ANALISIS DAN EVALUASI KEAMANAN WIRELESS LAN PADA PT. BUMI JAGE DALAM

Azhar Andika Putra, M.Kom.

Universitas Sjakhyakirti
Email: Azharandikaputra@unisti.ac.id

ABSTRACT

This study aims to determine the level of security of the WLan network at PT Bumi Jage Dalam. The method used is the Action Research method (Diagnosing, Action Planning, Action Taking, Evaluating And Learning). The results of network analysis research using Wifi Analyzer tools, the attacker gets information about the IP, Mac Address and security used by the target. Penetration testing using the WiFi Password tool fails to get the WLan password. For MITM attacks with the Zanti tool, the attacker succeeds in obtaining information and activities carried out by the target in the network. The next test was terminating the target connection with Arcai.com's NetCut tools and it was successful, while testing to enter the Router Settings tool settings successfully accessed the modem login page and entered the settings. This research is limited to applications on the android smartphone. It is hoped that with this study users of wifi or public networks will be more vigilant because of the many risks that threaten.

Keywords: *Penetration Testing, Wireless LAN, Gray Box Testing, Keamanan Jaringan, Action Research.*

PENDAHULUAN

Jaringan nirkabel atau dikenal dengan Wifi atau wireless Fidelity saat ini sudah banyak digunakan pada organisasi-organisasi maupun di tempat-tempat umum karena kemudahannya penggunaan, karena wifi hanya memerlukan udara sebagai media perantara untuk koneksinya dan tidak lagi menggunakan media kabel. Dibalik kemudahan yang ditawarkan oleh jaringan wifi terdapat kerentanan yang dapat membahayakan pengguna karena pemakaiannya yang bersifat umum. Perusahaan Kaspersky melakukan pemungutan suara secara global melalui acebook pada tahun 2013 tentang keamanan jaringan nirkabel, dan hasilnya menunjukkan bahwa lebih dari 42% pengguna mengatakan bahwa mereka menggunakan Wi-Fi umum tanpa mempertimbangkan keamanannya (Cosmas Eko Suharyanto, 2017).

PT. Jage Dalam yang merupakan perusahaan yang bergerak di bidang konsultan lingkungan memanfaatkan internet baik yang menggunakan media kabel maupun wifi untuk mendukung kegiatan bisnisnya, untuk mengetahui tingkat keamanan penggunaan internet dalam hal ini jaringan wifi maupun bahaya yang mungkin dapat mengancam penggunanya maka penulis melakukan penelitian dengan judul Analisis dan Evaluasi Keamanan Wireless LAN (WLan) Pada PT. Bumi Jage Dalam.

TINJAUAN PUSTAKA DAN PENGEMBANGAN HIPOTESIS

a) Jaringan Komputer

Jaringan komputer *(computer networks)* adalah suatu himpunan interkoneksi sejumlah computer *autonomous*. Jaringan komputer terdiri atas perangkat-perangkat yang saling terhubung satu sama lain melalui media perantara seperti router, switch dan sebagainya. Media perantara ini bisa berupa media kabel ataupun media tanpa kabel (nirkabel) (Samsumar L Delsi & Gunawan K, 2017). *Wireless* (nirkabel) adalah teknologi yang menghubungkan dua piranti untuk bertukar data tanpa media kabel. Adapun *Wireless Fidelity* (WiFi), yaitu perangkat standar yang digunakan untuk komunikasi jaringan lokal tanpa kabel (*WirelessLocal Area Network*/WLAN) yang didasari pada spesifikasi IEEE 802.11 (Sofana, 2013).

Jaringan komputer adalah suatu kumpulan atau beberapa komputer yang dihubungkan sehingga dapat berkomunikasi, termasuk juga printer dan peralatan lainnya yang saling terhubung. Data atau informasi ditransfer melalui kabel maupun wireless sehingga orang yang menggunakan computer dapat saling bertukar dokumen dan data, mencetak pada printer yang sama dan bersama-sama menggunakan hardwarehardware yang terhubung dengan jaringan (Rahman, A. 2014).

