BAB 2
LANDASAN TEORI

2.1 Koperasi

Koperasi adalah entitas bisnis yang didirikan atas dasar kerja sama dan kebersamaan antaranggotanya. Dalam struktur koperasi, setiap anggota memiliki peran aktif dalam pengambilan keputusan dan manajemen usaha. Anggota koperasi berpartisipasi secara aktif dalam kegiatan dan keputusan bisnis, serta berbagi keuntungan dan manfaat lainnya yang dihasilkan oleh koperasi. Sementara itu, menurut Kamus Besar Bahasa Indonesia (KBBI), koperasi adalah perserikatan yang bertujuan memenuhi keperluan para anggotanya dengan cara menjual barang keperluan sehari-hari dengan harga murah (tidak bermaksud mencari untung).

Berdasarkan Undang-Undang Nomor 25 Tahun 1992, koperasi adalah suatu badan usaha, yang dibentuk oleh anggota-anggotanya untuk melakukan kegiatan usaha, menunjang kepentingan ekonomi anggotanya sehingga mencapai kesejahteraan anggotanya.. Asas koperasi yang ditegaskan dalam Pasal 2 UU Nomor 25 Tahun 1992 Tentang Perkoperasian adalah kekeluargaan dan gotong royong. Asas kekeluargaan mengandung makna bahwa koperasi dijalankan dengan semangat persaudaraan dan kebersamaan. Hubungan antara anggota koperasi seharusnya mencerminkan nilai-nilai kekeluargaan, di mana setiap anggota dianggap sebagai bagian dari satu keluarga besar. Asas gotong royong mencerminkan semangat kerjasama dan saling bantu-membantu di antara anggota koperasi. Anggota koperasi bekerja bersama-sama untuk mencapai tujuan bersama, berbagi tanggung jawab, dan saling mendukung dalam mengatasi tantangan. Dengan gotong royong, koperasi dapat memaksimalkan potensi kolektif anggotanya untuk mencapai kesejahteraan bersama.

2.2 Profil Koperasi Serba Usaha Postra (KSU Postra)

Koperasi Serba Usaha (KSU) Postra adalah merupakan transformasi dari sebuah koperasi bernama Koperasi Karyawan PT. Pos Soreang (Kopkarpos) yang didirikan tanggal 9 Januari 2004 oleh para karyawan PT. Pos Indonesia Soreang yang beralamat di Jl, Raya Soreang No. 412 Soreang Kabupaten Bandung dan telah

terdaftar di Dinas Koperasi Kabupaten Bandung serta telah mendapatkan pengesahan sebagai badan hukum pada tanggal 28 Oktober 2004.

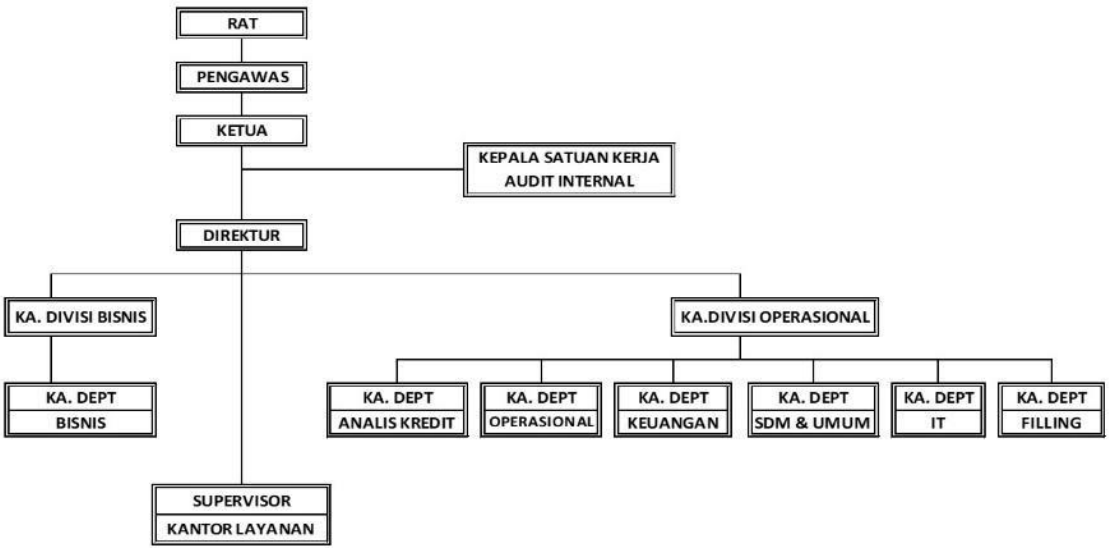
Seiring dengan berjalannya waktu, pengurus dan anggota Kopkarpos Soreang mimiliki keinginan untuk mengembangkan bisnis yang ada, tidak hanya sekedar koperasi simpan saja. Oleh karena itu pada tanggal 9 Januari 2015 dilakukan rapat anggota tahunan yang menghasilkan keputusan untuk mengembangkan koperasi baik dari segi bisnis maupun dari segi keanggotaan dan wilayan kerja.

Untuk mengakomodir keputusan ini, akhirnya dilakukan perubagan AD/ART yang menghasilkan perubahan nama dari Koperasi Karyawan Kantor Pos Soreang 40900 menjadi Koperasi Serba Usaha.

Fokus utama Koperasi Postra adalah memenuhi kebutuhan keuangan para pensiunan PNS, TNI/POLRI, serta karyawan di perusahaan BUMN dan swasta. Dengan pusat operasi di Bandung, koperasi ini telah mengalami pertumbuhan pesat dan telah membuka lebih dari 50 kantor layanan di seluruh kepulauan Jawa dan provinsi Nusa Tenggara Timur.

