SKRIPSI

VULNERABILITY ASSESSMENT DALAM ANALISIS KEAMANAN WLAN DEPARTEMEN TEKNIK ELEKTRO FT-UH

Disusun dan diajukan oleh

MIFTAHUL FAHRINA

D041181025

PROGRAM STUDI SARJANA TEKNIK ELEKTRO

FAKULTAS TEKNIK

UNIVERSITAS HASANUDDIN

GOWA

2023

LEMBAR PENGESAHAN SKRIPSI

VULNERABILITY ASSESSMENT DALAM ANALISIS KEAMANAN WLAN DEPARTEMEN TEKNIK ELEKTRO FT-UH

Disusun dan diajukan oleh

MIFTAHUL FAHRINA
D041181025

Telah dipertahankan di hadapan Panitia Ujian yang dibentuk dalam rangka Penyelesaian
Studi Program Sarjana Program Studi Teknik Elektro
Fakultas Teknik Universitas Hasanuddin
Pada Tanggal 5 April 2023
dan dinyatakan telah memenuhi syarat kelulusan

Menyetujui,

Pembimbing Utama,	Pembimbing Pendamping,
Prof. Dr. Ir. Andani Achmad, M.T.	Dr.Eng. Wardi, S.T., M.Eng.
NIP. 19601231 198703 1 022	NIP. 19720828 199903 1 003

Ketua Departemen Teknik Elektro,

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

PERNYATAAN KEASLIAN

Yang bertanda tangan dibawah ini

Nama	: Miftahul Fahrina
NIM	: D041181025
Program Studi	: Teknik Elektro
Jenjang	: S1

Menyatakan dengan ini bahwa karya tulisan saya berjudul

VULNERABILITY ASSESSMENT DALAM ANALISIS KEAMANAN WLAN DEPARTEMEN TEKNIK ELEKTRO FT-UH

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, 10 April 2023

Yang menyatakan

Miftahul Fahrina

KATA PENGANTAR

Segala puji bagi Allah SWT dengan segala anugerah dan berkah-Nya yang selalu menyertai setiap langkah penulis. Setelah pemilihan lab *research*, penulis akhirnya mendapat topik yang akan diriset secara *advance* dalam suatu penelitian. Penelitian ini dijadikan Tugas Akhir (TA) yang menjadi syarat kelulusan untuk pendidikan S1. Setelah melewati tahap pengajuan dan persetujuan dari pihak pembimbing dalam bentuk proposal yang kemudian dibuatkan laporan untuk disusun menjadi skripsi yang berjudul ***Vulnerability Assessment* dalam Analisis Keamanan WLAN Departemen Teknik Elektro FT-UH** untuk menguraikan proses pengamatan dan hasil yang didapatkan selama penelitian dilakukan.

Melalui halaman ini juga, penulis sampaikan terima kasih kepada pihak-pihak berikut.

1. Prof. Dr. Ir. Andani Achmad, M.T. dengan Dr.Eng. Wardi, S.T., M.Eng. selaku Pembimbing TA penulis.

2. Semua pihak yang berbagi kebaikan selama penulis melakukan penelitian sampai penyusunan skripsi ini.

Dari pelaksanaan penelitian ini, penulis berharap hasil riset yang didapatkan bisa menjadi ilmu yang begitu *insightful*, serta menjadi bahan topik untuk penelitian selanjutnya atau bahkan berguna untuk keperluan *security auditing* pada sistem jaringan kampus.

Gowa, 10 April 2023

Penulis

ABSTRAK

MIFTAHUL FAHRINA. *Vulnerability Assessment dalam Analisis Keamanan WLAN Depertemen Teknik Elektro FT-UH* (dibimbing oleh Andani Achmad dan Wardi).

Wireless Local Area Network (WLAN) telah menjadi bagian dari teknologi modern namun dengan peningkatan penggunaannya memunculkan *vulnerability* pada keamanannya. *Vulnerability* keamanan jaringan yang berdampak pada semua perangkat Wi-Fi sudah ditemukan sejak tahun 1997. Bahkan berbagai penelitian juga telah menemukan *vulnerability* dari sistem keamanan WLAN. Oleh karena itu, pengujian keamanan WLAN sangat penting, terutama di institusi seperti kampus di mana fasilitas ini diperlukan untuk semua pengguna kampus yang dapat digunakan dengan aman. Penelitian ini menyelidiki keamanan WLAN di gedung Departemen Teknik Elektro FT-UH, menggunakan *penetration testing* untuk menyelidiki dampak *vulnerability* WLAN dan menilai *severity level* dari *vulnerability* tersebut dengan menggunakan metode *vulnerability assessment*. Pengujian yang dilakukan termasuk *sniffing traffic*, *deauthenticating client*, dan *cracking* WPA menggunakan *tool* seperti Nmap, Wireshark, Ettercap, dan Aircrack-ng pada Kali Linux OS. Penelitian ini menemukan bahwa, berdasarkan pengujian yang dilakukan dengan *adjacent network* dari koneksi *victim machine* ke AP, *attacker* dapat melihat kredensial *login* dari *web* HTTP. Namun, sistem *hashing* dari *login web* jaringan kampus membuat *password* tidak ditransmisikan dalam *plain text*. Penelitian ini juga mengungkap serangan *deauthenticating client* yang mengakibatkan DoS serta pengungkapan *password* dari AP WPA2-PSK. Namun ditemukan bahwa jika koneksi *victim* dari AP *Open-Encrypted*, maka secara otomatis akan terhubung kembali ke AP. Penelitian ini menggunakan CVSS v3.1 *calculator* untuk menilai *severity level* dari *vulnerability* keamanan WLAN kampus, yang mendapatkan skor 5.4, secara kualitatif termasuk kategori Medium. Ini berarti bahwa kerentanan keamanan yang ditemukan masih berpotensi merugikan jaringan dan penggunanya.

Kata kunci: Keamanan, WLAN, *Vulnerability Assessment*, *Penetration Testing*

ABSTRACT

MIFTAHUL FAHRINA. *Vulnerability Assessment in WLAN Security Analysis at Electrical Engineering Department, Faculty of Engineering, Hasanuddin University* (supervised by Andani Achmad and Wardi).

Wireless Local Area Networks (WLANs) have become an integral part of modern communication systems. However, with the increasing reliance on these networks, the security of WLANs has become a growing concern. In particular, vulnerabilities in WLAN security systems have been discovered since 1997, with various studies confirming their existence. As a result, testing the security of WLANs is essential, especially in institutions such as university campuses where WLAN facilities are necessary for all campus users to use securely. This study investigates the security vulnerabilities of WLAN in the Electrical Engineering Department building at FT-UH. The aim of the study is to assess the impact of WLAN vulnerabilities and evaluate their severity level using the vulnerability assessment method. The study conducts penetration testing, including sniffing traffic, deauthenticating client, and cracking WPA using various tools such as Nmap, Wireshark, Ettercap, and Aircrack-ng on Kali Linux OS. This study found that, based on tests conducted with the adjacent network from the victim machine's connection to the AP, an attacker can view login credentials from the HTTP web. However, the hashing system from the campus network web login does not transmit passwords in plain text. This study also revealed deauthenticating attacks that result in DoS and disclosure of passwords from a WPA2-PSK AP. Notably, this study discovered that if the victim's connection is from an open-encrypt AP, the victim automatically reconnects to the AP. This study used the CVSS v3.1 calculator to assess the severity level of campus WLAN security vulnerabilities, which obtained a score of 5.4, qualitatively belonging to the Medium category. This means that the security vulnerability discovered in the study could be potentially harmful to the network and its users.

Keywords: Security, WLAN, Vulnerability Assessment, Penetration Testing

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR SINGKATAN

Singkatan	Keterangan
AP	*Access Point*
ARP	*Address Resolution Protocol*
BSSID	*Basic Service Set IDentifier*
CVSS	*Common Vulnerability Scoring System*
ESSID	*Extended Service Set IDentifier*
HTTP	*Hypertext Transfer Protocol*
IP	*Internet Protocol*
MAC	*Media Access Control*
MITM	*Man in The Middle*
PSK	*Pre-Shared Key*
Wi-Fi	*Wireless Fidelity*
WLAN	*Wireless Local Area Network*
WPA	Wi-Fi *Protected Access*

BAB I
PENDAHULUAN

1.1 Latar Belakang

Cyber Culture telah menjadikan transformasi digital yang begitu signifikan terutama penggunaan jaringan *wireless* di berbagai aspek kehidupan karena kemudahan akan koneksinya. Ibarat koin dengan dua sisi, teknologi ini terus berkembang dengan pesat seiring dengan sisi *threat* yang terus mendampinginya. Bahkan sampai hari ini *threat* baru dengan penemuan solusi yang sesuai pun terus terjadi. Mengelola dan mengamankan jaringan yang semakin rumit tetap menjadi tantangan serius bagi sebagian besar *user* yang mungkin memiliki sedikit keahlian teknis untuk mengelola jaringan dan perangkat yang terkoneksi. Apalagi, *user* umumnya tidak terlalu menyadari risiko yang terlibat dalam jaringan komputer sehingga sering menjadi target bagi *hacker*. Keamanan jaringan dapat datang dalam berbagai bentuk dan merupakan proses yang ditargetkan untuk mendukung penggunaan serta integritas jaringan dan data, baik itu teknologi *software* maupun *hardware*-nya.

