SKRIPSI

ANALISIS *VULNERABILITY* JARINGAN WLAN DEPARTEMEN TEKNIK ELEKTRO FT-UH TERHADAP SERANGAN *DENIAL OF SERVICE* (DOS) DAN *MAN IN THE MIDDLE* (MITM)

Disusun dan diajukan oleh:

MUH. FHADLAN DINUL HAQ

D041 19 1024

PROGRAM STUDI SARJANA TEKNIK ELEKTRO

FAKULTAS TEKNIK

UNIVERSITAS HASANUDDIN

GOWA

2024

LEMBAR PENGESAHAN SKRIPSI

ANALISIS *VULNERABILITY* JARINGAN WLAN DEPARTEMEN TEKNIK ELEKTRO FT-UH TERHADAP SERANGAN *DENIAL OF SERVICE* (DOS) DAN *MAN IN THE MIDDLE* (MITM)

Disusun dan diajukan oleh

Muh. Fhadlan Dinul Haq

D041191024

Telah dipertahankan di hadapan Panitia Ujian yang dibentuk dalam rangka
Penyelesaian Studi Program Sarjana Program Studi Teknik Elektro
Fakultas Teknik Universitas Hasanuddin
Pada Tanggal 31 Januari 2024
dan dinyatakan telah memenuhi syarat kelulusan

Menyetujui,

Pembimbing Utama,

Dr. Eng. Wardi, S.T., M. Eng.
NIP 19720828 199903 1 003

Pembimbing Pendamping,

Azran Budi Arief, S.T., M.T.
NIP 19890201 201903 1 007

Ketua Program Studi,

Dr. Eng. Ir. Dewiani, M.T.
NIP 19691026 199412 2 001

PERNYATAAN KEASLIAN

Yang bertanda tangan dibawah ini :
Nama : Muh. Fhadlan Dinul Haq
NIM : D041191024
Program Studi : Teknik Elektro
Jenjang : S1

Menyatakan dengan ini bahwa karya tulisan saya berjudul

ANALISIS *VULNERABILITY* JARINGAN WLAN DEPARTEMEN TEKNIK ELEKTRO FT-UH TERHADAP SERANGAN *DENIAL OF SERVICE* (DOS) DAN *MAN IN THE MIDDLE* (MITM)

Adalah karya tulisan saya sendiri dan bukan merupakan pengambilan alihan tulisan orang lain dan bahwa skripsi yang saya tulis ini benar-benar merupakan hasil karya saya sendiri.

Semua informasi yang ditulis dalam skripsi yang berasal dari penulis lain telah diberi penghargaan, yakni dengan mengutip sumber dan tahun penerbitannya. Oleh karena itu semua tulisan dalam skripsi ini sepenuhnya menjadi tanggung jawab penulis. Apabila ada pihak manapun yang merasa ada kesamaan judul dan atau hasil temuan dalam skripsi ini, maka penulis siap untuk diklarifikasi dan mempertanggungjawabkan segala resiko.

Segala data dan informasi yang diperoleh selama proses pembuatan skripsi, yang akan dipublikasi oleh Penulis di masa depan harus mendapat persetujuan dari Dosen Pembimbing.

Apabila dikemudian hari terbukti atau dapat dibuktikan bahwa sebagian atau keseluruhan isi skripsi ini hasil karya orang lain, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Gowa, 31 Januari 2024

Yang Menyatakan

Muh. Fhadlan Dinul Haq

KATA PENGANTAR

Segala puji bagi Allah SWT, yang Maha Pengasih dan Maha Penyayang, yang telah melimpahkan segala anugerah dan berkah-Nya sehingga penulis dapat menyelesaikan Tugas Akhir dengan judul "**Analisis *Vulnerability* Jaringan WLAN Departemen Teknik Elektro FT-UH Terhadap Serangan *Denial Of Service* (DoS) Dan *Man In The Middle* (MITM)**" sebagai salah satu persyaratan dalam menyelesaikan Studi Kesarjanaan (S1) di Departemen Teknik Elektro, Fakultas Teknik Universitas Hasanuddin. Selawat serta salam senantiasa tercurah kepada *Rasulullah* Muhammad SAW yang kita nantikan syafaatnya di akhirat kelak.

Penulis menyadari bahwa dalam proses penulisan skripsi ini ada banyak kendala yang dialami, namun berkat kehendak dan kuasa Allah SWT. dan juga bimbingan serta dukungan dari beberapa pihak, sehingga kendala tersebut dapat diatasi. Dengan segala kerendahan hati, ucapan rasa syukur dan terima kasih yang sebesar-besarnya kepada:

1. Keluarga penulis, ayahanda penulis Drs. Maspa dan ibunda penulis Mahniar Ibrahim, S.P., yang senantiasa memberikan kasih sayang, dorongan doa, nasihat, motivasi, dan dukungan yang tiada hentinya kepada penulis. Kakak penulis, Muh. Alif Fhadyl Akbar, S.T., yang sangat penulis banggakan dan menjadi panutan bagi penulis. Adik penulis, Alifiah Aisyah Indira, yang memberikan dukungan dan menjadi semangat bagi penulis. Serta seluruh keluarga besar penulis yang tidak dapat disebutkan satu per satu, terima kasih atas segala dukungan, bantuan, dan motivasinya. Semoga senantiasa dalam lindungan Allah SWT.
2. Bapak Dr.Eng. Wardi, S.T., M.Eng dan Bapak Azran Budi Arief, S.T., M.T yang telah menjadi meluangkan waktu, tenaga, dan pikiran untuk membimbing dan memberikan arahan yang sangat berarti dalam penulisan skripsi ini.

3. Bapak Ir. Samuel Panggalo, M.T. dan Ibu Andini Dani Achmad, S.T., M.T. selaku penguji yang telah memberikan saran dan masukannya demi hasil penelitian yang maksimal.
4. Bapak dan Ibu Dosen Departemen Teknik Elektro Universitas Hasanuddin yang telah memberikan ilmu dan pengetahuan kepada penulis selama mengikuti perkuliahan hingga penulis menyelesaikan skripsi.
5. Seluruh staf Akademik Departemen Teknik Elektro Universitas Hasanuddin yang telah membantu penulis dalam pengurusan administrasi selama perkuliahan hingga penulis menyelesaikan skripsi.
6. Teman seperjuangan Research Group Jaringan Telekomunikasi dan Transmisi, Miftahul Ulum Harahap, Muhammad Padli, Sony Akbar Manarang, Nurkholik Katu, L.M. Ghafaar Alamsyah Alhan, Nur Iqrima Fitrahqalby, Muh. Reza Saputra, Andi Abdul Hakam Syukur, dan I Putu Kanatika yang senantiasa memberikan dukungan, bantuan, dan semangat selama berada di Laboratorium Telematika. Terutama Miftah dan Palli yang senantiasa menemani dalam lika-liku kesulitan dalam menyelesaikan tugas akhir ini.
7. Nurul Azizah Hamid, Rahmadien Fibrian I.Y.E., Muhammad Ferdiansyah, M. Farid Gifhari, Muhammad Al Muqit, Nurul Aulyah Paisal, Meiliana Nurul Rahmah, Muhammad Yusuf, Muhammad Fauzan Lukman, Muh. Dzulfadli Rusli selaku teman terdekat yang senantiasa memberikan bantuan, semangat, dan dukungannya selama ini.
8. Teman-teman “Exaction 2019”, teman-teman “TR19GER”, serta teman-teman “Orang Suskes” yang selalu menemani, mendukung, dan membantu penulis selama ini.
9. Serta semua pihak yang telah membantu namun tidak sempat disebutkan. Semoga semua kebaikan yang diberikan mendapatkan pahala yang berlipat ganda.

Semoga hasil penelitian ini bermanfaat bagi perkembangan ilmu pengetahuan serta menjadi bukti kesungguhan dan dedikasi penulis dalam mengabdikan ilmu dalam praktik nyata. Penulis menyadari bahwa penyusunan

skripsi ini masih memiliki banyak kekurangan. Oleh karena itu, penulis sangat mengharapkan saran dan tanggapan dari berbagai pihak.

Gowa, 17 Januari 2024

Penulis

ABSTRAK

MUH. FHADLAN DINUL HAQ. *Analisis Vulnerability Jaringan WLAN Departemen Teknik Elektro FT-UH Terhadap Serangan Denial of Service (DoS) dan Man In The Middle (MITM)* (dibimbing oleh Wardi dan Azran Budi Arief)

Dalam beberapa dekade terakhir, teknologi telah mengalami perubahan yang signifikan. Teknologi nirkabel menjadi salah satu faktor utama dalam perubahan ini, memungkinkan kita untuk berinteraksi dengan lingkungan sekitar dengan cara yang lebih efisien, terhubung, dan inovatif. Salah satu jenis dari teknologi nirkabel yaitu *Wireless Local Area Network* (WLAN). Teknologi ini memungkinkan pengguna untuk mengakses internet tanpa kabel. Namun, teknologi memiliki tantangan dalam hal keamanan, karena sinyal radio yang digunakan untuk transmisi data dapat dengan mudah disadap atau diinterferensi oleh pihak yang tidak berwenang. Karena pentingnya jaringan WLAN di institusi seperti kampus, pengujian keamanan WLAN menjadi sangat penting untuk dilakukan. Hal ini untuk memastikan bahwa jaringan WLAN tersebut aman. Penelitian ini bertujuan untuk mengidentifikasi tingkat keamanan jaringan WLAN kampus terhadap serangan *Denial of Service* (DoS) dan *Man In The Middle* (MITM). Lima jenis serangan yang diuji, yaitu ICMP *flood*, SYN *flood*, UDP *flood*, ARP *spoofing*, dan MAC *spoofing*. Metode pengujian mencakup *penetration testing* dan *vulnerability assessment* dengan menggunakan *Base Metrics* dari CVSS v4.0 sebagai kerangka penilaian. Hasil pengujian menunjukkan dampak serangan pada *throughput* WiFi, penggunaan CPU, dan pola paket yang ditangkap. Serangan ICMP *flood*, SYN *flood*, dan UDP *flood* mempengaruhi *throughput* dan beban CPU dengan fluktuasi yang berbeda, sedangkan serangan ARP *spoofing* dan MAC *spoofing* berhasil memanipulasi trafik pada tingkat protokol *data-link*. Penilaian tingkat keamanan menggunakan CVSS v4.0 memberikan skor 6.9 dengan predikat *Medium*. Hasil ini menggambarkan tingkat keamanan WiFi terhadap serangan yang dapat menyebabkan gangguan layanan dan pemalsuan identitas perangkat. Ini menunjukkan bahwa kerentanan yang ditemukan masih dapat dimanfaatkan oleh penyerang untuk merugikan jaringan dan penggunanya.

