OKTAL : Jurnal Ilmu Komputer dan Science
Volume 3, No. 9, September 2024
ISSN 2828-2442 (media online)
Hal 2250-2259

Implementasi Peretasan Dan Pengamanan Ssid Pada Jaringan Mikrotik RB941-2ND Dengan Metode *Deauther* dan *Evil Twin*

Ziska Andris[1*], Jaka Sutresna[1]

[1]Fakultas Ilmu Komputer, Teknik Informatika, Universitas Pamulang, Jl. Raya Puspiptek No. 46, Kel. Buaran, Kec. Serpong, Kota Tangerang Selatan. Banten 15310, Indonesia
Email: [1*]ziska.andris32@email.com, [2]dosen00833@unpam.ac.id

Abstrak− Internet dan website telah menjadi kebutuhan yang sangat penting bagi perorangan, organisasi, perusahaan, dan instansi pemerintah. Karena besarnya kebutuhan dunia akan internet dan website, serta pengaruh yang diberikan bagi seluruh kalangan, maka memahami manfaat internet dan website sangatlah penting. Keamanan teknologi informasi menjadi suatu hal yang sangat penting saat ini. Hal ini dimaksudkan guna menjamin keamanan terhadap seluruh informasi yang dikirim ataupun disimpan melalui internet tidak bisa diakses sembarangan oleh pihak yang tidak bertanggung jawab. Internet diakses oleh banyak orang tanpa terkecuali *hacker* dan *cracker*. Dengan alasan tertentu mereka melakukan penyusupan yang dapat merugikan para pemilik server dan jaringan komputer. Kecanggihan serangan dan *tools* pada jaringan komputer berbanding terbalik dengan pengetahuan tentang penyusupan pada jaringan komputer. peneliti mencoba untuk membuat suatu penelitian yang bermanfaat, peretasan ini menggunakan metode *deauther* dan *evil twin* dalam peretasan jaringan wifi. Perancangan penelitian ini berbasis *microcontroller*, alat yang digunakan penulis adalah NodeMCU untuk target peretasannya menggunakan MikroTik RB941-2ND, kemudian mengimplementasikan Simulasi Peretasan Dan Pengamanan Jaringan Mikrotik Rb941-2nd Dengan Metode *Deauther* Dan *Evil Twin*. Hasil dari penelitian ini didapatkan bawha Keduanya adalah teknik yang dapat digunakan untuk mengancam keamanan jaringan nirkabel. Mencegah serangan *Evil Twin* melibatkan waspada terhadap jaringan yang Anda sambungkan dan menghindari jaringan nirkabel yang tidak dikenal. Sementara itu, mencegah serangan *Deauther* dapat melibatkan penggunaan alat atau perlindungan keamanan tambahan yang dapat mendeteksi dan merespons serangan semacam itu untuk menjaga konektivitas perangkat Anda. Berdasarkan hasil penelitian yang sudah dilakukan maka kesimpulan yang di simpulkan adalah Peneliti mampu meretas dan melakukan keamanan pada jaringan internet di lingkungan RT 001 dengan atau tanpa *password* yang kuat, melakukan implementasi perakitan alat mikrokontroler yang saat ini dengan mudah didapatkan pada pasaran, dan mampu mencegah peretasan jaringan RT.001 dengan router MikroTik RB941-2ND dan upaya penelitian mengenai pemanfaatan kelalaian manusia dalam meretas jaringan nirkabel sambil mengedukasi masyarakat tentang keamanan siber dan cara merespons gangguan peretas.

