Nama : Riki Andika
NIM : 09011181320015

Hang on Training, Kamis 16 Maret 2017

Network scanner adalah metode bagaimana caranya mendapatkan informasi sebanyak-banyaknya dari IP/Network target yang akan dicari titik kelemahannya, kali ini dilakukan scanning dengan menggunakan simulasi yang menggunakan software virtualbox dengan dua sistem operasi linux, dengan 1 OS Linux digunakan sebagai Targen yang akan discan dengan alamat IP yang telah ditentukan 192.168.100.20, dan OS Linux yang satunya dijadikan sebagai penyerang dengan alamat IP 192.168.100.10. Berikut simulasi yang telah dilakukan sebagai berikut;

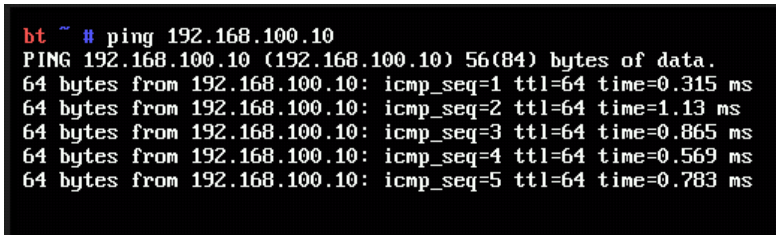
```
bt ~ # ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:41:4E:02
          inet addr:192.168.100.20  Bcast:192.168.100.255  Mask:255.255.255.0
          UP BROADCAST NOTRAILERS RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:83 errors:0 dropped:0 overruns:0 frame:0
          TX packets:84 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:9828 (9.5 KiB)  TX bytes:9502 (9.2 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:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)

bt ~ #
```

**Gambar 1.** If config sistem operasi target

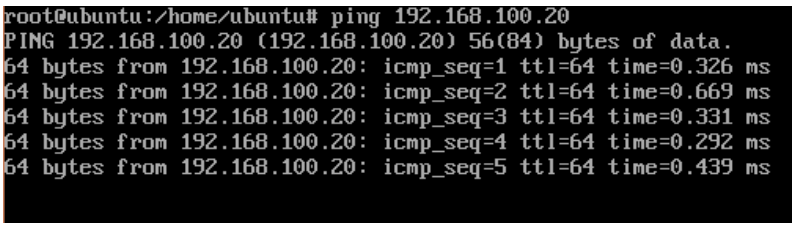
```
root@ubuntu:/home/ubuntu# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:10:8a:e2
          inet addr:192.168.100.10  Bcast:192.168.100.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe10:8ae2/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:104 errors:0 dropped:0 overruns:0 frame:0
          TX packets:135 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:10002 (10.0 KB)  TX bytes:18516 (18.5 KB)

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:78 errors:0 dropped:0 overruns:0 frame:0
          TX packets:78 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:5688 (5.6 KB)  TX bytes:5688 (5.6 KB)

root@ubuntu:/home/ubuntu#
```

**Gambar 2.** If config sistem operasi penyerang

Tahap awal ialah dengan menyamakan jaringan dari alamat IP Address yang digunakan, sehingga dapat memudahkan dalam pertukaran data dan informasi yang diingingkan, intiya agar dapat terhubung satu sama lain. Berikut testing penghubung antara dua sistem operasi yang telah dibuat, dengan melakukan ping pada sitiap sistem operasi yang telah dibuat;

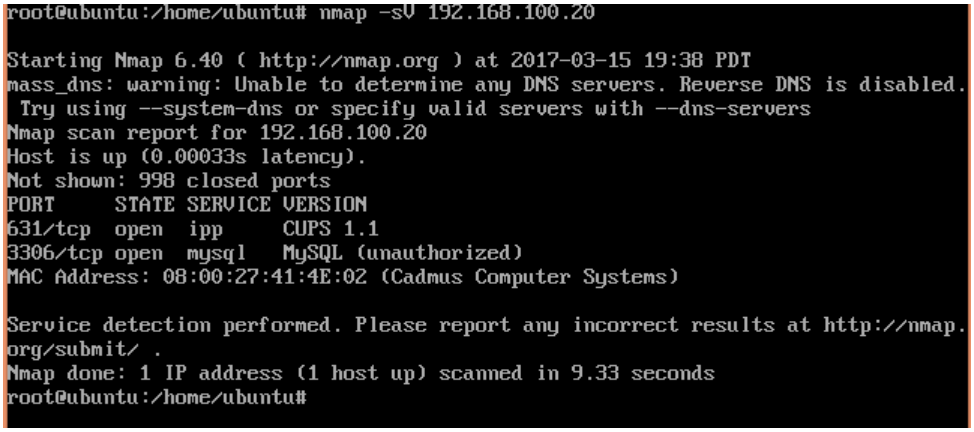



**Gambar 3.** Ping dari IP 192.168.100.20 (Target)

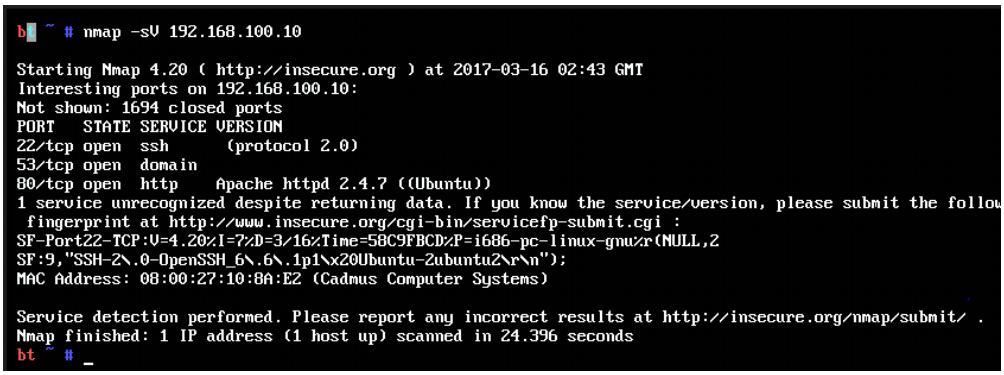



**Gambar 4.** Ping dari IP 192.168.100.10 (Penyerang)

Langkah pertama yang dilakukan dalam scanning kali ini ialah melihat service yang sedang berjalan pada website target, dengan menggunakan tools online yaitu NMAP (Network Mapper) yang merupakan sebuah aplikasi atau tool yang berfungsi untuk melakukan port scanning, dengan menggunakan perintah Nmap –sV 192.168.100.20. Berikut hasil screenshot dari proses yang telah dilakukan dapat dilihat pada gambar 5.

