Tugas 5 Keamanan Jaringan

Nama : Somame Morianus Daely
NIM : 09011281419058

Actual Exploit

Exploit adalah sebuah kode yang menyerang keamanan_komputer secara spesifik. Exploit banyak digunakan untuk penentrasi baik secara legal ataupun ilegal untuk mencari kelemahan (Vulnerability) pada komputer tujuan. Bisa juga dikatakan sebuah perangkat lunak yang menyerang kerapuhan keamanan (security vulnerability) yang spesifik namun tidak selalu bertujuan untuk melancarkan aksi yang tidak diinginkan. Banyak peneliti keamanan komputer menggunakan exploit untuk mendemonstrasikan bahwa suatu sistem memiliki kerapuhan.

Ada beberapa metode untuk mengklasifikasi exploit. Yang paling umum adalah dengan melihat cara exploit membuat kontak dengan perangkat lunak yang rentan. Remote exploit (eksploit jarak jauh) bekerja melalui jaringan dan mengeksploitasi celah keamanan tanpa adanya akses terlebih dahulu ke sistem korban. Local exploit (eksploit lokal) mengharuskan adanya akses terlebih dahulu ke sistem yang rentan dan biasanya meningkatkan keleluasaan orang yang menjalankan exploit melebihi yang diberikan oleh administrator sistem. Exploit yang menyerang aplikasi klien juga ada, biasanya terdiri dari server-server yang dimodifikasi yang mengirimkan exploit jika diakses dengan aplikasi klien. Exploit yang menyerang aplikasi klien juga mungkin memerlukan beberapa interaksi dengan pengguna, dengan demikian dapat digunakan dalam kombinasi dengan metode social engineering. Ini adalah cara hacker masuk ke komputer dan situs web untuk mencuri data.

Klasifikasi lain adalah dengan tindakan terhadap sistem korban: unauthorized akses data, eksekusi kode sewenang-wenang, penolakan layanan.

Banyak exploit dirancang untuk memberikan akses tingkat-"superuser" ke sistem komputer. Namun, namun mungkin juga menggunakan beberapa exploit, untuk mendapatkan akses tingkat rendah terlebih dahulu, kemudian meningkatkan hak akses berulang kali sampai mencapai root.

Biasanya exploit tunggal hanya dapat mengambil keuntungan dari satu celah keamanan software tertentu. Sering kali, setelah exploit diterbitkan, celah keamanan sistem diperbaiki melalui tambalan sehingga exploit tak berlaku lagi untuk perangkat lunak versi terbaru. Hal ini menjadi alasan mengapa beberapa blackhat hacker tidak mempublikasikan exploit mereka tetapi merahasiakannya untuk diri sendiri atau hacker lainnya. Exploit tersebut disebut sebagai 'exploit zero day' dan untuk mendapatkan akses ke exploit tersebut adalah keinginan utama dari penyerang-penyerang amatir, yang sering dijuluki script kiddie. Untuk melakukan exploit tools-tools yang biasa di gunakan yakni Hydr, Medusa, nmap, dan banyak tools lainnya.

