Keamanan Jaringan Komputer

Disusun Oleh

Nama : Kusuma Dwi Indriani

NIM : 09011181320017

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2017

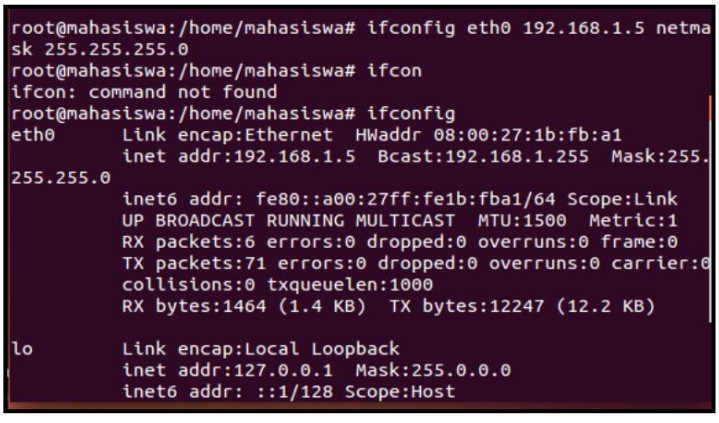
ACTUAL EXPLOIT

Exploit adalah sebuah kode yang menyerang keamanan komputer secara spesifik. Exploit banyak digunakan untuk penentrasi baik secara legal ataupun ilegal untuk mencari kelemahan (Vulnerability) pada komputer tujuan. Bisa juga dikatakan sebuah perangkat lunak yang menyerang kerapuhan keamanan(security vulnerability) yang spesifik namun tidak selalu bertujuan untuk melancarkan aksi yang tidak diinginkan. Banyak peneliti keamanan komputer menggunakan exploit untuk mendesmostrasikan bahwa suatu sistem memiliki kerapuhan.

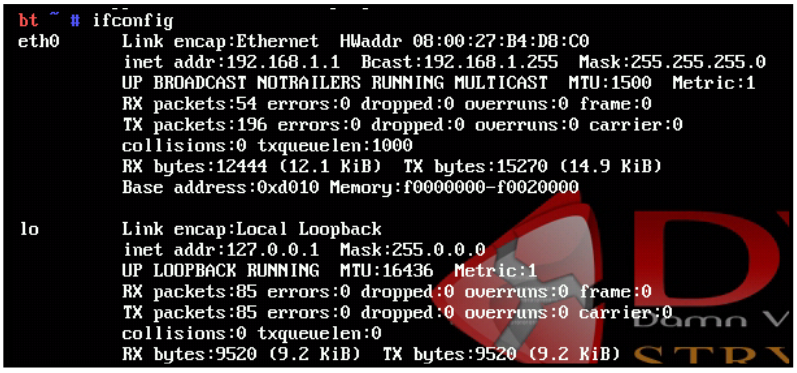
Berikut tahapan yang dilakukan pada saat hands di Laboratorium Jaringan Komputer:

1. Melalui virtual box dijalankan dua virtual machine yaitu Damn Vulnerable Linux (DVL) dan os linux. Terdapat dua hal yang perlu dilakukan saat akan menjalankan kedua virtual machine tersebut diantaranya, setting network pada kedua virtual machine ke ‘internal network’ dan pada general setting operating sistem pilih Linux 2.6.x hal tersebut karna saat memilih operating sistem yang lain tidak akan terjadi booting.

2. Masukkan ip address masing-masing virtual machine dengan ketentuan
   - DVL = 192.168.1.1
   - Linux ubuntu = 192.168.1.5

