CESS (Journal of Computing Engineering, System and Science) *e-ISSN: 2502-714x*
Vol. 9, No. 2, Juli 2024, pp.750-765 *p-ISSN: 2502-7131*

Contents list available at www.jurnal.unimed.ac.id

CESS
(Journal of Computing Engineering, System and Science)

journal homepage: https://jurnal.unimed.ac.id/2012/index.php/cess

Analisa Sistem Keamanan Jaringan Nirkabel Menggunakan Kerangka Kerja Issaf Pada PT. Gerak Puncak Lancar

Wireless Network Security System Analysis Using the Issaf Framework at PT. Gerak Puncak Lancar

Ari Nur Shaffan[1*], Nungky Awang Chandra[2], Alfin Hikmaturokhman[3]

[1,2]Teknik Informatika, Universitas Mercu Buana
Jl. Meruya Selatan No.1, RT.4/RW.1, Joglo, Jakarta 11650
[3]Teknik Telekomunikasi, Institut Teknologi Telkom Purwokerto
Jl. DI Panjaitan No.128, Karangreja, Kabupaten Banyumas, Jawa Tengah 53147
email: [1]arinurshaffan57@gmail.com, [2]nungkyac@yahoo.co.id, [3]alfin.hikmaturokhman@gmail.com

A B S T R A K

Keamanan data sebuah perusahaan adalah suatu hal yang sangat penting, maka diperlukannya keamanan untuk menjaga data-data penting tersebut agar tidak disalahgunakan. Salah satu celah yang dapat diserang ialah jaringan *nirkabel* karena dapat terlihat oleh publik. Pada PT. Gerak Puncak Lancar sendiri mempunyai jaringan nirkabel untuk akses internet karyawannya. Penelitian ini bertujuan untuk menguji seberapa kuat sistem keamanan dari perusahaan tersebut dengan metode *Penetration Test* ISSAF. ISSAF merupakan sebuah *framework* standar pengujian *Penetration Test* untuk berbagai keamanan. Seperti keamanan WLAN, website, keamanan Router, keamanan *Firewall* dan lain-lainnya. ISSAF sendiri mempunyai 9 aktivitas atau langkah meliputi Information *Gathering, Network Mapping, Vulnerability Identification, Penetration, Gaining Access & Privilage Escalation, Enumerating Further, Compromise Remote User/Sites, Maintaining Access dan Covering tracks*. Untuk WLAN *Security Assessment* sendiri mempunyai 6 tahap yakni, *Information Gathering, Scanning, Audit, Analysis & Research, Exploit & Attacks, Reporting & Presentation*. Hasil analisa penelitian ini, keamanan jaringan *nirkabel Access Point* staff PT. Gerak Puncak Lancar. Mempunyai nilai *Overall Risk Rating* tinggi atau High. Evaluasi pun dilakukan pada keamanan jaringan PT. Gerak Puncak Lancar, dan hasil evaluasi tersebut menurunkan *Overall Risak Rating* menjadi Medium.

Kata Kunci: *Uji Penestrasi; ISSAF; WLAN; Keamanan Jaringan; Aircrack-ng*

**Penulis Korespondensi:*
email: arinurshaffan57@gmail.com

A B S T R A C T
The security of a company's data is highly important, requiring measures to protect the crucial information from potential misuse. One vulnerability lies in the wireless network, which can be visible to the public. PT. Gerak Puncak Lancar has its own wireless network for its employees' internet access. This research aims to assess the strength of the company's security system using the ISSAF Penetration Test method, a standard framework for testing various security aspects like WLAN, website, router, firewall, and more. ISSAF involves 9 activities, including Information Gathering, Network Mapping, Vulnerability Identification, Penetration, Gaining Access & Privilege Escalation, Enumerating Further, Compromising Remote Users/Sites, Maintaining Access, and Covering Tracks. The WLAN Security Assessment has 6 stages: Information Gathering, Scanning, Audit, Analysis & Research, Exploit & Attacks, and Reporting & Presentation. The research analysis results indicate that the wireless network security of PT. Gerak Puncak Lancar's staff Access Point has a high Overall Risk Rating. An evaluation was conducted on the network security of PT. Gerak Puncak Lancar, and the evaluation results lowered the Overall Risk Rating to Medium.

Keywords: *Pentest; ISSAF; WLAN; Network Security; Aircrack-ng*

1. PENDAHULUAN

Pada awal tahun 2023, *cyber attacks* mengalami penurunan, dibandingkan pada akhir tahun 2022 dengan jumlah serangan tertinggi 3,314,301 serangan. Namun, pada bulan oktober 2023, *cyber attack* mengalami kenaikan yang hampir mendekati seperti tahun 2022, yaitu 3,231,537 serangan kenaikan yang cukup drastis dibandingkan tahun 2023 awal yang hanya 522,215[1].

Sebuah perusahaan yang mempunyai sistem keamanan yang minim pastinya akan rawan sekali terserang oleh pihak yang tidak bertanggung jawab, yang dapat beresiko pencurian data internal, penanaman *backdoor*, MITM (*man-in-the-middle*) dan hal-hal lainnya yang dapat merugikan perusahaan tersebut. Oleh karena itu, dilakukan sebuah *penetration test*, untuk menguji keamanan jaringan sebuah perusahaan, pada penelitian ini, penulis mencoba untuk menggunakan standard ISSAF untuk melakukan *penetration test*. Pentingnya analisis sistem keamanan jaringan nirkabel tidak hanya terkait dengan melindungi data dan informasi sensitif perusahaan, tetapi juga dengan menjaga kontinuitas operasional dan reputasi bisnis. Keberhasilan penelitian ini akan memberikan panduan yang jelas untuk memperkuat keamanan jaringan nirkabel PT. Gerak Puncak Lancar dan memberikan perlindungan yang lebih baik terhadap ancaman siber yang selalu berkembang. Dengan demikian, penelitian ini berkontribusi pada upaya menjaga keandalan dan integritas jaringan nirkabel dalam mendukung operasi bisnis PT. Gerak Puncak Lancar.