b) Vulnerability Assessment

Vulnerability atau celah keamanan adalah suatu kelemahan yang mengancam nilai *integrity, confidentiality* dan *availability* dari suatu aset. *Vulnerability* tidak hanya berupa *software bugs* atau kelemahan *security* jaringan. Namun kelemahan seperti pegawai yang tidak ditraining, dokumentasi yang tidak tersedia maupun prosedur yang tidak dijalankan dengan benar. *Vulnerability* bias dikategorikan ke dalam tiga bagian, yaitu kelemahan pada sistem itu sendiri, jalur akses menuju kelemahan sistem, serta kemampuan dari seorang *hacker* untuk melakukan *attacking.* (Siregar, 2010). Pengukuran atau *assessment* adalah hal yang mutlak dilakukan untuk mendapatkan peningkatan kualitas. Suatu perusahaan dapat meningkatkan penjualannya bila mengetahui bagaimana efisiensinya. Dengan adanya pengukuran maka perusahaan dapat mengetahui kelemahan yang ada, membandingkannya dengan contoh penerapan diperusahaan lain dan ujungnya adalah peningkatan keuntungan perusahaan. (Priandoyo, 2006).

Dijelaskan pula oleh Anjar Priandoyo tahun 2006 *Vulnerability assessment (VA)* adalah salah satu cara untuk pengukuran terhadap kemanan sistem. VA merupakan salah satu bagian pengendalian preventif dalam keseluruhan rangkaian pengendalian TI, disamping berbagai metode pengendalian terhadap keamanan yang lain seperti detektif dengan *Instrusion Detection System (IDS),* atau preventif dengan *antivirus* dan *firewall* dan pengendalian akan keamanan informasi dalam perusahaan. Proses VA sendiri memiliki berbagai tingkatan, sehingga perusahaan dapat memilih tingkatan mana yang akan digunakan dalam pengukurannya. Tingkatan ini dapat disesuaikan dengan kondisi di masing-masing tempat.

1 Tingkat I: Pengukuran peraturan dan kebijakan (*Policy Assessment*). Pengukuran ini meliputi peraturan, kebijaksanaan, standar operasi di *client* dalam cakupan keamanan informasi.
2 Tingkat II: Evaluasi Jaringan. Pengukuran ini meliputi kinerja jaringan, keamanan jaringan hingga ancaman-ancaman terhadap jaringan kerja. Pengukuran jenis ini memerlukan alat bantu seperti *scanning* atau *data capture.* Evaluasi jaringan ini bertujuan untuk mendapatkan informasi mengenai kondisi sebenarnya yang terjadi

dilapangan, bagaimanan tingkat kesadaran akan keamanan informasi yang sudah diterapkan selama ini.

3 Tingkat III: *Penetration Testing* atau *Pentest*. *Pentest* sebenarnya menggunakan prinsip yang sama dengan *Network Evaluation* dimana pembedanya bahwa *Pentest* dilakukan dalam kondisi gelap, tanpa mengetahui konfigurasi dan kondisi sebenarnya seperti apa. Pada *Pentest*, *tester* akan menjumpai sistem sebagai sebuah kotak tertutup menghadapi penetrasi yang datang dari luar.

c) Penetration Test

Penetration test atau biasa disebut dengan Pentest merupakan sebuah metode yang digunakan untuk mengevaluasi keamanan dari sebuah sistem maupun keamanan pada jaringan komputer. Evaluasi tersebut dilakukan dengan cara melakukan sebuah simulasi serangan (*attack*). Hasil dari pentest tersebut sangat penting bagi administrator sebagai umpan balik dari sistem atau jaringan komputernya, yang kemudian diperbaiki tingkat keamanan dari sistem komputernya, selain itu juga akan diberikan masukan terhadap kondisi *vulnerabilitas* sistem sehingga memudahkan dalam melaksanakan evaluasi dari sistem keamanan komputer yang sedang berjalan. Aktifitas pentes juga dikenal dengan istilah "ethical hacking".