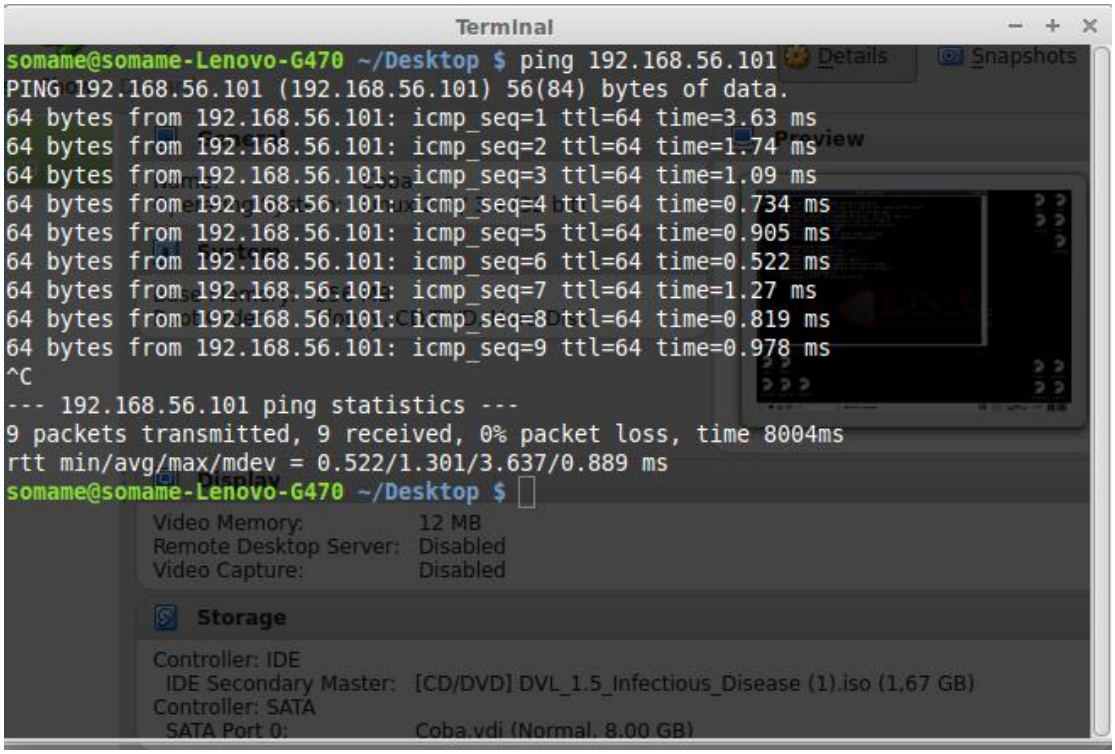
Tugas 5 Keamanan Jaringan

Pada percobaan ini ada 2 jenis ekxploit yang akan di lakukan yaitu menemukan password target dengan menggunakan tools hydra dan Webgoat SQL Injection pada target.

Untuk percobaan ini sistem operasi yang di gunakan adalah linux mint dan yang akan menjadi target adalah DVL. Sebelum Menyerang target hal pertama yang di ketahui adalah IP Address target. Untuk IP Address target dapat di lihat pada gambar di bawah ini.

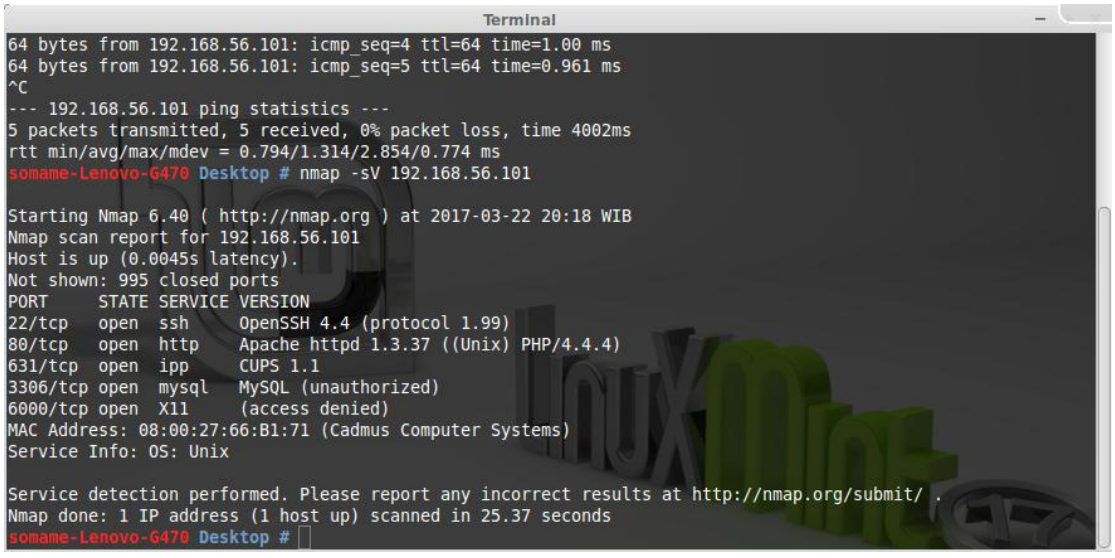
IP Address Target dalam hal ini DVL

Setelah itu kita harus mengecek apakah kita target kita sedang aktif dan apakah kita terhubung dengan target. Untuk itu kita akan melakukan perintah Ping ke IP Address target.



