TUGAS

KEAMANAN JARINNGAN KOMPUTER

“Penetration Testing: Actual Exploit”

DISUSUN OLEH :

MEILINDA EKA SURYANI (09011181320033)

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2017

Penetration Testing: Actual Exploit

Penetration Testing adalah jenis pengujian keamanan yang digunakan untuk menguji ketidak-amanan aplikasi. Hal ini dilakukan untuk menemukan resiko keamanan yang mungkin hadir dalam sistem. Jika sistem tidak dijamin, maka setiap penyerang dapat mengganggu atau mengambil hak akses ke sistem itu. resiko keamanan biasanya adalah kesalahan disengaja yang terjadi ketika mengembangkan dan menerapkan perangkat lunak. Misalnya, kesalahan konfigurasi, kesalahan desain, dan bug software, dan sebagainya.

Penetration Testing biasanya mengevaluasi kemampuan sistem untuk melindungi jaringannya, aplikasi, end point dan pengguna dari ancaman eksternal atau internal. Ini juga merupakan upaya untuk melindungi kontrol keamanan dan memastikan hanya akses yang berwenang.

Penetration Testing penting karena:

- mengidentifikasi lingkungan simulasi, bagaimana penyusup dapat menyerang sistem melalui white hat attack.
- membantu untuk menemukan daerah lemah di mana penyusup dapat menyerang untuk mendapatkan akses ke fitur komputer dan data.
- mendukung untuk menghindari black hat attack dan melindungi data asli.
- memperkirakan besarnya serangan terhadap potensi bisnis.
- memberikan bukti yang menunjukkan pentingnya meningkatkan investasi dalam aspek keamanan teknologi.

Penetration Testing dilakukan saat:

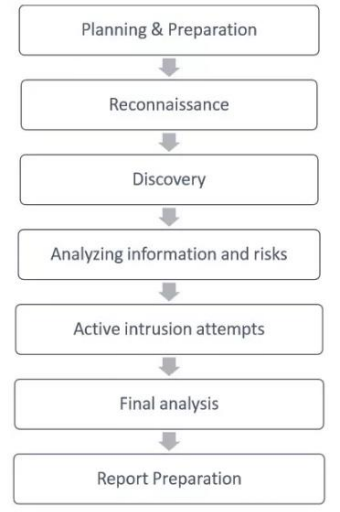
- Sistem keamanan menemukan ancaman baru oleh penyerang.
- Menambahkan infrastruktur jaringan baru.
- Memperbarui sistem anda atau menginstal perangkat lunak baru.
- Pengguna pindah kantor.
- Menyiapkan end-user / program kebijakan baru.

Penetration Testing menawarkan keuntungan sebagai berikut:

- Peningkatan Sistem Manajemen - memberikan informasi rinci tentang ancaman keamanan. Selain itu, juga mengkategorikan tingkat kerentanan dan menyarankan Anda, mana yang lebih rentan dan mana yang kurang. Jadi, Anda dapat dengan mudah dan akurat mengelola sistem keamanan Anda dengan mengalokasikan sumber daya keamanan yang sesuai.
- Menghindari Denda - Penetration Testing terus diperbarui dan sesuai dengan sistem audit. Jadi, Penetration Testing melindungi Anda dari denda.
- Perlindungan dari Kerusakan Keuangan - Sebuah pelanggaran sederhana dari sistem keamanan dapat menyebabkan kerugian jutaan dolar**.** pengujian penetrasi dapat melindungi organisasi Anda dari kerusakan tersebut.
- Perlindungan konsumen - Pelanggaran data pelanggan tunggal dapat menyebabkan kerugian keuangan yang besar serta kerusakan reputasi. Melindungi organisasi yang berurusan dengan pelanggan dan menyimpan data mereka utuh.

Penetration Testing adalah kombinasi dari teknik yang menganggap berbagai masalah sistem dan tes, analisis, dan memberikan solusi. Hal ini didasarkan pada prosedur terstruktur yang melakukan Penetration Testing langkah-demi-langkah.

Berikut ini adalah tujuh langkah Penetration Testing:



Gambar 1. Langkah-langkah Pentest

Perencanaan dan persiapan dimulai dengan mendefinisikan tujuan dan sasaran dari Penetration Testing. Klien dan tester bersama-sama menentukan tujuan sehingga kedua pihak memiliki tujuan dan pemahaman yang sama. Tujuan umum dari Penetration Testing adalah:

- Untuk mengidentifikasi kerentanan dan meningkatkan keamanan sistem teknis.
- Memiliki keamanan IT terkonfirmasi oleh pihak ketiga eksternal.
- Meningkatkan keamanan infrastruktur organisasi / personil.

Tester dimulai dengan menganalisis informasi yang tersedia dan jika diperlukan, meminta untuk informasi lebih lanjut seperti deskripsi sistem, rencana jaringan, dan lain-lain dari klien. Langkah ini adalah Penetration Testing pasif. Tujuannya adalah untuk mendapatkan informasi yang lengkap dan rinci dari sistem.

