KEAMANAN JARINGAN KOMPUTER

Eko Pratama

09011181320004

Program Studi Sistem Komputer

Fakultas Ilmu Komputer

Universitas Sriwijaya

2017

TUGAS 5

ACTUAL EXPLOIT

Eksploitasi keamanan adalah aktifitas yang dilakukan untuk kerapuhan atau kelemahan keamanan (security vunerability) yang spesifik namun tidak selalu bertujuan untuk melancarkan aksi yang tidak diinginkan

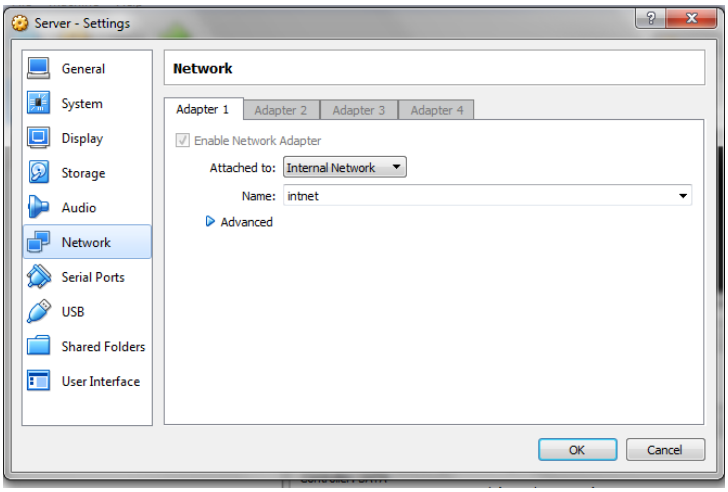
Tugas: Buat langkah langkah hasil dari training (Laporan)

1. **Setting IP dari Ubuntu Server dan DVL**

```
root@server:/home/server# ifconfig enp0s3 192.168.1.1 netmask 255.255.255.0 up
root@server:/home/server# ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:d1:83:71
          inet addr:192.168.1.1  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fed1:8371/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:84156 errors:0 dropped:0 overruns:0 frame:0
          TX packets:20855 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:116776247 (116.7 MB)  TX bytes:1296415 (1.2 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:165 errors:0 dropped:0 overruns:0 frame:0
          TX packets:165 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:12360 (12.3 KB)  TX bytes:12360 (12.3 KB)
```

```
bt ~ # ifconfig eth0 192.168.1.2 netmask 255.255.255.0 up
bt ~ # ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:FE:A7:5F
          inet addr:192.168.1.2  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST NOTRAILERS RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:119 errors:0 dropped:0 overruns:0 frame:0
          TX packets:108 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:13006 (12.7 KiB)  TX bytes:11798 (11.5 KiB)
          Base address:0xd010 Memory:f0000000-f0020000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:36 errors:0 dropped:0 overruns:0 frame:0
          TX packets:36 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:3024 (2.9 KiB)  TX bytes:3024 (2.9 KiB)

bt ~ #
```