Ping ke IP Address target

Setelah mengetahui IP Address target, hal yang kita lakukan yaitu melihat service apa yang sedang berjalan pada sistem target. Kita gunakan tools nmap untuk melihat service yang sedang berjalan dengan perinta. Nmap -sV Ip target.



Melihat service yang sedang berjalan dengan menggunakan tools nmap

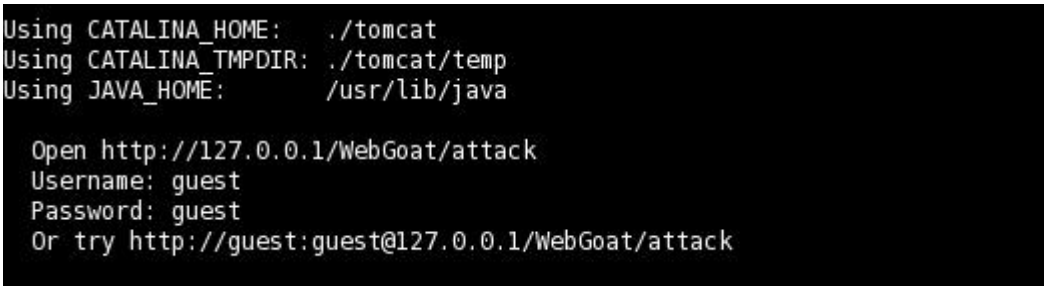
Dari gambar di atas dapat kita lihat service-service yang sedang berjalan yaitu ssh, http, mysql, dll. Selanjutnya kita akan melakukan bruteforce melalui service ssh dengan menggunakan tools hydra.

Tugas 5 Keamanan Jaringan

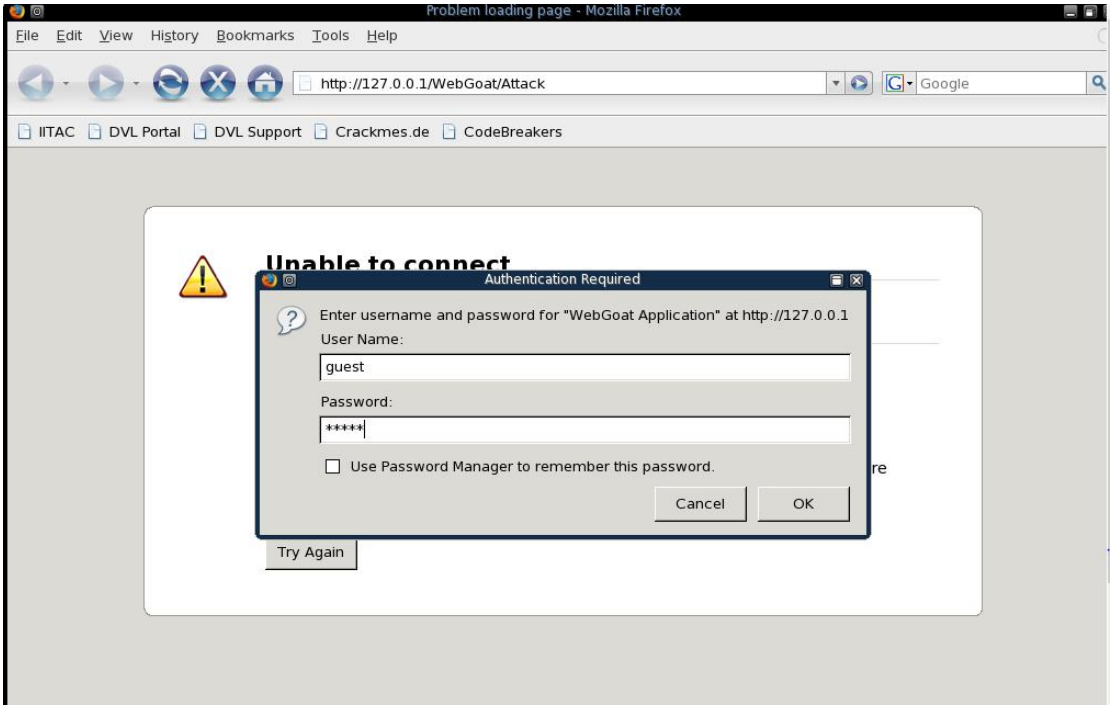
Untuk melakukan bruteforce kita memerlukan list password seluruh kemungkinan password yang di gunakan user. Dalam hal terdapat data password.list yang akan di gunakan. Perinta yang di lakukan yaitu;

