SKRIPSI

ANALISIS KEAMANAN JARINGAN WLAN SMA NEGERI 11 PANGKEP MENGGUNAKAN METODE *PENETRATION TESTING* DAN *VULNERABILITY ASSESSMENT*

Disusun dan diajukan oleh:

KHAIDIR ALIF

D041 20 1099

PROGRAM STUDI SARJANA TEKNIK ELEKTRO
FAKULTAS TEKNIK
UNIVERSITAS HASANUDDIN
GOWA

2024

LEMBAR PENGESAHAN SKRIPSI

ANALISIS KEAMANAN JARINGAN WLAN SMA NEGERI 11 PANGKEP MENGGUNAKAN METODE *PENETRATION TESTING* DAN *VULNERABILITY ASSESSMENT*

Disusun dan diajukan oleh

Khaidir Alif
D041201099

Telah dipertahankan di hadapan Panitia Ujian yang dibentuk dalam rangka
Penyelesaian Studi Program Sarjana Program Studi Teknik Elektro
Fakultas Teknik Universitas Hasanuddin
Pada tanggal 15 Agustus 2024
Dan dinyatakan telah memenuhi syarat kelulusan

Menyetujui,

Pembimbing Utama,

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

Ketua Program Studi,

Dr.Eng. Ir. Dewiani, MT.
NIP. 196910261994122001

PERNYATAAN KEASLIAN

Yang bertanda tangan di bawah ini:

Nama : Khaidir Alif

NIM : D041201099

Program Studi : Teknik Elektro

Jenjang : S1

Menyatakan dengan ini bahwa karya tulisan saya berjudul

ANALISIS KEAMANAN JARINGAN WLAN SMA NEGERI 11 PANGKEP MENGGUNAKAN METODE *PENETRATION TESTING* DAN *VULNERABILITY ASSESSMENT*

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 dipublikasikan 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, 15 Agustus 2024

Yang Menyatakan

Khaidir Alif

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 Keamanan Jaringan WLAN SMA Negeri 11 Pangkep Menggunakan Metode *Penetration Testing* dan *Vulnerability Assessment***" sebagai salah satu persyaratan dalam menyelesaikan Studi Kesarjanaan (S1) di Departemen Teknik Elektro, Fakultas Teknik Universitas Hasanuddin. Sholawat 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 Syamsir dan ibunda penulis Sumarni yang senantiasa memberikan kasih sayang, dorongan doa, nasihat, motivasi, dan dukungan yang tiada hentinya kepada penulis. Adik penulis, Muh. Taufik Nurhidayat dan Putri Amelia Tul Janna, 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 yang telah menjadi meluangkan waktu, tenaga, dan pikiran untuk membimbing dan memberikan arahan yang sangat berarti dalam penulisan skripsi ini.
3. Bapak Prof. Dr. Ir. H. Andani Achmad, M.T. dan Ibu Dr.Eng.Ir. Dewiani, M.T., IPM 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. Bapak Hajir dan Bapak Surya selaku pembimbing lapangan yang senantiasa meluangkan waktunya untuk membantu penelitian penulis.
7. Aliyya Mutmainnah Indra Prayitno yang telah membantu dan membersamai penulis selama perkuliahan dan sangat membantu penulis menyelesaikan skripsi ini.
8. Keluarga besar "PROCEZ20R" yang telah menemani penulis dari hari pertama hingga hari ini.
9. Seluruh pihak yang telah membantu dan mendukung penulis dalam pengerjaan tugas akhir ini, Terima Kasih.

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, 13 Agustus 2024

Penulis

ABSTRAK

KHAIDIR ALIF. *Analisis Keamanan Jaringan WLAN SMA Negeri 11 Pangkep Menggunakan Metode Penetration Testing dan Vulnerability Assessment.* (dibimbing oleh Wardi)

Keamanan jaringan *wireless* lebih rentan dari jaringan yang menggunakan kabel sehingga masalah keamanan perlu diperhatikan, apalagi di dalam sebuah korporasi atau sebuah lembaga yang peduli dengan keamanan data. SMA Negeri 11 Pangkep merupakan salah satu instansi yang bergerak di bidang pendidikan yang menjadikan *Wireless* LAN (WLAN) sebagai salah satu fasilitas penunjang dalam proses pembelajaran dan administrasi. Keamanan jaringan yang kuat dapat membantu mencegah akses yang tidak sah, pencurian data, dan pelanggaran privasi. Gangguan jaringan dapat mengganggu proses belajar mengajar, seperti akses ke platform pembelajaran online dan penggunaan perangkat lunak edukasi. Penelitian ini bertujuan untuk mengidentifikasi tingkat keamanan WLAN di SMAN 11 Pangkep dengan menggunakan metode *penetration testing* untuk menganalisis dampak *vulnerability* dan menilai tingkat keparahan dari *vulnerability* tersebut menggunakan *base metric* dari CVSS v4.0. Lima jenis serangan yang diuji, yaitu *brute force attack,* ICMP *flood,* SYN *flood,* UDP *flood,* dan MAC *spoofing*. Hasil *penetration testing* menunjukkan empat dari enam *access point* memiliki *password* yang mudah ditebak dan rentan terhadap serangan *brute force*. Serangan ICMP *flood,* SYN *flood,* dan UDP *flood* mempengaruhi *throughput* WiFi dengan fluktuasi yang sangat signifikan sebelum adanya serangan. Serangan MAC *spoofing* berhasil menemukan tidak adanya MAC *address filtering* sehingga koneksi layanan internet tetap terhubung. Berdasarkan *scoring system* CVSS v4.0, tingkat keparahan dari lima pengujian *penetration testing* yang dilakukan pada WLAN SMAN 11 Pangkep mendapatkan rata-rata skor 7.06 dengan *rating High*. *Rating High* menunjukkan bahwa kerentanan harus diperhatikan dengan serius dan perlu ditangani. Kerentanan ini memiliki dampak yang signifikan terhadap ketersediaan jaringan jika dieksploitasi.

Kata kunci: WLAN, Kerentanan, *Penetration Testing, Vulnerability Assessment.*

ABSTRACT

KHAIDIR ALIF. *Analysis of WLAN Network Security at SMA Negeri 11 Pangkep Using Penetration Testing and Vulnerability Assessment Methods.* (supervised by Wardi)

Network security *wireless* more vulnerable than networks that use cables, so security issues need to be considered, especially in a corporation or institution that cares about data security. SMA Negeri 11 Pangkep is one of the institutions that operates in the field of education which makes it possible *Wireless* LAN (WLAN) as a supporting facility in the learning and administration process. Strong network security can help prevent unauthorized access, data theft, and privacy violations. Network disruptions can disrupt teaching and learning processes, such as access to online learning platforms and use of educational software. This research aims to identify the level of WLAN security at SMAN 11 Pangkep using the method *penetration testing* to analyze impacts *vulnerability* and assess the severity of *vulnerability* it uses *base metric* from CVSS v4.0. Five types of attacks were tested, viz *brute force attack,* ICMP *flood,* SYN *flood,* UDP *flood,* and MAC *spoofing*. Results *penetration testing* shows four out of six *access point* own *password* which is easy to predict and vulnerable to attack *brute force*. ICMP attacks *flood,* SYN *flood,* and UDP *flood* influence *throughput* WiFi with very significant fluctuations before the attack. MAC Attack *spoofing* managed to find the absence of MAC *address filtering* so that the internet service connection remains connected. Based on the CVSS v4.0 scoring system, the severity of the five penetration tests conducted on the WLAN of SMAN 11 Pangkep received an average score of 7.06 with a High rating. *Rating High* indicates that vulnerabilities should be taken seriously and need to be addressed. This vulnerability has a significant impact on network availability if exploited.