ISSAF (*Information System Security Assessment Framework*) ISSAF merupakan *framework* untuk menguji keamanan jaringan, ISSAF telah dikembangkan oleh sekelompok peneliti pada bidang keamanan sistem informasi dan jaringan komputer. ISSAF akan mengevaluasi dengan cara melakukan pengujian layaknya penyerangan yang dilakukan oleh pihak yang tidak bertanggung jawab secara nyata. Orang-orang yang melakukan penetration test atau disebut *penetration tester* merupakan *ethical hacker* yang melakukan eksperimen ekstrim untuk menilai keamanan jaringan sebuah organisasi atau perusahaan dan keamanan data pada organisasi atau perusahaan tersebut[2].

Peneliti melakukan pengamatan dan menemukan bahwa sistem keamanan jaringan nirkabel pada PT. Gerak Puncak Lancar sangat standar, SSID (service set identifier) dapat dilihat oleh publik, serta tidak ada keamanan pendukung lainnya. untuk membantu mencegah serangan para pihak yang tidak bertanggung jawab. Keamanan yang digunakan pada perusahaan ini hanyalah WPA/PSK2.

Diketahui bahwa sebelumnya belum pernah terjadi serangan siber di perusahaan ini. Dengan itu peneliti menggunakan metode Delphi untuk memutuskan apakah pengujian *penetration test* benar-benar diperlukan pada perusahaan ini. Menurut Witkins (1984) mendefinisikan teknik delphi sebagai cara untuk menentukan pendapat secara konsensus (mufakat) di antara para pakar mengenai tujuan dan kebutuhan yang mendesak dari suatu institusi.[3] Peneliti menanyakan pertanyaan mengenai keamanan informasi ke beberapa ahli IT di kantor, dan mendapatkan konsensus sebagai berikut:

- Mayoritas ahli sepakat bahwa *penetration test* diperlukan untuk mengidentifikasi dan mengatasi kelemahan dalam jaringan nirkabel PT. Gerak Puncak Lancar
- Rekomendasi khusus adalah memfokuskan *penetration test* pada konfigurasi perangkat dan penggunaan protokol keamanan.
- Rekomendasi tambahan mencakup pertimbangan biaya dan dampak operasional sebagai faktor penting dalam keputusan.

Berdasarkan hasil pengamatan dan konsensus diatas, peneliti tertarik untuk melakukan lebih lanjut tentang seberapa kuat keamanan jaringan pada PT. Gerak Puncak Lancar, penelitian ini bertujuan untuk mengevaluasi keamanan jaringan, agar mencegah serangan pihak yang tidak bertanggung jawab di kemudian hari.

Peneliti ingin berfokus kepada mencari celah keamanan pada sistem keamanan jaringan wireless perusahaan. Untuk metodologi ISSAF, akan lebih berfokus pada information gathering, penetration test, hingga melakukan reporting. Penelitian ini juga menggunakan metologi OWASP yang bertujuan agar proses Reporting lebih detail dan spesifik. Dengan adanya OWASP ini akan menjadi pembeda antara penelitian sebelumnya.

2. TINJAUAN PUSTAKA

2.1. Wireless Local Area Network

WLAN (*Wireless Local Area Network*) atau IEEE 802.11 merupakan sebuah jaringan lokal area network nirkabel, WLAN menggunakan gelombang frekuensi radio untuk transfer data ke perangkat-perangkat lainnya. Pada saat ini, WLAN mempunyai 2 gelombang frekuensi, yaitu 2,4Ghz dan 5Ghz. Beberapa standar teknologi dari wireless yaitu, 802.11b, 802.11g, 802.11n, 802.11ac, dan 802.11ax. perkembangan lebih lanjut dalam bentuk WiFi 7 juga sedang dalam pengembangan. Standar terbaru ini akan membawa teknologi jaringan nirkabel ke tingkat yang lebih tinggi dengan kemampuan yang lebih canggih dan kecepatan transfer data yang lebih tinggi, mendukung aplikasi masa depan seperti realitas virtual, Internet of Things (IoT), dan kecerdasan buatan. Seiring dengan evolusi ini, IEEE tetap berperan dalam merumuskan standar yang memandu perkembangan jaringan nirkabel. [4]

2.2. Penetration Testing

Penetration Testing adalah upaya untuk mencoba mengeksploitasi sistem dengan cara yang diizinkan untuk menemukan potensi celah atau kerentanannya dalam sistem tersebut. [5]. Penetration Testing dapat membantu organisasi atau individu dalam meningkatkan keamanan sistem mereka dengan mengidentifikasi masalah keamanan yang ada.

Ada tiga strategi *Penetration Test* yang dikenal yang digunakan oleh penguji profesional. Berikut tiga teknik Penetration Test tersebut:

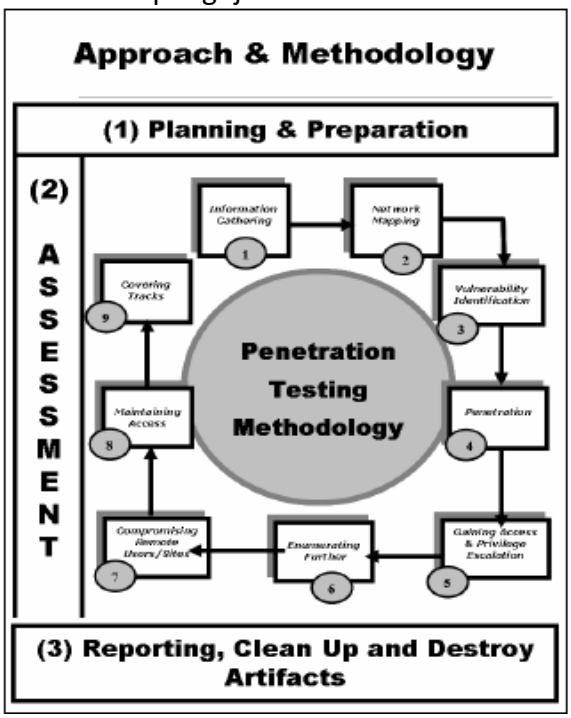
a. *Black Box Testing*
   BlackBox adalah teknik pengujian di mana penguji tidak mengetahui desain atau struktur internal target. Mereka harus memeriksa kesalahan pada fungsi yang salah atau hilang, atau kesalahan antarmuka. Strategi ini menyerupai blindtest dan prosedur yang diterapkan oleh penyerang sungguhan yang tidak memiliki pengetahuan atau informasi tentang jaringan organisasi.
b. *White Box Testing*
   Dalam teknik pengujian penetrasi WhiteBox, penguji memiliki pengetahuan lengkap tentang target. Penguji memiliki pemahaman yang sempurna tentang cara kerja internal sistem. Biasanya, penguji dan pengembang bekerja sama untuk menjalankan jenis pengujian ini, di mana semua informasi diberikan kepada tim sebelum menjalankan pengujian. Informasi ini dapat mencakup jalur jaringan, kredensial, prosedur, IP Address, protokol jaringan, dan sebagainya, yang digunakan dalam jaringan organisasi.
c. *Gray Box Testing*
   Teknik pengujian GreyBox terletak di antara pengujian BlackBox dan WhiteBox, dimana penguji memiliki sebagian pengetahuan tentang cara kerja internal target. Biasanya, penguji tidak diberikan semua informasi tentang target dan harus mengumpulkan informasi tambahan yang diperlukan sendiri sebelum menjalankan tes. [6]