2.3 Struktur Organisasi Koperasi Serba Usaha Postra

Berikut Struktur Organisasi pada Koperasi Serba Usaha Postra dapat dilihat pada gambar 2.1 berikut:



Gambar 2.1 Struktur Organisasi Postra

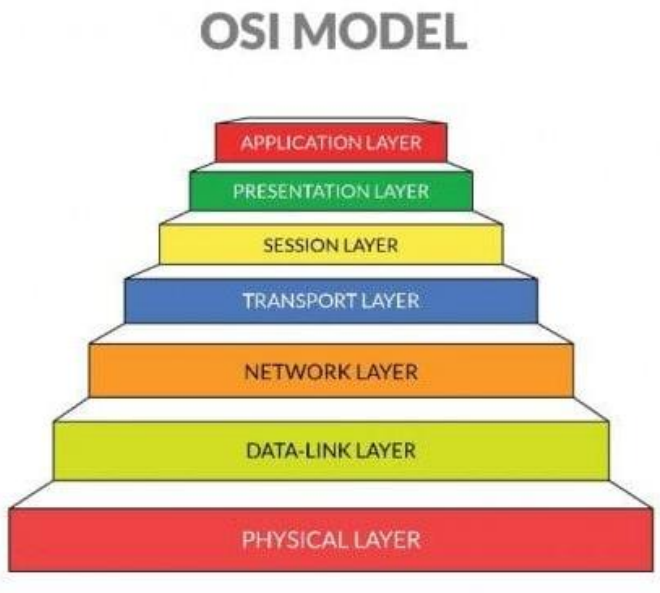
2.4 Sistem Informasi Helpdesk

Sistem Informasi Helpdesk Postra merupakan sistem pengolahan data yang berkaitan dengan proses bisnis di Postra, meliputi data nasabah, data kantor cabang, data pegawai serta sistem penyimpanan data dan dokumen untuk pendukung pengambilan keputusan oleh pengguna menggunakan sistem komputer. Sistem Informasi Helpdesk menyajikan informasi topik dalam bantuan atau kendala di dalam postra. Selain menjadi sumber informasi perusahaan, sistem informasi helpdesk berfungsi menjadi alat interaksi antara pegawai kantor pusat dan pegawai kantor cabang.

2.5 *Open Systems Interconnection* (OSI) Layer

Secara umum, model OSI membagi berbagai fungsi jaringan menjadi tujuh lapisan. Model tujuh lapisan OSI ini dipublikasikan oleh International Organization for Standardization (ISO) dan diperkenalkan pada tahun 1984[6].

Model OSI terdiri atas tujuh lapisan yaitu : *Physical, Data link, Network, TransPort, Session, Presentation, Application* .



Gambar 2.2 OSI Layer

a. Physical Layer

Lapisan ini mengatur masalah kelistrikan, gelombang, medan, serta berbagai prosedur dan fungsi yang terkait dengan koneksi fisik, seperti tegangan, arus listrik, panjang maksimal media transmisi, perubahan fasa, jenis kabel, dan berbagai bentuk antarmuka media transmisi. Contohnya meliputi RS-232, V.35, V.34, I.430, hub, repeater, serat optik, 802.11a/b/g/n, RJ45, Ethernet, NRZI, NRZ, dan B8ZS[6].

b. Data Link Layer (Lapisan Data Link)

Menentukan pengalamatan fisik, pendeteksian error, kontrol aliran data, dan topologi jaringan. Lapisan data link terbagi menjadi dua sub-lapisan, yaitu logical link control (LLC) dan media access control (MAC). LLC mengelola komunikasi seperti pemberitahuan error dan kontrol aliran data, sementara MAC mengatur pengalamatan fisik yang digunakan dalam komunikasi antar-adapter. Lapisan Data Link ini juga mengatur pengiriman data antara antarmuka yang berbeda, misalnya pengiriman data dari Ethernet 802.3 ke High-Level Data Link Control (HDLC) untuk pengiriman data WAN. Contoh dari teknologi yang bekerja di lapisan ini adalah Token Ring, Frame Relay, SDLC, HDLC, ISL, PPP, IEEE 802.2 / 802.3 (Ethernet), FDDI, dan ATM[6].

c. Network Layer (Lapisan Jaringan)

Lapisan ini bertanggung jawab untuk pengendalian dan menentukan jalur (routing) yang akan dilalui oleh data. Lapisan ini menyediakan penentuan rute tujuan, dengan contoh protokol seperti IPX, IP, ICMP, IPsec, ARP, RIP, IGRP, OSPF, dan NBF[6].

d. Trans*Port* Layer (Lapisan Trans*Port*)

Lapisan ini menyediakan protokol komunikasi end-to-end. Ia bertanggung jawab atas "keselamatan data" dan "segmentasi data," termasuk pengaturan kendali aliran data (flow control), deteksi error (error detection), koreksi (correction), urutan data (data sequencing), dan ukuran paket (size of the packet). Contoh protokol pada lapisan ini adalah TCP, SPX, UDP, SCTP, dan IPX[6].

e. Session Layer (Lapisan Sesi)

Lapisan sesi memfasilitasi pengguna untuk menetapkan sesi dengan pengguna lainnya. Lapisan ini bertanggung jawab untuk membuka, mengelola, dan menutup sesi antara aplikasi-aplikasi. Selain mendukung trans*Port*asi data seperti yang dilakukan oleh lapisan trans*Port*, sesi juga menyediakan layanan khusus untuk aplikasi tertentu[6]. Sebuah sesi dapat digunakan untuk memungkinkan pengguna untuk login ke sistem timesharing jarak jauh atau untuk mentransfer file dari satu mesin ke mesin lainnya. Mengatur sesi yang meliputi establishing, maintaining, terminating antar entitas, seperti : SQL,X WINDOW, DNS, NetBIOS, ASP, SCP, OS scheduling, RPC,dll.

f. Presentation Layer (Lapisan Presentasi)

Lapisan presentasi bertugas untuk menyediakan fungsi-fungsi yang diperlukan untuk memastikan interoperabilitas dalam menyelesaikan masalah tertentu. Lapisan ini tidak hanya menyediakan layanan untuk konversi, format, dan enkripsi data, tetapi juga mengelola berbagai format file seperti ASCII, EBCDIC, JPEG, MPEG, TIFF, PICT, MIDI, dan QuickTime[6].

