ANALISA DAN IMPLEMENTASI METODE *WARDRIVING* UNTUK MENGUJI KEAMANAN JARINGAN *WIRELESS* PADA CV. SABAR MAJU PAMULANG

Mukhamat Rifqi Ali[1]. Niki Ratama[2]

[1]Jurusan Teknik Informatika, Fakultas Teknik, Universitas Pamulang, Jl. Raya Puspitek, Tangerang Selatan, 15310, Indonesia
E-mail; [1]rifqipacitan@gmail.com, [2]dosen00835@unpam.ac.id

Abstract

Wireless network has been used as an excellent internet provider. By utilizing a wireless network, users can enjoy the internet without having to connect a cable. Cv. Sabar Maju Pamulang already using Wireless as an internet provider that can be used by employees who already have a login. Wireless networks are good must have good security in order to avoid the threat of crime. Wardriving, is an activity in which a person or group of people equipped with the tools and expertise to access a wireless network for free or without login. Wardriving is a threat to the Cv. Sabar Maju Pamulang for important data that is processed using a wireless network is not secured. To find out how strong the security of wireless networks at Cv. Sabar Maju Pamulang, the necessary analysis. From the analysis that has been done, the result are wireless network at the municipal Cv. Sabar Maju Pamulang not safe because there is still a hotspot point can do crack.

Keywords : *Wireless*, *Wardriving*, Sabar Pamulang.

Abstrak

Jaringan *Wireless* selama ini digunakan sebagai penyedia internet yang sangat baik. Dengan memanfaatkan jaringan *Wireless*, pengguna dapat menikmati internet tanpa harus tersambung pada sebuah kabel. Cv. Sabar Maju Pamulang sudah menggunakan *Wireless* sebagai penyedia internet yang dapat digunakan oleh pegawai yang sudah memiliki *login*. Jaringan *Wireless* yang baik haruslah memiliki keamanan yang baik agar terhindar dari ancaman kejahatan. *Wardriving*, adalah suatu kegiatan diamana seseorang maupun sekelompok orang yang dibekali alat dan keahlian untuk mengakses sebuah jaringan *Wireless* secara gratis atau tanpa melakukan *login*. *Wardriving* merupakan ancaman bagi Cv. Sabar Maju Pamulang karena data penting yang diolah menggunakan jaringan *Wireless* tidak terjamin keamanannya. Untuk mengetahui seberapa kuat keamanan jaringan Wireless pada Cv. Sabar Maju Pamulang, maka diperlukan analisis. Dari hasil analisis yang telah dilakukan, didapatlah kesimpulan bahwa jaringan *wireless* pada Cv. Sabar Maju Pamulang tidak aman karena masih ada titik hotspot yang dapat dilakukan *crack.*

Kata Kunci : *Wireless, Wardriving,* Sabar Pamulang.

1. PENDAHULUAN

Jaringan *wireless* pada era digital saat ini sudah menjadi kebutuhan penting bagi suatu lembaga, jaringan *wireless* memudahkan para penggunanya untuk memperoleh internet yang dapat digunakan dalam memperoleh informasi. Pada suatu perusahaan atau perkantoran tentu mempunyai jaringan *wireless* yang diproteksi oleh keamanan, seperti menggunakan *username* dan *password* untuk login agar dapat menggunakan jaringan *wireless* tersebut. Keberadaan jaringan *wireless* yang luas menimbulkan niat bagi orang atau sekelompok orang untuk mendapatkan jaringan *wireless* tersebut secara gratis ataupun dimanfaatkan untuk memperoleh data dari suatu lembaga maupun merusaknya[1].

Kemajuan teknologi informasi pada masa kini semakin berkembang seiring kebutuhan manusia yang memerlukan kemudahan, kecepatan, ketepatan, dan keamanan dalam

memperoleh suatu informasi. Teknologi informasi juga tidak terlepas dari teknologi jaringan *nirkabel* yang menghubungkan dua perangkat atau lebih dalam proses pertukaran informasi tanpa kabel yang menimbulkan *efisiensi* dan optimasi kerja.

CV. Sabar Maju Pamulang sebagai toko yang menjual peralatan rumah tangga dan restoran untuk menunjang operasional sehari-hari menggunakan jaringan internet dan *Wi-Fi*. Contohnya saat melakukan transaksi kasir, penerimaan barang, *stock opname*, cuci kasir, laporan omzet harian dan lain-lain. Jaringan internet pada CV. Sabar Maju Pamulang juga terkoneksi ke semua cabang dan *Head Office*.

Karena jaringan internet dan sistemnya saling terkoneksi antara semua cabang dan *Head Office*. tentunya penting untuk menjaga keamanan jaringan *wireless* agar tidak dirusak oleh orang yang tidak bertanggung jawab. Sebagai solusinya adalah peneliti akan menganalisis dan mengimplementasikan metode *wardriving.*

Wardriving adalah salah satu perilaku atau kegiatan yang sekarang biasa dilakukan untuk masuk kedalam jaringan internet yang disediakan melalui *Wireless Ethernet*. Selain merugikan, ini akan menjadi masalah serius dikemudian hari, karna semakin banyak *tools* yang bisa digunakan sebagai penyokong dari *Wardriving*[2].

Di pilihnya metode *wardriving* salah satunya kita bisa melakukan *sniffing* untuk mendapatkan *username* dan *password user* lain yang melakukan *login email, facebook, twiter* dan lainnya. Atau juga melakukan aksi pencurian data dengan memanfaatkan kelalaian pengguna lain yang sedang melakukan *file sharing.*

2. PENELITIAN YANG TERKAIT

Penelitian ini dilakukan oleh Rizki Wahyu Ismail (Universitas Bina Insani, 2020) yang berjudul **"Metode *Penetration Testing* pada Keamanan Jaringan *Wireless Wardriving* PT. Puma Makmur Aneka Engineering Bekasi"**, yang membahas tentang keamanan jaringan perusahaan menggunakan metode *wardriving* untuk mengetahui tingkat keamanan jaringan perusahaan dengan tujuan mengidentifikasi kerentanan keamanan di bawah keadaan yang dikendalikan sehingaa mereka dapat dihilangkan sebelum pengguna yang tidak berwenang mengeksploitasi[3]. (*ISSN :2528-6919 Vol. 5 NO.1 Agustus 2020).*

Penelitian yang dilakukan oleh Marti Widya Sari (Universitas PGRI Yogyakarta, 2018). Yang berjudul **"Analisis Keamanan Jaringan *Wireless Local Area Network* (Wlan) Menggunakan Metode Wardriving Di Fakultas Teknik Universitas Pgri Yogyakarta"**, yang membahas tentang keamanan jaringan Universitas PGRI Yogyakarta menggunakan metode wardriving dengan cara melakukan scan sinyal wireless menggunakan tools inSSIDer dan kismet. (*ISSN : 1907-2430, Juli 2018)*

Penelitian yang dilakukan oleh Amin Waluyo (Unversitas AMIKOM Yogyakarta, 2018) yang berjudul **"Implementasi Dan Analisis Metode *Wardriving* Untuk Pengukuran Tingkat Keamanan Jaringan *Nirkabel* Wilayah Kota Magelang"**, Yang membahas banyaknya acces poin di area publik kota Magelang yang tidak menggunakan enkripsi yang lebih aman.

Penelitian yang dilakukan Bambang Sugiantoro (UIN Sunan Kalijaga Yogyakarta, 2017) yang berjudul **"*Analisis* Tingkat Keamanan pada Dinas XYZ Terhadap Serangan Pengguna Wifi"** bertujuan unuk analisis keamanan untuk *Maturity* Model dengan skala 0-5 dan dilanjutkan dengan penetration test menggunakan metode ARP *Spoofing* dengan menggunakan tools yakni *CommView for Wifi ver.6.3, Aircrack-ng* 1.1 serta *Cain and Abel ver.4.9.35*. Penelitian ini berhasil menangkap username dan password yang dikirim dari komputer client. Oleh karena itu jaringan wireless yang diterapkan di kantor dinas XYZ tergolong belum cukup aman dalam hal keamanan jaringan[4]. *(ISSN : 2579-5406, Mei 2017)*

Penelitian yang dilakukan M.I. Rusdi (Universitas Cokroaminoto Palopo, 2019) dengan judul ***"Penetration Testing Pada Jaringan Wifi Menggunakan Kali Linux"*** bertujuan untuk Menganalisa fitur sistem keamanan WPA-PSK, WPA2-PSK pada jaringan *wireless*, dengan menggunakan sistem operasi Kali Linux[5].

Penelitian yang dilakukan B. Saloko Cahyo Saputro (Kampus STMIK MIC Cikarang, 2019) yang berjudul **"Analisa Keamanan Jaringan *Wireless* Menggunakan Metode *Wardriving* Pada Kampus STMIK MIC Cikarang"** bertujuan untuk menguji kekuatan enkripsi dari WEP *(Wired Equivalent Privacy)* yang di *setting* oleh kampus dengan metode wardriving[6]. *(ISSN : 2654-3168, Vol 2 2019)*

Penelitian yang dilakukan Mochamad Gilang Hari Wibowo (Fakultas Teknologi Idustri Yogyakarta, 2017) yang berjudul **"Keamanan Jaringan Wlan Terhadap Serangan *Wireless Hacking* Pada Dinas Komunikasi & Informatika DIY"** bertujuan untuk menguji keamanan *wireless* Kantor Dinas Komunikasi dan Informatika Daerah Istimewa Yogyakarta (Dinas

Kominfo DIY). Penelitian yang dilakukan M. Rido Wijayanto dan Linna Oktaviana Sari (Fakultas Teknik Universitas Riau, 2021) yang berjudul "*Analisis Wireless Access* Point Pada *Wifi* Dengan Menggunakan Metode Wardriving Di Kecamatan Tampan Kota Pekanbaru (Studi Kasus: Kecamatan Tampan)" Yang bertujuan untuk menemukan infomasi *Access Point* pada WiFi yang berupa SSID, Keamanan, Kualitas sinyal, *channel* atau frekuensi yang digunakan oleh pancaran sinyal sekitarnya dan mengetahui titik keberadaan pancaran sinyal wireless *access point* pada WiFi[7].

Penelitian yang dilakukan Muh. Yamin (Universitas Halu Oleo Kendari, 2017) yang berjudul **"Analisis Sistem Keamanan Jaringan Wireless (Wep, Wpapsk/Wpa2psk) Mac Address, Menggunakan Metode Penetration Testing"** Yang bertujuan untuk menganalisa sistem keamanan jaringan wireless menggunakan serangan *Cracking the Encryption* dan *bypassing* WLAN *Authentication*[8]. *(ISSN : 2502-8928, Vol.3 2017*

Penelitian yang dilakukan M. Rido Wijayanto dan Linna Oktaviana Sari (Fakultas Teknik Universitas Riau, 2021)yang berjudul **"*Analisis Wireless Access* Point Pada *Wifi* Dengan Menggunakan Metode Wardriving Di Kecamatan Tampan Kota Pekanbaru (Studi Kasus: Kecamatan Tampan)"** Yang bertujuan untuk menemukan informasi *Access Point* pada WiFi yang berupa SSID, Keamanan, Kualitas sinyal, *channel* atau frekuensi yang digunakan oleh pancaran sinyal sekitarnya dan mengetahui titik keberadaan pancaran sinyal wireless *access point* pada WiFi[9].

Penelitian yang dilakukan Derdi Kurniawan (Universitas Sriwijaya, 2017) yang berjudul "*WarDriving* Menggunkan Tools "*Wigle*" dan Mapping menggunkan "GoogleEarth" Dikawasan Kampus Indrlaya Universitas Sriwijaya" bertujuan untuk mendapatkan titik *acccess point* pada *wifi* Universitas Sriwijaya kampus Indralaya. Penelitian yang dilakukan Mochamad Gilang Hari Wibowo (Fakultas Teknologi Idustri Yogyakarta, 2017) yang berjudul "Keamanan Jaringan Wlan Terhadap Serangan *Wireless Hacking* Pada Dinas Komunikasi & Informatika DIY" bertujuan untuk menguji keamanan *wireless* Kantor Dinas Komunikasi dan Informatika Daerah Istimewa Yogyakarta (Dinas Kominfo DIY)[10].

3. METODE PENELITIAN

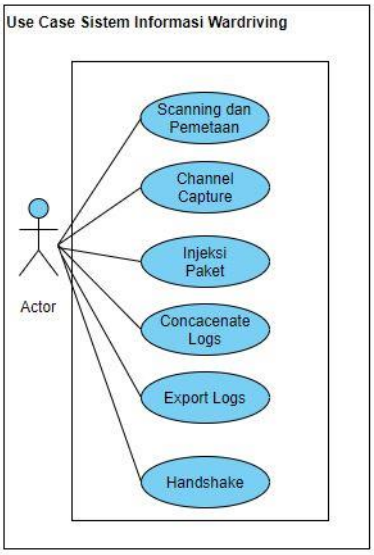
Untuk mendapatkan data-data yang mendukung penyelesaian laporan ini, penulis menggunakan beberapa metode. Metode-metode yang digunakan sebagai berikut :

1. Pengumpulan Data
   Ada tiga tahapan yang harus dilakukan dalam proses pengumpulan data adalah sebagai berikut :
   a. Metode Kepustakaan
      Metode ini digunakan untuk mengumpulkan data-data dan rumus-rumus yang diperlukan.
   b. Wawancara
      Metode ini dilakukan dengan mengadakan tanya jawab (wawancara) secara langsung dengan pihak-pihak yang berkaitan dengan informasi.
   c. Metode observasi
      Metode ini dilaksanakan dengan melakukan peninjauan langsung pada objek penelitian serta melakukan pencatatan mengenai hal-hal dan semua.
2. Pengembangan Sistem
   Adapun Metode pengujian yang digunakan untuk penelitian ini adalah metode *Wardriving*. *Wardriving* adalah kegiatan seseorang yang melakukan kegiatan berkeliling ke berbagai ke tempat dalam usahanya mencari, mengeksplorasi, bahkan mungkin juga mengeksploitasi jaringan *wireless* yang ditemukannya. Kemudian orang yang melakukan kegiatan tersebut disebut sebagai *Wardriver*, dalam upayanya itu dia melakukan pengumpulan data dan menganalisis sistem *Security*-nya[11].
   Tahapan dari metode Wardriving adalah :
   a) Penguatan Signal
      Untuk mendapatkan sinyal lebih kuat, peneliti akan menggunakan Wajan Bolic. Penggunaan Wajan Bolic agar sinyal dari jaringan *wireless* pada CV. Sabar Maju Pamulang dapat ditembus dari jarak yang lebih jauh.
   b) *Scanning*
      Untuk melakukan Scaning, peneliti akan menggunakan Tools G-MoN yang dioperasikan di Android. *Software* ini akan memberikan informasi tentang *Channel*, *MAC address, SSID, Speed*, tipe *Enkripsi*, dari jaringan *wireless* yang akan di teliti yaitu jaringan *wireless* pada toko Sabar Maju Pamulang.
   c) Pemetaan
      Setelah dilakukan *Wardriving*, Informasi yang dihasilkan dari G-MoN akan diolah menggunakan Laptop sistem *Operasi Windows*. Titik-titik *Hotspot* yang sudah

di *capture* menggunakan G-MoN akan disambungkan ke *Google Earth* sehingga hasil dari *Wardriving* dapat dipetakan.

d) Cracking

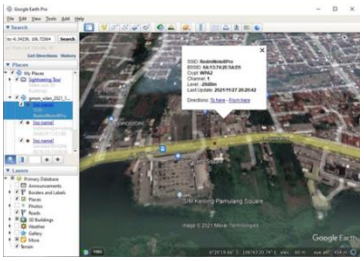
Setelah mendapatkan informasi berupa AP *(Access Point)*, MAC *address (Media Access Control Address)*, Tipe Enkripsi dan BSSID *(Basic Service Set Identification)*, peneliti akan melakukan *Crack* untuk mendapatkan akses dari *wireless* tersebut sesuai dari Tipe keamanan. Peneliti akan menggunakan *software CommView for Wifi* versi 6 dan *Aircrack* jika tipe keamanan yang digunakan adalah WEP. Jika Tipe keamanan yang digunakan adalah WPA atau WPA2 peneliti akan menambahkan teknik *Brute Force Atack* sebagai usaha untuk mendapatkan akses internet pada jaringan *wireless* CV. Sabar Maju Pamulang.



Gambar 1 Sistem Informasi *Wardriving*

4. HASIL DAN PEMBAHASAN

Dari hasil penelitian dihasilkan dan pembahasannya adalah sebagai berikut :



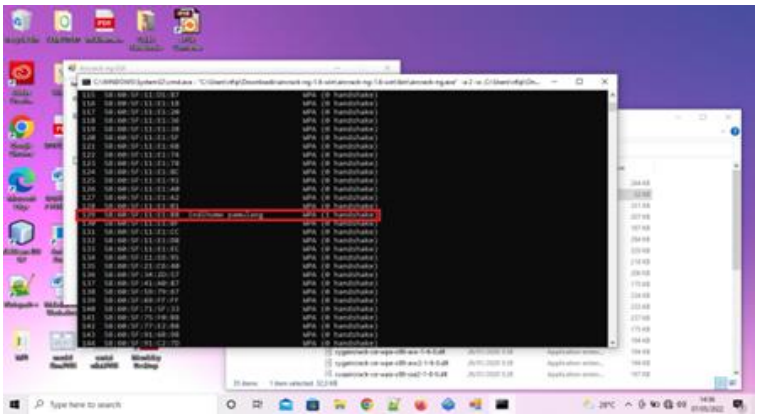
Gambar 2 *Scanning* dan pemetaan

Pada gambar 0.1 adalah hasil pemetaan menggunakan *software* G-Mon, dapat dilihat ada beberapa titik hotspot yang berhasil dicapture menggunakan G-Mon. Warna pada titik hotspot tersebut adalah jenis keamanan yang digunakan. Titik yang berwarna merah adalah hotspot yang menggunakan keamanan WPA2 dan titik-titik yang berwarna orange adalah hotspot yang menggunakan keamanan WPA. Berikut adalah hasil pemetaan menggunakan G-Mon dalam bentuk tabel.

Tabel 0.1 *Channel Capture*

No	SSID	Tipe Keamanan	*Channel*
1	RedmiNote8Pro	WPA2	1
2	Indihomepamulang	WPA	1
3	SAHABATPHONE	WPA	1

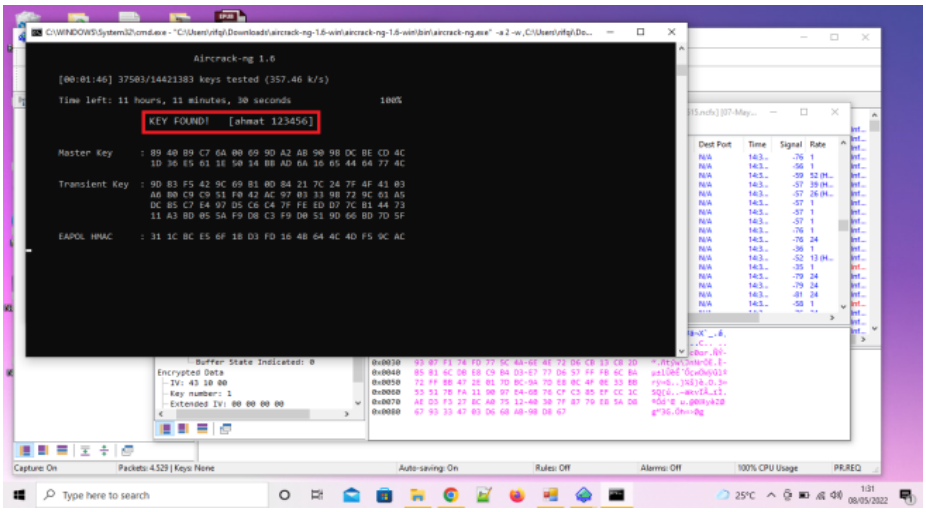
Dari hasil pemetaan yang dilakukan menggunakan *software* G-Mon dapat dilihat jumlah titik *hotspot* yang berhasil ter-*capture*, SSID, tipe keamanan dan juga *channel*. Pada saat melakukan pemetaan menggunakan *software* G-Mon peneliti juga mendapati titik hotspot diluar dari toko sabar.



Gambar 3 Injeksi Paket

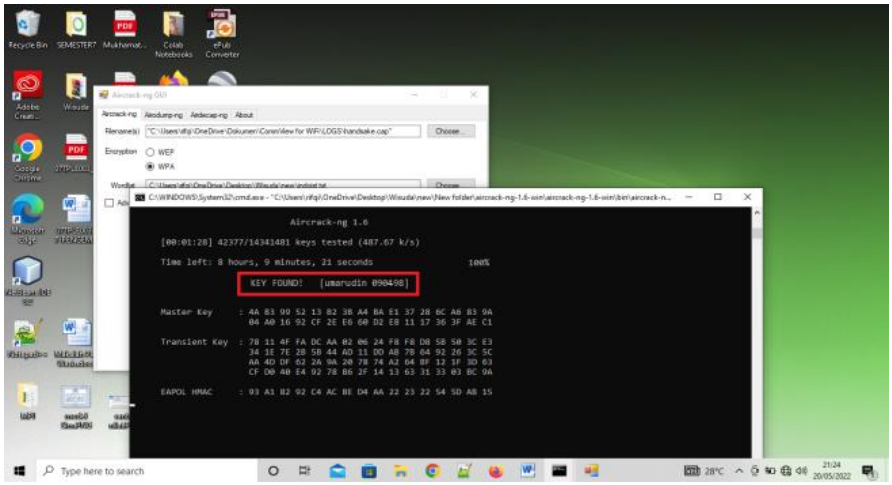
Hasil *cracking* berupa *Comand Prompt* yang berisikan paket lalu lintas jaringan yang berhasil ditangkap yang didalamnya terdapat informasi *username* dan *keys*/*password*. Selanjutnya peneliti memilih no. 129 untuk melanjutkan *crack.*

1) Pengujian Pertama



Gambar 4 *username* dan *key*/*password* ditemukan

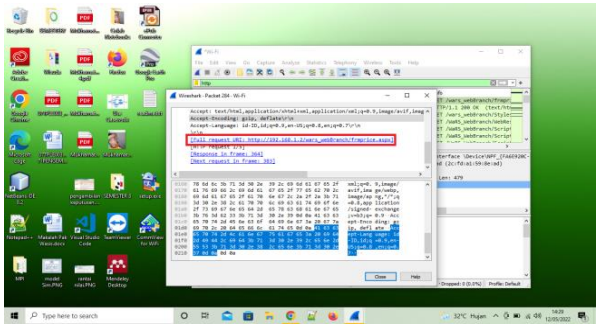
2) Pengujian Kedua



Gambar 5 Pengujian Kedua

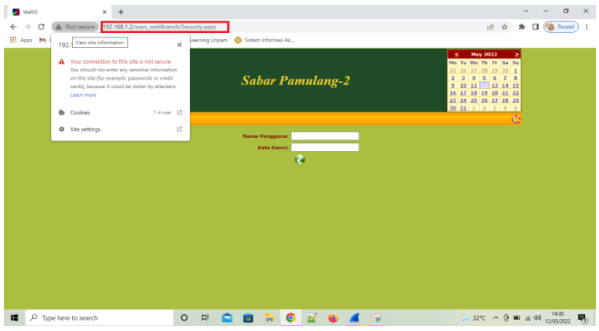
Sniffing

Setelah proses *cracking keys* terhadap *Hotspot* Toko Sabar Maju Pamulang selesai, peneliti ingin melakukan *sniffing* untuk menguji kebenaran *username* dan *keys*/*password* target yang telah di-*crack*. Peneliti menggunakan aplikasi *wireshark* untuk mendapatkan paket data pada lalu lintas jaringan.

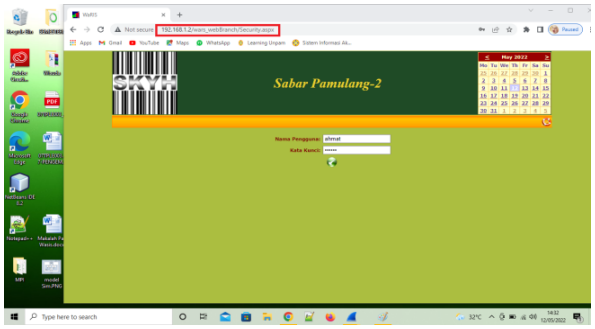


Gambar 0.1 Lalu lintas paket data

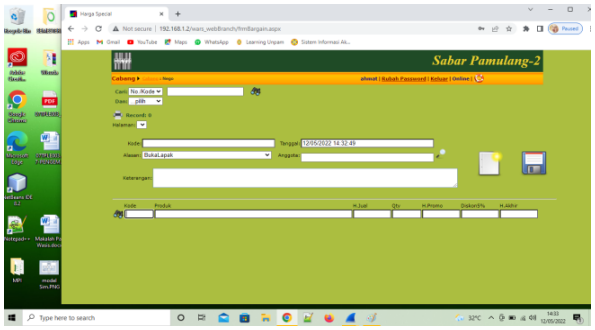
Setelah mendapatkan paket datanya seperti pada gambar 6, peneliti mencoba mengakses alamat website yang telah berhasil di *capture.*



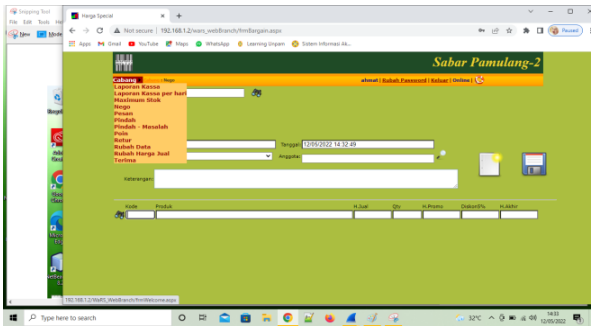
Gambar 0.2 Berhasil mengakses *website*



Gambar 0.3 Mencoba *login*



Gambar 0.4 Berhasil *login*



Gambar 0.5 Tampilan menu *website* yang berhasil diakses.

.

5. KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan mengenai Analisa Dan Implementasi Metode *Wardriving* Untuk Menguji Keamanan Jaringan *Wireless* Pada Cv. Sabar Maju Pamulang dapat disimpulkan sebagai berikut :

a. Dengan cara mengimplementasikan metode wardriving pada Hotspot Cv Sabar Maju Pamulang peneliti berhasil mendapatkan atau meng-crack username dan keys/password.
b. Agar suatu jaringan nirkabel agar tidak dirusak/dimasuki oleh orang yang bertanggung jawab perlunya meningkatkan tipe keamanan jaringan wireless. Hal ini diperkuat dari hasil pengujian dengan metode wardriving yang peneliti lakukan.