Kata kunci: WLAN, Kerentanan, *Vulnerability Assessment*, *Penetration Testing*, *Denial of Service*, *Man In The Middle.*

ABSTRACT

MUH. FHADLAN DINUL HAQ. *Analysis of WLAN Network Vulnerability of the Department of Electrical Engineering FT-UH Against Denial of Service (DoS) and Man In The Middle (MITM) Attacks (Supervised by Wardi and Azran Budi Arief)*

In recent decades, technology has undergone significant changes. Wireless technology is one of the main factors in this change, allowing us to interact with our surroundings in more efficient, connected, and innovative ways. One type of wireless technology is the Wireless Local Area Network (WLAN). This technology allows users to access the internet without cables. However, the technology has challenges in terms of security, because radio signals used for data transmission can easily be intercepted or interfered with by unauthorized parties. Due to the importance of WLAN networks in institutions such as campuses, WLAN security testing is essential. This is to ensure that the WLAN network is secure. This research aims to identify the level of vulnerability of campus WLAN networks to Denial of Service (DoS) and Man In The Middle (MITM) attacks. Five types of attacks were tested, namely ICMP flooding, SYN flooding, UDP flooding, ARP spoofing, and MAC spoofing. Testing methods include penetration testing and vulnerability assessment using Base Metrics from CVSS v4.0 as an assessment framework. Test results show the impact of attacks on WiFi throughput, CPU usage, and captured packet patterns. ICMP flood, SYN flood, and UDP flood attacks affect throughput and CPU load with different valleys, while ARP spoofing and MAC spoofing attacks successfully manipulate traffic at the data-link protocol level. Security level assessment using CVSS v4.0 gave a score of 6.9 with a Medium predicate. These results illustrate the security level of WiFi to attacks that can cause service disruption and device identity fraud. This shows that attackers can still exploit the security vulnerabilities found to harm the network and its users.

Keywords: WLAN, Vulnerability, Vulnerability Assessment, Penetration Testing, Denial of Service, Man In The Middle.

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

BAB I
PENDAHULUAN

1.1 Latar Belakang

Dalam beberapa dekade terakhir, terjadi perubahan mendasar dalam teknologi yang telah mengubah cara kita berinteraksi dengan lingkungan sekitar. Internet dan teknologi nirkabel telah menjadi pendorong utama dalam evolusi ini, membuka jalan bagi solusi yang lebih efisien, terhubung, dan inovatif. Internet telah menjadi alat yang digunakan oleh semua orang, dari anak-anak hingga perusahaan besar, untuk berbagai tujuan seperti pendidikan, bisnis, dan hiburan. Salah satu aspek penting dari perubahan ini adalah peran yang semakin besar dari jaringan nirkabel (WLAN) dalam memfasilitasi konektivitas tanpa batas. Jaringan WLAN telah menjadi infrastruktur utama di berbagai institusi, termasuk kampus-kampus pendidikan, karena kemampuannya untuk memberikan akses internet yang cepat, pertukaran data yang efisien, dan berbagai layanan penting lainnya.

Jaringan *wireless* merupakan teknologi yang memungkinkan pengguna untuk mengakses internet tanpa kabel. Namun, jaringan *wireless* juga memiliki tantangan dalam hal keamanan, karena sinyal radio yang digunakan untuk transmisi data dapat dengan mudah disadap atau diinterferensi oleh pihak yang tidak berwenang. Hal ini dapat menyebabkan kerugian data, privasi, atau bahkan layanan bagi pengguna jaringan *wireless* (Saputra, 2020).

Ada ancaman besar yang selalu mengintai penggunanya, termasuk serangan seperti *phising*, *sniffing*, *hacking*, *cracking*, *denial of service attack*, dan berbagai tindakan jahat lainnya. Ancaman-ancaman ini dapat digunakan baik untuk menguji keamanan sistem maupun untuk tujuan yang tidak bertanggung jawab seperti pencurian data atau penyalahgunaan akses. Karena adanya potensi ancaman tersebut, penting bagi kita sebagai pengguna internet untuk merasa aman dan dilindungi.

Salah satu ancaman utama terhadap keamanan jaringan nirkabel adalah serangan *Denial of Service* (DoS). Serangan ini bertujuan untuk menghentikan atau mengurangi ketersediaan layanan yang disediakan oleh *server* atau sistem yang

ditargetkan. Serangan ini dapat dilakukan dengan berbagai cara, seperti mengirimkan permintaan palsu, membanjiri *bandwidth*, mengubah informasi *routing*, atau mengeksploitasi kerentanan protokol. Serangan DoS dapat menimbulkan kerugian besar bagi penyedia layanan, pengguna, dan organisasi yang terlibat (Mirkovic, 2004).

Ancaman lainnya adalah serangan *Man In The Middle* (MITM). Serangan *Man in the Middle* (MITM) adalah salah satu serangan yang dilakukan dari dalam jaringan untuk melakukan penyadapan informasi dengan cara membelokkan jalur koneksi dimana penyerang (*attacker*) berada di antara dua target yang sedang melakukan komunikasi (Putra, 2011). Serangan ini memanfaatkan celah yang ada pada sistem untuk memanipulasi atau mencuri data yang sedang dikirimkan. Penyerang (*attacker*) akan memasukkan dirinya di antara dua pihak atau perangkat dalam tanpa diketahui sehingga semua paket yang berlintas antara kedua pihak yang sah itu dialihkan melalui penyerang tersebut (Riadi, 2020).

Pada penelitian yang telah dilakukan oleh Rachman (2021), penelitian tersebut bertujuan untuk menganalisis tingkat keamanan jaringan WLAN yang digunakan oleh PT. PLN (Persero) Sektor Pengendalian Pembangkitan Pekanbaru dengan menggunakan metode *penetration testing*. *Penetration testing* adalah simulasi serangan terhadap jaringan untuk menguji kerentanan dan menemukan solusi. Penelitian ini menggunakan sistem operasi Kali Linux yang memiliki berbagai *tools* untuk melakukan *penetration testing*. Dalam lingkup WLAN Departemen Teknik Elektro FT-UH telah terdapat penelitian sebelumnya, yaitu penelitian Miftahul Fahrina (2023) bertujuan untuk melakukan analisis keamanan WLAN Departemen Teknik Elektro FT-UH dengan melakukan uji coba jenis serangan *Sniffing traffic* (ARP *Spoofing*), *Deauthenticating client*, dan *Cracking* WPA. Dalam lingkup Departemen Teknik Elektro FT-UH, belum ada penelitian yang membahas mengenai jenis serangan *Denial of Service* (DoS) dan *Man In The Middle* terhadap WLAN Departemen Teknik Elektro FT-UH. Alasan ini yang menjadi dasar oleh penulis untuk mengimplementasikan jenis serangan *Denial of Service* (DoS) dan *Man In The Middle* (MITM) untuk menguji kemanan WLAN Departemen Teknik Elektro FT-UH.

Penelitian ini bertujuan untuk menguji keamanan jaringan WLAN Departemen Teknik Elektro FT-UH dengan melakukan uji coba serangan *Denial of Service* (DoS) dan serangan *Man in the Middle* (MITM) menggunakan metode *Penetration Testing*. Ada beberapa alasan digunakan jenis serangan ini, karena tidak semua jenis serangan relevan untuk setiap sistem. Misalnya, serangan *Cross-site scripting* (XSS) dan SQL *injection* lebih relevan untuk aplikasi web daripada jaringan WLAN. *Denial of Service* (DoS) dan *Man In The Middle* (MITM) merupakan jenis serangan yang umum dan dapat diimplementasikan oleh berbagai pihak. Alasan lainnya, beberapa jenis serangan dapat menimbulkan risiko yang lebih besar daripada manfaatnya. Misalnya, serangan yang merusak sistem atau data dapat memiliki konsekuensi negatif yang signifikan, terutama jika sistem tersebut digunakan untuk operasi sistem. Adapun serangan yang digunakan yaitu, ICMP *flood*, SYN *flood*, UDP *flood*, ARP *Spoofing*, dan MAC *Spoofing*. Serangan ini dipilih karena relevan mengenai dampak serangan pada sumber daya jaringan, lalu lintas data, atau kinerja jaringan secara umum. Pemilihan jenis serangan dapat disesuaikan untuk memenuhi tujuan pengukuran ini.

Dalam penelitian ini, jenis serangan MITM yang lain, yaitu serangan DNS *Spoofing* tidak diujikan karena fokus penelitian ini ada pada tingkat dasar jaringan dan lapisan *data-link*. Hal ini relevan dengan serangan ICMP *flood*, SYN *flood*, UDP *flood*, ARP *spoofing*, dan MAC *spoofing* untuk memahami dampaknya pada keamanan jaringan. Selain itu, menghindari serangan ini juga mempertimbangkan untuk meminimalkan risiko tambahan yang lebih kompleks dari manipulasi DNS. Dengan fokus pada serangan yang lebih umum, penelitian dapat memberikan wawasan lebih spesifik tentang potensi kerentanan pada lapisan *data-link* tanpa mengujikan kompleksitas yang tidak perlu melalui serangan DNS *Spoofing*.

Penelitian ini dimulai dengan melakukan fase *pre-attack*, yang meliputi pengumpulan informasi yang berkaitan dengan korban (*victim*) serta *tools* apa saja yang diperlukan dalam dalam uji penetrasi. Selanjutnya akan dilakukan fase *attack*, dengan melakukan serangan *Denial of Service* dapat menghabiskan sumber daya, membebani kapasitas, atau memicu kesalahan sistem atau jaringan korban sehingga layanan menjadi tidak tersedia atau menjadi lambat pada jaringan korban (*victim*)

sehingga layanan menjadi tidak tersedia atau menjadi lambat (Zlomislić, 2017) dan serangan dan *Man in the Middle* (MITM) dimana penyerang (*attacker*) akan memasukkan dirinya di antara dua pihak atau perangkat dalam tanpa diketahui sehingga semua paket yang berlintas antara kedua pihak yang sah itu dialihkan melalui penyerang tersebut (Riadi, 2020). Terakhir, yaitu fase *post-attack* dengan melakukan pembersihan proses pengujian dan mengembalikkan sistem yang diuji kembali ke status pengujiannya serta menilai dampak keparahan keamanan WLAN. Hasil dari penelitian ini diharapkan dapat menunjukkan tingkat keamanan WLAN Departemen Teknik Elektro FT-UH yang digunakan terhadap serangan DoS dan MITM serta menjadi bahan evaluasi dari sistem keamanan jaringan.