2.3. ISSAF

ISSAF (*Information Systems Security Assessment Framework*) adalah kerangka kerja yang dikembangkan oleh OISS.org. ISSAF ini digunakan untuk melakukan penilaian keamanan jaringan dan sistem informasi. ISSAF juga membantu profesional keamanan dalam merencanakan, melaksanakan, dan mengevaluasi uji penetrasi atau penilaian keamanan jaringan dengan pendekatan yang terstruktur. ISSAF menyediakan panduan dan pedoman untuk menjalankan pengujian keamanan dengan tujuan mengidentifikasi kerentanan, mengukur kekuatan keamanan, dan merancang strategi perbaikan. ISSAF menguraikan tiga area tindakan yang terdefinisi dengan baik, serta detail sembilan langkah yang menyusun fase utama, seperti berikut:

1. Perencanaan dan Persiapan (*Planning and Preparation*): Tahap pertama mencakup langkah-langkah yang diperlukan untuk menyiapkan lingkungan pengujian, seperti perencanaan dan persiapan alat uji, kontrak dan perlindungan hukum, definisi tim yang terlibat, batas waktu, persyaratan, dan struktur laporan akhir.
2. Penilaian (*Assessment*): Fase inti dari metodologi, di mana uji penetrasi sebenarnya dilakukan. Fase penilaian diuraikan dalam aktivitas berikut:
   a. Pengumpulan Informasi (*Information Gathering*): Langkah ini fokus pada pengumpulan informasi yang relevan tentang target yang akan diuji. Informasi ini dapat mencakup data tentang jaringan, sistem, aplikasi, dan infrastruktur. Tujuan utama adalah untuk memahami lebih baik lingkungan target dan mengidentifikasi potensi titik lemah.
   b. Pemetaan Jaringan (*Network Mapping*): Pada langkah ini, pengujian mencoba untuk memetakan jaringan target. Ini melibatkan identifikasi semua host yang aktif, alamat IP, layanan yang berjalan, dan topologi jaringan. Pemetaan jaringan membantu dalam memahami bagaimana komponen jaringan terhubung satu sama lain.

c. Identifikasi Kerentanan (*Vulnerability Identification*): Di sini, pengujian mencari kerentanan yang mungkin ada dalam sistem dan perangkat lunak yang berjalan di dalamnya. Hal ini dapat melibatkan penggunaan alat pemindai kerentanan atau pengujian manual untuk mengidentifikasi kerentanan potensial.
d. Penetrasi (*Penetration*): Langkah ini adalah inti dari uji penetrasi, di mana pengujian mencoba untuk mengeksploitasi kerentanan yang telah diidentifikasi. Tujuannya adalah untuk menentukan apakah kerentanannya dapat dimanfaatkan untuk mendapatkan akses yang tidak sah ke sistem atau data yang sensitif.
e. Memperoleh Akses & Eskalasi Hak (*Gaining Access & Privilege Escalation*): Setelah berhasil mendapatkan akses yang tidak sah, langkah ini melibatkan upaya untuk meningkatkan hak akses. Ini mungkin melibatkan perubahan hak akses dari pengguna biasa ke hak akses administrator atau pengguna yang memiliki hak lebih tinggi.
f. Enumerasi Lanjutan (*Enumerating Further*): Langkah ini mencakup upaya untuk mengidentifikasi lebih lanjut informasi sensitif dan kerentanan tambahan yang dapat dieksploitasi. Ini dapat mencakup penelusuran lebih lanjut dalam jaringan atau sistem target.
g. Mengkompromikan Situs Pengguna Jarak Jauh (*Compromise Remote Users Sites*): Di sini, pengujian mencoba untuk mengkompromikan situs atau sistem pengguna jarak jauh yang dapat digunakan sebagai titik awal untuk serangan lebih lanjut.
h. Memelihara Akses (*Maintaining Access*): Setelah berhasil mengakses sistem target, langkah ini melibatkan upaya untuk mempertahankan akses tersebut. Tujuannya adalah untuk tetap tidak terdeteksi dan mempertahankan kontrol atas sistem.
i. Menghilangkan Jejak (*Covering Tracks*): Pada langkah ini, pengujian mencoba untuk menghapus jejak aktivitas yang mencurigakan yang telah dilakukan selama uji penetrasi. Ini termasuk menghapus catatan log atau aktivitas yang dapat mengungkapkan kehadiran pengujian



Gambar 1. Garis Besar Kerangka Kerja ISSAF

3. Pelaporan, Pembersihan, dan Menghancurkan Artefak (*Reporting, Clean-up and Destroy Artifacts*): Pada tahap ini, di akhir bagian aktif metodologi, para pengujian harus menulis laporan lengkap dan menghancurkan artefak yang dibangun selama fase Penilaian.

ISSAF menyediakan struktur yang terorganisir untuk melakukan penilaian keamanan jaringan dengan metodologi yang sesuai. Ini membantu organisasi untuk mengidentifikasi risiko potensial, mengurangi kerentanan, dan meningkatkan keamanan jaringan mereka. [7][8].