Kata Kunci: Peretasan, Pengamanan Jaringan, Mikrotik RB941-2ND, Metode *Deauther* dan *Evil Twin*

Abstract− *The internet and websites have become a very important need for individuals, organizations, companies and government agencies. Because of the world's great need for the internet and websites, as well as the influence it has on all groups, understanding the benefits of the internet and websites is very important. Information technology security is very important nowadays. This is intended to ensure the security of all information sent or stored via the internet and cannot be accessed carelessly by irresponsible parties. The internet is accessed by many people, including hackers and crackers. For certain reasons, they carry out intrusions that can harm server and computer network owners. The sophistication of attacks and tools on computer networks is inversely proportional to knowledge about intrusions on computer networks. The researcher tries to make useful research, this hack uses the deauther and evil twin method in hacking WiFi networks. The design of this research is microcontroller based, the tool used by the author is NodeMCU for the hacking target using the MikroTik RB941-2ND, then implementing the Hacking and Network Security Simulation of the Mikrotik Rb941-2nd Using the Deauther and Evil Twin Method. The results of this research show that both are techniques that can be used to threaten the security of wireless networks. Preventing Evil Twin attacks involves being aware of the networks you connect to and avoiding unknown wireless networks. Meanwhile, preventing Deauther attacks may involve using additional security tools or protections that can detect and respond to such attacks to maintain the connectivity of your devices. Based on the results of the research that has been carried out, the conclusion that can be concluded is that the researcher was able to hack and carry out security on the internet network in the RT 001 environment with or without a strong password, implemented the assembly of microcontroller tools which are currently easily available on the market, and was able to prevent hacking. RT.001 network with a MikroTik RB941-2ND router and research efforts regarding the use of human error in hacking wireless networks while educating the public about cyber security and how to respond to hacker intrusions.*

Keywords*: Hacking, Network Security, Mikrotik RB941-2ND, Deauther and Evil Twin Methods*

OKTAL : Jurnal Ilmu Komputer dan Science
Volume 3, No. 9, September 2024
ISSN 2828-2442 (media online)
Hal 2250-2259

1. PENDAHULUAN

Internet dan website telah menjadi kebutuhan yang sangat penting bagi perorangan, organisasi, perusahaan, dan instansi pemerintah. Karena besarnya kebutuhan dunia akan internet dan *website*, serta pengaruh yang diberikan bagi seluruh kalangan, maka memahami manfaat internet dan website sangatlah penting. (Maharani dkk, 2021).

Dilansir dari *website* IlmuKomputer.Com Jaringan *wireless* sangatlah rentan terhadap serangan, hal ini dikarenakan jaringan *wireless* tidak dapat dibatasi oleh sebuah gedung seperti yang diterapkan pada jaringan berbasis kabel. Sinyal radio yang dipancarkan oleh perangkat *wireless* dalam melakukan proses transmisi data didalam sebuah jaringan dapat dengan mudah diterima / ditangkap oleh pengguna komputer lain selain pengguna dalam satu jaringan hanya dengan menggunakan perangkat yang kompatibel dengan jaringan wireless seperti kartu jaringan *wireless*. *Hacker* biasanya mencari jaringan *wireless* LAN untuk menonaktifkan atau berusaha untuk mendapatkan akses masuk ke jaringan *wireless* LAN melalui berbagai cara.

Berdasarkan observasi yang dilakukan di Perumahan Puri Harmoni Cikasungka RT.001 Kecamatan Solear, Kabupaten Tangerang. pada hari Kamis tanggal 14 September 2023, hasil yang diperoleh di lingkungan RT.001 pernah beberapa kali mengalami gangguan Internet, Saat menggunakan *router* MikroTik RB941-2ND, RT.001 menjelaskan bahwa jaringan tiba-tiba berhenti berfungsi dan kecepatan Internet tiba-tiba melambat.dan RT.001 mengetahui dan tidak menduga gangguan tersebut disebabkan oleh peretasan, cuaca atau hal lainnya karena menurut informasi mereka tidak curiga karena *router* menggunakan *password* yang cukup kuat. Karena peretasan jaringan, bekerja di lingkungan RT.001 mengalami kendala dan penundaan saat menggunakan Internet. Berdasarkan informasi yang ada, gangguan tersebut disebabkan oleh seseorang yang mencoba meretas kata sandinya. Lalu peneliti mensosialisasikan tentang adanya peretasan jaringan kepada pihak RT.001 dan bertanya apakah bapak tau tentang *deauther attack* dan *evil twin attack*, lalu pihak RT.001 menjawab, tidak tahu dan tidak penah dengar istilah seperti itu. Tindakan yang dapat dilakukan jika terjadi peretasan jaringan disana adalah cukup dengan mengganti kata sandi secara berkala.

