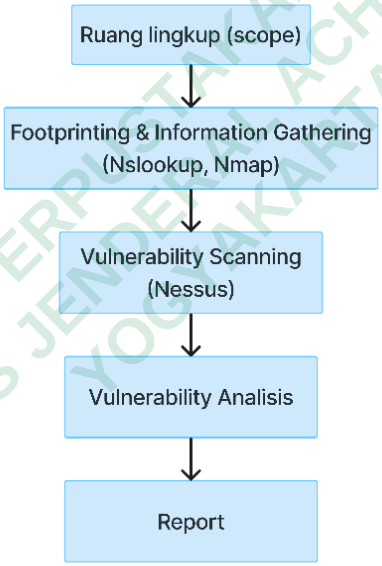
BAB 3
METODE PENELITIAN

Penelitian ini dilakukan dengan metode *Vulnerability Assessment* yang berpusat pada tahap *Footprinting* dan *Vulnerability Scanning* untuk melakukan evaluasi kerentanan. Target penelitian ini adalah *website e-learning* FKES UNJAYA, yang akan dites kerentanannya menggunakan alat dan aplikasi pemindaian kerentanan untuk mendapatkan informasi tentang kerentanan tersebut. Berikut tahapan penelitian dapat dilihat pada Gambar 3.1 di bawah ini.



Gambar 3.1 Tahapan Penelitian

1. Ruang lingkup (*scope*): langkah pertama dalam penelitian ini adalah menetapkan ruang lingkup terhadap *website* target yang akan dites. Dalam hal ini, penelitian ini hanya melakukan pemindaian kerentanan, tanpa melakukan eksploitasi terhadap sistem seperti mengubah tampilan, melakukan serangan, dan sejenisnya.
2. *Footprinting & Information Gathering*: langkah ini diambil untuk mengumpulkan sejumlah besar informasi yang berkaitan dengan *website e-*

learning. Ini melibatkan pemindaian menggunakan Nslookup dan Nmap untuk mendapatkan data dari server *Domain Name System* (DNS), serta melakukan pemindaian untuk mengetahui *port* yang terbuka dan tertutup.

3. *Vulnerability Scanning*: dalam tahap ini, melakukan pemindaian untuk memperoleh informasi tentang kerentanan target, dilakukan dengan menggunakan alat *Vulnerability Scanner* Nessus. Ini mencakup sumber informasi seperti potensi kerentanan situs web yang ada.
4. *Vulnerability Analysis*: pada tahap ini, akan melakukan analisis dari hasil *scanning* kerentanan yang telah ditemukan setelah melakukan pemindaian terhadap target menggunakan alat *scanner*. Selanjutnya, akan diberikan saran tentang cara memperbaiki atau mengatasi kerentanan yang telah teridentifikasi.
5. *Report*: langkah ini akan mencatat hasil analisis dari kerentanan keamanan pada *website* target, yang nantinya dapat dijadikan acuan oleh pengelola *website* target untuk memahami apa saja yang telah ditemukan.

3.1 BAHAN DAN ALAT PENELITIAN

Dalam penelitian ini, memanfaatkan berbagai sumber data, diantaranya alamat *website e-learning* FKES UNJAYA (eling.fkes.unjaya.ac.id) dan informasi tentang *website* FKES UNJAYA yang diperoleh melalui hasil *Footprinting* dan *Information Gathering*.

Pada penelitian ini, memakai sebuah laptop yang memiliki kriteria yang memadai untuk menjalankan berbagai *tools*, serta dilengkapi dengan jaringan internet. Penelitian ini memanfaatkan sistem operasi dan berbagai *tools* berikut:

1. Laptop dengan sistem operasi *Windows* 11

   Prosesor : AMD Ryzen 5 4500U *with* Radeon Graphics. 2.38 GHz
   RAM : 8.00 GB (7.37 GB usable)
   Edisi : *Windows 11 Home Single Language*
   Versi : 23H2
2. Microsoft Edge

3. NsLookup

   Digunakan untuk mengakses dan mengumpulkan informasi dari server *Domain Name System* (DNS).

4. Nmap

   Digunakan untuk pemindaian jaringan dan audit keamanan dengan melakukan *scanning* sebuah *port-port* yang terbuka dan tertutup.

5. Nessus

   Digunakan untuk mengenali kerentanan pada sistem komputer, termasuk serangan yang berbahaya.

3.2 JALAN PENELITIAN

Dalam penelitian ini menggunakan metode *Vulnerability Assessment* dengan proses melakukan pemindaian pada target dengan rentang waktu 10 Juni 2024 sampai dengan 27 Juni 2024. Metode ini dipilih sebab sangat krusial untuk menganalisis kerentanan pada *website e-learning* FKES UNJAYA. Pada tahap penelitian analisis ini, akan dilakukan 5 langkah tahapan sebagai berikut:

1. Melakukan identifikasi dan analisis guna menetapkan perumusan masalah, dan studi literatur.
2. Persiapan dilakukan sebelum melakukan pengumpulan data, seperti menentukan *tools* yang akan digunakan, melakukan pemasangan atau pengunduhan *tools* yang akan digunakan untuk melakukan *scanning* pada *website* target.
3. Permohonan izin kepada pihak atau pengelola *website*, yaitu FKES UNJAYA untuk melakukan *scanning* pada *website* target.
4. Pengumpulan dan pengolahan data menggunakan beberapa *tools*, sebagai berikut:
   a. NsLookup untuk menemukan alamat IP yang terkait dengan domain *website e-learning* FKES UNJAYA.
   b. Nmap untuk melakukan pemindaian port, mengidentifikasi host, mendeteksi versi layanan dan sistem operasi.

c. Nessus digunakan untuk melakukan *vulnerability scanning*, untuk melakukan identifikasi potensi kerentanan dan analisis lebih lanjut pada *website* target.

5. Analisis dan penulisan laporan, merupakan tahapan akhir untuk memaparkan hasil dari semua temuan tahapan diatas pada penelitian ini.