Pada langkah penemuan, tester penetrasi kemungkinan besar akan menggunakan alat otomatis untuk memindai aset target untuk menemukan kerentanan. Alat-alat ini biasanya memiliki database mereka sendiri memberikan rincian kerentanan terbaru. Namun, tester menemukan:

- Network Discovery - Seperti penemuan sistem tambahan, server, dan perangkat lainnya.
- Penemuan tuan rumah - Menentukan port yang terbuka pada perangkat ini.
- Layanan Interogasi - Ini menginterogasi port untuk menemukan layanan yang sebenarnya yang berjalan pada mereka.

Pada menganalisis informasi dan resiko, tester menganalisa dan menilai informasi yang dikumpulkan sebelum langkah-langkah tes secara dinamis menembus sistem. Karena jumlah yang lebih besar dari sistem dan ukuran infrastruktur, hal ini sangat memakan waktu. Sementara pada tahap analisis, tester menganggap unsur-unsur berikut:

- Tujuan yang ditetapkan dari uji penetrasi.
- Potensi resiko terhadap sistem.
- Perkiraan waktu yang dibutuhkan untuk mengevaluasi kelemahan keamanan potensial untuk pengujian penetrasi aktif berikutnya.

Namun, dari daftar sistem diidentifikasi, tester dapat memilih untuk menguji hanya mereka yang mengandung potensi kerentanan. Analisis akhir adalah langkah yang paling penting yang harus dilakukan dengan hati-hati. Langkah ini memerlukan sejauh mana kerentanan potensial yang diidentifikasi dalam langkah penemuan yang memiliki resiko yang sebenarnya. Langkah ini harus dilakukan ketika verifikasi kerentanan potensial yang dibutuhkan. Untuk sistem-sistem yang memiliki persyaratan integritas yang sangat tinggi, potensi kerentanan dan risiko perlu dipertimbangkan dengan cermat sebelum melakukan prosedur pembersihan secara kritis.

Laporan persiapan harus dimulai dengan prosedur pengujian secara keseluruhan, diikuti dengan analisis kerentanan dan resiko. Resiko tinggi dan kerentanan kritis harus memiliki prioritas dan kemudian diikuti dengan urutan yang lebih rendah.

Namun, selama mendokumentasikan laporan akhir, poin-poin berikut perlu dipertimbangkan:

- Keseluruhan ringkasan Penetration Test.
- Rincian dari setiap langkah dan informasi yang dikumpulkan selama Penetration Test.
- Rincian dari semua kerentanan dan resiko ditemukan.
- Rincian membersihkan dan memperbaiki sistem.
- Saran untuk keamanan masa depan.

Penetration Test Vs Vulnerability

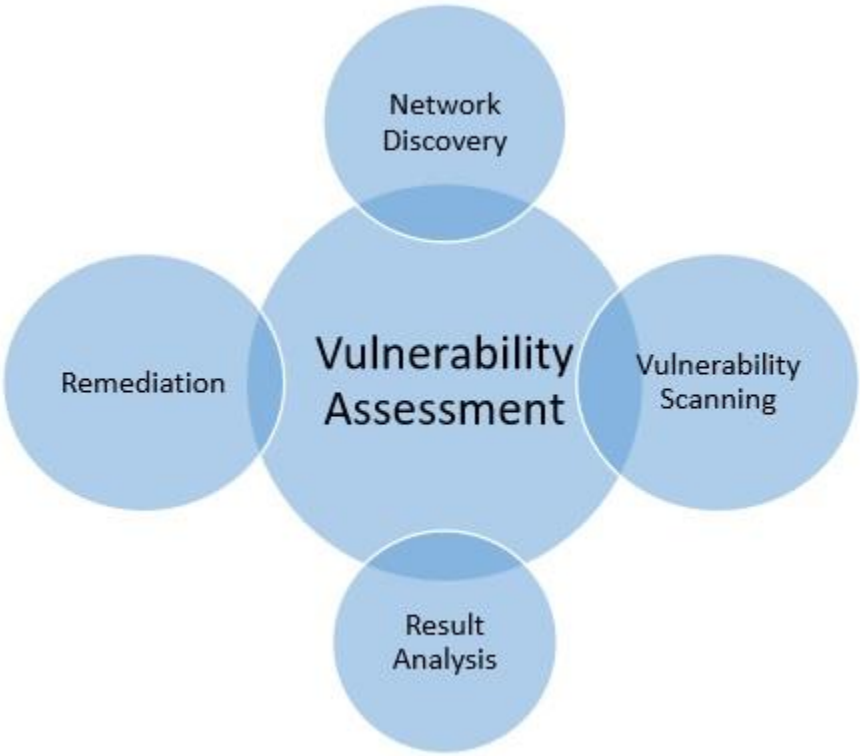
Umumnya, kedua istilah ini, yaitu, Penetration Test dan penilaian Vulnerability digunakan secara bergantian oleh banyak orang. Tapi, kedua istilah yang berbeda satu sama lain dalam hal tujuan mereka dan cara lain. Namun, sebelum menjelaskan perbedaan, mari kita memahami kedua istilah satu-persatu.

