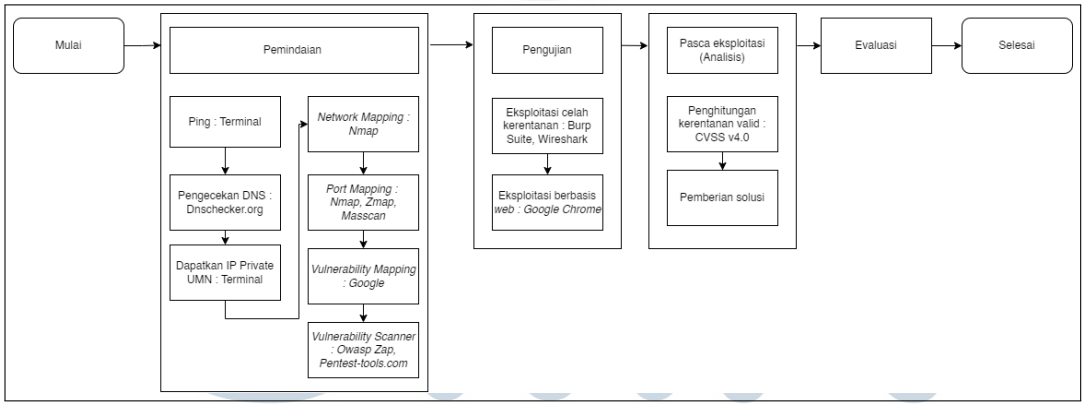
BAB 3
METODOLOGI PENELITIAN

Pada penelitian ini, penulis akan menggunakan metode *Zero Entry Hacking* (ZEH). Menurut Engebretson (2013), ZEH memiliki 4 tahapan sebagai berikut [10]:

1. Pengintaian (*Reconnaisance*)
2. Pemindaian (*Scanning*)
3. Exploitasi celah kerentanan (*Exploitation*)
4. Pasca exploitasi (*Post exploitation*)

Pada penelitian ini, penulis tidak akan melakukan tahap pertama dalam ZEH yaitu pengintaian dikarenakan *website* yang akan diuji sudah diketahui dan tidak perlu lagi diintai, sehingga akan langsung masuk ke tahap kedua yaitu pemindaian. Tahapan yang akan dilakukan pada penelitian ini dapat dilihat pada Gambar 3.1 sebagai berikut :



Gambar 3.1. Bagan Metode Penelitian

Berdasarkan Gambar 3.1 diatas, berikut ini penjelasan lebih lengkap mengenai masing - masing tahapan metodologi yang dapat dilihat pada Tabel 3.1 sebagai berikut.

Tabel 3.1: Detail tahapan metodologi

No	Metodologi	Tahapan	*Tools*	Tujuan
1	Pemindaian (*Scanning*)	Ping	Terminal, dnschecker.org	Mencari tahu apakah *website* yang diujikan aktif atau tidak
		Network Mapping	NMAP	Mendapatkan informasi / gambaran mengenai jaringan
		Port Mapping	NMAP, ZMAP, Masscan	Mencari *port* yang terbuka
		Vulnerability Mapping	Google	Mencari tahu kerentanan dari *port* yang terbuka
		Vulnerability Scanner	Pentest-tools.com, Owasp Zap	Mencari celah kerentanan yang ada pada *website* yang diujikan
2	Eploitasi Celah Kerentanan (*Exploitation*)	Eksploitasi berbasis *web*	Google Chrome, Wireshark, Burp Suite	Menguji kerentanan yang didapat dari tahap sebelumnya
3	Pasca Eksploitasi (*Post Exploitation*)	Penghitungan Kerentanan	CVSS 4.0	Melihat prioritas kerentanan untuk dilakukannya perbaikan.

3.1 Pengumpulan Data

Cara yang akan dilakukan penulis untuk melakukan pengumpulan data pada penelitian ini adalah dengan melakukan pemindaian terhadap *website gapura.umn.ac.id* dan *academic.umn.ac.id*. Dari pemindaian tersebut, data - data yang ingin diperoleh adalah apakah kedua *website* yang diujikan aktif atau tidak, dan apa saja *port* yang terbuka sehingga dapat dimanfaatkan untuk

tahap selanjutnya. Selain kedua hal tersebut, tahapan pemindaian ini juga ingin memperoleh data kerentanan apa saja yang terdapat pada kedua *website* yang diujikan. Untuk memperoleh data - data tersebut, tahap pemindaian ini akan dibagi menjadi lima tahapan lebih lanjut sebagai berikut :

1. Menentukan apakah *gapura.umn.ac.id* dan *academic.umn.ac.id* dapat di *ping*. Tujuan dari *ping* adalah untuk melihat apakah target terhubung dengan jaringan atau tidak, apakah hanya dapat diakses dari jaringan lokal saja, atau bisa diakses oleh publik. Selain itu, *ping* juga dilakukan untuk melihat bagus atau tidaknya kualitas koneksi target, berapa durasi yang dibutuhkan target untuk membalas *ping*.

2. *Network mapping* sistem menggunakan *tools* Nmap terhadap *gapura.umn.ac.id* dan *academic.umn.ac.id*. Tujuan dari *network mapping* adalah untuk membuat peta visual dari infrastruktur jaringan yang bertujuan untuk memahami topologi, meningkatkan keamanan, dan memudahkan manajemen serta pemantauan kinerja jaringan.