Hydra -l –P password.list 192.168.100.10 ssh

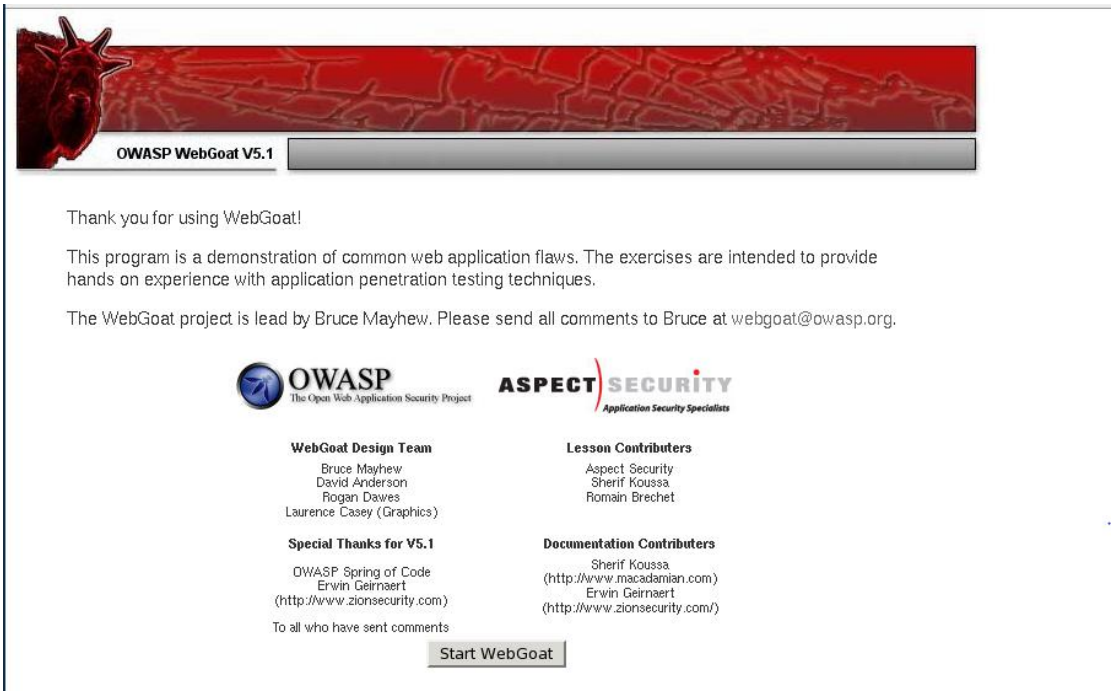
Menu Webgoat



Password dan Username webgoat



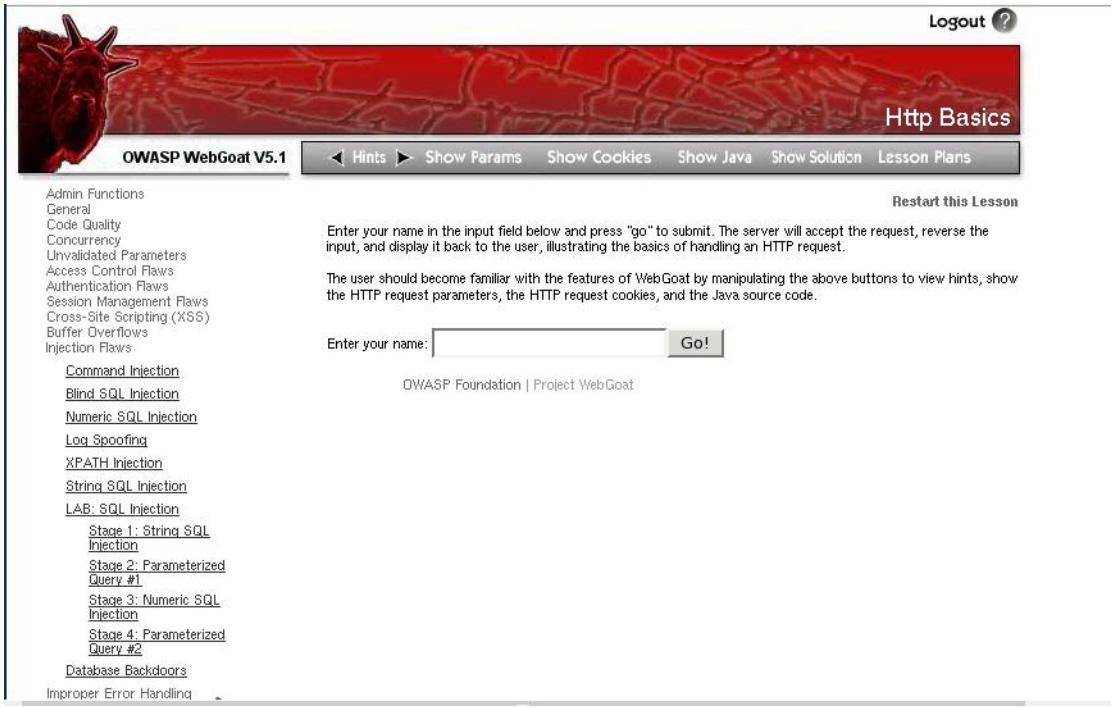
Login pada Webgoat



