TUGAS

“KEAMANAN JARINGAN KOMPUTER”

Disusun Oleh :

Nama : Erick Okvanty Haris

Nim : 09011181320012

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2017

Berikut adalah hasil dari evaluasi keamanan sistem actual exploit:

- Ifconfig berfungsi untuk mengecek IP

```
bt ~ # ifconfig eth0 192.168.100.20 netmask 255.255.255.0_
```

```
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 ~ #
```

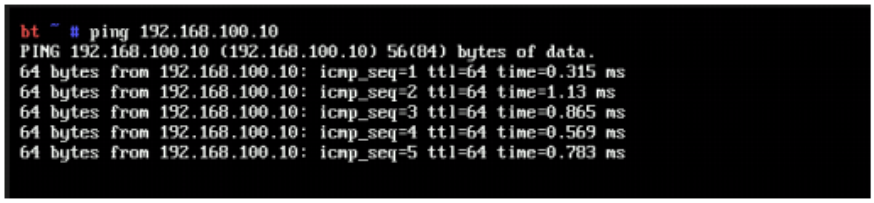
```
root@ubuntu:/home/ubuntu# ifconfig eth0 192.168.100.10 netmask 255.255.255.0
```

```
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#
```

- Ping 192.168.100.20

```
root@ubuntu:/home/ubuntu# ping 192.168.100.20
PING 192.168.100.20 (192.168.100.20) 56(84) bytes of data.
64 bytes from 192.168.100.20: icmp_seq=1 ttl=64 time=0.326 ms
64 bytes from 192.168.100.20: icmp_seq=2 ttl=64 time=0.669 ms
64 bytes from 192.168.100.20: icmp_seq=3 ttl=64 time=0.331 ms
64 bytes from 192.168.100.20: icmp_seq=4 ttl=64 time=0.292 ms
64 bytes from 192.168.100.20: icmp_seq=5 ttl=64 time=0.439 ms
```