Penetration Test meniru tindakan eksternal dan/atau internal yang dimaksudkan untuk memecahkan keamanan informasi dan hack data berharga atau mengganggu fungsi normal dari organisasi. Jadi, dengan bantuan alat canggih dan teknik, Penetration Tester (juga dikenal sebagai etical hacker) membuat upaya untuk mengontrol sistem kritis dan memperoleh akses ke data sensitif.

Di sisi lain, penilaian kerentanan adalah teknik identifikasi (discovery) dan mengukur kerentanan keamanan (scanning) dalam suatu lingkungan tertentu. Ini adalah penilaian yang

komprehensif dari posisi keamanan informasi (analisis hasil). Selanjutnya, mengidentifikasi kelemahan potensial dan memberikan langkah-langkah mitigasi yang tepat (remediasi) baik menghapus kelemahan-kelemahan atau mengurangi tingkat resiko.

Diagram berikut menyajikan penilaian kerentanan:



Gambar 2. Diagram penilaian Vulnerability

Tabel berikut menggambarkan perbedaan mendasar antara penetration test dan penilaian vulnerability:

Tabel perbedaan mendasar antara penetration test dan penilaian vulnerability.

Penetration Test	Penilaian vulnerability
Menentukan ruang lingkup serangan.	Membuat direktori aset dan sumber daya dalam sistem tertentu.
Tes pengumpulan data sensitif.	Menemukan potensi ancaman untuk setiap sumber daya.
Mengumpulkan ditargetkan informasi dan / atau memeriksa sistem.	Mengalokasikan nilai kuantitatif dan signifikansi untuk sumber daya yang tersedia.
Membersihkan sistem dan memberikan laporan akhir.	Upaya untuk mengurangi atau menghilangkan kerentanan potensi sumber daya yang berharga.
Ini adalah non-intrusif, dokumentasi dan tinjauan lingkungan dan analisis.	analisis yang komprehensif dan melalui penelaahan terhadap sistem target dan lingkungannya.
Ini sangat ideal untuk lingkungan fisik dan arsitektur jaringan.	Ini sangat ideal untuk lingkungan laboratorium.
Hal ini dimaksudkan untuk sistem real-time kritis.	Hal ini dimaksudkan untuk sistem non-kritis.

Kedua metode memiliki fungsi dan pendekatan yang berbeda, sehingga tergantung pada posisi keamanan sistem masing-masing. Namun, karena perbedaan mendasar antara pengujian penetrasi dan penilaian kerentanan, teknik kedua lebih menguntungkan daripada yang pertama.

penilaian kerentanan mengidentifikasi kelemahan dan memberikan solusi untuk memperbaikinya. Di sisi lain, pengujian penetrasi hanya menjawab pertanyaan yang "bisa ada break-in keamanan sistem dan jika demikian, maka apa salahnya bisa dia lakukan?"

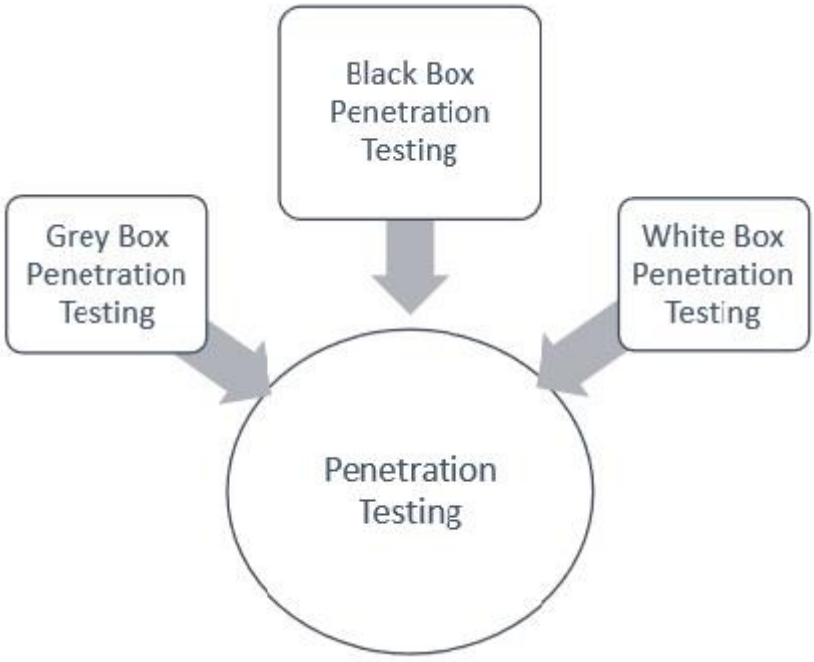
Selanjutnya, penilaian kerentanan mencoba untuk meningkatkan sistem keamanan dan mengembangkan, program keamanan terpadu yang lebih matang. Di sisi lain, pengujian penetrasi hanya memberikan gambaran efektivitas program keamanan Anda.

