Metode *Penetration Testing* pada Keamanan Jaringan Wireless Wardriving PT. Puma Makmur Aneka Engineering Bekasi

Rizky Wahyu Ismail [1], Rully Pramudita[2]

[1] Teknik Informatika; Universitas Bina Insani; Jln. Raya Siliwangi No. 6 Rawa Panjang Kota Bekasi, 021 82436886 / 021 82436996; e-mail: rizkywhsmail97@gmail.com
[2] Manajemen Informatika; Universitas Bina Insani; Jln. Raya Siliwangi No. 6 Rawa Panjang Kota Bekasi, 021 82436886 / 021 82436996; e-mail: rullypramudita@binainsani.ac.id

* Korespondensi: e-mail: rullypramudita@binainsani.ac.id

Diterima: 26 Juli 2020; Review: 28 Juli 2020; Disetujui: 10 Agustus 2020

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

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. PT. Puma Makmur Aneka Engineering sudah menggunakan *Wireless* sebagai penyedia internet yang dapat digunakan oleh pegawai. 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 PT. Puma Makmur Aneka Engineering karena data penting yang diolah menggunakan jaringan *Wireless* tidak terjamin keamanannya. Untuk mengetahui seberapa kuat keamanan jaringan *Wireless* pada PT. Puma Makmur Aneka Engineering, maka diperlukan analisis. Dari hasil analisis yang telah dilakukan, didapatlah kesimpulan bahwa jaringan *wireless* pada PT. Puma Makmur Aneka Engineering tidak aman karena masih ada titik *hotspot* yang dapat dilakukan *crack*.

Kata kunci: jaringan *wireless*, keamanan jaringan, *wardriving*, *wireless*

Abstract: *Wireless networks have been used as an excellent internet provider. By utilizing Wireless network, users can enjoy the internet without having to connect to a cable. PT. Puma Makmur Aneka Engineering Bekasi is already using Wireless as an internet provider that can be used by employees. A good Wireless Network must have good security to avoid the threat of crime. Wardriving is an activity where someone or a group of people equipped with the tools and expertise to access a Wireless network for free or without logging in. Wardriving is a threat to PT. Puma Makmur Aneka Engineering Bekasi because important data is processed using Wireless network is not guaranteed security. To find out how strong the security of Wireless network on PT. Puma Makmur Aneka Engineering Bekasi, then needed analysis. From the results of the analysis that has been done, got the conclusion that the wireless network on PT. Puma Makmur Aneka Engineering Bekasi not safe because there are still hotspots that can be done crack.*

Keywords*: network security, wardriving, wireless network, wireless*

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.

Keamanan jaringan sangat vital bagi sebuah jaringan komputer. Kelemahan-kelemahan yang terdapat pada jaringan komputer jika tidak dilindungi dan dijaga dengan baik akan menyebabkan hak akses bagi siapa saja tanpa diketahui ,kerugian berupa kehilangan data, kerusakan sistem server, tidak maksimal dalam melayani *user* atau bahkan kehilangan aset-aset berharga institusi.

PT.Puma Makmur Aneka Engineering adalah perusahaan yang bergerak dalam bidang *sealing element product*, *rubber finish production*, *polyurethane finish production, plant services, engineering services dan fabrication spare parts food industry dan pharmacy* PT Puma Makmur Aneka Engineering berdiri pada tanggal 16 januari 2007 di daerah Komplek Permata Cimahi Blok L-2 No. 03 RT 002 RW 014 Desa Tanimulya Kec Ngamprah, Bandung Barat. Pendiri sekaligus direktur utama PT Puma Makmur Aneka Engineering pada tanggal 12 Maret 2010 membuka cabang baru yang berlokasi di Jl. Kaliabang Blok A05 No.14 A Bekasi Utara.

Metode *Wardriving* adalah kegiatan yang bergerak mengelilingi area tertentu dan memetakan memetakan 4 populasi *access point wireless* untuk tujuan statistik. *Wardriving* bergerak mengelilingi area yang sudah dipetakan rutenya untuk menentukan *access point wireless* pada area tersebut [1]. Tujuan utama dari penilaian kerentanan adalah untuk mengidentifikasi kerentanan keamanan di bawah keadaan yang dikendalikan sehingaa mereka dapat dihilangkan sebelum pengguna yang tidak berwenang mengeksploitasi mereka [2]. Oleh karena itu dibutuhkan pengujian jaringan *wireless wardriving* pada jaringan perusahaan menggunakan metode *penetration testing* yang bertujuan untuk mengetahui tingkat keamanan jaringan perusahaan.