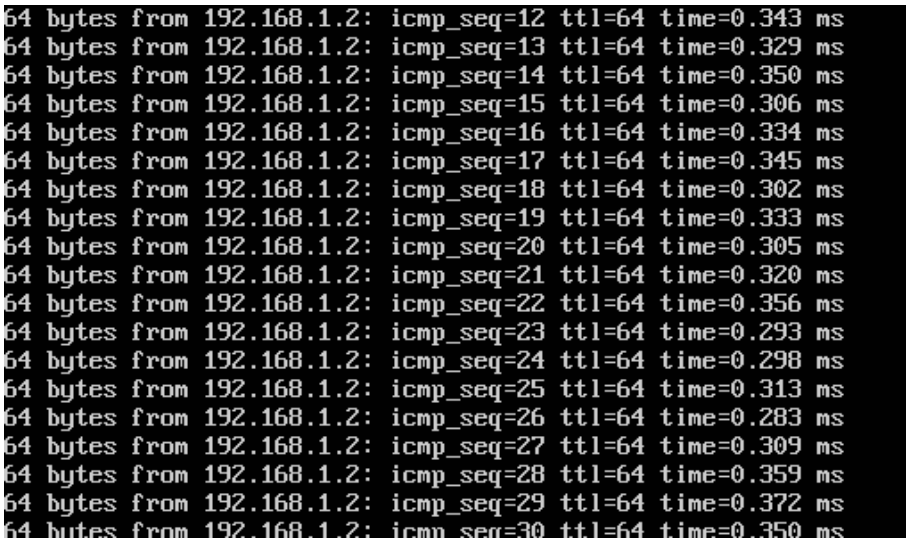
Gambar 1.1. Setting IP



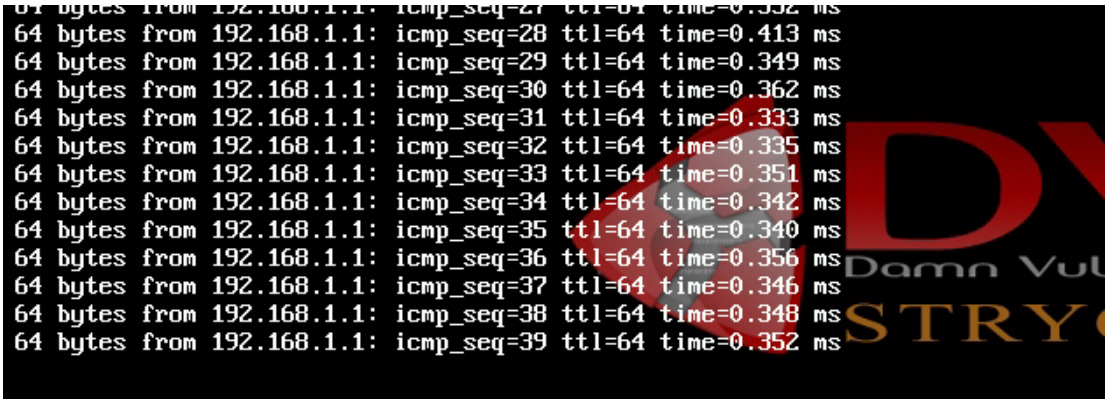
Gambar 1.2. Setting Network

Gambar 2.1. merupakan setting IP dimana pada Ubuntu server diberikan IP 192.168.1.1 sedangkan pada DVL diberikan IP 192.168.1.2 . setelah melakukan setting IP langkah berikutnya adalah melakukan setting network menjadi Internal Network seperti pada Gambar 1.2. terhadap kedua mesin yang sedang berjalan dimana tujuan dari setting tersebut untuk membuat kedua mesin tersebut menjadi jaringan lokal.

2. Ping IP Address



Gambar 2.1. Ping DVL



Gambar 2.2. Ping Ubuntu Server

Setelah melakukan Setting IP dan Setting Network langkah yang harus dilakukan adalah melakukan ping untuk membuktikan bahwa kedua jaringan tersebut sudah saling terhubung. Pada Gambar 2.2. Ubuntu server (192.168.1.1) berhasil terhubung ke DVL (192.168.1.2).

3. Melihat service yang sedang berjalan

```
root@server:/home/server# nmap -sV 192.168.1.2

Starting Nmap 7.01 ( https://nmap.org ) at 2017-03-21 20:48 WIB
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-
dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.1.2
Host is up (0.00010s latency).
Not shown: 992 closed ports
PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH 4.4 (protocol 1.99)
80/tcp   open  http       Apache httpd 1.3.37
631/tcp  open  ipp        CUPS 1.1
3306/tcp open  mysql      MySQL (unauthorized)
5801/tcp open  http-proxy sslstrip
5901/tcp open  vnc        VNC (protocol 3.7)
6000/tcp open  X11        (access denied)
6001/tcp open  X11        (access denied)
MAC Address: 08:00:27:53:83:20 (Oracle VirtualBox virtual NIC)
Service Info: Host: bt.example.net; OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.26 seconds
root@server:/home/server#
```

Gambar 3.1. Scanning nmap

Seperti dapat kita lihat pada gambar 3.1. dimana ketika kita memasukan perintah seperti gambar diatas maka aplikasi tersebut akan melakukan scanning port yang terbuka pada IP target (192.168.1.2). dimana pada langkah sebelumnya kita telah membuka/menjalankan seluruh aplikasi yang terdapat pada mesin DVL dan yang terjadi ketika kita melakukan scanning pada target yaitu mesin DVL maka aplikasi yang sedang berjalan itulah yang dianggap sebagai celah untuh menyerang karena port dalam keadaan terbuka.

