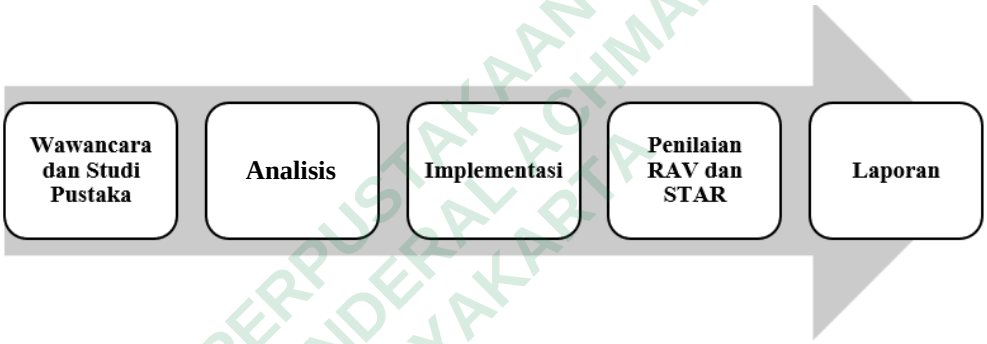
BAB 3
METODE PENELITIAN

Untuk menilai kerentanan yang ada pada situs *website Repository* Unjaya , penelitian ini menggunakan *Open Source Security Testing Methodology Manual* (OSSTMM). Penelitian ini berkonsentrasi pada tahap identifikasi kelemahan, peneliti menggunakan aplikasi Netcraft, Nmap dan OWASP ZAP. Adapun alur penelitian menggunakan metode *Open Source Security Testhing Methodology Manual* (OSSTMM) tercantum pada bagan dibawah ini:



Gambar 3.1 Alur Penelitian

Alur penelitian ditunjukan pada Gambar.1 dimulai dengan melakukan wawancara dan studi literatur, analisis, implementasi, penilaian RAV dan STAR, serta alur terakhir adalah menyusun laporan.

3.1 BAHAN DAN ALAT PENELITIAN

Penelitian ini menggunakan *website* Repository Unjaya dengan alamat domain *repository.unjaya.ac.*id sebagai objek untuk dicari celah keamanan dan kerentanannya.

Penelitian ini menggunakan Laptop dengan spesifikasi RAM 8GB dan media penyimpanan 512GB untuk menjalankan *operating system* (OS) dan software pengembangan serta terkoneksi dengan internet. Selain Laptop dengan spesifikasi yang cukup, penelitian ini juga memerlukan OS dan software berikut:

1. OS Windows 11.
2. Software Google Crome

PERPUSTAKAAN UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA

3. Software Edge
4. Netcraft
5. Nmap
6. Nikto Scanner
7. Oracle VM Virtual Manager
8. OWASP ZAP

3.2 JALAN PENELITIAN

Penelitian ini akan dilakukan dengan 5 tahap. Tahapan ini dilakukan untuk menciptakan penelitian yang berjalan dengan lancar dan terstruktur, tahapan-tahapan yang digunakan dalam *"Analisis Kerentanan Pada Domain repository.unjaya.ac.id Menggunakan metode Open Source Security Testing Methodology Manual (OSSTMM)"* ini adalah

1. Wawancara dan Studi Pustaka
2. Analisis
3. Implementasi
4. Penilaian menggunakan RAV dan STAR
5. Laporan

3.2.1 Wawancara

Wawancara dilakukan kepada pihak pengelola *website repository.unjaya.ac.id* di Universitas Jenderal Achmad Yani Yogyakarta untuk menggali informasi terkait Sistem yang diteliti. Sedangkan untuk memperoleh pengetahuan tentang kajian ilmu seperti tes keamanan, pengujian *website*, kerentanan *website* dan serangan *website* serta kajian lain yang pernah dilakukan sebelumnya.

3.2.2 Analisis

Analisis diperlukan sebelum melakukan penelitian ini guna mendapat informasi lebih lanjut dari data-data yang diperoleh dari tahap sebelumnya. Penelitian ini menggunakan OSSTMM versi 3.0 untuk menentukan:

PERPUSTAKAAN UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA

1. Aset

   Segala sesuatu yang memiliki nilai dan objek yang akan dilindungi.

2. *Zona Engagement*

   Ruang lingkup pengujian dilakukan dapat mencakup jaringan, sistem atau lingkungan fisik dari aset

3. Skop

   Batasan-batasan yang ditetapkan dalam pengujian

4. *Vektor*

   Pengelompokan aset-aset yang ada di dalam skop berdasarkan arah interaksinya.