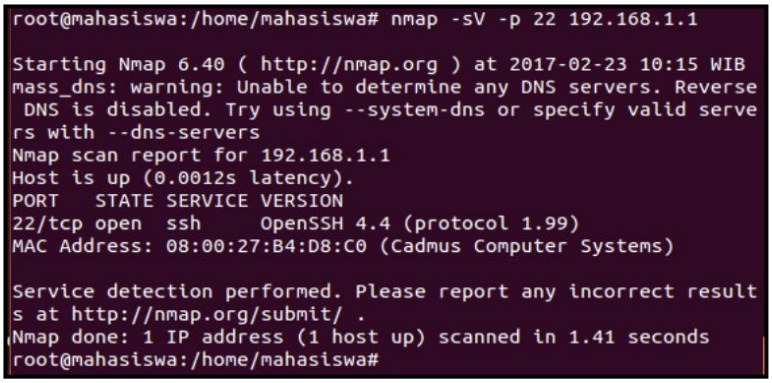


Gambar 1. Pemberian IP address pada ubuntu

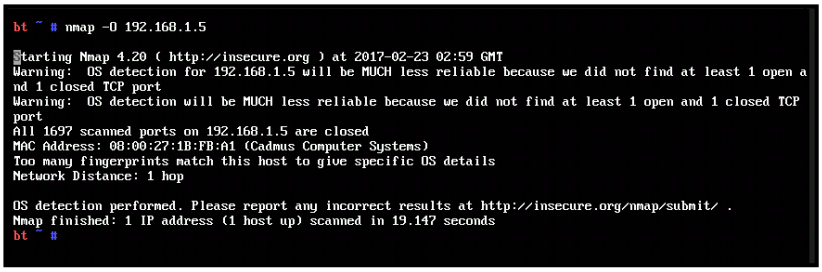


Gambar 2. Pemberian IP address pada DVL

3. Melakukan proses scaning menggunakan nmap melalui ubuntu (gambar 5) dan melalui DVL (gambar 6)



Gambar 3. Nmap ke DVL melalui ubuntu

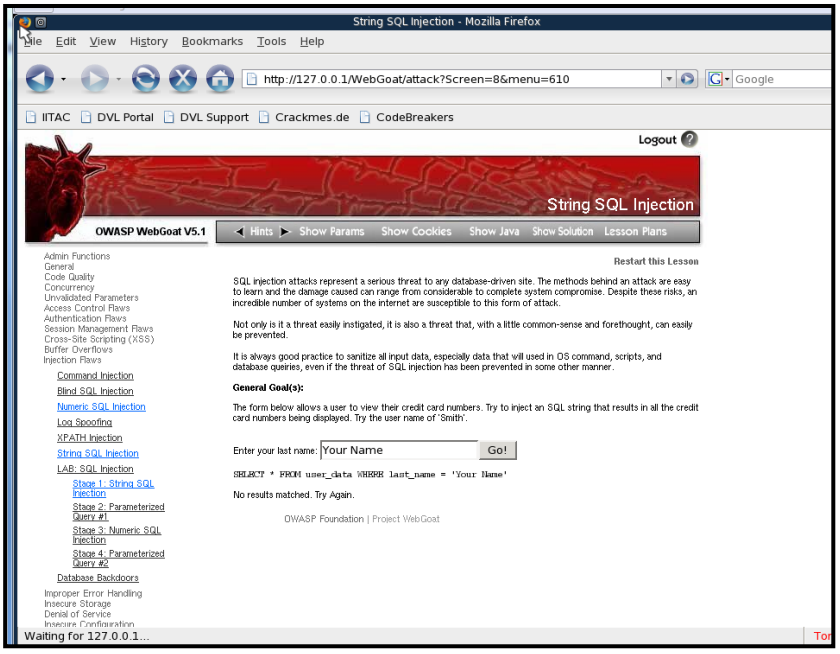


Gambar 4. Nmap Ubuntu ke DVL

4. Ada beberapa kesalahan yang dilakukan oleh admin diantaranya :
   a. Bruteforce : mencoba melakukan input password ke sistem menggunakan tools. Tools tersebut berupa John The Ripper dan Hydra.
   b. Salah konfigurasi
   c. Salah implementasi : kurang cermat pada saat melakukan proses coding(tidak melakukan filter input).

      Cara mengatasi salah implementasi

      - Buka DVL
      - Buka web browser Mozzilla, masukkan url http://127.0.0.1/WebGoat/attack
      - Masukkan username ; guest dan password;guest
      - Saat telah login kemudian pilih String SQL injection ditunjukkan seperti pada gambar 5

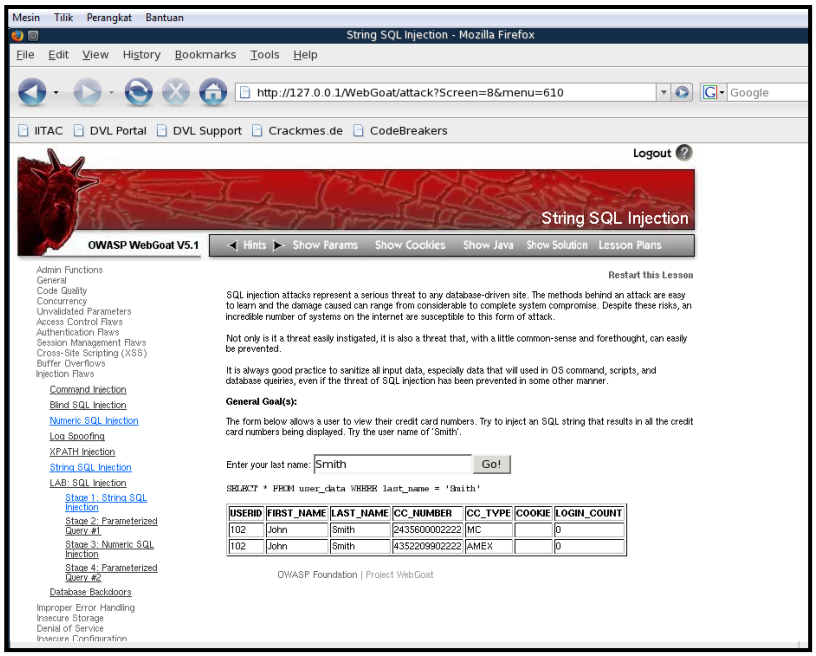


Gambar 5. Hasil setelah login pada WebGoat

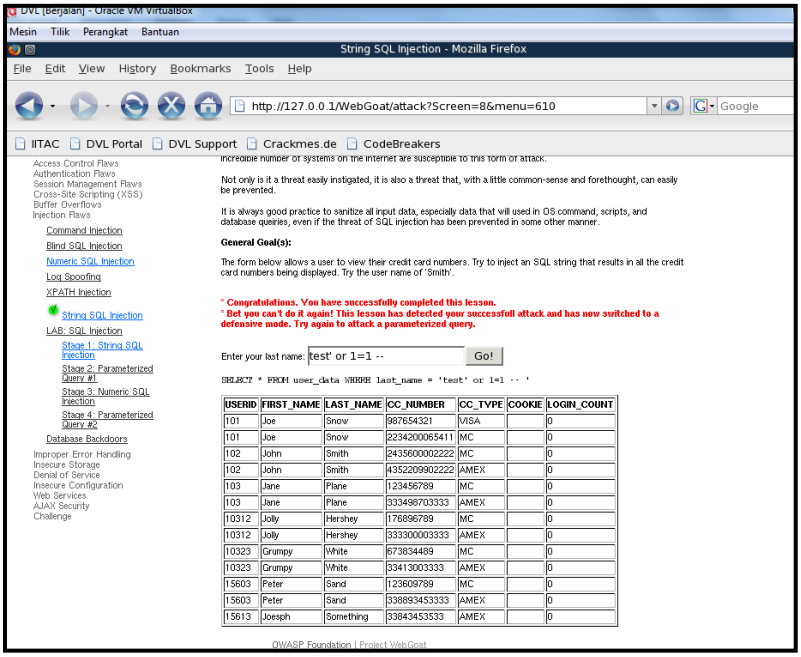
serangan injeksi SQL merupakan ancaman serius ke situs database-driven. Metode balik serangan yang mudah untuk

dipelajari dan kerusakan yang disebabkan dapat berkisar untuk melengkapi sistem.

- Contoh yang dapat dilakukan pada pilihan String SQL injection seperti pada gambar 6 dan gambar 7.



Gambar 6. Hasil penggunaan String SQL injection



Gambar 7. Hasil penggunaan String SQL injection

5. Bug adalah kesalahan yang terjadi pada komputer baik disebabkan oleh perangkat lunak (software) ataupun perangkat keras (hardware) sehingga mempengaruhi kinerja komputer. Berikut jenis-jenis bug :
    - Divide by Zero
    - Infinite Loop
    - Buffer Overflow
    - Deadlock
    - Memory Leak
    - Access Violation
    - Off by One Error