Untuk melihat kualitas keamanan jaringan maka perlu dilakukan analisa terhadap sistem keamanan yang ada dalam jaringan tersebut. Salah satu metode yang dapat digunakan dalam mengevaluasi jaringan adalah dengan cara melakukan pengujian terhadap sistem dengan mensimulasikan bentuk-bentuk serangan terhadap jaringan atau biasa yang dikenal dengan metode *Penetration Testing (Chow, E (2011)).*

Berbagai metode pentest yang dapat digunakan antara lain: *black box*, *white box* dan *grey box*. *Black box testing* adalah metode pentest yang mengasumsikan tester tidak mengetahui sama sekali infrastruktur dari target pentest. Sehingga, tester dengan metode ini harus mencoba menggali dariawal semua informasi yang diperlukan kemudian melakukan analisis serta menentukan jenis serangan yang akan dilakukan. Pada *White box testing* terjadi sebaliknya, tester telah mengetahui semua informasi yang diperlukan untuk melakukan pentest. Sementara *grey box* mengkombinasikan dari kondisi *black box* dan *white box*. Istilah lain dari *white box* adalah *full disclosure*, *grey box* adalah *partial disclosure* dan *black box* adalah *blind disclosure*. (Saskara Gede, A.J. dkk, 2019).

d) Ethical Hacking

Hacking sendiri adalah suatu aktifitas dari hacker yaitu orang yang tertarik dan mendalami sistem operasi komputer sehingga mengetahui kelemahan yang ada pada suatu sistem tetapi tidak memanfaatkan kelemahan tersebut untuk hal kejahatan dan merugikan. Berbeda dengan Cracker dimana mereka memasuki sistem orang lain dengan tujuan kurang baik. Di dalam dunia hacker ada tingkatan-tingkatan tertentu yang biasa disebut dengan julukan dan biasanya hacker mempunyai etika. Di bawah ini adalah tingkatan dalam dunia hacker beserta etika hacker (Prasetya, 2012):

1 Elite: Merupakan ujung tombak industri keamanan jaringan. Mereka mengerti sistem operasi luar dan dalam, sanggup mengkofigurasi dan menyambungkan jaringan secara gelobal. Mereka tidak akan menghancurkan data karena mengikuti aturan yang ada.

2 Semi Elite: Hacker ini biasanya lebih muda daripada Elite. Mereka juga mempunyai kemampuan dan pengetahuan luas tentang komputer. Mereka mengerti tentang sistem operasi, termasuk lubangnya. Biasanya dilengkapi dengan sejumlah program

kecil yang cukup untuk membuat program eksploit. Banyak serangan yang dilakukan dan dipublikasikan oleh Hacker kaliber ini, sialnya oleh para Elite mereka sering kali di kategorikan Lamer.

3 Developed Kiddie: Julukan ini diberikan terutama karena umur kelompok ini masih muda (ABG) dan masih duduk di bangku sekolah. Mereka membaca tentang metoda hacking dan caranya di berbagai kesempatan. Mereka mencoba berbagai sistem sampai akhirnya berhasil dan memproklamirkan kemenangan ke lainnya. Umumnya mereka menggunakan Grafik User Interface (GUI) dan baru belajar dasar dari UNIX, tanpa mampu menemukan lubang kelemahan baru di sistem operasi.

4 Script Kiddie: Seperti developed kiddie, Script Kiddie biasanya melakukan aktifitas yang sama. Seperti juga Lamers, mereka hanya mempunyai pengetahuan teknis networking yang sangat minimal. Biasanya tidak lepas dari GUI. Aktivitas hacking dilakukan menggunakan trojan untuk menakuti dan menyusahkan hidup sebagian pengguna internet.

5 Lamer: Mereka adalah orang tanpa pengalaman dan pengetahuan yang ingin menjadi Hacker (wanna-be Hacker). Mereka biasanya membaca atau mendengar tentang Hacker dan ingin seperti itu. Penggunaan computer mereka terutama untuk tukar menukar software prirate, bermain game, IRC, dan mencuri kartu kredit. Biasanya melakukan hacking menggunakan nuke, DoS, dan software trojan. Biasanya menyombongkan diri melalui IRC channel dan lain-lain. Karena banyak kekurangannya untuk mencapai level elite, dalam perkembangannya mereka hanya akan sampai tingkatan developed kiddie atau script kiddie saja.

e) Penyerangan Jaringan Wireless

Penyerangan Jaringan Wireless di bagi menjadi:

1 Serangan Logical

Logical attack selalu berhubungan dengan sistem, perangkat lunak dan data pada jaringan. Dalam kasus ini penyerang mencari kelemahan dan informasi pada jaringan yang akan membantu penyerang untuk mengakses jaringan mendapatkan gaining dan mengambil data sensitif pada suatu jaringan. Sasaran utama pada serangan ini adalah untuk menemukan dan mengambil data pada jaringan. Jika penyerang berhasil maka serangan ini akan menghasilkan banyak masalah terhadap kondisi suatu jaringan. Berikut merupakan contoh dari Logical Attack dengan teknik mitigasi.