Lapisan presentasi tidak bertujuan untuk mengijinkan pengguna menyelesaikan masalah sendiri. Berbeda dengan lapisan di bawahnya yang hanya bertanggung jawab untuk memindahkan bit dari satu lokasi ke lokasi lainnya, lapisan presentasi memperhatikan tata bahasa (syntax) dan makna (semantik) dari informasi yang dikirimkan.

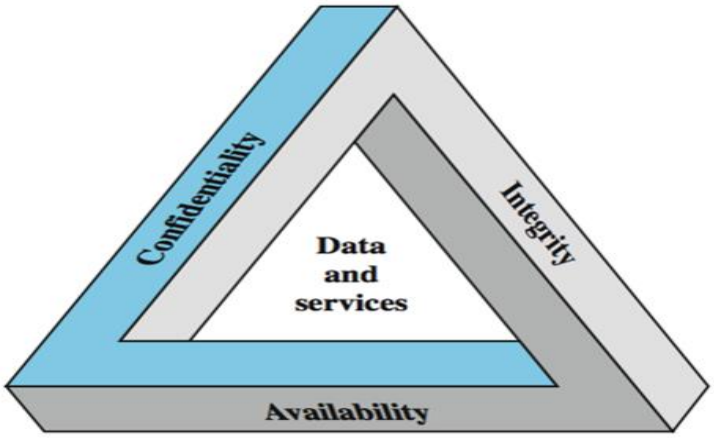
g. Application Layer (Lapisan Aplikasi)

Lapisan ini bertugas memberikan sarana pelayanan langsung ke user, yang berupa aplikasi-aplikasi dan mengadakan komunikasi dari program ke program. Jika kita mencari suatu file dari file server untuk digunakan sebagai aplikasi pengolah kata, maka proses ini bekerja melalui layer ini. Application Layer mengacu pada pelayanan komunikasi pada suatu aplikasi atau user interface. Contoh : NNTP, HTTP, HTTPS, SMTP, SNMP, Telnet, dan FTP[6]. Ini adalah

lapisan yang paling sering diuji, mencakup serangan terhadap aplikasi web dan layanan online. Tes ini melibatkan mencari kelemahan seperti SQL injection, XSS, CSRF, buffer overflow, dan lain-lain.

2.6 Keamanan Sistem Informasi

Keamanan diartikan sebagai tidak adanya bahaya. Istilah bahaya disini dapat diartikan sebagai gangguan, ancaman, kecelakaan, atau hal lain yang tidak diinginkan. Dalam konteks keamanan komputer dijelaskan bahwa suatu sistem dapat dikatakan aman jika sumber daya yang digunakan dan aksesnya sesuai dengan keinginan pengguna dalam segala keadaan[7]. Keamanan informasi terdiri dari 3 aspek penting yaitu confidentiality, integrity, dan availability atau bisa disebut dengan CIA Triad[8]:



Gambar 2.3 Aspek Keamanan Informasi CIA Triad

Diagram diatas menunjukkan bahwa CIA Triad mencakup aspek kerahasiaan (confidentiality), integritas (integrity), dan ketersedian (availability). Berikut adalah penjelasan mengenai ketiga aspek dari CIA Triad:

a. Confidentiality (kerahasiaan) Aspek yang menjamin kerahasiaan data atau informasi, memastikan bahwa informasi hanya dapat diakses oleh orang yang berwenang dan menjamin kerahasiaan data yang dikirim, diterima dan disimpan.
b. Integrity (integritas) Aspek yang menjamin bahwa data tidak dirubah tanpa ada ijin pihak yang berwenang (authorized), harus terjaga keakuratan dan

keutuhan informasi.

c. Availability (ketersediaan) Aspek yang menjamin bahwa data akan tersedia saat dibutuhkan, memastikan user yang berhak dapat menggunakan informasi dan perangkat terkait bilamana diperlukan.

Keamanan informasi merujuk pada upaya menjaga keamanan aset informasi, termasuk perangkat, infrastruktur, dan data baik digital maupun non-digital, untuk memastikan bahwa informasi tersebut tetap rahasia, utuh, dan dapat diakses sesuai kebutuhan. Ini dilakukan melalui implementasi kebijakan, prosedur, dan teknologi yang sesuai dengan standar keamanan. Tiga aspek utama dalam perlindungan informasi adalah menjaga kerahasiaan informasi dari pihak yang tidak berwenang, memastikan integritas informasi untuk mempertahankan kebenaran dan kelengkapan, serta menjaga ketersediaan informasi agar dapat diakses ketika dibutuhkan[9].

2.7 Tipe Ancaman Keamanan Sistem Komputer

Fungsi sistem komputer dapat digunakan sebagai dasar untuk menentukan model tipe ancaman dari suatu sistem komputer. Berdasarkan fungsi sistem komputer sebagai penyedia informasi, ancaman terhadap sistem komputer dikategorikan menjadi empat, yaitu:

1. Interruption adalah ancaman terhadap ketersediaan, di mana informasi atau data yang ada dalam sistem komputer dapat dihancurkan atau dihapus, sehingga tidak lagi tersedia jika dibutuhkan[10].
2. Interception adalah ancaman terhadap kerahasiaan. Informasi dalam sistem dapat disadap oleh pihak yang tidak berhak[10].
3. Modification merupakan ancaman terhadap integritas. Pihak yang tidak berhak dapat menyadap lalu lintas informasi yang sedang dikirim dan mengubahnya sesuai keinginan mereka[10].
4. Fabrication merupakan ancaman terhadap integritas. Pihak yang tidak berhak dapat meniru atau memalsukan informasi sehingga penerima informasi menganggap informasi tersebut berasal dari sumber yang dikehendaki[10].