Dari uraian latar belakang diatas, maka penulis mencoba untuk membuat suatu penelitian yang bermanfaat, peretasan ini menggunakan metode *deauther* dan *evil twin* dalam peretasan jaringan wifi. Perancangan penelitian ini berbasis *microcontroller*, alat yang digunakan penulis adalah NodeMCU untuk target peretasannya menggunakan MikroTik RB941-2ND. Oleh karena itu maka penulis mengambil judul "Implementasi Simulasi Peretasan Dan Pengamanan Jaringan Mikrotik Rb941-2nd Dengan Metode *Deauther* dan *Evil Twin*".

2. METODOLOGI PENELITIAN

2.1 Observasi

Teknik observasi ini dilakukan dengan mengunjungi lokasi studi kasus dan mengamati langsung permasalahan yang terjadi di komplek perumahan Puri Harmoni Cikasungka. Tujuan observasi ini adalah untuk mengumpulkan informasi mengenai isu-isu terkini untuk memudahkan penyusunan laporan.

2.2 Wawancara

Wawancara ini dilakukan dengan melakukan wawancara terhadap warga RT.001 untuk menjelaskan permasalahan dan permasalahan yang terjadi di perumahan Puri Harmoni Cikasungka.

2.3 Metode Studi Pustaka

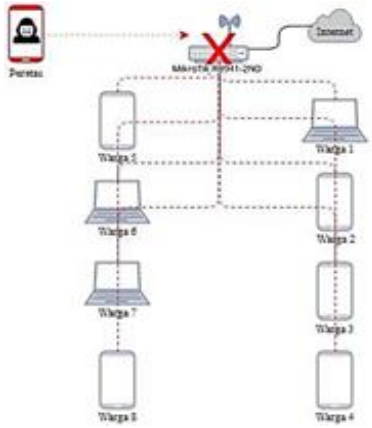
Pengumpulan data dan informasi tertulis maupun secara teoritis dan empiris yang terkait dengan topik penelitian. Selain itu studi pustaka yang dilakukan peneliti pengumpulan bahan bahan yang terkait dengan judul skripsi melalui buku-buku bacaan dan situs internet, penelitian yang terkait dengan penelitian yang sedang dikembangkan sehingga dapat dimplementasikan dalam penelitian ini.

OKTAL : Jurnal Ilmu Komputer dan Science
Volume 3, No. 9, September 2024
ISSN 2828-2442 (media online)
Hal 2250-2259

3. ANALISA DAN PEMBAHASAN

3.1 Analisa Jaringan Berjalan

Menganalisis jaringan aktif bertujuan untuk mengetahui lebih jelas bagaimana jaringan beroperasi dan permasalahan apa saja yang dihadapi sehingga dapat dibuat rekomendasi perancangan jaringan.



Gambar 1. Analisa Jaringan Berjalan

Pada saat ini masyarakat warga hanya menyambungkan internet dengan jaringan RT 001 hanya menggunkan wifi dan siapapun bahkan warga yang bukan RT001 dapat melihat SSID atau nama pada jaringan ini. Maka peretas dapat juga melihat SSID tersebut.

3.2 Topologi Jaringan Berjalan

Topologi jaringan yang berjalan menggunakan topologi *Basic Service Set (BSS)*, karena tujuannya adalah agar konektivitas antar *router client* pada topologi ini disediakan oleh perangkat *router*. Setiap klien nirkabel yang ingin terhubung ke klien lain harus terhubung terlebih dahulu ke titik akses yang digunakan.

3.3 Arsitektur Jaringan Berjalan

Arsitektur jaringan yang ada pada router MikroTik RB941-2ND membuka SSID nya ke area publik dan dapat di akses oleh siapapun yang belum terhubung pada jaringan tersebut, dan frekuensi nya masih menggunakan 2.4Ghz yang berdampak akan terlihat oleh alat NodeMCU milik peretas, efek dari terbukanya SSID dan frekuensi 2.4Ghz maka bisa terserang dengan metode *Deauther* dan *EvilTwin* menjadikan semua yang terhubung pada jaringan tersebut akan lumpuh atau putus koneksi, dan peretas membuat jaringan tiruan untuk mengelabui para *user* agar membingungkan dan susah membedakan jaringan wifi yang asli atau bukan. Dan bahayanya peretas jika mendapat akses ke *router MikroTik RB941-2ND* bisa mengatur konfigurasi di dalam tersebut.