DAFTAR PUSTAKA

[1] Amin Waluyo, "Implementasi Dan Analisis Metode Wardriving Untuk Pengukuran Tingkat Keamanan Jaringan Nirkabel Wilayah Kota Magelang," *J. Penelit. Tek. Informaatika,5.*, Vol. 4, Pp. 9–15, 2018.

[2] M. W. Sari, "Analisis Keamanan Jaringan Wireless Local Area Network (Wlan) Menggunakan Metode Wardriving Di Fakultas Teknik Universitas Pgri Yogyakarta," *J. Teknol. Inf. Respati*, Pp. 53–64, 2018.

[3] R. W. Ismail, "Metode Penetration Testing Pada Keamanan Jaringan Wireless Wardriving Pt . Puma Makmur Aneka Engineering Bekasi," *J. Mhs. Bina Insa.*, Vol. 5, No. 1, Pp. 53–62, 2020.

[4] B. Sugiantoro, "Analisis Tingkat Keamanan Pada Dinas Xyz Terhadap Serangan Pengguna Wifi," *Semin. Nas. Teknol. Inf. Komun. Dan Ind.*, Pp. 64–70, 2017, [Online]. Available: Http://Ejournal.Uin-Suska.Ac.Id/Index.Php/Sntiki/Article/View/3209.

[5] M. I. Rusdi And D. Prasti, "Penetration Testing Pada Jaringan Wifi Menggunakan Kali Linux," *Semin. Nas. Teknol. Inf. Dan Komput. 2019*, Pp. 260–269, 2019.

[6] B. H. I. Saloko Cahyo Saputro, Tri Hargi Saputro, "Analisa Keamanan Jaringan Wireless Menggunakan Metode Wardriving Pada Kampus Stmik Mic Cikarang," *Pros. Semin. Nas. Unimus*, Vol. 2, No. E-Issn : 2654-3168, P-Issn : 2654-3257, Pp. 455–461, 2019.

[7] M. G. H. Wibowo, J. Triyono, And E. Sutanta, "Keamanan Jaringan Wlan Terhadap Serangan Wireless Hacking Pada Dinas Komunikasi & Informatika Diy," *Semin. Nas. Call Pap. Pengemb. Smart City Menuju Pembang. Kota Yang Cerdas Dan Berkelanjutan*, Vol. 1, No. 1, Pp. 2–9, 2017, [Online]. Available: Http://Jurnal.Unmuhjember.Ac.Id/Index.Php/Sensei17/Article/View/844.

[8] D. M. Sari, M. Yamin, And L. B. Aksara, "Analisis Sistem Keamanan Jaringan Wireless (Wep, Wpapsk/Wpa2psk) Mac Address, Menggunakan Metode Penetration Testing," *Semantik*, Vol. 3, No. 2, Pp. 203–208, 2017, Doi: 10.1016/J.Neuropharm.2007.08.010.

[9] M. R. Wijayanto And Linna Oktaviana, "Analisis Wireless Access Point Pada Wifi Dengan Menggunakan Metode Wardriving Di Kecamatan Tampan Kota Pekanbaru (Studi Kasus: Kecamatan Tampan)," Vol. 8, Pp. 1–9, 2021.

[10] J. S. Informasi, F. I. Komputer, U. Sriwijaya, K. O. Ilir, And S. Selatan, "Analisis Wardriving Mengguna Kan Tools 'Wigle' Dan Mapping Menggunakan 'Googleearth' Dikawasan Auditorium Kampus Indralaya Universitas Sriwijaya," Vol. 1, No. 09031181520009, 2017.

[11] M. W. Sari, "Analisis Keamanan Jaringan Wireless Local Area Network (Wlan) Menggunakan Metode Wardriving Di Fakultas Teknik Universitas Pgri Yogyakarta," *J. Teknol. Inf. Respati*, Pp. 53–64, 2018.