Sebagaimana telah kita lihat di sini, penilaian kerentanan lebih menguntungkan dan memberikan hasil yang lebih baik dibandingkan dengan pengujian penetrasi. Tapi, para ahli menyarankan bahwa, sebagai bagian dari sistem manajemen keamanan, kedua teknik harus dilakukan secara rutin untuk memastikan lingkungan yang sempurna aman.

Jenis pengujian penetrasi biasanya tergantung pada ruang lingkup dan keinginan organisasi dan persyaratan. Bab ini membahas tentang berbagai jenis Pengujian penetrasi. Hal ini juga dikenal sebagai Penetration Test**.**

Berikut ini adalah jenis penting dari Penetration Test:

- Pengujian Black Box Penetrasi
- Pengujian White Box Penetrasi
- Pengujian Abu-abu Box Penetrasi



Gambar 3. Jenis-jenis Pentest

- Dalam black box, tester tidak tahu tentang sistem bahwa ia akan menguji. Ia tertarik untuk mengumpulkan informasi tentang jaringan target atau sistem. Misalnya, dalam pengujian ini, tester hanya tahu apa yang seharusnya menjadi hasil yang diharapkan dan ia tidak tahu bagaimana hasil tiba. Dia tidak memeriksa kode pemrograman.

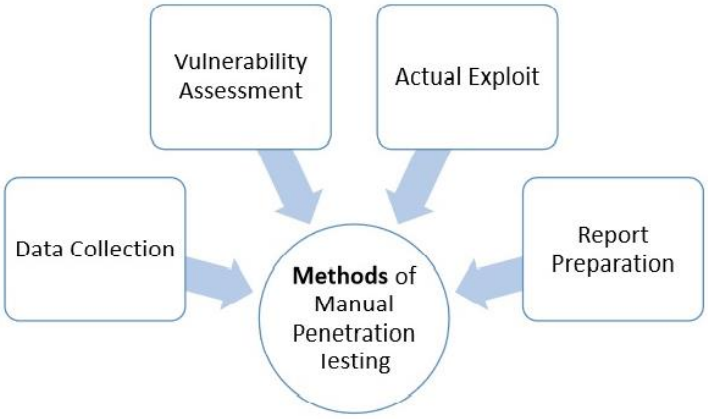
- Penetrasi White box adalah pengujian yang komprehensif, sebagai tester telah disediakan dengan berbagai macam informasi tentang sistem dan / atau jaringan seperti Skema, Source code, rincian OS, alamat IP, dll Hal ini biasanya dianggap sebagai simulasi serangan oleh sumber internal. Hal ini juga dikenal sebagai struktural, kotak kaca, kotak yang jelas, dan pengujian kotak terbuka. Putih pengujian penetrasi kotak meneliti kode cakupan dan melakukan pengujian aliran data, pengujian jalan, pengujian lingkaran, dll.

- Dalam jenis pengujian, tester biasanya memberikan informasi parsial atau terbatas tentang rincian internal program dari suatu sistem. Hal ini dapat dianggap sebagai serangan oleh hacker eksternal yang telah memperoleh akses tidak sah ke dokumen infrastruktur jaringan organisasi.

Penetration Test pengguna adalah pengujian yang dilakukan oleh manusia. Dalam jenis seperti pengujian, kerentanan dan risiko mesin diuji oleh seorang insinyur ahli.