Keywords: WLAN, Vulnerability, *Penetration Testing, Vulnerability Assessment.*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR SINGKATAN

Singkatan	Keterangan
AP	*Access Point*
BSSID	*Basic Service Set Identifier*
CVSS	*Common Vulnerability Scoring System*
ESSID	*Extended Service Set Identifier*
ICMP	*Internet Control Messege Protocol*
IP	*Internet Protocol*
MAC	*Media Access Protocol*
PSK	*Pre-Shared Key*
SYN-ACK	*Synchronize-Acknowledge*
UDP	*User Datagram Protocol*
WiFi	*Wireless Fidelity*
WLAN	*Wireless Local Area Network*
WPA	Wi-Fi *Protected Access*

DAFTAR LAMPIRAN

BAB I
PENDAHULUAN

1.1 Latar Belakang

Jaringan komputer merupakan salah satu teknologi yang berkembang di bidang transmisi data. Jaringan komputer memiliki 2 jenis media transmisi data, yaitu kabel dan nirkabel atau *wireless*. Jaringan nirkabel memanfaatkan gelombang radio sebagai media transmisi data, sehingga jaringan nirkabel tidak memerlukan kabel untuk bisa saling terhubung antara perangkat yang satu dengan perangkat yang lainnya. Jaringan nirkabel atau *wireless* yang saat ini sangat sering digunakan bahkan dikembangkan karena jaringan nirkabel bisa digunakan pada setiap aspek skenario (Saraun et al., 2021).

Jaringan *wireless* lebih nyaman digunakan karena dapat menjangkau area yang luas sehingga memungkinkan *user* dapat berpindah tempat, tetapi sangat sedikit yang memperhatikan keamanan komunikasi data pada jaringan *wireless* tersebut mengingat dari segi keamanan bahwa jaringan nirkabel lebih rentan dari jaringan yang menggunakan kabel (Dayan et al., 2023). Salah satu penyebabnya adalah karena mudahnya pengguna umum terhubung dengan jaringan WLAN sehingga tentunya masalah keamanan perlu diperhatikan, apalagi didalam sebuah korporasi atau sebuah lembaga yang peduli dengan keamanan data (Saraun et al., 2021). Jaringan *wireless* yang menggunakan gelombang radio sebagai media transmisi sehingga jaringan akan lebih mudah dimasuki oleh penyusup.

SMA Negeri 11 Pangkep merupakan salah satu instansi yang bergerak di bidang pendidikan yang menjadikan *Wireless* LAN (WLAN) sebagai salah satu fasilitas penunjang dalam proses pembelajaran dan administrasi. Jaringan sekolah menyimpan banyak data sensitif, seperti data siswa, keuangan, dan informasi pribadi pegawai dan staf. Keamanan jaringan yang kuat dapat membantu mencegah akses yang tidak sah, pencurian data, dan pelanggaran privasi (Kamajaya et al., 2020). Gangguan jaringan dapat mengganggu proses belajar mengajar, seperti akses ke platform pembelajaran *online* dan penggunaan perangkat lunak edukasi. Keamanan jaringan yang baik dapat membantu memastikan kelancaran dan stabilitas jaringan, sehingga proses belajar mengajar tidak terhambat.

SMAN 11 Pangkep saat ini menggunakan jaringan yang terdiri dari 6 perangkat *wireless* LAN yang mencakup berbagai ruangan di SMAN 11 Pangkep dengan menggunakan keamanan WPA2-PSK. Untuk mengetahui bagaimana kualitas keamanan jaringan di SMA Negeri 11 Pangkep maka perlu dilakukan pengujian terhadap sistem keamanan yang ada pada jaringan tersebut. Metode yang dapat digunakan untuk pengujian sistem keamanan jaringan *Wireless* LAN (WLAN) yaitu dengan metode *penetration testing* yang dilakukan pada jaringan instansi terkait untuk menemukan kelemahan yang ada pada jaringan tersebut (Martias et al., 2020).

Penetration testing adalah serangan jaringan yang disimulasikan pada jaringan untuk menemukan kerentanan, ancaman, dan resiko dalam jaringan yang dapat digunakan penyerang. Suatu pendekatan untuk menguji dan mengevaluasi tingkat keamanan jaringan dengan melakukan percobaan serangan secara sistematis dan beretika. (Haeruddin & Kurniadi, 2021). Serangan jaringan yang akan disimulasikan adalah *Cracking the Encryption, Denial of Service,* dan *Bypassing MAC Authentication.*

Cracking The Encryption adalah upaya untuk mendapatkan akses tidak sah ke jaringan nirkabel dengan memecahkan kata sandi yang digunakan untuk mengenkripsi data yang ditransmisikan. Serangan *Cracking the encryption* merupakan serangan yang bertujuan untuk mendapatkan kata sandi dari *access point* yang digunakan, sehingga bisa mengakses jaringan LAN secara ilegal (Galang Saputra et al., 2023).

Denial of Service menjadi salah satu jenis serangan *cyber* teratas dan cukup banyak digunakan oleh penyerang dengan tujuan untuk melumpuhkan targetnya. Serangan DoS menggunakan volume dan intensitas tertentu yang menyebabkan target menjadi kehabisan *resource* bahkan *down* ketika menangani permintaan layanan dari pengguna, sehingga membuat pengguna layanan yang sah kesulitan atau bahkan tidak dapat mengakses layanan. DoS memiliki beberapa jenis tipe serangan, diantaranya SYN-*Flooding*, UDP-*Flooding*, ICMP-*Flooding* (Haris et al., 2022).

Bypassing MAC Authentication adalah teknik yang digunakan penyerang untuk mendapatkan akses ke jaringan walaupun perangkat mereka tidak terdaftar

dan memiliki alamat MAC yang diizinkan. Autentikasi MAC adalah salah satu cara untuk mengontrol akses ke jaringan nirkabel dengan membatasi akses berdasarkan alamat MAC (alamat fisik unik yang terkait dengan perangkat jaringan) (Haeruddin & Kurniadi, 2021).

Oleh karena itu, berdasarkan permasalahan tersebut penulis tertarik untuk mengangkat judul penelitian **"Analisis Keamanan Jaringan WLAN SMA Negeri 11 Pangkep Menggunakan Metode *Penetration Testing* dan *Vulnerability Assessment*".**

1.2 Rumusan Masalah

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

1. Bagaimana dampak serangan *Cracking the Encryption, Denial of Service,* dan *Bypassing MAC Authentication* terhadap jaringan WLAN SMA Negeri 11 Pangkep?
2. Bagaimana tingkat keamanan jaringan WLAN SMA Negeri 11 Pangkep terhadap serangan *Cracking the Encryption, Denial of Service,* dan *Bypassing MAC Authentication* sesuai dengan *Vulnerability Assessment*?