Berdasarkan artikel BLEEPINGCOMPUTER yang ditulis oleh Sergiu Gatlan bahwa, *vulnerability* keamanan Wi-Fi yang baru ditemukan secara kolektif dikenal sebagai *FragAttacks* berdampak pada semua perangkat Wi-Fi sejak tahun 1997. Akhir tahun 2022, jumlah *vulnerability* yang dilaporkan pada *web* CVE Details, lebih dari 25226 *vulnerability* tercatat dari bulan Januari, dibandingkan dengan 20171 *vulnerability* pada tahun 2021. *User* harus terus-menerus waspada terhadap kemungkinan dari *vulnerability* dan kebanyakan *vulnerability* tersebut muncul karena pengaturan jaringan yang *default*.

Kampus menjadi salah satu yang membutuhkan fasilitas WLAN yang dipakai oleh semua warga kampus. Karena merupakan Wi-Fi *public* bagi warga kampus sehingga perlu jaminan bagi *user* untuk dapat dengan aman mengakses jaringan dan terlindungi dari *threat* dan *vulnerability*. Meninjau belum adanya penelitian terdahulu mengenai topik tersebut di Depatemen Teknik Elektro Fakultas Teknik Universitas Hasanuddin sehingga secara *basic* mendorong

penulis untuk menganalisis *security level* dari sisi WLAN.

Selama bertahun-tahun, berbagai jenis *tool* telah dikembangkan dengan tujuan untuk menguji keamanan jaringan dan mengeksploitasi *vulnerability* jaringan. Pakar keamanan J.Long menyebutkan dalam "Kali Linux *Revealed*" bahwa orang tidak menyadari betapa beruntungnya mereka memiliki Kali Linux di zaman modern ini. Beliau menjelaskan bahwa dulu timnya harus menghabiskan banyak waktu untuk memetakan dan membuat katalog *tool* dengan benar untuk mempertahankan kegunaannya dalam pengujian jaringan. Proses tersebut kemudian menjadi usang dengan dirilisnya Kali Linux.

Penelitian yang telah dilakukan Rendro et al. (2020) untuk menganalisis keamanan jaringan dengan penerapan *tool* Nmap untuk *scanning* jaringan dalam mengetahui *vulnerability* dari sistem keamanan jaringan. Dari penelitian ini disimpulkan, *sysadmin* dapat mengetahui informasi secara *real-time* untuk dapat melakukan tindakan *preventif* terhadap keamanan jaringan *router* maupun pada *website* yang digunakan. Hasil penelitian Sudirman and Yaqin (2021) dengan metode yang sama menggunakan Nmap untuk membuka informasi *traffic* pada jaringan target, seperti jumlah *host* pada perangkat terhubung, IP *address*, *network*, perangkat *router*, *port* TCP/UDP terbuka dan tertutup. *Vulnerability* yang diketahui dapat menjadi upaya perbaikan dalam membentuk sistem keamanan jaringan yang lebih kuat sehingga dapat meyakinkan seluruh user yang mengakses pada wilayah jaringan tetap aman dan privasi terjaga. Begitu juga dengan penelitian Fahlevi and Putri (2021) dengan *scanning* Nmap dapat melihat *port* terbuka setelah di-*monitoring* dalam keamanan jaringan baik terhadap router maupun pada *website* yang digunakan. Adapun dari penelitian Fatimah et al. (2022) yang menganalisis hasil pengujian pada keamanan jaringan menggunakan aplikasi Wireshark dan Ettercap (OS Kali Linux) dengan hasil bahwa tidak didapatkan adanya aktivitas seperti mengakses akun situs. Pada saat dilakukan serangan *packet sniffing* diketahui bahwa jaringan Wi-Fi sudah dilindungi keamanannya dengan *security* atau *encryption* keamanan WPA2. Berbeda dengan penelitian Nurdiana, et al. (2021) yang memanfaatkan Wireshark untuk metode *sniffing* jaringan WiFi yang berbasis protokol untuk mendapatkan hasil *capture*

traffic dan mendapatkan *username* dan *password* dari suatu situs *web*.

Penelitian-penelitian tersebut menerapkan metode *sniffing* dengan *tool* Nmap dan Wireshark yang memberikan hasil *scan port* dan *capture traffic* namun hasil percobaan yang telah dilakukan hanya menampilkan *port* yang terbuka dan untuk *capture traffic* juga sangat bergantung dari protokol keamanan *website* yang dijadikan target. Di samping itu, metode tersebut tidak bisa menembus *encryption* WPA2. Dengan metode lain yang telah digunakan dari penelitian Lu & Yu (2021) yaitu *penetration testing* dengan metode *monitoring, scanning, capturing*, dan analisis data; *password cracking*; serta *spoofing fake* AP pada OS Kali Linux dengan ditemukannya masalah tersembunyi pada jaringan yang berguna untuk meningkatkan keamanan jaringan Wi-Fi. *Penetration testing* juga diujikan Setyawan (2022) dengan metode *Brute force* pada *password cracking*, dengan *hijacking network* untuk *deauthentication user*, serta serangan ARP *spoofing*. Alasan ini mendasari penulis dalam mengimplementasikan *vulnerability assessment* dalam proses analisis keamanan WLAN kampus dengan *penetration testing* pada pengujiannya.

Adapun metode yang diusulkan dalam penelitian ini memanfaatkan *tool* Kali Linux dalam pengujian jaringan *wireless*. Dari metode tersebut kemudian dianalisis *tool* apa saja yang diperlukan dengan meninjau fase *Penetration Testing* diantaranya *pre-attack*, *attack*, dan *post-attack*, yang disesuaikan dengan standar *security assessment* (Ec-Council, 2021). Pada fase *pre-attack* akan dijadikan langkah awal dalam mengumpulkan informasi jaringan target untuk memetakan jaringan untuk merencanakan strategi serangan yang dilanjut dengan fase *attack* dengan mengeksekusi strategi yang telah direncanakan guna mengeksploitasi *vulnerability* yang ditemukan selama fase *pre-attack* untuk mendapatkan akses ke sistem. Selanjutnya, fase *post-attack* melibatkan pembersihan proses pengujian, menghapus *vulnerability* yang dibuat (bukan *vulnerability* yang ada pada awalnya), eksploitasi yang dibuat, dan seterusnya, hingga semua sistem yang diuji dikembalikan ke statusnya sebelum pengujian. Hasil dari penelitian ini diharapkan dapat menunjukkan tingkat keamanan Wi-Fi *access point* yang digunakan serta menjadi bahan evaluasi dari sistem keamanan dari WLAN di Departemen Teknik

Elektro Fakultas Teknik Universitas Hasanuddin.

1.2 Rumusan Masalah

Dengan mengacu pada *background* penelitian ini maka pengujian keamanan WLAN di kampus Fakultas Teknik Universitas Hasanuddin adalah masalah utama yang meliputi poin berikut.

1. Bagaimana dampak *vulnerability* yang ditemukan ketika menjalankan *penetration testing* berdasarkan jenis serangan yang terjadi?
2. Bagaimana *severity level* akibat *vulnerability* yang terekspos oleh konfigurasi jaringan Wi-Fi dengan metode *vulnerability assessment*?

1.3 Tujuan Penelitian

Penelitian ini dimaksudkan untuk menguji dan menganalisis keamanan WLAN kampus Fakultas Teknik Universitas Hasanuddin. Berikut tujuan yang ingin dicapai dari penelitian ini.

1. Mengidentifikasi dampak *vulnerability* berdasarkan jenis serangan yang terjadi dengan *penetration testing*.
2. Menyelidiki *severity level* akibat *vulnerability* yang terekspos oleh konfigurasi jaringan Wi-Fi dengan metode *vulnerability assessment*.

1.4 Manfaat Penelitian

Manfaat yang diharapkan dari terlaksananya penelitian ini:

1. Menyadari pentingnya *network security* dan mempelajari jenis *threat* atau *vulnerability* pada jaringan Wi-Fi.
2. Menambah *skill* baru dalam hal ini kemampuan analisis dari berbagai *tool* Kali Linux.
3. Memahami cara mengidentifikasi serangan pada WLAN demi menjaga keamanan jaringan.

1.5 Ruang Lingkup

Penelitian ini berfokus pada pengujian jaringan Wi-Fi melalui koneksi *access point* yang merupakan bagian WLAN sistem jaringan kampus gedung Departemen Teknik Elektro Fakultas Teknik Universitas Hasanuddin.

Ruang lingkup ilmu penelitian ini sendiri adalah pengimplementasian metode *vulnerability assessment* dengan *penetration testing* pada jaringan Wi-Fi melalui *tool* Kali Linux. Dengan memberikan batasan masalah berikut.

1. Melakukan proses analisis dari *attacker machine* dan *victim machine* yang terkoneksi dengan jaringan kampus.
2. IP atau MAC *address* dari *victim* yang akan diujikan telah diketahui sebelum melakukan pengujian.
3. Pengujian yang dilakukan hanya mencakup tiga serangan: *sniffing traffic*, *deauthenticating client*, dan *cracking* WPA.
4. Berfokus pada pengujian keamanan WLAN kampus.
5. Sesuai dengan tujuan maka dalam penelitian ini sebatas menilai tingkat keparahan *vulnerability* yang telah terekspos.