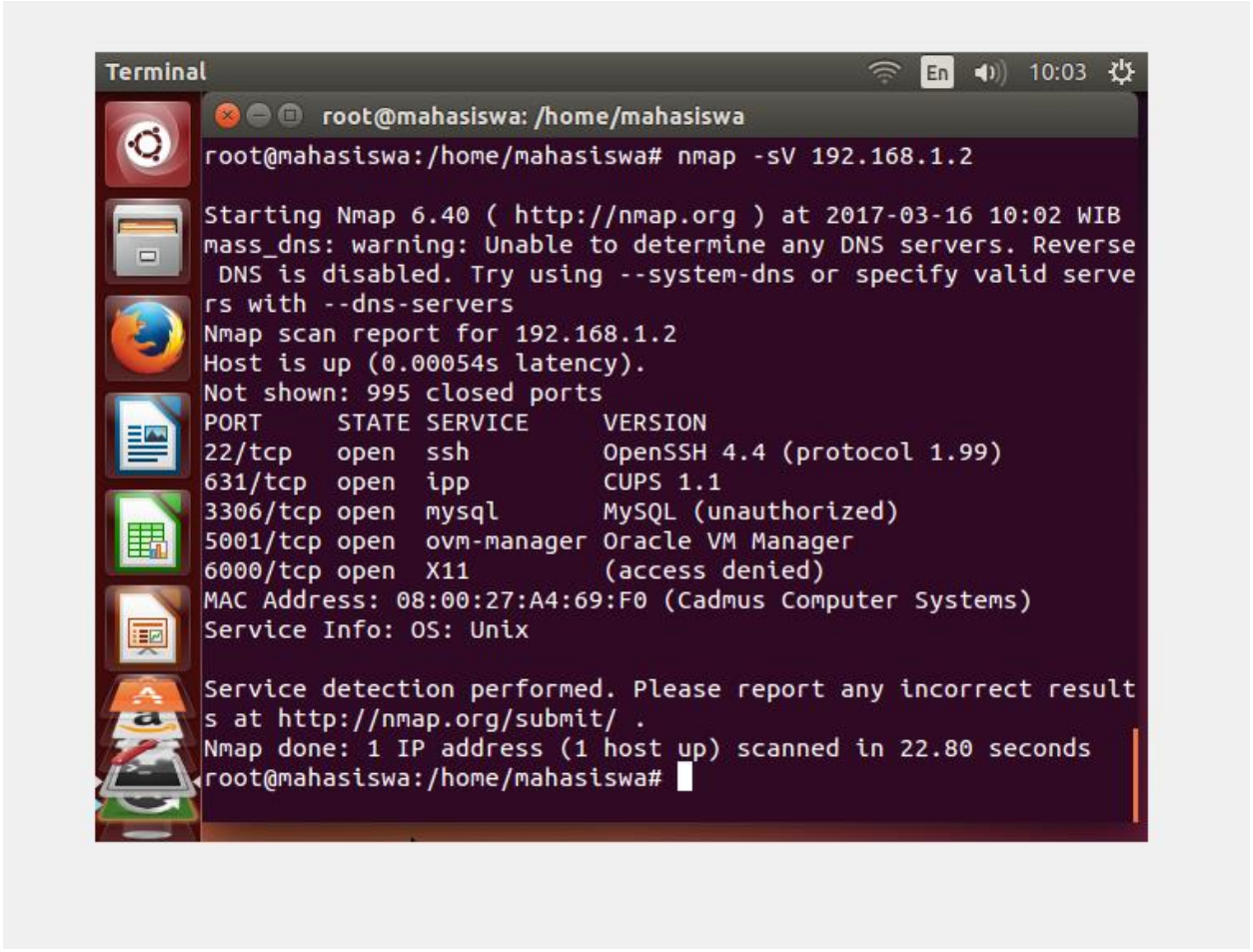
Umumnya, pada pengujian dilakukan metode berikut:

- Pengumpulan Data - Pengumpulan data memainkan peran kunci untuk pengujian. Satu baik dapat mengumpulkan data secara manual atau dapat menggunakan layanan alat (seperti teknik analisis kode sumber halaman web, dll) bebas tersedia secara online. Alat-alat ini membantu untuk mengumpulkan informasi seperti nama tabel, versi DB, database, software, hardware, atau bahkan tentang plugin pihak ketiga yang berbeda, dan lain-lain.
- Penilaian Kerentanan - Setelah data dikumpulkan, hal ini membantu para penguji untuk mengidentifikasi kelemahan keamanan dan mengambil langkah-langkah pencegahan yang sesuai.
- Actual Exploit - Ini adalah metode yang khas yang menggunakan tester ahli untuk melancarkan serangan pada sistem target dan juga, mengurangi risiko serangan.
- Laporan Persiapan - Setelah penetrasi dilakukan, tester menyiapkan laporan akhir yang menjelaskan segala sesuatu tentang sistem. Akhirnya laporan tersebut dianalisis untuk mengambil langkah-langkah korektif untuk melindungi sistem target.



Gambar 4. Metode-metode Pentest

Dalam Hands-on kali ini kami menggunakan metode Actual Exploit dengan satu buah DVL yang digunakan sebagai target, dan satu buah sistem operasi Ubuntu yang berperan sebagai penyerang. Sistem operasi-sistem operasi ini berupa virtual menggunakan Virtualbox. Pada DVL diberi IP address 192.168.1.1 sedangkan sistem operasi Ubuntu diberi IP address 192.168.1.2. setelah IP address selesai diatur, lakukan ping antar mesin, untuk memastikan bahwa kedua mesin dapat saling terhubung. Jika kedua mesin dapat dipastikan bias terhubung, mulai proses penetration testing dari Ubuntu ke DVL menggunakan Nmap dengan memasukkan perintah **nmap –sV 192.168.1.1** dalam root. Maka didapatkan hasil seperti berikut ini.



Gambar 5. Pentest menggunakan Nmap

Selain menggunakan Nmap dapat juga melakukan penetration testing menggunakan tool hydra. Hydra merupakan tool yang dapat dipakai untuk mencari password (menguji apakah password aman).