- Spoofing of MAC address
- Serangan Denial of Service
- Serangan Man in the Middle
- Default Access Point Configuration
- Serangan Reconnainssance
- Conversation Sniffing
- Serangan Dynamic Host Configuration Protocol

2 Serangan Fisik

Sebuah physical attack selalu berkaitan dengan hardware atau perangkat keras dan design dari sebuah jaringan. Dalam jenis serangan ini tujuan penyerang adalah mengganggu atau mengurangi kinerja jaringan daripada mencari data sensitif dan kemudian membuat beberapa perubahan dengan data. Yang perlu di ingat bahwa serangan jenis ini selalu memjadi jembatan langsung terhadap Logical Attack. Beberapa Physical attack didefinisikan di bawah ini:

- Rogue Access Points
- Physical placement of Access points - Access Point coverage
- Spam Attacks (Vivek, 2012).

f) Keamanan Jaringan

Menurut Kusumawati, M, 2014 dalam Antoni pada dasarnya, terdapat tiga jenis mode keamanan jaringan nirkabel. Wired Equivalent Privacy (WEP) Merupakan standar keamanan pertama dari jaringan nirkabel yang dibuat dengan menggunakan algoritma enkripsi RC4. Algoritma ini sederhana dan mudah diimplementasikan karena tidak membutuhkan perhitungan yang berat, sehingga tidak membutuhkan hardware yang canggih. Walaupun pengamanan metode WEP ini memiliki banyak celah keamanan, masih banyak orang menggunakannya.

Wi-fi Protected Access (WPA) WPA dikenal juga dengan sebutan WEPv2 alias WEP versi 2, yang dirilis pada bulan April 2003. WPA merupakan perbaikan dari WEP, jadi bukan merupakan sebuah metode keamanan yang baru, sehingga kelemahan yang terdapat pada WEP masih tetap ada pada WPA. Dimana sistem enkripsi yang digunakan masih menerapkan RC4. Konfigurasi kemanan pada WPA sangatlah sederhana karena hanya perlu memilih WPA sebagai metode pada klien dan juga pada access point. Wi-fi Protected Access 2 (WPA2). WPA2 diperkenalkan pada bulan septermber 2014 oleh Wi-Fi Alliance. WPA2 sepenuhnya menerapkan standar IEEE 802.11i dan merupakan pengembangan lebih dari WPA. Perkembangan signifikan adalah perkenalan Coutner Mode with Chiper Block Chaining Message Uthentication Code Protocol (CCMP) yang menggunakan block chipper Advanced Encryption Standard (AES) utnuk enkripsi data, tetapi aliran chipper TKIP tersedia untuk kompabilitas dengan hardware WAP yang ada. Otentikasi WPA2 juga memiliki dua mode: Pre Shared Key dan Enterprise mirip dengan WPA.

g) Sistem Operasi Android

Android sistem operasi berbasis Linux yang dirancang untuk perangkat bergerak layar sentuh seperti telepon pintar dan komputer tablet. Android awalnya dikembangkan oleh Android, Inc., dengan dukungan finansial dari Google, yang kemudian membelinya pada tahun 2005. Sistem operasi ini dirilis secara resmi pada tahun 2007, bersamaan dengan didirikannya Open Handset Alliance, konsorsium dari perusahaan-perusahaan perangkat keras, perangkat lunak, dan telekomunikasi yang bertujuan untuk memajukan standar terbuka perangkat seluler. Ponsel Android pertama mulai dijual pada bulan Oktober 2008 (https://id.wikipedia.org/wiki/Android_(sistem_operasi)), saat ini sistem operasi android terbaru adalah versi 11 yang dirilis pada tanggal 8 September 2020.