BAB II
TINJAUAN PUSTAKA

2.1 Studi Kepustakaan

Tabel 1 Penelitian terdahulu

Peneliti	Metode	Keterangan
Rendro, et al. (2020)	*Network scanning* (Nmap)	Hasil *scanning* jaringan secara *real-time* sesuai dengan keadaan yang terjadi untuk dapat melakukan tindakan *preventif* keamanan jaringan baik terhadap *router* maupun pada *website* yang digunakan.
Sudirman and Yaqin (2021)	*Port scanning* (Nmap)	Hasil yang diperoleh dari jaringan target dapat membuka informasi *traffic* pada jaringan, seperti jumlah *host* pada perangkat terhubung, IP *address*, *network*, perangkat *router*, *port* TCP/UDP terbuka dan tertutup.
Fahlevi and Putri (2021)	*Network scanning, port scanning* (Nmap)	Dari hasil pengujian mampu melakukan *scanning* jaringan secara mudah untuk mendapatkan informasi yang ada pada jaringan. *Software* Nmap dapat digunakan untuk melakukan *scanning* jaringan pada *host* target berupa IP *Address* serta dapat melakukan *port scanning* jaringan dengan fitur layanan dan pendeteksi OS.
Lu and Yu (2021)	*Penetration testing* (Kali Linux)	Bertujuan pada *vulnerability* jaringan *wireless*, dengan mengusulkan metode *penetration testing* Wi-Fi dengan menggunakan metode *monitoring, scanning, capturing*, analisis data, *password cracking*, *spoofing fake* AP, dan metode lainnya dari Kali Linux yang diproses di lingkungan simulasi.
Satria (2022)	Perbandingan WPA dan WPA2-PSK (*aircrack*)	Hasil analisis keamanan menggunakan metode WPA2-PSK lebih sulit mendapatkan *handshake* dikarenakan memiliki keamanan yang lebih unggul. Penggunaan metode WPA-PSK maupun WPA2-PSK harus memiliki pencarian data yang sesuai dari uniknya *password* target.
Antoni (2020)	*Evil twin attack*	Pada pengujian metode *evil twin attack*, memanfaatkan MAC *address* yang ada untuk membuat AP palsu beserta web pancingannya.
Sasi, et al. (2020)	*Ten hands-on exercises on networking protocols*	Memahami skema *addressing* IPv4, panggilan *Domain Name System* (DNS) melalui *Nslookup*, memperoleh *record* DNS *type* NS, kalkulasi UDP *checksum* dan proses 3-*way handshake Transmission Control Protocol*

Peneliti	Metode	Keterangan
	(Wireshark, Nmap, dan DOS)	(TCP) adalah lima langkah pertama yang dipertimbangkan di sini. Lima tugas lainnya adalah seperti *termination* TCP, *Ping address* IP *public versus private*, identifikasi *server firewall*, peran *server firewall* pada permintaan paket *Internet Control Message Protocol* (ICMP), dan memahami *sequence* dan *acknowledge number* selama transfer data aplikasi di TCP.
Gierszewski and Matuśkiewicz (2020)	*Password attack*	Untuk protokol WEP, perintah *aircrack-ng* menunjukkan bahwa seberapa kompleks *password* yang digunakan tetap saja rentan akan serangan. Serangan *deauthentication* pada WPA2 diperlukan informasi dari perintah *airodump-ng* dan mengirim paket pembatalan *authentication* dengan *aireplay-ng*. Adapun serangan WPA/WPA2 PSK dengan keefektifan yang bergantung dari PSK key dalam *dictionary*.
Martin and Jasri (2021)	*penetration testing* (c*racking the encryption,* SSID *fake*)	Mengevaluasi setiap celah keamanan dari sistem jaringan dengan menghasilkan analisis bagaimana *attack*er dapat memperoleh akses ke dalam sistem jaringan tersebut. Untuk pengujian *cracking the encryption* tidak di temukan dikarenakan sistem keamanan *password* sudah baik. *Attacker* juga dapat melakukan pemalsuan MAC address komputer dari client yang terdapat di dalam jaringan. Di samping itu, *attacker* yang berada dalam WLAN, dapat membuat SSID *fake* untuk Wi-Fi yang ditargetkan.
Michael, et al. (2021)	*penetration testing* (tool *interface* berbasis *desktop*)	Penelitian ini berhasil menyederhanakan penggunaan *tool* yang masih menggunakan *command-line* berbasis text dengan *interface* berbasis *desktop* yang telah dimodifikasi. Hasil perbandingan WPA2-PSK dan *captive portal* dengan melakukan pengujian pada 10 sampel sistem keamanan WPA2-PSK dengan serangan *packet capture, deauthentication, brute force*, dan ARP *attack*. WPA2-PSK memiliki sistem keamanan yang lebih baik dibandingkan *captive portal*.
Astrida, et al. (2022)	Penetration *Testing* Execution Standard	Hasil dari penelitian ini menunjukkan untuk serangan pada WPA2 key bisa dilakukan *crack* dengan *aircrack-ng*, Koneksi *client* ke *access point* mudah ter-*disconnect*, penggunaan *default password* menjadikan level

Peneliti	Metode	Keterangan
		vulnerability tinggi, dengan NetCut bisa melakukan serangan *client-to-client*.
Zaidan (2021)	DoS, *dictionary attack, evil twin*	Mengidentifikasi *vulnerability* keamanan yang terkait dengan protokol WEP, WPA, dan WPA2 beserta solusi peningkatan keamanan jaringan *wireless* guna menghadapi *attacker*. Dari penelitian ini dijelaskan bahwa protokol WPA-WPA2 lebih baik dibandingkan dengan WEP, tapi kelemahan tetap berlaku untuk ketiga protokol tersebut jika menggunakan *password* lemah.
Nurdiana, et al. (2021)	*Sniffing* (Wireshark)	Penelitian ini mencoba melakukan metode *sniffing* pada jaringan WiFi yang berbasis protokol untuk mendapatkan hasil *capture traffic* dan mendapatkan *username* dan *password* sebuah *station*.
Mulyanto, et al. (2022)	*penetration testing* (*password cracking*)	Hasil pengujian bahwa adanya *access point* dengan *password* yang sangat mudah di tebak dan rentan terhadap serangan, sehingga perlu penanganan yang lebih baik serta menggunakan *passphrase*.
Setyawan (2022)	*penetration testing* (*Bruteforce, hijacking network,* ARP *Spoofing*)	Hasil penelitian dari metode *Bruteforce* menunjukkan tingkat kerumitan *password* sangat memengaruhi waktu *cracking* serangan ini. Setelah terkoneksi jaringan dilanjutkan dengan serangan *hijacking network* yang mengakibatkan *user* tidak dapat mengakses *internet* dan mengalami penurunan kecepatan *internet* serta serangan ARP *Spoofing* yang bergantung dari protokol keamanan *website* yang diakses.
Rachman (2021)	*Packet sniffing, cracking the encryption, Man in The Middle*	Dengan menganalisis *network traffic* menggunakan Wireshark, dapat ditangkap komunikasi data dari protokol ARP and DNS, sehingga mampu didapatkan informasi yang berupa IP *address, time, source, destination, protocol, length*, dan info. Satu yang berstatus gagal yaitu pada jenis serangan *cracking the encryption*. Pengujian *Man in The Middle* (MITM) dengan ARP poisoning dalam memantau *website* yang diakses target dengan tingkat keberhasilan yang bergantung dari protokol keamanan *website* tersebut.
Susanto and Raharja (2021)	*Man in The Middle,* ARP *Poisoning,*	Pada penelitian ini, serangan *Man in The Middle* pada jaringan WI-Fi publik mendapatkan akses informasi pengguna dengan cara ilegal Serangan ARP *Poisoning*

Peneliti	Metode	Keterangan
	Session Hijacking, SSL *Striping*	terhadap protokol ARP pada lalu lintas data antara desktop virtual dan server virtual dan ponsel dengan server virtual dapat mencegat dan memanipulasi penyediaan informasi *address* MAC. Serangan *session hijacking* pada protokol HTTPS tidak berhasil mencegat *session id*. Serangan SSL *Striping* tidak berhasil menurunkan versi protokol HTTPS ke HTTP.
Fatimah et al. (2022)	*Packet sniffing* (Wireshark, Ettercap)	Pengujian serangan pada jaringan Wi-Fi tidak didapatkan adanya aktivitas dari hasil *capturing* seperti mengakses akun situs karena sudah dilindungi keamanannya dengan *security* atau *encryption* keamanan WPA2.