Secara garis besar, ada dua cara untuk menemukan sebuah password. Cara pertama adalah dengan mencoba seluruh kombinasi password yang ada. Cara ini membutuhkan waktu yang sangat lama dan hampir mustahil bila pengguna memakai password yang panjang. Sebagai contoh, anggap saja pengguna membuat password 6 karakter yang terdiri atas huruf A sampai Z. Kombinasi password yang mungkin dapat dihitung dengan rumus 26^6 (26 x 26 x 26 x 26 x 26 x 26) dimana hasilnya adalah 308.915.776 kombinasi. Bila seandainya dalam 1 menit saya dapat memproses 600 kombinasi, maka waktu yang saya butuhkan untuk menemukan password adalah 514.859 menit atau 8.580 jam atau 358 hari. Butuh waktu hampir setahun. Ini masih belum menyertakan karakter seperti huruf kecil, angka dan simbol.

Untuk melakukan Penetration Test menggunakan tool hydra, kita bias memasukkan salah satu perintah dari hydra yaitu **hydra –l root –P password list 192.168.1.1 ssh**. Dimana **hydra –l root –P** adalah perintah untuk mengetahui list password, sedangkan **password list** merupakan nama file, dan **192.168.1.1** adalah IP address dari target, serta **ssh** adalah service pada target. Jadi perintah tersebut merupakan perintah yang digunakan untuk mencari list password dari file password list pada service ssh target.

Selain dua tool di atas, kita juga dapat melakukan penetration test menggunakan webgoat. Webgoat adalah aplikasi berbasis java (JSP) untuk simulasi hacking. Di sini kita dapat melakukan penetration test separti SQL injection, dan sebagainya. SQL injection terjadi ketika attacker bisa meng insert beberapa SQL statement ke 'query'

dengan cara manipulasi data input ke applikasi tersebut.

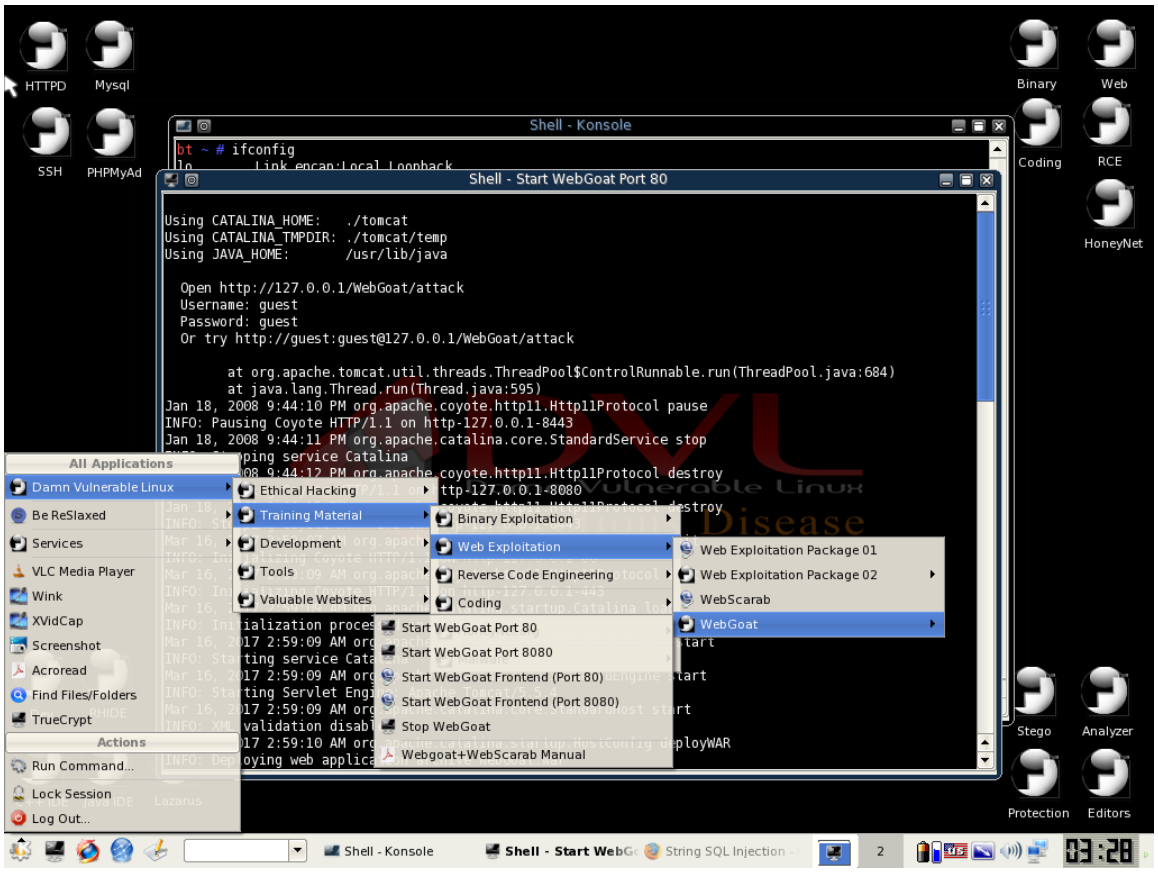
Diantara DB format seperti PHP + MySQL dan ASP + MSACCESS atau dengan MySql. Biasanya Sql Injection dilakukan pada login page pada asp seperti di :