1.3 Tujuan Penelitian

Tujuan yang ingin dicapai dalam penelitian ini adalah:

1. Menganalisis dampak serangan *Cracking the Encryption, Denial of Service,* dan *Bypassing MAC Authentication* terhadap jaringan WLAN SMA Negeri 11 Pangkep.
2. Mengidentifikasi tingkat keamanan jaringan WLAN SMA Negeri 11 Pangkep terhadap serangan *Cracking the Encryption, Denial of Service,* dan *Bypassing MAC Authentication* sesuai dengan *Vulnerability Assessment.*

1.4 Manfaat Penelitian

Manfaat dari penelitian ini meliputi:

1. Manfaat secara teoritis, penelitian ini mampu meningkatkan pemahaman tentang kerentanan jaringan WLAN di sekolah dan memberikan wawasan untuk menganalisis kerentanan jaringan WLAN.
2. Manfaat secara praktis, penelitian ini mengidentifikasi kerentanan yang ada pada jaringan WLAN SMA Negeri 11 Pangkep sehingga menjadi panduan dalam memahami dan mengatasi potensi serangan *Cracking the Encryption, Denial of Service,* dan *Bypassing MAC Authentication.*

1.5 Ruang Lingkup

Adapun batasan masalah pada penelitian ini:

1. Penelitian ini akan berfokus pada evaluasi kerentanan jaringan WLAN dan tidak membahas pencegahan atau perlindungan terhadap serangan tersebut.
2. IP dan MAC *address* dari *victim* dan *attacker* telah diketahui sebelum melakukan pengujian.
3. Jenis serangan yang akan dievaluasi dibatasi pada serangan *Brute Force Attack,* ICMP *flood,* SYN *flood,* UDP *flood,* dan MAC *spoofing.*
4. Sisi *Attacker* menggunakan sistem operasi Kali Linux dan sisi *Victim* menggunakan sistem operasi Windows.
5. Jenis *assessment* yang digunakan untuk menilai kerentanan adalah *Base Metric* dari *Forum of Incident Response and Security Teams* (FIRST) CVSS v4.0

BAB II
TINJAUAN PUSTAKA

2.1 Penelitian Terdahulu

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 lalu lintas 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: Analisis *Vulnerability* Jaringan WLAN Departemen Teknik Elektro FT-UH Terhadap Serangan *Denial Of Service* (DoS) Dan *Man In The Middle* (MITM) Tahun: 2024 Peneliti: Muh. Fhadlan Dinul Haq	Penelitian ini menguji keamanan jaringan *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 serangan DoS dan MITM. Serangan *Denial of Service* (DoS) dapat menciptakan beban pada *throughput* Wi-Fi dan beban CPU sedangkan serangan MAC *Spoofing* berhasil mengubah alamat MAC pada perangkat *attacker*. Berdasarkan CVSSv4.0 diketahui bahwa tingkat keamanan WLAN terhadap serangan *Denial of Service* (DoS) dan *Man In The Middle* (MITM) kampus dari *base metric* menghasilkan *score* 6.9 atau secara kualitatif berada di kategori *Medium.*
JUDUL: Analisis Keamanan Jaringan WPA2-PSK Menggunakan Metode *Penetration Testing* (Studi Kasus: TP-Link Archer A6) Tahun: 2021	Penelitian ini mengkaji sistem keamanan jaringan WLAN ditempat umum, *hotspot,* dan kafe. Pengujian kali ini ditujukan pada sebuah *router,* yaitu TP-Link Archer A6. Metode yang digunakan dalam penelitian ini adalah *penetration testing.* Pengujian dilakukan dengan tiga tahapan, yaitu *cracking the encryption, bypassing MAC address authentication,* dan

Deskripsi Jurnal	Pembahasan
Penulis: Haeruddin, Arif Kurniadi	*attacking the infrastructure.* Hasil penelitian didapatkan adalah keamanan jaringan dengan menggunakan metode pengujian *Penetration Testing* pada TP-Link Archer A6 masih banyak kelemahan sistem, dikarenakan masih menggunakan konfigurasi *default* dari vendor. Oleh karena itu diperlukan peningkatan keamanan pada TP-*Link Archer* A6 dengan mengkonfigurasi lebih aman dan tidak menggunakan konfigurasi *default router*. Hasil penelitian menunjukan bahwa dari tiga serangan yang dilakukan, hanya satu serangan yang memiliki status gagal, yaitu tipe serangan *Bypassing MAC address Authentication*.
JUDUL: Analisa Keamanan Jaringan Nirkabel IEEE 802.11 pada Kantor Dinas Pendidikan Kabupaten Minahasa Tahun: 2021 Penulis: Astri Saraun, Arie S.M. Lumenta, Daniel Febrian Sengkey	Penelitian ini menganalisis celah keamanan dalam jaringan *wireless* pada Kantor Dinas Pendidikan Kabupaten Minahasa dengan menggunakan metode *penetration testing* dengan mensimulasikan serangan *cracking the encryption, denial of service* dan *ARP Poisoning*. Hasil yang didapatkan adalah sistem keamanan jaringan yang diterapkan oleh Kantor Dinas Pendidikan Kabupaten Minahasa masih belum sepenuhnya dikatakan aman karena serangan *cracking the encryption* yang disimulasikan berstatus berhasil. Serangan *cracking the encryption* yang dilakukan menghasilkan kata sandi yang ada pada *access point* bisa ditemukan atau dipecahkan dengan teknik *brute force* dengan menggunakan *tools crunch, airmon-ng, airodump-ng, aireplay-ng, aircrack-ng* dan *wireshark*. Serangan *denial of service* yang di simulasikan berstatus berhasil. Serangan *denial of service* yang dilakukan menghasilkan pengguna dan *access point* terputus sehingga pengguna tidak bisa terkoneksi dengan *access point* dengan menggunakan *tools airmon-ng, airodump-ng dan aireplay-ng.* Serangan ARP *Poisoning* berstatus berhasil. serangan ARP *poisoning* yang dilakukan menghasilkan informasi - informasi penting pengguna bisa diketahui dengan menggunakan tools *ettercap* dan *wireshark*.

Deskripsi Jurnal	Pembahasan
JUDUL: Analisis Keamanan Jaringan *Wireless* menggunakan Metode *Penetration Testing Execution Standard* (PTES) Tahun: 2023 Penulis: Satria Galang Saputra, Bita Parga Zen, Abdurahman	Penelitian ini menguji keamanan jaringan *wireless* pada Kantor Balai Desa Kalisapu Kecamatan Slawi Kabupaten Tegal yang merupakan tempat layanan publik dengan menggunakan metode *Penetration Testing Execution Standard.* Uji simulasi serangan yang dilakukan yaitu *cacking the encryption, bypassing MAC authentication,* dan ARP *spoofing.* Hasil yang didapatkan berdasarkan tahap uji penetrasi yang dilakukan, sistem keamanan jaringan *wireless* di Kantor Balai Desa Kalisapu cukup aman dengan sudah menerapkan sistem enkripsi WPA2-PSK akan tetapi masih rentan terhadap serangan, berdasarkan uji serangan *cracking the encryption* keamanan tersebut masih bisa diekspolitasi dengan teknik *brute force* untuk mencari kata sandi berdasarkan paket *handshake* dan *wordlist* yang telah dibuat. dalam tahap uji serangan yang lainnya menggunakan teknik *Bypassing MAC Address* serta *ARP Spoofing* pengujian ini berstatus berhasil selama lima kali pengujian.
JUDUL: Analisis Keamanan Jaringan Pada *Wireless Local Area Network* Terhadap Serangan *Brute Force* Menggunakan Metode *Penetration Testing* Tahun: 2023 Penulis: Rozi Dayan, Yusuf Muhyidin, Dayan Singasatia	Penelitian ini menguji keamanan WLAN yang terdapat pada Politeknik Bhakti Asih. Metode yang digunakan adalah *penetration testing* dengan melakukan simulasi serangan *brute force*. Adapun yang diuji adalah perangkat yang menggunakan keamanan WPA2-PSK. Hasil pengujian menunjukkan bahwa titik akses pertama, yaitu titik akses di ruangan yayasan, memiliki kata sandi yang mudah ditebak dan rentan terhadap serangan. Oleh karena itu, perlu adanya penanganan yang lebih baik dan penggunaan frase sandi yang lebih kuat.