2.2 Dasar Teori

2.2.1 *Security Attack*

1. *Threat*

Threat adalah potensi terjadinya suatu peristiwa yang tidak diinginkan yang pada akhirnya dapat merusak dan mengganggu kegiatan operasional dan fungsional suatu organisasi. *Threat* dapat berupa semua jenis entitas atau tindakan yang dilakukan pada aset fisik atau non-fisik yang dapat mengganggu keamanan. Adanya *threat* dapat bersifat kebetulan, disengaja, atau karena dampak dari tindakan lain. *Attacker* menggunakan *threat cyber* untuk menyusup dan mencuri data seperti informasi pribadi, informasi keuangan, dan kredensial *login*. (Ec-Council, 2021)

2. *Vulnerability*

Vulnerability mengacu pada kelemahan dalam desain atau implementasi sistem yang dapat dieksploitasi untuk membahayakan keamanan sistem. Ini sering merupakan celah keamanan yang memungkinkan *attacker* memasuki sistem dengan melewati otentikasi pengguna. Adanya *vulnerability* dalam jaringan dan sistem dapat memberikan beberapa dampak seperti: situs web atau aplikasi dapat mengekspos informasi khusus sistem; mencegah pengguna mengakses layanan situs web atau sumber daya lainnya; *attacker* dapat memperoleh akses tidak sah

ke sistem, jaringan, data, atau aplikasi; menyebabkan pengambilan dan transmisi data sensitif secara tidak sah; memungkinkan *attacker* tetap tidak terdeteksi bahkan setelah melakukan serangan; serta dapat memudahkan untuk menginfeksi dan menyebarkan *virus* dalam jaringan. (Ec-Council, 2021)

3. *Attack*

Berdasarkan buku terbitan Ec-Counsil (2021), *attacker* umumnya memiliki motif (sasaran), dan tujuan di balik serangan keamanan informasi mereka. Motif berasal dari gagasan bahwa sistem target menyimpan atau memproses sesuatu yang berharga, yang mengarah pada *threat* serangan terhadap sistem. Tujuan serangan mungkin untuk mengganggu operasi bisnis organisasi target, mencuri informasi berharga demi rasa ingin tahu, atau bahkan untuk membalas dendam. Oleh karena itu, motif atau tujuan ini bergantung pada keadaan pikiran *attacker*, alasan mereka melakukan aktivitas tersebut, serta sumber daya dan kemampuan mereka.

Attacks* = *Motive* (*Goal*) + *Method* + *Vulnerability

Setelah *attacker* menentukan tujuan mereka, mereka dapat menggunakan berbagai tool, teknik serangan, dan metode untuk mengeksploitasi *vulnerability* dalam sistem komputer atau kebijakan dan kontrol keamanan.

Dari buku Ec-Council (2021), serangan keamanan diklasifikasikan menjadi lima kategori:

i. Serangan pasif melibatkan penyadapan dan pemantauan *traffic* jaringan dan aliran data pada jaringan target dan tidak merusak data. Serangan ini sangat sulit dideteksi karena *attacker* tidak memiliki interaksi aktif dengan sistem atau jaringan target.
ii. Serangan aktif merusak data dalam transit atau mengganggu komunikasi atau layanan antar sistem untuk melakukan *bypass* atau membobol sistem yang aman. *Attacker* meluncurkan serangan pada sistem atau jaringan target dengan mengirimkan *traffic* secara aktif yang dapat dideteksi.
iii. Serangan *Close-in* dilakukan saat *attacker* berada di dekat *proximity* fisik

dengan sistem atau jaringan target untuk mengumpulkan, modifikasi informasi atau mengganggu aksesnya.

iv. Serangan orang dalam dilakukan oleh orang terpercaya yang memiliki akses fisik ke aset kritis target. Orang dalam dapat dengan mudah melewati aturan keamanan, merusak sumber daya berharga, dan mengakses informasi sensitif.

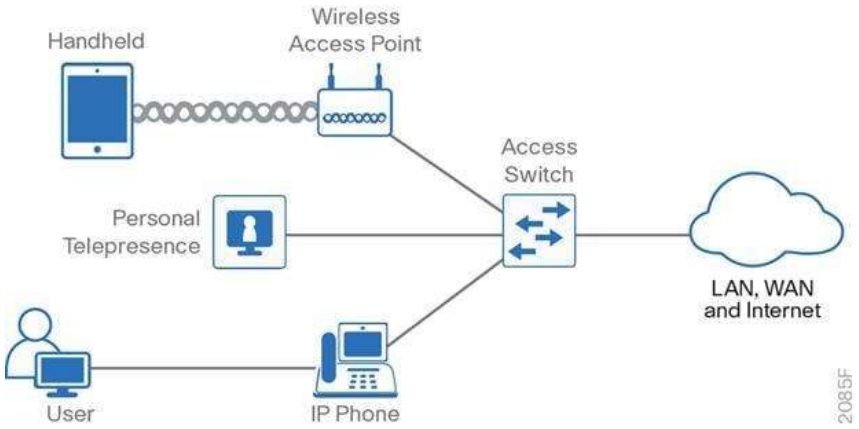
v. Serangan distribusi terjadi ketika *attacker* mengutak-atik *hardware* atau *software* sebelum instalasi.

2.2.2 *Wireless Network*

1. Wi-Fi

Wireless Fidelity (Wi-Fi) adalah bagian dari *Institute of Electrical and Electronics Engineers* (IEEE) 802.11 standar jaringan *wireless*. Teknologi ini menggunakan gelombang radio atau *microwave* untuk memungkinkan perangkat elektronik bertukar data atau terhubung ke *internet*. Banyak perangkat seperti komputer pribadi, laptop, kamera digital, smartphone, dan apa pun yang mendukung teknologi Wi-Fi.

Wi-Fi beroperasi di pita frekuensi antara 2,4 GHz dan 5 GHz. Jaringan Wi-Fi menggunakan gelombang radio untuk mengirimkan sinyal melalui jaringan. Untuk tujuan ini, komputer harus memiliki adaptor *wireless* untuk menerjemahkan data menjadi sinyal radio dan meneruskannya melalui antena dan *router*. Di sinilah pesan diterjemahkan, dan data dikirim ke internet atau melalui jaringan lain. Hotspot adalah area yang memiliki ketersediaan Wi-Fi, di mana pengguna dapat mengaktifkan Wi-Fi di perangkat mereka dan terhubung ke internet melalui *hotspot*. (Ec-Council, 2021)



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

Gambar 1 LAN dengan WLAN (Wi-Fi)

2. Jenis-jenis *Wireless Encryption*

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*.

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*.

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.

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.

2.2.3 *Network-level Attack*

Attacker menggunakan berbagai strategi serangan untuk membahayakan keamanan jaringan, yang berpotensi menyebabkan gangguan, kerusakan, dan

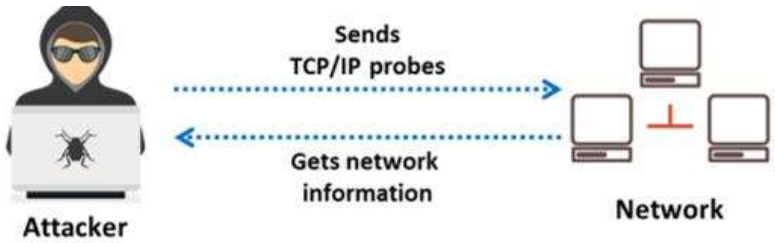
kerugian bagi organisasi dan individu. Adapun berikut yang merupakan jenis-jenis serangan pada tingkat jaringan.

a. Serangan *Reconnaissance*

Dalam serangan *reconnaissance*, *attacker* berusaha untuk mendapatkan semua informasi yang mungkin tentang jaringan target, termasuk sistem informasi, layanan, dan *vulnerability* yang mungkin ada di jaringan. *Attacker* dapat menggunakan teknik berikut untuk mengumpulkan informasi jaringan tentang target: *Social Engineering, Port Scanning*, DNS *Footprinting*, dan *Ping Sweeping*. Tujuan utama serangan *reconnaissance* termasuk mengumpulkan informasi jaringan target, informasi sistem, dan informasi organisasi.

b. *Network Scanning*

Network Scanning digunakan untuk mengidentifikasi *host*, *port*, dan layanan dalam jaringan. *Network Scanning* juga digunakan untuk menemukan komputer aktif dalam jaringan dan mengidentifikasi OS yang berjalan pada komputer target. Dalam proses *scanning*, *attacker* mencoba mengumpulkan informasi, termasuk *address* IP tertentu yang dapat diakses melalui jaringan, OS dan arsitektur sistem target, dan *port* beserta layanannya masing-masing yang berjalan di setiap komputer.



Sumber: Ec-Council, 2021

Gambar 2 *Network scanning attack*

Dalam fase *scanning attack*, *attacker* mencoba menemukan berbagai cara untuk menyusup ke sistem target. *Attacker* juga mencoba menemukan lebih banyak informasi tentang sistem target untuk menentukan adanya penyimpangan konfigurasi. *Attacker* kemudian menggunakan informasi yang diperoleh untuk

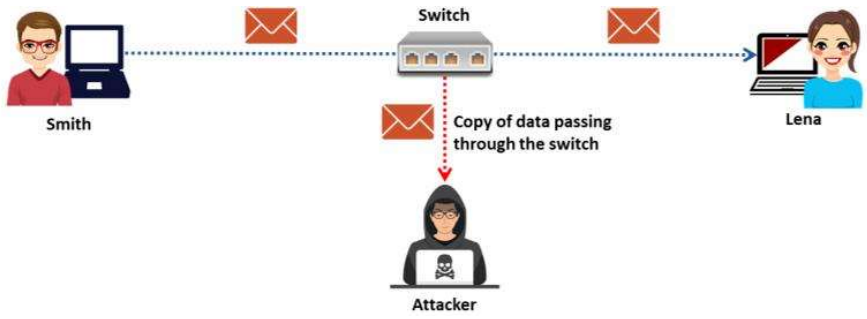
mengembangkan strategi serangan.

c. DNS *Footprinting*

DNS *footprinting* mengungkapkan informasi tentang data zona DNS. Data zona DNS termasuk nama domain DNS, nama komputer, *address* IP, dan banyak lagi informasi tentang jaringan. *Attacker* menggunakan informasi DNS untuk menentukan *host* kunci dalam jaringan dan kemudian melakukan serangan *social engineering* untuk mengumpulkan lebih banyak informasi.

d. Packet Sniffing

Packet sniffing adalah proses memonitor dan menangkap semua paket data yang melewati jaringan tertentu menggunakan aplikasi perangkat lunak atau perangkat keras.



