TUGAS KEAMANAN JARINGAN KOMPUTER
TRAINING EKSPLOITASI KEAMANAN

NAMA : Yayang Prayoga

NIM : 09011181320006

KELAS : SK8A

SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA

Eksploitasi Keamanan

Keamanan jaringan menjadi semakin penting dengan semakin banyaknya waktu yang dihabiskan orang untuk berhubungan. Mengganggu keamanan jaringan sering lebih mudah daripada fisik atau lokal, dan lebih umum. Celah-celah keamanan jaringan sering digunakan untuk menjebol suatu sistem dibawah ini beberapa Eksploitasi yang dilakukan untuk masuk dalam keamanan suatu sistem.

Anatomi Suatu Serangan Hacking

1. **Footprinting**

   Mencari rincian informasi terhadap sistem-sistem untuk dijadikan sasaran, mencakup pencarian informasi dengan search engine, whois, dan DNS zone transfer. hacker baru mencari-cari sistem mana yang dapat disusupi. Footprinting merupakan kegiatan pencarian data berupa:

   - Menentukan ruang lingkup (scope) aktivitas atau serangan
   - Network enumeration
   - Interogasi DNS
   - Mengintai jaringan

   Semua kegiatan ini dapat dilakukan dengan tools dan informasi yang tersedia bebas di Internet. Kegiatan footprinting ini diibaratkan mencari informasi yang tersedia umum melalui buku telepon. Tools yang tersedia untuk ini di antaranya :

   - Teleport Pro: Dalam menentukan ruang lingkup, hacker dapat men-download keseluruhan situs-situs web yang potensial dijadikan sasaran untuk dipelajari alamat, nomor telepon,contact person,dan lain seagainya.
   - Whois for 95/9/NT: Mencari informasi mengenai pendaftaran domain yang digunakan suatu organisasi. Di sini ada bahaya laten pencurian domain (domain hijack).
   - NSLookup: Mencari hubungan antara domain name dengan IP address.
   - Traceroute 0.2: Memetakan topologi jaringan, baik yang menuju sasaran maupun konfigurasi internet jaringan sasaran.

2. **Scanning**

Scanning terhadap sasaran tertentu dicari pintu masuk yang paling mungkin. Digunakan ping sweep dan portscan.

3. **Enumeration**

Telaah intensif terhadap sasaran,yang mencariuser accountabsah, network resource and share, dan aplikasi untuk mendapatkan mana yang proteksinya lemah. enumerasi sudah bersifat sangat intrusif terhadap suatu sistem. Di sini penyusup mencari account name yang absah,password,serta share resources yang ada. Pada tahap ini,khusus untuk sistem-sistem Windows, terdapat port 139 (NetBIOS session service) yang terbuka untuk resource sharing antar-pemakai dalam jaringan. Anda mungkin berpikir bahwa hard disk yang di-share itu hanya dapat dilihat oleh pemakai dalam LAN saja. Kenyataannya tidak demikian.NetBIOS session service dapat dilihat oleh siapa pun yang terhubung ke Internet di seluruh dunia! Tools seperti Legion,SMBScanner ,atau SharesFinder membuat akses ke komputer orang menjadi begitu mudah (karena pemiliknya lengah membuka resource share tanpa password).

4. **Gaining Access**

Mendapatkan data lebih banyak lagi untuk mulai mencoba mengakses sasaran.Meliputi mengintip dan merampas password,menebak password, serta melakukan buffer overflow. gaining access adalah mencoba mendapatkan akses ke dalam suatu sistem sebagai user biasa.Ini adalah kelanjutan dari kegiatan enumerasi,sehingga biasanya di sini penyerang sudah mempunyai paling tidak user account yang absah,dan tinggal mencari passwordnya saja. Bila resource share-nya diproteksi dengan password, maka passwordini dapat saja ditebak (karena banyak yang menggunakan password sederhana dalam melindungi komputernya).Menebaknya dapat secara otomatis melalui dictionary attack (mencobakan kata-kata dari kamus sebagai password) atau brute-force attack (mencobakan kombinasi semua karakter sebagai password).Dari sini penyerang mungkin akan berhasil memperoleh logon sebagai user yang absah.