2.2 Jaringan Komputer

Jaringan komputer adalah sebuah sistem yang terdiri atas komputer-komputer yang didesain untuk dapat berbagi sumber daya (*printer*, CPU), berkomunikasi (surel, pesan instan), dan dapat mengakses informasi (peramban *web*). Tujuan dari jaringan komputer adalah agar dapat mencapai tujuannya, setiap bagian dari jaringan komputer dapat meminta dan memberikan layanan (*service*). Pihak yang meminta/menerima layanan disebut klien (*client*) dan yang memberikan/mengirim

layanan disebut peladen (*server*). Desain ini disebut dengan sistem *client-server*, dan digunakan pada hampir seluruh aplikasi jaringan komputer.

Berdasarkan jangkauan geografis dibedakan menjadi:

1. Jaringan LAN

   Jaringan komputer yang jaringannya hanya mencakup wilayah kecil; seperti jaringan komputer kampus, gedung, kantor, dalam rumah, sekolah atau yang lebih kecil. Saat ini, kebanyakan LAN berbasis pada teknologi IEEE 802.3 *Ethernet* menggunakan perangkat *switch*, yang mempunyai kecepatan transfer data 10, 100, atau 1000 Mbit/s. Selain teknologi *Ethernet*, saat ini teknologi 802.11b (atau biasa disebut Wi-fi) juga sering digunakan untuk membentuk LAN. Tempat-tempat yang menyediakan koneksi LAN dengan teknologi Wi-fi biasa disebut *hotspot*.

   Pada sebuah LAN, setiap node atau komputer mempunyai daya komputasi sendiri, berbeda dengan konsep *dump* terminal. Setiap komputer juga dapat mengakses sumber daya yang ada di LAN sesuai dengan hak akses yang telah diatur. Sumber daya tersebut dapat berupa data atau perangkat seperti *printer.* Pada LAN, seorang pengguna juga dapat berkomunikasi dengan pengguna yang lain dengan menggunakan aplikasi yang sesuai.

2. Jaringan WAN

   WAN adalah singkatan dari istilah teknologi informasi dalam bahasa Inggris: *Wide Area Network* merupakan jaringan komputer yang mencakup area yang besar sebagai contoh yaitu jaringan komputer antar wilayah, kota atau bahkan negara, atau dapat didefinisikan juga sebagai jaringan komputer yang membutuhkan *router* dan saluran komunikasi publik. WAN digunakan untuk menghubungkan jaringan lokal yang satu dengan jaringan lokal yang lain, sehingga pengguna atau komputer di lokasi yang satu dapat berkomunikasi dengan pengguna dan komputer di lokasi yang lain.

3. Jaringan MAN

   Metropolitan area network atau disingkat dengan MAN. Suatu jaringan dalam suatu kota dengan transfer data berkecepatan tinggi, yang menghubungkan berbagai lokasi seperti kampus, perkantoran,

pemerintahan, dan sebagainya. Jaringan MAN adalah gabungan dari beberapa LAN. Jangkauan dari MAN ini antar 10 hingga 50 km, MAN ini merupakan jaringan yang tepat untuk membangun jaringan antar kantor-kantor dalam satu kota antara pabrik/instansi dan kantor pusat yang berada dalam jangkauannya (Jafar Noor Yudianto, 2014).

2.3 *Wireless Local Area Network (*WLAN*)*

Pengertian *Wireless* LAN atau kadang disingkat dengan WLAN adalah sebuah sistem komunikasi data yang fleksibel yang dapat diaplikasikan sebagai ekstensi ataupun sebagai alternatif pengganti untuk jaringan LAN kabel. *Wireless* LAN menggunakan teknologi frekuensi radio, mengirim dan menerima data melalui media udara, dengan meminimalisasi kebutuhan akan sambungan kabel. Dengan begitu, *wireless* LAN telah dapat mengkombinasikan antara konektivitas data dengan mobilitas *user. Wireless* LAN adalah sebuah alternatif dimana untuk alternatif LAN kabel sulit atau tidak mungkin dibangun. Tempat-tempat seperti bangunan tua yang dilindungi atau ruang-ruang kelas (Wongkar et al., 2015).

Jaringan ini lebih mudah dan ekonomis untuk dibangun karena tanpa harus melakukan perancangan jalur-jalur kabel dan tidak perlu kabel sebagai perangkat. WLAN saat ini menggunakan dua frekuensi yaitu 2,4 GHz dan 5 GHz. Pada frekuensi 2,4 GHz, sering terjadi interferensi dikarenakan frekuensi ini juga digunakan oleh Bluetooth. Sedangkan untuk frekuensi 5 GHz jarang terjadi interferensi tetapi memiliki daya pancar lebih rendah (Jatmiko et al., 2021).

2.4 Keamanan Jaringan *Wireless*

Kerentanan jaringan WLAN terhadap keamanan data, informasi, dan ketersediaan layanan menjadi topik yang tidak henti-hentinya menjadi sorotan dan perbincangan. Untuk itu, dikemukakan suatu teori bahwa suatu jaringan komputer dikatakan aman apabila:

1. *Privacy & Confidentiality Privacy* merupakan suatu mekanisme yang yang dilakukan untuk melindungi suatu informasi dari pengguna jaringan yang tidak memiliki hak, sedangkan *confidentiality* lebih mengarah kepada

tujuan dari informasi yang diberikan dan hanya boleh untuk tujuan tersebut saja.

2. *Integrity* merupakan aspek yang mengutamakan akses informasi yang ditujukan untuk pengguna tertentu, dimana integritas dari informasi tersebut masih terjaga.
3. *Authentication.* Aspek ini mengutamakan validitas dari user yang melakukan akses terhadap suatu data, informasi, atau layanan dari suatu institusi.
4. *Availability* merupakan aspek yang berhubungan dengan ketersediaan data, informasi, atau layanan, ketika data, informasi atau layanan tersebut diperlukan.
5. *Access Control*, dimana aspek ini berhubungan dengan klasifikasi pengguna dan cara pengaksesan informasi yang dilakukan oleh pengguna.
6. *Non-Repudiation* merupakan aspek yang berkaitan dengan pencatatan pengguna, agar pengguna data, informasi atau layanan tidak dapat menyangkal bahwa telah melakukan akses terhadap data, informasi, ataupun layanan yang tersedia (Sari et al., 2017).