Sumber: Ec-Council, 2021

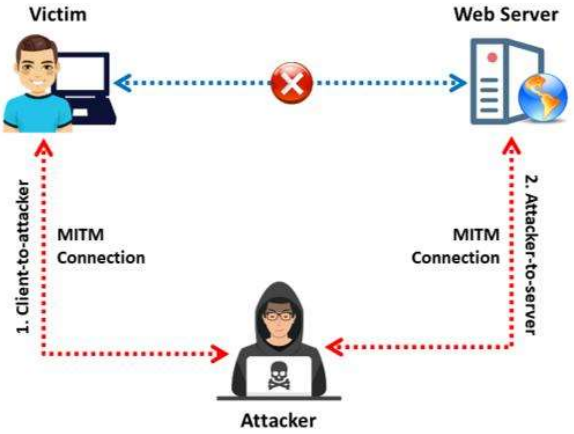
Gambar 3 *Packet sniffing attack*

Program *packet sniffing* (juga dikenal sebagai *sniffer*) dapat menangkap paket data hanya dari dalam *subnet* tertentu, yang berarti bahwa program tersebut tidak dapat *sniffing* paket dari jaringan lain. Seringkali, laptop adapun dapat terhubung ke jaringan dan mendapatkan akses ke sana.

e. Serangan *Man-in-the-Middle*

Serangan *man-in-the-middle* (MITM) digunakan untuk mengganggu koneksi yang ada antara sistem dan untuk mencegat pesan yang sedang dikirim. Dalam serangan ini, *attacker* menggunakan teknik yang berbeda dan membagi koneksi

TCP menjadi dua: koneksi klien ke *attacker* dan koneksi *attacker* ke server. Setelah penyadapan koneksi TCP berhasil, *attacker* dapat membaca, memodifikasi, dan memasukkan data palsu ke dalam komunikasi yang disadap. Dalam kasus transaksi HTTP, koneksi TCP antara klien dan server adalah targetnya.

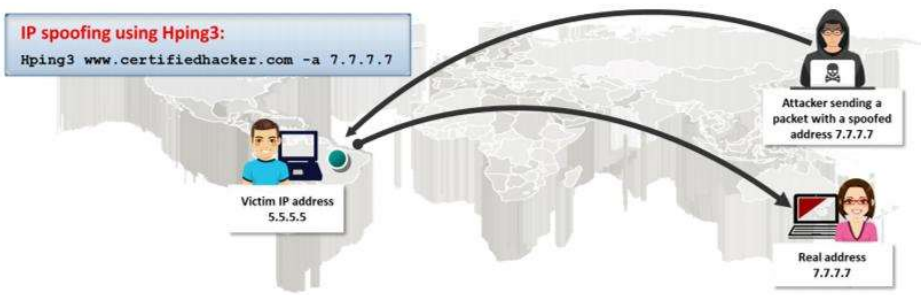


Sumber: Ec-Council, 2021

Gambar 4 *Man-in-the-middle attack*

f. IP *Address Spoofing*

Spoofing address IP adalah teknik pembajakan di mana *attacker* memperoleh *address* IP komputer, mengubah header paket, dan mengirimkan paket permintaan ke mesin target, berpura-pura menjadi *host* yang sah. Paket tampaknya dikirim dari mesin yang sah tetapi sebenarnya dikirim dari mesin *attacker*, sementara IP *address machine*-nya disembunyikan. Ketika korban membalas ke *address* tersebut, itu akan kembali ke *address* palsu dan bukan ke *address* asli *attacker*.



Sumber: Ec-Council, 2021

Gambar 5 IP *address spoofing*

g. *Password Cracking*

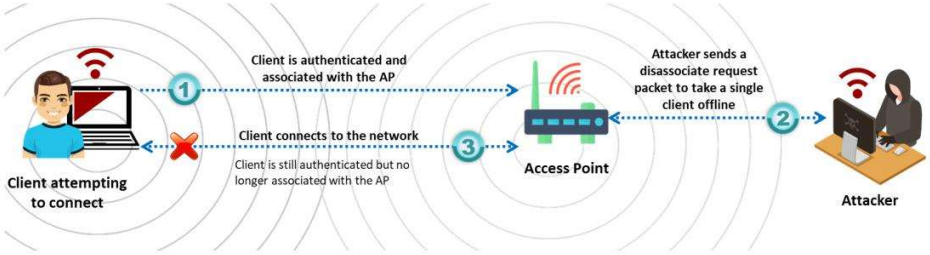
Peretasan sering kali dimulai dengan upaya peretasan *password*. *Password cracking* adalah proses pemulihan *password* dari data yang dikirimkan oleh sistem komputer atau dari data yang tersimpan di dalamnya. Tujuan meretas *password* mungkin untuk membantu pengguna memulihkan *password* yang terlupakan atau hilang, atau sebagai tindakan pencegahan oleh administrator sistem untuk memeriksa *password* yang mudah dipecahkan, atau untuk digunakan oleh *attacker* untuk mendapatkan akses sistem yang tidak sah. Berikut klasifikasi dari serangan ini.

1) *Dictionary Attack*, file *dictionary* dibuat untuk serangan ini yang berisi beberapa kata yang umum digunakan sebagai *password*. Program akan menggunakan setiap kata dalam *dictionary* sampai menemukan *password*.
2) *Brute-Force Attack*, di sini *attacker* mencoba kombinasi karakter sampai *password* ditembus. *Brute-force attack* menguji semua kemungkinan *key* dalam memulihkan *plaintext* yang digunakan untuk menghasilkan *ciphertext.*
3) *Hybrid Attack*, menggunakan *dictionary attack* untuk *common word*, phrases, and character substitutions, yang dikombinasikan *brute force attack* untuk mencoba semua kemungkinan kombinasi karakter.
4) *Rainbow Table Attack*, dengan *precomputed table* yang berisi *hash* dari berbagai *password* untuk menemukan *hash* pada tabel yang cocok dengan *hash target password* .
5) WPA/WPA2 *Cracking*, menargetkan *wireless network security protocol* (WPA/WPA2) untuk mendapatkan akses ke *network* dengan *cracking password*. Diperlukan *capturing network traffic* dan *tool* seperti Aircrack-ng untuk *decrypt password*.

h. Denial-of-Service

Jaringan *wireless* rentan terhadap DoS *attack* karena *physical*, data-link, dan *network layer*. Serangan *wireless* DoS mencakup *disassociation attack* dan *deauthentication attack*. Pada *disassociation attack*, *attacker* mengakibatkan *victim unavailable* terhadap *wireless device* dengan mengganggu koneksi antara

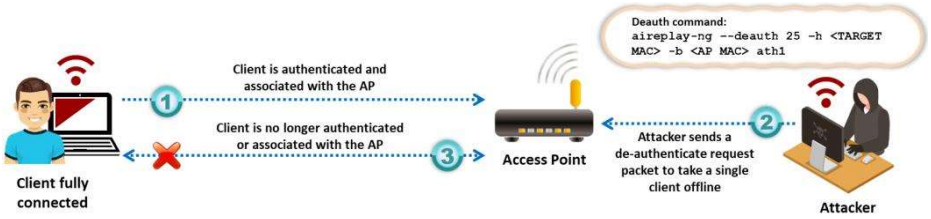
AP dengan *client*.



Sumber: Ec-Council, 2021

Gambar 6 *Disassociation attack*

Untuk *deauthentication attack*, *attacker* menyibukkan *station* dengan mem-*forget deauthenticate* atau *disassociate* sehingga *user* ter-*disconnect* dari AP.



Sumber: Ec-Council, 2021

Gambar 7 *Deauthentication attack*

2.2.4 *Network Security Assessment*

1. *Vulnerability Assessment*

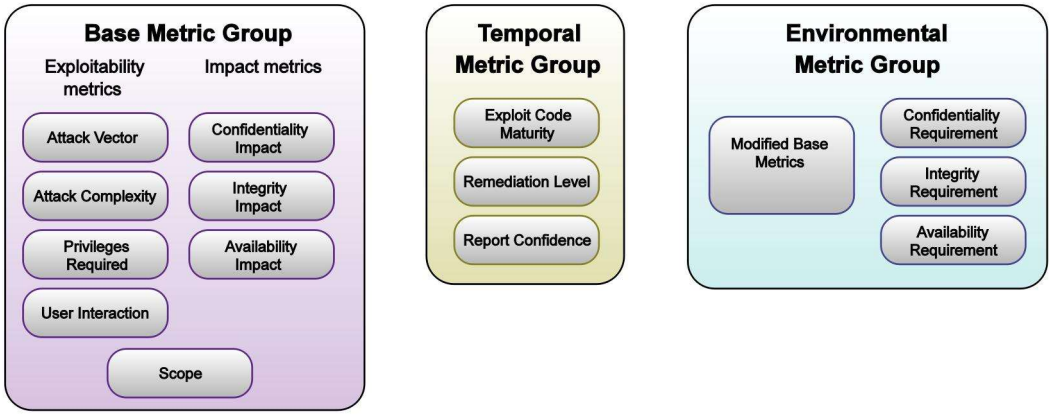
Vulnerability Assessment adalah pemeriksaan mendalam terhadap kemampuan sistem atau aplikasi, termasuk prosedur dan kontrol keamanan saat ini, untuk menahan eksploitasi. Dilakukan *scan* jaringan untuk mengetahui kelemahan keamanan, dan mengenali, mengukur, serta mengklasifikasikan *vulnerability* keamanan dalam sistem komputer, jaringan, dan saluran komunikasi. Ini mengidentifikasi, mengukur, dan memberi peringkat kemungkinan *vulnerability* terhadap *threat* dalam suatu sistem. (Ec-Council, 2021)

Tulisan Wyliey and Crawle (2020) yang menyatakan bahwa, *vulnerability scanning* sering kali merupakan bagian dari pentest, tetapi itu tidak diperlukan. *Pentester* dapat secara manual menemukan *vulnerability* tanpa menggunakan

vulnerability scanning. *Vulnerability scanning* sering kali merupakan peran pekerjaan dalam program manajemen *threat* dan *vulnerability*. *Vulnerability scanning* digunakan untuk mendeteksi *vulnerability* spesifik yang diketahui publik dan yang telah diuji oleh programmer, dan dapat membantu mempercepat proses penemuan *vulnerability*. *Vulnerability scanning* berulang yang dijadwalkan harus menjadi bagian dari program manajemen *threat* dan *vulnerability*. *Vulnerability scanning* adalah *tool* penting dalam *pentester*, dan salah satu langkah pertama dalam *pentest*.

Biasanya, *tool vulnerability scanning* mencari segmen jaringan untuk perangkat yang mendukung IP dan menghitung sistem, sistem operasi, dan aplikasi untuk mengidentifikasi *vulnerability* akibat kelalaian vendor, aktivitas administrasi sistem atau jaringan, atau aktivitas sehari-hari. Perangkat lunak *vulnerability scanning* melakukan *scan* pada komputer berdasarkan indeks *Common Vulnerability and Exposures* (CVE) dan buletin keamanan yang disediakan oleh vendor perangkat lunak.

Vulnerability scoring system and vulnerability database digunakan oleh *security analyst* untuk me-*ranking* sistem informasi vulnerability dan memberikan skor secara keseluruhan dari tingkat keparahan dan risiko dari *vulnerability* yang teridentifikasi. *Vulnerability databases* mengumpulkan dan *maintaining* data berbagai *vulnerability* yang ada dalam sistem informasi. *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*). CVSS sendiri dikelola oleh FIRST.Org, Inc. (FIRST) yang merupakan organisasi non-*profit* US dengan misi membantu tim respons insiden keamanan komputer di seluruh dunia. Merujuk pada *website* FIRST, bahwa CVSS memiliki 3 jenis metrik yaitu, *base*, *temporal*, dan *environmental*.



Sumber: https://www.first.org/cvss/v3.1/specification-document

Gambar 8 Tiga metrik dalam CVSS

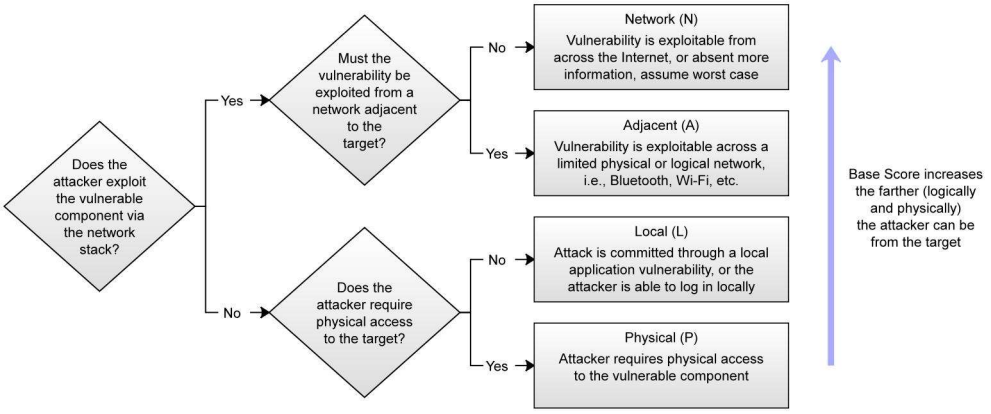
Base metric terdiri dari dua set metrik, metrik *Exploitability* yang mencerminkan kemudahan dalam mengeksploitasi *vulnerability* dan metrik *Impact* mengenai konsekuensi dari keberhasilan eksploitasi. Potensi untuk mengukur dampak *vulnerability* diperkenalkan dengan metrik S*cope*. *Base metric* kemudian disempurnakan dengan *temporal metric* dan *environment metric*. Penskoran dengan kedua metrik tersebut tidak harus digunakan tetapi direkomendasikan untuk skor yang lebih akurat. Skor *Base* menunjukkkan tingkat keparahan *vulnerability* sesuai dengan karakteristik yang konstan dari waktu ke waktu dan mengasumsikan dampak *worst case* di berbagai lingkungan yang disebarkan. Metrik *Temporal* menyesuaikan Tingkat keparahan *Base* dari *vulnerability* berdasarkan faktor-faktor yang berubah dari waktu ke waktu, seperti *avalability* kode eksploitasi. Metrik *Environmental* menyesuaikan Tingkat keparahan *Base* dan *Temporal* ke lingkungan komputasi tertentu yang mempertimbangkan faktor-faktor seperti adanya mitigasi di lingkungan tersebut. Akan ada banyak kemungkinan yang berbeda dalam menilai *vulnerability* namun *vulnerability scoring* memang dimaksudkan untuk bersifat *agnostic* bagi individu maupun organisasinya. Berikut yang termasuk dalam metrik *Exploitability*.

Tabel 2 *Attack Vector* (AV)

Metrik	Keterangan
Network (N)	*Vulnerability* yang berkaitan dengan *network stack* yang memungkinkan penyerangan melalui *internet*. Kerentanan ini dianggap sebagai serangan yang dapat dieksploitasi pada tingkat protokol satu atau lebih jaringan yang dilewati (misalnya, di satu atau

Metrik	Keterangan
	lebih *router*). Contoh serangan jaringan adalah penyerang yang menyebabkan DoS dengan mengirimkan paket TCP yang dibuat khusus melalui WAN.
Adjacent (A)	Serangan *vulnerability* ini terbatas pada tingkat protokol ke topologi yang berdekatan berarti serangan harus diluncurkan dari *shared physical network* (Bluetooth atau IEEE 802.11) atau *logical network* (subnet IP lokal), atau dari dalam domain administratif yang aman atau terbatas (MPLS, VPN aman ke zona jaringan administratif). Salah satu contoh serangan yang berdekatan adalah serangan ARP (IPv4) yang menyebabkan DoS pada segmen LAN lokal.
Local (L)	Penyerang mengeksploitasi *vulnerability* dengan mengakses sistem target secara lokal (misalnya *keyboard*, konsol), atau dari jarak jauh (SSH); atau penyerang 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 penyerang untuk secara fisik memanipulasi *vulnerable* komponen. Interaksi fisik mungkin singkat (mis., *evil maid attack*) 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. Contoh lain termasuk serangan periferal melalui FireWire/USB *Direct Memory Access* (DMA).

Sumber: https://www.first.org/cvss/v3.1/specification-document



Sumber: https://www.first.org/cvss/v3.1/user-guide

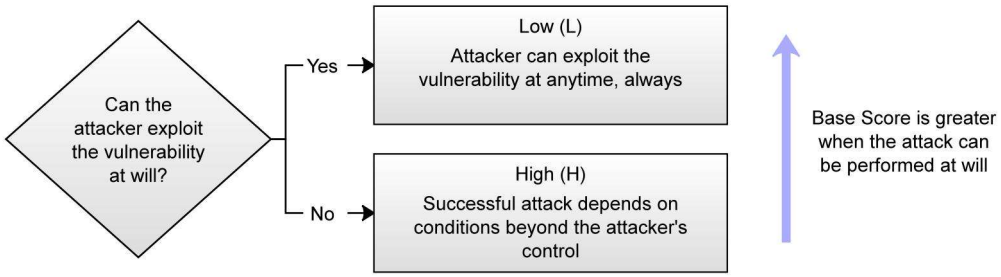
Gambar 9 Rubrik penskoran *Attack Vector* (AV)

Jika serangan bisa melalui WAN atau di luar domain jaringan administratif maka dikategorikan sebagai metrik *Network*. Metrik *Network* juga harus digunakan meskipun penyerang harus berada dalam *intranet* yang sama, seperti penyerang hanya bisa mengeksploitasi *vulnerability* dari dalam jaringan perusahaan.

Tabel 3 *Attack Complexity* (AC)

Metrik	Keterangan
Low (L)	Tidak adanya kondisi khusus yang harus diatur sebelum mengeksekusi serangan. Penyerang selalu berhasil jika melakukan serangan yang sama.
High (H)	Serangan yang berhasil tergantung pada kondisi di luar kendali penyerang, misalnya penyerang harus menginjeksikan diri ke *logical network* antara target dan *resource* yang akan dibuat modifikasi pada *network communication* (*man in the middle*).

Sumber: https://www.first.org/cvss/v3.1/specification-document



Sumber: https://www.first.org/cvss/v3.1/user-guide

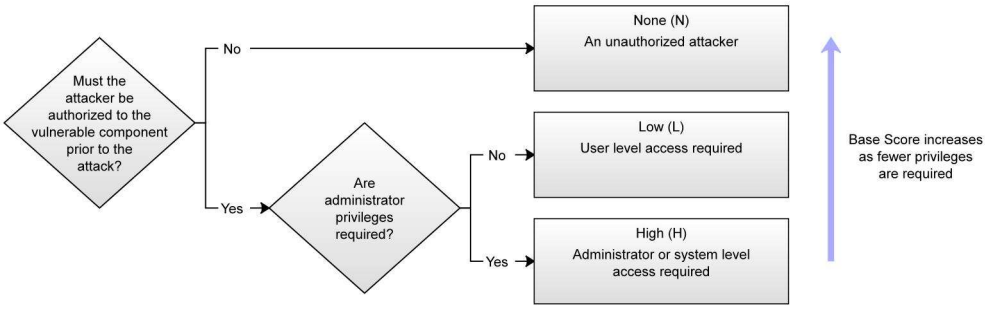
Gambar 10 Rubrik penskoran *Attack Complexity* (AC)

Tabel 4 *Privileges Required* (PR)

Metrik	Keterangan
None (N)	Penyerang tidak memerlukan akses apa pun ke pengaturan ataupun file dari kerentanan sistem.
Low (L)	Penyerang memerlukan *privilege* yang normalnya dapat memengaruhi pengaturan dan file *user*. Dengan *low-privilege*, penyerang hanya bisa mengakses *non-sensitive resource*.
High (H)	Penyerang perlu *privilege* yang bisa mengontrol (administratif) kerentanan untuk mengakses keseluruhan pengaturan dan file.

Sumber: https://www.first.org/cvss/v3.1/specification-document

Penskoran ini biasanya dikategorikan *none* untuk *vulnerability* yang tidak memerlukan *social engineering*.



Sumber: https://www.first.org/cvss/v3.1/user-guide

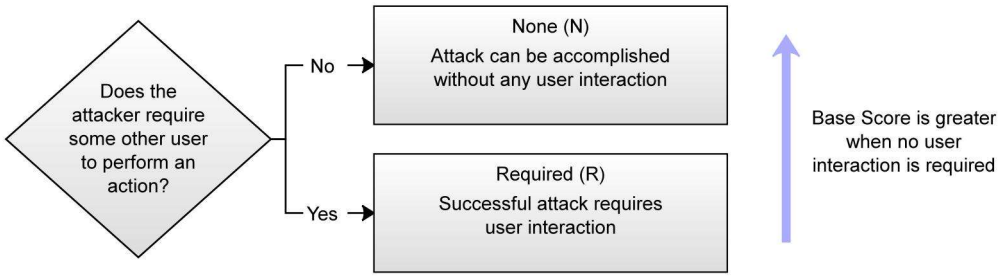
Gambar 11 Rubrik penskoran *Privileges Required* (PR)

Tabel 5 *User Interaction* (UI)

Metrik	Keterangan
None (N)	*Vulnerability* dapat dieksploitasi tanpa interaksi dari *user*.
Required (R)	Keberhasilan eksploitasi memerlukan *user* dalam melakukan tindakan sebelum *vulnerability* dieksploitasi. Misalnya, hanya bisa dilakukan selama *system administrator* melakukan *install* aplikasi.

Sumber: https://www.first.org/cvss/v3.1/specification-document

Metrik *Scope* menilai apakah *vulnerability* suatu komponen memengaruhi *resource* komponen di luar cakupan keamanannya.



Sumber: https://www.first.org/cvss/v3.1/user-guide

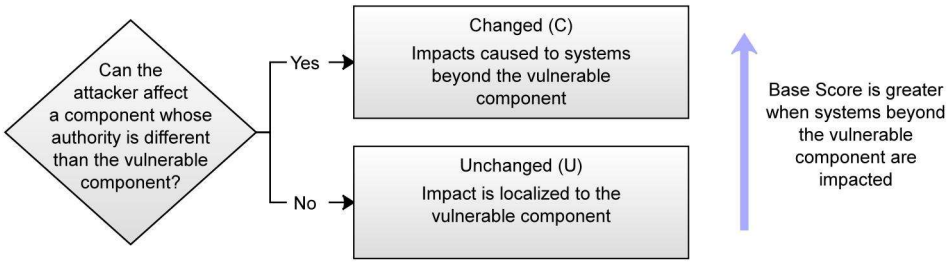
Gambar 12 Rubrik penskoran *User Interaction* (UI)

Tabel 6 *Scope*

Metrik	Keterangan
Unchanged (U)	*Vulnerability* yang dieksploitasi hanya dapat memengaruhi *resource* yang dikelola oleh *security authority* yang sama. Komponen yang rentan dengan yang terkena *impact* dalam *security authority* yang sama.
Changed (C)	*Vulnerability* yang dieksploitasi dapat memengaruhi *resource* di luar cakupan keamanan yang dikelola oleh *security authority* komponen yang rentan. Dalam hal ini, komponen yang rentan dan komponen yang terkena *impact* berbeda dan dikelola oleh *security authority* yang berbeda.

Sumber: https://www.first.org/cvss/v3.1/specification-document

Metrik *Impact* menilai dampak dari *vulnerability* yang berhasil dieksploitasi untuk komponen yang paling rentan.



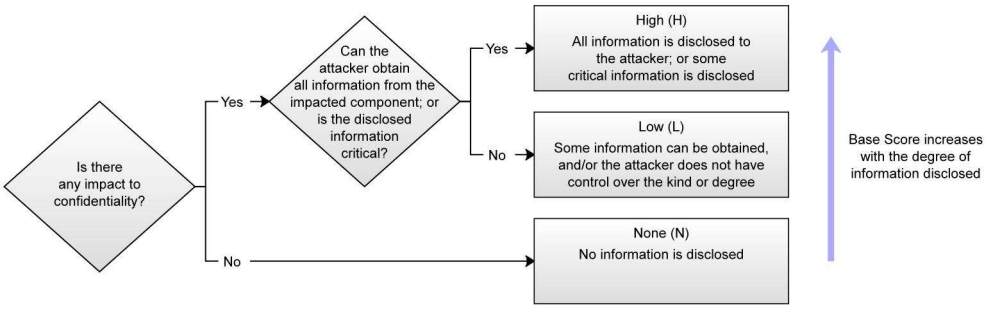
Sumber: https://www.first.org/cvss/v3.1/user-guide

Gambar 13 Rubrik penskoran *Scope*

Tabel 7 *Confidentiality* (C)

Metrik	Keterangan
High (H)	Akses ke beberapa informasi terbatas, tetapi informasi yang diungkapkan memberikan dampak serius. Misalnya, penyerang mencuri *password* administrator, atau *private encryption key* dari *web server*.
Low (L)	Akses ke beberapa informasi terbatas, penyerang tidak memiliki kendali atas informasi apa yang diperoleh, atau jenis kerugian dibatasi. Pengungkapan informasi tidak menyebabkan kerugian serius terhadap komponen yang terkena dampak.
None (N)	Tidak ada pengungkapan kerahasiaan pada komponen yang terkena dampak.

Sumber: https://www.first.org/cvss/v3.1/specification-document



Sumber: https://www.first.org/cvss/v3.1/user-guide

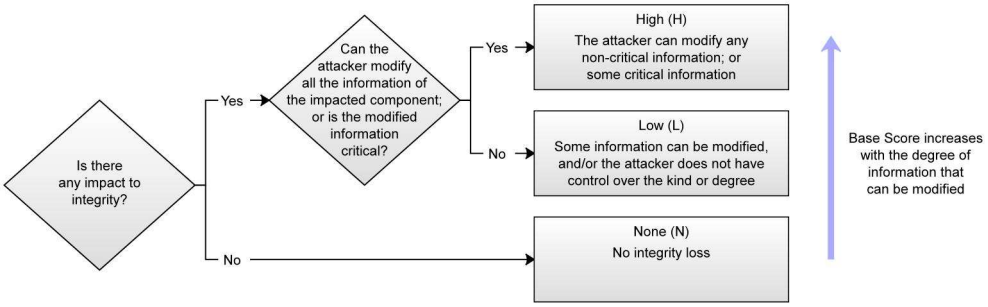
Gambar 14 Rubrik penskoran *Confidentiality* (C)

Tabel 8 *Integrity* (I)

Metrik	Keterangan
High (H)	Misalnya, penyerang dapat mengubah sebagian/semua file yang dilindungi oleh komponen yang terkena dampak. Hanya beberapa file yang dapat dimodifikasi, tetapi modifikasi *malicious* akan menimbulkan konsekuensi serius pada komponen yang terkena dampak.
Low (L)	Modifikasi data dimungkinkan, tetapi penyerang tidak memiliki kendali atas konsekuensi modifikasi, atau jumlah modifikasi dibatasi. Modifikasi data tidak berdampak serius pada komponen yang terkena

Metrik	Keterangan
	dampak.
None (N)	Tidak ada kehilangan integritas dalam komponen yang terkena dampak.