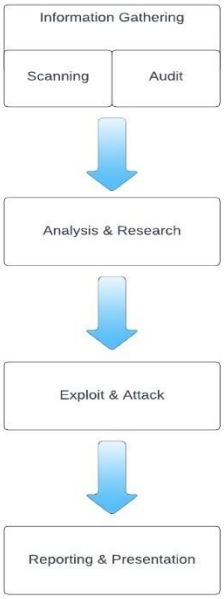
3. METODOLOGI PENELITIAN

Metodologi penelitian adalah pendekatan sistematis yang digunakan untuk merencanakan, melaksanakan, dan menganalisis sebuah penelitian, memastikan validitas dan reliabilitas temuan, serta memberikan kerangka kerja yang konsisten bagi peneliti. Metodologi penelitian mencakup berbagai aspek, mulai dari desain penelitian, pengumpulan data, analisis data, hingga interpretasi hasil dan penyusunan kesimpulan serta rekomendasi. Dari beberapa penelitian yang ada, penelitian ini mempunyai fokus:

1. Penelitian berfokus pada metode penetration test ISSAF WLAN *Security Assessment*.
2. Penelitian berfokus pada scope BlackBox dan hanya sampai *Reporting phase*.

3.1. Tahapan Penelitian

Dalam kerangka kerja ISSAF (*Information System Security Assessment Framework*) terdapat banyak metodologi, pada penelitian ini penulis akan menggunakan metodologi WLAN *Security Assessment* yang mempunyai beberapa langkah yang harus diikuti, dapat dilihat pada Gambar 2.



Gambar 2. Tahapan Metodologi WLAN *Security Assessment*

3.2.1 Metodologi

- *Information Gathering*

  Information Gathering adalah langkah pertama dalam *penetration test* suatu sistem atau jaringan. Pada tahap ini, penulis mencoba mengumpulkan data, informasi, dan pemahaman yang diperlukan tentang sistem atau jaringan yang akan diuji. Dengan tujuan agar dapat membantu memahami keamanan jaringan nirkabel target.

- *Scanning*
  Pada tahap ini, peneliti akan melakukan beberapa hal: 1.) Melakukan identifikasi jaringan WLAN, 2.) Melakukan pengujian channels/saluran dan ESSID, 3.) Melakukan pemantauan paket *beacon broadcast* dan mencatat informasinya, 4.) Melakukan pengujian *rogue access point* atau pengujian akses WLAN yang seharusnya hanya dapat diakses di sekitar lingkungan, tetapi ternyata terdapat beberapa titik yang dapat dijangkau dari luar gedung. 5) Mendapatkan IP *Address* dari *Access Point* beserta IP *Address* para penggunanya, 6.) Mendapatkan MAC *Address* dari *Access Point* beserta IP *Address* para penggunanya
- *Audit & Review* – Pertanyaan
  - *Implementation Control*
    - *Access Control: Apakah Access* Control diterapkan pada MAC Address perangkat di sistem keamanan jaringan?
    - Firewall: Apakah diterapkan keamanan *Firewall* pada sistem keamanan jaringan?
  - *Technical Controls*
    - Ports on Device: Apakah port komunikasi tertentu pada titik akses telah dinonaktifkan atau dilindungi dengan kata sandi untuk mencegah akses yang tidak sah?
    - SNMP: Apakah nama pada *Community* SNMP *default* sudah dirubah?
    - Apakah SSID Broadcast dimatikan?
    - Apakah menggunakan SSID default?
    - Apakah *Beacon Interval* sudah diatur ke pengaturan maksimal?
    - Apakah melakukan peningkatan sistem *firmware* secara berkala?
  - *Management Control*
    - Apakah menerapkan *Usage Policy?*
      Usage Policy merupakan ketentuan penggunaan jaringan WLAN, seperti kata sandi yang minimal terdapat simbol, huruf besar, angka, dan minimal 8 karakter. Contoh lainnya ialah hanya karyawan yang dapat mengakses jaringan WLAN.
- *Security Analys & Research*
  - Mencari Access Point yang masih mengaktifkan WEP
  - Mengambil data enkripsi WEP
  - Melihat MAC Address yang valid untuk terhubung ke jaringan WLAN
  - Mencoba akses Access Point dari berbagai cara, seperti Telnet, web, SNMP dan FTP
  - Mencari tahu metode otentikasi yang digunakan pada Access Point
  - Mencari tahu core Access Point
  - Mencoba berkomunikasi dengan titik akses untuk mengidentifikasi potensi kerentanan atau celah keamanan.
  - Mencoba terhubung ke Access Point dengan menggunakan NIC.
  - Melakukan pengumpulan data yang melalui 802.11 jaringan nirkabel
  - Mencari data-data yang sensitif
- *Exploitation & Attacks*
  - Identifikasi Kunci Otentikasi
    Untuk dapat melakukan *crack key* keamanan jaringan, setidaknya dapat menangkap sekitar 20.000 – 40.000 untuk dapat meretas WPA2/PSK dengan password yang

pendek atau umum 150.000 hingga 300.000 untuk WEP Key. Ada beberapa alat yang bisa digunakan dalam menangkap paket enkripsi WEP atau WPA, yaitu WepLab, AirCrack Suite, WepCrack. Alat untuk membantu mempercepat memperoleh data yaitu AirCrack Suite

- *Bypassing MAC Filttering*
  MAC Filtering bisa di *bypass* menggunakan alat berikut: SMAC, ini adalah alat untuk mengubah MAC di windows, dan dapat membantu untuk melakukan *spoof* sebuah MAC Address.
- Melakukan pengujian *login*
- *Disassociation attack*. Ini adalah serangan yang dilakukan dengan cara mengirimkan pesan palsu (spoofed) yang menyebabkan pemutusan koneksi antara pengguna dan Access Point. Serangan ini dapat menyebabkan layanan internet tidak bisa diakses atau bisa disebut dengan serangan DoS dan memungkinkan penyerang untuk mendapatkan informasi seperti SSID yang tersembunyi saat klien terhubung kembali. Alat seperti AirJack, essid-jack, dan monkey-jack dapat digunakan untuk ini.
- MITM
  Serangan *Man-in-the-Middle* adalah serangan di mana penyerang memposisikan diri di tengah-tengah komunikasi antara dua pihak yang sah. Pada jaringan nirkabel, serangan MITM lebih mudah dilakukan dibandingkan dengan jaringan kabel karena tidak memerlukan akses fisik ke jaringan. Serangan MITM dapat terjadi dalam dua bentuk umum: *Eavesdropping*: Penyerang hanya mendengarkan komunikasi tanpa mengubah data. Tujuannya adalah untuk mencuri informasi atau data rahasia. *Manipulation*: Penyerang aktif memanipulasi atau mengubah data yang mengalir antara dua pihak, misalnya mengganti pesan atau data yang dikirim. Tujuan bisa beragam, termasuk pencurian informasi, pengacauan komunikasi, atau penyusupan ke dalam jaringan.