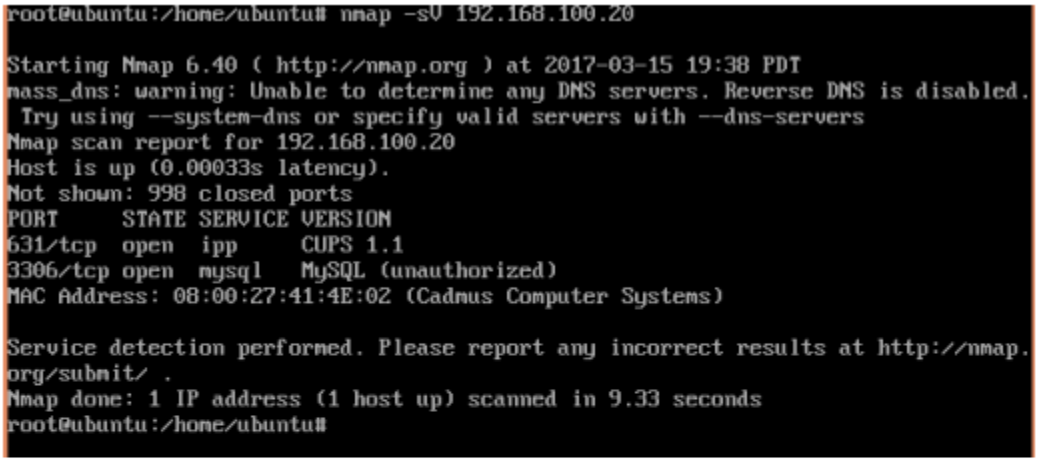
- Ping 192.168.100.10

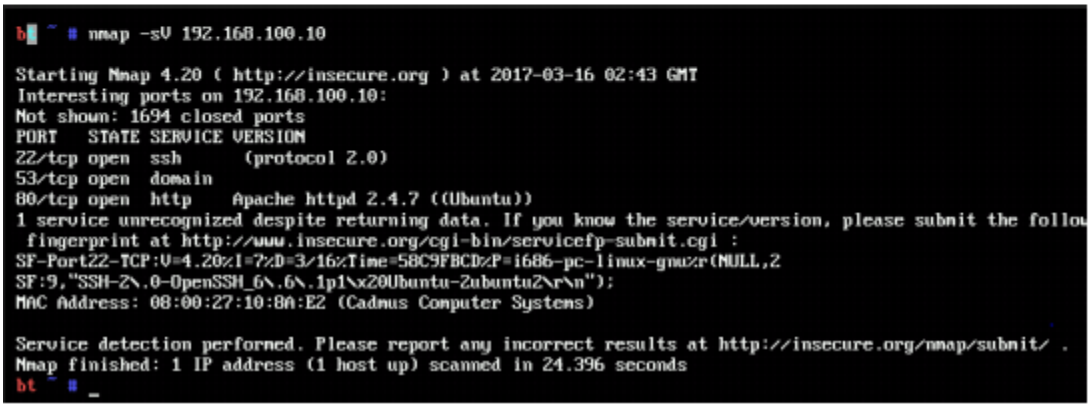


Ping berfungsi untuk mengetahui mesin mana saja yang aktif di network target. Proses diatas adalah ping dari server DVL ke server ubuntu.

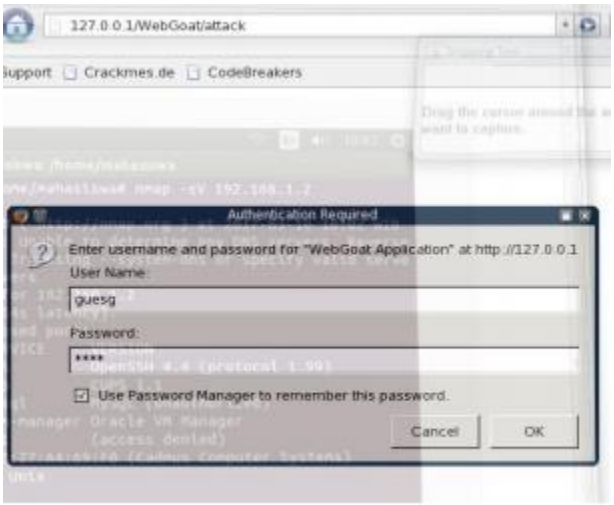
Nmap –sV 192.168.100.10

Nmap –sv berfungsi untuk memeriksa service yang sedang berjalan. nmap – sV<host/IP target>