5. *Channel*

   Channel adalah mengidentifikasi peralatan yang dibutuhkan untuk melakukan uji dan mengkategorikannya berdasarkan fungsi atau dapat diartikan juga sebagai saluran komunikasi antar entitas.

   a. *Human security channel* (Saluran keamanan manusia)
   b. *Physical security channel* (Saluran keamanan aset fisik)
   c. *Wireless security channel* (Saluran keamanan nirkabel)
   d. *Telecommunication security channel* (Saluran keamanan telekomunikasi)
   e. *Data network channel* (Saluran jaringan data)

6. Jenis Uji.

   Melakukan uji yang digunakan dalam setiap pengujian harus didasari dengan informasi apa yang ingin dihasilkan. Berikut adalah uji yang ada pada Open Source Securiy Testhing Methodology Manual (OSSTMM) :

   a. *Black box testing*

      Metode pengujian perangkat lunak yang dilakukan tanpa mengetahui detail internal dari kode atau struktur internal dari sistem yang diuji. Dalam *black box testing*, pengujian dilakukan berdasarkan spesifikasi fungsional dan persyaratan eksternal dari perangkat lunak tersebut.

UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA PERPUSTAKAAN

b. *Double Blind*

Uji yang dilakukan kedua belah pihak, yaitu penguji dan target tujuannya untuk mensimulasikan serangan dari penyerang tidak dikenal, dengan syarat penguji tidak memiliki akses informasi target dan sebaliknya.

c. *Blind*

Uji yang dilakukan satu arah, namun penguji memiliki pengetahuan penuh tentang target.

d. *Gray Box*

Penguji hanya memiliki pengetahuan terbatas tentang target

e. *Double Gray Box*

Pengetahuan penguji tentang target terbatas dan kedua pihak tidak memiliki informasi lengkap tentang satu sama lain.

f. *Tandem*

Uji ini melibatkan dua tim penguji terpisah tetapi tetap berkoordinasi satu sama lain,, nantinya satu tim penguji berperan sebagai penyerang dan tim lain bertahan tujuannya untuk mensimulasikan respon yang realistis dalam situasi nyata.

g. *Reversal*

Uji ini adalah kebalikan dari uji tandem, kedua tim akan bertukar tugas tujuannya untuk memahami perspektif dan strategi dari kedua belah pihak

7. *Rules of engagement*

Pedoman tersebut dirancang untuk menjamin bahwa pengujian keamanan dilaksanakan dengan benar, sehingga menghindari kesalahpahaman atau hasil yang tidak akurat.

3.2.3 Implementasi

Implementasi dilakukan dengan menggunakan Sistem Oprasi Windows dan aplikasi testing yang ada seperti Netcraft, Nmap, Nikto dan OWASP ZAP. Adapun tahapan yang ada pada implementasi ini berupa;

PERPUSTAKAAN UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA

1. *Reconnaissance* / *information gathering*

   Tahapan *Reconnaissance* / information *gathering* ini menggunakan aplikasi Netcraft untuk mengumpulkan informasi dari *website* Repositori Unjaya. Netcraft adalah sebuah *tools* browser *anti-phishing* yang dapat berjalan di Microsoft Internet Explorer dan Firefox. Teknik yang digunakan Netcraft untuk menentukan keabsahan sebuah situs web meliputi teknik *sniffing* (analisis lalu lintas jaringan), metode *heuristik* (mendeteksi ancaman atau anomali) dan daftar situs web yang masuk daftar hitam yang tersimpan dalam basis data Netcraft. Selain itu, *toolbar* ini juga memeriksa popularitas situs, lokasi *hosting*, dan penilaian dari pengguna(Nduati dkk., t.t.).

2. *Scanning network*

   Scanning *network* dilakukan dengan memanfaatkan aplikasi Nmap untuk melakukan *scanning port* pada *website* Repository Unjaya . Nmap dirancang untuk dapat melakukan pemindaian jaringan besar maupun pemindaian *host* tunggal. Alat ini menggunakan paket IP untuk mengidentifikasi host yang aktif di dalam jaringan, *port-port* yang terbuka, sistem operasi yang digunakan, dan jenis *firewall* yang diterapkan. Nmap, singkatan dari *Network Mapper*, adalah alat sumber terbuka yang digunakan khusus untuk eksplorasi jaringan dan audit keamanan jaringan (Bayu Rendro & Nugroho Aji, 2020).