- *Reporting*
  Reporting adalah tahap terakhir dalam metodologi ini, reporting ini berguna untuk mencatat serta mengumpulkan segala hasil yang ditemukan pada saat melakukan penetration test.
  Ada beberapa hal yang perlu diperhatikan dalam melakukan reporting, yaitu:
  - Mengorganisir dokumentasi berdasarkan hasil yang telah ditetapkan.
  - Memastikan bahwa dokumen pelaporan mencantumkan klasifikasi data.
  - Memastikan bahwa prosedur pengendalian dokumen diikuti.
  - Menampilkan pratinjau struktur pelaporan kepada klien sebelum dokumen akhir diserahkan.

Risiko keamanan informasi di dalam organisasi memiliki beragam tujuan. Oleh karena itu, sangat penting untuk mempertimbangkan cakupan penerapan risiko keamanan informasi dalam sebuah organisasi berdasarkan isu-isu internal dan eksternal lingkungan organisasi serta pemangku kepentingan yang terlibat, sehingga implementasinya menjadi lebih sistematis, dapat diukur, dan terkontrol[9].

Berikut ini adalah nilai untuk setiap level dampak atau *impact* pada setiap serangan penetration test, semakin tinggi nilai yang didapatkan, maka semakin besar dampak dari kerusakan keamanan jaringan tersebut. Pada tahap Reporting penulis akan menggunakan

templat parameter metodologi OWASP Risk Rating dan membedakan antara parameter *likelihood* atau kemungkinan dan parameter *impact* atau dampak seperti sebagai berikut:

a. *The Likelihood* (kemungkinan)

- Vulnerability Factors

  Vulnerability Factors ini bertujuan untuk memperkirakan kemungkinan dari kerentanan tertentu yang akan ditemukan dan diserang.
  - Ease of Discovery = Seberapa mudah penyerang menemukan kerentanan jaringan ini. Hampir tidak mungkin (1), susah (3), mudah (7), sangat mudah (9).
  - Ease of Exploit = Seberapa mudah penyerang dalam menyerang kerentanan yang mereka temukan. Hanya sebatas teori (1), susah (3), mudah (5), sangat mudah (9).
  - Awareness = Seberapa penyerang tau tentang adanya kerentanan di jaringan ini. Tidak diketahui (1), tersembunyi (4), terlihat jelas (6), orang-orang awam mengetahuinya (9).
  - Intrusion Detection = Bagaimana serangan ini dapat terdeteksi. Terdapat deteksi aktif pada sistem (1), masuk ke dalam log lalu dilihat (3), masuk ke dalam log dan tidak dilihat (8), tidak masuk log (9).
- Threat Agent Factors

  Threat Agent Factors ini bertujuan untuk memperkirakan keahlian penyerang yang dapat berhasil melakukan serangannya pada jaringan ini.
  - Skill Level = Seberapa ahli penyerang secara teknis. Tidak ada keahlian (1), beberapa keahlian teknis (3), pengguna komputer yang ahli (5), seorang yang mempunyai kemampuan jaringan komputer dan pemrograman (6), seorang pentester keamanan (9).
  - Motive = Apa yang memotivasi penyerang dalam serangan ini. Tidak ada keuntungan (1), ada kemungkinan keuntungan (4), keuntungan yang banyak (9).
  - Opportunity = Alat dan peluang apa yang diperlukan untuk dapat menemukan dan menyerang vulnerability atau kerentanan. Akses penuh (admin) dan alat yang mahal (0), akses tertentu dan alat yang mahal (4), sebagian akses tertentu dan alat seadanya (7), tidak perlu akses dan alat seadanya (9).
  - Size = Berada pada lingkup apa penyerang. Developers (2), system administrator (2), pengguna lokal (4), rekan (5), pengguna yang telah terotentikasi pada sistem (6), pengguna internet yang tidak dikenal (9).

b. *Technical Impact* (dampak)

- *Business Impact*

  Bussiness Impact atau dampak bisnis pada sebuah perusahaan ini meliputi kerugian perusahaan, reputasi perusahaan, dan identitas karyawan perusahaan.
  - F*inancial damage* = Berapa banyak kerugian yang dihasilkan dari serangan tersebut. Kategori Rp.0 – Rp.1.000.000 (2), kategori Rp.1.100.000 – Rp.10.000.000 (5), Kategori Rp.10.100.000 – Rp.100.000.000 (8).
  - *Reputation damage* = Sebesar apa dampak pada reputasi perusahaan. Kerusakan reputasi sangat kecil dan tidak berdampak signifikan terhadap keseluruhan bisnis (2), kehilangan akun utama yang meliputi catatan penjualan dan lainnya (5), kerusakan terhadap citra perusahaan, penurunan penjualan dan kepercayaan pelanggan (9)
  - *Privacy violation* = Berapa banyak identitas orang yang terungkap akibat serangan. Hanya satu orang (3), seratus orang (5), ribuan orang (7), jutaan orang (9).