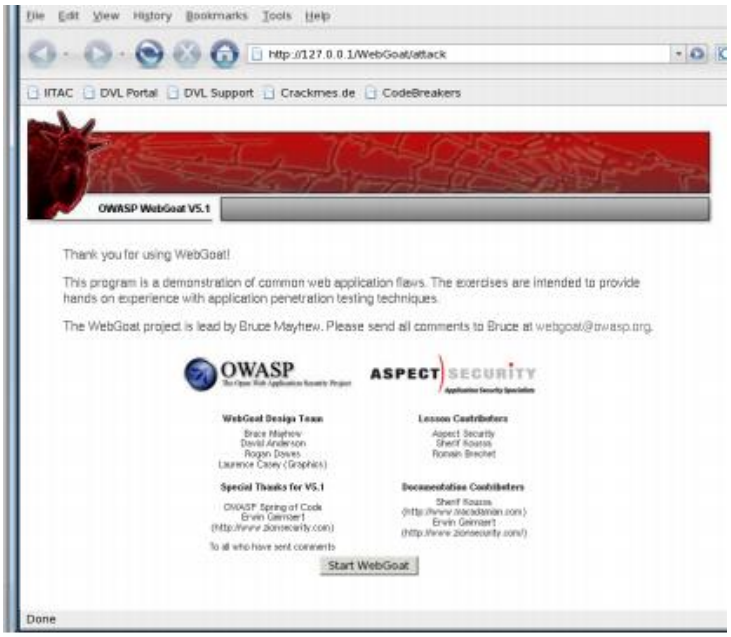


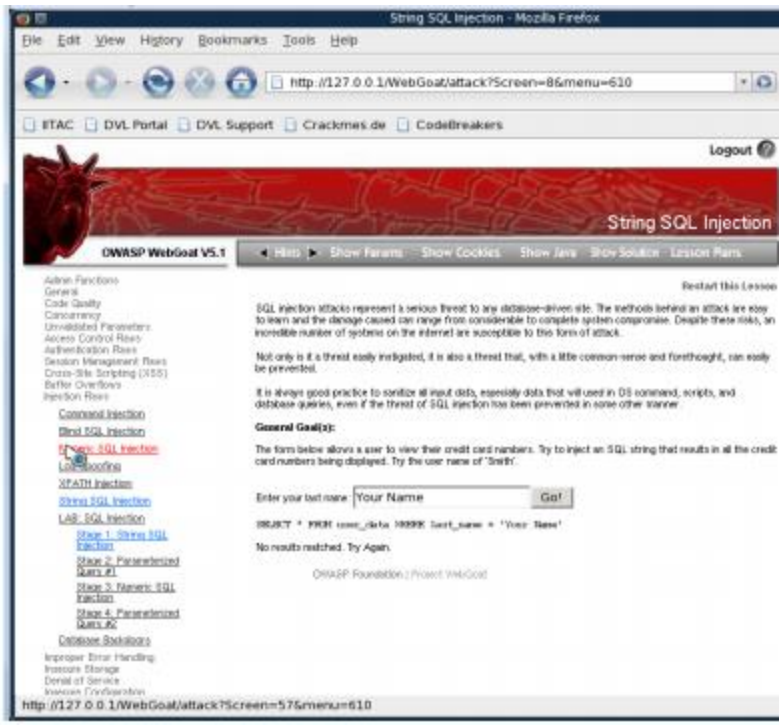


Service ssh menggunakan bruteforce mencoba melakukan input password menggunakaan tool. Tools yg bisa di gunakan adalah *Hydra dan Nmap.* Pada percobaan ini menggunakan tools Hydra. **Hydra -l –P password.list 192.168.100.10 ssh** Setelah melakukan perintah diatas, selanjutnya kita melakukan pencarian ke alamat http://127.0.0.1/WebGoat/Attack kemudian akan muncul autentikasi berupa username dan password, dengan username dan password nya adalah guest.

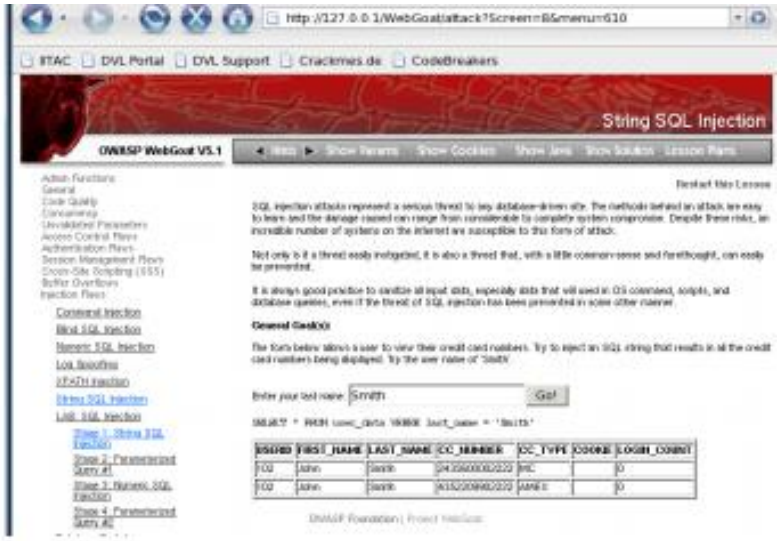


Setelah login berhasil, selanjutnya akan tampil halaman home webgoat di bawah ini, kemudian kita klik start untuk memulai pencarian.