2.4.1 *Wired Equivalent Privacy* (WEP) *Encryption*

WEP adalah upaya awal untuk melindungi jaringan wireless dari pelanggaran keamanan, tetapi seiring dengan kemajuan teknologi, menjadi jelas bahwa informasi yang dienkripsi dengan WEP rentan terhadap serangan. WEP adalah komponen dari standar IEEE 802.11 WLAN. Tujuan utamanya adalah untuk memastikan kerahasiaan data pada jaringan *wireless* pada tingkat yang setara dengan LAN kabel, yang dapat menggunakan keamanan fisik untuk menghentikan akses tidak sah ke jaringan. Dalam WLAN, pengguna atau *attacker* dapat mengakses jaringan tanpa terhubung secara fisik ke LAN. Oleh karena itu, WEP menggunakan mekanisme *encryption* pada lapisan data link untuk meminimalkan akses tidak sah ke WLAN. Hal ini dilakukan dengan mengenkripsi data dengan algoritma *encryption Rivest Cipher* 4 (RC4) simetris, yang merupakan mekanisme kriptografi untuk mempertahankan sistem dari *threat* (Fahrina, 2023).

2.4.2 *Wi-Fi Protected Access* (WPA) *Encryption*

Wi-Fi Protected Access (WPA) adalah protokol keamanan yang ditentukan oleh standar 802.11i. WPA memiliki keamanan *encryption* data yang lebih baik daripada WEP karena pesan melewati *Message Integrity Check* (MIC) menggunakan *Temporal Key Integrity Protocol* (TKIP), yang memanfaatkan *encryption stream cipher* RC4 dengan 128-bit *key* dan MIC 64-bit untuk menyediakan *encryption* yang kuat dengan otentikasi. WPA adalah contoh bagaimana 802.11i menyediakan *encryption* yang lebih kuat dan mengaktifkan *pre-shared key* (PSK) atau otentikasi EAP. WPA menggunakan TKIP untuk data *encryption*, yang menutupi kelemahan WEP dengan memasukkan fungsi pencampuran per-paket, MIC, perluasan IV dan mekanisme *re-keying* (Fahrina, 2023).

2.4.3 WPA2 *Encryption*

Wi-Fi *Protected Access* 2 (WPA2) adalah protokol keamanan yang digunakan untuk melindungi jaringan *wireless*. WPA2 menggantikan WPA pada tahun 2006. Ini kompatibel dengan standar 802.11i dan mendukung banyak fitur keamanan yang tidak dimiliki WPA. WPA2 memperkenalkan penggunaan algoritma *encryption* AES yang memberikan perlindungan data dan kontrol akses jaringan yang lebih kuat daripada WPA. Selain itu, ini memberikan tingkat keamanan yang tinggi untuk koneksi Wi-Fi sehingga hanya pengguna yang berwenang yang dapat mengakses jaringan (Fahrina, 2023).

2.4.4 WPA3 *Encryption*

Wi-Fi *Protected Access* 3 (WPA3) diumumkan oleh Wi-Fi Alliance pada Januari 2018 sebagai implementasi lanjutan dari WPA2 yang menyediakan protokol perintis. WPA3 menyediakan fitur mutakhir untuk menyederhanakan keamanan Wi-Fi dan menyediakan kemampuan yang diperlukan untuk mendukung penyebaran jaringan yang berbeda mulai dari jaringan perusahaan hingga jaringan rumah. Ini juga memastikan konsistensi kriptografi menggunakan algoritma *encryption* seperti AES dan TKIP untuk mempertahankan sistem dari serangan jaringan. Selain itu, juga memberikan ketahanan jaringan melalui *Protected*

Management Frames (PMF) yang memberikan perlindungan tingkat tinggi terhadap serangan penyadapan dan penempaan (Fahrina, 2023).

2.5 *Netwrok-level Attack Techniques*

Serangan jaringan merujuk pada berbagai tindakan yang dilakukan oleh penyerang untuk mencapai tujuan tertentu yang merugikan pada suatu jaringan komputer atau sistem. Tujuan dari serangan jaringan bisa bermacam-macam, mulai dari mencuri data rahasia hingga merusak atau mengganggu operasi sistem atau jaringan. Serangan jaringan dapat dilakukan dengan menggunakan berbagai teknik dan alat, dan bisa menyasar berbagai lapisan atau komponen jaringan, termasuk perangkat keras (seperti *router* atau *switch*), perangkat lunak (seperti sistem operasi atau aplikasi), atau protokol jaringan. Berikut jenis serangan pada tingkat jaringan:

a. *Denial of Service* (DoS)

Serangan *Denial of Service* (DoS) adalah serangan yang mengakibatkan setiap korbannya akan berhenti merespon atau berlaku tidak lazim. Contoh serangan klasik DoS adalah *Ping of Death dan Syn Flood* yang untungnya sudah hampir tidak dapat dijumpai pada saat sekarang. Biasanya serangan DoS menyerang celah yang terdapat pada layanan sistem atau pada protokol jaringan kerja untuk menyebabkan layanan tidak dapat digunakan. Teknik yang lainnya adalah menyebabkan sistem korban tersedak dikarenakan banyaknya paket yang diterima yang harus diproses melebihi kemampuan dari sistem itu sendiri atau menyebabkan terjadinya *bottleneck* pada *bandwidth* yang dipakai oleh sistem. Serangan *Distributed Denial of Service* (DDoS) merupakan tipe serangan yang lebih terorganisasi. Jenis serangan ini biasanya membutuhkan persiapan dan juga taktik untuk dapat menjatuhkan korbannya dengan cepat dan sebelumnya biasanya para penyerang akan mencari sistem kecil yang dapat dikuasai. Setelah mendapat banyak sistem kecil, penyerang akan menyerang sistem yang besar dengan menjalankan ribuan bahkan puluhan ribu sistem kecil secara bersamaan untuk menjatuhkan sebuah sistem besar (Wajong, 2012).

b. Man In The Middle

Serangan *man-in-the-middle* adalah salah satu bentuk serangan tidak langsung. Mode serangan ini adalah untuk menempatkan komputer yang

dikendalikan penyusup antara dua komputer yang saling berkomunikasi yang terhubung ke jaringan melalui berbagai cara teknis. Komputer ini dapat mencegat serta mengutak-atik data komunikasi tanpa pihak komputer *host* dan komputer *client* menyadarinya. Ketika *host* A dan *host* B berkomunikasi, infomasi akan dteruskan oleh *host* C yang berperan sebagai perantara. Dengan cara ini, *host* C dapat menguping dan mengutak-atik informasi dari proses komunikasi tersebut dan mencapai tujuannya dengan mengirimkan informasi palsu ke salah satu *host* (Pinontoan, 2024).

c. *Viruses*

Salah satu definisi dari program virus adalah menyisipkan dirinya kepada objek lain seperti *file executable* dan beberapa jenis dokumen yang banyak dipakai orang. Selain kemampuan untuk mereplikasi dirinya sendiri, virus dapat menyimpan dan menjalankan sebuah tugas spesifik. Tugas tersebut bisa bersifat menghancurkan atau sekadar menampilkan sesuatu ke layar monitor korban dan bisa saja bertugas untuk mencari suatu jenis *file* untuk dikirimkan secara acak ke internet bahkan dapat melakukan format pada *hard disk* korban.