2.8 Kerentanan *Website*

Website dapat diartikan sebagai kumpulan halaman yang berisi informasi data digital baik berupa teks, gambar, animasi, suara dan video atau gabungan dari semuanya yang disediakan melalui jalur koneksi internet sehingga dapat diakses dan dilihat oleh semua orang diseluruh dunia[11].Secara umum *Website* dibagi menjadi 3 jenis yaitu :

1. *Website* Statis

   Website statis yaitu jenis *Website* yang isinya tidak diperbaharui secara berkala, sehingga isinya dari waktu akan selalu tetap. *Website* jenis ini biasanya hanya digunakan untuk menampilkan profil dari pemilik *Website* seperti profil perusahaan atau organisasi.

2. *Website* Dinamis

   Website Dinamis yaitu jenis *Website* yang isinya terus diperbaharui secara berkala oleh pengelola web atau pemilik *Website*. *Website* jenis ini banyak dimiliki oleh perusahaan atau perorangan yang aktifitas bisnisnya memang berkaitan dengan internet. Contoh paling mudah dari *Website* jenis ini yaitu web blog dan *Website* berita.

3. *Website* Interaktif

   Website Interaktif pada dasarnya termasuk dalam kategori *Website* dinamis, dimana isi informasinya selalu diperbaharui dari waktu ke waktu. Hanya saja, isi informasi tidak hanya diubah oleh pengelola *Website* tetapi lebih banyak dilakukan oleh pengguna *Website* itu sendiri. Contoh *Website* jenis ini yaitu *Website* jejaring sosial seperti bukalapak, tokopedia, dan sebagainya.

Berdasarkan OWASP TOP 10 tahun 2021 terdapat berbagai kerentanan pada *Website* yang dapat ditemukan berkaitan dengan lemahnya keamanan yang diterapkan sebagai berikut[12].

Tabel 2.1 OWASP TOP 10 Tahun 2021

No	Jenis Kerentanan	Informasi Terjadinya Kerentanan
1	Broken Access Control	Kesalahan dalam mengimplementasikan kontrol

No	Jenis Kerentanan	Informasi Terjadinya Kerentanan
		akses, sehingga pengguna dapat mengakses sumber daya yang tidak seharusnya mereka akses. Melewati pemeriksaan kontrol akses dengan memodifikasi URL (modifikasi parameter), status aplikasi internal, atau halaman HTML, atau dengan menggunakan alat serangan yang memodifikasi permintaan API.
2	Cryptographic Failures	Kelemahan dalam implementasi kriptografi pada aplikasi web yang dapat mengakibatkan kebocoran data atau manipulasi data yang tidak sah. Ini termasuk penggunaan algoritma kriptografi yang lemah, manajemen kunci yang buruk, pengaturan kriptografi yang salah, kesalahan dalam proses enkripsi dan dekripsi, serta penggunaan pesan yang tidak aman.
3	Injection	Serangan injeksi terjadi ketika data yang tidak valid dimasukkan ke dalam input suatu sistem, yang dapat menyebabkan eksekusi kode yang tidak diinginkan oleh sistem. Kerentanan terhadap serangan seperti SQL, NoSQL, dan lain sebagainya.
4	Insecure Design	Kerentanan ini membuat kontrol keamanan tidak dapat melindungi sistem dari serangan karena tidak adanya pemahaman yang cukup tentang risiko bisnis yang terlibat dalam sistem tersebut.
5	Security Misconfiguration	Tidak adanya penguatan keamanan yang sesuai, ,Fitur yang tidak perlu diaktifkan atau diinstal (misalnya, *Port*, layanan, halaman, akun, atau hak istimewa yang tidak perlu). Akun default dan

No	Jenis Kerentanan	Informasi Terjadinya Kerentanan
		password masih diaktifkan dan tidak diubah.
6	Vulnerable and Outdated	Kerentanan terhadap serangan keamanan karena menggunakan versi yang usang atau tidak diperbarui dari perangkat lunak atau komponen yang terlibat. Tidak ada pembaruan yang diterapkan, sistem tetap rentan terhadap serangan yang memanfaatkan kerentanan tersebut.
7	Identification and Authentication Failures	Kerentanan pada sistem atau aplikasi gagal dalam memverifikasi identitas pengguna dengan tepat sebelum memberikan akses ke sumber daya atau layanan yang diinginkan. Sistem tidak menerapkan lapisan keamanan tambahan seperti multi-factor authentication (MFA) atau verifikasi berdasarkan risiko (risk-based authentication).
8	Software and Data Integrity Failures	Kerentanan terkait pembaruan perangkat lunak, dan pipeline CI/CD tanpa memverifikasi integritas. Aplikasi yang bergantung pada plugins, libraries, atau modules yang asalnya dari sumber yang tidak dipercaya, repositori - repositori, Content Delivery Network (CDNs). CI/CD Pipeline yang tidak aman dapat menyebabkan munculnya akses illegal/tidak sah, kode yang berbahaya, atau kerusakan sistem.
9	Security Logging and Monitoring Failures	Kerentanan ini terjadi akibat kegagalan pendeteksian sehingga pelanggaran tidak dapat didetksi dan terjadi penyerangan
10	Server-Side Request Forgery (SSRF)	Kerentanan dengan memanipulasi server untuk melakukan permintaan terhadap sumber daya lain di dalam atau di luar jaringan yang dapat diakses oleh server tersebut. Serangan ini terjadi ketika

No	Jenis Kerentanan	Informasi Terjadinya Kerentanan
		aplikasi web tidak memvalidasi URL atau memfilter input pengguna dengan benar yang digunakan untuk membuat permintaan HTTP atau HTTPS.

2.9 Penetration Testing

Metode pengetesan penetrasi, yang juga dikenal sebagai "pentest", merupakan suatu praktek yang dilakukan untuk menguji keamanan sistem komputer, jaringan, atau aplikasi web dengan tujuan mengenali dan mengevaluasi kerentanan keamanan yang mungkin bisa dimanfaatkan oleh pihak yang tidak diinginkan, melalui simulasi serangan terhadap sistem yang bersangkutan[13].Sistem dievaluasi dengan melakukan simulasi serangan pada sistem atau jaringan untuk mendeteksi celah keamanan yang disebabkan oleh kerentanan sistem atau jaringan, kesalahan konfigurasi, atau kerentanan operasional dalam proses teknis serta potensi pihak yang tidak berwenang untuk dapat akses ke fitur dan data sistem.

