BAB II
LANDASAN TEORI

2.1 Profil dan tempat penelitian

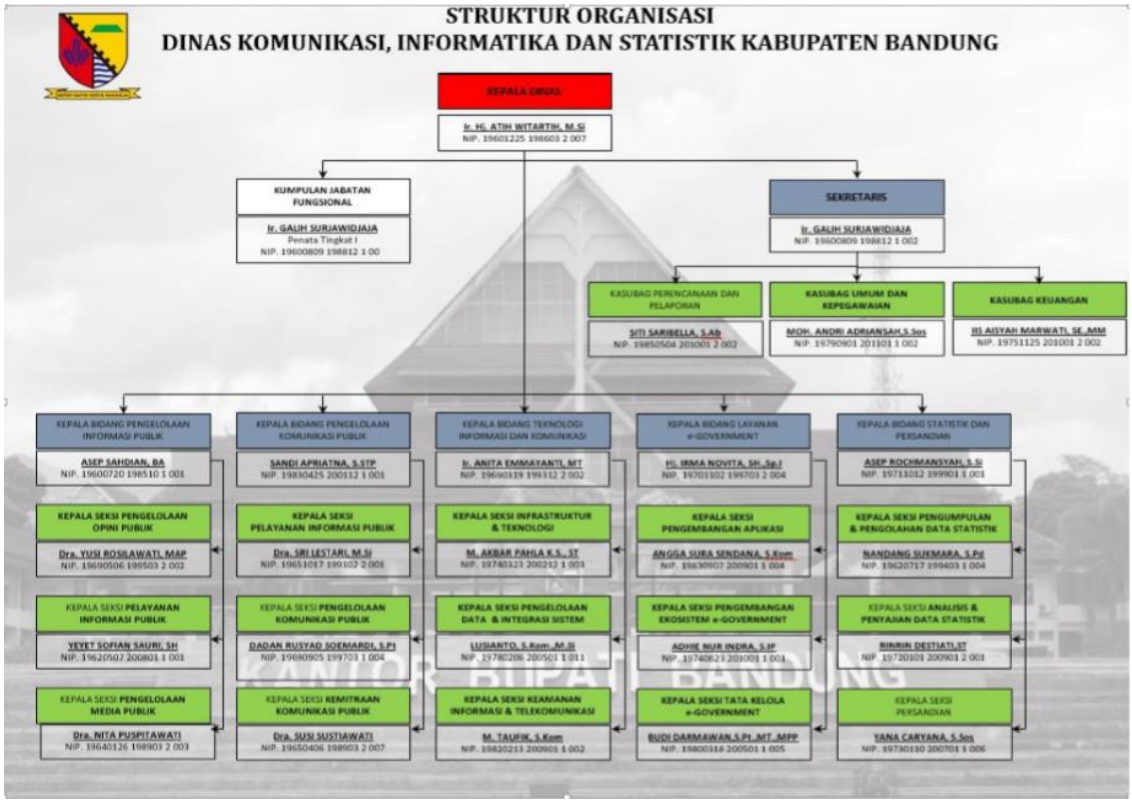
Pada bagian profil dan tempat penelitian akan dijelaskan beberapa informasi mengenai tempat di mana dilakukannya penelitian, bagan organisasi yang berada ditempat penelitian serta tugas pokok dari tiap-tiap bagian organisasi.

2.1.1 Profil Diskominfo Kabupaten Bandung

Dinas Komunikasi ,Informasi dan Statistik Kabupaten Bandung merupakan salah satu Satuan Kerja Perangkat Daerah yang dimiliki oleh Pemerintah Kabupaten Bandung yang berfokus pada "Layanan pengelolaan informasi TIK, layanan *E-Government* dan layanan statistik dan persandian".Pada periode-periode sebelumnya Dinas Komunikasi, Informasi dan Statistik berasal dari BAPAPSI yang dibentuk berdasarkan Peraturan Daerah Kabupaten Bandung No.21 tahun 2007 tentang Pembentukan Organisasi Lembaga Teknis Daerah Kabupaten Bandung Terhitung 1 April 2008. Berdasarkan Perda No.21 tahun 2017 ini Kantor Perpustakaan Daerah, Kantor Arsip Daerah, Badan Pengembangan Informasi Darah dan Kantor Pengolahan Data Elektronik digabungkan menjadi SKPD baru dengan nama BAPAPSI (Badan Perpustakaan, Arsip dan Pengembangan Sistem Informasi) yang kemudian terpecah kembali menjadi beberapa dinas dan salah-satunya adalah DISKOMINFO (Dinas Komunikasi, Informasi dan Statistik) yang didirikan di masa transisi pada tahun 2016 hingga 2017 awal.

2.1.2 Struktur Organisasi

Struktur Organisasi merupakan relasi kedudukan penanggung jawab dari masing-masing divisi yang berada di dalam suatu organisasi, dimulai dari



Gambar 2. 1 Struktur Organisasi Diskominfo Kabupaten Bandung

kedudukan tertinggi hingga yang terendah. Berikut merupakan struktur Organisasi dari Dinas Komunikasi, Informasi dan Statistik Kabupaten Bandung [4]

Dalam menjalankan Tugas Pokok, Fungsi dan Tata Kerja Dinas Komunikasi, Informasi dan Statistik Kabupaten Bandung, dipimpin oleh Kepala Dinas yang pelaksanaannya dibantu oleh beberapa komponen pendukung lainya. Berikut merupakan rincian Tugas Pokok, Fungsi dan Tata Kerja Dinas Komunikasi, Informasi dan Statistik Kabupaten Bandung.

1. Kepala Dinas

   Mempunyai tugas pokok memimpin, mengatur, merumuskan, membina, mengendalikan, mengkoordinasikan dan mempertanggung jawabkan kebijakan dan pelaksanaan urusan pemerintahan di bidang pengelolaan Komunikasi Publik, Informatika, Statistik dan Persandian.

2. Sekretaris

Mempunyai tugas pokok memimpin, mengkoordinasikan dan mengendalikan tugas di bidang pengelolaan pelayanan kesekretariatan yang meliputi pengkoordinasian penyusunan program, pengelolaan umum dan kepegawaian serta pengelolaan keuangan.

3. Subbagian Penyusunan Program

   Mempunyai tugas pokok merencanakan, melaksanakan, mengevaluasi dan melaporkan pelaksanaan tugas pelayanan dan pengkoordinasian penyusunan rencana dan program Diskominfo.

4. Subbagian Umum dan Kepegawaian

   Mempunyai tugas pokok merencanakan, melaksanakan, mengevaluasi dan melaporkan pelaksanaan tugas pelayanan administrasi umum dan kerumahtanggaan serta administrasi kepegawaian.

5. Subbagian Keuangan

   Mempunyai tugas pokok merencanakan, melaksanakan, mengevaluasi dan melaporkan pelaksanaan tugas pengelolaan administrasi dan pertanggungjawaban pengelolaan keuangan Diskominfo.

6. Bidang Pengelolaan Informasi publik

   Mempunyai tugas pokok memimpin, mengkoordinasikan dan mengendalikan tugas di bidang Pengelolaan Opini Publik, Pengelolaan Informasi Publik dan Pengelolaan Media Publik.

7. Seksi Pengelolaan Opini Publik

   Mempunyai tugas pokok merencanakan, melaksanakan, mengevaluasi dan melaporkan pelaksanaan tugas pelayanan dan pengelolaan opini publik.

8. Seksi Pengelolaan Informasi Publik

   Mempunyai tugas pokok merencanakan, melaksanakan, mengevaluasi dan melaporkan pelaksanaan tugas pelayanan dan pengelolaan informasi publik.

9. Seksi Pengelolaan Media Publik

Mempunyai tugas pokok merencanakan, melaksanakan, mengevaluasi dan melaporkan pelaksanaan tugas pelayanan dan pengembangan informasi multimedia.

10. Bidang Pengelolaan Komunikasi Publik

    Mempunyai tugas pokok memimpin, mengkoordinasikan dan mengendalikan tugas di bidang pelayanan informasi publik, pelayanan komunikasi publik, dan kemitraan komunikasi publik.

11. Seksi Pelayanan Informasi Publik

    Mempunyai tugas pokok merencanakan, melaksanakan, mengevaluasi dan melaporkan pelaksanaan tugas pengelolaan dan pelayanan informasi publik.

12. Seksi Pelayanan Komunikasi Publik

    Mempunyai tugas pokok merencanakan, melaksanakan, mengevaluasi dan melaporkan pelaksanaan tugas pelayanan dan pelayanan komunikasi publik.

13. Seksi Kemitraan Komunikasi Publik

    Mempunyai tugas pokok merencanakan, melaksanakan, mengevaluasi dan melaporkan pelaksanaan tugas pengelolaan kemitraan komunikasi publik.

14. Bidang Teknologi, Informasi dan Komunikasi

    Mempunyai tugas pokok memimpin, mengkoordinasikan dan mengendalikan tugas di bidang infrastruktur dan teknologi, pengelolaan data dan integrasi sistem informasi dan keamanan informasi dan telekomunikasi.

15. Seksi Infrastruktur dan Teknologi

    Mempunyai tugas pokok merencanakan, melaksanakan, mengevaluasi dan melaporkan pelaksanaan tugas pelayanan dan pengembangan infrastruktur dan teknologi.

16. Seksi Pengelolaan Data dan Integrasi Sistem Informasi

Mempunyai tugas pokok merencanakan, melaksanakan, mengevaluasi dan melaporkan pelaksanaan tugas pelayanan dan pengelolaan data dan integrasi sistem informasi.

17. Seksi Keamanan Informasi dan Telekomunikasi

    Mempunyai tugas pokok merencanakan, melaksanakan, mengevaluasi dan melaporkan pelaksanaan tugas pelayanan keamanan informasi dan telekomunikasi.

18. Bidang Layanan *e-Government*

    Mempunyai tugas pokok memimpin, mengkoordinasikan dan mengendalikan tugas di bidang Pengembangan Aplikasi, Pengembangan Ekosistem *e-Government* dan Tata Kelola *e-Government.*

19. Seksi Pengembangan Aplikasi

    Mempunyai tugas pokok merencanakan, melaksanakan, mengevaluasi dan melaporkan pelaksanaan tugas pelayanan dan pengembangan aplikasi.

20. Seksi Pengembangan Ekosistem *e-Government*

    Mempunyai tugas pokok merencanakan, melaksanakan, mengevaluasi dan melaporkan pelaksanaan tugas pelayanan dan pengembangan ekosistem *e-government*.

21. Seksi Tata Kelola *e-Government*

    mempunyai tugas pokok merencanakan, melaksanakan, mengevaluasi dan melaporkan pelaksanaan tugas pelayanan dan pengembangan tata kelola *e-government*.

22. Bidang Statistik dan Persandian

    Mempunyai tugas pokok memimpin, mengkoordinasikan dan mengendalikan tugas di bidang pengumpulan dan pengolahan data statistik, analisa dan penyajian data statistik dan persandian.

23. Seksi Pengumpulan dan Pengolahan Data Statistik

Mempunyai tugas pokok merencanakan, melaksanakan, mengevaluasi dan melaporkan pelaksanaan tugas pelayanan pengumpulan dan pengolahan data statistik.

24. Seksi Analisa dan Penyajian Data Statistik

    Mempunyai tugas pokok merencanakan, melaksanakan, mengevaluasi dan melaporkan pelaksanaan tugas pelayanan dan pengembangan analisa dan penyajian data statistik.

25. Seksi Persandian

    Mempunyai tugas pokok merencanakan, melaksanakan, mengevaluasi dan melaporkan pelaksanaan tugas pelayanan dan pengembangan analisa dan penyajian data statistik.

2.2 Landasan Teori

Pada Landasan Teori akan dijelaskan metode yang digunakan di dalam penelitian, teori-teori pendukung serta tools yang yang digunakan penelitian.

2.2.1 Internet

Internet merupakan hubungan antara berbagai jenis komputer dan jaringan di dunia yang berbeda sistem operasi maupun aplikasinya, di mana hubungan tersebut memanfaatkan kemajuan komunikasi (telepon dan satelit) yang menggunakan protokol standar dalam berkomunikasi yaitu protokol *TCP/IP* (*Transmission Control/Internet Protocol*) [5].

Secara sederhana internet dapat diartikan sebagai kumpulan dari beberapa komputer, bahkan jutaan komputer di seluruh dunia yang saling berhubungan atau terkoneksi satu sama lainnya. Media yang digunakan bisa menggunakan kabel/serat optik, satelit atau melalui sambungan telepon [6]. Internet sudah menjadi sebuah kebutuhan yang tidak dapat dipisahkan dari kehidupan sehari-hari, baik kalangan remaja, pekerja dan lansia membutuhkan internet sebagai sarana untuk mendapatkan dan penyampaian informasi.

Dalam penelitian ini koneksi internet dibutuhkan untuk dapat melakukan tahapan I*nformation Gathering* dan *security assessment* pada *website* yang ditargetkan dalam penelitian ini.

2.2.2 Keamanan Informasi

Landasan dari Keamanan adalah aset yang harus dilindungi, aset bisa berbentuk manusia sesuatu yang dibuat oleh manusia atau alam namun di dalam Keamanan Informasi, hal yang menjadi aset merupakan informasi. Baik itu informasi yang dapat dikemukakan secara publik maupun rahasia [7].

Masalah yang terdapat di dalam keamanan informasi terbagi menjadi dua yaitu *Threats* (Ancaman) dan *Vulnerability* (Kerentanan). Ancaman merupakan aksi yang dilakukan baik dari dalam atau pun dari luar sistem yang dapat menimbulkan terganggunya keseimbangan sistem informasi. Ancaman terhadap sistem informasi ini dilakukan oleh individu, organisasi, mekanisme, atau kejadian yang memiliki potensi untuk menyebabkan kerusakan terhadap sumber informasi perusahaan. Ancaman juga dapat ditimbulkan dengan sengaja atau tidak sengaja. Kemudian Kerentanan adalah kelemahan dari suatu sistem yang digunakan terlepas dari dilakukan pemeliharaan, saat sistem tidak terpelihara dengan baik maka akan terdapat kerentanan yang dapat di *eksploitasi* oleh individu atau pun organisasi.

Keamanan Informasi terdiri dari perlindungan terhadap beberapa aspek-aspek sebagai berikut [8] :

1. *Confidentality* (Kerahasiaan) aspek yang menjamin kerahasiaan data atau informasi, memastikan bahwa informasi hanya dapat diakses oleh orang yang berwenang dan menjamin kerahasiaan data yang di kirim, di terima dan di simpan.
2. *Integrity* (Integritas) Aspek yang menjamin bahwa data tidak diubah tanpa izin pihak yang berwenang, menjaga keakuratan dan keutuhan informasi serta metode prosesnya untuk menjamin aspek integritas ini.

3. *Availability* (Ketersediaan) aspek yang menjamin bahwa data akan tersedia saat dibutuhkan, memastikan pengguna yang berhak dapat menggunakan informasi dan perangkat terkait.



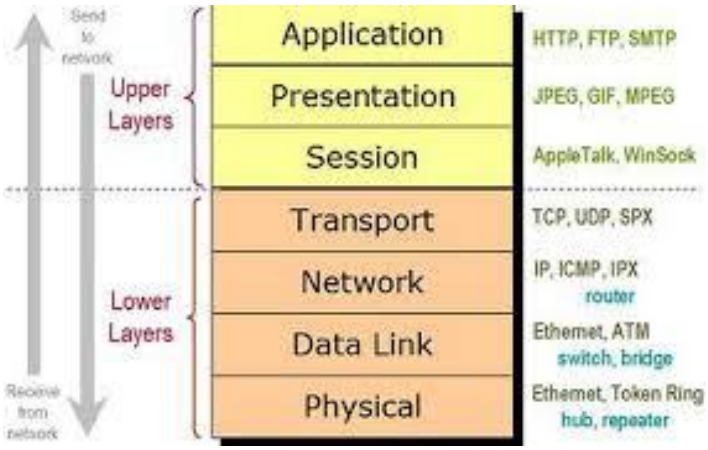
Gambar 2. 2 Elemen -Elemen Keamanan Informasi

Keamanan informasi merupakan salah satu aspek sangat penting dan harus dipahami, karena di dalam penelitian ini keamanan informasi salah satu landasan dan alasan mengapa penelitian ini dilakukan.

2.2.3 Open Sistem Interconnection

Model *Open Systems Inteconnection (OSI)* merupakan kerangka terstruktur mengenai proses komunikasi data dan interaksi yang terjadi melalui jaringan yang diciptakan oleh *Organization for Standardization (ISO)* untuk industri komputer agar komputer dapat berkomunikasi dengan jaringan yang berbeda secara efisien [9].

Tujuan dari penggunaan Model *Open Systems Interconnection* adalah untuk membantu desainer jaringan agar memahami fungsi dari tiap-tiap layer yang berhubungan dengan aliran komunikasi data. Model *Open System Interconnection* dibagi menjadi tujuh layer, dengan karakteristik dan fungsinya masing-masing. Setiap layer dapat saling berkomunikasi dengan layer di atasnya maupun dibawanya secara langsung melalui serentetan protokol.



Gambar 2. 3 Model *Open Systems Interconnection (OSI)*

Berikut merupakan penjelasan dari masing masing layer :

1. *Application Layer*

   Application Layer terdiri dari bermacam-macan protokol. *Application Layer* berfungsi sebagai antarmuka aplikasi dengan fungsionalitas jaringan, mengatur bagaimana aplikasi dapat mengakses jaringan, dan kemudian membuat pesan-pesan kesalahan. Protokol dalam lapisan ini adalah *HTTP, FTP, SMTP* dan *NFS.*

2. *Presentation Layer*

   Presentation Layer memiliki fungsi untuk metranslasikan data yang hendak ditransmisikan dari aplikasi ke dalam format yang dapat ditransmisikan jaringan. Protokol yang berada dalam *Presentation Layer* ini adalah penghubung aplikasi, seperti layanan *Workstation, Network Shell, Virtual Network Computing* dan *Remote Desktop Protocol*.

3. *Session Layer*

   Session Layer memiliki fungsi untuk mendefinisikan koneksi agar dapat di buat, di perlihatkan atau di hancurkan. Selain itu di dalam *Session Layer* juga dilakukan resolusi nama.

4. *Transport Layer*

Transport Layer memiliki fungsi untuk memecah data ke dalam beberapa paker data serta memberikan nomor urut untuk masing-masing paket sehingga dapat disusun kembali pada sisi tujuan setelah masing-masing paket dikirimkan. Selain itu pada *Transport Layer* akan melakukan transmisi ulang bila terdapat paket yang hilang saat dilakukan pengiriman.

5. *Network Layer*

   Network Layer memiliki fungsi untuk mendefinisikan alamat-alamat IP dan membuat *header* untuk setiap paket data kemudian melakukan *routing* melalui *internetworking* dengan menggunakan *router* dan *switch*.

6. *Data Link Layer*

   Data Link Layer memiliki Fungsi untuk menentukan bagai mana bit-bit data yang dikirimkan dapat di kelompokan menjadi sebuah format dengan nama *Frame*. Selain itu, di dalam *layer* ini telah erjadi koreksi kesalahan, *flow cotrol*, pengelamatan perangkat keras (*MAC Address*), dan menentukan bagaimana perangkat-perangkat jaringan seperti *hub, bridge, repeater* dan *switch layer 2* beroperasi.

7. *Physical Layer*

   Physical Layer memiliki fungsi untuk mendefinisikan media transmisi jaringan, metode pensinyalan, sinkronisasi bit, arsitektur jaringan, topologi jaringan, dan pengkabelan. Selain itu, di dalam *layer* ini mendefinisikan bagaimana *NIC* dapat berinteraksi dengan media kabel dan radio.

Masing-masing layer dapat dilakukan pengujian penetrasi dan di dalam penelitian ini layer yang digunakan dalam *penetration testing* berada di *Application Layer*.

2.2.4 Proof Of Concept Exploit(PoC)

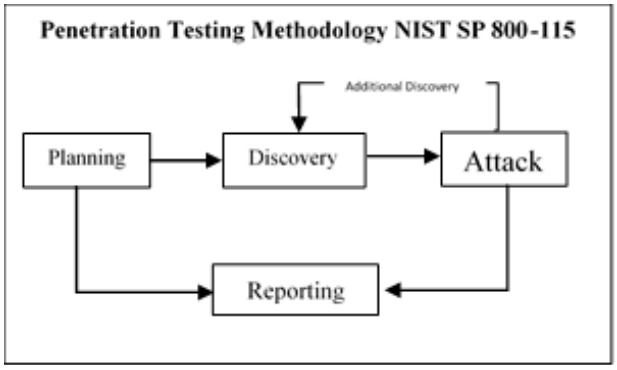
Proof Of Concept Exploit (PoC) merupakan sebuah bukti dari jenis eksploitasi terhadap sistem komputer atau jaringan yang dilakukan. Hal ini dilakukan untuk menunjukkan bahwa eksloitasi memang benar dilakukan, dan pada umumnya tidak menimbulkan kerugian dan ditujukan untuk memberitahukan bagaimana *hacker* memanfaatkan kerentanan yang terdapat pada suatu aplikasi.

Terdapat metode-metode penyerangan yang dapat dibuktikan *PoC* salah satu contohnya adalah *Sql Injection*. Dengan memperagakan persiapan dalam penyerangan, fase penyerangan dan eksploitasi celah. Selain itu masih banyak *PoC* lainya yang digunakan untuk melakukan penyerangan terhadap *website* yang dituju.

Di dalam penelitian ini *PoC* dibutuhkan untuk menunjukkan bahwa di dalam fase Penetrasi, eksploitasi yang dilakukan terhadap kerentanan *website*, telah berhasil atau tidak.

2.2.5 NIST SP 800-115

NIST SP 800-115 merupakan panduan yang dikeluarkan oleh *The National Institute of Standards and Technology (NIST) yang* berdiri pada tahun 1901 dan sekarang telah bergabung dengan Departemen perdagangan Amerika Serikat [3]. *Document* ini dikelukan untuk membantu proses pengujian *website* akan kerentanan-kerentanan yang terdapat pada *website*, metode yang dapat dilakukan dalam pengujian (*Pentration Testing*) dan rekomendasi yang harus dilakukan dalam menangani kerentanan pada *website*.



Gambar 2. 4 Metode NIST SP 800-115

Berikut merupakan tahapan-tahapan dari metode NIST SP 800-115 berdasarkan pada gambar 2.4.

1) Planning

Pada tahapan ini akan ditentukan aturan-aturan yang akan disepakati untuk melakukan *penetration testing*, tujuan akhir dari *penetration testing* dan persiapan persiapan yang harus dilakukan untuk berjalanya *penetration testing*.

2) Discovery

Pada tahap *Discovery* terdapat dua fase yang harus dilakukan yaitu :

1) Information Gathering

Information Gathering merupakan pengumpulan informasi-Informasi mengenai *website* yang akan diuji. Salah satu contoh adalah *Network Mapping*.

2) *Vulnerability Scanning*.

Vulnerability Scanning merupakan tahapan di mana *website* akan melakukan pemindaian menggunakan *tools* khusus yang digunakan untuk memindai kerentanan.

3) Attack

Pada tahap ini akan dilakukan eksploitasi atau pengujian terhadap kerentanan yang telah ditemukan, mendapatkan hak akses dari *website* yang diuji dan melakukan validasi terhadap kerentanan yang ditemui.

4) Report

Pada tahap ini, hasil analisis dari kerentanan yang telah berhasil diuji, dilaporkan kepada pihak yang berkaitan.

Dokumen NIST SP 800-115 digunakan untuk membantu individual atau organisasi dalam melakukan perencanaan dan pengujian teknikal keamanan informasi. Dokumen ini memberikan rekomendasi untuk melakukan desain, implementasi dan pemeliharaan pengujian keamanan informasi sesuai prosedur.

Selain itu, *NIST SP-800-115* menyediakan metode *Penetration Testing* yang dibutuhkan dalam penelitian ini.

2.2.6 OWASP Risk Ranting Methodology

OWASP Risk Rating Methodology merupakan metodelogi yang digunakan untuk menentukan standar keamanan aplikasi. Standar menentukan risiko menurut *OWASP Risk Rating Methodology* yaitu [10]:

$$Risk = Likelihood * Impact$$

Untuk menentukan faktor *Likelihood* dan *Impact* maka dibutuhkan beberapa langkah yang harus dilakukan. Langkah-langkah tersebut adalah sebagai berikut [10] :

1. Identifikasi Risiko

   Langkah pertama yang dilakukan adalah mengidentifikasi risiko *security* yang akan di ranting. Penguji harus mengumpulkan informasi mengenai ancaman yang mungkin akan digunakan oleh penyerang, kerentanan dan dampak dari suksesnya penyerang melakukan eksploitasi pada kerentanan.

2. Faktor yang digunakan untuk estimasi *Likelihood*

   Setelah penguji mengidentifikasi potensi dari risiko tersebut dan mengetahui seberapa seriusnya ancamannya pada sistem, maka langkah selanjutnya adalah menentukan *Likelihood.* *Likelihood* pada dasarnya dibagi menjadi tiga level yaitu *low, medium* dan *high*.

   Berikut beberapa faktor yang digunakan untuk menentukan *likelihood.*

   1) *Threat agent Factor*

      Beberapa hal yang harus diperhatikan di dalam *Thread Agent Factor* adalah *Skill level, Motive, Opportunity* dan *Size*. Masing-masing dari pilihan memiliki nilai yang telah ditetapkan sebagai berikut

Tabel 2. 1 ***Threat Agent Factor***

Skill Level	Nilai diberikan berdasarkan keterampilan penguji atau penyerang 1. Berikan 1 jika tidak memiliki keterampilan 2. Berikan nilai 5 jika memiliki keterampilan teknik 3. Berikan nilai 6 untuk pengguna komputer lanjut 4. Beri nilai 9 jika memiliki Keterampilan Memprogram dan jaringan
Motive	Nilai diberikan berdasarkan motivasi penguji atau penyerang. 1. Berikan nilai 1 jika motivasi rendah 2. Berikan nilai 4 jika memungkinkan mendapat hadiah 3. Berikan nilai 9 untuk hadiah yang terima memuaskan
Opportunity	Berikan nilai berdasarkan kebutuhan yang di butuhkan oleh penyerang atau penguji dalam mencari dan melakukan eksploitasi kerentanan. 1. Berikan nilai 0 jika akses penuh atau kebutuhan yang dibutuhkan tinggi 2. Berikan nilai 4 jika terdapat akses spesial dan membutuhkan kebutuhan 3. Berikan nilai 7 jika terdapat beberapa akses dan kebutuhan 4. Berikan nilai 9 jika tidak ada akses dan tidak ada kebutuhan yang

	dibutuhkan
Size	Berikan nilai berdasarkan jenis penyerang. 1. Berikan nilai 2 untuk *developers* 2. Berikan nilai 2 untuk *system administrator* 3. Berikan nilai 4 untuk *intranet user* 4. Berikan nilai 5 untuk *patners* 5. Berikan nilai 6 untuk *authenticated users* 6. Berikan nilai 9 untuk pengguna internet yang tidak diketahui

2) Vulnerability Factor

Untuk faktor selanjutnya adalah *Vulnerability Factor* di mana faktor ini memiliki penilaian untuk *Ease of discovery, Ease of Exploit, Awareness* dan *Intrusion detection* yang nilainya telah ditetapkan. berikut merupakan nilai untuk setiap pilihan yang bias dipilih.

Tabel 2. 2 *Vulnerability Factor*

Ease of Discovery	Berikan nilai menemukan kerentanan. 1. Jika tidak mungkin ditemukan beri nilai 1 2. Jika sulit beri nilai 3 3. Jika mudah beri nilai 7 4. Jika tersedia *tools* otomatis beri nilai 9
Ease of Exploit	Berikan nilai berdasarkan seberapa mudah di lakukan eksploitasi. 1. Jika berdasarkan teori beri nilai 1 2. Jika sulit beri nilai 2 3. Jika muda beri nilai 5

	4. Jika tersedia *tools* otomatis beri nilai *9*
Awareness	Berikan nilai berdasarkan seberapa grup *threat agents* mengenal kerentanan. 1. Jika tidak di ketahui beri nilai 1 2. Jika tersembunyi beri nilai 4 3. Jika mengerti beri nilai 6 4. Jika di ketahui publik beri nilai 9
Intrusion detection	Berikan nilai berdasarkan bagai mana eksploitasi terdeteksi. 1. Jika menggunakan aplikasi pendeteksi beri nilai 1 2. Jika masuk dan ditinjau beri nilai 3 3. Jika masuk tanpa ditinjau beri nilai 8 4. Jika tidak masuk beri nilai 9

3. Faktor yang digunakan untuk estimasi *Impact*

   Selanjutnya jika di misalkan bahwa eksploitasi telah berhasil dilakukan oleh penyerang. Maka dibutuhkan estimasi tentang dampak yang dirasakan karena eksploitasi tersebut. Berikut merupakan faktor yang diperhatikan dalam menentukan estimasi *Impact :*

   1) Technical Impact Factors

   Pada faktor ini hal-hal yang harus diperhatikan dan ditentukan nilainya *adalah Loss of confidentiality, Loss of Intergrity, Loss of availability* dan *Loss of accountability* setiap nilai dari masing-masing pilihan telah ditetapkan.

Tabel 2. 3 *Technical Impact Factor*

Loss of confidentiality	Berikan nilai berdasarkan data yang terungkap atau bersifat sensitif.

	1. Untuk data bersifat non-sensitif dan terungkap beri nilai 2, 2. untuk data kritikal minimum yang terungkap beri nilai 6, 3. untuk data non-sensitif terungkap secara besar beri nilai 6, 4. untuk kritikal data terungkap luas beri nilai 7 5. untuk semua data terungkap beri nilai 9
Los of intergrity	Berikan nilai berdasarkan seberapa besar kerusakan data. 1. Jika minimal beri nilai 1 2. Jika serius dalam jumlah kecil beri nilai 3 3. Jika dalam sekala luas beri nilai 5 4. Jika serius dalam sekala luas beri nilai 6 5. Jika semua data rusak beri nilai 9
Loss of availability	Berikan nilai berdasarkan layanan yang hilang dan seberapa vital. 1. Jika pelayanan sekunder terganggu beri nilai 1 2. Jika pelayanan utama yang terganggu beri nilai 5 3. Jika pelayanan sekunder dalam skala luas beri nilai 5 4. Jika pelayanan primer dalam skala luas beri nilai 7 5. Jika semua layanan terganggu beri nilai 9

Loss of accountability	Berikan nilai berdasarkan aksi penyerang yang terdeteksi. 1. Jika terdeteksi penuh beri nilai 1 2. Jika kemungkinan terdeteksi beri nilai 7 3. jika tidak diketahui beri nilai 9

2) Business Impact Factors

Pada faktor ini hal-hal yang harus diperhatikan dan ditentukan nilainya adalah *Financial damage, Reputation damage, Non-compliance* dan *Privacy Violation*.

Financial damage	Berikan nilai berdasarkan kerusakan finansial yang terjadi karena eksploitasi. 1. Jika kurang dari biaya perbaikan kerentanan beri nilai 1 2. Jika terjadi efek kecil pada profit tahunan beri nilai 3 3. Jika terdapat efek signifikan pada profit tahunan beri nilai 7 4. Jika dapat menimbulkan bangkrut beri nilai 9
Reputation damage	Berikan nilai berdasarkan seberapa hasil eksploitasi dalam kerusakan reputasi, apakah dapat membahayakan bisnis. 1. Jika kerusakan kecil beri nilai 1 2. Jika kehilangan banyak akun beri nilai 4 3. Jika kehilangan niat baik beri nilai 5 4. Jika merusak merek beri nilai 9
Non-compliance	Berikan nilai berdasarkan ditemukannya pelanggaran

	1. Jika pelanggaran kecil beri nilai 2 2. Jika pelanggaran jelas beri nilai 5 3. Jika profil pelanggaran tinggi beri nilai 7
Privacy violation	Berikan nilai berdasarkan informasi personal yang terungkap 1. Jika personal beri nilai 3 2. Jika ratusan orang maka beri nilai 5 3. Jika ribuan orang maka beri nilai 7 4. Jika miliaran orang maka beri nilai 9

4. Menentukan tingkat risiko

   Setelah *Likelihood* dan *Impact* ditentukan. Langkah selanjutnya yang dilakukan adalah menentukan tingkat dari risiko, di mana

Likelihood and Impact Levels	
0 to <3	LOW
3 to <6	MEDIUM
6 to 9	HIGH

Gambar 2. 5 Tingkat resiko untuk *Likelihood* dan *Impact*

tingkat risiko dapat dilihat pada gambar berikut. :

tentukan nilai rata-rata dari *Likelihood* dan *Impact*, setalah nilai rata-ratanya didapat gunakan nilai *Likehood* dan *Impact* untuk menentukan risiko. Perlu diperhatikan jika memiliki *Business Impact Information* yang bagus, maka gunakan nilai dari *Tenichal Impact Information* untuk nilai *Impact*, namun jika tidak nilai *tenichal Impact* masih dapat digunakan.

Overall Risk Severity				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
	Likelihood			

Gambar 2. 6 klasifikasi tingkat resiko berdasarkan *Likelihood* dan *Impact*

Berikut merupakan tabel risiko yang digunakan untuk menentukan risiko.

5. Menentukan hal yang harus diperbaiki

   dengan demikian setelah tingkat risiko pada *website* telah diketahui dan diklasifikasikan maka akan mudah untuk mengatur *website* mana yang pertama harus di perbaiki.

Di dalam penelitian ini akan dilakukan *Risk Rating* menggunakan *OWASP Risk Rating Methodology* agar dapat menentukan risiko masing-masing *website* yang di kelola oleh Diskominfo Kabupaten Bandung.

2.2.7 Apache

Apache HTTP Server Project merupakan upaya pengembangan *software* kolaboratif yang bertujuan untuk menciptakan kuat, kelas komersial, *featureful*, dan bebas-tersedia penerapan kode sumber *HTTP* (Web) Server. Proyek ini dikelola bersama oleh sekelompok sukarelawan yang terletak di seluruh dunia, menggunakan Internet dan *website* untuk berkomunikasi, merencanakan, dan mengembangkan server dan dokumentasi terkait [11].

Proyek ini merupakan bagian dari *Apache Software Foundation.* Selain itu, ratusan pengguna telah menyumbangkan ide-ide, kode, dan dokumentasi untuk proyek. *File* ini dimaksudkan untuk menjelaskan secara singkat sejarah Server *Apache* HTTP dan mengakui banyak kontributor. *Apache* dikembangkan di bawah naungan *Apache Software Foundation* [11].

Dalam penelitian ini penting untuk mengetahui web server yang digunakan oleh *website* yang diuji, dan dalam penelitian ini, *website* yang diuji menggunakan *webserver Apache*.

2.2.8 *Common Weakness Enumeration* (*CWE*)

Common Weakness Enumeration (*CWE*) menyediakan antarmuka yang mudah digunakan data kerentanan web serta dapat menelusuri vendor, produk dan versi *CWE*. Anda dapat melihat statistik tentang vendor, produk dan versi produk. Rincian *CWE* ditampilkan dengan mudah secara satu halaman.

Data kerentanan *CWE* diambil dan dikelola oleh MITRE. Kerentanan diklasifikasikan oleh https://cwe.miter.org/ menggunakan pencocokan kata kunci dan nomor cwe jika memungkinkan, tapi kebanyakan berdasarkan kata kunci.

Di dalam penelitian ini *CWE* digunakan sebagai panduan untuk mengenali kerentanan yang terdapat pada *website* yang diuji.

2.2.9 Eksploitasi terhadap Website

2.2.9.1 Deface

Deface merupakan sebuah eksploitasi terhadap sebuah *website* di mana penyerang mengirimkan *scipt shell* yang digunakan untuk memodifikasi dan mengubah tampilan *website*. Eksploitasi ini dilakukan dengan tujuan untuk memperburuk citra dari pemilik *website*. dengan demikian perusahaan atau pemilik dari *website* tersebut akan mengalami kerugian baik dari bidang sosial maupun ekonomi.

Dalam penelitian pengujian terhadap celah yang memungkinkan untuk *deface* akan diuji karena eksploitasi ini pernah terjadi pada salah satu domain yang diuji.

2.2.9.2 SQL Injection

SQL Injection (SQLi) Merupakan eksploitasi berupa injeksi di mana penyerang dapat mengeksekusi pernyataan *SQL* (juga sering disebut sebagai *payload*) yang dapat mempengaruhi server *database website*. Karena kerentanan

SQL Injection dapat memengaruhi situs *website* dan merupakan salah satu kerentanan aplikasi web tertua, paling umum, dan paling berbahaya.

Dengan memanfaatkan kerentanan *SQL Injection*, dan terdapat *website* yang memiliki kerentanan tersebut, penyerang dapat melakukan exploitsi terhadap autentikasi dan otorisasi pada *website* dan mengambil konten dari seluruh basis data. Selain itu *SQLi* juga dapat digunakan untuk menambah, memodifikasi dan menghapus data di dalam *database*, sehingga mempengaruhi integritas data.

SQLi merupakan salah satu kerentanan *website* yang diuji di dalam penelitian ini.

2.2.9.3 XXS(Cross Site Scriting)

Cross-site Scripting (XSS) mengacu pada eksploitasi injeksi kode dari sisi-klien di mana penyerang dapat mengeksekusi skrip jahat (juga sering disebut sebagai *payload*) ke dalam situs *website* yang sah. *XSS* adalah salah satu kerentanan aplikasi web yang paling merajalela dan terjadi ketika aplikasi web memanfaatkan *form input* yang tidak divalidasi atau tidak dienkode dalam *output* yang dihasilkannya.

Dengan memanfaatkan *XSS*, penyerang tidak menargetkan korban secara langsung. Sebaliknya, penyerang akan mengeksploitasi kerentanan dalam situs *website* yang akan dikunjungi korban, di mana *website* yang dikunjungi korban memiliki kerentanan sehingga penyerang dapat mengirimkan skrip jahat ke browser korban.

XXS merupakan salah satu kerentanan *website* yang di uji di dalam penelitian ini.

2.2.9.4 Denial of Service(DoS)

Eksploitasi *Denial of Service (DOS)* adalah jenis aktivitas berbahaya yang bertujuan mengganggu ketersediaan server atau layanan sehingga tidak dapat lagi menyediakan fungsionalitasnya. Eksploitasi semacam itu dimotivasi baik secara politis (misalnya negara pesaing atau pihak lawan), secara finansial (misalnya untuk melumpuhkan pesaing), sebagai protes (misalnya oleh aktivis seperti

Anonim) atau hanya untuk hak-hak yang menyombongkan diri. Ada beberapa variasi eksploitasi *DOS*, tergantung pada bagaimana eksploitasi itu dilakukan, dan apakah itu berasal dari satu sumber, atau beberapa sumber.

Eksploitasi *DOS* dapat dilakukan dengan hanya membanjiri layanan / server dengan permintaan yang sah, sehingga tidak dapat lagi membalas secara tepat waktu dan akhirnya berhenti berfungsi. Sebuah alternatif, adalah untuk mengeksploitasi kerentanan yang ada dalam layanan yang memungkinkan penyebaran *malware* untuk mengonsumsi sumber daya atau menyebabkan layanan *crash* atau menjadi tidak responsif.

2.2.10 Unified Modeling Language (UML)

Unified Modeling Language (UML) adalah Bahasa Pemodelan Standar yang digunakan untuk pembangunan sistem. Bahasa pemodelan ini dibuat menggunakan *pseudocode*, gambar, diagram dan deskripsi yang dapat membantu untuk menggambarkan sistem yang dibangun. [12]

Berikut merupakan komponen-komponen bagian dari *UML* yang digunakan untuk menggambarkan sistem yang dibangun.

1. *Use Case Diagram*

   Use Case Diagram merupakan abstraksi dari interaksi antara sistem dan actor. *Use Case* bekerja dengan cara mendeskripsikan tipe interaksi antara pengguna sebuah sistem dengan sistemnya. *Use Case* juga dapat diartikan sebagai konstruksi untuk mendeskripsikan bagai mana sistem akan terlihat dimata pengguna.

2. *Activity Diagram*

   Activity Diagram menggambarkan rangkaian aliran dari aktivitas, digunakan untuk mendeskripsikan aktivitas yang terbentuk di dalam suatu operasi sehingga dapat juga digunakan untuk aktivitas lainya.

3. *Class Diagram*

   Class Diagram adalah deskripsi dari objek-objek, perilaku dan relasi antar objek tersebut. Sehingga dapat memberikan pandangan dari sudut padang sistem

4. *Sequence Diagram*

   Sequence diagram merupakan gambaran perilaku antara pengguna dan ojek. *Sequence* diagram akan menunjukkan rangkaian interaksi antar objek dan pesan yang dikirimkan antar ojek yang berjalan pada sistem.

Di dalam penelitian ini *UML* digunakan untuk mendeskripsikan sistem yang dibangun agar proses-proses yang terjadi di dalam sistem dapat dipahami.

2.2.11 Black Box Testing

Black Box Testing adalah pengujian yang dilakukan dengan mengamati hasil eksekusi melalui data uji dan melakukan pemeriksaan fungsionalitas pada perangkat lunak.

Pada pengujian ini, penguji hanya dapat melihat *interface* dan fungsionalitasnya saja tanpa perlu mengetahui proses yang terjadi di dalamnya. Selain itu, penguji hanya mengetahui alamat dari *website* saja untuk dapat melakukan pengujian terhadap *website* tersebut, sehingga penguji perlu melakukan pengumpulan informasi sebanyak-banyak melalui media lain seperti internet atau dengan *tool-tool* khusus yang digunakan untuk pengumpulan informasi untuk dapat melakukan analisis seta menentukan jenis eksploitasi yang dilakukan dalam fase *penetration testing*.

Dalam pengujian ini *Black Box Testing* merupakan pondasi yang digunakan dalam melakukan *penetration testing*. Di mana data yang digunakan merupakan domain yang disediakan oleh pihak Diskominfo Kabupaten Bandung tanpa mengetahui detail proses yang terjadi di dalam *website* tersebut

2.2.12 Whois

Setiap tahun, jutaan individu, bisnis, organisasi dan pemerintah yang membuat sistem dengan platform *website* akan mendaftarkan nama domain. Identitas dan informasi kontak mencakup: nama, alamat, email, nomor telepon, kontak administratif dan teknis harus tersedia dalam proses pendaftaran domain tersebut dan salah satu situs penyedia informasi mengenai domain tersebut disebut adalah WHOIS.

Siapa pun dapat menggunakan protokol *WHOIS* untuk mencari *database* mereka dan mengidentifikasi pemegang nama atau "*registrant*" dari nama domain terdaftar.

Di dalam penelitian ini *Whois* Digunakan dalam tahapan *Information Gathering*, sehingga Informasi mengenai *website* yang dituju dapat diketahui

2.2.13 Nmap

Nmap (*Network Mapper*) merupakan aplikasi gratis dan *open source* yang digunakan menemukan, memetakan jaringan dan audit keamanan, selain itu banyak sistem dan administrasi jaringan yang menggunakan aplikasi ini sebagai tempa penyimpanan jaringan, manajemen jadwal perawatan jaringan dan memonitoring host. [13]

Nmap menggunakan IP (*Internet Protocol*) mentah untuk menentukan apakah host tesedia atau tidak di dalam jaringan, *service* apa yang di gunakan,OS (*Operating System*) apa yang berjalan, tipe dari *firewall* yang digunakan dan masih banyak fungsi lainya yang dapat digunakan.

Nmap sangat dibutuhkan untuk *penetration testing* dalam penelitian ini, Aplikasi ini digunakan dalam tahapan *information gathering* untuk memetakan jaringan yang berada dalam ruang lingkup *website* yang diteliti.

2.2.14 Acunetix Vulnerabilities Scanner

Pada bulan Juli 2005, *Acunetix Web Vulnerability Scanner* dirilis: alat *heuristik* yang dirancang untuk meniru metodologi hacker untuk menemukan kerentanan berbahaya seperti *SQL injection* dan *cross site scripting*. Satu dekade *kemudian Acunetix Vulnerability Scanner* telah menjadi alat pilihan bagi banyak pelanggan di Pemerintah, Militer, Pendidikan, Telekomunikasi, Perbankan, Keuangan, dan *E-Commerce* sektor, termasuk banyak perusahaan Fortune 500.

Acunetix Vulnerability Scanner tersedia baik sebagai *online* dan di solusi premis. *Acunetix Vulnerability Scanner* mendeteksi dan melaporkan berbagai macam kerentanan dalam aplikasi yang dibangun pada arsitektur seperti *WordPress, PHP, ASP.NET, Java Frameworks, Ruby on Rails* dan banyak

lainnya. *Acunetix Vulnerability Scanner* membawa fitur-set yang luas dari kedua alat pengujian penetrasi otomatis dan manual, memungkinkan analis keamanan untuk melakukan penilaian kerentanan yang lengkap, dan perbaikan terdeteksi ancaman, dengan hanya satu produk. Hasil dapat digunakan untuk menghasilkan laporan yang ditujukan terhadap pengembang dan manajemen sama [14].

Di dalam penelitian ini *Acunetix* merupakan *tools* yang digunakan untuk melakukan pemindaian kerentanan pada *website* yang diuji.

2.2.15 Vega

Vega merupakan aplikasi open *source* dan gratis yang digunakan untuk memindai keamanan dari *websites*. Vega dapat membantu dalam pencarian kerentanan seperti *SQL Injection, Cross-Site scripting, Inadvertently disclosed sensitive information*, dan lain lain [15].

Vega memiliki dua jenis fungsi utama yang dapat digunakan yang pertama merupakan *Automated scanner* untuk *scan* cepat dan yang kedua adalah *Interceting Proxy* yang digunakan untuk *teknikal* inspeksi. Aplikasi ini tersedia untuk platform Windows, Linux dan *Mac*.

Di dalam penelitian ini Vega di gunakan sebagai *tools* pendukung untuk memindai dan menemukan kerentanan pada *website* yang diuji.

2.2.16 C#

C# merupakan bahasa pemogramman berorientasi *object* yang dikembangkan oleh *Microsoft* guna mengekspolitasi Net Framework sebagai platform modern yang digunakan dalam membangun aplikasi-aplikasi komputer. C# pertama kali dirilis pada tahun 2000 yang secara umum didesain oleh Anders Hejlsberg. Bahasa ini memiliki kesamaan sintak dengan C dan C++ namun menawarkan fiut-fitur yang lebih banyak serta banyak digunakan untuk membangun program dengan berbagai jenis *flatform* seperti Aplikasi Dekstop, Web dan juga Android [16].