admin\login.asp

login.asp

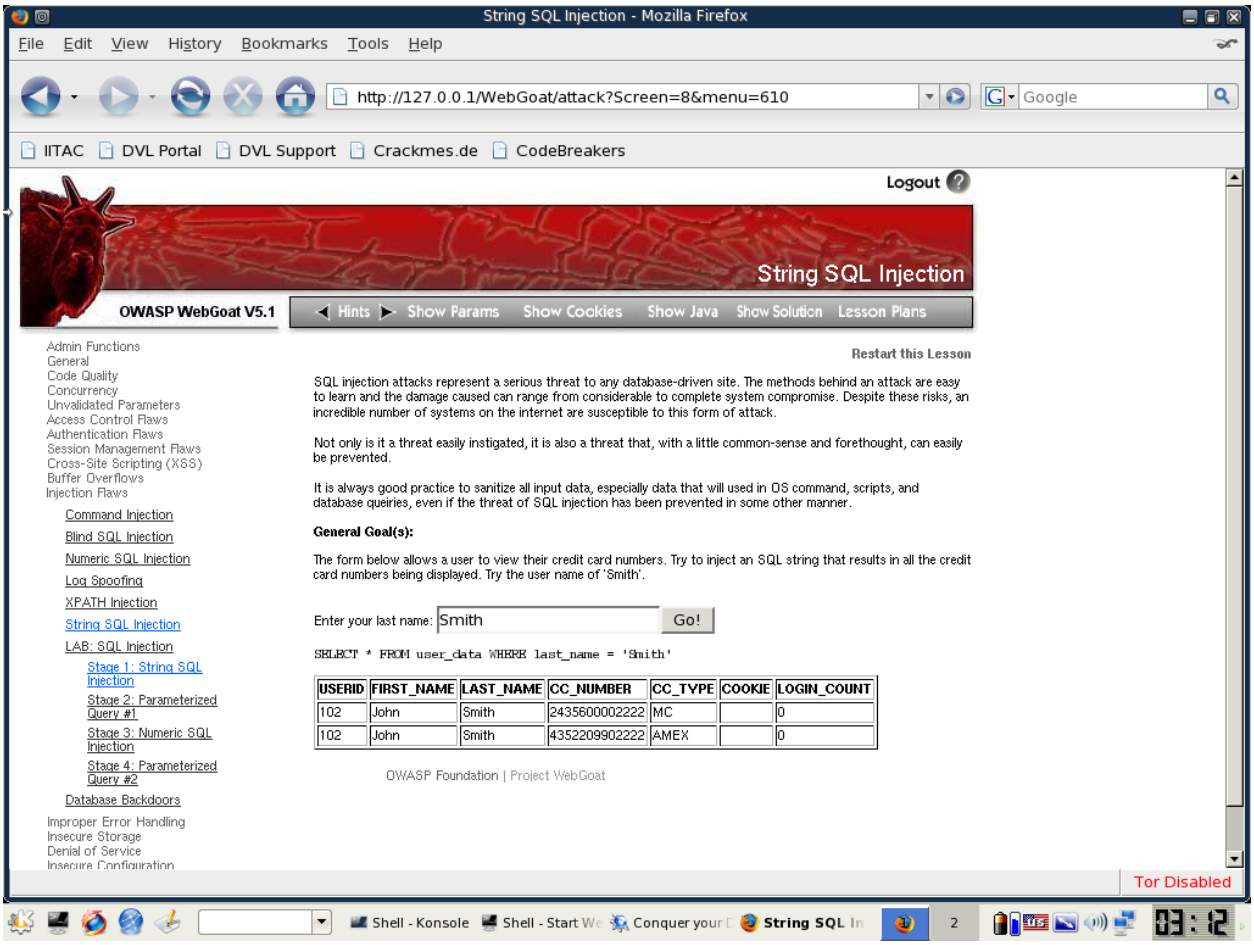
Jadi yang akan menjadi target itu page tersebut.

Untuk menjalankan webgoat ini, langkah awal yang hasrus dilakukan adalah membuka webgoat dengan klik setting, Damn Vulnerable Linux, Training Material, Web Exploitation, WebGoat, Start WebGoat Port 80 seperti berikut.