Virus yang tersebar di internet dan belum dikenali tidak akan dapat ditangkap oleh program antivirus ataupun semacamnya, sehingga apabila korban telah terjangkit, tetap tidak mengetahuinya. Perangkat lunak antivirus biasanya mengenali virus atau calon virus melalui tanda yang spesifik yang terdapat pada bagian inti virus itu sendiri. Beberapa virus menggunakan teknik *polymorphic* agar luput terdeteksi oleh antivirus. Kebiasaan virus *polymorphic* adalah merubah dirinya pada setiap infeksi yang terjadi yang menyebabkan pendeteksian menjadi jauh lebih sulit. Praktisnya setiap *platform* komputer mempunyai virus masing-masing dan ada beberapa virus yang mempunyai kemampuan menjangkiti beberapa platform yang berbeda (*multi-platform*). Virus *multi-platform* biasanya menyerang *executable* ataupun dokumen pada Windows dikarenakan kepopuleran oleh sistem operasi Microsoft Windows dan Microsoft Office sehingga banyak ditemukan virus yang bertujuan untuk menghancurkan kerajaan Microsoft Corp (Wajong, 2012).

d. Scanning

Scanning adalah metode bagaimana caranya mendapatkan informasi sebanyak-banyaknya dari IP/*Network* korban. Biasanya *scanning* dijalankan secara otomatis mengingat *scanning* pada *multiple host* sangat menyita waktu. *Hackers* biasanya mengumpulkan informasi dari hasil *scanning* ini. Dengan mengumpulkan informasi yang dibutuhkan maka *hackers* dapat menyiapkan serangan yang akan dilancarkannya. Nmap adalah sebuah *network scanner* yang banyak digunakan oleh para profesional di bidang *network security*, walaupun ada *tool* khusus dibuat untuk tujuan *hacking*, tetap belum dapat mengalahkan kepopuleran Nmap. *Nessus* juga merupakan *network scanner* tapi dapat melaporkan apabila terdapat celah keamanan pada target yang diperiksanya. Hacker biasanya menggunakan *Nessus* untuk pengumpulan informasi sebelum benar-benar meluncurkan serangan. Untungnya beberapa *scanner* meninggalkan jejak unik yang memungkinkan para *system* administrator untuk mengetahui bahwa sistem mereka telah di-*scanning* sehingga mereka bisa segera membaca artikel terbaru yang berhubungan dengan informasi log (Wajong, 2012).

e. *Password Cracking*

Brute-force adalah sebuah teknik di mana akan dicobakan semua kemungkinan kata kunci (*password*) untuk bisa ditebak untuk akses ke dalam sebuah sistem. Membongkar kata kunci dengan teknik ini sangat lambat tapi efisien, semua kata kunci dapat ditebak asalkan waktu tersedia. Membalikkan *hash* pada kata kunci merupakan hal yang mustahil, tapi ada beberapa cara untuk membongkar kata kunci tersebut walaupun tingkat keberhasilannya tergantung dari kuat-lemahnya pemilihan kata kunci oleh pengguna. Bila seseorang dapat mengambil data hash yang menyimpan kata kunci, cara yang lumayan efisien adalah menggunakan metode dictionary attack yang dapat dilakukan oleh *utility John The Ripper* (Wajong, 2012).

f. *SQL Injection Attack*

Penyerangan SQL *injection* adalah salah satu jenis serangan yang sangat rentan terjadi, terutama di Indonesia. Para *developer* kadang lupa memberikan keamanan tambahan pada *form login*. Oleh karena itu, perlu dilakukan upaya untuk mengantisipasi serangan tersebut, seperti memberikan *filter* dari *source*

code untuk *query* dan menggunakan verifikasi captca. Biasanya para peretas mencari letak *form login* dan mulai memasukan sintax SQL *Injection* yang dengan secara paksa login tanpa harus mengetahui *username* dan *password*. Pada dasarnya, serangan SQL *Injection* dilakukan melalui *form login* admin dengan melakukan injeksi menggunakan *software* khusus atau dengan cara paksa (penetrasi). *Hacker* akan mencoba untuk memasukkan *username* dan *password* khusus yang mengandung kolaborasi antara angka dan huruf dengan panjang karakter yang ditentukan. Seorang penyerang biasanya akan mencoba membajak *field login* yang tidak terlindungi untuk memperoleh akses *database*. Oleh karena itu, sangat penting untuk melindungi *website* dari serangan SQL *Injection* dengan menggunakan teknik-teknik yang efektif dalam pengamanan *website* (Ferdianto, 2023).

2.6 *Penetration Testing*

Penetration testing adalah alat penilaian jaminan bernilai yang menguntungkan baik bisnis dan operasinya. Dari segi operasional, *penetration testing* membantu membentuk strategi keamanan informasi melalui identifikasi kerentanan yang cepat dan akurat. *Penetration testing* membagikan informasi rinci tentang ancamanan keamanan secara aktual, yang dapat dieksploitasi jika tercakup dalam aliran dan proses keamanan organisasi. Hal ini akan membantu organisasi untuk mengidentifikasi dengan cepat dan akurat potensi kerentanan yang nyata.

Tujuan mendasar dari evaluasi kerentanan adalah mengidentifikasi kerentanan keamanan di bawah keadaan yang dikendalikan, sehingga dapat diantisipasi sebelum pengguna yang tidak berhak mengeksploitasi sistem suatu organisasi. Ahli sistem penetrasi menggunakan uji penetrasi untuk mengatasi masalah yang menyangkut dalam penilaian kerentanan, dengan fokus pada kerentanan dengan tingkat keparahan yang tinggi. Tes penetrasi dianggap bagian dari proses manajemen resiko keamanan IT yang mungkin digerakkan oleh persyaratan internal atau eksternal sesuai dengan situasi individu. Penting untuk diingat bahwa tes penetrasi hanya satu komponen dalam mengevaluasi keamanan sistem jaringan. Dan yang paling utama tes penetrasi dapat memberikan bukti nyata

masalah keamanan, namun harus menjadi bagian dari sebuah tinjauan komprehensif tentang keamanan organisasi (Hasibuan & Elhanafi, 2022).

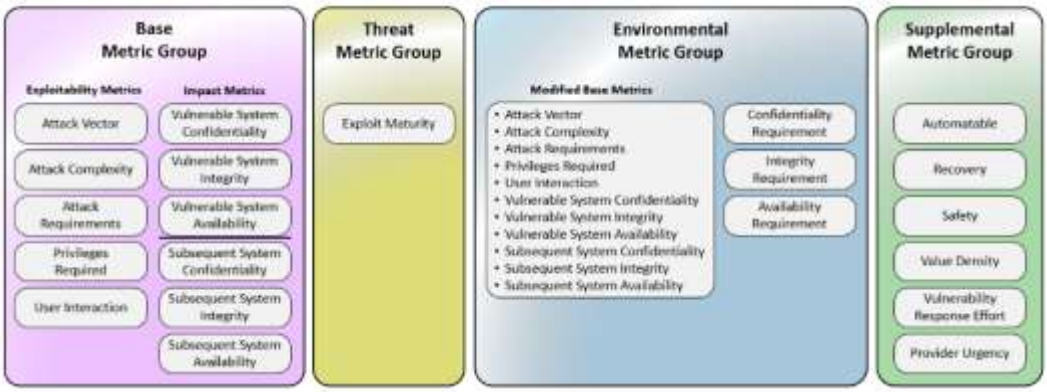
2.7 *Vulnerability Assessment*

Celah keamanan *(vulnerability)* sistem jaringan komputer merupakan sebuah kelemahan, kekurangan atau celah pada sistem yang dapat dimanfaatkan oleh satu atau lebih dari penyerang untuk melakukan serangan yang dapat membahayakan kerahasiaan, integritas, atau ketersediaan suatu sistem. *Vulnerability* adalah suatu kelemahan yang mengancam nilai *integrity, confidentiality, dan availability* dari suatu aset.