3.4 Usulan Analisa Jaringan

Setelah menganalisis jaringan yang berjalan ini, penulis mengusulkan untuk melakukan penelitian implementasi peretasan jaringan menggunakan tool NodeMCU dengan teknik pengujian penetrasi, metode *deauther* dan *evil twin* pada router MikroTik RB941-2ND. karena jaringan pada router semakin tidak aman jika SSID ditampilkan di area publik.

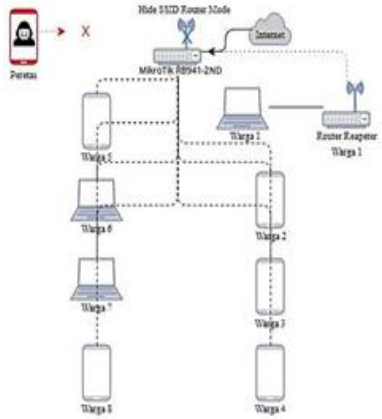
3.5 Topologi Jaringan Berjalan

Extend Service Set, karena tujuannya untuk menjangkau domain yang lebih luas. Oleh karena itu, topologi *ESS* dapat dikatakan merupakan gabungan atau kumpulan topologi *BSS*. Pada topologi *BSS* atau *ESS* dapat digabungkan dengan jaringan kabel. Koneksi ini sering disebut sebagai infrastruktur, dimana klien nirkabel dapat terhubung dan berkomunikasi dengan klien lain di jaringan kabel.

OKTAL : Jurnal Ilmu Komputer dan Science
Volume 3, No. 9, September 2024
ISSN 2828-2442 (media online)
Hal 2250-2259

3.6 Pengujian Sistem

Menghadapi permasalahan yang ada, penulis memberikan rekomendasi konfigurasi jaringan untuk MikroTik RB941-2ND. Berikut ini adalah diagram jaringan yang diusulkan.



Gambar 2. Skema Jaringan Usulan

Pada jaringan usulan yang di lakukan peneliti adalah melakukan konfigurasi topologi BSS dan ESS yang dimana jaringan yang tersambung pada wifi RT001 telah Sebagian menggunakan kabel dan Sebagian masih menggunakan wifi, tetapi jaringan SSID telah di nonaktifkan boardcastnya atau di hidden, agar peretas tidak mampu scanning nama jaringan RT001 lagi.

3.7 Konfigurasi Perangkat Penelitian

Gambar 3. Diagram Proses Konfigurasi NodeMCU dan MikroTik

OKTAL : Jurnal Ilmu Komputer dan Science
Volume 3, No. 9, September 2024
ISSN 2828-2442 (media online)
Hal 2250-2259

4. IMPLEMENTASI

4.1 Implementasi NodeMCU (board v.3 Lolin) ESP8266

Gambar 4. NodeMCU ESP8266

Gambar 5. NodeMCU

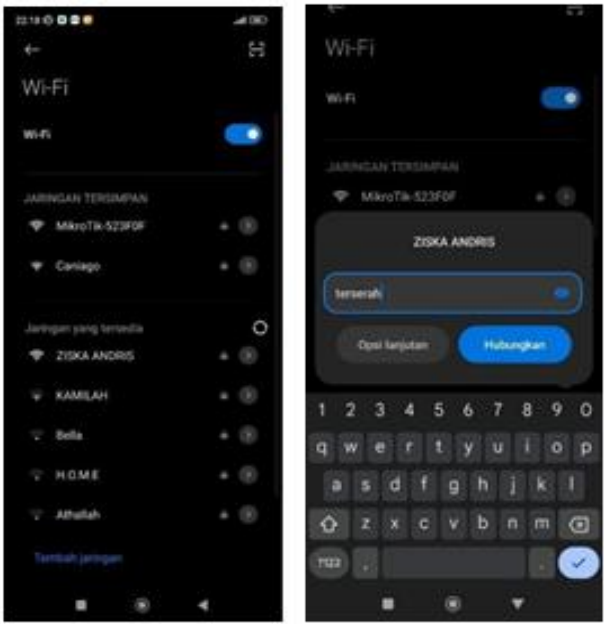
4.2 Implementasi Pengujian

Pada penelitian ini penulis melakukan pengujian peretasan dan pengamanan, menggunakan mikrokontroler NodeMCU pada MikroTik RB941-2ND untuk menguji jaringan.

4.3 Implementasi Peretasan

Dalam implementasi penelitian ini penulis melakukan peretasan dengan mikrokontroller NodeMCU menggunakan teknik metode *deauther* dan *evil twin* untuk menguji jaringan MikroTik RB941-2ND.

a. Masuk Wifi NodeMCU ZISKA ANDRIS



Gambar 6. Masuk Wifi NodeMCU ZISKA ANDRIS

OKTAL : Jurnal Ilmu Komputer dan Science
Volume 3, No. 9, September 2024
ISSN 2828-2442 (media online)
Hal 2250-2259

b. Halaman Utama Menu Peretasan

Gambar 7. Halaman Utama Menu Peretasan

c. Pilih Jaringan yang akan di Retas

Gambar 8. Pilih Jaringan yang akan di Retas

d. Peretasan Dengan Metode *Deauther*

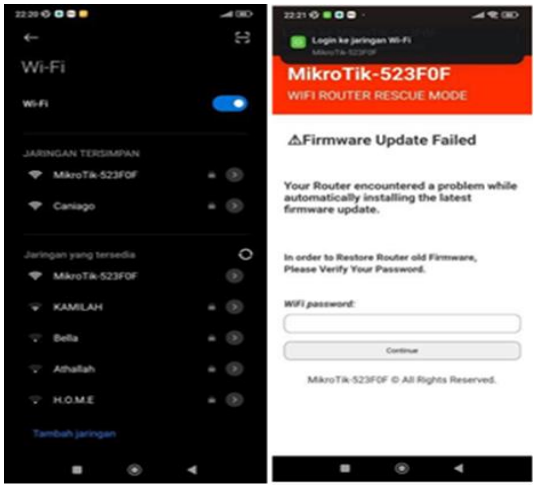
Gambar 9. Peretasan Dengan Metode *Deauther*

OKTAL : Jurnal Ilmu Komputer dan Science
Volume 3, No. 9, September 2024
ISSN 2828-2442 (media online)
Hal 2250-2259

e. Peretasan Dengan Metode *Evil Twin*

Gambar 10. Peretasan Dengan Metode *Evil Twin*

f. Tampilan Menu Jaringan Palsu



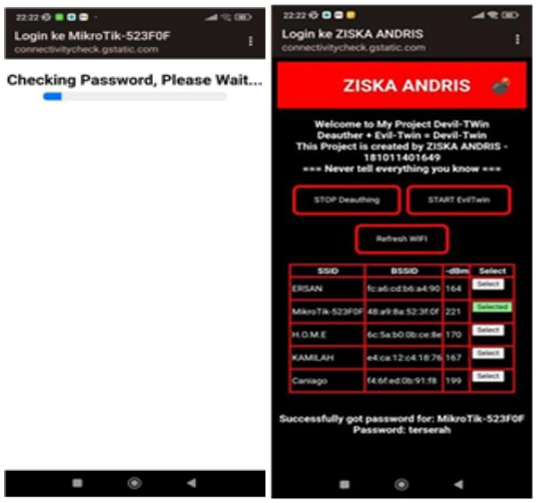
Gambar 11. Tampilan Menu Jaringan Palsu

g. Tampilan *User* Terjebak Peretasan

Gambar 12. Tampilan *User* Terjebak Peretasan

OKTAL : Jurnal Ilmu Komputer dan Science
Volume 3, No. 9, September 2024
ISSN 2828-2442 (media online)
Hal 2250-2259

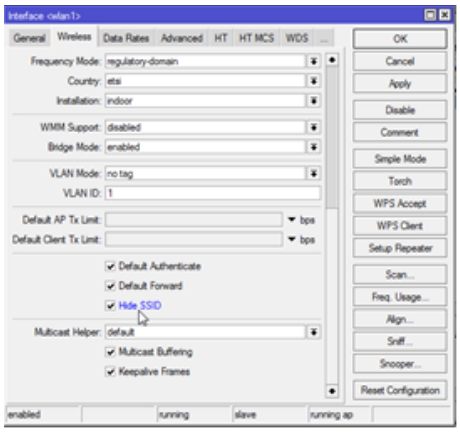
h. Tampilan Proses Mendapatkan *Password* Jaringan



Gambar 13. Tampilan Proses Mendapatkan *Password* Jaringan

4.4 Implementasi Pengamanan

a. Implementasi Pengamanan MikroTik RB941-2ND



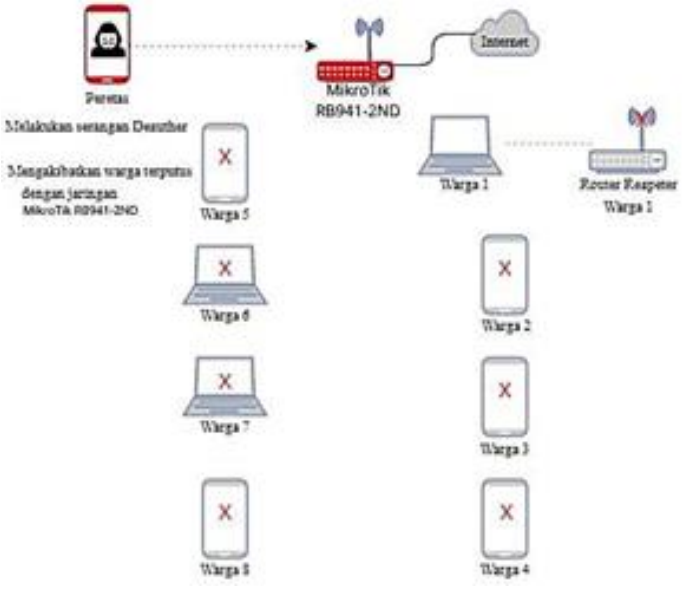
Gambar 14. Implementasi Pengamanan MikroTik RB941-2ND

Gambar 15. NodeMCU Scanning Gagal ke Jaringan Target

OKTAL : Jurnal Ilmu Komputer dan Science
Volume 3, No. 9, September 2024
ISSN 2828-2442 (media online)
Hal 2250-2259