3. *Scanning vulnerability*

   Tahapan *scanning vulnerability* menggunakan Nikto, Nikto akan mulai melakukan *scanning* terhadap target yaitu *website repository.unjaya.ac.id.* Proses ini akan mencari berbagai jenis kerentanan dan kelemahan yang umumnya terdapat pada aplikasi web dan server. Setelah proses *scanning* selesai, Nikto akan menyediakan laporan yang mencakup informasi tentang kerentanan yang ditemukan, potensi risiko yang terkait, dan saran untuk mitigasi.

UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA PERPUSTAKAAN

4. *Penetration test*

Tahap implementasi keempat *penetration testing*, pada tahapan ini akan dilakukan scanning dan penyerangan otomatis menggunakan aplikasi OWASP ZAP. *Open Web Application Security Project- Zed Attack Proxcy* (OWASP ZAP) adalah aplikasi atau *tools* pengujian kerentanan bersifat *open source* yang digunakan untuk menemukan kerentanan melalui proses *attack* dan *scanning website* tertentu, dan memberikan rekomendasi untuk memperbaiki kerentanan yang ditemukan di *website* tersebut. Sedangkan *Open Web Application Security Project* (OWASP) sendiri merupakan organisasi yang menemukan aplikasi OWASP ZAP (Abdul F dkk., 2023).

Tabel 3.1 Informasi dari *Tools*

No.	Tahapan	Tools	Informasi Diperoleh
1.	*Information Gathering*	Netcraft	• *Register domain name* • Tanggal pendaftaran dan Kadaluarsa • Informasi pribasi pemilik domain (nama, alamat, informasi kontak dan innformasi lainnya) • Informasi server dan alamat IP • Server *web* • Sistem oprasi • Perangkat lunak • Keberadaan, konfigurasi dan hosting • Sejarah *uptime* dan Performa server
2.	*Scanning Network*	Nmap	• *Port* terbuka • Topologi *port* • Versi perangkat lunak yang berjalan di *port* • Sistem operasi yang dijalankan host

PERPUSTAKAAN UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA

No.	Tahapan	Tools	Informasi Diperoleh
3.	*Scanning Vulnerability*	Nikto *Scanner*	• Kerentanan (bug, celah keamanan, atau konfigurasi yang rentan) • Kofigurasi server *web* yang tidak aman/potensial • Kerentanan *scripting*
4	*Penetration Testing*	OWASP ZAP	• Kerentanan yang dapat dieksploitasi secara aktif di server dan *web* • Eksploitasi kerentanan

Tabel 3.1 menunjukkan informasi yang diperoleh dari penggunaan *tools* Netcraft, Nmap, dan OWASP ZAP Informasi dari *tools-tools* inilah yang nantinya akan digunakan peneliti untuk mencari *RAV Score* dan pertanyaan penelitian.

3.2.4 Penilaian RAV dan STAR

Pengujian menggunakan metode OSSTMM juga memerlukan RAV (*Risk Assessment Value*) dan STAR (*Security Testing Audit Report)* didalamnya. Berikut adalah penjelasan lebih lanjut tentang RAV dan STAR yang digunakan dalam penelitian ini berdasarkan ISECOM 3.0.

1. *Risk Assessment Value* (RAV)

Risk Assessment Value adalah metrik yang menunjukan kualitas proteksi keamananan dari ancaman yang mungkin terjadi (Fernando & Abdillah, 2016). RAV adalah penilaian kuantitatif yang digunakan untuk menganalisis hasil uji dan menentukan *RAV Score*. Kriteria yang digunakan untuk mencari *RAV Score* adalah *Oprational Security*, *Loss Control* dan *Limitations* (Ilmi dkk., 2022).

a. *Opsec (Oprational Security)*

Oprational Security adalah penilaian yang berkaitan dengan perlindungan sistem dari gangguan, penyusupan dan kegagalan termasuk memverifikasi langkah-langkah keamanan tetap efektif walau dalam ancaman tinggi, serta memastikan sistem dapat diakses tepat waktu ke layanan dan oprasi yang diperlukan oleh pengguna,

PERPUSTAKAAN UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA

kedua kondisi ini biasa disebut dengan ketahanan dan kontinuitas. *Opsec* memiliki tiga kategori penilaian dengan skala penilaian yang berbeda dimasing-masing kategorinya, yaitu :

1) *Visibility* memiliki skala penilaiann 0 sampai 3, menunjukkan seberapa terlihat operasi terhadap ancaman potensial.
2) *Access* memiliki skala penilaian 0 sampai 3, menunjukkan seberapa mudah entitas tidak sah dapat mengakses sistem.
3) *Trust* memiliki skala penilaian 0 sampai 4, mengevaluasi tingkat kepercayaan dalam oprasi.