1.2 Rumusan Masalah

Berdasarkan pemahaman atas latar belakang penelitian, maka dapat dirumuskan masalah sebagai berikut:

1. Bagaimana dampak serangan DoS dan MITM terhadap jaringan WLAN kampus?
2. Bagaimana tingkat keamanan jaringan WLAN kampus terhadap serangan DoS dan MITM sesuai metode *vulnerability assessment*?

1.3 Tujuan Penelitian

Tujuan yang ingin dicapai dalam penelitian ini adalah:

1. Menganalisis dampak serangan DoS dan MITM terhadap jaringan WLAN kampus.
2. Mengidentifikasi tingkat keamanan jaringan WLAN kampus terhadap serangan DoS dan MITM sesuai dengan metode *vulnerability assessment.*

1.4 Manfaat Penelitian

Manfaat dari penelitian ini meliputi:

1. Bagi pengelola jaringan kampus, penelitian ini dapat menjadi panduan dalam memahami dan mengatasi potensi serangan DoS dan MITM terhadap jaringan WLAN.
2. Dalam bidang pendidikan, penelitian ini dapat menjadi sumber referensi bahan pembelajaran serta memberikan wawasan tentang kerentanan yang perlu diatasi dalam konteks jaringan kampus.
3. Bagi penelitian masa depan, penelitian ini dapat menjadi dasar untuk pengembangan strategi perlindungan yang lebih baik terhadap serangan DoS dan MITM pada jaringan WLAN.

1.5 Ruang Lingkup

Ruang lingkup penelitian ini adalah pengimplementasian metode *vulnerability assessment* dengan *penetration testing* melalui serangan DoS dan MITM. Adapun batasan masalah pada penelitian ini:

1. Penelitian ini akan berfokus pada evaluasi kerentanan jaringan WLAN kampus terhadap serangan DoS dan MITM dan tidak membahas langkah-langkah mitigasi atau perlindungan terhadap serangan tersebut.
2. IP dan MAC *address* dari *victim* dan *attacker* telah diketahui sebelum melakukan pengujian. Pengujian akan dilakukan dalam lingkungan yang mencakup jaringan WLAN Departemen Teknik Elektro FT-UH.
3. Jenis serangan DoS dan MITM yang akan dievaluasi akan dibatasi pada serangan ICMP *flood, SYN flood,* UDP *flood,* ARP *spoofing,* dan MAC *Spoofing.*
4. Sisi *Attacker* menggunakan sistem operasi Kali Linux dan sisi *Victim* menggunakan sistem operasi Windows.
5. Parameter yang diuji pada serangan DoS adalah *throughput* WiFi dan *utilization* CPU, pada serangan ARP *Spoofing* adalah perubahan tabel ARP (ARP *Cache*), dan pada serangan MAC *Spoofing* adalah perubahan MAC *Address Attacker*

6. Jenis *assessment* yang digunakan untuk menilai kerentanan adalah *Base Metric* dari *Forum of Incident Response and Security Teams* (FIRST) CVSS v4.0

1.6 Sistematika Penulisan

Untuk memudahkan pemahaman terhadap penelitian ini, maka diuraikan sistematika penulisan sebagai berikut:

BAB I PENDAHULUAN

Pada bab ini berisi tentang penguraian secara singkat latar belakang, Rumusan masalah, Tujuan penelitian, Manfaat Penelitian, Ruang Lingkup dan Sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Pada bab ini berisi penjelasan tentang teori penunjang yang relevan untuk bahan penelitian yang diperoleh dari sumber referensi untuk menyusun laporan tugas akhir ini.

BAB III METODOLOGI PENELITIAN

Bab ini membahas mengenai rancangan penelitian, waktu dan tempat penelitian, diagram alir perencanaan, alat dan bahan yang digunakan, serta teknik pengumpulan dan analisis data pada penelitian tugas akhir ini.

BAB IV ANALISIS DAN PEMBAHASAN

Bab ini membahas mengenai hasil dan pembahasan analisis penelitian yang dilakukan, meliputi analisis fase pengujian dan pembahasan keadaan sebelum serangan, keadaan setelah serangan, serta skor penilaian tingkat keamanan wifi.

BAB V KESIMPULAN DAN SARAN

Bab ini merupakan bab penutup yang berisi kesimpulan dari penelitian yang dilakukan serta saran untuk pengembangan yang berguna pada studi lanjut tugas akhir berikutnya.

BAB II

TINJAUAN PUSTAKA

2.1 Penelitian Terdahulu

Berikut merupakan penelitian-penelitian terdahulu yang terkait dengan penelitian ini:

Tabel 1 Penelitian terdahulu

Deskripsi Jurnal	**Pembahasan**
JUDUL: Analisis Keamanan Jaringan *Wireless* LAN (WLAN) Dengan Metode *Penetration Testing* Pada PT. PLN (Persero)Sektor Pengendalian Pembangkitan Pekanbaru Tahun: 2021 Peneliti: RIVALDI RACHMAN	Penelitian ini menguji keamanan jaringan *Wireless Local Area Network* (WLAN) di PT. PLN (Persero) Sektor Pengendalian Pembangkitan Pekanbaru menggunakan metode *Penetration Testing*. Hasil penelitian menunjukkan bahwa jaringan WLAN ini memiliki beberapa celah keamanan yang dapat dieksploitasi. Analisis lalulintas jaringan menggunakan Wireshark mengungkapkan informasi penting seperti alamat IP, waktu, sumber, tujuan, protokol, panjang, dan lainnya. Meskipun tiga jenis serangan dilakukan, hanya serangan *cracking the encryption* yang gagal. Pengujian *Man In The Middle* (MITM) juga menunjukkan bahwa jaringan WLAN belum memberikan keamanan yang cukup kepada pengguna yang terkoneksi, meninggalkan mereka rentan terhadap gangguan dan penyadapan saat mengakses layanan internet yang sama.
JUDUL: *VULNERABILITY ASSESSMENT* DALAM ANALISIS KEAMANAN WLAN DEPARTEMEN TEKNIK ELEKTRO FT-U Tahun: 2023 Peneliti: MIFTAHUL FARINA	Penelitian ini fokus pada keamanan *Wireless Local Area Network* (WLAN) di gedung Departemen Teknik Elektro FT-UH dengan menggunakan metode *penetration testing* dan *vulnerability assessment*. Hasil pengujian mengungkap dampak dari *vulnerability*, termasuk pengungkapan informasi kredensial *login* saat mengakses web HTTP, serangan *deauthenticating client* dan pengungkapan *password* dari AP WPA2-PSK. Namun, sistem *hashing* dari *login* web jaringan kampus mencegah *password* ditransmisikan dalam bentuk teks biasa. Evaluasi kerentanan ini dengan CVSS v3.1 menghasilkan skor 5.4, dikategorikan sebagai *Medium*, menunjukkan bahwa kerentanan ini masih berpotensi merugikan jaringan dan penggunanya, terutama pada koneksi AP WPA2-PSK dan AP *Open-Encrypted* pada WLAN kampus.

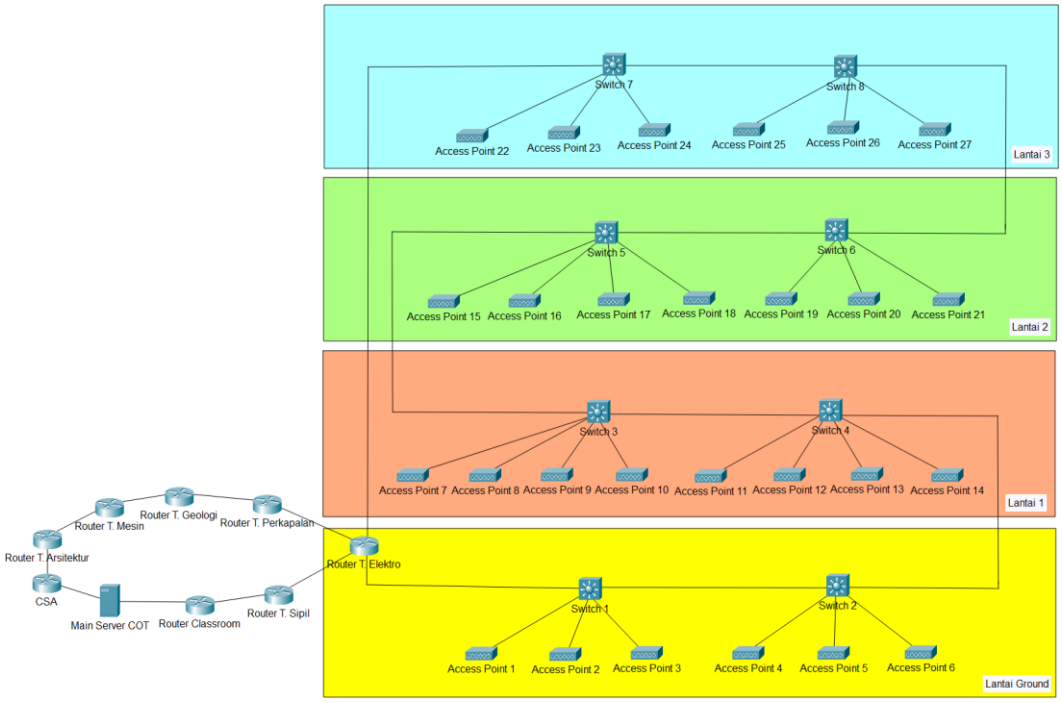
JUDUL: Analisis Pengamanan Jaringan Menggunakan Router Mikrotik dari Serangan DoS dan Pengaruhnya Terhadap Performansi Tahun: 2021 Penulis: Arief Indriarto Haris, Budhi Riyanto, Farry Surachman, Ardito Adi Ramadhan	Penelitian ini mengkaji serangan *Denial of Service* (DoS) dalam konteks penggunaan router MikroTik sebagai *gateway* dalam jaringan. Hasil penelitian menunjukkan bahwa serangan DoS memiliki dampak destruktif terhadap target, terutama dalam peningkatan penggunaan sumber daya, terutama CPU dan latensi. Secara keseluruhan, penggunaan fitur-fitur keamanan bawaan router MikroTik dianggap kurang efektif dalam menghadapi serangan DoS, dengan tingkat penggunaan CPU yang tinggi dan tidak dapat menghilangkan sepenuhnya *traffic* DoS. Oleh karena itu, untuk mengamankan jaringan dari serangan DoS, diperlukan dukungan perangkat tambahan selain dari router. Studi berikutnya disarankan untuk mengeksplorasi metode, arsitektur, dan integrasi dengan perangkat tambahan lainnya untuk meningkatkan deteksi dan mitigasi serangan DoS secara lebih efektif.
JUDUL: Manajemen Pencegahan erangan Jaringan Wireless Dari Serangan *Man In The Middle Attack* Tahun: 2022 Penulis: Tengku Mohd Diansyah, Ilham Faisal, Dodi Siregar	Penelitian ini menganalisis celah keamanan dalam jaringan *wireless* yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab, terutama serangan *Man In The Middle*. Sebanyak lima percobaan serangan *Man In The Middle* dilakukan, dengan hasil bahwa serangan tersebut berhasil menyebabkan *packet loss* yang signifikan dalam komunikasi *wireless*. Untuk mencegah serangan semacam ini, penting untuk memahami teknik serangan yang digunakan dalam jaringan *wireless* dan menggunakan alat seperti *ettercap* pada Kali Linux. Melalui serangkaian pengujian dan analisis, solusi yang dihasilkan adalah untuk meningkatkan keamanan pada website atau SSL (*secure sockets layer*) guna menghindari serangan *Man In The Middle*.
JUDUL: Analisis Keamanan Jaringan pada Jaringan *Wireless* dari *Serangan Man In The Middle Attack DNS Spoofing* Tahun: 2022 Penulis: Teguh Pangestu, Risko Liza	Penelitian ini kendala keamanan seperti serangan ilegal Man In The Middle dan DNS *spoofing* pada jaringan *wireless*. Penelitian ini melakukan serangkaian uji coba dengan menghitung *Quality of Service* (QoS) berdasarkan *packet loss* dalam tujuh pengujian yang berbeda. Hasil menunjukkan bahwa beberapa serangan *Man In The Middle* berhasil dengan *packet loss* yang bervariasi. Penggunaan sistem keamanan firewall terbukti mampu mencegah komunikasi antara penyerang dan korban, tetapi tidak mengatasi serangan sepenuhnya.