- *Techical Impact Factors*
  Technical Impact Factors ini meliputi CIAA yaitu *confidentiality*, *availability*, *integrity,* dan *accountability*. Technical Impact Factors ini bertujuan untuk mengetahui seberapa besar dampak pada sistem.
  - *Loss of Confidentility* = Berapa banyak data yang terungkap dan seberapa sensitif data tersebut. Sedikit data yang tidak sensitif terungkap (2), sedikit data yang sensitif terungkap (6), banyak data yang tidak sensitif terungkap (6), banyak data yang sensitif terungkap (7), semua data terungkap (9).
  - *Loss of Integrity* = Berapa banyak data yang terinfeksi atau rusak. Sedikit data yang rusak dan kerusakan ringan (1), sedikit data yang rusak dan kerusakan serius (3), banyak data yang rusak dan kerusakan ringan (5), banyak data yang rusak dan kerusakan serius (7), semua data rusak dan kerusakan serius (9)
  - *Loss of Availability* = Berapa banyak layanan yang terdampak, seperti akses FTP, internet, dll. Sedikit layanan yang tidak kritis terdampak (1), sedikit layanan yang penting terdampak (5), banyak layanan yang tidak kritis terdampak (5), banyak layanan yang penting terdampak (7), semua layanan terdampak (9).
  - *Loss of Accountability* = Sejauh mana penyerang dapat terlacak. Penyerang dapat ditelusuri kembali secara lengkap ke individu tertentu (1), penyerang mungkin dapat ditelusuri kembali ke individu tertentu, namun jejaknya mungkin tidak lengkap atau tidak pasti (7), penyerang benar-benar anonim dan tidak dapat ditelusuri kembali ke individu tertentu (9)[10].

Tabel 1. Level Kerentanan

Impact	Assigned Value
Highly	6 – 9
Average	3 < 6
Low	0 < 3

Di bawah ini merupakan contoh indikator dalam melakukan penetration test pada sebuah organisasi atau perusahaan.

'"Threat agent factors"'					'"Vulnerability factors"'			
Skill level	Motive	Opportunity	Size		Ease of discovery	Ease of exploit	Awareness	Intrusion detection
5	2	7	1		3	6	9	2
Overall likelihood=4.375 (MEDIUM)								
Technical Impact					**Business Impact**			
Loss of confidentiality	Loss of integrity	Loss of availability	Loss of accountability		Financial damage	Reputation damage	Non-compliance	Privacy violation
9	7	5	8		1	2	1	5
Overall technical impact=7.25 (HIGH)					Overall business impact=2.25 (LOW)			

Gambar 3. Contoh Hasil Penetration Test

Untuk dapat mengetahui hasil keseluruhan atau hasil akhir, hasil dari *likehood* dan *impact* akan digabung. Seperti contoh gambar dibawah ini.

Overall Risk Severity				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
	Likelihood			

Gambar 4. Contoh Hasil Keseluruhan Pengujian

Pada Gambar 4 kita dapat melihat hasil dari *likehood* adalah *medium* sedangkan hasil dari *technical impact* adalah *high.* Jika kita masukkan pada tabel *Overall Risk Severity* Gambar 4, maka hasilnya akan berupa *high*. Dengan hasil keseluruhan adalah *high* maka akan diperlukan sebuah evaluasi agar dapat mencegah serangan di waktu mendatang.

Dalam menentukan *Risk Rating* pada metodologi OWASP, *pentester* dapat melakukan sebuah penyesuaian parameter pengujian. Seperti jika mendapati kendala tidak adanya informasi mengenai Business Impact, maka penggabungan nilai dari Likehood dengan Impact diganti menjadi Technical Impact, tetapi akan lebih baik jika mengetahui informasi tentang Business Impact.

4. HASIL DAN PEMBAHASAN

Pengimplementasian metodologi ISSAF pada PT. Gerak Puncak Lancar ini menggunakan Access Point yang telah dilakukan konfigurasi semirip mungkin dengan Access Point, penggunaan Access Point *dummy* ini dikarenakan Access Point Staff terlalu banyak pengguna dan dapat mengganggu pekerjaan karyawan lainnya.

4.1. Information Gathering

Penulis melakukan pencarian informasi publik pada internet dan melakukan pengamatan langsung, didapati informasi sebagai berikut:

Tabel 2. Hasil Information Gathering

Information Gathering	
Nama Perusahaan	PT. Gerak Puncak Lancar
Jumlah Karyawan	24
Bergerak di bidang	Teknologi dan Informasi
Jumlah Access Point	4 (hidden 2, terlihat 1, diluar jangkauan 1)
Jenis Keamanan	WPA2/PSK, WPS, WPA2, AES-CCM
Alamat	Head Office Mangga Besar IV E/30A Jakarta 11150 Indonesia Tel: +62 21 6491379 / 6261171 Fax: +62 21 6492443

Semua simbol yang telah digunakan dalam persamaan harus didefinisikan dalam teks berikut.

4.2. Scanning

Pada proses Scanning ini, penulis akan melakukan beberapa hal seperti memantau SSID, Channel, dan informasi lainnya pada Access Point PT. Gerak Puncak Lancar menggunakan Kismet. Serta memantau Packet Rate menggunakan Wireshark.

Tabel 3. Hasil Scanning

Scanning	
SSID WLAN sekitar	Terdapat 13 SSID dalam jangkauan
Channel dan ESSID	Channel 1 MyRepublic_C35C
Pemantaun packet beacon dan mencatatnya	Paket beacon berisikan SSID : MyRepublic_C35C BSSID : 90:72:82:DD:C3:5C Keamanan : WPA2/PSK, WPA2, WPS Enkripsi : AES-CCM Channel : 1 Client : 1 Kekuatan sinyal : -128dbm
Rogue Test dari luar wilayah perusahaan	SSID dapat dijangkau Kekuatan sinyal : -135dbm
Pengumpulan data IP Address pengguna dari Access Point.	-
Pengumpulan data MAC Address pengguna dari Access Point.	90:72:82:DD:C3:5C C6:6C:1D:AC:D3:AA

4.3. Audit & Review

Tabel 4. Hasil Wawancara pada tahap Audit & Review

Audit & Review - Pertanyaan	
Apakah Access Control diterapkan pada MAC Address perangkat di sistem keamanan jaringan?	Tidak
Apakah diterapkan keamanan Firewall pada sistem keamanan jaringan?	Access Point menggunakan Firewall
Apakah port komunikasi tertentu pada titik akses telah dinonaktifkan atau dilindungi dengan kata sandi untuk mencegah akses yang tidak sah?	Access Point menggunakan WEP2/PSK, dan menggunakan WPS. FTP, SSH, dan Telnet menggunakan kata sandi.
Apakah nama/string pada Community SNMP default sudah dirubah?	Tidak
Apakah SSID Broadcast dimatikan?	Menyala, serta dalam beberapa waktu, Channel AP berganti.
Apakah menggunakan SSID default?	Tidak
Apakah Beacon Interval sudah diatur ke pengaturan maksimal?	Default