Vulnerabilitty Assessment (VA) adalah proses pemindaian sistem atau *software* dan jaringan untuk mengetahui kelemahan dan celah yang ada. Celah ini memberikan *backdoor* ke penyerang untuk menyerang korban (Zirwan, 2022).

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*) (Fahrina, 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 v4.0 memiliki 4 jenis metrik yaitu: *Base, Threat, Environmental,* dan *Supplemental.*



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

Gambar 1 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:

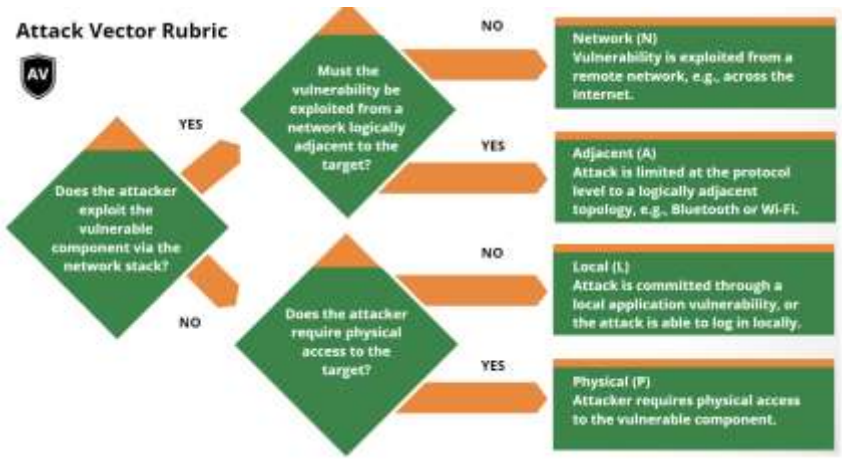
1. *Attack Vector* (AV)

   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 2 Rubrik *Attack Vector*

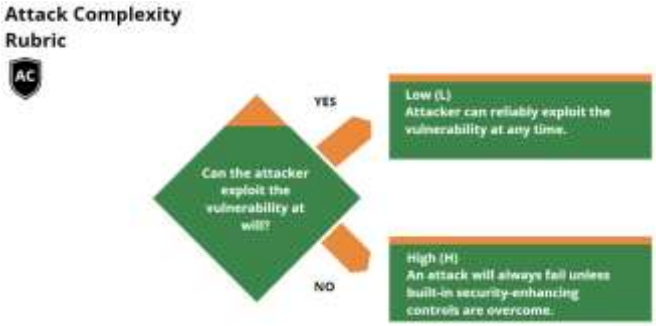
2. *Attack Complexity* (AC)

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 3 Rubrik skor *Attack Complexity*

3. *Attack Requirements* (AT)

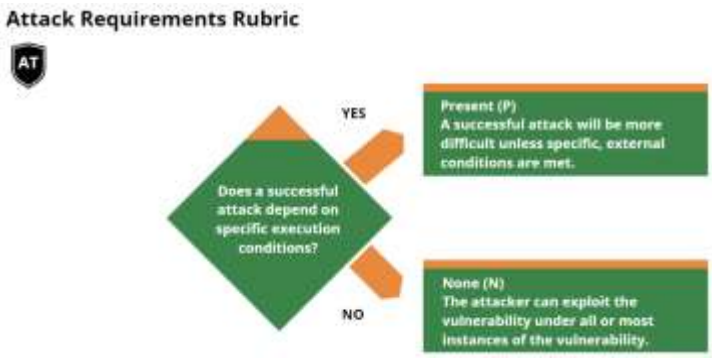
Metrik ini mengukur kondisi atau pengaturan bawaan dari sistem yang rentan, yang sebenarnya tidak dibuat khusus untuk mencegah serangan, tapi justru muncul secara alami karena cara sistem tersebut dipasang dan dijalankan.

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 4 Rubrik *Attack Requirements*

4. *Previleges Required* (PR)

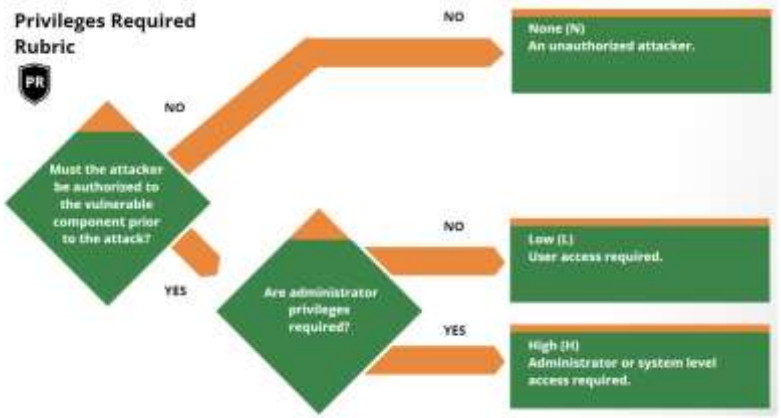
Metrik ini mengukur tingkat kewenangan yang dibutuhkan penyerang untuk mengeksploitasi kerentanan. Semakin tinggi kewenangan yang dibutuhkan, semakin sulit (dan berbahaya) serangan tersebut.

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.
High (H)	*Attacker* memerlukan akses ke pengaturan atau file kerentanan sistem, dan akses tersebut memberikan kontrol

Metrik	Deskripsi
	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 5 Rubrik *Previleges Required*

5. *User Interaction* (UI)

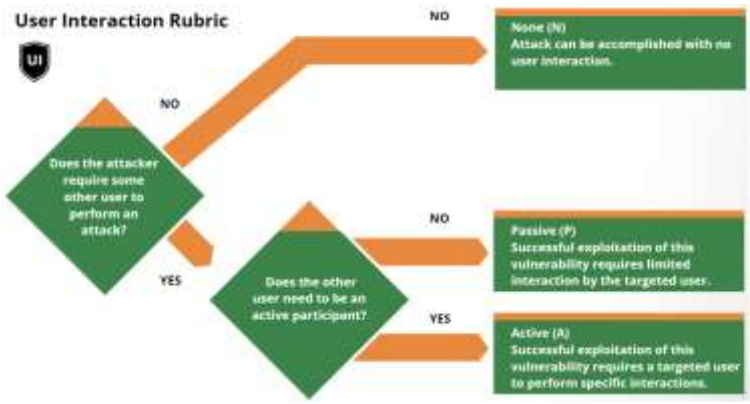
Metrik ini menilai apakah kerentanan bisa dieksploitasi sepenuhnya oleh penyerang saja, atau perlu ada keterlibatan pengguna lain (misal, klik tautan berbahaya, jalankan program tertentu). Semakin minim keterlibatan pengguna, semakin tinggi level bahayanya (karena penyerang bisa langsung melancarkan 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 aktif menumbangkan mekanisme perlindungan yang akan mengarah pada eksploitasi kerentanan. Contohnya meliputi: mengimpor *file* ke dalam sistem yang rentan

Metrik	Deskripsi
	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 6 Rubrik *User Interaction*