2.2 Dasar Teori

2.2.1 *Wireless Network*

Jaringan nirkabel (*Wireless Network*) adalah jaringan yang menggunakan gelombang radio untuk menghubungkan perangkat, tanpa perlu menggunakan kabel apa pun. Jaringan nirkabel bekerja mirip dengan jaringan kabel, namun jaringan nirkabel harus mengubah sinyal informasi menjadi bentuk yang sesuai untuk transmisi melalui media udara. Jaringan nirkabel melayani banyak tujuan. Dalam beberapa kasus, jaringan nirkabel digunakan sebagai pengganti kabel, sementara dalam kasus lain digunakan untuk menyediakan akses ke data perusahaan dari lokasi yang jauh (Salazar, 2017).

Infrastruktur nirkabel dapat dibangun dengan biaya yang sangat sedikit dibandingkan dengan alternatif kabel tradisional. Penghematan waktu dan tenaga dengan memiliki akses terhadap jaringan informasi global menghasilkan kekayaan dalam skala lokal, karena lebih banyak pekerjaan dapat diselesaikan dalam waktu dan usaha yang lebih sedikit (Salazar, 2017).



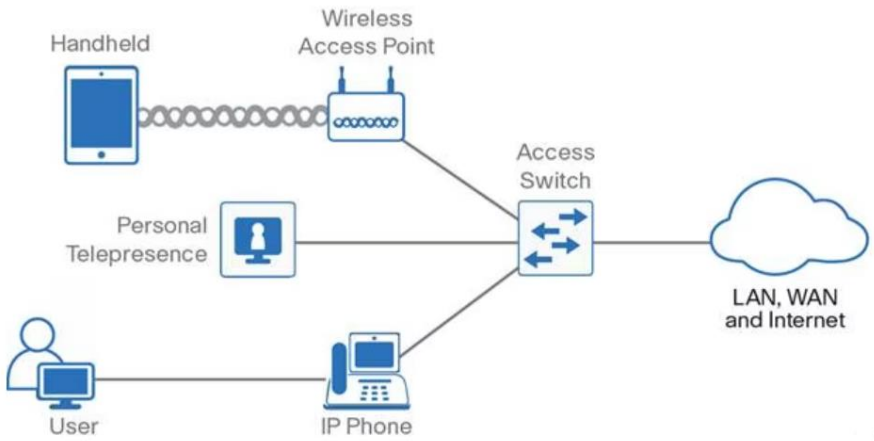
Sumber : Dibuat oleh penulis

Gambar 1 Arsitektur jaringan Departemen Teknik Elektro FT-UH

Jaringan nirkabel dapat diklasifikasikan menjadi empat kelompok tertentu menurut wilayahnya aplikasi dan jangkauan sinyal. Klasifikasi tersebut antara lain: *Wireless Personal-Area Networks* (WPAN), *Wireless Local-Area Networks* (WLAN), *Wireless Metropolitan-Area Networks* (WMAN), dan *Wireless Wide-Area Networks* (WWAN) (Salazar, 2017).

2.2.2 *Wireless Local Area Network (WLAN)*

Wireless Local Area Network (WLAN) dirancang untuk menyediakan akses nirkabel di area dengan jangkauan tipikal hingga 100 meter dan, sebagian besar digunakan di lingkungan rumah, sekolah, laboratorium komputer, atau kantor seperti pada Gambar 2. Hal ini memberikan pengguna kemampuan untuk berpindah-pindah dalam area jangkauan lokal dan tetap terhubung ke jaringan (Salazar, 2017).



Sumber : https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-campus-lan-wlan-design-guide.html

Gambar 2 Contoh diagram WLAN sederhana

WLAN didasarkan pada standar IEEE 802.11, dipasarkan dengan merek Wi-Fi. IEEE 802.11 lebih sederhana untuk diimplementasikan dan lebih cepat dipasarkan. IEEE 802.11 adalah rangkaian standar berbeda untuk jaringan area lokal nirkabel. IEEE 802.11b adalah standar pertama yang diterima, mendukung hingga 11 Mbps pada pita spektrum 2,4 GHz tanpa izin. Kemudian, standar IEEE 802.11g dirancang sebagai penerus IEEE 802.11b dengan *bandwidth* yang lebih tinggi. Jalur akses IEEE 802.11g akan mendukung klien 802.11b dan 802.11g.

Demikian pula, laptop dengan kartu IEEE 802.11g akan dapat mengakses titik akses 802.11b yang ada serta titik akses 802.11g yang baru. Hal ini karena LAN nirkabel berbasis 802.11g akan menggunakan pita 2,4 GHz yang sama dengan yang digunakan 802.11b. Kecepatan transfer maksimum untuk tautan nirkabel IEEE 802.11g adalah 54 Mbps, namun secara otomatis akan mundur dari 54 Mbps ketika sinyal radio lemah atau ketika gangguan terdeteksi (Salazar, 2017).

2.2.3 *Cyber Security*

Security didefinisikan sebagai "perlindungan terhadap pengungkapan, penghancuran, atau modifikasi data yang tidak diinginkan dalam suatu sistem dan juga perlindungan sistem itu sendiri" (Valeriano, 2018). Menurut ISACA "*Cyber security* berkaitan dengan keamanan dan privasi aset digital, mulai dari jaringan hingga perangkat komputasi dan informasi yang diproses, disimpan, atau dipertukarkan oleh sistem informasi yang terhubung melalui internet" (Von Solms, 2018). Menurut Persatuan Telekomunikasi Internasional, keamanan siber adalah kumpulan teknik, aturan, kebijakan, praktik terbaik, dan pendekatan yang digunakan untuk melindungi aset pengguna dan organisasi siber (Ron, 2018). Keamanan siber didefinisikan sebagai "menjaga integritas, kerahasiaan, dan ketersediaan informasi tepat waktu di dunia maya" (Von Solms, 2018). Kamus Merriam-Webster mendefinisikan *cyber security* sebagai melindungi sistem komputer dari akses dan serangan tidak sah (Al Mazari, 2018). Menurut Von Solms, *cyber security* didefinisikan sebagai proses dan teknologi yang digunakan untuk melindungi perangkat komputasi dan jaringan dari akses tidak sah dan serangan melalui Internet. Keamanan siber adalah perlindungan komponen fisik dan non-fisik organisasi dari akses ilegal (Hansen, 2009).

Berdasarkan definisi ini, para peneliti mendefinisikan *cyber security* dengan cara yang berbeda-beda. Definisi yang ada berfokus pada aspek keamanan siber yang berbeda. Misalnya, beberapa definisi berfokus pada perlindungan dan privasi, sementara definisi lain menegaskan perlunya mendefinisikan aturan dan kebijakan untuk integritas, kerahasiaan, dan ketersediaan informasi. Selain itu, peneliti lain menekankan perlunya mendefinisikan proses dan teknologi untuk melindungi

perangkat komputasi. Keamanan siber dapat dianggap sebagai mekanisme untuk melindungi aset individu dan organisasi dari akses tidak sah. Definisi ini juga menegaskan pentingnya lingkungan siber dan perlindungannya (Humayun, 2020).

2.2.4 *Network-level Attack Techniques*

Serangan adalah tindakan yang diambil untuk merusak sistem atau mengganggu operasi rutinnya dengan mengeksploitasi kerentanan menggunakan berbagai alat dan teknik. Penyerang (*Attacker*) meluncurkan ini serangan untuk mencapai tujuan jahat mereka, baik untuk kepuasan diri sendiri atau untuk imbalan finansial (Johnson, 2016).