Apakah melakukan peningkatan sistem firmware secara berkala?	Iya
Apakah menerapkan Usage Policy?	- Menggunakan beberapa ketentuan yaitu hanya karyawan yang boleh menggunakan Access Point - Password dirahasiakan - Dilarang membuka situs berbahaya/rawan

4.4. Analysis & Research

Beberapa informasi yang didapatkan pada tahap Information Gathering dan Scanning yaitu, Packet Rate yang tinggi, memungkinkan penulis untuk mengumpulkan data lebih cepat, pengumpulan data tersebut bertujuan untuk meningkatkan kesuksesan saat penyerangan menggunakan AirCrack-ng. Serta pada *Information Gathering* diatas pun MAC-Address berhasil didapatkan.

Packet EAPOL pun dapat diperoleh, dengan begitu otentikasi WPA2/PSK dapat dilakukan. Walaupun jumlah data yang dikumpulkan banyak, jika tidak mendapatkan EAPOL (yang mengandung otentikasi) maka kata sandi AP target akan sangat sulit untuk diretas.

Saat menjalankan Deauth penulis mendapatkan PMKID (*Pairwise Master Key Identifier*), PMKID sendiri adalah sebuah paket yang berisikan beberapa informasi salah satunya adalah kata sandi, isi paket tersebut tentunya terenkripsi.

4.5. Exploit & Attack

Pada tahap ini, penulis menggunakan informasi-informasi yang telah didapatkan pada sesi sebelumnya untuk melakukan penyerangan AP target.

Tabel 5. Hasil *Exploit & Attacks*

	Exploit & Attacks
Identifikasi Kunci Otentikasi dan peretasan Password. AirCrack-NG	WEP2/PSK, WPA2, WPS. Password dapat diretas dalam kurun waktu 1557721009 hari, 2 jam, 44, menit, 16 detik. WPS Pin Attack menghabiskan waktu yang cukup lama. Tetapi ada kemungkinan diretas.
Bypassing MAC Filttering	Tidak ada keamanan MAC Filtering
NMAP vulnerability scan	Port open pada IP 192.168.5.1 (AP Target) 21, 22, 23, 80, 443, 5431 serta terdapat port yang terbuka dan IP Address pengguna lainnya.
Wireshark Sniffing Attack 192.168.5.7	Berhasil mendapatkan akun login suatu website http: Username : “32148932” Password : “*********”
DNS Spoofing target tanpa HSTS	Berhasil mendapatkan akun percobaan yang login dari www.kompas.com Username : “ghfghgfh@dfdt” Password : “dfgdfg”
DNS Spoofing target dengan HSTS	Tidak memungkinkan

DDOS External Aireplay-ng deauth	Berhasil membuat semua pengguna *disconnect* dari AP target (tidak berpengaruh terhadap pengguna yang menggunakan Wired LAN)
DDOS Internal Ettercap DDOS Plugin	Berhasil membuat traffic menjadi *down* dan mengganggu aktifitas berselancar di internet. Serta mengganggu CCTV, layanan FTP, Printer, dan lainnya.

4.6. Report

Dalam pentest ini terdapat beberapa kerentanan yang penulis temukan dan terdapat beberapa keamanan yang cukup kuat, seperti kata sandi WPA2/PSK yang cukup kuat, konfigurasi yang secara otomatis mengubah channel setiap beberapa jam, dan membatasi akses percobaan pin pada WPS. Untuk bagian Internal Attack, terdapat beberapa kerentanan dan terdapat beberapa keamanan yang mencegah penyerang mendapatkan informasi dari pengguna, seperti pengguna yang sudah mempunyai HSTS.

Di bawah ini merupakan hasil penyerangan pada Access Point PT. Gerak Puncak Lancar.

Tabel 6. Hasil Pentest PT. Gerak Puncak Lancar

Threat Agent Factors				**Vulnerability Factors**			
Skill level	Motive	Opportunity	Size	Ease of Discover	Ease of Exploit	Awareness	Intrusion Detection
5	4	7	6	5	5	4	3
Overall Likehood = 4.875 (Medium)							
Technical Impact							
Lose Of Confidentility		Lose Of Integrity		Lose Of Availbility		Lose Of Accountability	
6		4		7		7	
Overall Techincal Impact = 6 (High)							

Hasil dari Pentest menunjukkan Overall Likehood mendapatkan hasil Medium, Overall Technical Impact mendapatkan hasil High, dan Overall Business Impact mendapatkan hasil Low. Jika kita masukkan ke dalam tabel keseluruhan pengujian pentest pada Gambar 3.3, PT. Gerak Puncak Lancar mendapatkan hasil keseluruhan High. Dikarenakan kurangnya informasi tentang Business Impact, penulis memutuskan untuk tidak menampilkan Business Impact didalam hasil Pentest diatas.

4.7. Evaluasi

4.7.1 Sebelum Evaluasi

Di bawah ini merupakan nilai-nilai Pentest sebelum Evaluasi :

- Overall Likehood = 4.875 (Medium)
- Overall Technical Impact = 6 (High)

Menurut tabel *Overall Risk* Rating hasil dari Pentest jaringan PT. Gerak Puncak Lancar mendapati nilai *High*. Serangan dapat berdampak sangat serius jika terjadi terus menerus selama beberapa hari atau bahkan selama beberapa minggu. Dengan adanya kemungkinan yang lebih buruk, atau kerugian yang lebih parah, perusahaan harus melakukan evaluasi pada keamanan jaringan mereka.

1. Techincal Impact

Dapat dilihat nilai *Overall Techical Impact* adalah High, yang artinya mempunyai keamanan yang rendah, karena *Technical Impact* meliputi kerusakan data, kehilangan data, kehilangan layanan, dan juga identifikasi pelaku penyerang.