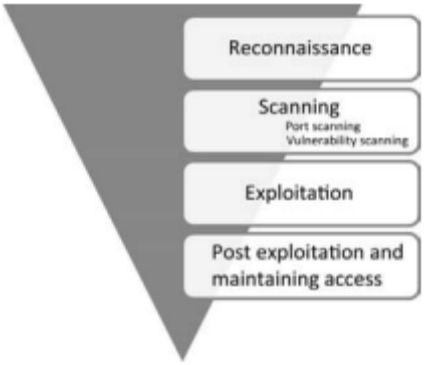
2.10 Grey Box Testing

Grey Box Testing adalah pendekatan di mana pengujian dilakukan dengan sebagian pengetahuan tentang desain internal, struktur, atau algoritma dari sistem yang diuji. "grey box" dalam ilmu komputer atau rekayasa perangkat lunak, mengacu pada teknik pengujian perangkat lunak di mana pengujian dilakukan dengan sejumlah pengetahuan internal tentang sistem yang diuji[14].

2.11 Zero Entry Hacking (ZEH)

Pada Zero Entry Hacking (ZEH) terdapat 4 tahapan yang harus dilalui dalam pengujian sistem. Tahapan-tahapan dalam metode yaitu, Pengintai Sistem (*Reconnaisance*), Pemindaian (*Scanning*). Eksploitasi Celah Keamanan (*Exploit*ation), dan Pasca Eksploitasi (Post *Exploit*ation)[15].

.



Gambar 2.4 Metode Penetrasi Zero Entry Hacking

Berikut Penjelasannya:

1. Pengintaian Sistem (*Reconnaisance*)

   Reconnaisance adalah langkah pertama yang dilakukan dengan merancang dan mencari informasi sebanyak mungkin dari sebuah target
2. Pemindaian (*Scanning*)

   Scanning adalah sebuah tahapan dimana seorang penyerang menggunakan berbagai macam *tools* untuk mencari celah yang akan digunakan sebagai target sasaran.
3. Eksploitasi Keamanan (*Exploit*ation)

   Pada tahap ini celah kerentanan yang telah ditemukan akan di uji untuk memperoleh akses ke sebuah sistem.
4. Pasca Eksploitasi (Post *Exploit*ation)

   Pada tahap ini akan dilakukan upaya untuk mempertahankan akses yang didapatkan, kemudian akan patch rekomendasi celah keamanan pada sistem dari ancaman hacker atau penyusup yang dapat merubah data atau informasi.

2.12 Kali Linux

Kali Linux adalah sebuah sistem operasi open-source yang dirancang untuk kegiatan hacking dan pengujian penetrasi pada jaringan komputer. Dikembangkan oleh Offensive Security, Kali Linux pertama kali diperkenalkan pada tahun 2013 dan berasal dari Debian Linux. OS ini didesain khusus untuk keperluan keamanan jaringan dan telah menjadi standar industri dalam bidang pengujian penetrasi dan forensik

digital. Kali Linux dilengkapi dengan berbagai perangkat lunak hacking dan penetrasi seperti nmap, metasploit, aircrack-ng, dan banyak lagi. Sistem operasi ini mengedepankan keamanan dan privasi, serta dapat digunakan sebagai OS utama atau dalam mode live melalui USB atau CD[16]. Secara umum, Kali Linux terdiri dari beberapa jenis, diantaranya:

1. Kali Linux Full: Versi standar dari Kali Linux yang menyediakan semua alat dan fitur hacking serta pengujian penetrasi yang diperlukan.
2. Kali NetHunter: Dirancang untuk perangkat mobile Android, Kali NetHunter memungkinkan pengguna untuk melakukan pengujian penetrasi pada jaringan secara langsung dari perangkat mobile mereka.
3. Kali Linux Light: Versi yang lebih ringan dari Kali Linux, cocok untuk digunakan pada sistem dengan spesifikasi yang lebih rendah atau dalam skenario di mana pengguna hanya membutuhkan akses terbatas ke alat-alat tertentu.
4. Kali Linux ARM: Versi yang dioptimalkan untuk arsitektur ARM, yang biasanya digunakan pada perangkat seperti Raspberry Pi atau perangkat IoT (Internet of Things).
5. Kali Linux Docker Image: Docker image Kali Linux yang memungkinkan pengguna untuk menjalankan Kali dalam wadah Docker, mempermudah penggunaan dan integrasi dengan lingkungan pengembangan atau pengujian.

2.13 Whois Lookup

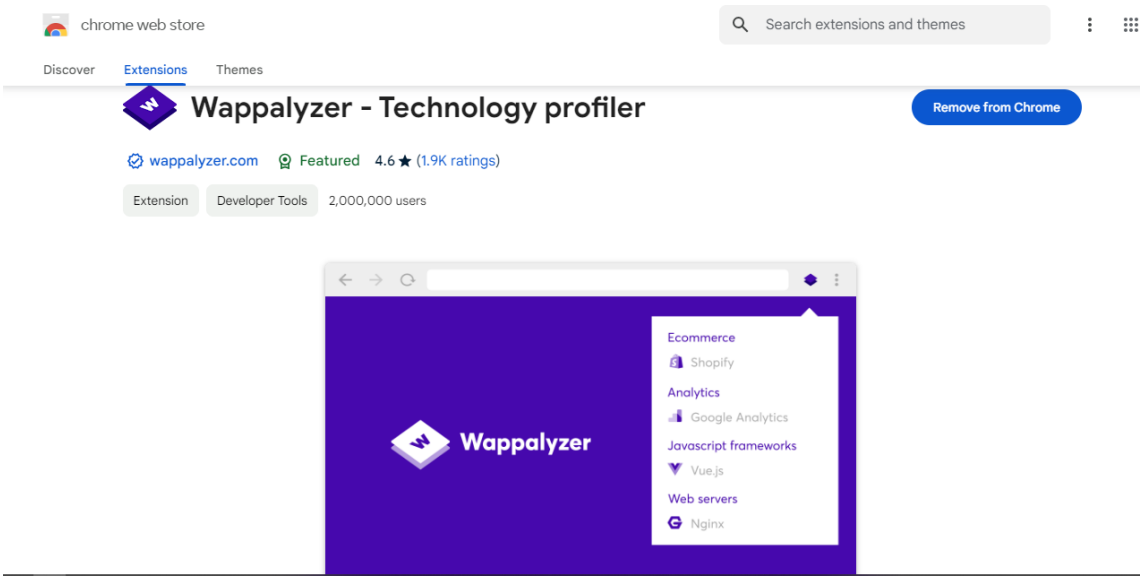
Whois adalah protokol dan layanan yang digunakan untuk mencari informasi tentang kepemilikan atau registrasi suatu *Domain* internet, atau alamat IP. Ini memungkinkan pengguna untuk menemukan informasi seperti nama pemilik *Domain*, informasi kontak, tanggal kadaluarsa *Domain*, dan server nama (DNS) yang terkait dengan *Domain* tersebut[17]. Sejak tahun 2005, Whois telah menawarkan alat untuk mencari alamat IP di *Domain* tingkat atas (TLD) dan *Domain* tingkat kedua (SLD).*who is* dapat diinstall menggunakan terminal dengan perintah *sudo apt install whois* dengan size 387 KB pada versi 5.5.23 dengan bantuan dependencies