3. *Port mapping* sistem menggunakan *tools* Nmap , Zmap, dan pentest-tools.com terhadap *gapura.umn.ac.id* dan *academic.umn.ac.id*. Tujuan dari *port mapping* adalah untuk mengidentifikasi dan memetakan *port* yang terbuka pada suatu perangkat atau jaringan, yang membantu dalam pemantauan keamanan, konfigurasi jaringan, dan pengaturan aliran lalu lintas.

4. *Vulnerability mapping* sistem menggunakan *tools* google untuk menentukan atau membuat *list* kerentanan apa saja yang dapat ditimbulkan dari *port* terbuka yang ditemukan pada tahap *port mapping*.

5. Pemindaian *gapura.umn.ac.id* dan *academic.umn.ac.id* menggunakan *tools vulnerability scanner*. Pemindaian sistem bertujuan untuk mengecek *vulnerability* apa saja yang terdapat pada *website* UMN. *Tools* yang akan digunakan untuk pemindaian adalah Owasp Zap dan juga pentest-tools.com.

3.2 Pengujian dan Analisis

Tahap pengujian dan analisis akan dibagi lagi menjadi dua tahap yang lebih lengkap yaitu eksploitasi celah kerentanan dan juga pasca eksploitasi. Penjelasan mengenai masing - masing tahap, akan dijelaskan sebagai berikut.

3.2.1 Eploitasi Celah Kerentanan (Exploitation)

Pada tahap kedua ini, penulis akan memanfaatkan kerentanan yang telah ditemukan pada tahap sebelumnya, yaitu pengumpulan data. Tahap ini dikenal sebagai tahap eksploitasi, di mana penulis akan menggunakan pendekatan berbasis *web* dan juga memanfaatkan beberapa *tools* yang tersedia.

Eksploitasi berbasis *web* adalah upaya yang dilakukan untuk mengeksploitasi aplikasi berbasis *web*. Ini dilakukan dengan memanfaatkan celah keamanan yang telah terungkap selama proses *scanning*. Dengan memanfaatkan celah ini, penulis dapat mengeksploitasi sistem dan mendapatkan akses yang tidak seharusnya. Selain melakukan eksploitasi berbasis *web*, penulis juga akan menggunakan beberapa *tools* eksploitasi. Beberapa di antaranya adalah Burp Suite dan Wireshark. Kedua *tools* ini memiliki fungsi dan fitur yang berbeda, namun keduanya sangat berguna dalam proses eksploitasi.

Burp Suite adalah *tool* yang dirancang untuk menguji keamanan aplikasi berbasis *web*. Dengan menggunakan Burp Suite, penulis dapat melakukan berbagai jenis serangan terhadap aplikasi dan menemukan celah keamanan yang mungkin ada. Sementara itu, Wireshark adalah *tool* yang digunakan untuk menganalisis lalu lintas jaringan. Dengan Wireshark, penulis dapat melihat detail dari setiap paket data yang dikirim dan diterima oleh sistem. Ini sangat berguna untuk menemukan informasi sensitif yang mungkin dikirim tanpa enkripsi yang tepat. Tujuan dari penggunaan *tools* ini adalah untuk membantu penulis dalam mengeksploitasi dua *website* yang diujikan yaitu *gapura.umn.ac.id* dan *academic.umn.ac.id*. Dengan memanfaatkan kerentanan yang ditemukan, penulis berharap dapat meningkatkan keamanan dari kedua *website* ini.

3.2.2 Pasca Eksploitasi (Post Exploitation)

Dalam tahap yang terakhir pada ZEH, hasil dari tahap eksploitasi akan dirangkum dan digolongkan menjadi tiga jenis kerentanan yaitu valid, valid tapi tidak berpengaruh, dan *false positive*. Kerentanan yang dikategorikan sebagai valid adalah kerentanan yang benar-benar ada dan dapat dieksploitasi. Ini adalah kerentanan yang paling kritis dan memerlukan perhatian segera. Sementara itu, kerentanan yang dikategorikan sebagai valid tapi tidak berpengaruh adalah kerentanan yang ditemukan pada tahap pemindaian, namun ketika di eksploitasi tidak berpengaruh pada sistem. Kerentanan yang dikategorikan sebagai *false*

positive adalah kerentanan yang ditemukan namun tidak benar. Ini biasanya terjadi karena kesalahan dalam proses deteksi kerentanan. Kerentanan jenis ini biasanya tidak memerlukan tindakan perbaikan.

Untuk kerentanan yang dikategorikan sebagai valid, penulis akan menghitung prioritas kerentanan menggunakan kalkulator CVSS v4.0. *Common Vulnerability Scoring System* (CVSS) adalah standar industri untuk menentukan tingkat keparahan kerentanan. Dengan menggunakan kalkulator CVSS v4.0, penulis dapat menentukan skala prioritas kerentanan. Tujuan dari tahap ini adalah untuk melihat skala prioritas kerentanan. Dengan mengetahui prioritas kerentanan, penulis dapat menentukan kerentanan mana yang lebih penting untuk diperbaiki terlebih dahulu.