2. Vulnerability Factors

Vulnerability Factors mendapatkan nilai rata-rata 4.25 masih dikategorikan Medium. *Vulnerability Factors* ini meliputi seberapa mudahnya penyerang menemukan kerentanan, seberapa mudahnya menyerang kerentanan tersebut, dan lainnya.

4.7.2 Sesudah Evaluasi

Di bawah nilai-nilai setelah Evaluasi dilakukan:

Tabel 7. Hasil Pentest Setelah Evaluasi

Technical Impact			
Lose Confidentility Of	Lose Integrity Of	Lose Availbility Of	Lose Accountability Of
2	1	5	7
Overall Techincal Impact = 3.75 (Medium)			
Vulnerability Factors			
Ease of Discover	Ease of Exploit	Awareness	Intrusion Detection
3	3	1	3
Vulnerability Factors = 2.5 (Low)			

Setelah melakukan Evaluasi kita mendapati nilai Overall Technical Impact 3.75 (Medium), sedangkan Vulnerability Factors 2.5 (Low). Untuk mendapatkan Overall Likelihood : (Vulnerability Factors + Threat Agent Factors)/jumlah parameter Likelihood = (10+22)/8 = 4 (Medium)

Kita mendapati Overall Likelihood 4 (Medium).

Tabel 8. Perbandingan Hasil Pentest Sebelum dan Sesudah Evaluasi

Sebelum Evaluasi				**Sesudah Evaluasi**		
Technical Impact	Vulnerability Factors	Threat Agent Factors		Technical Impact	Vulnerability Factors	Threat Agent Factors
6 (High)	4.25 (Medium	5.5 (Medium)		3.75 (Medium)	2.5 (Low)	5.5 (Medium)
	Likelihood = 4.875 (Medium)				Likelihood = 4 (Medium)	
Overall Risk Rating = High				Overall Risk Rating = Medium		

Kita bisa lihat di atas, *Overall Risak Rating* sudah turun dari yang sebelumnya High menjadi Medium dan juga dari perbandingan di atas penulis ingin mengetahui berapa persentase perubahan yang terjadi setelah evaluasi menggunakan rumus persentase perubahan :

Persentase perubahan Technical Impact :

$$persentase\ perubahan = \left(\frac{perubahan}{nilai\ awal}\right) * 100\%$$

Perubahan = Nilai sesudah evaluasi – Nilai awal = 3.75 – 6 = -2.25

Persentase perubahan = (-2.25/6)*100% = (-0.375)*100% = 37.5%

Jadi pada Technical Impact 37.5% lebih aman dari keamanan sebelumnya.

Persentase perubahan Vulnerability Factors :

$$persentase\ perubahan = \left(\frac{perubahan}{nilai\ awal}\right) * 100\%$$

Perubahan = Nilai sesudah evaluasi – Nilai awal = 2.5 – 4.25 = -1.75
Persentase perubahan = (-1.75/4.25)*100% = (-41.18)*100% = 41.18%
Sedangkan pada Vulnerability Factors 41.18% lebih aman dari keamanan sebelumnya.

5. KESIMPULAN

Metode ISSAF mampu menggambarkan Tingkat Resiko pengujian keamanan nirkabel di PT. Gerak Puncak Lancar. Berdasarkan hasil analisa, *Technical Impact* atau dampak teknis dari uji serangan masih *High*, sedangkan untuk Likelihood, berada pada level *Medium*. Dan mendapati bahwa *Overall Risk* Rating berada pada level *High*, yang artinya mempunyai resiko tinggi terhadap terganggunya layanan jaringan, kehilangan data, kerusakan data, kerugian, dll. Dengan hasil *Overall Risk* Rating yang tinggi, penulis memutuskan untuk melakukan evaluasi pada keamanan PT. Gerak Puncak Lancar yang bertujuan untuk menurunkan nilai *Overall Risk* Rating keamanan jaringan tersebut. Dan setelah dilakukannya evaluasi, hasil *Overall Risk* Rating dari keamanan perusahaan ini telah turun menjadi Medium yang mana hasil tersebut dapat diterima perusahaan.

REFERENSI

[1] "Honeynet Map | BSSN." Accessed: Oct. 21, 2023. [Online]. Available: https://honeynet.bssn.go.id/
[2] M. Rusdan, D. T. H Manurung, and F. Kharisma Genta, "Evaluation of Wireless Network Security Using Information System Security Assessment Framework (ISSAF) (Case Study: PT. Keberlanjutan Strategis Indonesia)," *TEST Engineering and Management*, vol. 83, no. 15714, pp. 15714 – 15719, 2020.
[3] B. RUTH WITKIN Belle Ruth Witkin -PhD and V. Scholar, "Articles Needs Assessment Since 1981: The State of the Practice."
[4] "Discover Wi-Fi | Wi-Fi Alliance." Accessed: Apr. 02, 2023. [Online]. Available: https://www.wi-fi.org/discover-wi-fi
[5] F. Fachri, A. Fadlil, I. Riadi, A. Dahlan, Y. Jln Soepomo, and I. Artikel, "Analisis Keamanan Webserver Menggunakan Penetration Test," *JURNAL INFORMATIKA*, vol. 8, no. 2, 2021, [Online]. Available: http://ejournal.bsi.ac.id/ejurnal/index.php/ji
[6] I. Yaqoob, S. A. Hussain, S. Mamoon, N. Nasseer, J. Akram, and A. ur Rehman, "Penetration Testing and Vulnerability Assessments," no. February 2021, pp. 1–2, 2017.
[7] A. Zein, J. Raya, P. Serpong, N. 10 Tangerang, and S. Banten, "Evaluasi Keamanan Wireless Lan Menggunakan Issaf (*Information System Security Assessment Framework*)", doi: 10.37277/stch.v32i2.
[8] "Information Systems Security Assessment Framework (ISSAF) draft 0.2," 2005.
[9] N. A. Chandra, K. Ramli, A. A. P. Ratna, and T. S. Gunawan, "Information Security Risk Assessment Using Situational Awareness Frameworks and Application Tools," *Risks*, vol. 10, no. 8, Aug. 2022, doi: 10.3390/risks10080165.
[10] "OWASP Risk Rating Methodology | OWASP Foundation." Accessed: May 01, 2024. [Online]. Available: https://owasp.org/www-community/OWASP_Risk_Rating_Methodology