b. *Loss Control*

Control adalah mekanisme keamanan yang diterapkan untuk melindungi sistem. Ada dua kelas yang terdiri dari masing-masing 5 kategori control yang harus dicari nilainya untuk menentukan nilai total *Loss Control* (Herzog, 2010). Berbeda dengan *Opsec* skala penilaian pada *Loss Control* ditentukan oleh peneliti, misalnya peneliti menyediakan 10 pertanyaan terkait, maka masing-masing pertanyaan akan mendapatkan nilai 1, apabila sistem yang diuji memenuhi pertanyaan maka akan mendapat nilai 1, jika tidak akan masuk ke nilai *missing*. Sedangkan dua kelas yang dimiliki oleh *Loss Control* adalah sebagai berikut :

1) Interactive
   a) *Autentication* (Authentikasi)
   b) *Indemnification* (Indemnifikasi)
   c) *Resilience* (Ketahanan)
   d) *Subjugation* (Subjugasi)
   e) *Continuity* (Kontinuitas)

2) Process
   a) *Non-repudiation* (Non-repudiaton)
   b) *Confidentiality* (Kerahasiaan)
   c) *Privacy* (Privasi)
   d) *Integrity* (Integritas)

UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA PERPUSTAKAAN

e) Alarm

c. Limitations

Limitations adalah cacat yang ditemukan dalam proteksi dan kontrol, nilai dari *limitations* diturunkan dari nilai *Opsec* dan *Loss Control* yang telah ditetapkan. Skala penilian dari *Limitations* diperoleh dari *scanning* menggunakan *tools-tools* penelitian. Penilaiannya dibagi kedalam 5 kategori, yaitu:

1) *Vulnerabilities* (kerentanan)
2) *Weaknesses* (kelemahan)
3) *Concerns* (kekhawatiran)
4) *Exposure* (paparan)
5) *Anomalies* (penyimpangan)

Hasil akhir dari *Opsec, Loss Controls* dan *Limitations* akan berupa *RAV score*, dengan *RAV score* inilah akan ditentukan apakah sistem tersebut memiliki keamanan yang sempurna, keamanan lemah atau keamanan berlebih. Berikut adalah tabel kategori yang digunakan dalam menentukan kategori *RAV Score* berdasarkan OSSTMM 3.0 (Ilmi dkk., 2022).

