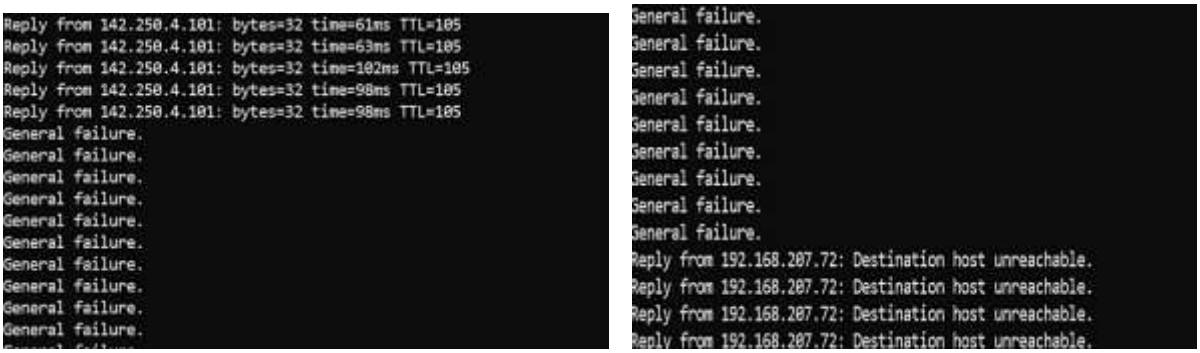
Pada bagian pengujian keamanan *WPA2/PSK* Sama seperti pada serangan keamanan *OPN* yang pertama dilakukan yaitu *scanning* jaringan untuk melihat informasi jaringan terdekat yang akan diteliti, seperti pada gambar 6.



Gambar 6 *scanning* informasi jaringan

Untuk melihat atau mengecek, apakah koneksi *user* terganggu atau terputus dari jaringan, bisa dilihat melalui *CMD*





Gambar 7 serangan *Ddos Attack* sedang berlangsung

ANALISIS HASIL

Dari hasil yang di peroleh terlihat bawa lamanya waktu serangan yang dibutuhkan hingga terputusnya koneksi user terhadap jaringan dipengaruhi oleh jarak antara komputer tester dan user, juga dipengaruhi oleh banyaknya target yang akan di serang maka semakin lama waktu yang dibutuhkan untuk melakukan serangan terhadap target.

Tabel 2 keamanan *OPN*

Jenis Serangan	Informasi Yang Di Butuhkan	Status Keamanan OPN
Cracking The Encryption	Channel yang digunakan dan BSSID dari access point.	Berhasil
Attacking The Infrastructure	Attacker harus berada dalam jangkauan jaringan Wireless, MAC Address dari perangkat tester.	Berhasil

Tabel 3 Keamanan *WPA2-PSK*

Jenis Serangan	Informasi Yang Di Butuhkan	Status Keamanan Wpa2/Psk
Cracking The Encryption	Channel yang digunakan dan BSSID dari access point.	Berhasil
Attacking The Infrastructure	Attacker harus berada dalam jangkauan jaringan Wireless, MAC Address dari perangkat tester.	Berhasil

KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan selama perancanga sampai Analisa Keamanan Jaringan *Wireless* SMK Bangun Negeri Hu'u dengan Metode *Penetration Testing* dengan menggunakan serangan *(Cracking The Encryption, Attacking The Infrastructure,* dan *Carcking Password)* menggunakan *Kali Linux ,Tools Aircrack dan Script David Bombal*, pada jaringan *wireless* SMK Bangun Negeri Hu'u, maka dapat diambil kesimpulan bahwa keamanan yang dimiliki oleh jaringan *wireless* SMK Bangun Negeri Hu'u masih kurang pada keamanan *OPN.* Hal ini dibuktikan dengan hasil penelitian yang dilakukan bahwa dari tiga jenis serangan yang dilakukan, ketiganya berhasil. Dan juga keamanan OPN bebas memberikan akses kepada siapa saja, hal ini memberikan peluang kepada seorang *hacker.* Sedangkan keamanan *WPA2* memiliki tingkat keamanan yang lebih kuat, karena harus menggunakan *password* untuk bisa masuk ke jaringan.