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

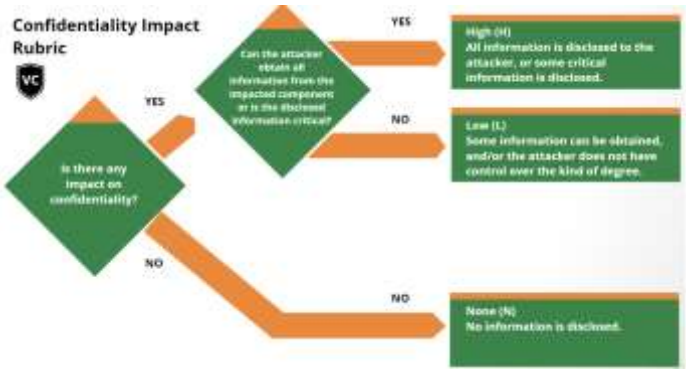
Metrik ini mengukur seberapa parah dampak eksploitasi kerentanan terhadap kerahasiaan informasi yang dikelola untuk sistem yang rentan. Kerahasiaan artinya membatasi akses dan pengungkapan informasi hanya kepada pengguna yang berwenang, serta mencegah akses oleh pihak yang tidak berwenang.

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 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.

Metrik	Deskripsi
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 7 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 informasi tersebut tidak menimbulkan kerugian yang serius dan langsung terhadap Sistem Selanjutnya.
None (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

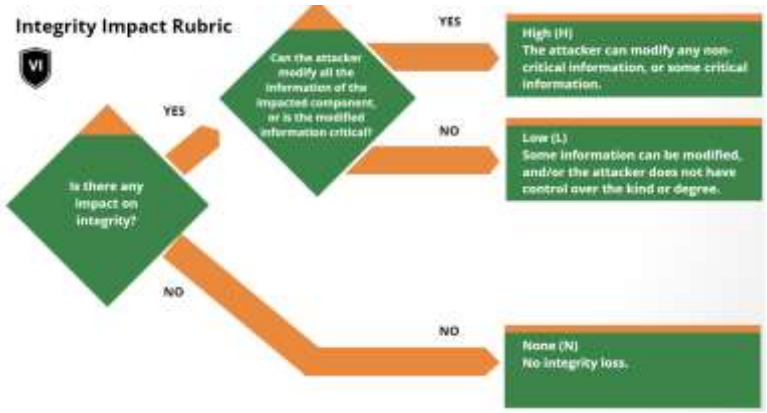
8. *Integrity Impact to the Vulnerable System* (VI)

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 8 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

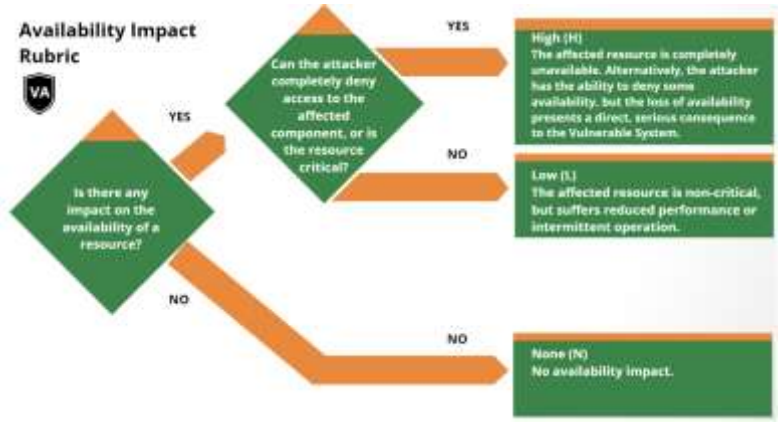
10. *Availability Impact to the Vulnerable System* (VA)

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 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 9 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 13.

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

2.8 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. Penelitian ini direncanakan menggunakan OS Kali Linux, yang menyediakan berbagai *tools vulnerability scanning* dan *penetration testing*. Berikut uraiannya:

a. Nmap

   Berdasarkan *website* nmap.org, nmap (*Network Mapper*) adalah utilitas *open source* dan gratis untuk penemuan jaringan dan audit keamanan. Nmap dapat digunakan untuk eksplorasi dan peretasan jaringan yang memungkinkan penemuan *host, port*, dan layanan di jaringan komputer, sehingga menciptakan "*map*" jaringan.

b. Wireshark

   Berdasarkan *website* wireshark.org, wireshark adalah penganalisis protokol jaringan. *Wireshark* memungkinkan kita menangkap dan menelusuri lalu lintas yang berjalan di jaringan komputer secara interaktif.

Fitur *Wireshark* menampilkan *filter* yang menyaring lalu lintas di jaringan target berdasarkan jenis protokol, *address* IP, *port*, dan sebagainya. Wireshark tersedia secara bebas sebagai *open source* dalam berbagai sistem operasi termasuk Windows, macOS, Linux, dan UNIX.

c. *Aircrack-ng*

Berdasarkan *website* aircrack-ng.org, *Aircrack-ng* adalah seperangkat alat lengkap untuk menilai keamanan jaringan WiFi. Ini berfokus pada berbagai bidang keamanan WiFi, yaitu:

i. Pengambilan paket dan ekspor data ke *file* teks untuk diproses lebih lanjut oleh alat pihak ketiga
ii. Serangan ulangan, deautentikasi, jalur akses palsu dan lain-lain melalui injeksi paket
iii. Pengecekan kartu WiFi dan kemampuan *driver* (*capture* dan *injection*)
iv. Peretasan WEP dan WPA PSK (WPA 1 dan 2)

Semua alat adalah baris perintah yang memungkinkan pembuatan skrip berat. Banyak GUI yang memanfaatkan fitur ini. Ia bekerja terutama di Linux tetapi juga Windows, macOS, FreeBSD, OpenBSD, NetBSD, serta Solaris dan bahkan eComStation 2.

d. Crunch

Berdasarkan *website* kali.org, Crunch adalah generator daftar kata di mana dapat menentukan kumpulan karakter standar atau kumpulan karakter apa pun yang akan digunakan dalam membuat daftar kata. Daftar kata dibuat melalui kombinasi dan permutasi sekumpulan karakter serta dapat menentukan jumlah karakter dan ukuran daftar. Program ini mendukung angka dan simbol, karakter huruf besar dan kecil secara terpisah dan Unicode.

e. Hping3

Berdasarkan *website* kali.org, Hping3 adalah *tools* jaringan yang mampu mengirim paket ICMP/UDP/TCP khusus dan menampilkan balasan target seperti yang dilakukan ping dengan balasan ICMP. *Tools* ini mampu mengatur ukuran paket, kecepatan pengiriman paket, serta dapat

digunakan untuk mentransfer *file* di bawah protokol yang didukung (mengatur jenis paket jaringan). Hping3 menggunakan skrip dengan bahasa Tcl. Pada penelitian ini, pengaturan pada tools hping3 hanya didasarkan pada jenis paket dan kecepatan pengiriman paket (serangan), yang diatur pada kecepatan maksimal guna memperoleh hasil yang maksimal.

f. Macchanger

Berdasarkan *website* kali.org, Macchanger adalah *tools* yang digunakan untuk manipulasi alamat MAC *Address*. Alamat MAC adalah pengidentifikasi unik pada jaringan, alamat tersebut hanya perlu unik, alamat tersebut dapat diubah pada sebagian besar perangkat keras jaringan.