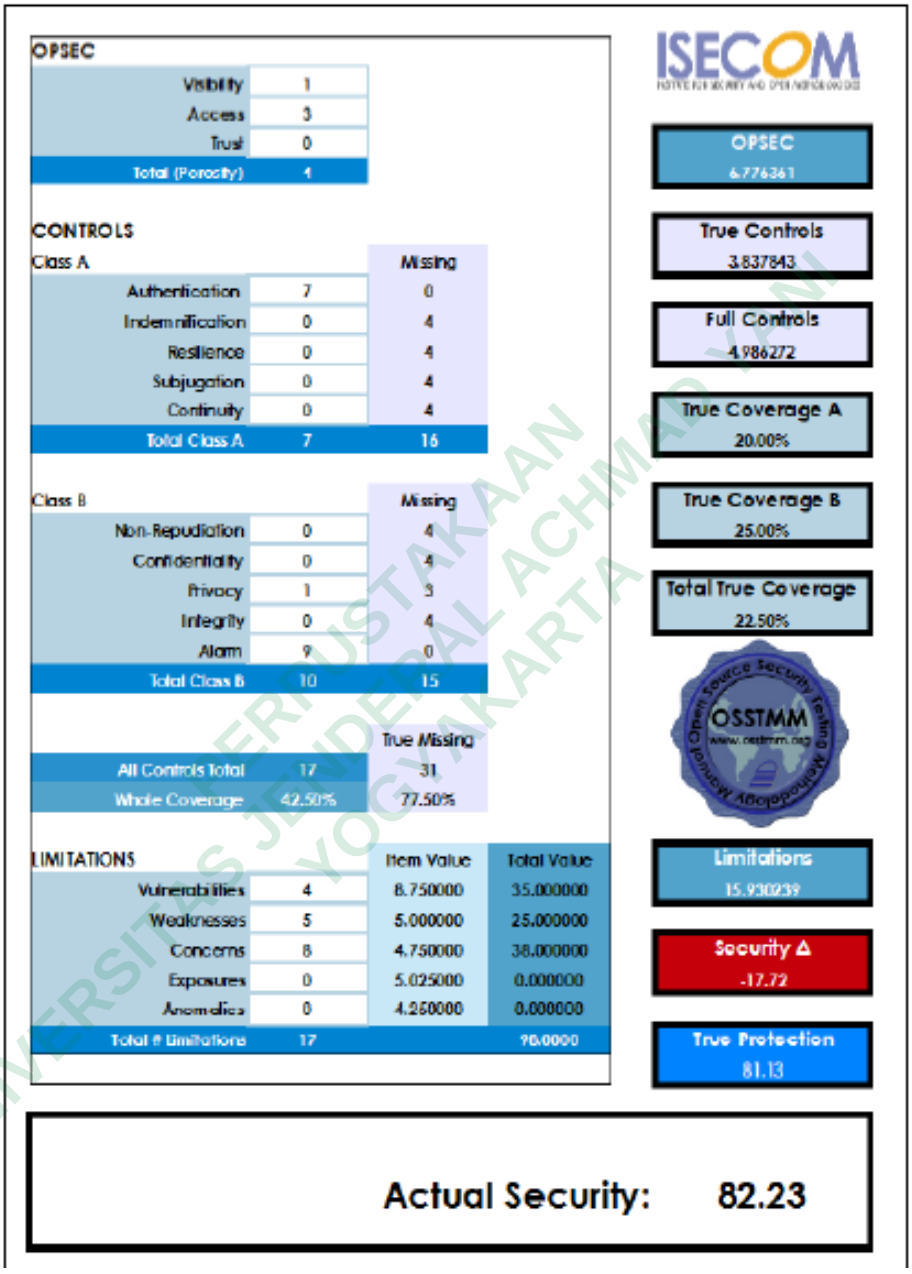
Tabel 3.2 Kategori *RAV Score*

Hasil	Keterangan
100	**Keamanan sempurna**. Nilai ini didapat dari hasil interaksi dan kontrol yang seimbang
<100	**Keamanan kurang.** Nilai ini diperoleh dari jumlah interaksi yang lebih banyak dari kontrol sehingga serangan *(attack suface)* lebih besar.
>100	**Keamanan berlebihan**. Nilai ini diperoleh dari jumlah interaksi yang lebih sedikit sibandingkan dengan jumlah kontrol. Hal ini dapat mengakibatkan terjadinya kompleksitas dan pemeliharaan.

Tabel 3.2 menunjukkan pengelompokan hasil test yang dilakukan menggunakan RAV bila mendapat hasil nilai 100 maka keamananan *website* tersebut stabil/sempurna, bila mendapatkan hasil nilai <100 maka

PERPUSTAKAAN UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA

keamanannya masih lemah, dan apabila mendapatkan hasil nilai >100 maka keamananya berlebihan.



Gambar 3.2 Form Penilaian RAV

Gambar 3.2 menunjukkan contoh penilaian RAV menggunakan OSSTMM 3.0 memiliki *RAV Score* 82.23 dan termasuk ke kategori sistem dengan keamanan kurang.

2. STAR (*Security Testing Audit Reposrt*)

Security Testing Audit Report (STAR) adalah status dan komentar yang dihasilkan dari pengujian keamanan yang dilakukan (Nabila dkk., 2023), atau pengertian lebih detailnya adalah dokumen yang berperan sebagai laporan pengujian mendetail, mencatat setiap aspek penelitian keamanan yang dilakukan termasuk informasi seperti tanggal dan waktu pengujian, durasi, identitas analis, jenis dan cakupan pengujian, serta berbagai metrik yang digunakan untuk menilai permukaan serangan. Dokumen ini juga mencatat masalah yang dihadapi selama pengujian, selesai tidaknya pengujian, seberapa valid hasilnya, limitasi yang mempengaruhi hasil.

3.2.5 Laporan

Laporan ini merupakan hasil dari rangkaian tahapan yang dilakukan dalam penelitian ini. Tujuan dari penyusunan laporan ini adalah untuk menyajikan temuan dan hasil evaluasi dari *website repository.unjaya.ac.id.* Laporan ini disusun secara sistematis dimulai dari latar belakang, tujuan penelitian, tinjauan pustaka, landasan teori, metode penelitian dan jadwal penelitian, yang menjelaskan latar belakang, tujuan, dan ruang lingkup penelitian. Selain itu penelitian ini menyajikan hasil penilaian menggunakan RAV *(Risk Asessment Value)* dan STAR *(Security Testing Audit Report),* yang akan memberikan gambaran lebih jelas tentang tingkat risiko terkait dari setiap kerentanan yang ditemukan.

Laporan ini diharapkan dapat menjadi panduan berharga bagi pihak terkait, termasuk pengelola *website repository.unjaya.ac.id* dan pihak yang bertanggungjawab atas keamanan informasi di lingkungan tersebut untuk pemeliharaan dan pengelolaan *website* di masa mendatang.

PERPUSTAKAAN UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA