BAB II
LANDASAN TEORI

2.1 Jaringan Komputer

Jaringan komputer yaitu dua atau lebih komputer yang saling berhubungan melalui media perantara sehingga dapat berbagi sumber daya atau resource. Media perantara ini dapat berupa media kabel atau wired dan media tanpa kabel atau nirkabel. Berdasarkan fungsinya jaringan komputer dapat dibagai menjadi dua jenis antara lain :

1. Client Server

Client server adalah jaringan komputer yang salah satu atau boleh lebih komputer difungsikan sebagai server komputer lain. Server melayani komputer lain yang disebut klien. Client server banyak dipakai pada internet, namun jaringan lokal juga dapat diimplementasikan client server. Hal ini sangat bergantung pada kebutuhan masing-masing (Sofana,2008:6).

2. Peer to Peer

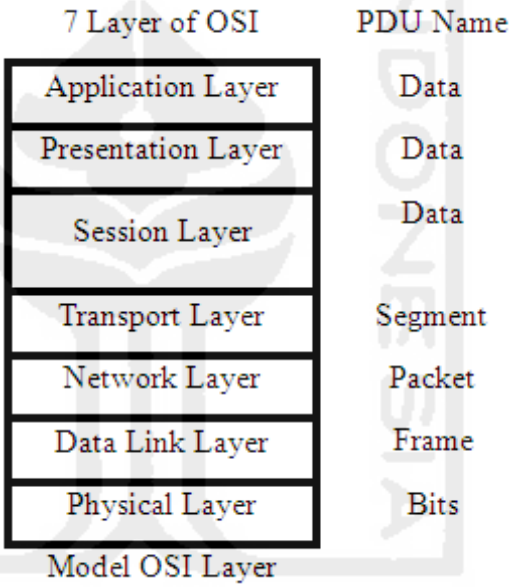
Jaringan peer to peer atau juga disebut P2P yaitu satu atau lebih komputer yang saling terhubung baik media atau nirkabel dan tiap komputer dapat berkomunikasi secara langsung. Pada jaringan P2P, sebuah komputer dapat menjadi client sekaligus server pada saat yang bersamaan dan tidak ada autentikasi secara terpusat. Autentikasi dapat diatur disetiap node yang memberikan layanan (sisjarkom, 2011:4).

2.1.2 Model OSI

Model OSI dibuat untuk mengatasi kendala internetworking akibat perbedaan arsitektur dan protokol jaringan. Dahulu, komunikasi antar komputer dari vendor yang berbedasangat sulit dilakukan. Masing-masing vendor menggunakan protokol dan format data yang berbeda sehingga International for Standardization (ISO) membuat sebuah arsitektur komunikasi yang dikenal

sebagai Open System Interconnection (OSI) model yang mendefinisikan standar untuk menghubungkan komputer-komputer dari vendor yang berbeda.

OSI model terdiri dari tujuh layer dan secara umum dibagi menjadi dua kelompok yaitu upper layer (application layer) dan lower layer (data transport layer). Layer yang tergolong upper layer mendefinisikan bagaimana aplikasi sebuah host akan berkomunikasi dengan user dan host lainnya. Sedangkan lower layer mendefinisikan bagaimana data terkirim dari host satu ke host lainnya. Proses komunikasi dan pertukaran informasi dari tiap-tiap layer menggunakan sebuah protokol yang disebut Protocol Data Unit (PDU).



Gambar 2.1 Layer OSI

Secara umum, fungsi dari tujuh bagian OSI ini adalah :

1. Layer 7 (Application Layer)

Berfungsi sebagai antar muka (penghubung) aplikasi dengan fungsionalitas jaringan, mengatur bagaimana aplikasi dapat mengakses jaringan dan kemudian membuat pesan kesalahan. Pada layer ini user berinteraksi dengan jaringan. Contoh protokol yang berada pada layer ini dalah FTP, SMTP, HTTP, POP3 (Sofana,2008:81).

2. Layer 6 (Presentation Layer)

Berfungsi untuk mentranslasikan data yang hendak ditransmisikan oleh aplikasi dalam format yang dapat ditransmisikan melalui jaringan.

3. Layer 5 (Session Layer)

Berfungsi untuk mendefinisikan bagaimana koneksi dimulai, dipelihara dan diakhiri.

4. Layer 4 (Transport Layer)

Berfungsi untuk memecah data menjadi paket-paket data serta memberikan nomor urut setiap paket sehingga dapat disusun kembali setelah diterima paket. paket yang diterima dengan sukses akan diberi tanda (acknowledgeent). Sedangkan paket yang rusak atau hilang ditengah jalan akan dikirim ulang. Contoh protokol yang digunakan TCP dan UDP (Sofana,2008:82).

5. Layer 3 (Network)

Berfungsi mendefinisikan alamat-alamat IP, membuat header untuk paket-paket dan melakukan routing melalui internetworking dengan menggunakan router dan switch layer 3.

6. Layer 2 (Data Link)

Berfungsi untuk menentukan bagaimana bit-bit data dikelompokkan menjadi frame. Pada level ini terjadi error correction, flow control, pengalamatan perangkat keras (MAC Address) dan menentukan bagaimana perangkat-perangkat jaringan seperti bridge dan switch layer 2 beroperasi (Sofana,2008:82).

7. Layer 1 (Physical)

Berfungsi mendefinisikan media transmisi jaringan, metode persinyalan, sinkronisasi bit, arsitektur jaringan, topologi jaringan dan pengkabelan. Selain itu level ini juga mendefinisikan bagaimana network interface card (NIC) berinteraksi dengan media wire atau wireless (Sofana,2008:83).

2.2 Keamanan Sistem Informasi

Keamanan informasi adalah perlindungan informasi dan sistem informasi dari akses pihak yang tidak berwenang, penggunaan, gangguan, modifikasi atau bahkan perusakan. Keamanan informasi mengacu pada setiap kegiatan yang dirancang untuk melindungi sistem informasi. Kegiatan ini terdiri dari teknologi dan proses yang dilakukan untuk melindungi sistem komputer dari ancaman internal atau ancaman eksternal. Sistem keamanan informasi melibatkan semua organisasi, perusahaan dan lembaga untuk melindungi aset demi kelangsungan perusahaan.

Menurut John D. Howard dalam bukunya "An Analysis of Security Incidents On The Internet" menyatakan bahwa keamanan komputer adalah tindakan pencegahan dari serangan pengguna komputer atau pengakses jaringan yang tidak bertanggung jawab. Sedangkan menurut Gollman pada tahun 1999 dalam bukunya "Computer Security" menyatakan bahwa keamanan komputer adalah berhubungan dengan pencegahan diri dan deteksi terhadap tindakan penganggu yang tidak dikenali dalam sistem komputer. Sedangkan menurut Garfinkel dan Spafford sebagai ahli keamanan komputer menyatakan bahwa komputer dikatakan aman jika bisa diandalkan dan perangkat lunaknya bekerja sesuai dengan yang diharapkan.

2.3 Vulnerability Assessment

Menurut GOV-CSIRT (Goverment Computer Security Incident Response Team), vulnerability assessment adalah melakukan identifikasi vulnerability dari suatu aplikasi, sistem operasi dan infrastruktur jaringan. Vulnerability assessment tidak melakukan eksploitasi celah atau kelemahan dari suatu sistem. Sedangkan vulnerability adalah suatu kelemahan dalam desain sistem, implementasi sistem atau operasi dan manajemen yang dapat dimanfaatkan untuk melanggar kebijakan kemanan sistem. Vulnerability assessment lebih fokus untuk menemukan beragam public vulnerability pada seluruh sistem komputer dalam jaringan target. Dalam vulnerability assessment tidak menuju ke proses eksploitasi namun memiliki

potensi untuk di eksploitasi sehingga harus ditutup kerentanan yang ditemukan tersebut.

Tahapan yang dilakukan dalam kegiatan vulnerability assessment antara lain :

1. Adjusting Scope

Adjusting scope adalah proses untuk menentukan batas apa saja yang termasuk dalam proses uji penetrasi. Seperti contoh batas jaringan, alamat IP, server dan sebagainya.

2. Target Enumeration

Target enumeration merupakan aktifitas selanjutnya untuk mengidentifikasi topologi jaringan yang tepat dan sistem operasi serta versi aplikasi dan juga port yang terbuka pada sistem.

3. Network Server Assessment

Tahap ini untuk menentukan komponen jaringan baik router, firewall, server, IDS/IPS untuk mengenali kerentanan dan menetapkan level resiko untuk setiap kerentanan. Level kerentanan dibagi menjadi tiga bagian yaitu level low, level medium, level high serta melakukan analisa solusi kebijakan mitigasi yang sesuai dan tepat. Hal yang dilakukan antara lain hardening sistem, menerapkan, patch serta membuat kebijakan keamanan.

4. Application Assessment

Tahap ini melakukan analisa aplikasi untuk menentukan kerentanan dan menetapkan nilai resiko untuk setiap kerentanan yang ditemukan yaitu level low, level medium, level high. Menerapkan soluasi kebijajakan mitigasi yang sesuai dan tepat. Hal yang dilakukan antara lain hardening sistem, menerapkan patch serta membuat kebijakan keamanan.

Vulnerability atau kerentanan dibagi menjadi tiga penilaian antara lain :

1. Level High (Tinggi)

Pada level ini terdapat kelemahan yang berpotensi tinggi menjadi ancaman sedangkan fitur ataupun langkah untuk tingkat pencegahan maupun penanganannya tidak memadai.

2. Level Medium (Sedang)

Pada level ini tingkatan kelemahan bersifat lokal dan upaya penanganan dan pencegahan besifat lokal juga.

3. Level Low (Rendah)

Pada level ini kelemahan rendah dan upaya pencegahan dan penanganan yang diharapkan sangat memadai.

Berikut ini adalah daftar dampak kerentanan yang dibagi menjadi 5 bagian yaitu :

Dampak	Deskripsi	Contoh
Tidak Ada Dampak	Kerentanan tidak mempengaruhi	Pencurian kabel usb tidak akan mempengaruhi jalannya perusahaan.
Dampak Kecil	Kerentanan yang berdampak kecil mengakibatkan sedikit ketidaknyamanan dan mengakibatkan perubahan dalam prosedur.	Merk tertentu dan jenis hard disk yang kurang bagus itu mengharuskan adanya drive cadangan serta perangkat tersebut diuji secara periodik.
Dampak Signifikan	Kerentanan ini menghasilkan hilangnya produktifitas karyawan karena downtime dan juga pengeluaran modal untuk meringankan masalah tersebut dapat dianggap signifikan.	Malware yang dimasukkan kedalam jaringan dapat diklasifikasikan sebagai kerentanan yang signifikan. Malware tersebut dapat mempengaruhi kinerja jaringan komputer.
Dampak Utama	Kerentanan utama adalah kerentanan yang memiliki	Pencurian produk, pencurian data dan aset

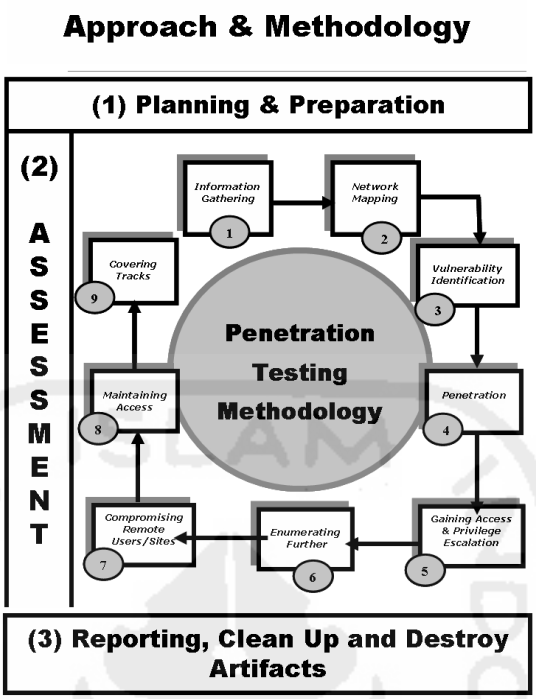
	dampak negatif yang cukup besar pada pendapatan perusahaan	perusahaan melalui backdoor yang ditanam oleh pihak yang tidak sah atau tidak bertanggung jawab atau pihak ilegal dapat dianggap sebagai kerentanan yang besar
Dampak Bencana	Kerentanan yang disebabkan karena peristiwa bencana akan menyebabkan perusahaan berhenti berfungsi atau lumpuh dalam kapasitasnya untuk bekerja.	Bencana kebakaran meghancurkan bangunan kantor dan semua data perusahaan, hal ini bisa menjadi kerentanan dalam kategori bencana.

Tabel 2.1 Tabel Dampak Akibat Kerentanan

Dari tabel diatas dapat diketahui deskripsi dan contoh dari mulai tidak ada dampai sampai kepada terdapat dampak kerentanan yang berbahaya serta akibat yang ditimbulkan.

.2.4 Penetration Testing

Penetration testing adalah subkategori dari *etchical hacking* yaitu sebuah metode dan prosedur yang bertujuan untuk menguji dan melindungi keamanan informasi. *Penetration testing* merupakan aktifitas mengevaluasi sistem keamanan yang sudah dibuat dengan cara melakukan simulasi serangan menggunakan metode yang biasa digunakan oleh peretas. Kegiatan ini perlu mendapat persetujuan legal dari pemilik sistem tersebut.



Gambar 2.2 Metodologi Penetration Testing

Aktifitas penetration testing juga menganalisa vulnerability dari hasil temuan untuk menentukan tingkat resiko yang mungkin dapat terjadi pada sistem. Dalam proses kegiatan penetration testing yang dilakukan, terdapat metode atau jalur yang digunakan yaitu antara lain :

1. Black Box Testing

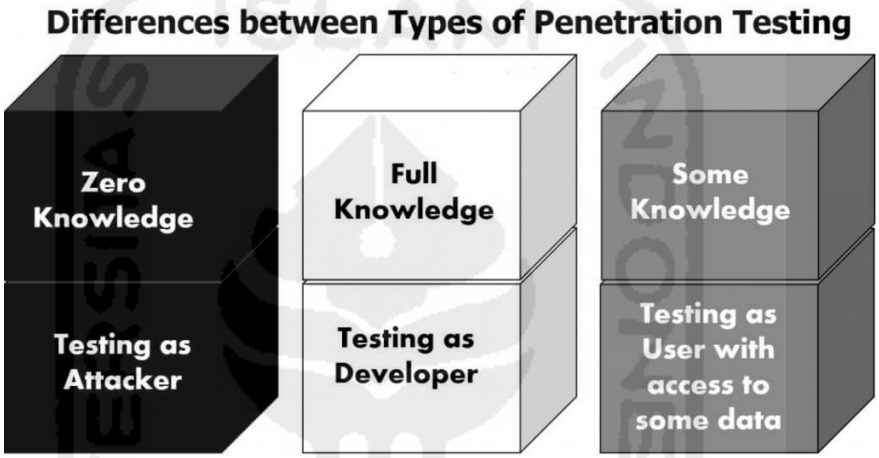
Black box testing adalah penetration testing yang dilakukan tanpa mengetahui informasi sebelumnya dari pihat target yang akan ditest baik dari sistem jaringan, sistem operasi yang digunakan oleh target, topologi jaringan, port yang terbuka atau service apa sajakah yang sedang berjalan pada sistem target.

2. Grey Box Testing

Grey box testing adalah penetration testing yang dilakukan dengan mengetahui sedikit informasi dari target yang akan diuji keamanannya. Hal ini sedikit membantu pentester dalam melakukan kegiatan aktifitas penetration testing.

3. White Box Testing

White box testing adalah penetration testing yang dilakukan dengan informasi-informasi mengenai sistem target sudah diketahui terlebih dahulu. Tetapi hal ini tidak menjamin untuk memberikan kemudahan dalam melakukan pentest, hal tersebut bergantung kepada tester yang melakukan pengujian dan menilai sejauh mana kelemahan-kelemahan yang terdapat pada target atau didalam sistem maupun jaringan.



Gambar 2.3 Perbedaan Tipe Mekanisme Penetration Testing

Selain pengujian terhadap sistem atau jaringan, juga terdapat pengujian pada web aplikasi dengan metode yang digunakan antara lain :

1. Passive Penetration Testing

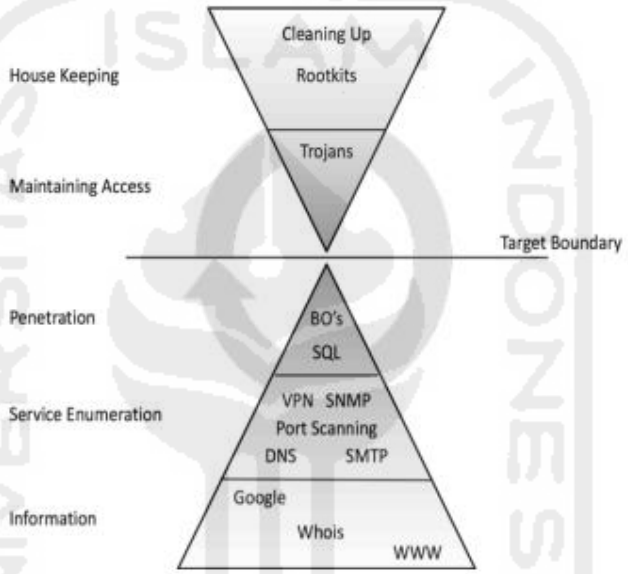
Passive penetration test dilakukan dengan pemetaan dan pengujian terhadap kontrol yang ada didalam web aplikasi, login dan konfigurasinya sehingga dapat memetakan target sistem.

2. Active Penetration Testing

Active penetration testing dilakukan dengan kegiatan yang aktif dalam pengujian terhadap target yaitu dengan melakukan manipulasi input, pengambilan akses serta melakukan pengujian terhadap kerentanan yang sudah ada.

3. Aggressive Penetration Testing

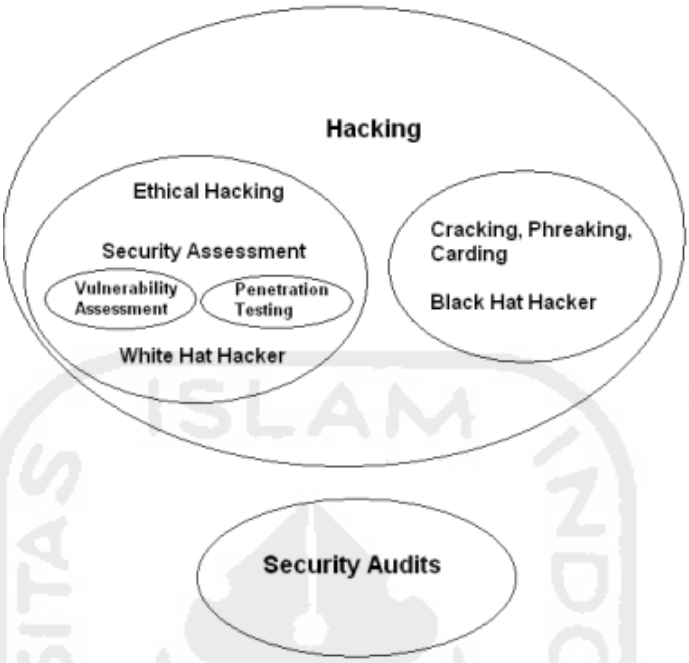
Aggressive penetration testing dilakukan dengan mengeksploitasi kerentanan dan melakukan reverse engineering terhadap software, menanam backdoor, mengunduh kode serta mengambil alih finansial dan informasi yang ada pada target.



Gambar 2.4 Fase Penetration Testing

2.5 Perbedaan Vulnerability Assessment dan Penetration Testing

Vulnerability assessment dan *penetration testing* memiliki definisi dan tujuan yang berbeda. *Vulnerability assessment* lebih difokuskan dalam mencari tahu seluruh kerentanan dalam aset jaringan. melakukan identifikasi *vulnerability* dari suatu aplikasi, sistem operasi dan infrastruktur jaringan. Melakukan evaluasi dan analisa terhadap vulnerability dari hasil temuan untuk menentukan tingkat resiko yang mungkin dapat terjadi. Selain itu memberikan sebuah laporan dan rekomendasi atas temuan yang didapat dari kegiatan *vulnerability assessment*.

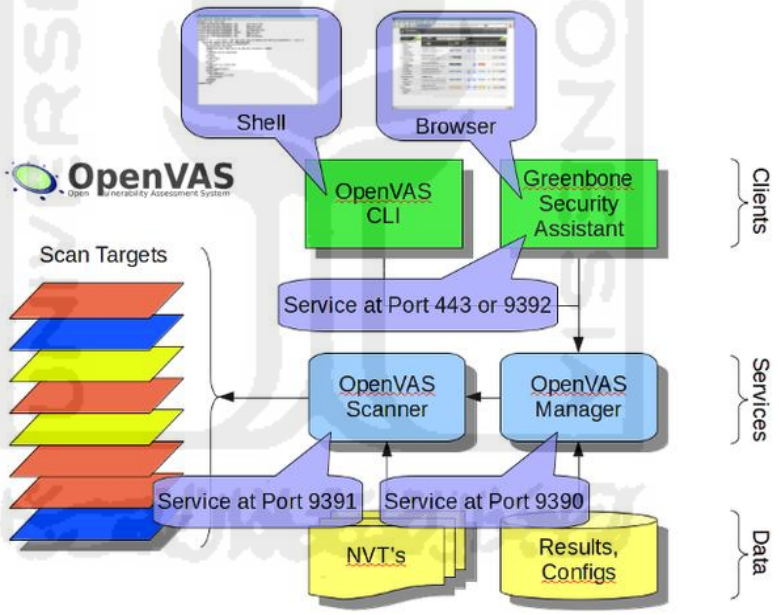


Gambar 2.5 Perbedaan Kegiatan Evaluasi Keamanan Informasi

Sedangkan uji penetrasi adalah melakukan langkah tambahan evaluasi terhadap sistem dengan mensimulasikan sebagai penyerang agar dapat dilihat apakah benar-benar dapat mengeksploitasi kerentanan dan mendokumentasikan kerentanan tersebut atau tidak. Tujuannya adalah untuk memberikan bukti dan menunjukkan pola serangan yang dapat dilakukan apabila terdapat kerentanan atau celah yang ditemukan. Selain itu aktifitas evaluasi keamanan juga dilakukan berdasarkan acuan pada sebuah standar yang dinamakan security audit. Pengujian ini dilakukan dengan menggunakan checklist yang sudah dituangkan kedalam sebuah dokumen.

2.6 OpenVAS (Open Network Vulnerability Assessment)

Openvas adalah framework dari beberapa layanan dan aplikasi yang menyediakan fitur vulnerability scanning. Openvas merupakan sistem yang mempunyai kemampuan untuk melakukan scanning dalam menangani vulnerability dalam jaringan terhadap gangguan berdasarkan statistik serangan yang terjadi. Openvas difungsikan untuk melakukan deteksi terhadap celah keamanan dan dapat menyajikan laporan tingkat resiko sesuai dari celah keamanan yang ditemukan lalu kemudian disimpan dalam sebuah log. Openvas merupakan pengembangan dari Nessus 2.2 setelah pada tahun 2005 Nessus menjadi alat scanner yang berbayar atau komersil. Openvas juga kerangka dari beberapa penyedia atau alat-alat kerentanan sistem.



Gambar 2.6 Openvas

Openvas memiliki komponen yang saling terkait satu dengan yang lain. Komponen tersebut antara lain :

1. Openvas Scanner

Openvas scanner adalah komponen inti dari openvas. Openvas scanner adalah sebagai penyedia layanan scan dengan memanfaatkan plugin NVT. NVT

feed tersebut dapat diakses melalui openvas NVT feed yang bebas atau menggunakan NVT feed yang komersial.

2. Openvas Manager

Openvas Manager adalah komponen sentral karena letaknya di tengah-tengah dan berfungsi sebagai pusat layanan yang memproses dan melakukan pekerjaan intelegensi dengan mengolah hasil mentah vulnerability scanning menjadi solusi bagaimana menangani vulnerability. Openvas Manager juga menggunakan basis dara SQL(sqlite) untuk menyimpan konfigurasi dan data hasil scan.

Hasil pemrosesan openvas manager dapat diakses oleh beragam klien OMP (Openvas Management Protocol). OMP ini merupakan protokol yang digunakan untuk mengakses hasil pemrosesan oleh openvas manager. OMP mempunyai tiga pilihan klien yaitu antara lain :

a. Openvas CLI
   Openvas CLI menyediakan akses terminal.
b. Greenbone Security Assistant (GSA)
   GSA menyediakan akses berbasis web.
c. Greenbone Security Desktop (GSD)
   GSD menyediakan akses berbasiskan klien GUI.

2.7 CVE (Common Vulnerability and Exposure)

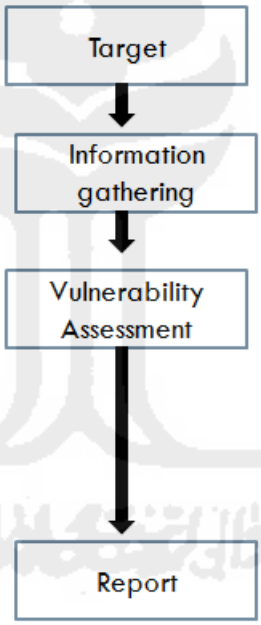
CVE adalah sebuah database mengenai setiap kerentanan atau vulnerability yang dipublikasikan. CVE menyediakan referensi mengenai kerentanan atau vulnerability yang ada pada suatu produk. Cara kerja CVE checker yaitu dengan melakukan scanning terhadap sistem operasi. Kemudian aplikasi tersebut akan dicocokan dengan database dari CVE yang ada dengan menggunakan CVE checker dan akan diberitahu hasilnya.

2.8 NVT (Network Vulnerability Tests)

NVT adalah sebuah layanan scanning yang digunakan openvas untuk menelusuri kerentanan yang ada dalamsebuah sistem. NVT feed ini dapat diakses melalui Openvas NVT feed yang gratis atau menggunakan NVT yang berbayar.

2.9 Penilaian Kerentanan

Langkah atau proses penilaian ini menggunakan openvas sebagai alat uji kerentan. Openvas dapat berfungsi sebagai network scanner, host scanner, database scanner, web application scanner untuk memulai vulnerability assessment. Dalam penelitian ini menekankan pada kerentanan dalam level resiko tinggi (high). Pada level ini kerentanan harus dimanajemen dengan baik.



Gambar 2.7 Alur Mekanisme Vulnerability Assessment

Mekanisme assessment dimulai dari menentukan target yang akan ditelusuri kerentanannya, kemudian mengumpulkan informasi mengenai target, lalu melakukan assessment dari hasil penelusuran celah keamanan yang ditemukan untuk kemudian dianalisa dan dibuat laporan rekomendasi perbaikan.