libc6,libcrypt1,libidn2-0.

2.14 Wappalyzer

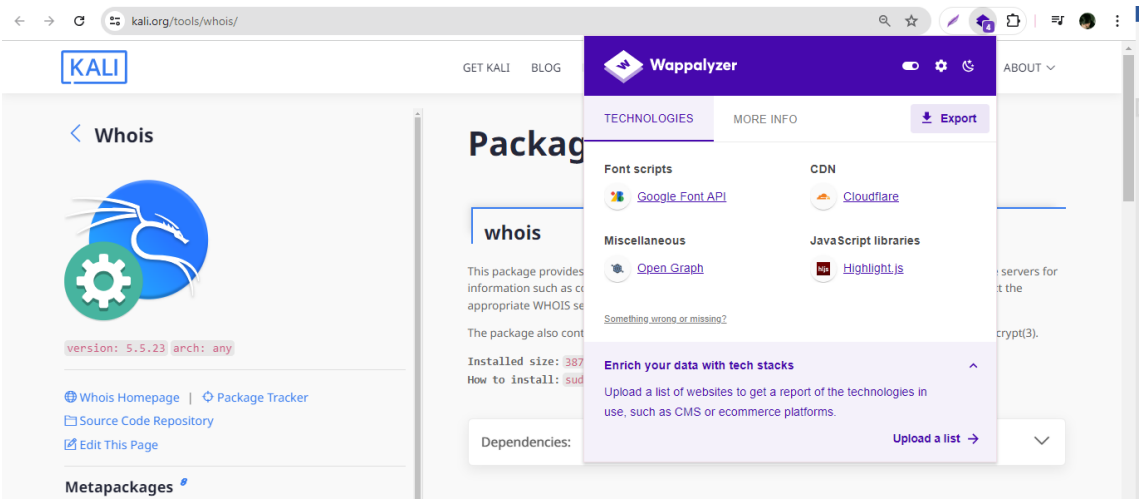
Wappalyzer /wæpəlʌɪzər/ adalah profiler teknologi dan penyedia data prospek yang didirikan oleh Elbert Alias pada tahun 2008. Wappalyzer adalah alat analisis web yang digunakan untuk mengidentifikasi berbagai teknologi yang digunakan oleh situs web. Ini termasuk mendeteksi sistem manajemen konten (CMS), *Framework* web, platform e-commerce, alat analisis, server web, bahasa pemrograman, perpustakaan Java*Script*, dan banyak lagi. Wappalyzer tersedia sebagai ekstensi browser untuk Chrome dan Firefox, serta dalam bentuk layanan API dan alat baris perintah. Wappalyzer tersedia sebagai ekstensi untuk browser Chrome dan Firefox, memungkinkan pengguna untuk mengidentifikasi teknologi situs web langsung dari browser dengan satu klik. Wappalyzer bekerja dengan menganalisis berbagai elemen dari halaman web dengan cara memeriksa header HTTP untuk informasi tentang server web dan teknologi lainnya, Menganalisis kode sumber HTML untuk mencari tanda tangan khusus dari berbagai teknologi, Memeriksa cookies untuk mengidentifikasi layanan analitik dan teknologi lainnya. Mendeteksi library dan *Framework* Java*Script* yang digunakan di halaman[18].Pada gambar Wappalyzer dapat diinstal menggunakan extension google chrome dengan cara mengunjungi *Website https://chromewebstore.google.com/* dan mencari pada search bar

Wappalyzer klik lalu install pada browser.



Gambar 2.5 Extension Wappalyzer

Menggunakan Wappalyzer sederhana dengan pin kan extension pada mainbar lalu klik Wappalyzer ekstension maka akan muncul informasi terkait teknologi yang digunakan seperti pada gambar 2.6 .



Gambar 2.6 Penggunaan Wappalyzer

2.15 What Web

WhatWeb adalah alat analisis web yang digunakan untuk mengidentifikasi berbagai teknologi dan informasi yang digunakan oleh situs web. Ini mencakup deteksi sistem manajemen konten (CMS), server web, platform e-commerce,

Framework web, bahasa pemrograman, pustaka Java*Script*, dan banyak lagi. WhatWeb dikenal karena kemampuannya dalam melakukan fingerprinting terhadap situs web dan memberikan informasi terperinci tentang infrastruktur teknologi yang digunakan[19].