Service ssh menggunakan bruteforce mencoba melakukan input password menggunakaan beberapa tools

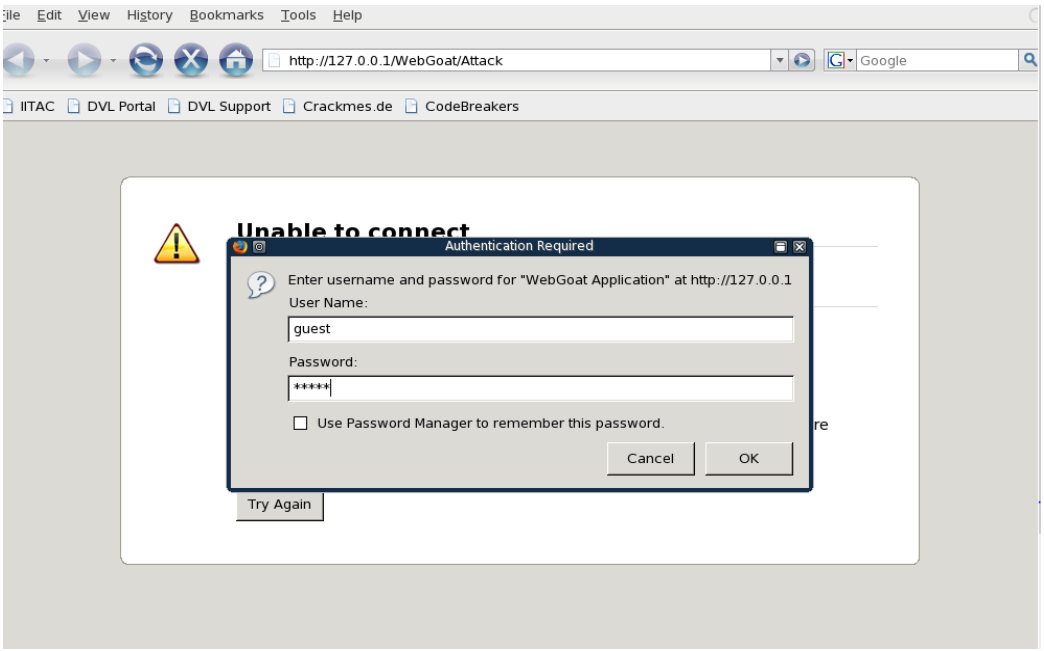
Berikut merupakan beberapa tools yang digunakan:

- Hydra
- Nmap

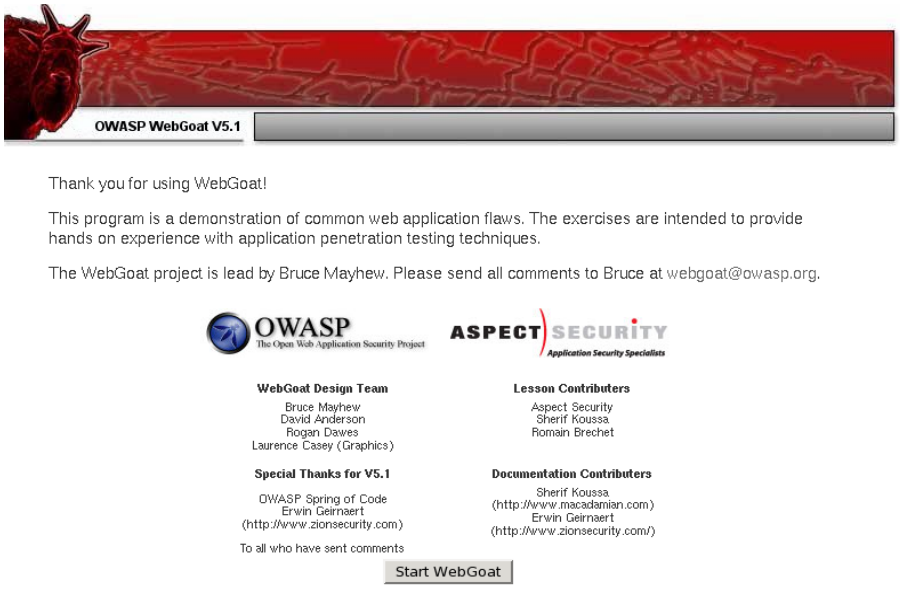
4. Buka Web Goat pada DVL

Gambar 4.1. membuka Web Goat

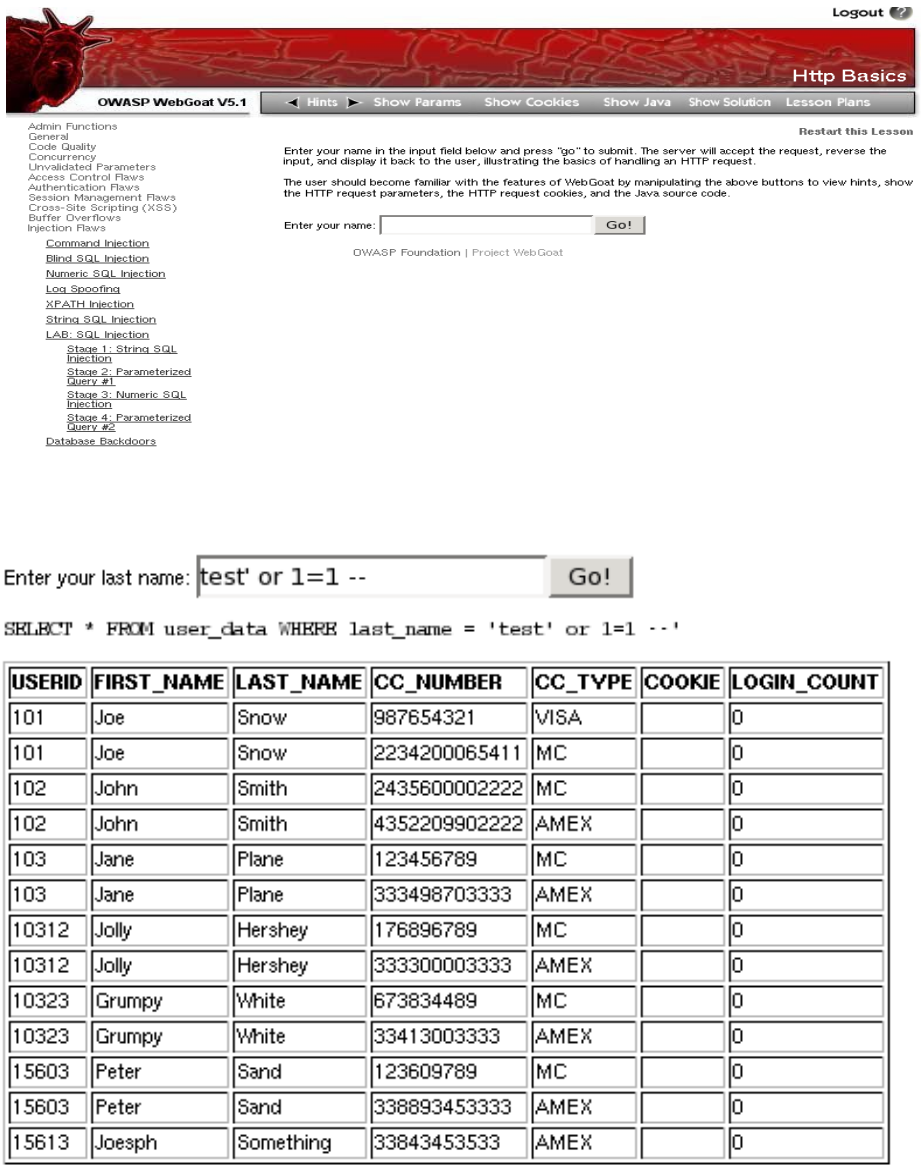
Web Goat adalah project Open Source yang dapat digunakan agar orang lain bisa belajar web hacking salah satunya adalah SQL Injection. Langkah yang dilakukan seperti gambar 4.1 diatas setelah berhasil masuk maka akan muncul tampilan seperti gambar 4.2 untuk login. Lalu, masukkan username “guest” dan password “guest” untuk melanjutkan membuka Web Goat. Jika berhasil maka akan langsumh masuk ke interfaces tampilan awal Web Goat seperti gambar 4.3



Gambar 4.2. Login Web Goat



Gambar 4.3. Interfaces Web Goat



Gambar 4.4. Percobaan Web Goat

Pada gambar 4.4. terlihat bahwa ketika saya mencoba melakukan percobaan dengan memasukan query seperti gambar diatas maka didapatlah data tersebut. Maksud dari query tersebut adalah :

Test : nama file dari database tersebut
‘ : menghentikan query yang diinputkan
Command 1=1 : memberikan querry yang diinputkan jika 1=1 bernilai true