METODE PENELITIAN

a) Metode Penelitian Action Research

Metode penelitian yang digunakan dalam penelitian ini menggunakan metode penelitan tindakan atau action research. Action research adalah kegiatan dan atau tindakan perbaikan sesuatu yang perencanaan, pelaksanaan, dan evaluasinya digarap secara sistematik sehingga validitas dan reabilitasnya mencapai tingkatan riset.(Gunawan, 2006). Ada lima tahapan dalam penelitian yang merupakan siklus dari action research, yaitu:

1 Melakukan diagnosa (Diagnosing). Pada tahapan ini peneliti akan melakukan identifikasi masalah-masalah yaitu diagnose sistem keamanan pada situsweb www.pusdikpenerbad.mil.id.
2 Membuat rencana tindakan (Action Planning). Tahapan ini peneliti melakukan pemahaman pokok masalah yang ada dan menyusun rencana tindakan yang tepat untuk menyelesaikan masalah yang ada. Peneliti akan mulai menyusun rencana pengujian yang akan dilakukan.
3 Melakukan tindakan (Action Taking). Mengimplementasikan rencana tindakan yang telah disusun. Pada langkah ini peneliti mulai melakukan tahapan-tahapan investigasi guna mendapatkan informasi kelemahan sistem dan mengujinya secara langsung dengan menggunakan tipe-tipe ancaman terhadap situsweb.
4 Melakukan evaluasi (Evaluating). Setelah tahapan Action Taking dilaksanakan, peneliti mulai melakukan evaluasi dan menyimpulkan hasil dari langkah sebelumnya.
5 Pembelajaran (Learning). Langkah ini merupakan tahap akhir dari penelitian yaitu melakukan review terhadap hasil dari tahapan-tahapan yang telah dilalui.

Dalam penyusunan penelitian ini peneliti mengumpulkan data yang dibutuhkan menggunakan metode pengumpulan data sebagai berikut:

1 Studi Literature. Merupakan suatu cara pengumpulan data yang dilakukan dengan cara mencari bahan dari internet, jurnal dan perpustakaan serta buku yang sesuai dengan objek yang akan diteliti.
2 Pengamatan (Observation). Merupakan suatu pengumpulan data yang dilakukan dengan cara mengamati permasalahan pada objek yang diteliti secara langsung.

b) Metode Deskriptif

Menurut Nasir (2003:54), Metode deskriptif adalah suatu metode dalam meneliti status sekelompok manusia, suatu objek, suatu set kondisi, suatu sistem pemikiran, ataupun suatu kelas peristiwa pada masa sekarang. Tujuan dari penelitian deskriptif ini adalah untuk membuat deskripsi, gambaran atau lukisan secara sistematis, faktual dan akurat mengenai fakta-fakta, sifat-sifat serta hubungan antar fenomena yang diselidiki.

c) Metode Gray Box dan Penetration Testing

Grey box testing adalah penetration testing yang dilakukan dengan mengetahui sedikit informasi dari target yang akan diuji keamanannya. Hal ini sedikit membantu pentester dalam melakukan kegiatan aktifitas penetration testing Pentest adalah cara yang paling efektif untuk mengidentifikasi kelemahan sistem dan kelemahan di dalam suatu program, dengan mencoba untuk menghindari kontrol dan mekanisme keamanan (Kennedy et al, 2011)

d) Peralatan Yang Dibutuhkan

Peralatan yang digunkan pada penelitian ini adalah sebagai berikut:

1. Satu unit Smartphone merk Redmi 7 sebagai attacker dengan RAM 2 GB, Prosesor Snapdragon 632, Sistem operasi android Pie dengan Custom ROM AEX Extended 6.7.
2. Tools yang digunakan untuk menyerang target pada penelitian ini adalah WiFi Password, Zanti, Arcai.com's NetCut, dan Router Settings yang semunya berbasis android.

HASIL DAN PEMBAHASAN

A. Analisis

Analisis jaringan yang akan dijadikan target serangan dilakukan menggunakan tools Wifi Analyzer, diketahui Wireless LAN BUMI JAGE DALAM dari Modem yang dikeluarkan oleh Huawei Technology Co LTD dengan Mac Address 80:41:26:ec:6c:4c menggunakan keamanan WPA2.