Penyerang (*Attacker*) menggunakan berbagai strategi serangan jaringan untuk membahayakan keamanan jaringan. Adapun jenis serangan atau *vulnerability* pada tingkat jaringan, antara lain:

a. *Denial of Service* (DoS)

Denial of Service (DoS) Jenis serangan ini merupakan upaya untuk membuat mesin atau sumber daya jaringan tidak dapat diakses oleh pengguna yang dituju. Hal ini disebabkan oleh peristiwa apa pun yang melemahkan atau menghilangkan kapasitas jaringan untuk menjalankan fungsi yang diharapkan. Karena kemampuan memori yang rendah dan sumber daya yang terbatas, sebagian besar perangkat komputasi di lingkungan IoT rentan terhadap serangan ini (Chonka, 2012). Ada beberapa jenis serangan DoS antara lain:

1. SYN *Flood*

Serangan ini mengeksploitasi proses *three-way handshake* dari *Transmission Control Protocol* (TCP) untuk menghabiskan sumber daya *server*. Penyerang mengirimkan paket SYN dalam jumlah besar ke *server*, tetapi tidak menyelesaikan proses jabat tangan dengan mengirimkan paket ACK terakhir, meninggalkan *server* menunggu paket ACK dan tidak dapat menanggapi permintaan yang sah (Ali, 2018).

Paket SYN dan ACK adalah dua jenis paket yang digunakan dalam protokol *Transmission Control Protocol* (TCP). TCP adalah protokol lapisan *transport* yang digunakan untuk komunikasi yang andal dan

terkontrol. Paket SYN (*Synchronization*) digunakan untuk memulai koneksi TCP. Paket SYN berisi nomor urutan awal yang akan digunakan untuk data yang dikirimkan oleh klien. Server yang menerima paket SYN akan membalas dengan paket SYN-ACK (*Synchronization-Acknowledgement*). Paket SYN-ACK berisi nomor urutan awal yang akan digunakan untuk data yang dikirimkan oleh server, serta nomor urutan yang diharapkan diterima dari klien. Paket ACK (*Acknowledgement*) digunakan untuk mengakui penerimaan data. Paket ACK berisi nomor urutan data yang telah diterima. Paket SYN dan ACK adalah bagian dari *three-way handshake* yang digunakan untuk memulai koneksi TCP. Three-way handshake arah memastikan bahwa kedua belah pihak setuju untuk membuat koneksi, serta menetapkan nomor urutan yang akan digunakan untuk data yang dikirimkan (Kurose, 2017)

2. ICMP *Flood*

   Serangan ICMP *Flood* atau biasa disebut Ping *Flood* mengirimkan sejumlah besar paket *Internet Control Message Protocol* (ICMP) ke *server*, membebani lalu lintas dan membuatnya tidak dapat merespons permintaan yang sah (Ali, 2018).

   Paket ICMP adalah paket jaringan yang digunakan untuk mengirimkan pesan kontrol antara perangkat jaringan. Paket ICMP dapat digunakan untuk berbagai tujuan, termasuk: menyampaikan pesan kesalahan, seperti pesan "alamat tidak ditemukan" atau pesan "koneksi ditolak"; melakukan *ping* pada perangkat jaringan untuk memeriksa apakah perangkat tersebut terhubung dan tersedia; serta melakukan *traceroute* untuk menentukan jalur yang diambil oleh paket data saat melintasi jaringan (Kurose, 2017).

3. UDP *Flood*

   Serangan ini mengirimkan sejumlah besar paket *User Datagram Protocol* (UDP) ke *server*, membebani lalu lintas dan membuatnya tidak dapat merespons permintaan yang sah (Ali, 2018).

Paket UDP adalah paket yang digunakan untuk komunikasi data yang tidak memerlukan jaminan. Artinya, paket UDP tidak memastikan bahwa data yang dikirimkan akan diterima dalam keadaan utuh dan benar. Paket UDP tidak menggunakan mekanisme *three-way handshake*, sehingga data dapat dikirimkan langsung dari satu *host* ke *host* lainnya. (Kurose, 2017).

b. *Man In The Middle*

Man In The Middle (MITM) adalah serangan di mana pihak ketiga yang tidak berwenang diam-diam menguasai saluran komunikasi antara beberapa titik akhir. Penyerang MITM dapat mengganggu, memanipulasi atau bahkan mengganti lalu lintas komunikasi target korban. Lebih lanjut, korban tidak menyadari adanya penyusup, sehingga percaya bahwa saluran komunikasi aman dan terlindungi (Indre, 2016). Adapun contoh serangan dari MITM, yaitu:

1. ARP *Spoofing*

Dalam serangan ARP *spoofing*, *attacker* menyamar sebagai entitas sah dalam jaringan nirkabel. *Attacker* memalsukan paket ARP untuk memodifikasi (*poisoning*) tabel ARP dari *host* target, sehingga dapat menyebabkan berkurangnya efisiensi jaringan, kemacetan, dan potensi pencurian informasi (Zhu, 2022).

Paket ARP adalah paket yang digunakan untuk menentukan alamat MAC perangkat jaringan yang memiliki alamat IP tertentu. Alamat IP adalah alamat logis yang digunakan untuk mengidentifikasi *host* dalam jaringan, sedangkan alamat MAC adalah alamat fisik yang digunakan untuk mengidentifikasi perangkat keras jaringan. Tabel ARP adalah tabel yang menyimpan informasi tentang alamat IP dan alamat MAC dari host di jaringan (Kurose, 2017).

2. DNS *Spoofing*

DNS *Spoofing* adalah jenis serangan di mana penyerang memalsukan respons DNS untuk mengarahkan pengguna ke situs web jahat atau mencegat komunikasi mereka. Dalam serangan *spoofing* DNS,

penyerang dapat memanipulasi *cache* DNS dari *host* target, menyebabkannya mengaitkan nama *domain* yang sah dengan alamat IP berbeda yang dikendalikan oleh penyerang (Nasser, 2022).

3. MAC Spoofing

MAC *spoofing* adalah kegiatan memalsukan alamat *Media Access Control* (MAC) di suatu perangkat komputer untuk meniru identitas perangkat lain di jaringan (Nasser, 2022).

c. *Malware*

Dalam serangan ini, penyerang menyebarkan *malware* program perangkat lunak untuk mendapatkan akses tidak sah ke sistem komputer dengan mengeksploitasi kerentanan keamanannya (Gantsou, 2015).

d. *Phising*

Phishing adalah aktivitas melanggar hukum yang menggunakan media sosial teknik dan teknologi untuk mengumpulkan informasi sensitif dari pengguna Internet. Teknik *phishing* memanfaatkan berbagai metode komunikasi, seperti *email*, pesan instan, pesan *pop-up* atau halaman Web (Hesar, 2014).

e. SQL *Injection Attack*

Dalam serangan ini, *string input* adalah disuntikkan melalui aplikasi untuk mengubah atau memanipulasi SQL untuk keuntungan penyerang. Serangan ini merusak *database* dalam beberapa cara, termasuk akses tidak sah dan manipulasi *database*, dan pengungkapan data sensitif. Serangan ini berisiko seperti hal ini dapat menyebabkan hilangnya data atau penyalahgunaan data oleh kelompok siapa tidak diizinkan, dan akibatnya, fungsionalitas dan kerahasiaan dihancurkan. Selanjutnya, perintah tingkat sistem juga dijalankan dalam kategori serangan ini, mengakibatkan pengguna yang berwenang tidak dapat mengakses informasi yang diperlukan (Hu, 2016).

f. *Cross-site scripting* (XSS)

Dalam jenis serangan ini, penyerang jahat mencoba menjalankan kode *JavaScript* di klien browser untuk mencuri data sensitif klien. XSS merupakan kerentanan yang umum digunakan ditemukan di situs web (Jing, 2012).

2.2.5 Penetration Testing

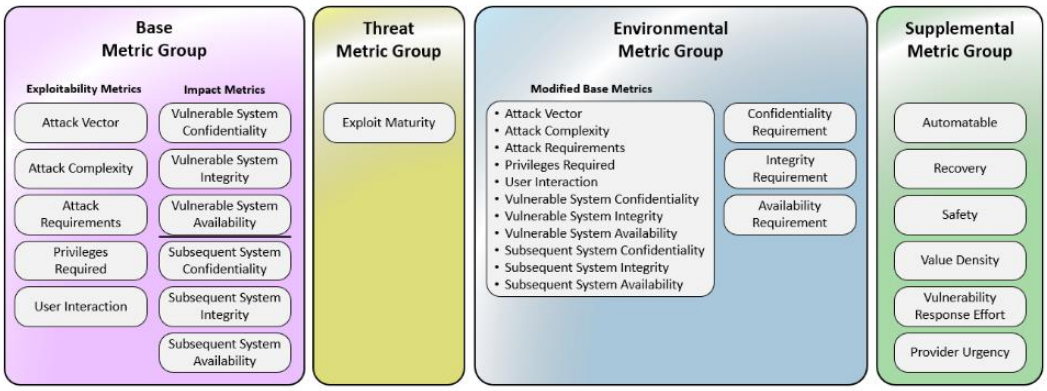
Penetration Testing atau biasa disebut dengan *pen testing* adalah pengujian keamanan dimana seorang penguji meniru serangan yang biasa sering terjadi untuk mengidentifikasi metode peretasan fitur keamanan aplikasi, sistem, atau jaringan. Pengujian ini dilakukan oleh penguji menggunakan serangan yang nyata, sistem yang nyata, dan data yang nyata menggunakan alat dan teknik yang sering dipakai oleh seorang *Hacker*. *Penetration Testing* biasanya dilakukan bersamaan dengan *Vulnerability Assessment* (VA) (Rachman, 2021).

2.2.6 *Vulnerability Assessment*

Vulnerability Assessment (Penilaian Kerentanan) adalah proses mengidentifikasi kerentanan pada komponen jaringan, termasuk OS, aplikasi web, dan *server* web. Sistem menilai kerentanan dan memprioritaskannya, serta merancang metode untuk memperbaiki situasi tersebut. Metode penilaian membantu mengukur efektivitas solusi tersebut. Tujuan dari penilaian kerentanan mencakup pemindaian, pemeriksaan, evaluasi, dan pelaporan kerentanan dalam jaringan untuk meminimalkan tingkat risiko terhadap organisasi (Ec-Council, 2020).

Common Vulnerability Scoring System (CVSS) merupakan standar yang telah dipublikasi dengan menyediakan *open framework* dalam membahas karakteristik dan dampak dari IT *vulnerability*. Data yang diberikan merupakan model kuantitatif yang memastikan pengukuran akurat dan *repeatable* sekaligus memastikan *user* dapat melihat karakteristik dasar *vulnerability* dalam penentuan skor. Skor yang dihasilkan kemudian dibuat representasi kualitatifnya (seperti, *low, medium, high*, atau *critical*) (Farina, 2023).