5. **Escalating Privilege**

Bila baru mendapatkan user password di tahap sebelumnya, di tahap ini diusahakan mendapat privilese admin jaringan dengan password cracking atau exploit sejenis getadmin, sechole, atau lc_messages. Escalating Privilege mengasumsikan bahwa penyerang sudah mendapatkan logon access pada sistem sebagai user biasa. Penyerang kini berusaha naik kelas menjadi admin (pada sistem Windows) atau menjadi root (pada sistem Unix/Linux).Teknik yang digunakan sudah tidak lagi dictionary attack atau brute-force attack yang memakan waktu itu, melainkan mencuri password file yang tersimpan dalam sistem dan memanfaatkan kelemahan sistem. Pada sistem Windows 9x/ME password disimpan dalam file .PWL sedangkan pada Windows NT/2000 dalam file .SAM.

6. **Pilfering**

Proses pengumpulan informasi dimulai lagi untuk mengidentifikasi mekanisme untuk mendapatkan akses ke trusted system. Mencakup evaluasi trust dan pencarian cleartext password di registry,config file,dan user data.

7. **Covering Track**

Begitu kontrol penuh terhadap sistem diperoleh,maka menutup jejak menjadi prioritas. Meliputi membersihkan network log dan penggunaan hide tool seperti macam-macam rootkit dan file streaming. penyerang sudah berada dan menguasai suatu sistem dan kini berusaha untuk mencari informasi lanjutan (pilfering),menutupi jejak penyusupannya (covering tracks),dan menyiapkan pintu belakang (creating backdoor) agar lain kali dapat dengan mudah masuk lagi ke dalam sistem.Adanya Trojan pada suatu sistem berarti suatu sistem dapat dengan mudah dimasuki penyerang tanpa harus bersusah payah melalui tahapan-tahapan di atas, hanya karena kecerobohan pemakai komputer itu sendiri.

8. **Creating Backdoors**

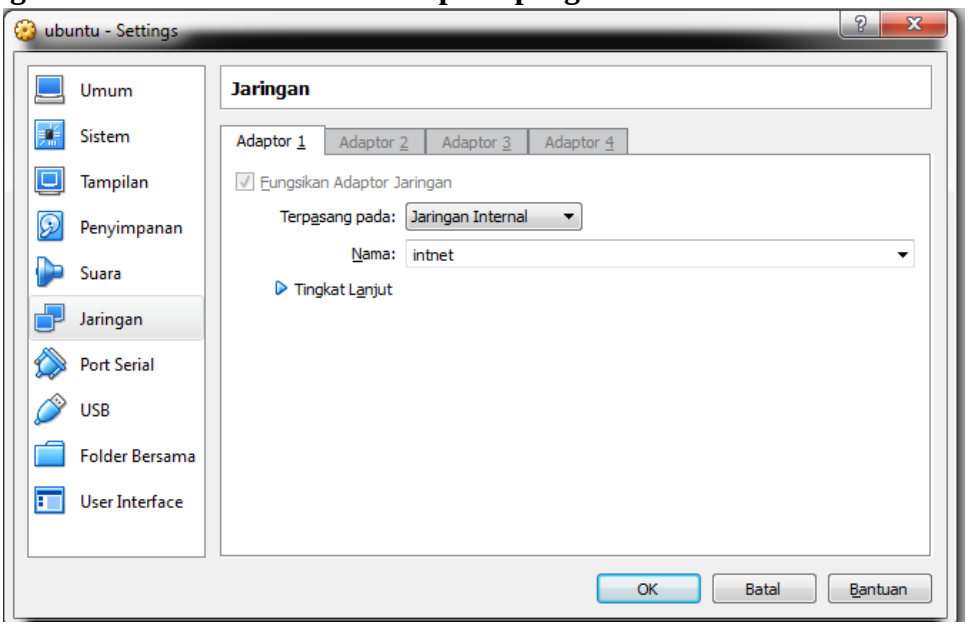
Pintu belakang diciptakan pada berbagai bagian dari sistem untuk memudahkan masuk kembali ke sistem ini dengan cara membentuk user account palsu,menjadwalkan batch job,mengubah startup file, menanamkan servis pengendali jarak jauh serta monitoring tool,dan menggantikan aplikasi dengan trojan.

9. Denial Of Service

Bila semua usaha di atas gagal, penyerang dapat melumpuhkan sasaran sebagai usaha terakhir.Meliputi SYN flood,teknik-teknik ICMP, Supernuke, land/latierra, teardrop, bonk, newtear, trincoo, smurf,dan lain-lain. kalau penyerang sudah frustrasi tidak dapat masuk ke dalam sistem yang kuat pertahanannya,maka yang dapat dilakukannya adalah melumpuhkan saja sistem itu dengan menyerangnya menggunakan paket-paket data yang bertubi-tubi sampai sistem itu crash. Denial of service attack sangat sulit dicegah,sebab memakan habis bandwidth yang digunakan untuk suatu situs. Pencegahannya harus melibatkan ISP yang bersangkutan. Para script kiddies yang pengetahuan hacking-nya terbatas justru paling gemar melakukan kegiatan yang sudah digolongkan tindakan kriminal di beberapa negara ini.

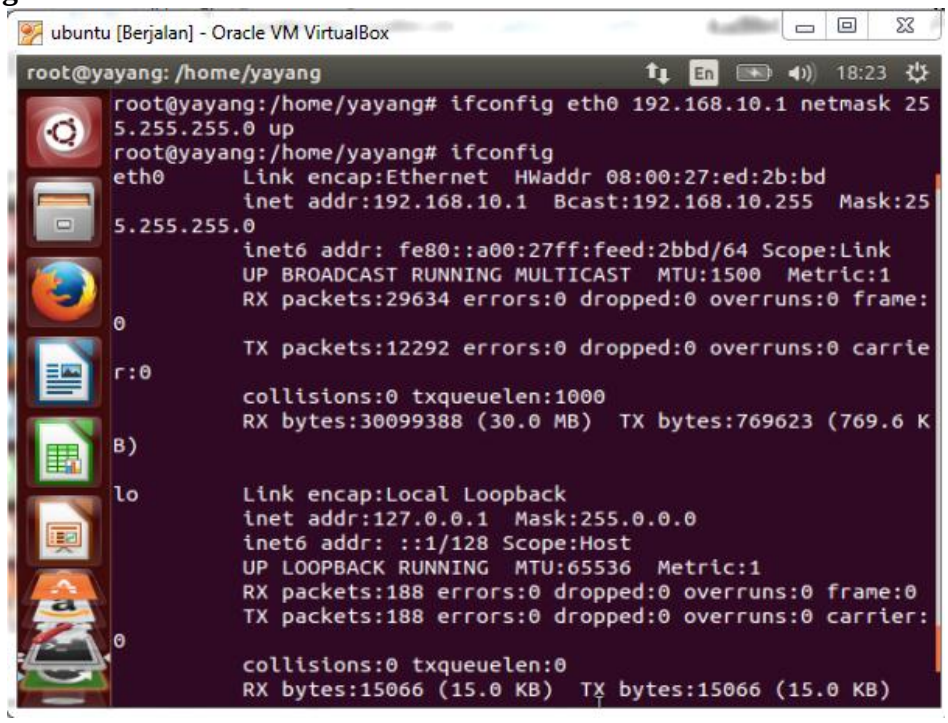
Langkah-langkah dalam melakukan percobaan Exploitasi

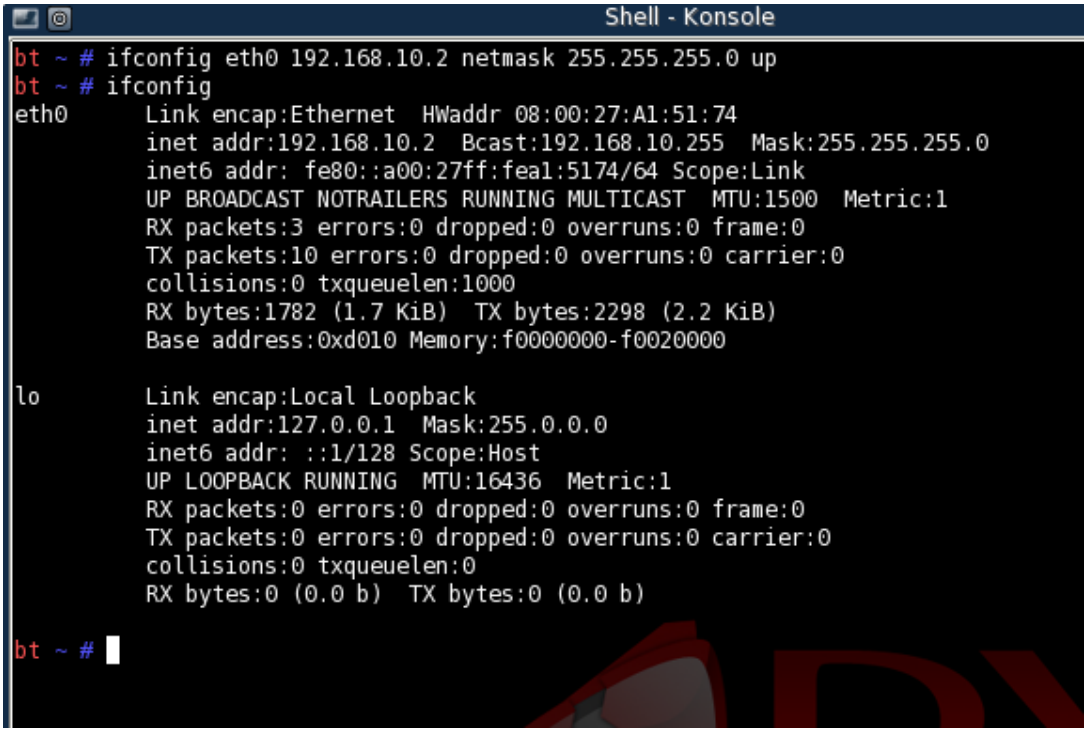
1. **Setting network di Ubuntu dan DVL pada pengaturan VirtualBox**



Langkah ini hanya untuk menghubungkan Ubuntu dan DVL dalam satu jaringan internal. Namun jika Ubuntu dan DVL diletakan pada komputer yang berbeda maka langkah ini tidak diperlukan namun harus menggunakan koneksi internet atau bisa menggunakan perantara penghubung seperti router dan sebagainya.

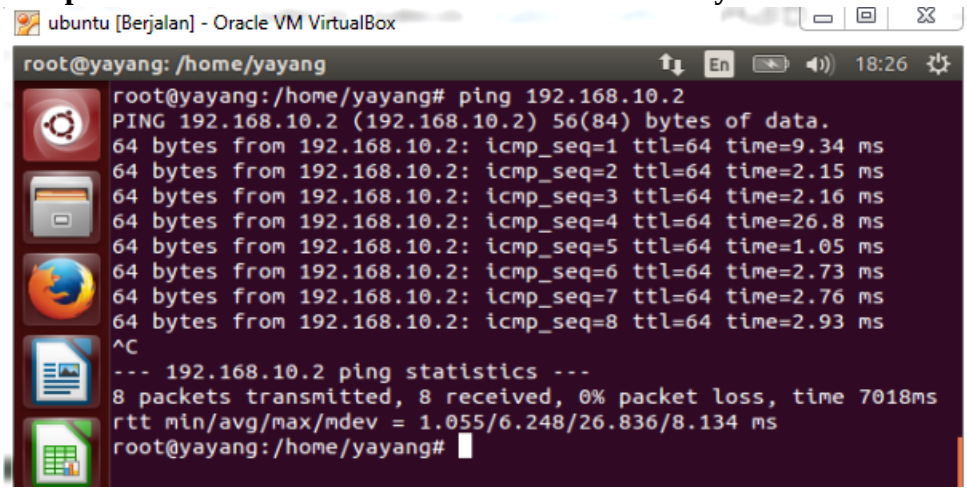
2. **Setting IP Address di Ubuntu dan DVL**

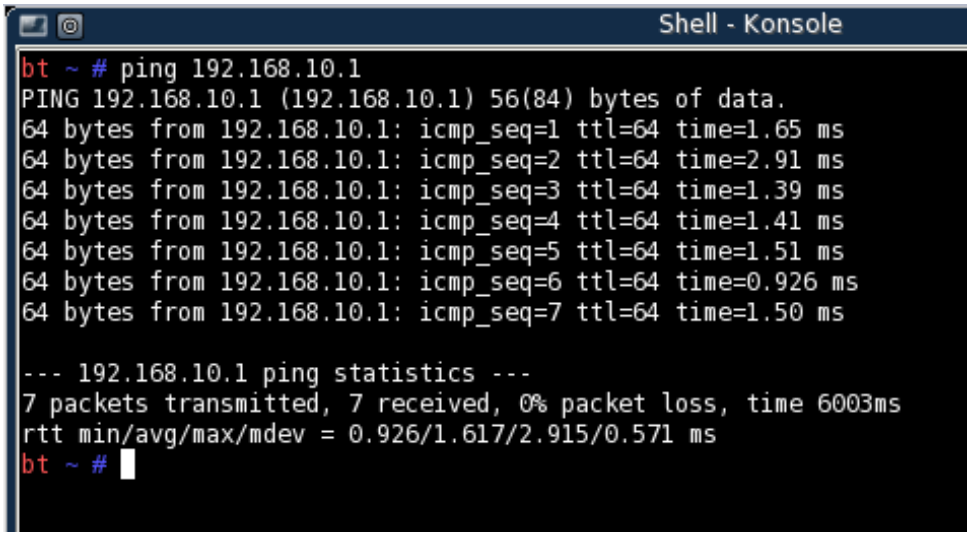




Langkah ini diperlukan jika dilakukan dalam jaringan internal untuk mengetahui IP Address masing-masing agar mudah dalam melakukan percobaan penyerangan sebagai bahan pembelajaran.

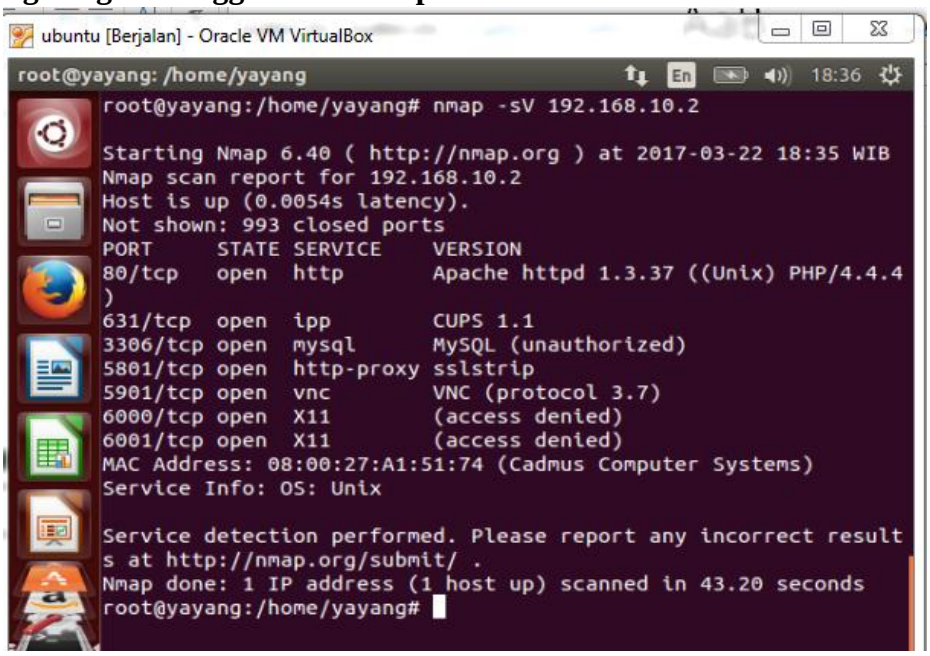
3. Lakukan proses PING dari Ubuntu ke DVL dan sebaliknya





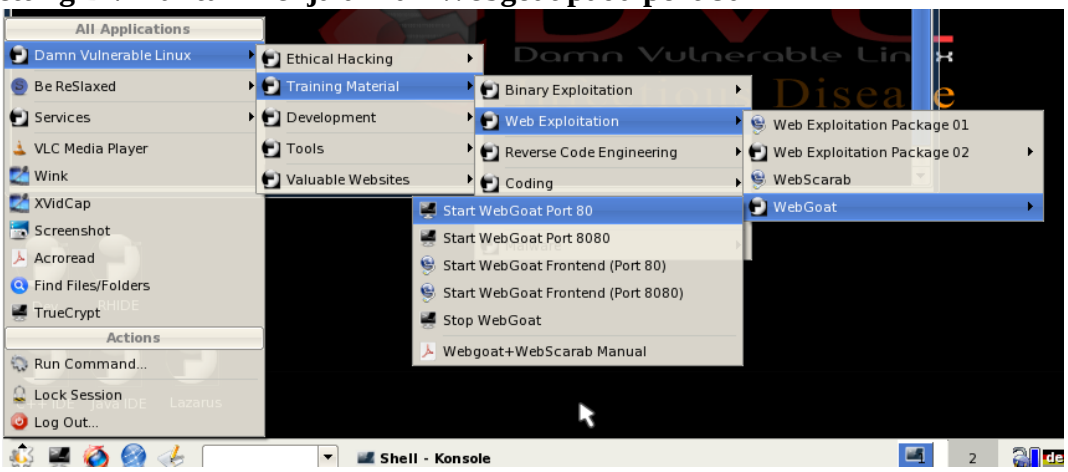
Langkah ini diperlukan untuk memeriksa apakah kedua sistem telah terhubung atau belum.

4. Scanning dengan menggunakan nmap dari Ubuntu



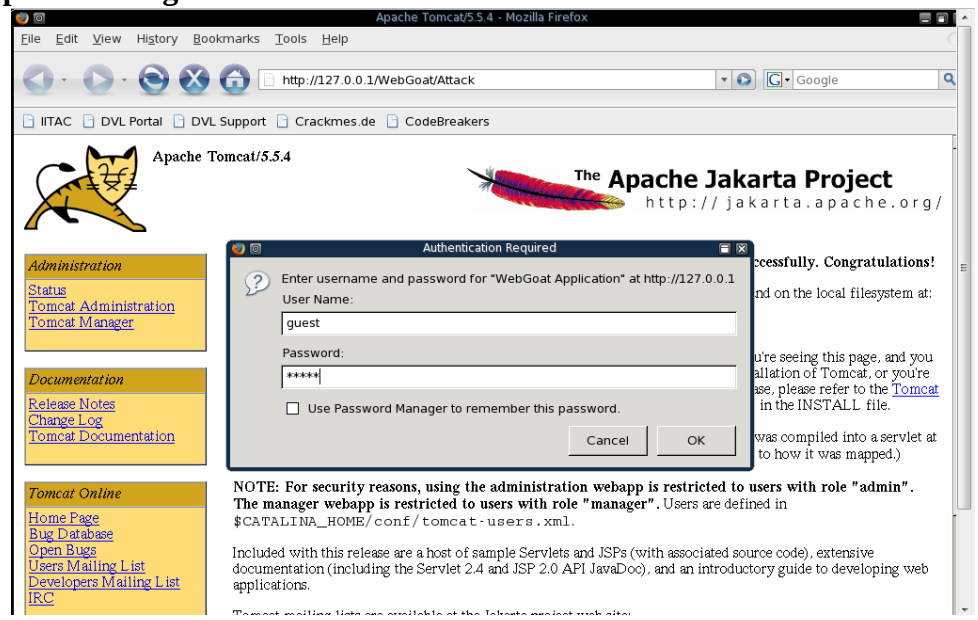
Langkah ini dilakukan untuk memeriksa service apa saja yang terbuka pada DVL. Dalam hal ini service yang aktif adalah http, ipp, mysql, http-proxy, vnc dan x11. Pada tab version adalah versi yang digunakan oleh service tersebut dan dapat digunakan untuk mengetahui kelemahan dari service tersebut dengan bantuan website seperti https://cve.mitre.org atau website lainnya.

5. **Setting DVL untuk menjalankan Webgoat pada port 80**



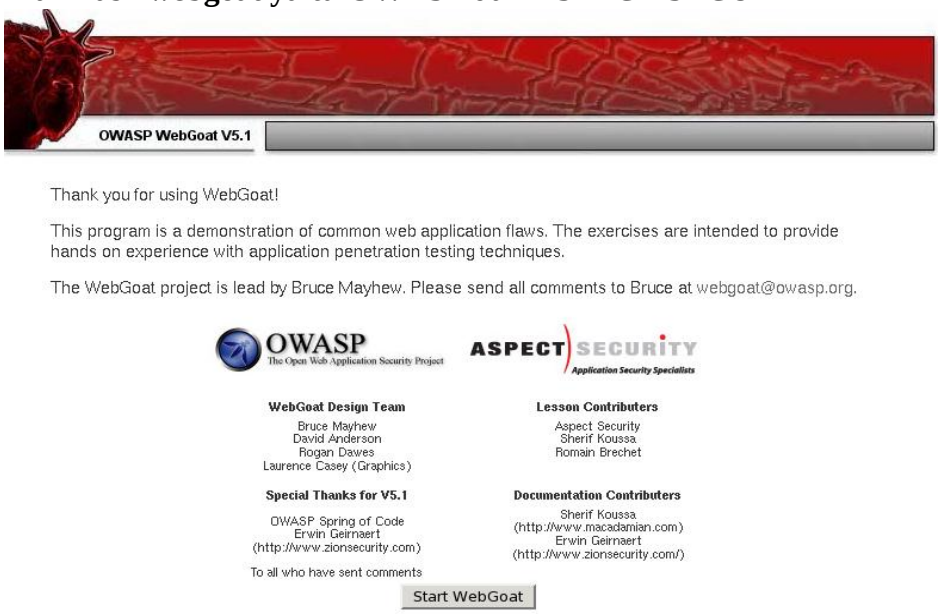
Langkah ini untuk menjalankan salah satu service yang ada pada DVL untuk melakukan percobaan Exploitasi yaitu WebGoat yang di setting agar berjalan di port 80. Web Goat sendiri adalah sebuah project open source yang digunakan sebagai media pembelajaran web hacking.

6. **Tampilkan Webgoat**



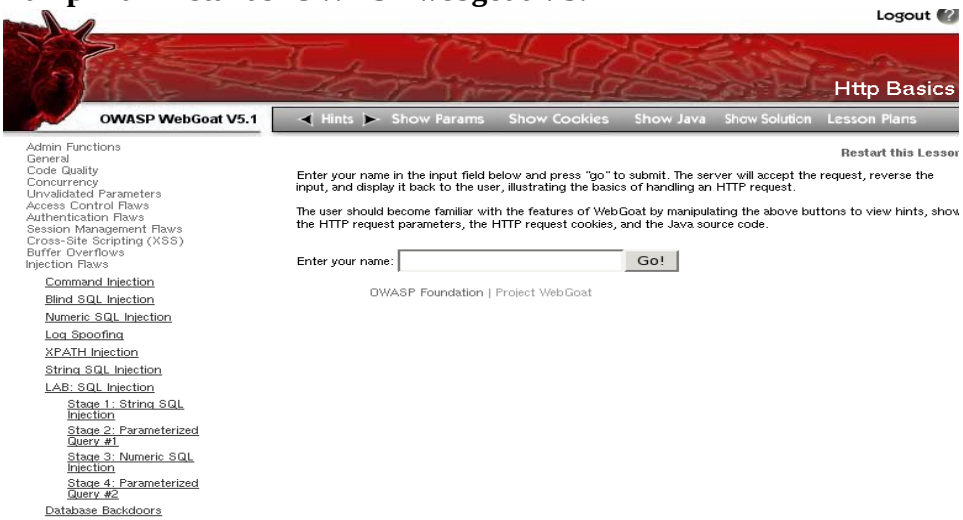
Setelah melakukan setting web goat pada port 80, selanjutnya kita akses webgoat tersebut dengan cara input http://127.0.0.1/WebGoat/Attack pada address bar di web browser. IP address 127.0.0.1 adalah IP address lokal. Setelah kita akses alamat tersebut maka akan tampil form login untuk masuk ke dalam webgoat.

7. **Tampilkan hasil webgoat yaitu OWASP dan ASPECT SECURITY**



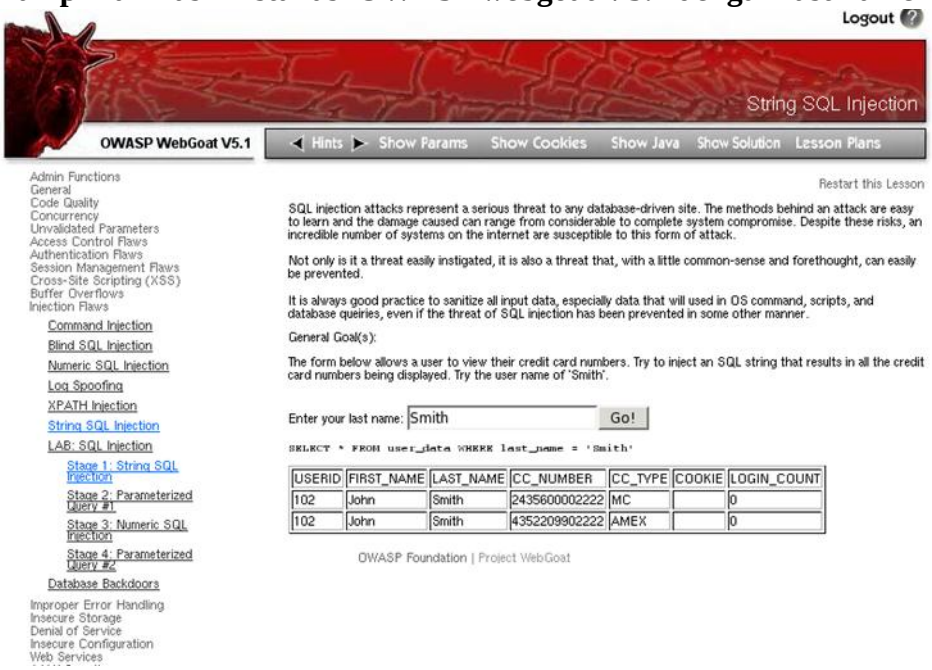
Setelah berhasil login maka akan muncul OWASP dan ASPECT SECURITY. Hal ini dikarenakan DVL menggunakan WebGoat versi lama dan di sarankan untuk mengupdatenya, banyak perbaikan bug dan beberapa update.

8. **Tampilkan installasi OWASP webgoat VS.1**



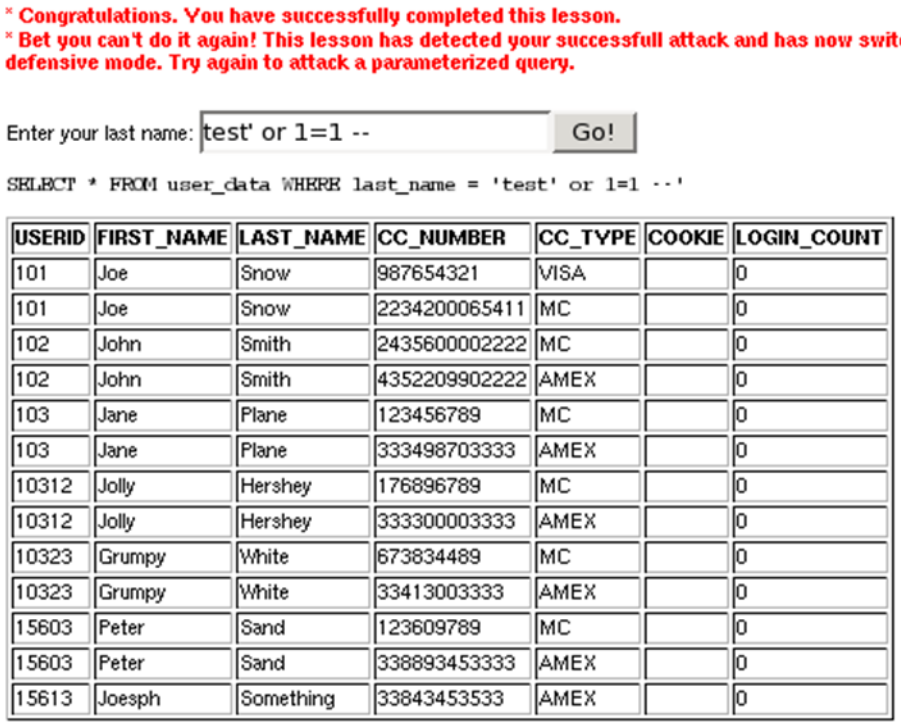
Setelah kita klik “Start Webgoat” kita harus menginput last name untuk menginstall WebGoat. Hal ini dikarenakan WebGoat adalah sebuah aplikasi web yang dikelola oleh OWASP dan dirancang sebagai media pelajaran keamanan aplikasi web. WebGoat memiliki lebih dari satu pelajaran tentang hacking, petunjuk hacking, dan solusi untuk terhindar dari hacking.

9. **Tampilkan hasil installasi OWASP webgoat VS.1 dengan last name ‘smith’**



Salah satu contoh installasi ketika kita input last name “smith” maka akan muncul data table yang berisi USER_DATA, FIRST NAME, LAST_NAME, CC_NUMBER, CC TYPE, COOKIE dan LOGIN_COUNT. Data yang dipatkan dengan input last name “smith” pada OWASP wegoat VS.1 memiliki 2 data saja, itu berarti terdapat 2 kali installasi dengan last name “smith”.

10. **Tampilkan hasil installasi OWASP webgoat VS.1 dengan last name “test’ or 1=1”**



Berbeda hasilnya jika kita input last name “ test’ or 1=1 ..” maka akan tampil banyak data.

ANALISA

Eksploitasi keamanan jaringan adalah sebuah cara untuk melakukan serangan terhadap target dengan melemahkan kemanan pada server target untuk mencuri data-data yang ada di dalam server tersebut. Salah satu contohnya adalah penyerangan terhadap website untuk mencuri data ataupun melumpuhkan website tersebut dengan SQL Injections.

Dalam kasus ini percobaan untuk melakukan serangan tersebut dapat dilakukan dengan menggunakan DVL sebagai media penyerangan. Di dalam DVL terdapat sebuah aplikasi open source yang dapat digunakan untuk bahan pembelajaran dalam hacking. Aplikasi tersebut salah satunya adalah WebGoat.

WebGoat adalah aplikasi open source untuk media pembelajaran hacking yang di kembangkan oleh OWASP. Webgoat sendiri adalah sebuah web dengan keaman yang sangat rendah sehingga dapat dengan mudah diserang.