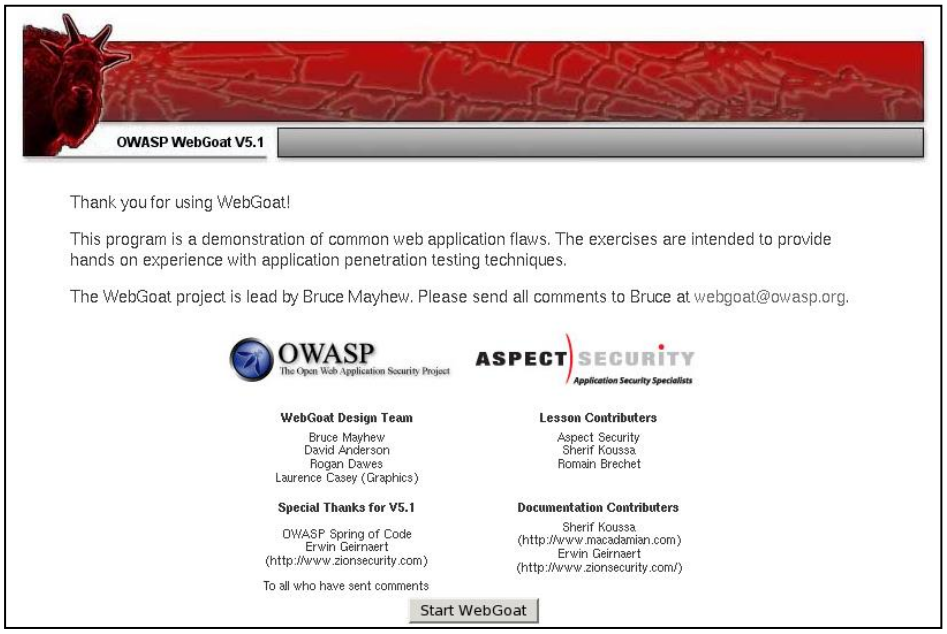



**Gambar 5.** Melihat service yang sedang berjalan



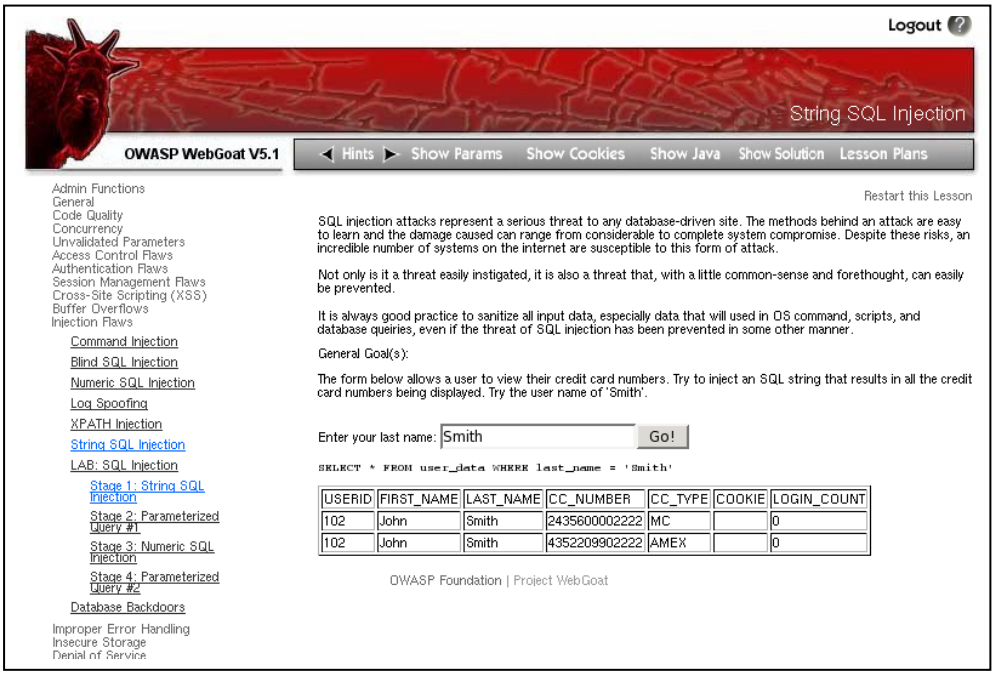

**Gambar 6.** Melihat service yang sedang berjalan

Dari gambar 5 dan 6 dapat dilihat terdapat beberapa service yang sedang sunning atau berjalan dari masing-masing target yang akan dijadikan sebagai celah dalam melakukan penyerangan dari website tersebut. Dengan menggunakan tools port scanning NMAP dapat juga menggunakan tools hydra untuk melihat service ssh menggunakan bruteforce dengan mencoba melakukan input password menggunakaan tool hydra. Secure Shell (ssh) adalah suatu protokol yang memfasilitasi sistem komunikasi yang aman diantara dua sistem yang menggunakan arsitektur client/server, serta memungkinkan seorang user untuk login ke server secara remote. Wegoat merupakan aplikasi berbasis web PHP dan Mysql untuk belajar ekploitasi aplikasi suatu website dengan menampilkan bug – bug yang memanfaatkan aplikasi web tersebut. Berikut screen shot dari hydra yang digunakan;

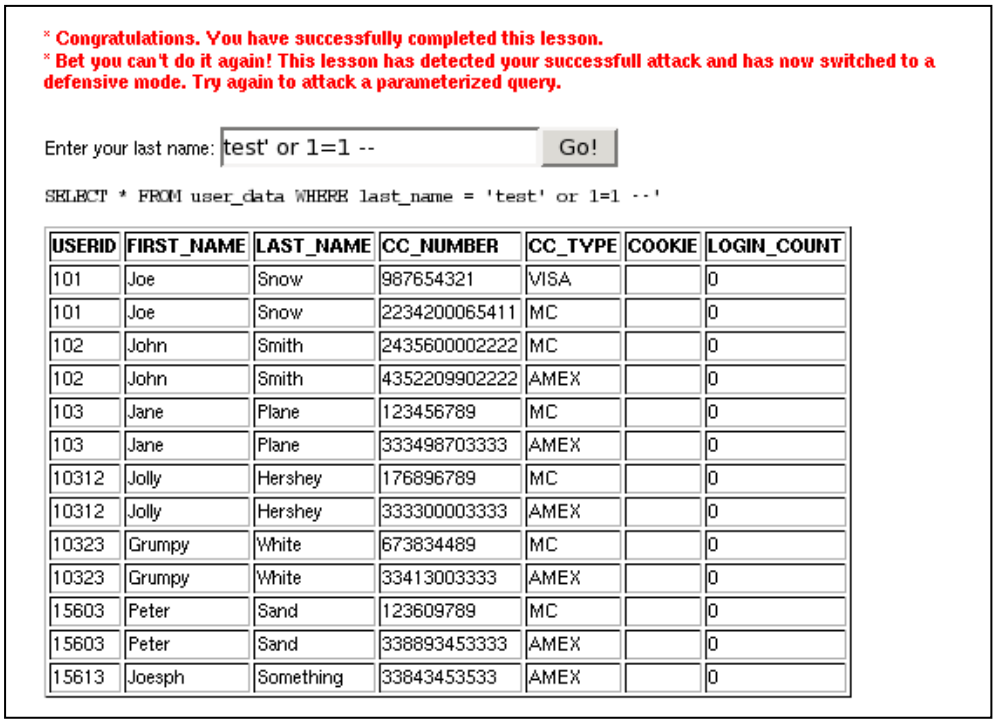



**Gambar 7.** Web exploitation webgoat

Setelah masuk dan wegoat dijalankan, lakukan pencarian semua nama dengan last name Smith atau user name Smith yang menghasilkan tabel serta query yang digunakan, yang dapat dilihat pada gambar 8 berikut;




**Gambar 8.** Penggunaan wegoat dengan memasukkan kata smith




**Gambar 9.** Menampilkan semua data yang ada

Penambahan tanda petik yang ada diawal dan akan membaca last name yg kita masukkan , maksud 1=1 adalah boolean true walaupun kita salah masih akan bernilai true. Hal ini lah yang menjadi kesalahan dari program tersebut, karena tidak melakukan pemfilteran terlebih dahulu, sebab berdasarkan dari perintah yang telah dilakukan dalam kolom pencarian yang ada pada lembar kerja wegoat dengan perintah test' or 1=1 – yang menampilkan semua data dalam bentuk tabel yang ada. Hal ini dapat dijadikan sebagai landasan bagi attecker untuk melakuka percobaan dalam penginputan password karena sudah mengetahui bug-bug yang dimiliki.

SQL injeksi dalam serangan terdiri dari penyisip query SQL yang diperoleh melalui input data dari attecker ke aplikasi, dengan SQL injection dapat mengeksploitasi dan membaca data yang penting dari sebuah database yang dilakukkan scanning, memodifikasi data database (Insert / Update / Delete), melakukan operasi administrasi pada database seperti shutdown database manajemen sistem (DBMS)