CVSS sendiri dikelola oleh *Forum of Incident Response and Security Teams, Inc* (FIRST.Org, Inc.) yang merupakan organisasi non-profit US dengan misi membantu tim respons insiden keamanan komputer di seluruh dunia. Merujuk pada website FIRST, bahwa CVSS memiliki 3 jenis metrik yaitu, *base*, *temporal*, dan *environmental*.



Sumber : https://www.first.org/cvss/v4.0/specification-document

Gambar 3 Jenis metrik berdasarkan *Forum of Incident Response and Security Teams* (FIRST)

Base Metric Group mewakili karakteristik intrinsik kerentanan yang konstan sepanjang waktu dan di seluruh lingkungan pengguna. *The Threat Metric Group* mencerminkan karakteristik kerentanan yang dapat berubah seiring waktu namun tidak di seluruh lingkungan pengguna. *Enviromental Metric Group* mewakili karakteristik kerentanan yang relevan dan unik terhadap lingkungan pengguna tertentu. *The Supplemental metric group* merupakan sekelompok metrik yang memberikan konteks serta menjelaskan dan mengukur atribut ekstrinsik tambahan dari sebuah kerentanan. Metrik tambahan ini tidak memiliki dampak langsung pada skor CVSS akhir dan memberikan karakteristik tambahan dari kerentanan tersebut.

Pada penelitian ini, jenis *metric group* yang digunakan adalah *base metric group,* dengan parameter (*variable)* antara lain: *Attack Vector*, *Attack Complexity*, *Attack Requirements*, *Previleges Required*, *Confidentiality*, *Integrity*, *Availability.* Dilansir pada website FIRST, masing-masing metrik ini dibahas secara lebih rinci. Adapun tabel dan rubrik penskoran pada base metric CVSS v4.0, yaitu:

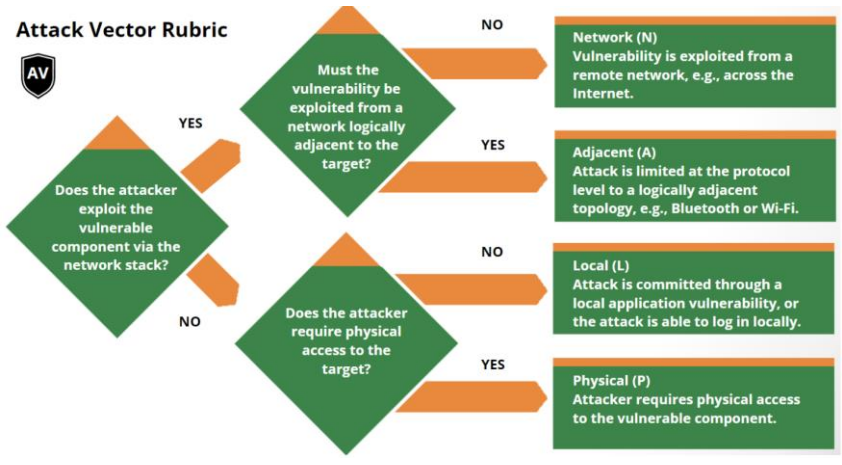
1. *Attack Vector* (AV)

   Metrik ini mencerminkan konteks yang memungkinkan eksploitasi kerentanan. Semakin jauh (secara logika dan fisik) seorang penyerang dapat berada saat mengeksploitasi sistem yang rentan, nilai metrik akan semakin besar.

Tabel 2 Rubik skor *Attack Vector* (AV)

Metrik	Deskripsi
Network (N)	*Vulnerability* yang berkaitan dengan *network* stack yang memungkinkan penyerangan melalui internet. *Vulnerability* seperti ini sering disebut "dapat dieksploitasi dari jarak jauh" dan dapat dianggap sebagai serangan yang dapat dieksploitasi pada tingkat protokol yang berjarak satu atau lebih jaringan (misalnya, pada satu atau lebih router). Contoh serangan jaringan ini adalah *Denial of Service* (DoS) dengan mengirimkan paket TCP yang dibuat khusus melalui jaringan area luas.
Adjacent (A)	Vulnerability terikat pada *network stack*, namun serangannya terbatas pada tingkat protokol hingga topologi yang berdekatan secara *logical*. Hal ini berarti serangan harus diluncurkan dari *shared physical network* (misalnya Bluetooth atau IEEE 802.11) atau network logical (misalnya subnet IP lokal), atau dari dalam domain administratif yang aman atau terbatas (misalnya MPLS, VPN aman untuk zona jaringan administratif).
Local (L)	*Attacker* mengeksploitasi *vulnerability* dengan mengakses sistem target secara lokal (misalnya *keyboard*, konsol), atau dari jarak jauh (SSH); atau *attacker* bergantung pada *user interaction* orang lain dalam mengeksploitasi *vulnerability* (seperti *social engineering* untuk mengelabui user yang sah agar membuka dokumen *malicious*).
Physical (P)	Serangan tersebut mengharuskan *attacker* untuk secara fisik memanipulasi *vulnerable* komponen. Interaksi fisik mungkin singkat atau terus-menerus. Contoh serangan semacam itu adalah serangan *cold boot* di mana penyerang mendapatkan akses ke kunci enkripsi disk setelah secara fisik mengakses sistem target.

Sumber : https://www.first.org/cvss/v4.0/specification-document



Sumber : https://www.first.org/cvss/v4.0/user-guide

Gambar 4 Rubrik *Attack Vector*

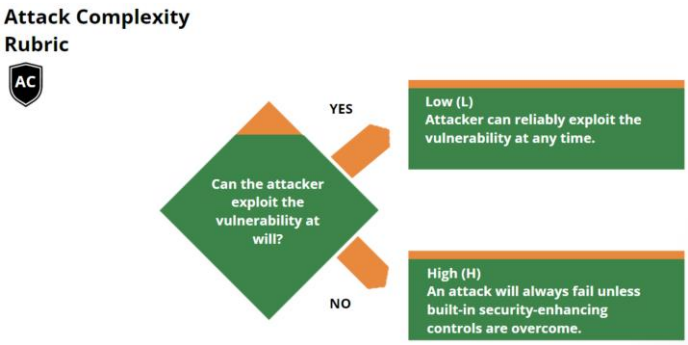
2. *Attack Complexity* (AC)

Metrik ini mengukur seberapa sulit bagi penyerang untuk mengeksploitasi kerentanan. Metrik ini dapat digunakan untuk menilai tingkat keparahan kerentanan dan menentukan prioritas mitigasi.

Tabel 3 Rubrik skor *Attack Complexity* (AT)

Metrik	Deskripsi
Low (L)	Kondisi akses khusus atau keadaan khusus tidak ada. Seorang penyerang dapat mengharapkan keberhasilan yang berulang ketika menyerang komponen yang rentan.
High (H)	Keberhasilan serangan bergantung pada kondisi di luar kendali penyerang. Artinya, serangan yang berhasil tidak dapat dilakukan sesuka hati. Serangan ini sering kali bergantung pada *vulnerability* yang baru atau jarang diketahui, atau pada pengetahuan teknis yang mendalam. Serangan dengan kompleksitas tinggi sering kali membutuhkan alat dan sumber daya yang kompleks untuk dieksekusi.

Sumber : https://www.first.org/cvss/v4.0/specification-document



Sumber : https://www.first.org/cvss/v4.0/user-guide

Gambar 5 Rubrik *Attack Complexity*

3. *Attack Requirements* (AT)

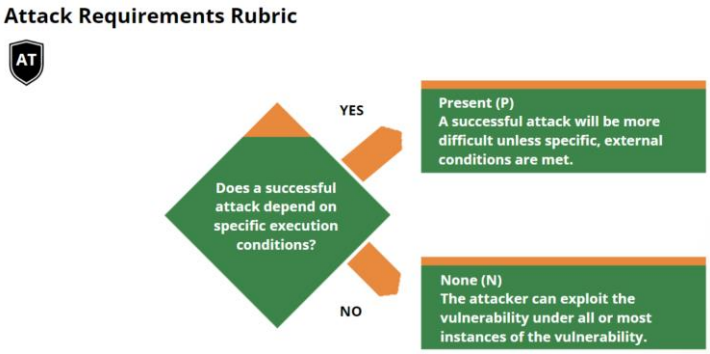
Metrik ini mengukur kondisi atau pengaturan bawaan dari sistem yang rentan, yang sebenarnya tidak dibuat khusus untuk mencegah serangan, tapi justru muncul secara alami karena cara sistem tersebut dipasang dan dijalankan.

Tabel 4 Rubrik skor *Attack Requirements* (AT)

Metrik	Deskripsi
None (N)	Serangan yang berhasil tidak bergantung pada kondisi penerapan dan eksekusi kerentanan sistem. *Attacker* diharapkan dapat mencapai *vulnerability* dan mengeksploitasi semua atau sebagian besar *vulnerability*. Serangan ini dapat dilakukan dengan sukses di semua atau

Metrik	Deskripsi
	sebagian besar kasus *vulnerability* dan tidak memerlukan suatu kondisi.
Present (P)	Keberhasilan serangan bergantung pada penerapan dan kondisi eksekusi yang spesifik dari kerentanan sistem yang memungkinkan terjadinya serangan. Hal ini termasuk: keberhasilan penyerangan dikondisikan pada kondisi eksekusi yang tidak berada dalam kendali penuh *attacker*, serangan tersebut mungkin perlu diluncurkan beberapa kali terhadap satu serangan sebelum berhasil, ataupun penyerang harus memasukkan dirinya ke dalam jalur jaringan logis antara target dan sumber daya yang diminta oleh korban (misalnya *vulnerability* yang memerlukan *attacker* di jalur tersebut). Dengan kata lain, serangan ini hanya dapat dilakukan jika kondisi tertentu terpenuhi. Kondisi ini dapat membuat serangan lebih sulit dilakukan, tetapi juga dapat membuatnya lebih sulit dideteksi dan dilindungi.