DAFTAR PUSTAKA

Access, P., Key, S., Access, W. P., & Key, S. (2021). *ANALISIS PERBANDINGAN SISTEM KEAMANAN JARINGAN WI-FI*. *09*(01), 108–118.

Adiguna, M. A., Widagdo, B. W., & Masalah, A. L. B. (2022). *Analisis Keamanan Jaringan Wpa2-Psk Menggunakan Metode Penetration Testing (Studi Kasus : Router Tp-Link Mercusys*. *5*.

Amuda, S., Mulya, M. F., & Kurniadi, F. I. (2021). *Analisis dan Perancangan Simulasi Perbandingan Kinerja Jaringan Komputer Menggunakan Metode Protokol Routing Statis , Open Shortest Path First (OSPF) dan Border Gateway Protocol (BGP) (Studi Kasus Tanri Abeng University)*. *IV*(2).

Chandra, Y. I., & Azis, N. (2021). *Wireless Network Security Using WEP (Wired Equivalent Privacy) Method With RC4 Stream Cipher Encryption*. *1*, 61–67.

Hasibuan, M., & Elhanafi, A. M. (2022). *Penetration Testing Sistem Jaringan Komputer Menggunakan Kali Linux Untuk Mengetahui Kerentanan Keamanan Server Dengan Metode Black Box*.

No, V., Hal, J., & Setiawan, P. (2023). *Rancang Bangun Jaringan Wireless Local Area Network (WLAN) menggunakan Microtik dan Routing Statik pada MTs Al Barokah Poncowarno Lampung Tengah*. *1*(2), 85–93.

Rusdi, M. I., & Prasti, D. (2019). *Penetration Testing Pada Jaringan Wifi Menggunakan Kali Linux*.

Saputra, S. G., Kom, S., Saputra, S. G., & Zen, B. P. (2023). *Analisis Keamanan Jaringan Wireless menggunakan Metode Penetration Testing Execution Standard (PTES)*. *1*(2), 43–51.

Satria, A., & Ramadhani, F. (2023). *Keamanan Jaringan Komputer Menggunakan Switch Port Security Pada Cisco Packet Tracer*.

Susanto, M. I., Hasad, A., & Bakri, M. A. (n.d.). *Sistem Proteksi Jaringan Wlan Terhadap Serangan Wireless Hacking*. *7*(1), 25–34.

Wahyudi, E., Luthfi, E. T., & Efendi, M. M. (2019). *Jurnal Explore STMIK Mataram – Volume 9 No 1 Tahun 2019 Wireless Penetration Testing Method To Analyze WPA2-PSK System Security And Captive Portal ISSN : 2087-894 Jurnal Explore STMIK Mataram – Volume 9 No 1 Tahun 2019 ISSN : 2087-894*. *9*(1), 1–7.

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

Subli, M. (2020). Implementasi Aplikasi User Manager Mikrotik Berbasis Web Pada Sma Negeri 7 Mataram. *Explore*, *10*(2), 12. https://doi.org/10.35200/explore.v10i2.374

Kholiq, A., & Khoirunnisa, D. (2019). Analisis Keamanan Wireless Local Area Network (WLAN) dengan Metode Penetration Testing Execution Standard (PTES) (Studi Kasus: PT. Win Prima Logistik). *Jurnal Ilmiah Fakultas Teknik LIMIT'S*, *1*(1), 46–55. https://teknik.usni.ac.id/jurnal/ABDUL KHOLIQ.pdf

Haeruddin, H., & Kurniadi, A. (2021). Analisis Keamanan Jaringan WPA2-PSK Menggunakan Metode Penetration Testing (Studi Kasus: TP- Link Archer A6). *CoMBInES-Conference on Management …*, *1*(1), 508–515. https://journal.uib.ac.id/index.php/combines/article/view/4475

Kholiq, A., & Khoirunnisa, D. (2019). Analisis Keamanan Wireless Local Area Network (WLAN) dengan Metode Penetration Testing Execution