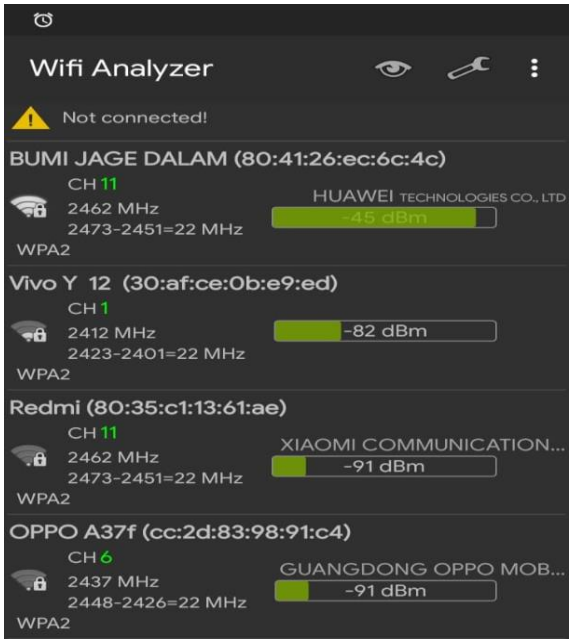

Figure 1. Analisis Jaringan Menggunakan Tools Wifi Analyzer

1. Analisis Pengujian External

Pengujian external dilakukan dari luar jaringan dengan metode black box testing dimana seakan-akan peneliti tidak mengetai informasi tentang jaringan yang akan dijadikan target serangan

1.1 Penetrasi Key

Pada pengujian Penetrasi Key dilakukan dengan tools bernama WiFi Password yang dikembangkan oleh Global Wifi Technology. Dari hasil percobaan diketahui bahwa Penetrasi key yang dilakukan pada wifi dengan SSID BUMI JAGE DALAM tidak berhasil, attacker gagal masuk ke dalam jaringan wifi yang menggunakan otentifikasi WPA2.

Figure 2: Penetrasi Ke Jaringan

1.2 Penetration Testing

Pada bagian ini peneliti akan melakukan *Penetration Testing* langsung pada WLAN PT Bumi Jage Dalam.

a) Man in the Middle Attack (MITM)

Pengujian untuk melakukan Man in the Middle Attack pada pengguna yang terhubung ke jaringan wifi dilakukan dengan bantuan tools zANTI (Zimperium Android Network Toolkit). zANTI adalah perangkat pengujian penetrasi seluler pada perangkat android yang dikembangkan oleh Zimperium. Dari hasil scan jaringan dapat dilihat ada 4 perangkat yang terhubung ke jaringan wifi, di ketahui modem dengan merk Huawei Technologies dengan IP 92.168.100.1 dengan MAC address 80:41:26:EC:6C:45 akan dijadikan target serangan.

Figure 3. Scan Jaringan Dengan Zanti

Dari hasil scanning diketahui 5 logged request user dan 0 password, attacker dapat melihat aktifitas yang dilakukan oleh target, selain itu attacker juga bisa mendapatkan username dan password jika target login pada suatu situs atau layanan.

Figure 4: Hasil Scanning Target

Saat dilakukan serangan MITM, kecepatan koneksi internet target melambat dan sulit untuk mengakses internet, bahkan koneksi internet terputus.

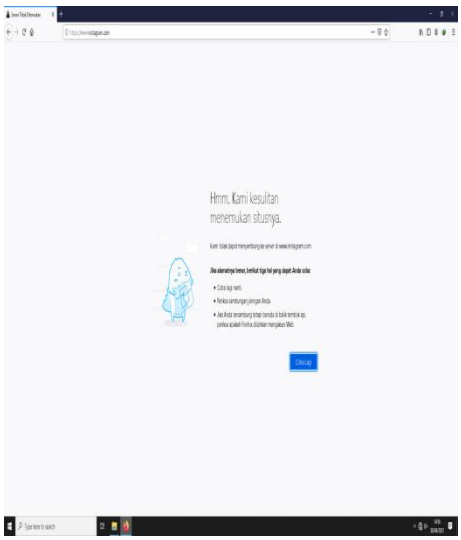

Figure 5: Koneksi Internet Target Terputus

b) Disconnected Computer Client

Untuk pengujian Disconnected Computer Client dilakukan menggunakan tools Arcai.com's NetCut.