Salah satu aplikasi kompiler yang digunakan untuk menerjemahkan bahasa pemograman C# adalah *Microsoft Visual Studi*o. Aplikasi ini juga di kembangkan oleh Microsoft diluncurkan pada tanggal 19 November 2007. Saat ini versi terbaru dari aplikasi ini adalah visual studio 2017.

Di dalam penelitian ini bahasa pemogramman C# akan digunakan di dalam pembangunan sistem laporan kerentanan dengan bantuan aplikasi kompiler *Microsoft Studio* 2015.

2.2.17 *Object Oriented Programming* (OOP)

Object Oriented Programming (OOP) merupakan teknik pemoramman yang digunakan dalam membangun suatu aplikasi yang berbasis pada Obyek, di mana pembangunan aplikasi tidaklah menggunakan orientasi linear melainkan berorientasikan pada obyek yang terpisah pisah. Suatu perintah yang dibuat menggunakan bahasa program akan diwakili oleh obyek, lalu dikumpulkan dalam *form* yang membentuk sebuah proyek. Berikut merupakan dasar-dasar OOP yang harus dipahami [17].

1. Kelas

   Kelas merupakan kumpulan atas definisi data dan fungsi-fungsi dalam suatu uni tertentu.
2. Obyek

   Obyek merupakan bungkusan dari kelas yang menjadi sebuah unit di dalam sebuah program yang dibangun.
3. Abstraksi

   Abstraki merupakan kemampuan untuk melewati aspek informasi yang diproses.
4. Enkapsulasi

   Enkapsulasi merupakan kemampuan untuk membatasi hak akses atas kelas dalam suatu objek, agar tidak dapat diakses secara sembarangan.
5. *Polimorfisme*

Polimorfisme merupakan kemampuan mengizinkan kelas induk untuk mendefinisikan sebuah fungsi *general* untuk semua kelas turunanya.

Dengan memahami teknik *OOP* ini, maka sistem yang akan dibangun dapat lebih teratur dan mudah untuk dibangun. Sehingga di dalam penelitian ini *OOP* akan digunakan untuk menjadi dasar dalam membangun sistem *report* kerentanan *website* yang dikelola oleh diskominfo.

2.2.18 Xampp

XAMPP merupakan perangkat lunak yang digunakan dalam pembangunan sistem berbasis *client-server* atau sistem yang menggunakan *database* sebagai tempat penyimpanan data . Aplikasi ini berfungsi sebagai server yang berdiri sendiri yang terdiri dari *Apache Http Server* dan *Mysql database*.

Xampp dapat berjalan di banyak sistem operasi seperti *windows, linux, mac* dan *Solaris* sehingga banyak di gunakan dan mudah dalam penggunaannya. Aplikasi Xampp dapat diunduh pada *website* www.apachefriends.org/index.html secara gratis.

Aplikasi *Xampp* ini digunakan untuk mendukung tempat penyimpanan data dari sistem yang dibangun.

2.2.19 Kali Linux

Kali Linux adalah salah satu distribusi Linux tingkat lanjut untuk *Penetration Testing* dan audit keamanan. Kali juga dikembangkan oleh *Offensive Security* sebagai penerus *BackTrack* Linux. Kali menyediakan pengguna dengan mudah akses terhadap koleksi yang besar dan komprehensif untuk alat yang berhubungan dengan keamanan, termasuk *port scanner* untuk *password cracker* [18].

Berikut merupakan fitur-fitur yang terdapat dalam kali linux :

1. Lebih dari 300 *tools penetration testing*: Setelah melakukan *review* setiap *tools* yang terdapat pada *BackTrack*, kami

menghilangkan *tools* dalam jumlah besar baik yang tidak bekerja atau memiliki *tools* yang tersedia yang menyediakan fungsi serupa.

2. Gratis dan akan selalu gratis: Kali Linux, seperti pendahulunya , benar – benar gratis dan akan selalu gratis. Anda tidak pernah akan diminta membayar untuk Kali Linux.
3. *Open source Git tree*: Kami sangat mendukung perangkat lunak *open source* dan *development tree* Tersedia untuk semua orang yang ingin melihatnya, dan semua *source* tersedia bagi mereka yang ingin mengubah dan membangun ulang seluruh paket.
4. Mengikuti *FHS compliant*: Kali telah dikembangkan untuk mematuhi *FHS (Filesystem Hierarchy Standard),* yang memungkinkan semua pengguna Linux dengan mudah mencari *file binary, support file, library,* dan lain-lain.
5. Dukungan perangkat *wireless* yang luas: Kami telah membangun Kali Linux untuk mendukung perangkat Wireless sebanyak mungkin yang kami bisa, yang memungkinkan berjalan dengan baik pada berbagai perangkat keras dan kompatibel dengan berbagai USB dan perangkat *wireless* lainnya.
6. Modifikasi *kernel* yang sudah di *patch* untuk *injection*
7. Lingkungan pengembangan yang aman : Kali Linux team terdiri dari sekelompok orang terpercaya yang hanya dapat *commit* paket dan berinteraksi dengan repositori saat menggunakan beberapa protokol yang aman.
8. GPG menandai beberapa paket dan repo: Semua paket Kali ditandai oleh masing-masing individu pengembang ketika paket-paket tersebut dibuat dan di *commit*, kemudian repositori menandai paket.
9. Banyak bahasa : Meskipun *tools penetration* testing cenderung ditulis dalam bahasa Inggris, kami telah memastikan bahwa Kali Linux memiliki dukungan beberapa bahasa, memungkinkan lebih banyak pengguna untuk mengoperasikannya dalam bahasa mereka

dan menemukan *tools* yang mereka *butuhkan* untuk pekerjaan tersebut.

10. Dapat di ubah sepenuhnya : Kami benar-benar memahami bahwa tidak semua orang akan setuju dengan keputusan desain kami sehingga kami telah membuatnya semudah mungkin bagi pengguna berpengalaman untuk mengubah Kali Linux sesuai keinginan mereka.
11. Mendukung ARMEL dan ARMHF : Sejak sistem berbasis ARM menjadi lebih umum dan murah, kami mengetahui bahwa dukungan ARM Kali Linux akan sekuat seperti yang dapat kami kelola, sehingga installasi dapat bekerja untuk kedua sistem ARMEL & ARMHF. Kali Linux mempunyai repositori ARM terintegrasi dengan jalur distribusi utama sehingga tools untuk ARM akan diupdate dalam hubungannya dengan sisa dari distribusi

Didalam penelitian ini sistem operasi Kali linux dibutuhkan untuk melakukan *penetration testing*.