Keamanan jaringan komputer saat ini telah menjadi isu utama di dunia. Hal ini dikarenakan dunia telah semakin sempit dengan terkoneksinya dalam sebuah internet sebagai *open system interconnection.* Dengan internet kita dapat mengakses dan berkomunikasi dengan orang lain dan banyak hal lainnya. Hal tersebut memang memudahkan transfer informasi akan tetapi juga membawa efek *negative* dengan keamanan informasi kita.[3]

Sebuah jaringan yang biasanya terdiri dari dua atau lebih komputer yang saling berhubungan diantara satu dengan yang lainnya, dan saling berbagi sumber daya misalnya *CDROM, Printer*, Pertukaran *File*, atau memungkinkan untuk saling berkomunikasi secara elektronik.[4]

Topologi berhubungan dengan struktur dan teknologi yang digunakarn oleh Jaringan komputer. Bayangkan jaringan komputer seperti jalan-jalan yang menghubungkan rumah, gedung, dan tempat-tempat lain pada sebuah kota. Agar lalu lintas menjadi teratur tentunya harus ada suatu aturan dan sistem yang diberlakukan kepada pengguna jalan.[5]

Jaringan *wireless* adalah jaringan yang memungkinkan pengiriman informasi (atau data) antar *host* dilakukan tanpa menggunakan media kabel. Jaringan *wireless* atau teknologi *wireless* ini mengunakan gelombang *elektromagnetik* untuk membawa informasi antara satu *host* dengan *host* lainnya.[6]

Keamanan system *wireless* bisa dibagi menjadi empat bagian yaitu a) Keamanan aplikasi. Yang berarti keamanan aplikasi *user* dan aplikasi standar seperti email. b) Keamanan perangkat. Bagaimana memproteksi perangkat fisik dari kasus kerusakan, hilang ataupun dicuri. c) Keamanan dari komunikasi *wireless*. Bagaimana memproteksi pesan saat dikirimkan. d) Keamanan server yang terkoneksi menggunakan internet atau jaringan kabel. Resiko serangan yang mungkin akan terjadi pada standard 802.11b dapat dikatagorikan kedalam tujuh jenis serangan, yaitu *Insertion Attack, Interception* dan *Monitoring Traffic Wireless, Jamming* (dikenal dengan *denial of service*), *Client-to-Client Attack, Brute Force Attack Againts Access point Password, Attack againts encription,*dan *Misconfiguratio.* [7]

Firewall adalah sebuah sistem pengaman, jadi firewall bisa berupa apapun baik *hardware* maupun *software*. *Firewall* dapat digunakan untuk memfilter paket-paket dari luar dan dalam jaringan di mana ia berada. Jika pada kondisi normal semua orang dari luar jaringan anda dapat bermain-main ke komputer anda, dengan *firewall* semua itu dapat diatasi dengan mudah.[8]

ISSN: 2528-6919 (Online); 53 – 62

Common Vulnerability Scoring System (CVSS) merupakan sebuah kerangka (*framework*) terbuka yang digunakan untuk mengkomunikasikan karakteristik dan dampak yang ditimbulkan oleh sebuah kerentanan aplikasi.[9]

Tabel 1. *NVD Vulnerability Severity Ratings*

Severity	***Base Score Range***
Low	0.0-3.9
Medium	4.0-6.9
High	7.0-10.0

Sumber: https://nvd.nist.gov/vuln-metrics/cvss

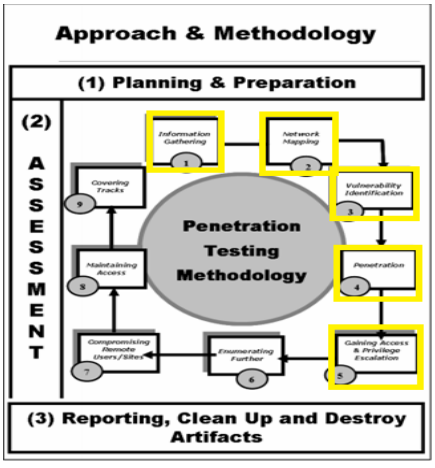
Tujuan utama dari penilaian kerentanan adalah untuk mengidentifikasi kerentanan keamanan di bawah keadaan yang dikendalikan sehingaa mereka dapat dihilangkan sebelum pengguna yang tidak berwenang mengeksploitasi mereka. Ahli sistem komputasi menggunakan uji penetrasi untuk mengatasi masalah yang melekat dalam penilaian kerentanan, dengan fokus pada kerentanan dengan tingkat keparahan yang tinggi. Uji penetrasi adalah alat penilaian jaminan bernilai yang menguntungkan baik bisnis dan operasinya.[10]

Wardriving adalah tindakan mencari *Wi-Fi* jaringan nirkabel oleh seseorang dalam kendaraan yang bergerak , menggunakan komputer portable , smartphone atau personal digital assistant (PDA). Istilah ini mulai berkembang karna teknologi yang semakin hari semakin cepat kemajuannya. Banyak programmer yang berlomba lomba membuat tools baru untuk membobol jaringan yang bersifat *Wireless*.[11]

Pada penelitian kualitatif, kualitas riset sangat tergantung pada kualitas dan kelengkapan data yang dihasilkan. Pertanyaan yang selalu diperhatikan dalam pengumpulan data adalah apa, siapa, dimana, kapan, dan bagaimana. Penelitian kualitatif bertumpu pada triangulation data yang dihasilkan dari tigametode : *interview*, *participan to observation*, dan telaah catatan organisasi (*document records*).[12]

2. Metode Penelitian

Model pengembangan adalah suatu perencanaan yang digunakan dalam merencanakan penelitian ataupun pengembangan. Model pengembangan yang dilakukan untuk melakukan Pengujian Keamanan Jaringan *Wireless Wardriving* Menggunakan Metode *Penetration Testing* Pada PT. Puma Makmur Aneka Engineering Bekasi adalah *Penetration Testing*.



Sumber: Pujiarto, dkk (2013)

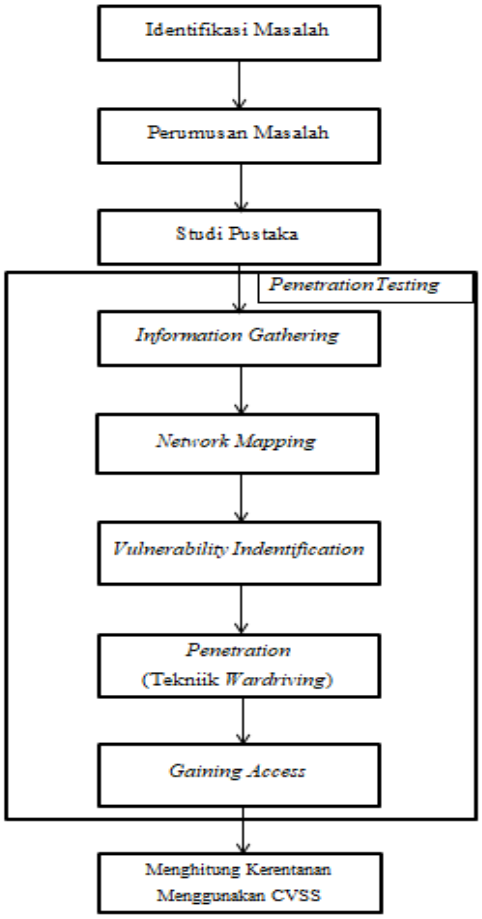
Gambar 1 *Penetration Testing Methodology*

Pada penelitian ini menggunakan metode *penetration testing* yang terdiri dari tahapan, *Planning and Preperation* tahap ini merupakan tahap pengenalan dan penyesuaian antara pelaku dan pihak yang akan dijadikan objek dengan saling bertukar informasi. Kesepakatan

kedua pihak sangat dibutuhkan untuk perlindungan hukum bersama. Tahap ini juga menentukan tim yang terlibat dalam pengujian, rencana waktu yang tepat dan aturan lainnya.

Assessment Tahap ini merupakan tahap dilakukan *penetration testing* yang terdiri dari beberapa pendekatan berlapis. *Layer-layer* disini adalah sebagai berikut a) *Information Gathering* Ini adalah tahap awal audit keamanan informasi, yang cenderung dimiliki banyak orang mengabaikan. Saat melakukan tes apapun pada sistem informasi, informasi pengumpulan dan pengumpulan data sangat penting dan memberi Anda semua informasi yang mungkin untuk melanjutkan tes. Sementara melakukan pengumpulan informasi, penting untuk diperhatikan sebagai imajinatif mungkin. b) *Network Mapping* Pemetaan jaringan akan membantu asesor menyempurnakan informasi sebelumnya diperoleh dan untuk mengkonfirmasi atau memberhentikan beberapa hipotesis mengenai sistem target (tujuan, merek perangkat lunak / perangkat keras, konfigurasi, ar*site*ktur, hubungan dengan sumber daya dan hubungan lain dengan proses bisnis). c) *Vulnerability Identification* Selama identifikasi kerentanan, penilai akan melakukan beberapa kegiatan untuk mendeteksi titik lemah yang dapat dieksploitasi. d) *Penetration* Penilai mencoba untuk mendapatkan akses yang tidak sah dengan menghindari keamanan Langkah-langkah di tempat dan mencoba mencapai tingkat akses seluas mungkin. e) *Gaining Access* Kegiatan di bagian ini akan memungkinkan para penilai untuk mengkonfirmasi dan mendokumentasikan kemungkinan gangguan dan atau serangan otomatis hal ini memungkinkan dilakukannya penilaian dampak yang lebih baik untuk target organisasi secara keseluruhan.

Reporting, Clean Up and Destroy Artefacts Tahap akhir dari pengujian dengan membuat beberapa laporan hasil penemuan selama melakukan *penetration testing*. Setelah melakukan tindakan perlu menghapus *log* yang bisa membahayakan sistem yang dapat dimanfaatkan orang lain.



Sumber : Hasil Penelitian (2020)

Gambar 2. Kerangka Pemikiran

ISSN: 2528-6919 (Online); 53 – 62

3. Hasil dan Pembahasan

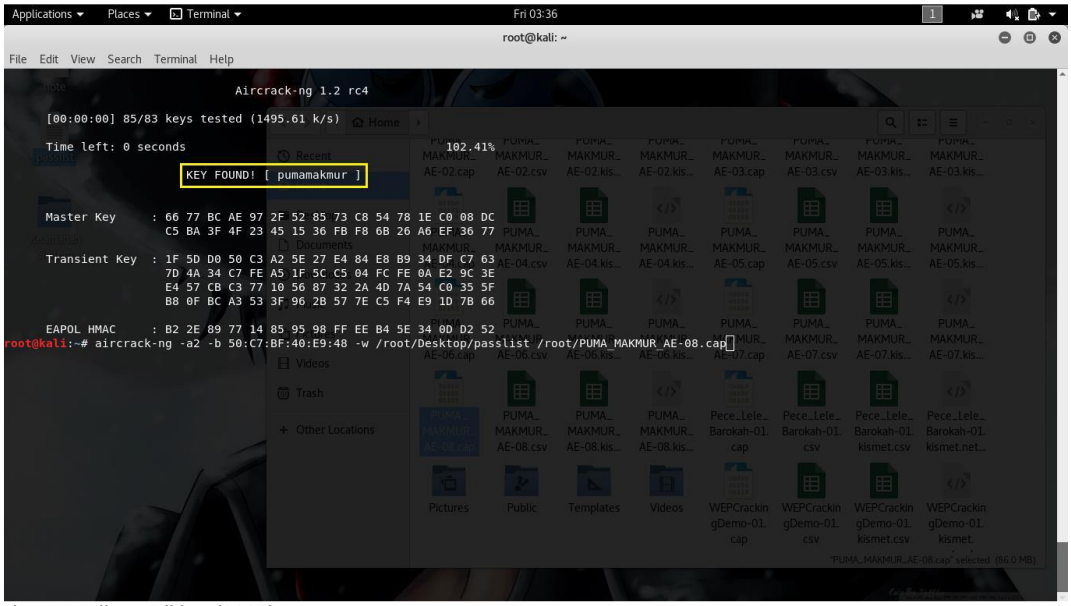
Information Gathering, *p*ada tahap ini dilakukan proses pencarian data berupa *SSID* target, *MAC Address*, dan keamanan *access point*. *SSID* yang bernama Puma Makmur AE, *MAC Address*-nya adalah 50:c7:bf:40:e9:48 dan keamanan *access point*-nya *WPA2 Key*. Berdasarkan data yang didapat dengan menggunakan aplikasi *Wigle Wifi* pada *Android*, ditemukan *access point* target dengan *SSID* bernama Puma Makmur AE, *Mac Address* 50:c7:bf:40:e9:48 dan keamanan *WPA2 Key*. Pada tahap ini sama seperti scanning mengunakan *Wigle Wifi* di *Android* yang ditemukannya *SSID* target dengan nama Puma Makmur AE, *MAC Address* 50:c7:bf:40:e9:48, dan keamanan *access point* menggunakan *WPA2 Key*.

Sumber : Hasil Penelitian (2020)

Gambar 3 Pencarian *Wifi Wardriving*

Network Mapping*, p*ada proses bertujuan untuk mencari celah pada *access point* yang di uji dan sebelumnya sudah mendapatkan ip dan akses untuk masuk ke dalam *access point*. IP yang didapat adalah 192.168.1. 1) IP tersebut didapatkan dari melihat bagian belakang *access point. 1) Vulnerability Identification, p*ada tahap ini disimpulkan bahwa hasil dari *Information Gathering* ditemukan kerentanan yang dapat diuji berupa serangan *WPA Cracking, DoS, Password Login Router Wireless Cracking. 2) Penetration, p*ada tahap ini dilakukan penyerang terhadap access point target dengan melakukan kemungkinan yang terjadi pada *Vulnerability Identification*. Pada proses penetration terdapat beberapa tahapan, tahapan pertama *WPA*

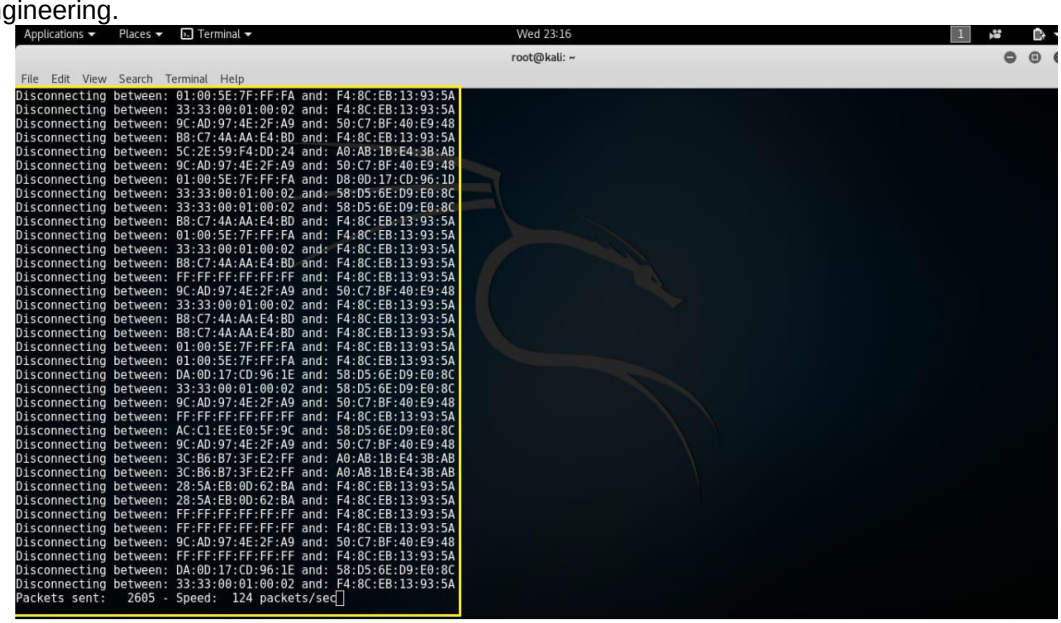
*Cracking, p*ada tahap ini dilakukan proses pencarian *WPA2 Key* menggunakan *Aircrack-ng*. Pada tahap ini telah ditemukan *password access point* "pumamakmur" pada *wifi* target dan disimpulkan bahwa *WPA2 Key* dapat di *crack*.



Sumber : Hasil Penelitian (2020)

Gambar 4 Hasil *WPA Cracking*

Tahapan kedua *DoS,* pada tahap ini telah ditemukan *password access point* "pumamakmur" pada *wifi* target dan disimpulkan bahwa *WPA2 Key* dapat di *crack*. Pada tahap ini dilakukan proses *DoS* untuk memutuskan jaringan *wireless* pada PT. Puma Makmur Aneka Engineering.



Sumber : Hasil Penelitian (2020)

Gambar 5. Hasil *DoS*

Tahapan ketiga *password login router wireless cracking*, pada tahap ini dilakukan proses cracking untuk masuk kedalam *Login router wireless* agar hak aksesnya dapat diubah – ubah seperti membatasi pengguna, menambahkan jumlah SSID didalam satu *Access Point*, dan mengganti password wireless maupun nama SSID nya. Tahapan ke empat *Access Point Isolation,* pada tahap ini dilakukan pengujian terhadap *access point* untuk mengetahui apakah *access point* sudah menyalakan fitur *access point isolation* pada *access point*. Hasil dari

ISSN: 2528-6919 (Online); 53 – 62

scanning host pada aplikasi *ettercap* di *kali linux* ditemukan host, dapat disimpulkan bahwa *access point* tidak menyalakan fitur *access point isolation* pada *access point*. Hal ini dapat berdampak pada serangan dari dalam atau *Client to Client.* Serta tahapan terakhir pada penetration adalah *Gaining Access,* tahap ini adalah tahap proses untuk memakai atau menggunakan *password* atau *WPA key* yang didapat pada proses *penetration*.

Pengujian Kondisi Infrastruktur Jaringan setelah ditemukannya masalah yang ada pada jaringan wireless PT. Puma Makmur Aneka Engineering, maka adapun pengujian perhitungan nilai kerentanan yang dilakukan yaitu Perhitungan Nilai Kerentanan. Setelah pengujian dilakukan pada *access point* target, maka setelah itu dilakukan perhitungan tingkat kerentanan menggunakan *CVSS*. Berikut hasil dari nilai kerentanan pada *Access Point* jaringan PT. Puma Makmur Aneka Engineering. Pada proses perhitungan nilai kerentanan ini didapatkan hasil sebagai berikut a) *WPA2 Cracking,* berdasarkan hasil perhitungan yang telah dilakukan, dampak kerentanan dari serangan *WPA2 Cracking* untuk tingkat kerentanan sedang karena *password* yang digunakan belum menggunakan karakter yang unik dan kuat minimal 15 karakter. b) *DoS, b*erdasarkan hasil perhitungan yang telah dilakukan dampak kerentanan dari serangan *DoS* untuk tingkat kerentanan tinggi karena proses memutuskan koneksi *Client* dalam *access point* sangat mudah karena hanya membutuhkan *MAC Address* dan *SSID* dari *Access Point. c) Password Router Wireless Cracking,* berdasarkan hasil perhitungan yang telah dilakukan dampak kerentanan dari serangan *Password Router Wireless Cracking* untuk tingkat kerentanan tinggi karena *access point* hanya menggunakan *password default*. d) *Access Point Isolation,* berdasarkan hasil perhitungan yang telah dilakukan dampak kerentanan dari serangan *Access Point Isolation* untuk tingkat kerentanan sedang karena disebabkan *Client* dapat menyerang *Client* atau *Client to Client* hanya dengan menyamakan *workgroup client* saja.

Berdasarkan hasil perhitungan nilai kerentanan maka dibuatlah solusi perbaikan kerentanan. Berikut tabel dari solusi perbaikan kerentanan:

Tabel 2. Solusi Perbaikan Kerentanan *Access Point* Puma Makmur AE.

No.	Serangan	Kerentanan	Solusi Perbaikan
1.	*WPA2 Cracking*	Berhasil mendapatkan *Password Wifi* yang *valid*.	Menggunakan *WPA2 Key* yang unik dan kuat minimal 15 karakter
2.	*DoS*	Menyebabkan koneksi jaringan terputus	Menggunakan antena *sectoral* sebagai antena jaringan *wireless*
3.	*Passwordd Router Wireless Cracking*	Berhasil mendapatkan *Username* dan *Password* untuk *login* pada *Web Router Wireless*	Menggunakan *Password* yang unik dan kuat minimal 15 karakter
4.	*Access Point Isolation*	Sesama *Client* dapat melakukan *PING* dan dapat terkena serangan *ARP Poisoning*	Melakukan konfigurasi *AP Isolation* pada *Access Point*

Sumber : Hasil Penelitian (2020)

Setelah dilakukannya perhitungan pengujian kondisi inftastuktur jaringan wireless pada PT. Puma Makmur Aneka Engineering maka dilanjutkan dengan memperbaiki hasil kerentanan dan melakukan pengujian. Untuk perbaikan hasil kerentanan dilakukan setelah melakukan pengujian kerentanan dan melakukan perhitungan tingkat kerentanan yang ada, tahap selanjutanya adalah melakukan perbaikan sesuai dengan solusi perbaikan kerentanan. a) Proses Mengganti *WPA2 Key,* pada tahap ini dilakukan proses pernggantian *WPA2 Key* pada *Access Point* dengan *WPA2 Key* menggunakan karakter yang unik. Maksud digantinya *Password Wireless* pada *Access Point* adalah untuk meminimalisir pengguna asing yang sering masuk ke dalam *Access Point* kantor PT. Puma Makmur Aneka Engineering yang menyebabkan kinerja karyawan tidak maksimal. b) *DoS, b*erdasarkan tabel solusi kerentanan yang telah diberikan, maka harus diganti dengan antena *sectoral*. Namun dengan kondisi yang ada, tidak memungkinkan untuk melakukan pergantian perangkat untuk menggunakan antena *sectoral* sehingga kerentanan pada *DoS* tidak mengurangi tingkat kerentanannya. c) Proses Mengganti *Password Router Wireless,* pada tahap ini dilakukan proses *penggantian Password Router Wireless* pada *Access Point*. Maksud digantinya *Password Router Wireless* pada *Access Point* adalah untuk meminimalisir pengguna asing yang sering masuk ke dalam *Access Point* kantor PT. Puma Makmur Aneka Engineering. d) Proses menghidupkan *Mode AP Isolation, p*ada tahap ini dilakukan proses menyalakan *mode Access Point Isolation.*

Langkah selanjutnya adalaha pengujian hasil perbaikan, hal ini dilakukan guna mengetahui apakah pengujian ulang membuahkan hasil yang berbeda dari hasil yang telah dilakukan dalam pengujian kerentanan pada *Access Point* Puma Makmur AE. a) *WPA2 Cracking,* berdasarkan hasil *WPA2 Cracking* yang dilakukan tidak ditemukannya *WPA2 Key* maka disimpulkan bahwa Proses *Cracking* pada *WPA2 key* tersebut aman karena sudah menggunakan *password* yang unik. Dengan mengganti password yang unik di harapkan meminimalisir *cracking* oleh orang yang tidak bertanggung jawab. b) *DoS,* berdasarkan solusi perbaikan kerentanan yang telah dipaparkan sebelumnya, menggunakan antena sectoral untuk mencegas terjadinya serangan *DoS* adalah solusinya. Namun pada kondisi yang ada, tidak memungkinkan untuk menggunakan antena *sectoral*. Sehingga kerentanan pada *DoS Attack* tidak dapat dilakukan perbaikan. c) *Password Router Wireless Cracking*, berdasarkan hasil *Password Router Wireless Cracking* yang dilakukan tidak ditemukannya *Username* dan *Password* dalam proses *cracking* menggunakan *Hydra*, hal tersebut dinyatakan aman karena menggunakan *password* yang unik. d) *AP Isolation Testing,* berdasarkan hasil *AP Isolation* yang dilakukan tidak ditemukannya *Client* yang terhubung dengan *access point* Puma Makmur AE, maka disimpulkan bahwa *Client* dan *Client* tidak bisa saling melakukan *PING*.

Dari semua proses yang dilakukan didapatkan hasil status perbaikan yang digambarkan pada tabel dibawah ini:

Tabel 3. Status Nilai Kerentanan Yang Sedang Berjalan

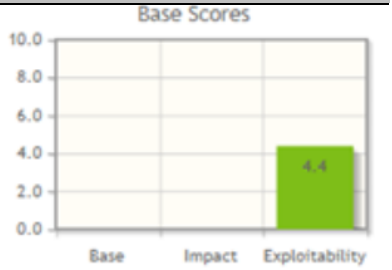
No.	Pengujian	Hasil Pengujian	Status
1.	*WPA2 Cracking*	*WPA2 Key* tidak dapat ditemukan	Aman
2.	*DoS*	Koneksi masih terputus sehingga tidak dapat menggunakan internet	Tidak Aman
3.	*Password Router Wireless Cracking*	*Password Router Wireless Cracking* tidak berhasil ditemukan	Aman
4.	*Access Point Isolation*	Koneksi *Client to Client* tidak bisa melakukan *PING*	Aman

Hasil Penelitian (2020)

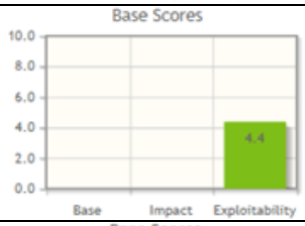
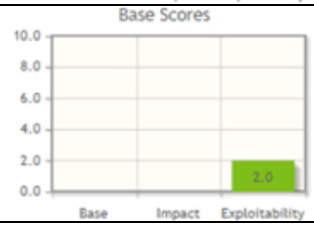
Untuk mengetahui tingkat penurunan nilai kerentanan dan resiko yang telah diperbaiki, maka dilakukan kembali perhitungan terhadap hasil perbaikan menggunakan *CVSS Version 2* seperti berikut a) *WPA2 Cracking,* berdasarkan hasil perhitungan yang telah dilakukan, dampak kerentanan dari serangan *WPA2 Cracking* mengalami penurunan karena telah menggunakan *password* dengan karakter yang unik. b) *DoS,* berdasarkan hasil perhitungan yang telah dilakukan dampak kerentanan dari serangan *DoS* untuk tingkat kerentanan tinggi proses memutuskan koneksi *Client* dalam *access point* sangat mudah karena hanya membutuhkan *MAC Address* dan *SSID* dari *Access Point*. c) *Password Wireless Router Cracking,* berdasarkan hasil perhitungan yang telah dilakukan, dampak kerentanan dari serangan *Password Router Wireless Cracking* mengalami penurunan karena telah menggunakan *password* dengan karakter yang unik. d) *Access Point Isolation,* berdasarkan hasil perhitungan yang telah dilakukan, dampak kerentanan dari serangan *Access Point Isolation Testing* mengalami penurunan karena *client* tidak dapat menyerang ke *client* dengan mudah.

