SKRIPSI

ANALISIS KEAMANAN APLIKASI SIKOLA V2.0 UNHAS MENGGUNAKAN METODE *PENETRATION TESTING* DENGAN PENYUSUNAN STANDARISASI DOKUMEN

Disusun dan diajukan oleh:

ANDI NURAINUN ANUGRAH AR
D121 20 1073

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS HASANUDDIN
GOWA
2024

LEMBAR PENGESAHAN SKRIPSI

ANALISIS KEAMANAN APLIKASI SIKOLA V2.0 UNHAS MENGGUNAKAN METODE *PENETRATION TESTING* DENGAN PENYUSUNAN STANDARISASI DOKUMEN

Disusun dan diajukan oleh

Andi Nurainun Anugrah AR
D121201073

Telah dipertahankan di hadapan Panitia Ujian yang dibentuk dalam rangka Penyelesaian Studi Program Sarjana Program Studi Departemen Teknik Informatika
Fakultas Teknik Universitas Hasanuddin
Pada tanggal 18 September 2024
dan dinyatakan telah memenuhi syarat kelulusan

Menyetujui,

Pembimbing Utama,

Dr. Eng. Ady Wahyudi Paundu, S.T., M.T.
NIP. 197503132009121003

Ketua Program Studi,

Prof. Dr. Indrabayu, S.T., M.T., M.Bus.Sys., IPM, ASEAN. Eng.
NIP. 197507162002121004

PERNYATAAN KEASLIAN

Yang bertanda tangan dibawah ini ;

Nama	:	Andi Nurainun Anugrah AR
NIM	:	D121201073
Program Studi	:	Teknik Informatika
Jenjang	:	S1

Menyatakan dengan ini bahwa karya tulisan saya berjudul

{ Analisis Keamanan Aplikasi Sikola V2.0 Unhas menggunakan Metode *Penetration Testing* dengan Penyusunan Standarisasi Dokumen }

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, 29 Juli 2024

Yang Menyatakan

Andi Nurainun Anugrah AR

ABSTRAK

ANDI NURAINUN ANUGRAH AR – D121201073**,** *Analisis Keamanan Aplikasi Sikola V2.0 Unhas menggunakan Metode Penetration Testing dengan Penyusunan Standarisasi Dokumen.* (dibimbing oleh Dr. Eng. Ady Wahyudi Paundu, S.T., M.T.)

Keamanan website merupakan suatu hal yang penting untuk menjaga keamanan serta melindungi data agar mencegah terjadinya serangan siber seperti kebocoran data. Dalam era digital saat ini, keamanan website menjadi sangat penting seperti yang kita ketahui website meliputi sebuah informasi sensitif, seperti data pengguna, informasi bisnis, bahkan catatan keuangan. Ancaman terhadap keamanan website dapat menjadi kerugian besar, seperti kehilangan data serta merusak reputasi sebuah institusi. Tujuan penelitian ini adalah untuk mengidentifikasi kerentanan yang mungkin ada serta memberikan rekomendasi perbaikan terkait kerentanan yang ditemukan pada aplikasi Sikola V2.0. Metode penelitian yang digunakan dalam penelitian ini adalah *Penetration Testing* dengan tahapan perencanaan (*Planning*), pengumpulan Informasi (*Information Gatherting*), pemindaian jaringan (*Network Mapping*), temuan kerentanan (*Vulnerability Found*), pelaporan (*Reporting*). Setelah itu, tingkat kerentanan diukur menggunakan *Common Vulnerability Scoring System* (CVSS), yang memungkinkan pemetaan tingkat kerentanan ke dalam kategori *none*, *low*, *medium*, *high*, dan *critical*. Hasil dari penelitian ini adalah ditemukan 8 kerentanan pada aplikasi Sikola V2.0. Dari 8 kerentanan tersebut, 2 dalam kategori *Medium*, 2 dalam kategori *Low*, dan 4 lainnya dalam kategori *Informational*. Kerentanan yang ditemukan yaitu *Cookie Without SameSite Attribute, Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s), X-Content-Type-Options Header Missing, Information Disclosure - Suspicious Comments, Loosely Scoped Cookie, Timestamp Disclosure – Unix, Cross Site Request Forgery (CSRF) dan Denial of Service (DoS).* Hasil skor tingkat kerentanan secara keseluruhan yang diperoleh berada pada angkat 3.4 yang termasuk dalam kategori *low*.

Kata Kunci: *Penetration Testing*, Sikola V2.0, Keamanan Website, Kerentanan.

ABSTRACT

ANDI NURAINUN ANUGRAH AR – D121201073**,** Security Analysis Sikola V2.0 Unhas Application Using Penetration Testing Method with Document Standardization Preparation. (supervised Dr. Eng. Ady Wahyudi Paundu, S.T., M.T.)

Website security is an important thing to maintain security and protect data to prevent cyber attacks such as data leaks. In today's digital era, website security is very important as we know that websites include sensitive information, such as user data, business information, and even financial records. Threats to website security can be a major loss, such as data loss and damage to an institution's reputation. The purpose of this study is to identify possible vulnerabilities and provide recommendations for improvements related to vulnerabilities found in the Sikola V2.0 application. The research method used in this study is Penetration Testing with stages of planning (Planning), Information Gathering (Information Gathering), network scanning (Network Mapping), vulnerability found (Vulnerability Found), reporting (Reporting). After that, the level of vulnerability is measured using the Common Vulnerability Scoring System (CVSS), which allows mapping the level of vulnerability into categories of none, low, medium, high, and critical. The results of this study were 8 vulnerabilities found in the Sikola V2.0 application. Of the 8 vulnerabilities, 2 into the Medium category, 2 into the Low category, and 4 others into the Informational category. The vulnerabilities found are Cookie Without SameSite Attribute, Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s), X-Content-Type-Options Header Missing, Information Disclosure - Suspicious Comments, Loosely Scoped Cookie, Timestamp Disclosure – Unix, Cross Site Request Forgery (CSRF) and Denial of Service (DoS). The overall vulnerability score obtained was at 3.4 which is included in the low category.

Keywords: Penetration Testing, Sikola V2.0, Website Security, Vulnerabilities.

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

DAFTAR SINGKATAN DAN ARTI SIMBOL

Lambang/Singkatan	Arti dan Keterangan
DoS	*Denial of Service*
MITM	*Man in the Middle*
XSS	*Cross-Site Scripting*
CSRF	*Cross-Site Request Forgery*
CVSS	*Common Vulnerability Scoring System*
TI	Teknologi Informasi
PAN	*Personal Area Network*
LAN	*Local Area Network*
MAN	*Metropolitas Area Network*
WAN	*Wide Area Network*
OSI	*Open System Interconnection*
TCP	*Transmission Control Protocol*
IP	*Internet Protocol*
UDP	*User Datagram Protocol*
LOIC	*Low Orbit Ion Cannon*
DDoS	*Distributed Denial of Service*
HTML	*Hypertext Markup Language*
OWASP	*Open Web Application Security Project*
ZAP	*Zed Attack Proxy*
CSS	*Cascading Style Sheets*
CMD	*Command Prompt*
ICMP	*Internet Control Message Protocol*
LMS	*Learning Management System*
HTTP	*Hypertext Transfer Protocol*
HTTPS	*Hypertext Transfer Protocol Secure*
PoC	*Proof of Concept*
TLS	*Transport Layer Security*
UNHAS	Universitas Hasanuddin
SIKOLA	Sistem Kelola Pembelajaran

Lambang/Singkatan	Arti dan Keterangan
SOP	Standar Operasional Prosedur
APT	*Advanced Persistent Threats*
ISO	*International Organization for Standardization*
KBBI	Kamus Besar Bahasa Indonesia
FTP	*File Transfer Protocol*
SMTP	*Simple Mail Transfer Protocol*
DNS	*Domain Name System*
WAF	*Web Application Firewall*

KATA PENGANTAR

Puji dan Syukur kita panjatkan kepada Allah SWT yang telah memberikan rahmat serta hidayah-Nya, Alhamdulillah atas segala pertolongan dan kasih sayang-Nya sehingga penulis dapat merampungkan skripsi ini. Shalawat serta salam semoga selalu tercurah kepada suri tauladan kita Rasulullah Muhammad SAW yang telah memberikan tuntunan dan petunjuk kepada umat manusia.

Penulis sangat menyadari skripsi ini masih jauh dari kata sempurna. Namun demikian penulis berharap skripsi ini dapat memenuhi persyaratan guna memperoleh gelar sarna (S1) dalam bidang Teknik Informatika Fakultas Teknik Departemen Teknik Elektro Universitas Hasanuddin.

Skripsi yang berjudul **"Analisis Keamanan Aplikasi Sikola V2.0 menggunakan Metode *Penetration Testing* dengan Penyusunan Standarisasi Dokumen",** akhirnya dapat diselesaikan sesuai dengan harapan penulis. Selama penyusunan skripsi ini tentunya ada banyak rintangan dan hambatan yang penulis hadapi. Namun berkat kesungguhan hati dan bantuan dari berbagai pihak, sehingga kesulitan tersebut dapat diatasi.

Pada kesempatan ini penulis juga hendak mengucapkan terima kasih kepada pihak-pihak yang telah membantu memberikan dukungan, bimbingan, bantuan kepada saya selama proses penyelesaian skripsi ini. Oleh karena itu, penulis ingin menyampaikan terima kasih yang sebesar-besarnya kepada:

1. **Bapak Prof. Dr. Ir. Jamaluddin Jompa, M.Sc.** selaku Rektor Universitas Hasanuddin
2. **Bapak Prof. Dr. Eng. Ir. Muhammad Isran Ramli, S.T., M.T., IPM., ASEAN.Eng.** selaku Dekan Fakultas Teknik Universitas Hasanuddin
3. **Bapak Prof. Dr. Indrabayu, ST., M.T., M.Bus.Sys., IPM, ASEAN. Eng.** dan **Ibu Elly Warni, S.T., M.T.** selaku Ketua Departemen Teknik Informatika Fakultas Teknik Universitas Hasanuddin dan Sekretaris Departemen Teknik Informatika Fakultas Teknik Universitas Hasanuddin.
4. **Bapak Dr. Eng. Ady Wahyudi Paundu, S.T., M.T.** selaku dosen pembimbing yang telah meluangkan waktu untuk memberikan bimbingan dan arahan sejak awal penelitian hingga penyelesaian skripsi ini.

5. Orang tua tersayang, Bapak Alm. **Andi Ruslan AS** dan ibunda **Prof. Dr. Ir. Jumriah Langkong M.P.** yang telah mendidik, menyayangi, memberikan dukungan, semangat dan doa restu.
6. Terima kasih juga kepada kakak **Andi Ariani Anggreni AR**, **Andi Nurazizah Almaidah AR**, dan **Andi Ichsan Saputra AR** yang selalu mendidik dan memberikan semangat dan dukungan.
7. Terima kasih juga kepada **Amaliah Ramadhani** sahabat yang selalu menemani serta membimbing, mendukung hingga proses penyelesaian skripsi ini.
8. Terima kasih juga kepada anak Staunch **Wardayanti Maria**, **Deasy Tri Ramadhani**, dan **Tisa Fitria Ramdani Salam** yang selalu mendukung dan memberikan semangat.
9. Terima kasih juga kepada anak tagihan **Nuca**, **Fikri** dan **Vito** yang mendukung dan memberikan semangat saat penyusunan proposal.
10. Terima kasih juga kepada anak Like a Dino **Tiwi**, **Yahdi**, **Ali**, **Adit**, **Adil**, **Iman** dan **Dzaky** yang membantu selalu dan memberikan canda tawa pada masa perkuliahan mulai dari maba hingga semester akhir.
11. Terima kasih juga kepada teman-teman seperjuangan **REZOLVER** yang semasa perkuliahan membantu dan memberikan canda tawa.

Gowa, 29 Juli 2024

Penulis

BAB I
PENDAHULUAN

1.1 Latar Belakang

Keamanan website merupakan suatu hal yang penting untuk menjaga keamanan serta melindungi data agar mencegah terjadinya serangan siber seperti kebocoran data. Dalam era digital saat ini, keamanan website menjadi sangat penting seperti yang kita ketahui website meliputi sebuah informasi sensitif, seperti data pengguna, informasi bisnis, bahkan catatan keuangan. Ancaman terhadap keamanan website dapat menjadi kerugian besar, seperti kehilangan data serta merusak reputasi sebuah institusi. Ancaman siber seperti peretasan data, pencurian data, dan penyebaran malware semakin meningkat. Penyerang terus berupaya menemukan celah keamanan pada suatu website agar mencapai tujuan mereka. Jika tidak adanya keamanan pada sistem maka hal tersebut menimbulkan keterbukaan untuk mengakses data pada website tersebut yang nantinya akan menjadi incaran bagi para Hacker untuk melakukan serangan agar dapat mengambil alih sistem yang dibangun. Oleh karena itu diperlukan upaya memecahkan masalah tersebut maka dibutuhkan penerapan metode yang dapat menjamin keamananan data.

Penetration Testing adalah metode pendekatan yang digunakan untuk mengidentifikasi kerentanan atau celah keamanan suatu sistem. Hal ini melibatkan upaya aktif untuk mencoba mengeksploitasi potensi kerentanan yang ada, dengan tujuan untuk mengidentifikasi dan memperbaiki sebelum penyerang melakukannya. *Penetration Testing* melibatkan serangkaian langkah sistematis yang mencakup *planning*, *information gathering*, *network mapping*, *vulnerability found* dan *reporting*. Melalui simulasi serangan nyata, *penetration testing* dapat memberikan gambaran yang jelas tentang sejauh mana sistem rentan terhadap serangan dan bagaimana cara mengatasinya.

Pada penelitian ini, penelitian akan berfokus pada analisis keamanan aplikasi Sikola V2.0 lebih mendalam dengan mengidentifikasi celah keamanan yang mungkin terdapat dalam sistem tersebut. Hal ini dapat berupa masalah celah dalam sistem yang nantinya dapat digunakan oleh penyerang untuk mencuri informasi serta mengeksploitasi aplikasi Sikola V2.0. Dengan pendekatan ini, diharapkan

dapat ditemukan solusi yang efektif untuk memperkuat keamanan Sikola V2.0 dan memberikan rekomendasi yang bermanfaat bagi pengelola sistem dalam menjaga keamanan informasi.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang telah diuraikan, maka rumusan masalah pada penelitian ini sebagai berikut:

1. Bagaimana menganalisis keamanan aplikasi Sikola V2.0 menggunakan metode *Penetration Testing*?
2. Bagaimana hasil analisis keamanan aplikasi Sikola V2.0 dikuantifikasi untuk mengukur dan mengelompokkan tingkat kerentanan yang ditemukan?
3. Bagaimana merancang dan menyusun Standarisasi dokumen *Penetration Testing Report* yang memberikan panduan praktis dan efektif bagi para pentester?

1.3 Tujuan Penelitian

Adapun tujuan dari penelitian yang akan dilakukan adalah:

1. Mengidentifikasi kerentanan keamanan aplikasi Sikola V2.0 menggunakan metode *Penetration Testing*.
2. Mengevaluasi tingkat risiko setiap kerentanan yang ditemukan untuk mencegah potensi terjadinya serangan siber, termasuk risiko kebocoran data.
3. Memahami cara penyusunan Standarisasi dokumen *Penetration Testing* yang mencakup kerangka kerja yang jelas dan terstruktur.

1.4 Manfaat Penelitian

Dengan dilakukannya penelitian ini, diharapkan dapat memberikan manfaat sebagai berikut:

1. Untuk mengidentifikasi kerentanan dan celah keamanan. Dengan mengetahui celah keamanan sehingga dapat dilakukan perbaikan dan

memperkuat sistem keamanan untuk melindungi dari ancaman serangan siber.

2. Mencegah serta melindungi dari serangan siber yang dilakukan oleh pihak yang tidak bertanggung jawab.
3. Penelitian ini akan memberikan kontribusi pada pemahaman umum praktik dalam pengujian *Penetration Testing*. Standarisasi dokumen yang dihasilkan dapat menjadi acuan bagi institusi pendidikan lainnya atau entitas dengan kebutuhan serupa untuk memitigasi risiko keamanan pada situs web mereka.

1.5 Ruang Lingkup

Adapun ruang lingkup atau batasan masalah pada penelitian ini sebagai berikut:

1. Penelitian ini berfokus pada analisis keamanan aplikasi Sikola V2.0. Tidak mencakup website lainnya yang terkait dengan Universitas Hasanuddin.
2. Penelitian mencakup analisis keamanan yang ditemukan. Namun, tidak mencakup implementasi atau perbaikan terhadap kerentanan yang diidentifikasi. Penelitian ini hanya memberikan rekomendasi untuk tindakan perbaikan, tetapi implementasi tersebut tidak termasuk dalam batasan penelitian.
3. Pengujian pada penelitian ini hanya bersifat non destruktif, yaitu pengujian yang tidak membuat kerusakan pada sistem.

BAB II
TINJAUAN PUSTAKA

2.1 Konsep Dasar Sistem

2.1.1 Pengertian Sistem

Menurut Kamus Besar Bahasa Indonesia (KBBI), sistem adalah perangkat unsur yang secara teratur saling berkaitan sehingga membentuk suatu totalitas. Dalam pengertian ini, sistem mencakup berbagai komponen yang bekerja bersama dalam suatu kesatuan yang terorganisir untuk mencapai tujuan tertentu.

Sistem dalam kamus Webster New Collegiate Dictionary menyatakan bahwa kata "syn" dan "Histanai" berasal dari bahasa Yunani, artinya menempatkan bersama. Sehingga menurut Arifin Rahman bahwa Pengertian Sistem adalah sekumpulan beberapa pendapat (Collection of opinions), prinsip-prinsip, dan lain-lain yang telah membentuk satu kesatuan yang saling berhubungan antar satu sama lain. (Arifin, 2020).

2.1.2 Karakteristik Sistem

Menurut Jogiyanto (2017), Bahwa suatu sistem mempunyai karakteristik atau sifat – sifat tertentu, yaitu memiliki komponen – komponen (*Components*), batas sistem (*Boundary*), lingkungan sistem (*Environment*), penghubung (*Interface*), masukan (*Input*), keluaran (*Output*), pengolah sistem (*Processing System*), dan sasaran (*Objective*), dan tujuan (*Goal*).

1. Komponen Sistem (*Component*)

   Suatu sistem terdiri dari sejumlah komponen yang saling berinteraksi, yang artinya saling bekerja sama membentuk satu kesatuan. Komponen sistem atau elemen –elemen sistem dapat berupa suatu subsistem atau bagian – bagian dari sistem. Setiap subsistem mempunyai sifat – sifat dari sistem untuk menjalankan suatu fungsi tertentu dan mempengaruhi suatu sistem secara keseluruhan.

2. Batasan Sistem (Boundary)

   Batas sistem merupakan daerah yang membatasi antara suatu sistem dengan sistem yang lain atau dengan lingkungan luarnya. Batas sistem ini memungkinkan suatu sistem di pandang sebagai satu kesatuan. Batas suatu sistem menunjukkan ruang lingkup dari sistem tersebut.

3. Lingkungan Luar Sistem (*Environment*)

   Lingkungan luar dari sistem adalah apapundiluar batas dari sistem yang mempengaruhi operasi sistem. Lingkungan luar sistem dapat bersifat menguntungkan (harus dijaga dan merupakan energi dari sistem) dan dapat bersifat merugikan (harus ditahan dan dikendalikan).

4. Penghubung Sistem (*Interface*)

   Penghubung merupakan media penghubung antara satu subsistem dengan subsistem yang lainnya. Melalui penghubung ini memungkinkan sumber-sumber daya mengalir dari subsistem ke subsistem yang lainnya. Keluaran (output) dari satu subsistem akan menjadi masukan (input) untuk subsistem yang lainnya melalui penghubung, Dengan penghubung satu subsistem dapat berinteraksi yang lainnya membentuk satu kesatuan.

5. Masukkan Sistem (*Input*)

   Masukan (input) adalah energi yang dimasukan ke dalam sistem. Masukan dapat berupa masukan perawatan (maintenanceinput) dan masukan sinyal (signalinput). Maintenanceinput adalah energi yang dimasukan supaya sistem tersebut dapat beroperasi. Signalinput adalah energi yang diproses untuk didapatkan keluaran.

6. Keluaran Sistem (*Output*)

   Keluaran adalah hasil dari energi yang diolah dan diklasifikasikan menjadi keluaran yang berguna dan sisa pembuangan. Keluaran dapat merupakan masukan subsistem yang lain atau kepada supersistem.

7. Pengolah Sistem (*Processing System*)

   Suatu sistem dapat mempunyai bagian pengolah yang akan merubah masukan menjadi keluaran.

8. Sasaran Sistem (*Objective*)

   Suatu sistem pasti mempunyai tujuan (*goal*) atau sasaran (*objective*). Kalau suatu sistem tidak mempunyai sasaran, maka operasi sistem tidak akan ada gunanya. Suatu sistem dikatakan berhasil bila mengenai sasaran atau tujuan.

2.2 Konsep Dasar Keamanan

Tiga konsep dasar keamanan yang penting untuk informasi di internet adalah kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*). Konsep yang berkaitan dengan orang-orang yang menggunakan informasi itu adalah *authentication*, *authorization* dan *nonrepudiation*. (Pesante, 2008).

2.2.1 Pengertian Keamanan Informasi

Keamanan informasi merupakan suatu bentuk perlindungan terhadap informasi dan unsur-unsur penting yang ada di dalamnya seperti kerahasiaan, integritas, dan ketersediaan tidak terkecuali sistem dan *hardware* untuk menyimpan dan mengirim informasi tersebut. (Whitman dan Mattord, 2010)

Tiga unsur penting dari keamanan informasi yaitu:

1. Kerahasiaan (*Confidentiality*)

   Kerahasiaan merupakan unsur untuk memastikan suatu informasi tersebut hanya bisa diakses oleh pihak yang memiliki wewenang atas akses ke informasi tertentu.

2. Integritas (*Integrity*)

   Integritas merupakan unsur yang memastikan bahwa kualitas, keutuhan, dan kelengkapan data terjaga sesuai dengan keaslian data.

3. Ketersediaan (*Availability*)

   Ketersediaan merupakan unsur yang memastikan bahwa pihak yang memiliki hak akses ke suatu informasi dapat mengakses informasi tersebut dalam bentuk yang dibutuhkan tanpa gangguan atau hambatan.

Menurut (ISO/IEC27002, 2013) tentang *Information Security Management System*. Keamanan Informasi memiliki kontrol keamanan yang berguna sebagai

upaya perlindungan dari berbagai macam ancaman, memastikan keberlanjutan bisnis dan meminimalkan resiko bisnis serta dapat meningkatkan investasi dan peluang bisnis.

2.2.2 Parameter Keamanan

Parameter keamanan merupakan variabel atau ukuran yang digunakan untuk menilai dan memastikan bahwa suatu sistem, jaringan, atau aplikasi memenuhi standar keamanan yang ditetapkan.

Parameter keamanan meliputi berbagai aspek seperti kontrol akses, otentikasi, integritas data, enkripsi, dan audit, yang semuanya dirancang untuk menjaga kerahasiaan, integritas, dan ketersediaan informasi. (Stallings, 2017)

Menurut (Simamarta, 2006) Sistem komputer memiliki empat parameter keamanan yang sangat penting, yaitu:

1. *Physical Security* (Keamanan Fisik)

   Keamanan Fisik disini membahas seputar perlindungan pertama yang langsung berhubungan dengan dunia luar. Dalam keamanan ini melindungi dan mencegah agar tidak ada hal yang tidak diinginkan terhadap peralatan computer dan sebagainya.

2. *System Security* (Keamanan Sistem)

   Keamanan Sistem disini membahas seputar perlindungan selanjutnya seperti bagaimana pengguna dapat masuk ke dalam sistem, siapa saja yang berhak mengakses sistem tersebut dan lainnya.

3. *Application System* (Sistem Aplikasi)

   Keamanan Aplikasi membahas mengenai seberapa amankah aplikasi yang digunakan, adakah celah dalam aplikasi yang digunakan, apakah aplikasi tersebut dapat disusupi atau tidak dan lainnya.

4. *Data Security* (Keamanan Data)

   Keamanan Data membahas mengenai seberapa amankah data yang disimpan, apakah data tersebut dapa diakses oleh yang tidak memiliki hak akses, adakah kemungkinan data tersebut terhapus, termodifikasi dan lainnya.

2.2.3 Ancaman Keamanan

1. *Malware* (Perangkat Lunak Berbahaya)

   Malware adalah istilah umum yang digunakan untuk merujuk pada berbagai bentuk perangkat lunak yang bermusuhan atau menganggu, termasuk virus, worm, trojan horse, ransomware, spyware, adware, dan program jahat lainnya. (Pfleeger, C. P., & Pfleeger, S. L., 2007)

2. *Phishing*

   Phishing adalah teknik untuk mendapatkan informasi pribadi secara curang, sering kali menggunakan email atau situs web berbahaya, dengan berpura-pura sebagai entitas yang dapat dipercaya. (Jakobsson & Myers, 2007)

3. *Denial of Service* (DoS)

   Serangan *Denial of Service* (DoS) bertujuan untuk membuat mesin atau sumber daya jaringan tidak tersedia bagi pengguna yang dituju dengan mengganggu layanan sementara atau tanpa batas waktu. (Stallings, 2017)

4. *Man-in-the-Middle* (MITM)

   Serangan *Man-in-the-Middle* terjadi ketika seorang penyerang mencegat dan menyampaikan pesan antara dua pihak yang percaya bahwa mereka berkomunikasi langsung satu sama lain. (Kurose & Ross, 2016)

5. SQL *Injection*

   SQL *Injection* adalah teknik injeksi kode yang mengeksploitasi kerentanan keamanan dalam perangkat lunak aplikasi dengan memanipulasi *query* SQL. (Halfond, Viegas & Orso, 2006)

6. *Cross-Site Scripting* (XSS)

   Serangan *Cross-Site Scripting* (XSS) terjadi ketika penyerang menggunakan aplikasi web untuk mengirimkan kode berbahaya, biasanya dalam bentuk skrip sisi klien, ke pengguna akhir lainnya. (Grossman, 2007)

7. *Advanced Persistent Threats* (APTs)

   Ancaman Persisten Lanjutan (APT) adalah serangan siber yang berkepanjangan dan ditargetkan di mana seorang penyusup mendapatkan akses ke jaringan dan tetap tidak terdeteksi untuk jangka waktu yang lama. (Cole, E., 2012)

8. *Insider Threat* (Ancaman dari Dalam)

   Ancaman dari dalam adalah ancaman jahat terhadap organisasi yang berasal dari orang-orang di dalam organisasi, seperti karyawan, mantan karyawan, kontraktor, atau mitra bisnis. (Cappelli & Trzeciak, 2012)

9. *Ransomware*

   Ransomware adalah jenis perangkat lunak berbahaya yang dirancang untuk memblokir akses ke sistem komputer atau data hingga sejumlah uang dibayarkan. (Richardson, 2017)

10. *Social Engineering* (Rekayasa Sosial)

    Rekayasa sosial adalah seni memanipulasi orang sehingga mereka menyerahkan informasi rahasia. (Mitnick, 2011)

2.2.4 Kerentanan (*Vulnerability*)

Kerentanan merupakan kelemahan atau kekurangan dalam suatu sistem yang dapat dieksploitasi oleh ancaman untuk mendapatkan akses tidak sah atau menyebabkan kerusakan.

Kerentanan adalah kelemahan dalam desain, implementasi, operasi, atau pengendalian internal sistem yang dapat dieksploitasi untuk menyebabkan kerugian atau kerusakan. (NIST SP 800-30 Rev. 1, 2012)

Kerentanan adalah kondisi yang memungkinkan ancaman untuk menyebabkan pelanggaran keamanan dengan mengeksploitasi kelemahan sistem. (ISO/IEC 27005, 2011)

Kerentanan didefinisikan sebagai cacat atau kelemahan dalam prosedur keamanan sistem, perancangan, implementasi, atau pengendalian internal yang dapat dilakukan (sengaja dipicu atau sengaja dieksploitasi) dan mengakibatkn pelanggaran keamanan atau pelanggaran terhadap kebijakan keamanan *system*. (Cole, 2011)

2.3 *Penetration Testing*

Penetration Testing atau Uji Penetrasi adalah metode evaluasi keamanan terhadap suatu sistem informasi atau jaringan dengan cara mensimulasikan serangan dari pihak luar atau pihak dalam yang berpotensi merusak sistem tersebut.

Penetration Testing melibatkan penggunaan berbagai teknik manual dan otomatis untuk mensimulasikan serangan terhadap pertahanan keamanan informasi organisasi. (Whitman, M. E., & Mattord, H. J., 2018)

Penetration Testing adalah proses menguji sistem komputer, jaringan, atau aplikasi web untuk menemukan kerentanan yang dapat dieksploitasi oleh penyerang. (Bishop, 2004)

Penetration Tests dapat diklasifikasikan menjadi *black-box testing*, *white-box testing*, dan *gray-box testing*, yang masing-masing bervariasi dalam tingkat pengetahuan yang dimiliki penguji tentang sistem yang diuji. (McGraw, 2006)

Berikut ini adalah beberapa jenis pengujian sistem dalam metode *Penetration Testing* yang umum digunakan:

1. ***Black Box Testing***

   Black Box Testing adalah proses pengujian di mana penguji tidak memiliki pengetahuan sebelumnya tentang sistem yang diuji. *Black box testing* sebenarnya bukan tentang membobol sistem. Sebaliknya, ini tentang menguji keamanan sistem dari sudut pandang penyerang. Tujuannya adalah untuk mengidentifikasi kelemahan keamanan apa pun yang dapat dieksploitasi oleh penyerang untuk mendapatkan akses ke sistem atau datanya.

2. ***White Box Testing***

   White Box Testing, sebaliknya, melibatkan pengujian dengan pengetahuan penuh tentang sistem, termasuk arsitektur dan kode sumbernya. Penguji menggunakan informasi ini untuk melakukan pengujian yang mendalam dan menyeluruh, mencari kerentanan yang mungkin tidak terlihat dari luar. Pendekatan ini memungkinkan evaluasi keamanan yang lebih mendalam dan sering digunakan untuk mengidentifikasi kelemahan internal sistem.

3. ***Grey Box Testing***

   Grey Box Testing, metode ini menggabungkan pengujian kotak hitam dan kotak putih terbaik, memungkinkan Anda menemukan dan mengeksploitasi kerentanan yang mungkin terlewatkan oleh metode lain.

Setiap jenis pengujian memiliki pendekatan dan tujuan yang berbeda, dan seringkali digunakan bersama-sama untuk memastikan cakupan pengujian yang komprehensif dan kualitas perangkat lunak yang tinggi. *Black box testing* fokus pada validasi fungsionalitas eksternal, *white box testing* memeriksa struktur internal, dan *grey box testing* menggabungkan kedua pendekatan untuk pengujian yang lebih mendalam.

2.4 *Vulnerability Assessment*

Vulnerability assessment adalah proses sistematis untuk mengidentifikasi, mengukur, dan memprioritaskan kerentanan keamanan dalam suatu sistem.

Vulnerability assessment adalah proses pengujian yang digunakan untuk mengidentifikasi dan menetapkan tingkat keparahan sebanyak mungkin cacat keamanan dalam suatu sistem informasi dalam jangka waktu tertentu. Proses ini melibatkan teknik otomatis dan manual dengan berbagai tingkat ketelitian serta penekanan pada cakupan yang komprehensif untuk mengidentifikasi celah keamanan. (Synopsys, 2023)

2.4.1 *Common Vulnerability Scoring System* (CVSS)

Common Vulnerability Scoring System (CVSS) merupakan kerangka kerja yang digunakan untuk menilai tingkat keparahan kerentanan keamanan komputer. CVSS memberikan skor numerik yang menunjukkan seberapa serius sebuah kerentanan, yang membantu organisasi dalam mengidentifikasi prioritas untuk menangani ancaman keamanan.

Menurut Leanne Mitton (2024) *Common Vulnerability Scoring System* (CVSS) adalah kerangka kerangka kerja yang dirancang untuk memberikan cara yang konsistem dan obyektif dalam menilai tingkat keparahan kerentanan keamanan dalam sistem TI. CVSS dirancang untuk menjadi standar industri terbuka yang tidak bergantung pada vendor dan digunakan untuk menyampaikan tingkat keparahan kerentanan dan membantu menentukan urgensi dan prioritas respons terhadap kerentanan. CVSS mengevaluasi setiap kerentanan berdasarkan berbagai faktor, seperti kemampuan eksploitasi, dampak, dan tingkat remediasi, lalu memberikan skor numerik yang menunjukkan tingkat keparahannya.

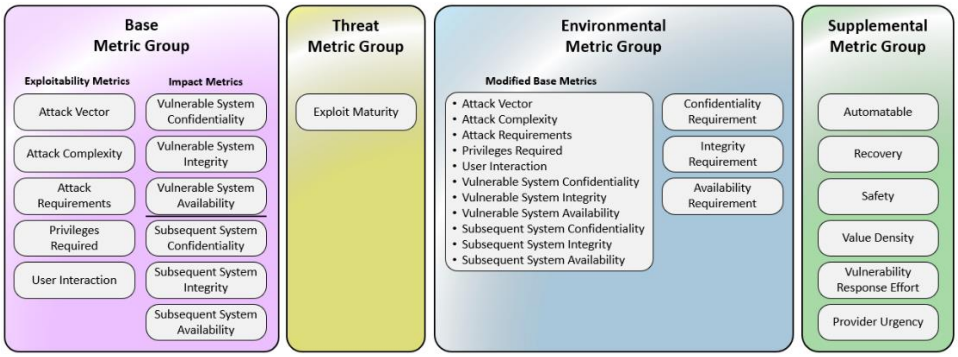
Sistem penilaian berkisar antara 0 hingga 10, dengan skor yang lebih tinggi menunjukkan kerentanan yang lebih parah.

Tabel 1. CVSS Score

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

Tim keamanan menggunakan skor tersebut sambil memprioritaskan strategi respons mereka, memastika bahwa ancaman paling berbahaya dimitigasi terlebih dahulu, sehingga meningkatkan postur keamanan organisasi secara keseluruhan.

CVSS terdiri dari empat kelompok metrik: Base, Threat, Environmental dan Supplemental untuk mengevaluasi risiko yang ditimbulkan oleh suatu kerentanan.



Gambar 1. CVSS Metrics Groups

1. *Base metrics*

   Metrik basis memberikan gambaran seberapa parah suatu kerentanan berdasarkan karakteristik intrinsiknya. Dampaknya tetap sama dari waktu ke waktu dan mengasumsikan dampak terburuk di berbagai lingkungan.

2. *Threat metrics*

   Kelompok *Threat metrics* menyesuaikan tingkat keparahan kerentanan berdasarkan faktor-faktor seperti ketersediaan kode pembuktian konsep atau eksploitasi aktif. Penting untuk dicatat bahwa kelompok metrik Ancaman

mencerminkan karakteristik kerentanan terkait ancaman, yang dapat berubah seiring waktu namun tidak harus di seluruh lingkungan pengguna. Jadi, penting untuk diingat bahwa nilai yang ditemukan dalam grup metrik ini dapat berubah seiring waktu dan tidak tetap konsisten seperti metrik basis.

3. *Environmental metrics*

   Kelompok *enviromental metrics* menangkap karakteristik kerentanan spesifik di lingkungan konsumen. Hal ini memperhitungkan faktor-faktor seperti adanya kontrol keamanan yang dapat mengurangi dampak serangan dan pentingnya sistem yang rentan dalam infrastruktur teknologi.

4. *Supplemental metrics*

   Grup *Supplemental metrics* terdiri dari metrik yang memberikan konteks dan menjelaskan atribut tambahan dari suatu kerentanan. Respons terhadap setiap metrik dalam grup ini ditentukan oleh konsumen CVSS, sehingga memungkinkan penggunaan sistem analisis risiko pengguna akhir untuk menetapkan tingkat keparahan yang signifikan secara lokal pada metrik dan nilai.

Setiap grup metrik memiliki bobot yang berbeda, dengan metrik Dasar yang memiliki bobot paling berat dan metrik Lingkungan memiliki dampak paling kecil terhadap skor keseluruhan. Hal ini memungkinkan organisasi untuk menyesuaikan skor CVSS mereka untuk mencerminkan profil risiko unik mereka.

2.5 Jaringan Komputer

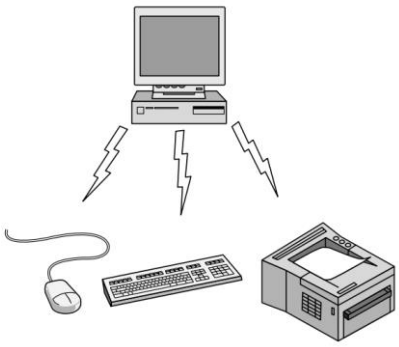
Jaringan komputer adalah kumpulan komputer otonom yang saling berhubungan satu sama lain melalui media komunikasi sehingga memungkinkan terjadinya pertukaran informasi dan pemakaian sumber daya secara bersama-sama. (Stallings, 2007)

2.5.1 Klasifikasi Jaringan Komputer

Komputer yang terhubung dalam jaringan dapat diklasifikasikan lebih lanjut berdasarkan skala jangkauannya. (Tanenbaum & Wetherall, 2011) sebagai berikut:

2.5.1.1 PAN (*Personal Area Networks*)

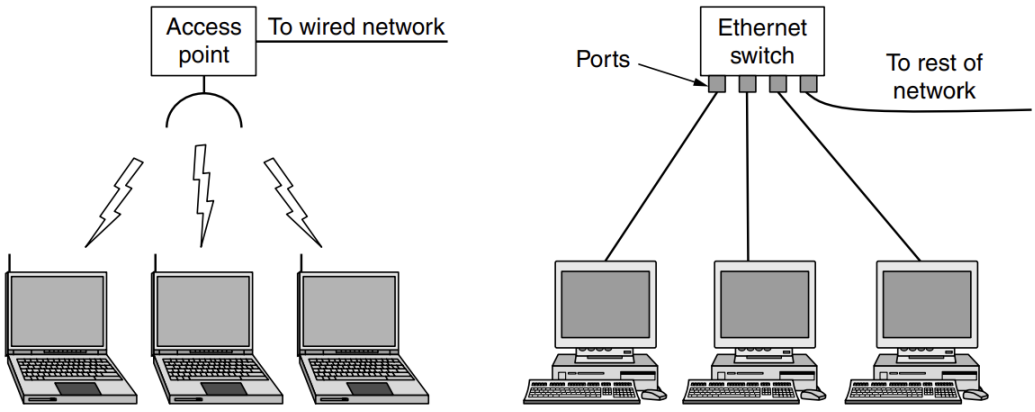
PAN (*Personal Area Networks*) memungkinkan perangkat berkomunikasi dalam jangkauan seseorang. Contoh umum adalah jaringan nirkabel yang menghubungkan komputer dengan periferalnya. Hampir setiap komputer memiliki monitor, keyboard, mouse, dan printer yang terpasang. Tanpa menggunakan wireless, koneksi ini harus dilakukan dengan kabel.



Gambar 2. Konfigurasi Bluetooth PAN

2.5.1.2 LAN (*Local Area Network*)

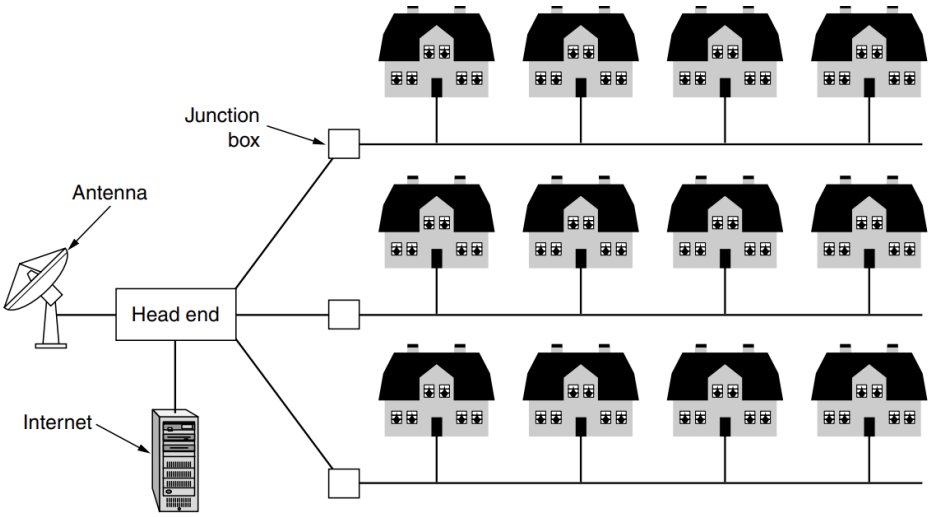
LAN adalah jaringan milik pribadi yang beroperasi di dalam dan di sekitar satu bangunan seperti rumah, kantor, atau pabrik. LAN banyak digunakan untuk menghubungkan komputer pribadi dan perangkat elektronik konsumen agar mereka dapat berbagi sumber daya (misalnya printer) dan bertukar informasi. LAN dapat dibagi menjadi dua jenis, yaitu *Wired* LAN yang menggunakan kabel untuk menghubungkan perangkat dan *Wireless* LAN yang menggunakan koneksi nirkabel.



Gambar 3. (a) Wireless LAN (b) Wired LAN

2.5.1.3 MAN (*Metropolitan Area Network*)

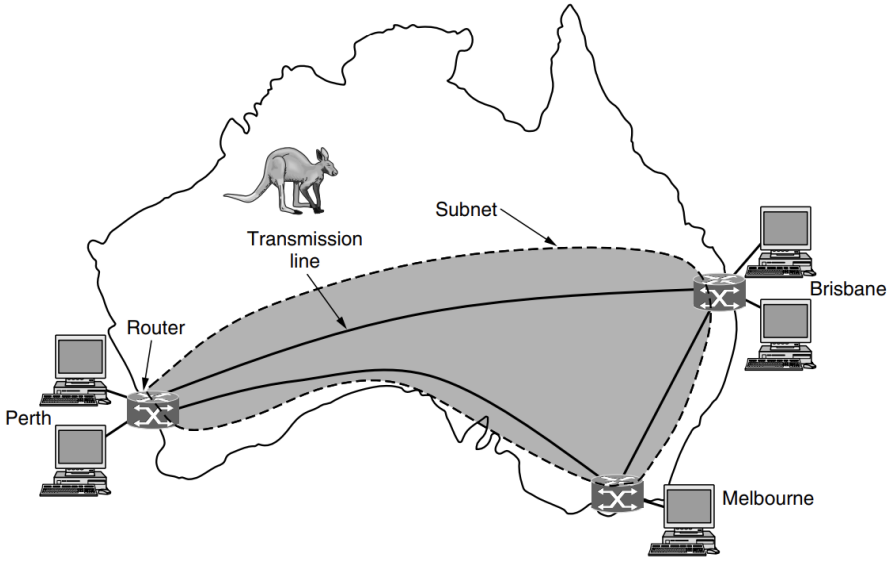
MAN mencakup suatu kota. Contoh MAN yang paling terkenal adalah jaringan televisi kabel yang tersedia di banyak kota.



Gambar 4. MAN berbasis TV Kabel

2.5.1.4 WAN (*Wide Area Network*)

WAN mencakup wilayah geografis yang sangat luas yang sering kali mencakup negara atau bahkan benua.



Gambar 5. WAN yang menghubungkan tiga kantor cabang di Australia

2.5.1.5 Internetworks

Banyak jaringan yang ada di dunia, seringkali dengan perangkat keras dan perangkat lunak yang berbeda. Orang-orang yang terhubung ke satu jaringan seringkali ingin berkomunikasi dengan orang-orang yang terhubung dengan orang lain. Pemenuhan keinginan ini memerlukan jaringan yang berbeda, dan seringkali tidak kompatibel, untuk dihubungkan. Kumpulan jaringan yang saling berhubungan disebut internetwork atau internet

2.5.2 Protokol Jaringan

Dalam arsitektur protokol, modul diatur dalam tumpukan, dimana setiap lapisan melakukan fungsi spesifik untuk berkomunikasi dengan sistem lain, bergantung pada lapisan di bawahnya. Idealnya, perubahan pada satu lapisan tidak mempengaruhi yang lain. Komunikasi dicapai melalui lapisan yang sesuai dalam dua sistem yang berkomunikasi, dengan mengikuti aturan atau konvensi yang dikenal sebagai protokol. (Stallings, 2007). Terdapat 3 fitur utama dari suatu protokol adalah sebagai berikut:

1. Sintaks: Mempertimbangkan format blok data
2. Semantik: Termasuk informasi kontrol untuk koordinasi dan penanganan kesalahan
3. Waktu: Termasuk pencocokan kecepatan dan pengurutan

2.5.2.1 OSI Layer

Model referensi *Open Systems Interconnection* (OSI) dikembangkan oleh International Organization for Standardization (ISO) sebagai model arsitektur protokol komputer dan sebagai kerangka kerja untuk mengembangkan standar protokol. Model OSI terdiri dari 7 lapisan sebagai berikut :

1. *Application*

   Menyediakan akses ke lingkungan OSI untuk pengguna dan juga menyediakan layanan informasi terdistribusi.
2. *Presentation*

   Memberikan kemandirian pada proses aplikasi dari perbedaan representasi data (sintaks).

3. *Session*

   Menyediakan struktur kontrol untuk komunikasi antar aplikasi, menetapkan, mengelola, dan mengakhiri koneksi (sesi) antar aplikasi yang bekerja sama

4. *Transport*

   Menyediakan transfer data yang andal dan transparan antara titik-titik akhir, serta menyediakan pemulihan kesalahan ujung ke ujung dan kontrol aliran.

5. *Network*

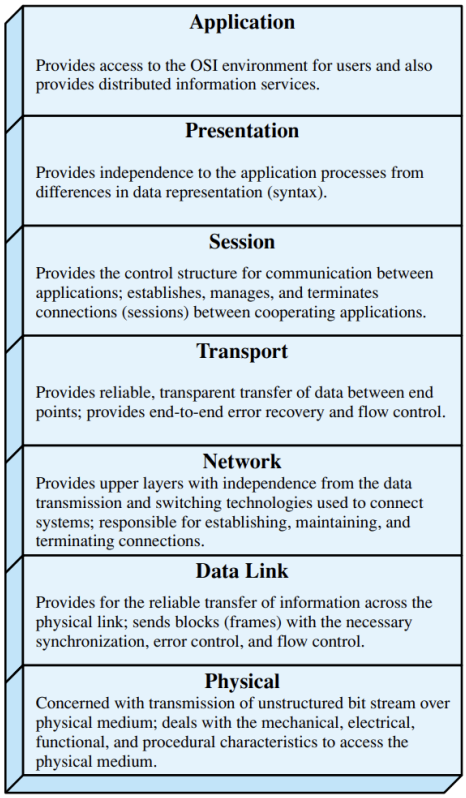
   Memberikan kebebasan pada lapisan atas dari data teknologi transmisi dan switching yang digunakan untuk menghubungkan sistem, bertanggung jawab untuk membangun, memelihara, dan mengakhiri koneksi.

6. *Data Link*

   Menyediakan transfer informasi yang andal di seluruh tautan fisik, mengirimkan blok (*frames*) dengan yang diperlukan sinkronisasi, kontrol kesalahan, dan kontrol aliran.

7. *Physical*

   Berkaitan dengan transmisi aliran bit yang tidak terstruktur melalui media fisik, serta berkaitan dengan karakteristik mekanik, listrik, fungsional, dan prosedural untuk mengakses media fisik.



Gambar 6. Model OSI Layer

2.5.2.2 Transmission Control Protocol / Internet Protocol (TCP/IP)

Transmission Control Protocol / Internet Protocol (TCP/IP) adalah kumpulan protokol yang digunakan untuk komunikasi data di jaringan komputer, termasuk internet. Protokol ini mencakup berbagai aturan dan standar untuk bagaimana data ditransmisikan, diterima, dan diatur antara perangkat jaringan yang berbeda. Terdapat 4 lapisan pada TCP/IP sebagai berikut (Kozierok, 2005):

1. **Aplikasi *(Application)***

   Lapisan ini menyediakan antarmuka antara perangkat lunak aplikasi dan jaringan. Protokol yang bekerja pada lapisan ini memungkinkan aplikasi untuk berkomunikasi dengan jaringan. Contoh protokol pada lapisan ini adalah HTTP, FTP, SMTP, dan DNS.

2. **Transport *(Transport)***

   Lapisan Transport bertanggung jawab untuk pengiriman data end-to-end yang handal. Protokol yang bekerja pada lapisan ini,

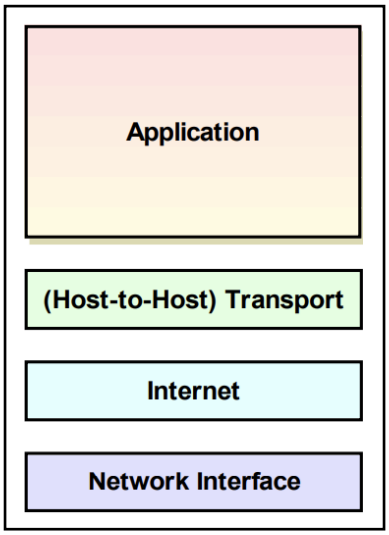
seperti TCP (Transmission Control Protocol) dan UDP (User Datagram Protocol), memastikan bahwa data dikirimkan dengan benar dan dalam urutan yang tepat.

3. **Internet (*Internet)***

   Lapisan *Internetwork* bertanggung jawab untuk routing paket data di antara perangkat yang berbeda dalam jaringan. Protokol utama pada lapisan ini adalah IP (Internet Protocol), yang mengatur pengalamatan dan pengiriman paket data ke tujuan yang benar.

4. **Antarmuka Jaringan *(Network Interface)***

   Lapisan Antarmuka Jaringan bertanggung jawab untuk pengiriman data melalui media fisik jaringan. Ini mencakup protokol yang mengatur bagaimana data ditransmisikan melalui perangkat keras jaringan seperti Ethernet atau Wi-Fi.



Gambar 7. Model TCP/IP