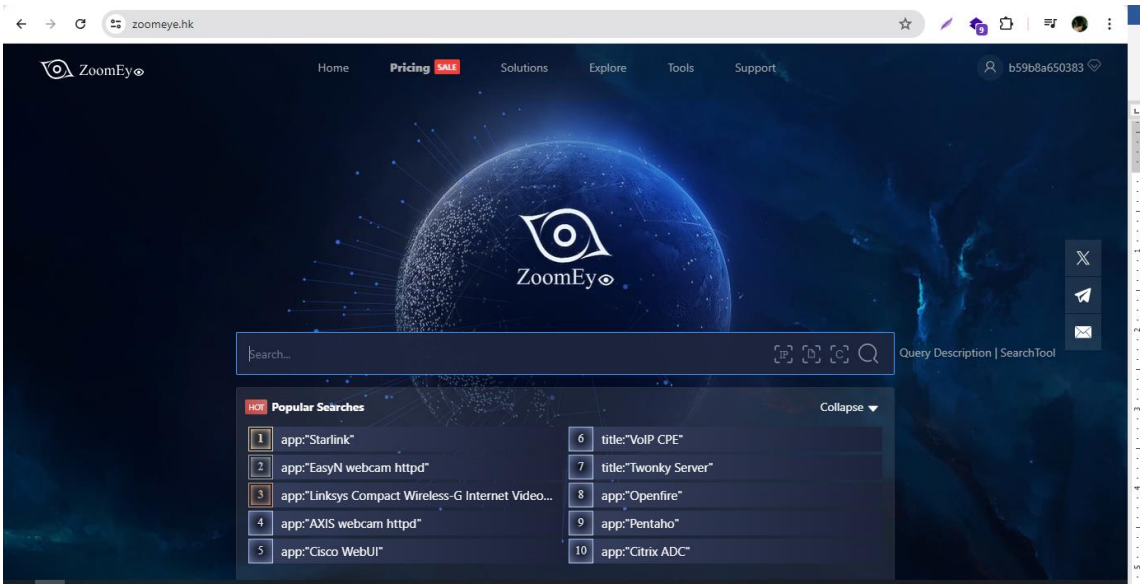
WhatWeb memiliki lebih dari 900 *plugins*, masing-masing untuk mengenali sesuatu yang berbeda. Plugin ini juga mengidentifikasi nomor versi, alamat email, ID akun, modul kerangka kerja web, kesalahan SQL, dan banyak lagi[19].Whatweb dapat install menggunakan terminal dengan perintah *sudo apt install whatweb* dengan size berukuran 18.58 MB dengan *dependecies ruby | ruby-interpreter, ruby-addressable ,ruby-ipaddress* atau dapat diakses pada *Domain https://www.whatweb.net/.*

2.16 CXSecurity

CXSecurity adalah platform dan database yang berfokus pada keamanan informasi, khususnya dalam hal pengumpulan, penyimpanan, dan penyebaran informasi tentang kerentanan keamanan yang ditemukan pada perangkat lunak dan sistem. *CXSecurity* dikelola oleh satu orang *independent* , Platform ini menawarkan berbagai layanan dan fitur yang berguna bagi profesional keamanan, peneliti, dan pengembang perangkat lunak untuk memahami dan mengatasi kerentanan keamanan. Database ini nantinya yang akan digunakan sebagai panduan untuk melakukan identifikasi terkait objek yang akan di uji .*CXSecurity* dapat diakses menggunakan *Domain cxsecurity.com*

2.17 Zoom Eye

ZoomEye adalah mesin pencari keamanan siber yang dikembangkan oleh perusahaan China, KnownSec. ZoomEye dirancang untuk mengindeks perangkat yang terhubung ke internet, seperti server, router, kamera, dan perangkat IoT lainnya. ZoomEye dapat memindai alamat IPv4 dan IPv6 global serta nama *Domain* situs web, mengidentifikasi dan menganalisis berbagai *Port* dan protokol layanan[20]. Zoom Eye dapat diakes pada *Domain* https://www.zoomeye.hk/ seperti gambar 2.7 .

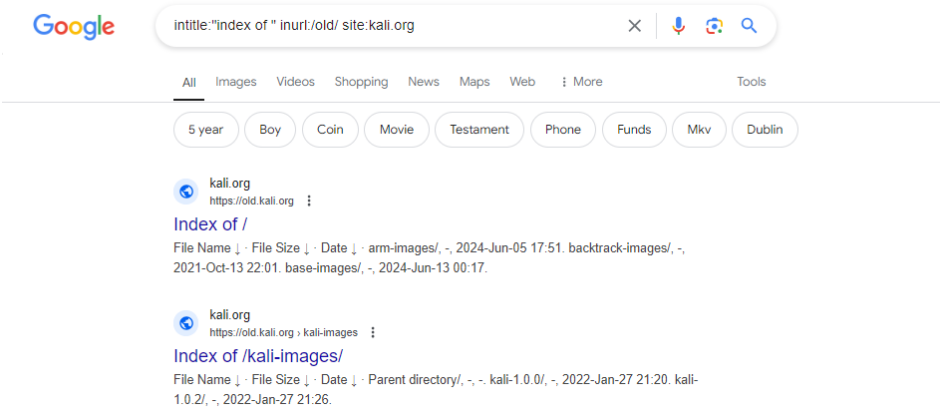


Gambar 2.7 Penggunaan Zoom Eye

Dokumentasi cara untuk melakukan query dapat diakes pada halaman *Domain* https://www.zoomeye.hk/doc?channel=user .