Sumber : https://www.first.org/cvss/v4.0/specification-document



Sumber : https://www.first.org/cvss/v4.0/user-guide

Gambar 6 Rubrik *Attack Requirements*

4. *Previleges Required* (PR)

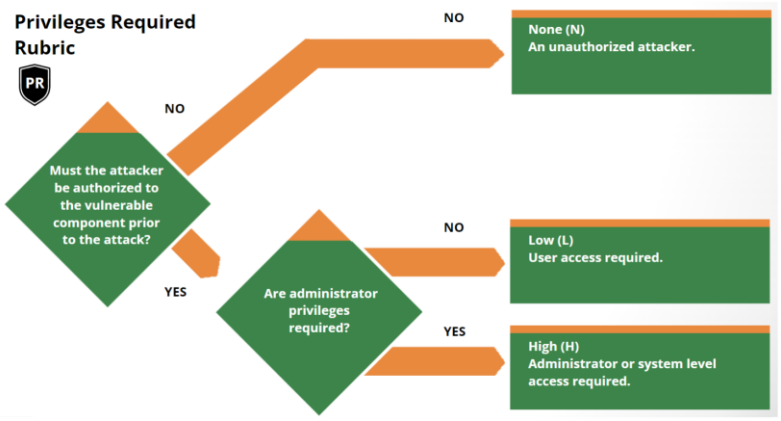
Metrik ini mengukur tingkat kewenangan yang dibutuhkan penyerang untuk mengeksploitasi kerentanan. Semakin tinggi kewenangan yang dibutuhkan, semakin sulit (dan berbahaya) serangan tersebut.

Tabel 5 Rubrik skor *Previleges Required* (PR)

Metrik	Deskripsi
None (N)	*Attacker* tidak memerlukan akses ke pengaturan atau file kerentanan sistem untuk melakukan serangan.
Low (L)	*Attacker* memerlukan akses ke pengaturan atau file kerentanan sistem, tetapi akses tersebut dibatasi pada pengaturan atau file yang dimiliki oleh pengguna dengan hak istimewa rendah.

Metrik	Deskripsi
High (H)	*Attacker* memerlukan akses ke pengaturan atau file kerentanan sistem, dan akses tersebut memberikan kontrol signifikan (misalnya, administratif) atas sistem yang rentan.

Sumber : https://www.first.org/cvss/v4.0/specification-document



Sumber : https://www.first.org/cvss/v4.0/user-guide

Gambar 7 Rubrik *Previleges Required*

5. *User Interaction* (UI)

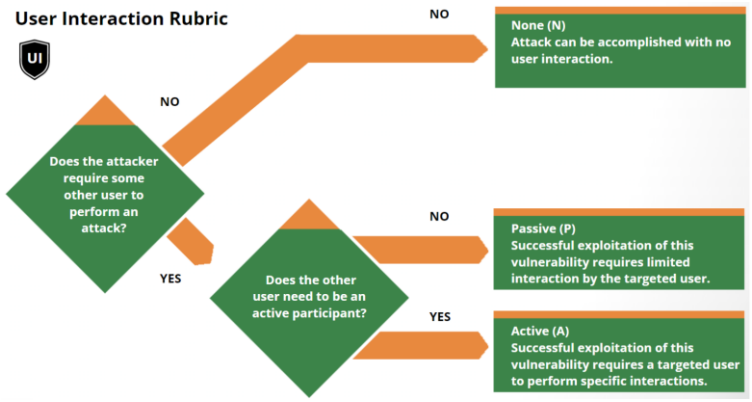
Metrik ini menilai apakah kerentanan bisa dieksploitasi sepenuhnya oleh penyerang saja, atau perlu ada keterlibatan pengguna lain (misal, klik tautan berbahaya, jalankan program tertentu). Semakin minim keterlibatan pengguna, semakin tinggi level bahayanya (karena penyerang bisa langsung melancarkan serangan).

Tabel 6 Rubrik skor *User Interaction* (UI)

Metrik	Deskripsi
None (N)	*Attacker* tidak memerlukan akses ke pengaturan atau file kerentanan sistem untuk melakukan serangan. Kerentanan sistem dapat dieksploitasi tanpa interaksi dari *user* mana pun, selain *attacker*.
Passive (P)	Keberhasilan eksploitasi kerentanan ini memerlukan interaksi terbatas oleh pengguna yang ditargetkan dengan sistem yang rentan dan muatan penyerang. Interaksi ini akan dianggap tidak disengaja dan tidak mengharuskan pengguna secara aktif menumbangkan perlindungan yang dibangun dalam sistem yang rentan.
Active (A)	Keberhasilan eksploitasi kerentanan ini memerlukan *user* yang ditargetkan untuk melakukan interaksi yang spesifik dan sadar dengan sistem yang rentan dan muatan penyerang, atau interaksi pengguna akan secara

Metrik	Deskripsi
	aktif menumbangkan mekanisme perlindungan yang akan mengarah pada eksploitasi kerentanan. Contohnya meliputi: mengimpor file ke dalam sistem yang rentan dengan cara tertentu, menempatkan file ke dalam direktori tertentu sebelum mengeksekusi kode.

Sumber : https://www.first.org/cvss/v4.0/specification-document



Sumber : https://www.first.org/cvss/v4.0/user-guide

Gambar 8 Rubrik *User Interaction*

6. *Confidentiality Impact to the Vulnerable System* (VC)

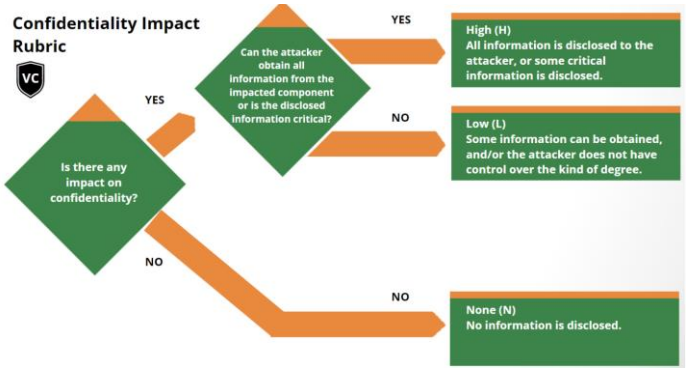
Metrik ini mengukur seberapa parah dampak eksploitasi kerentanan terhadap kerahasiaan informasi yang dikelola untuk sistem yang rentan. Kerahasiaan artinya membatasi akses dan pengungkapan informasi hanya kepada pengguna yang berwenang, serta mencegah akses oleh pihak yang tidak berwenang.

Tabel 7 Rubrik skor *Confidentiality Impact to the Vulnerable System* (VC)

Metrik	Deskripsi
High (H)	Ada total kehilangan kerahasiaan, mengakibatkan semua informasi dalam sistem yang rentan bocor ke *attacker*. Alternatifnya, akses ke beberapa informasi terbatas diperoleh, tetapi informasi yang diungkapkan menyajikan dampak langsung dan serius. Misalnya, *attacker* mencuri kata sandi administrator atau kunci enkripsi pribadi *server web*. Dengan demikian, semua informasi sensitif dalam sistem yang rentan dapat diakses oleh penyerang.
Low (L)	Ada beberapa kehilangan kerahasiaan. Akses ke beberapa informasi terbatas diperoleh, tetapi *attacker* tidak memiliki kontrol atas apa yang diperoleh, atau jumlah atau jenis kehilangan terbatas. Kebocoran informasi tidak menyebabkan dampak langsung dan serius pada

Metrik	Deskripsi
	kerentanan sistem. Dengan demikian, hanya beberapa informasi sensitif dalam sistem yang rentan yang dapat diakses oleh *attacker*. Informasi ini mungkin dibatasi pada informasi yang tidak terlalu penting atau tidak terlalu sensitif.
None (N)	Tidak ada pengungkapan kerahasiaan pada komponen yang terkena dampak.

Sumber : https://www.first.org/cvss/v4.0/specification-document



Sumber : https://www.first.org/cvss/v4.0/user-guide

Gambar 9 Rubrik *Confidentiality Impact*

7. *Confidentiality Impact to the Subsequent System* (SC)

Metrik ini mengukur seberapa parah dampak eksploitasi kerentanan terhadap kerahasiaan informasi yang dikelola sistem jika ada sistem lanjutan yang terdampak. Kerahasiaan artinya membatasi akses dan pengungkapan informasi hanya kepada pengguna yang berwenang, serta mencegah akses oleh pihak yang tidak berwenang.

Tabel 8 Rubrik skor *Confidentiality Impact to the Subsequent System* (SC)

Metrik	Deskripsi
High (H)	Kerahasiaan hilang total, mengakibatkan semua sumber daya dalam sistem selanjutnya dibocorkan kepada penyerang. Alternatifnya, hanya diperoleh akses terhadap beberapa informasi terbatas, namun informasi yang diungkapkan menimbulkan dampak langsung dan serius. Misalnya, penyerang mencuri kata sandi administrator, atau kunci enkripsi pribadi server web.
Low (L)	Ada beberapa hilangnya kerahasiaan. Akses ke beberapa informasi terbatas diperoleh, namun *attacker* tidak memiliki kendali atas informasi apa yang diperoleh, atau jumlah atau jenis kerugiannya terbatas. Keterbukaan

Metrik	Deskripsi
	informasi tersebut tidak menimbulkan kerugian yang serius dan langsung terhadap Sistem Selanjutnya.
Negligible (N)	Tidak ada hilangnya kerahasiaan dalam sistem atau semua dampak kerahasiaan dibatasi pada kerentanan sistem.

Sumber : https://www.first.org/cvss/v4.0/specification-document

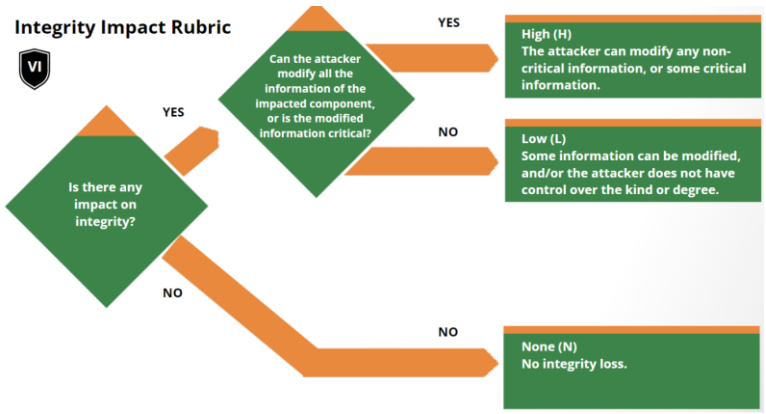
8. *Integrity Impact to the Vulnerable System* (VI)

Metrik ini mengukur seberapa parah dampak eksploitasi kerentanan terhadap kebenaran dan keakuratan data dalam suatu sistem yang rentan. Semakin parah dampak terhadap integritas, semakin tinggi nilainya.