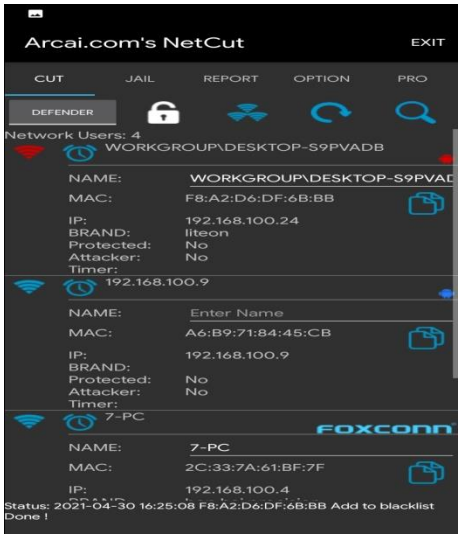

Figure 6: Koneksi Internet Target Terputus

Dari hasil pengujian seperti terlihat pada Gambar 7 di bawah ini, koneksi intenet target berhasil diputus diketahui walaupun keterangan koneksi wifi pada target masih tersambung.

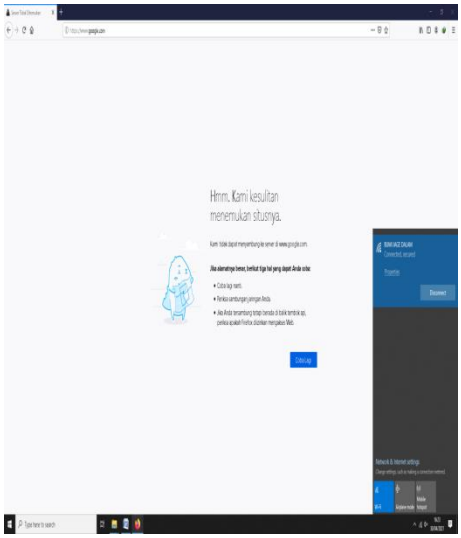

Figure 6: Koneksi Internet Target Terputus

c) Akses Login Page Modem

Dengan menggunakan tool Router Setting dengan pengembang Leon Zhang attacker dapat mengakses login page modem target, setelah mencoba memasukan Account dan Password default perangkat, attacker berhasil masuk ke pengaturan modem.

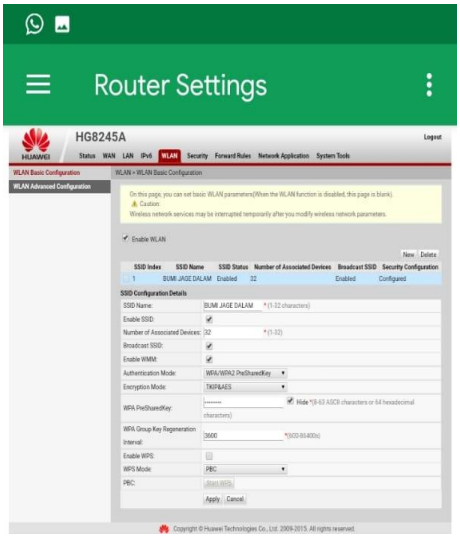

Figure 6. Login Page Modem

B. Melakukan Evaluasi *(Evaluating)*

1. Evaluasi Hasil Pembahasan

Setelah melakukan analisis jaringan dengan menggunakan tools Wifi Analyzer, attacker mendapatkan informasi mengenai IP, Mac Address dan keamanan yang dipakai oleh target. Selanjutnya Attacker melakukan penetration testing dengan menggunakan tool WiFi Password dan gagal mendapatkan password WLan. Untuk serangan MITM dengan tool Zanti, attacker berhasil mendapatkan informasi dan aktifitas yang dilakukan target didalam jaringan.

Pengujian selanjutnya attacker melakukan pemutusan koneksi target dengan tools Arcai.com's NetCut dan berhasil karena koneksi target langsung terputus, sedangkan pengujian untuk masuk ke dalam pengaturan tool Router Settings berhasil mengakses login page modem dan masuk kedalam pengaturan, dengan begitu attacker bisa merubah password WLan.