Berikut ini merupakan grafik perbandingan nilai kerentanan sebelum dan setelah dilakukan perbaikan terhadap masalah kerentanan yang ditemukan pada PT. Puma Makmur Aneka Engineering:

Tabel 4. Perbandingan Perhitungan Kerentanan Sebelum Perbaikan Dengan Setelah Perbaikan

No.	Pengujian	Sebelum Dilakukan Perbaikan	Sesudah Dilakukan Perbaikan
1.	*WPA2 Cracking*		

ISSN: 2528-6919 (Online); 53 – 62

No.	Pengujian	Sebelum Dilakukan Perbaikan	Sesudah Dilakukan Perbaikan
2.	*DoS*		
3.	*Password Router Wireless Cracking*		
4.	*Access Point Isolation*		

Sumber : Hasil Penelitian (2020)

Setelah dilakukannya pengujian terlihat pada grafik diatas bahwa sebelum dan sesudah dilakukannya pengujian jaringan wireless pada PT. Puma Makmur Aneka Engineering menunjukan penurunan tingkat grafik kecuali pengujian *DoS.* Karena berdasarkan solusi perbaikan kerentanan yang telah dipaparkan sebelumnya, menggunakan antena sectoral untuk mencegas terjadinya serangan *DoS* adalah solusinya.

4. Kesimpulan

Berdasarkan pengujian kerentanan yang dilakukan yaitu pengujian keamanan jaringan *wireless wardriving* menggunakan metode *Penetration Testing* pada PT. Puma Makmur Aneka Engineering, maka dapat diambil kesimpulan bahwa pengujian keamanan jaringan internal dan publik telah dilakukan dengan menggunakan metode *Penetration Testing* dan mendapatkan kerentanan seperti *WPA2 Cracking, Dos, Paswword Router Wireless Cracking,* dan *AP Isolation Testing* sehingga diketahui kerentanan pada jaringan internal dan publik. Setiap kerentanan yang ditemukan telah dilakukan perbaikan sehingga resiko dapat diturunkan. Penghitungan kerentanan telah dilakukan menggunakan *CVSS Calculator Version 2* sehingga didapatkan hasil nilai kerentanan disetiap perangkat jaringan yang dimiliki oleh perusahaan. Kerentanan yang ditemukan juga telah diatasi kemudian dilakukan perhitungan nilai kerentanan setelah proses perbaikan. Hasil perhitungan setelah perbaikan didapatkan penurunan resiko yang baik sehingga dapat dinyatakan bahwa jaringan perusahaan memiliki tingkat keamanan yang lebih baik. Dengan pengujian standar keamanan jaringan *wireless* ini, diharapkan aktivitas di PT. Puma Makmur Aneka Engineering dapat lebih efektif dan lebih efisien.

Referensi

[1] Jamaludin. 2019. Teknik Keamanan Jaringan *Wireless LAN* Pada Warnet Salsabila *Computer Net*. 1: 67–74
[2] Kawasati R. 2016. Teknik Pengumpulan Data Metode Kualitatif. 4.
[3] Primartha R. 2018. *SECURITY* JARINGAN KOMPUTER BERBASIS CEH. Bandung: Informatika Bandung.
[4] Rachmat FA. 2016. War Driving Menggunakan *Tools* " *Wigle* " dan *Mapping* Menggunakan "*GoogleEarth* " Dikawasan PemKab OI (Ogan Ilir). 1: 1–6.
[5] Riadi H. 2016. ANALISIS DAN OPTIMALISASI JARINGAN MENGGUNAKAN TEKNIK *LOAD BALANCING* (Studi Kasus : Jaringan UAD Kampus 3). 2: 1370–1378.

[6] Sari MW. 2014. Analisis Keamanan Jaringan *Wireless Local Area Network (WLAN)* Menggunakan Metode *Wardriving* Di Fakultas Teknik Universitas PGRI Yogyakarta. Yogyakarta. Jurnal Teknologi Informasi Respati
[7] Sondakh G, Najoan MEI, Lumenta AS. 2014. Perancangan *Filtering Firewall* Menggunakan *Iptables* Di Jaringan Pusat Teknologi Informasi Unsrat. 19–27.
[8] Tania AM, Setiyadi D, Khasanah FN. 2018. Keamanan *Website* Menggunakan *Vulnerabillity Assesment*. 2: 171-180
[9] Tarigan BV, Kusyanti A, Yahya W. 2017. Analisis Perbandingan Penetration Testing Tool Untuk Aplikasi Web. 1: 206–214.
[10] Towidjojo R, Eno M. 2015. Router Mikrotik : Implementasi *Wireless LAN Indoor*. Jasakom
[11] Yuliandoko H. 2018. Jaringan Komputer *Wire* dan *Wireless* Beserta Penerapannya. Yogyakarta. Deepublish.