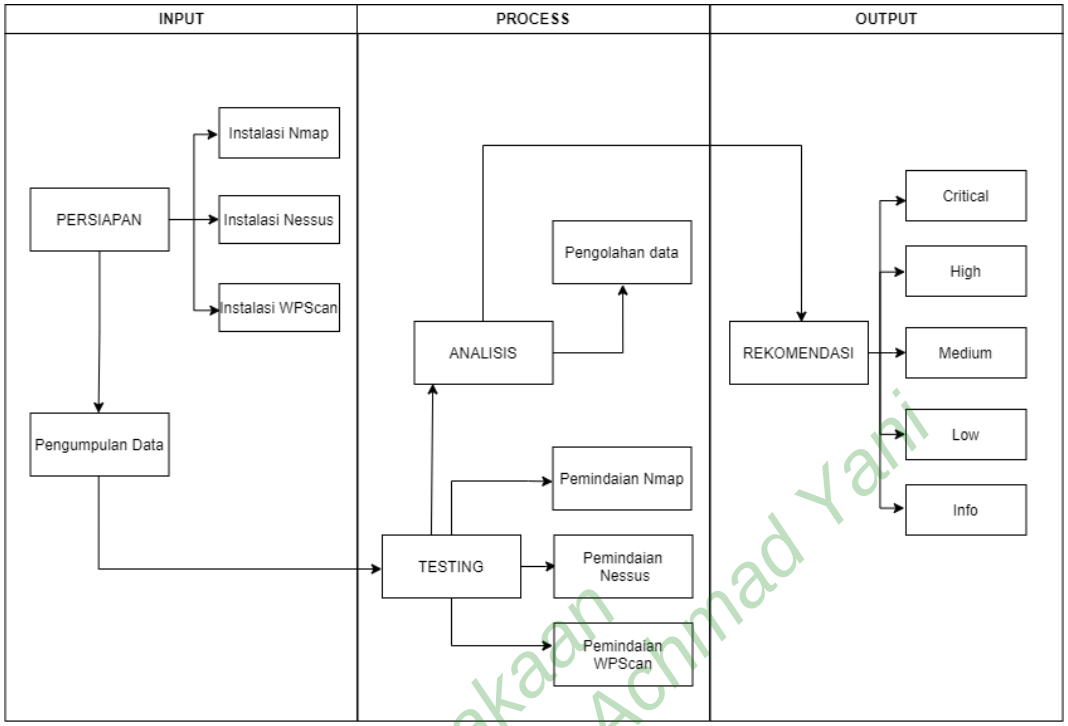
BAB 3
METODE PENELITIAN

Penelitian ini menggunakan metode *vulnerability assessment* dalam menilai kerentanan pada *situs web* target. Metode ini melalui beberapa tahapan seperti mengidentifikasi aset, menilai aset, mengidentifikasi kerentanan. Rangkaian proses dalam menganalisis vulnerability *situs web* yaitu dari persiapan sampai penilaian kerentanan pada sistem sebagai berikut:

1. Persiapan.
   a. Instalasi Nmap.
   b. Instalasi Nessus
   c. Instalasi WPScan
   d. Pengumpulan data dan memeriksa informasi pada DNS mengunakan DNSDumpster
2. Pemindaian kerentanan
3. Mengidentifikasi kerentanan
4. Analisis.

Dengan memanfaatkan alamat IP target dapat dipindai menggunakan aplikasi Zenmap untuk menentukan *host-host* yang aktif dalam jaringan kemudian menentukan informasi sistem operasi dan *port-port* yang terbuka dan jenis firewall yang digunakan oleh target. Kemudian untuk menentukan celah kerentanan pada target dapat dipindai menggunakan Nessus yang kemudian dianalisis tingkat kerentanan.



Gambar 3.1 Alur pengujian

Pada alur pengujian terdapat tiga tahapan yang menjelaskan jalannya penelitian ditunjukan pada Gambar 3.1 Pada tahap *input*, dimana persiapan alat pemindaian dilakukan instalasi terlebih dahulu, kemudian dilanjut dengan pengumpulan data *situs web* yang akan dipindai kerentanannya. Pengumpulan data dilakukan dengan meminta izin kepada pihak pusat sistem informasi dan meminta rekomendasi *situs web* FTTI yang akan dipindai dan memeriksa DNS pada setiap situs web menggunakan alat DNSdumpster untuk mengidentifikasi *Headers* situs web yang akan dipindai. Dengan demikian dilanjut pada tahap *process* yang dimulai dari *testing*. Namun sebelum melakukan pemindaian, terlebih dahulu dilakukan pemcarian *IP address* dengan menggunakan Command Prompt, *situs web* dapat diketahui *IP address* dengan menuliskan perintah *ping* yang diikuti alamat web. Lalu dilakukan pemindaian menggunakan ketiga alat pemindaian kerentanan. Dengan hasil pemindaian yang telah dilakukan, maka peneliti dapat menganalisis beberapa kerentanan yang terdapat dari masing-masing *situs web* kemudian dilakukan pengolahan data. Dari hasil analisis dan

pengolahan data maka dilanjut ke tahap *output.* Pada tahap ini penulis merangkum rekomendasi perbaikan dari masing masing tingkat risiko kerentanan yang ada.