2.18 Google *Dork*

Google memperkenalkan fitur kuat yang disebut "Directives" dengan tujuan meningkatkan efektivitas pencarian, sehingga lebih terarah dan akurat dalam mengumpulkan informasi dan file dari situs web tertentu[15]. Google *Dorking* adalah teknik menggunakan operator pencarian lanjutan di mesin pencari Google untuk menemukan informasi yang tidak mudah terlihat melalui pencarian standar. Informasi ini dapat mencakup data sensitif yang tidak seharusnya dipublikasikan, seperti email, informasi login, atau file yang disimpan secara tidak aman.Contoh penggunaan dalam menggunakan *google Dork* atau juga disebut *google hacking* seperti gambar



Gambar 2.8 Contoh Penggunaan *Google Dork*

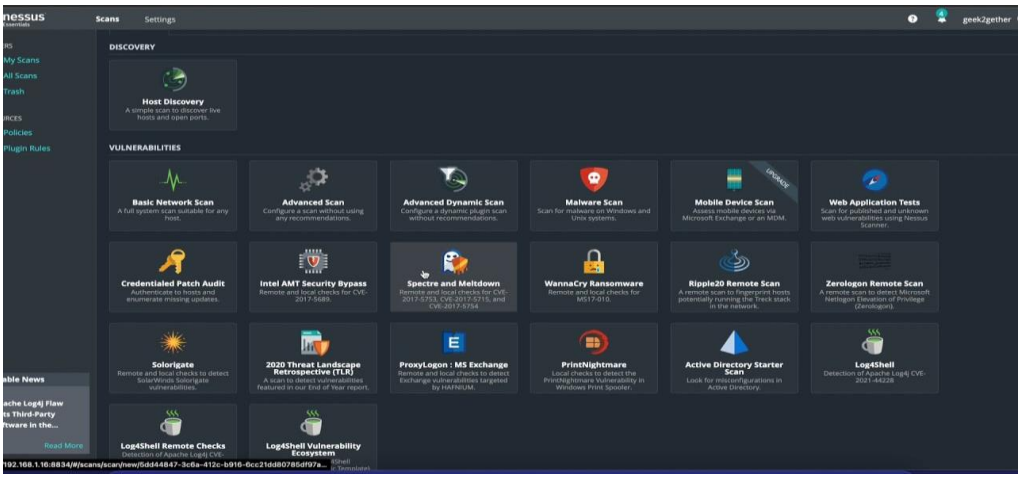
2.19 Nmap

Nmap ("Network Mapper") adalah alat open source untuk eksplorasi jaringan dan audit keamanan. Nmap menggunakan paket IP untuk mengidentifikasi host yang terhubung ke jaringan, layanan (nama aplikasi dan versi) yang berjalan, sistem operasi (dan versinya), jenis firewall/filter paket yang digunakan, dan berbagai karakteristik lainnya[21]. Output dari Nmap adalah daftar host target yang diperiksa beserta informasi tambahan sesuai dengan opsi yang digunakan. Salah satu informasi kunci adalah "tabel *Port* menarik" yang berisi daftar nomor *Port* dan protokol, nama layanan, serta statusnya. Status tersebut dapat berupa terbuka (open), difilter (filtered), tertutup (closed), atau tidak difilter (unfiltered). Status terbuka berarti bahwa aplikasi pada mesin target sedang mendengarkan koneksi/paket pada *Port* tersebut. Difilter berarti bahwa sebuah firewall, filter, atau penghalang jaringan

lainnya memblokir *Port* sehingga Nmap tidak dapat mengetahui apakah ia terbuka atau tertutup. Tertutup *Port* tidak memiliki aplikasi yang sedang mendengarkan, meskipun mereka dapat terbuka kapanpun. *Port* digolongkan sebagai tidak difilter ketika mereka menanggapi probe Nmap, namun Nmap tidak dapat menentukan apakah mereka terbuka atau tertutup. Nmap melaporkan kombinasi status open|filtered dan closed|filtered ketika tidak dapat menentukan status manakah yang menggambarkan sebuah *Port*[22].

2.20 Nessus

Nessus adalah salah satu produk evaluasi keamanan yang sering digunakan, pertama kali dirilis oleh Renaud Deraison pada tahun 1998. Nessus menyediakan pemindaian kerentanan untuk perangkat jaringan, virtual host, sistem operasi, basis data, aplikasi web, dan jaringan hibrid IPv4 / IPv6[23]. Nessus dapat didownload pada *Domain* https://www.tenable.com/downloads/nessus?loginAttempted=true, Dengan memilih version dan platform yang ingin digunakan sebagai contoh apabila menggunakan kali linux maka pilih platform Linux-Debian-amd64 dengan size 69,2 MB, Lalu ikuti pedoman instalasi dan konfigurasi pada url berikut https://www.tenable.com/blog/getting-started-with-nessus-on-kali-linux , Setalah instalasi dan konfigurasi selesai maka tampilan utama pada nessus seperti gambar 2.9.



Gambar 2.9 Tampilan Nessus

2.21 Burp-Suite

Burp Suite adalah platform terintegrasi untuk melakukan pengujian keamanan

aplikasi web. Alat ini dikembangkan oleh *Port*Swigger Web Security dan menyediakan berbagai fitur yang mendukung seluruh proses pengujian penetrasi pada aplikasi web. Burp Suite terdiri dari beberapa komponen yaitu *Proxy Server ,Sequencer ,Repeater ,Intruder* dan lainnya.

2.22 Common Vulnerability Scoring System (CVSS)

Common Vulnerability Scoring System (CVSS) adalah sebuah *Framework* standar yang digunakan untuk mengevaluasi dan mengukur tingkat keparahan kerentanan keamanan pada sistem komputer dan jaringan[24]. CVSS dirancang untuk memberikan metode yang konsisten dan objektif dalam mengklasifikasikan kerentanan berdasarkan serangkaian metrik yang terstruktur. Metrik-metrik ini mencakup aspek-aspek seperti dampak kerentanan terhadap kerahasiaan data, integritas sistem, dan ketersediaan layanan, serta karakteristik teknis lainnya seperti kompleksitas eksploitasi dan kebutuhan akses. CVSS memberikan skor numerik untuk setiap kerentanan yang dinilai, yang terdiri dari beberapa komponen:

1. Base Score: Skor dasar yang mencerminkan karakteristik intrinsik dari kerentanan itu sendiri, seperti dampak dan kompleksitas eksploitasi.
2. Temporal Score: Skor temporal yang mempertimbangkan faktor-faktor yang dapat berubah seiring waktu, seperti ketersediaan patch atau eksploitasi aktif.
3. Environmental Score: Skor lingkungan yang mempertimbangkan konteks penggunaan aplikasi atau sistem, seperti pengaruh dari kontrol keamanan tambahan yang diimplementasikan.