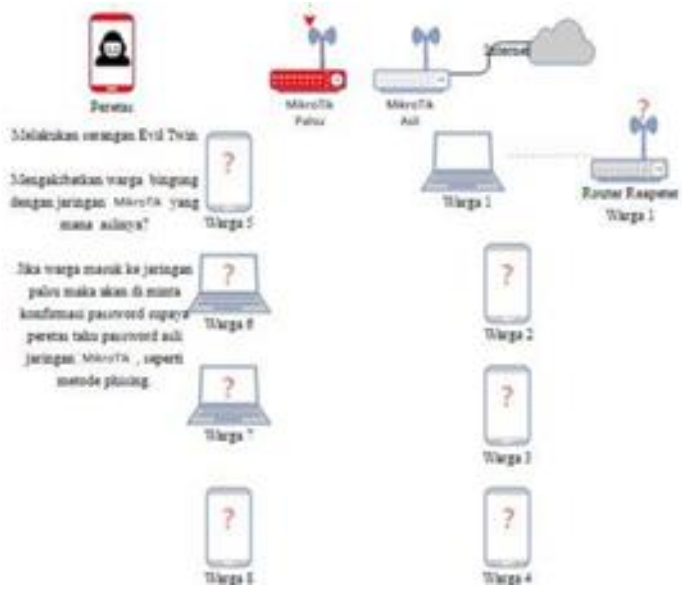
4.5 Kasus Dan Hasil Pengujian

4.5.1 Kasus Pengujian Metode *Deauther*



Gambar 16. Kasus Pengujian Metode *Deauther*

4.5.2 Kasus Pengujian Metode *Evil Twin*



Gambar 17. Kasus Pengujian Metode *Evil Twin*

4.5.3 Hasil Pengujian Dengan Metode *Deauther* Dan *Evil Twin*

Keduanya adalah teknik yang dapat digunakan untuk mengancam keamanan jaringan nirkabel. Mencegah serangan *Evil Twin* melibatkan waspada terhadap jaringan yang Anda sambungkan dan menghindari jaringan nirkabel yang tidak dikenal. Sementara itu, mencegah serangan *Deauther* dapat melibatkan penggunaan alat atau perlindungan keamanan tambahan yang dapat mendeteksi dan merespons serangan semacam itu untuk menjaga konektivitas perangkat Anda.

OKTAL : Jurnal Ilmu Komputer dan Science
Volume 3, No. 9, September 2024
ISSN 2828-2442 (media online)
Hal 2250-2259

5. KESIMPULAN

Berdasarkan hasil penelitian yang sudah dilakukan maka kesimpulan yang di simpulkan adalah Peneliti mampu meretas dan melakukan keamanan pada jaringan internet di lingkungan RT 001 dengan atau tanpa *password* yang kuat, melakukan implementasi perakitan alat mikrokontroler yang saat ini dengan mudah didapatkan pada pasaran, dan mampu mencegah peretasan jaringan RT.001 dengan router MikroTik RB941-2ND dan upaya penelitian mengenai pemanfaatan kelalaian manusia dalam meretas jaringan nirkabel sambil mengedukasi masyarakat tentang keamanan siber dan cara merespons gangguan peretas.

REFERENCES

Adiguna, Adhari, Mochamad, Widagdo, Wisnu, Bambang. (2022). Analisis Keamanan Jaringan Wpa2-Psk Menggunakan Metode Penetration Testing (Studi Kasus: Router Tp-Link Mercusys Mw302r). *Jurnal Sistem Komputer dan Kecerdasan Buatan*, Vol.5 No.2, Maret 2022.

Dwiyatno, Saleh, Sari, Purnama, Ayu, Irawan, Agus, Safig. (2019). Pendeteksi Serangan Ddos (Distributed Denial of Service) Menggunakan Honeypot Di Pt. Torini Jaya Abadi. *Jurnal SIMIKA*, Vol. 2 No. 2 Tahun 2019.

Ferianto, Kusno, Hidayati, Nurul, Uci. (2019). Efektifitas Pelatihan Penanggulangan Bencana Dengan Metode Simulasi Terhadap Perilaku Kesiapsiagaan Bencana Banjir Pada Siswa Sman 2 Tuban. *Jurnal Kesehatan Mesencephalon*, Vol.5 No.2, Oktober 2019, Hal: 88-94.

Jaya, Budi, Yunus, Yuhandri, Sumijan. (2020). Peningkatan Keamanan Router Mikrotik Terhadap Serangan Denial of Service (DoS). *Jurnal Sistim Informasi dan Teknologi*, Vol. 2 No. 4, Hal: 115-123, E-ISSN: 2686-3154.

Kurniawan, Adi, Turkhamun. (2020). Analisa Keamanan Jaringan Wifi Terhadap Serangan Packet Sniffing. *Jurnal Ilmiah Fakultas Teknik LIMIT'S*, Vol.16 No 2 September 2020, ISSN: 0216-1184.

Maharani, Dewi, Helmiah, Fauriatun, Rahmadani, Nurul. (2021). Penyuluhan Manfaat Menggunakan Internet dan Website Pada Masa Pandemi Covid-19. *ABDIFORMATIKA (Jurnal Pengabdian Masyarakat Informatika)*, Vol. 1, No. 1 - May 2021, Hal. 1-7.

Santoso, Adhi, Nugroho, Affandi, Bagus, Khaediar, Kurniawan, Dwi, Rifki. (2022). Implementasi Keamanan Jaringan Menggunakan Port Knocking. *Jurnal Janitra Informatika dan Sistem Informasi*, Vol. 2, No. 2 Oktober 2022, Hal. 90-95, E-ISSN: 2775-9490.