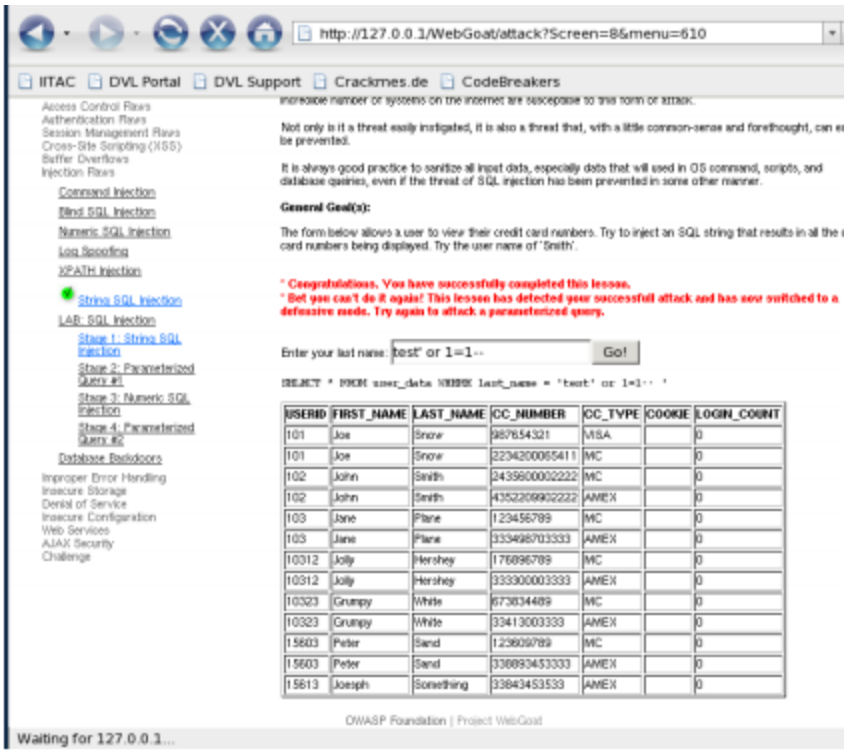




Lakukan pencarian sesuai dengan last name ,misalnya Smith atau user name Smith, smith Programmer. String SQL Injection, Tidak melakukan filter input yang masuk.



Lalu akan tampil gambar seperti di bawah ini. Awalnya akan menambahkan tanda petik dan akan membaca last name yang sudah dimasukkan tadi. 1=1 adalah **boolean true** walaupun salah maka masih akan bernilai true. Itu merupakan kesalahan dari program karna tidak memfilter terlebih dahulu.



- **Kesimpulan :**

Exploit Merupakan suatu aplikasi atau perangkat lunak yang bertujuan menyerang kerentanan mengenai rapuhnya keamanan atau security vurnerability, namun tidak bertujuan untuk melancarkan aksi yang tidak diinginkan atau suatu tindak kejahatan. Sedangkan WebGoat merupakan sebuah aplikasi berbasis web yangs engaja dibuat tidak aman dengan tujuan untuk mengajarkan pelatihan keamanan alikasi web, serta setelah itu dapat di Analisa dan di evaluasi sistem yang telah dibuat. Sehingga mengetahui dari evaluasi tersebut sejauh mana sistem tersebut aman dari segala jenis ancaman. Jika tidak melakukan evaluasi dapat terjadi suatu keteledoran sehingga dapat membiarkan sistem tersebut di bobol oleh pihak yan tidak bertanggung jawab dan dapat di salah gunakan, percobaan ini dimaksudkan agar dapat mempermudah melakukan pengujian dan pengevaluasian dari system yang telah dibuat.