Tabel 9 Rubrik skor *Integrity Impact to the Vulnerable System* (VI)

Metrik	Deskripsi
High (H)	Ada hilangnya integritas total, atau hilangnya perlindungan sepenuhnya dalam suatu sistem yang rentan. Misalnya, *attacker* dapat memodifikasi setiap/semua file yang dilindungi oleh kerenta. Alternatifnya, hanya beberapa file yang dapat dimodifikasi, namun modifikasi berbahaya akan menimbulkan konsekuensi langsung dan serius terhadap sistem rentan. Ada hilangnya integritas total, atau hilangnya perlindungan sepenuhnya. Misalnya, penyerang dapat memodifikasi setiap/semua file yang dilindungi.
Low (L)	Modifikasi data dimungkinkan, namun *attacker* tidak memiliki kendali atas konsekuensi modifikasi, atau jumlah modifikasi terbatas. Modifikasi data tidak mempunyai dampak langsung dan serius terhadap kerentanan sistem.
None (N)	Tidak ada hilangnya integritas dalam kerentanan sistem.

Sumber : https://www.first.org/cvss/v4.0/specification-document



Sumber : https://www.first.org/cvss/v4.0/user-guide

Gambar 10 Rubrik *Integrity Impact*

9. *Integrity Impact to the Subsequent System* (SI)

Metrik ini mengukur seberapa parah dampak eksploitasi kerentanan terhadap kebenaran dan keakuratan data dalam suatu sistem jika ada sistem lanjutan yang terdampak. Semakin parah dampak terhadap integritas, semakin tinggi nilainya.

Tabel 10 Rubrik skor *Integrity Impact to the Subsequent System* (SI)

Metrik	Deskripsi
High (H)	Ada hilangnya integritas total, atau hilangnya perlindungan sepenuhnya pada sistem lanjutan yang berdampak. Misalnya, *attacker* dapat memodifikasi setiap/semua file yang dilindungi oleh sistem. Alternatifnya, hanya beberapa file yang dapat dimodifikasi, namun modifikasi berbahaya akan menimbulkan konsekuensi langsung dan serius pada sistem lanjutan yang terdampak.
Low (L)	Modifikasi data dimungkinkan, namun penyerang tidak memiliki kendali atas konsekuensi modifikasi, atau jumlah modifikasi terbatas. Modifikasi data tersebut tidak mempunyai dampak langsung dan serius terhadap sistem selanjutnya.
None (N)	Tidak ada hilangnya integritas dalam sistem berikutnya atau semua dampak integritas terbatas pada sistem selanjutnya.

Sumber : https://www.first.org/cvss/v4.0/specification-document

10. *Availability Impact to the Vulnerable System* (VA)

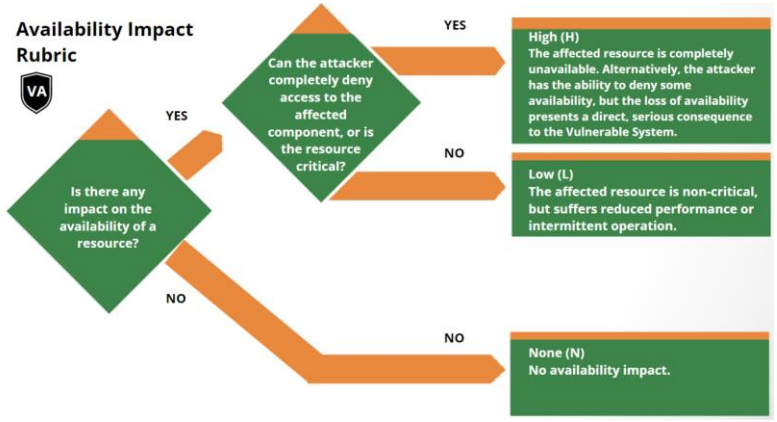
Metrik ini mengukur seberapa parah dampak eksploitasi kerentanan terhadap aksesibilitas sistem yang rentan. Berkaitan dengan apakah sistem masih bisa digunakan dengan normal atau tidak akibat serangan.

Tabel 11 Rubrik skor *Availability Impact to the Vulnerable System* (VA)

Metrik	Deskripsi
High (H)	Terdapat hilangnya ketersediaan total, sehingga *attacker* dapat sepenuhnya menolak akses ke sumber daya di sistem; kerugian ini bisa bertahan (saat *attacker* terus melancarkan serangan) atau terus-menerus (kondisi tetap ada bahkan setelah serangan selesai). Alternatifnya, penyerang mempunyai kemampuan untuk menolak beberapa ketersediaan, namun hilangnya ketersediaan menimbulkan konsekuensi langsung dan serius terhadap sistem (misalnya, *attacker* tidak dapat mengganggu koneksi yang sudah ada, namun dapat mencegah koneksi baru.
Low (L)	Performa berkurang atau ada gangguan pada ketersediaan sumber daya. Sekalipun eksploitasi kerentanan berulang kali dimungkinkan, *attacker* tidak memiliki kemampuan untuk sepenuhnya menolak layanan kepada pengguna yang

Metrik	Deskripsi
	sah. Sumber daya dalam sistem tersedia sebagian sepanjang waktu, atau tersedia sepenuhnya hanya pada waktu tertentu, namun secara keseluruhan tidak ada dampak langsung dan serius terhadap sistem.
None (N)	Tidak ada dampak terhadap ketersediaan dalam sistem.

Sumber : https://www.first.org/cvss/v4.0/specification-document



Sumber : https://www.first.org/cvss/v4.0/user-guide

Gambar 11 Rubrik *Availability Impact*

11. *Availability Impact to the Subsequent System* (SA)

Metrik ini mengukur seberapa parah dampak eksploitasi kerentanan terhadap aksesibilitas sistem jika ada sistem lanjutan yang terdampak. Berkaitan dengan apakah sistem masih bisa digunakan dengan normal atau tidak akibat serangan.

Tabel 12 Rubrik skor *Availability Impact to the Subsequent System* (SA)

Metrik	Deskripsi
High (H)	Terdapat hilangnya ketersediaan total, sehingga *attacker* dapat sepenuhnya menolak akses ke sumber daya di sistem lanjutan; kerugian ini bisa bertahan (saat *attacker* terus melancarkan serangan) atau terus-menerus (kondisi tetap ada bahkan setelah serangan selesai). Alternatifnya, *attacker* mempunyai kemampuan untuk menolak beberapa ketersediaan, namun hilangnya ketersediaan menimbulkan konsekuensi langsung dan serius terhadap sistem (misalnya, *attacker* tidak dapat mengganggu koneksi yang ada, namun dapat mencegah koneksi baru.
Low (L)	Performa berkurang atau ada gangguan pada ketersediaan sumber daya. Sekalipun eksploitasi kerentanan berulang kali dimungkinkan, *attacker* tidak memiliki kemampuan untuk sepenuhnya menolak layanan kepada pengguna yang sah. Sumber daya dalam sistem tersedia sebagian

	sepanjang waktu, atau tersedia sepenuhnya hanya pada waktu tertentu, namun secara keseluruhan tidak ada konsekuensi langsung dan serius terhadap sistem lanjutan.
None (N)	Tidak ada dampak terhadap ketersediaan dalam sistem atau semua dampak ketersediaan terbatas pada sistem lanjutan.

Sumber : https://www.first.org/cvss/v4.0/specification-document

Untuk menilai kerentanan, digunakan tabel skor *security level* atau tingkat keamanan berdasarkan CVSS v4.0 yang dapat diskalakan sehingga menghasilkan *score* seperti tabel 14.

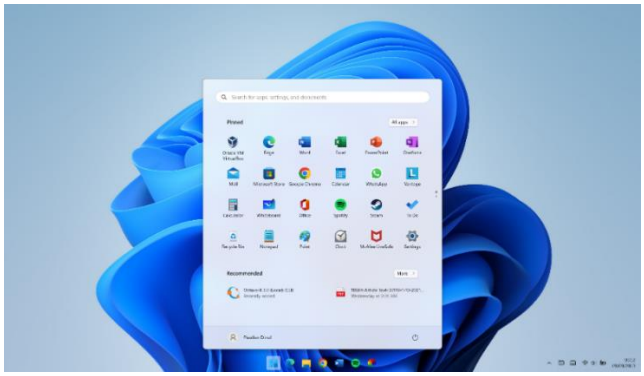
Tabel 13 Skala *rating security level* berdasarkan CVSS v4.0

Rating	***CVSS Score***
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

Sumber : https://www.first.org/cvss/v4.0/specification-document

2.2.7 Sistem Operasi Windows

Berdasarkan website it.telkomuniverity.ac.id, sistem operasi Windows adalah sebuah program komputer yang mengatur semua sumber daya komputer dan menyediakan layanan kepada aplikasi yang berjalan di atasnya. Sistem operasi ini dikembangkan oleh perusahaan Microsoft dan dirilis pada tahun 1985 dengan nama Windows 1.0. Sejak saat itu, sistem operasi Windows terus berkembang dan menjadi salah satu sistem operasi paling populer di dunia. Sistem operasi Windows dirancang untuk berjalan pada berbagai jenis perangkat keras, termasuk desktop, laptop, *server*, dan perangkat *mobile*.



Sumber : Diambil oleh penulis

Gambar 12 Sistem operasi Windows

2.2.8 Sistem Operasi Kali Linux

Berdasarkan website it.telkomuniverity.ac.id , kali Linux adalah sebuah sistem operasi (OS) *open-source* yang digunakan untuk tujuan *hacking* dan pengujian penetrasi pada jaringan komputer. Kali Linux pertama kali dirilis pada tahun 2013 oleh *Offensive Security* dan merupakan turunan dari Debian Linux. OS ini dikembangkan khusus untuk keperluan keamanan jaringan dan telah menjadi standar industri untuk pengujian penetrasi dan forensik digital. Kali Linux dilengkapi dengan berbagai alat *hacking* dan *pentesting*, seperti nmap, metasploit, aircrack-ng, dan banyak lagi. OS ini memiliki fokus pada keamanan dan privasi, serta dapat digunakan sebagai sistem operasi utama atau sebagai OS live pada USB atau CD.

Sumber : Diambil oleh penulis

Gambar 13 Sistem operasi Kali Linux