2. Pembelajaran *(Learning)*

Dokumentasi dan Pelaporan *(Documentation and Reporting)*

Dari hasil pengujian pada tahap-tahap sebelumnya didapatkan hasil sebagai berikut

Tabel 1: Dokumentasi dan Laporan

No	Jenis Serangan	Tools	Status	Koneksi
1.	Penetrasi Key	WiFi Password	Tidak berhasil	Tidak login
2.	Man in the Middle Attack (MITM)	Zanti	Berhasil	Login
3.	Disconnected Computer Client	Arcai.com's NetCut	Berhasil	Login
4.	Login Page Modem	Router Settings	berhasil	Login

KESIMPULAN

Dari hasil penetration testing yang dilakukan pada Wireless LAN PT. Bumi Jage Dalam dapat disimpulkan bahwa percobaan Penetration Key tidak berhasil mendapatkan password wifi yang diinginkan, sedangkan untuk uji coba serangan Man In The Middle Attack (MITM), Disconnected Computer Client, dan Login pada modem berhasil dilakukan dengan metode white box testing dimana atacker melakukan pengujian dari dalam dengan login pada jaringan wifi.

Dari semua serangan, yang paling berbahaya adalah serangan Man In The Middle Attack (MITM), dimana attacker bisa mengetahui aktifitas yang dilakukan target dan bisa juga mendapatkan informasi sensitif target berupa username dan password. Namun demikian diketahui selama attacker tidak bisa masuk ke jaringan wifi, serangan-serangan yang dilakukan tidak akan berhasil. Untuk itu administrator jaringan perlu merubah password wifi secara berkala. juga disarankan kepada pengguna wifi agar tidak mengakses hal-hal atau aktifitas sensitif selama menggunakan jaringan internet yang bersifat umum.

REFERENSI

Antoni. *Analisis Dan Pengujian Kemanan Kelemahan Jaringan Nirkabel Dengan Metode Evil Twin Attack Pada Kali Linux*.

Chow, E. 2011. *Ethical Hacking dan Penetration Testing*. IT Research Paper. Canada: The Centre for Information Integrity and Information Systems Assurance. University of Waterloo.

Cosmas Eko Suharyanto, P. S. (2017). Potential Threat Analysis Hypertext Transfer Protocol and Secure Hypertext Transfer Protocol of Public WiFi Users (Batam Case). International Journal of Scientific & Engineering Research, 8(3), 320– 326.

Gunawan. (2006). Penelitian Tindakan Kelas Proposal, analisis data, monitoring. Makalah disampaikan pada workshop.

https://id.wikipedia.org/wiki/Android_(sistem_operasi) diakses 3 april 2021.

Prasetya, A. (2012), Pengertian Hacker Beserta Tingkatannya dan Etika Hacker, Diakses 14 Juni 2014, dari http://alvaroaris.blogspot.com/2012/04/pengertian-hacker-beserta-tingkatannya.html.

Priandoyo, A. (2006), Vulnerablity Assessment untuk Meningkatkan Kesadaran Pentingnya Keamanan Informasi. Jurnal Sistem Informasi. Vol. 1, No. 2, pp.73-83.

Kennedy, D., Jim, O., Devons, K., & Mati, A. (2011). Metasploit The Penetration Tester's Guide. San Fransisco.

Nasir, M. (2003). Metode Penelitian. Jakarta. Halaman 54.

Rahman, A. (2014). *Rancangan Dan Impelemtasi Mikrotik Router OS pada Warung Internet QQ*. Jurusan Teknik Komputer AMIK GI MDP.

Ramachandran Vivek. (2012). *Backtrack 5 Wireless Penetration Testing*. PACKT Publishing.

Samsuar, L.D., & Gunawan, K. (2017). *Analisis Dan Evaluasi Tingkat Keamanan Jaringan Komputer Nirkabel (Wireless Lan); Studi Kasus Di Kampus Stmik Mataram*. Jurnal Ilmiah Teknologi Informasi Terapan Volume IV, No 1.

Saskara Gede, A. J. (2019*). Keamanan Jaringan Komputer Nirkabel Dengan Captive Portal Dan WPA/WPA2 Di Politeknik Ganesha Guru.* Jurnal Pendidikan Teknologi dan Kejuruan Vol. 16, No. 2.

Siregar, S. M. (2010), Istilah-istilah Pada Keamanan Komputer, Diakses 3 Juni 2014, dari http://sultanamuda.blogspot.com/2009/10/istilah-istilah-padakeamanan-komputer.html.

Sofana, Iwan. (2013). *Membangun Jaringan Komputer : Mudah membuat Jaringan Komputer (Wire & Wireless) untuk pengguna Windows dan Linux*. Bandung: Informatika.