3.1 BAHAN DAN ALAT PENELITIAN

Alat yang digunakan dalam penelitian ini adalah komputer dengan spesifikasi cukup untuk menjalankan beberapa *tool* serta koneksitas Internet. Sistem Operasi dan program-program aplikasi yang dipergunakan dalam dalam penelitian ini adalah:

1. Sistem Operasi: Windows 10.
2. Situs web sasaran pemindaian: ftti.unjaya.ac.id, elearning.ftti.unjaya.ac.id, dan app.ftti.unjaya.ac.id.
3. Google Chrome
4. DNSDumpster
5. Nessus
6. Aplikasi Zenmap yang merupakan Nmap versi GUI
7. WPScan
8. Powershell versi 7.2.6
9. Command Prompt.

3.2 JALAN PENELITIAN

Penelitian ini menggunakan metode *Vulnerability Assessment* yang dilanjut dengan pemindaian pada target. Metode ini dipilih karena sangat penting untuk melakukan analisis kerentanan pada situs web FTTI. Adapun situs web yang diizinkan oleh pihak PUSI untuk dilakukan analisis seperti ftti.unjaya.ac.id, elearning.ftti.unjaya.ac.id, dan app.ftti.unjaya.ac.id Dalam persiapan penelitan dilakukan penginstalan pada alat yang akan digunakan, kemudian melakukan pemindaian pada IP target menggunakan Nmap guna menentukan *host-host* yang aktif dan menentukan *port-port* yang terbuka. Sedangkan penilaian kerentanan pada IP target menggunakan Nessus. Pada proses *scanner* ini membutuhkan waktu yang cukup lama karena peneliti menganalisis situs web secara kompleks.

Dikarenakan situs web ftti.unjaya.ac.id menggunakan WordPress, maka peneliti menggunakan WPScan untuk memindai kerentanan yang ada. Dengan hasil penghitungan yang telah dilakukan maka akan dilakukan analisis. Adapun tahapan penelitian analisis ini terdiri dari 4 tahap, yaitu:

1. Tahap Persiapan dengan melakukan penginstalan pada alat dan aplikasi yang akan digunakan.
2. Permohonan izin kepada admin situs web FTTI.
3. Tahap pengumpulan dan pengelolahan data yang didapatkan melalui pemindaian, meliputi:
   a. Identifikasi *Headers* menggunakan DNSdumpster.
   b. Pemindaian dengan Nmap untuk menentukan port yang terbuka.
   c. Pemindaian dengan WPScan untuk mengetahui kerentanan pada situs web yang menggunakan WordPress.
   d. Pemindaian menggunakan Nessus untuk mengetahui kerentanan pada situs web target.
   e. Menganalisis data hasil pemindaian.

   Tahap penulisan laporan, yaitu tahapan akhir dalam penelitian ini.

3.3 METODE *VULNERABILITY ASSESSMENT*

Dalam penyusunan tugas akhir ini, penulis menggunakan beberapa metode *vulnerability assessment* yang sesuai dengan bidangnya yaitu topologi jaringan, testing, dan analisis. Pada metode ini juga beberapa alat yang digunakan untuk melakukan pemindaian kerentanan pada masing-masing situs web.

Tabel 3.1 Tabel alat pemindaian

ALAT	Situs web		
	ftti.unjaya.ac.id	app.ftti.unjaya.ac.id	elearning.ftti.unjaya.ac.id
Nmap	Ya	Ya	Ya
Nessus	Ya	Ya	Ya
WPScan	Ya	Tidak	Tidak

Metode ini menggunakan 3 (tiga) alat yaitu Nmap, Nessus, dan WPScan. Namun, seperti yang telah ditunjukan pada Tabel 3.1 bahwa hanya WPScan saja yang tidak digunakan untuk memindai situs web pada app.ftti.unjaya.ac.id dan elearning.ftti.unjaya.ac.id karena menggunakan CMS yang berbeda, menurut hasil dari pencarian pada DNSDumpster menjelaskan bahwa kedua situs web tersebut tidak menggunakan WordPress dan hanya ftti.unjaya.ac.id yang terdeteksi menggunakan WordPress. Sehingga tidak cocok untuk dilakukan pemindaian menggunakan WPScan.