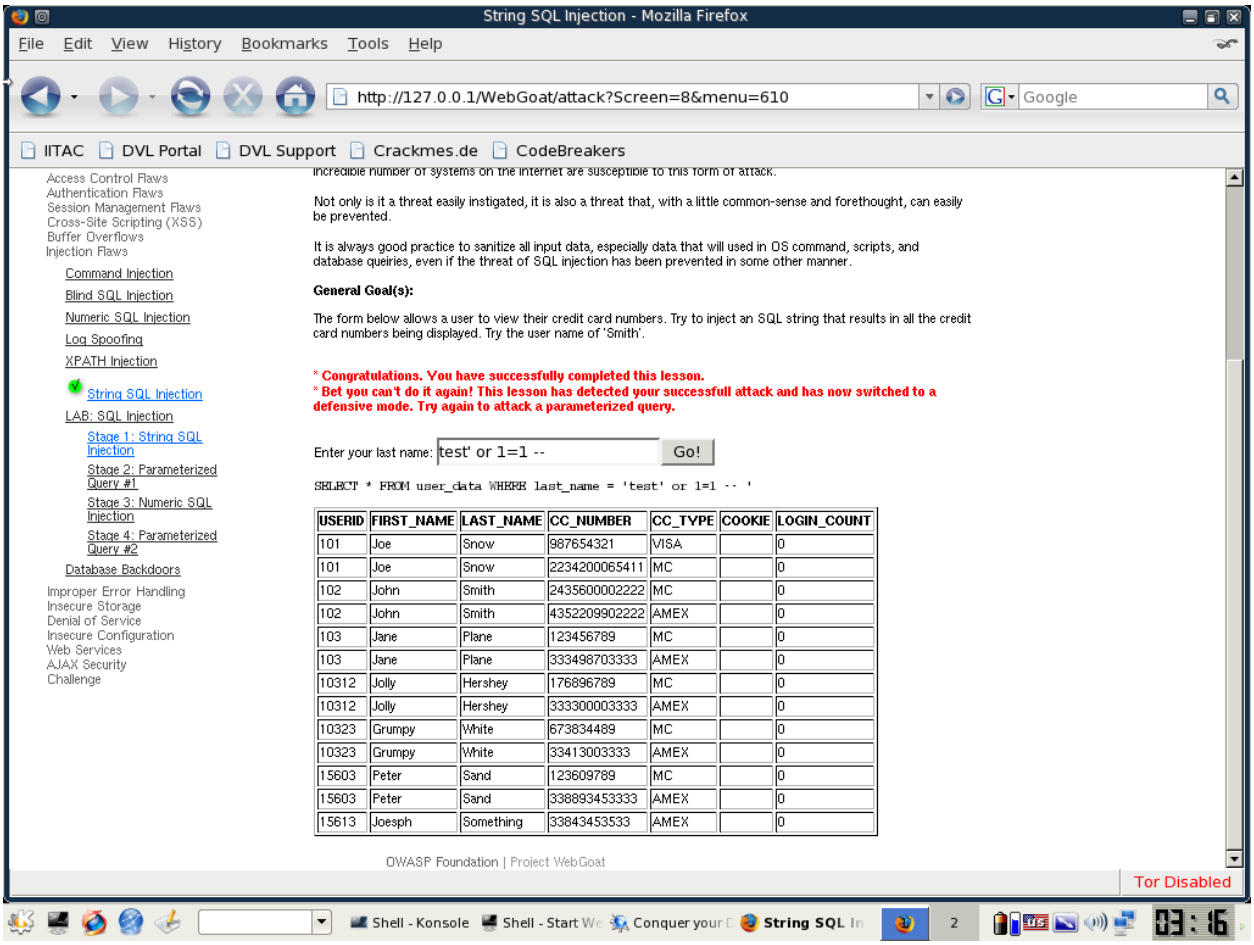
Gambar 6. Memulai WebGoat

Lalu akan tampillah Shell – Start WebGoat Port 80. Dalam shell itu terdapat alamat webgoat attack. Disini alamatnya adalah http://127.0.0.1/WebGoat/attack. masukkan alamat tersebut ke browser yang ada di DVL. Disana terdapat beberapa pilihan, kita pilih Stage 1 String SQL Injection. Disitu terdapat form yang memungkinkan pengguna untuk menampilkan nomor kartu kreditnya. Mencoba untuk menginjeksi SQL String yang mana hasilnya akan menampilkan semua nomor kartu kredit. Untuk mencobanya kita masukkan kata kunci yang berupa last name tersebut dengan ‘Smith’. Maka akan tampil user ID dari ‘Smith’ beserta nomor kartunya. Untuk lebih jelasnya dapat dilihat pada gambar berikut.



Gambar 7. Stage 1: String SQL Injection pada WebGoat

Lalu coba ke pilihan lainnya, yaitu String SQL Injection. Disana akan ada form seperti yang ada pada pilihan sebelumnya. Kita masukkan **test' or 1=1 --** maka akan tampillah hasil seperti berikut.



Gambar 8. String SQL Injection pada WebGoat