Sumber: https://www.first.org/cvss/v3.1/specification-document



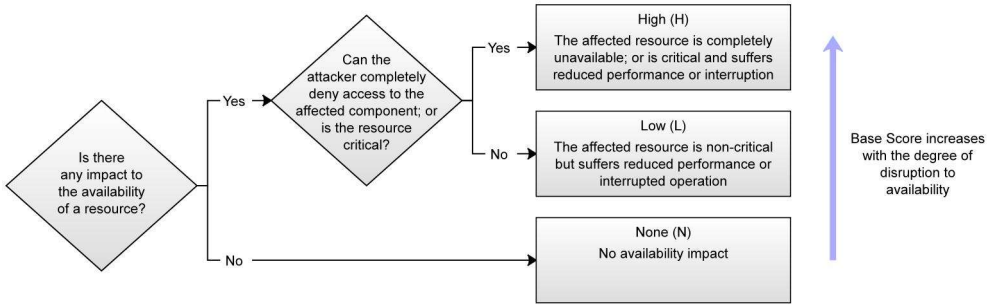
Sumber: https://www.first.org/cvss/v3.1/user-guide

Gambar 15 Rubrik penskoran *Integrity* (I)

Tabel 9 *Availability* (A)

Metrik	Keterangan
High (H)	Kerugian ini baik berkelanjutan (sementara penyerang terus memberikan serangan) atau persisten (kondisi tetap ada bahkan setelah serangan selesai). Penyerang memiliki kemampuan untuk menolak beberapa *availability*, tetapi menghadirkan konsekuensi serius terhadap komponen yang terkena dampak (mis., penyerang tidak dapat mengganggu koneksi yang ada, namun dapat mencegah koneksi baru; penyerang dapat berulang kali mengeksploitasi *vulnerability*, dalam setiap serangan yang berhasil, hanya membocorkan sejumlah kecil memori, tetapi setelah eksploitasi berulang kali menyebabkan layanan menjadi tidak tersedia sama sekali).
Low (L)	Kinerja berkurang atau ada gangguan dalam ketersediaan *resource*. Bahkan jika eksploitasi dilakukan berulang kali, penyerang tidak memiliki kemampuan untuk sepenuhnya menolak layanan terhadap *legitimate user*. *Resource* dalam komponen yang terkena dampak tersedia sebagian sepanjang waktu, atau hanya tersedia sepenuhnya pada sebagian waktu, tetapi secara keseluruhan tidak ada konsekuensi langsung dan serius terhadap komponen yang terkena dampak.
None (N)	Tidak ada dampak terhadap *availability* pada komponen yang terkena dampak.

Sumber: https://www.first.org/cvss/v3.1/specification-document



Sumber: https://www.first.org/cvss/v3.1/user-guide

Gambar 16 Rubrik penskoran *Availability* (A)

Setiap *metric* memiliki *numerical value* masing-masing untuk menilai *seveity level* dari suatu sistem yang dibuat penilaiannya.

Tabel 10 *Numerical value* tiap metrik

Metrik	***Metric Value***	***Numerical Value***
AV	*Network*	0.85
	Adjacent	0.62
	Local	0.55
	Physical	0.2
AC	*Low*	0.77
	High	0.44
PR	*None*	0.85
	Low	0.62 (C: 0.68)
	High	0.27 (C: 0.5)
UI	*None*	0.85
	Required	0.62
C/I/A	*High*	0.56
	Low	0.22
	None	0

Sumber: https://www.first.org/cvss/v3.1/specification-document

Secara keseluruhan skor penilaian *severity level* berdasarkan perhitungan kalkulator CVSS dapat diskalakan dengan *rating* kualitatif seperti dalam tabel berikut.

Tabel 11 Skala CVSS v3.1

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/v3.1/specification-document

2. *Penetration Testing*

Penetration testing, juga disebut *pen testing*, jenis pengujian keamanan yang mengevaluasi kemampuan organisasi untuk melindungi infrastrukturnya seperti jaringan, aplikasi, sistem, dan pengguna dari *threat* eksternal maupun internal. Hal ini melibatkan evaluasi aktif keamanan infrastruktur organisasi dengan melakukan simulasi serangan yang serupa dengan yang dilakukan oleh *attacker* nyata. Selama *penetration testing*, langkah-langkah keamanan secara aktif dianalisis untuk kelemahan desain, kelemahan teknis, dan *vulnerability*.

Ada tiga fase dalam *penetration testing*: fase *pre-attack*, serangan, dan *post-attack*.

A. Fase *pre-attack*

Fase ini berfokus pada pengumpulan informasi sebanyak mungkin tentang target. Informasi dapat dikumpulkan secara invasif, misalnya dengan pengintaian pasif dan aktif, *port*, layanan, dan OS *scanning*, atau dapat dikumpulkan secara noninvasif misalnya dengan meninjau catatan publik.

Dimulai dengan pengintaian pasif dan aktif, penguji mengumpulkan informasi sebanyak mungkin tentang perusahaan target. Sebagian besar informasi yang bocor terkait dengan topologi jaringan dan jenis layanan yang berjalan di dalamnya. Penguji dapat menggunakan informasi ini untuk sementara memetakan jaringan untuk merencanakan strategi serangan yang lebih terkoordinasi.

Pengintaian pasif melibatkan hal-hal berikut:

a. Pemetaan struktur direktori server web dan server FTP.
b. Mengumpulkan intelijen kompetitif.
c. Menentukan nilai infrastruktur yang berinteraksi dengan web.
d. Mengambil informasi pendaftaran jaringan dari database Whois dan situs keuangan.
e. Menentukan jangkauan produk dan penawaran layanan perusahaan target yang tersedia secara online atau dapat diminta secara offline.
f. Penyaringan dokumen, yang mengacu pada pengumpulan informasi semata-mata dari materi yang diterbitkan.
g. *Social Engineering* dapat dilakukan dengan mengidentifikasi saluran (seseorang yang dapat ditargetkan dengan mudah berdasarkan informasi yang diperoleh tentang personel) dan membuat profil mereka.

Dalam pengintaian aktif, proses pengumpulan informasi melanggar batas wilayah target. Di sini, pelaku dapat mengirimkan probe ke target dalam bentuk *port* scan, *network* sweeps, enumeration share dan *user* account, dan sebagainya. Penguji dapat mengadopsi teknik seperti *social engineering* dan menggunakan *tool* yang bisa otomatis melakukan pemindai dan *sniffer*.

B. Fase Attack

Informasi yang dikumpulkan dalam fase *pre-attack* membentuk dasar dari strategi serangan. Selama fase serangan, strategi serangan dikembangkan dan dieksekusi. Fase serangan melibatkan kompromi yang sebenarnya dari target. Penguji dapat mengeksploitasi *vulnerability* yang ditemukan selama fase *pre-attack* atau menggunakan celah keamanan seperti kebijakan keamanan yang lemah untuk mendapatkan akses ke sistem. Poin penting di sini adalah bahwa sementara penguji hanya membutuhkan satu *port* masuk, organisasi harus mempertahankan beberapa. Begitu masuk, penguji dapat meningkatkan hak istimewa mereka, memasang *backdoor* untuk mempertahankan akses ke sistem, dan mengeksploitasi untuk mencapai tujuan mereka.

C. Fase *post-attack*

Fase *post-attack* adalah bagian penting dari proses pengujian, karena penguji perlu memulihkan jaringan ke keadaan semula. Ini melibatkan pembersihan proses pengujian, menghapus *vulnerability* yang dibuat (bukan *vulnerability* yang ada pada awalnya), eksploitasi yang dibuat, dan seterusnya, hingga semua sistem yang diuji dikembalikan ke statusnya sebelum pengujian.

Tujuan dari tes ini adalah untuk menunjukkan di mana keamanan gagal. Kecuali ada penskalaan perjanjian uji penetrasi, di mana penguji diberi tanggung jawab untuk memperbaiki postur keamanan sistem, fase ini menyelesaikan proses *penetration testing*. Aktivitas dalam fase ini meliputi hal berikut.

a. Membalikkan semua manipulasi file dan pengaturan yang dilakukan selama pengujian.
b. Membalikkan semua perubahan pada hak istimewa dan pengaturan pengguna.
c. Pemetaan status jaringan.
d. Mendokumentasikan dan menangkap semua *log* yang terdaftar selama pengujian.

Penting untuk *penetration testing* mendokumentasikan semua aktivitas yang dilakukan dan mencatat semua pengamatan dan hasil sehingga pengujian dapat diulang dan diverifikasi dari keamanan yang diberikan organisasi.