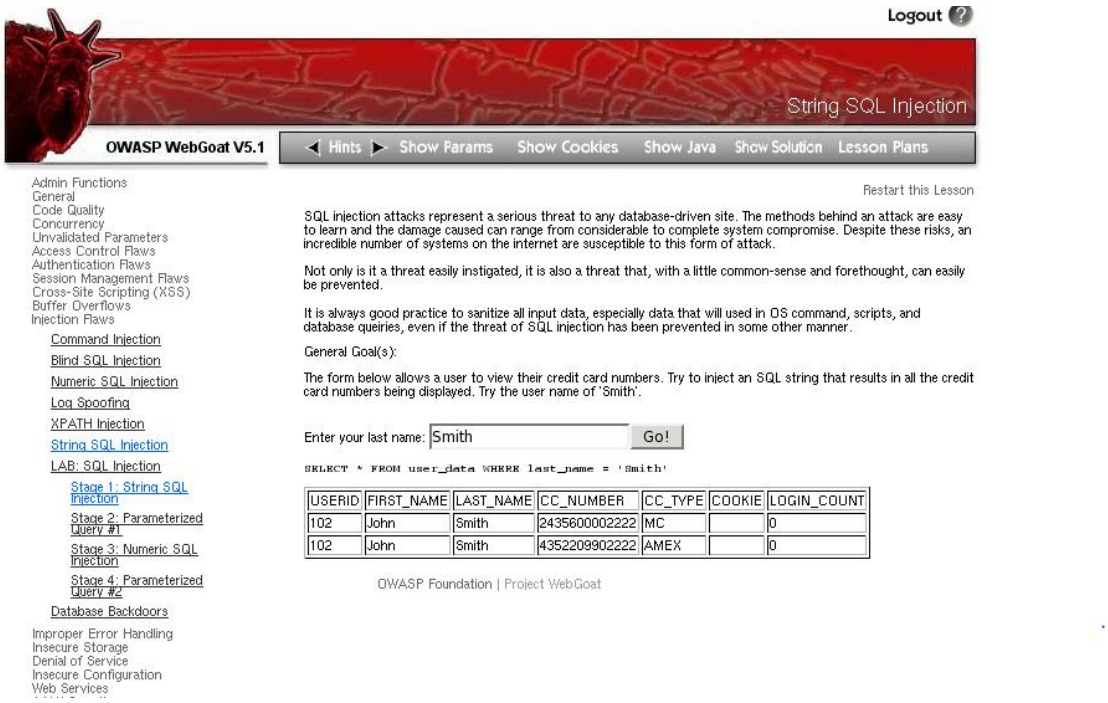
Tampilan Home Page webgoat

Selanjtunya kita memilih tombol start webgoat kemudian pilih menu Injection Flaws lalu pilih String SQL injetction.

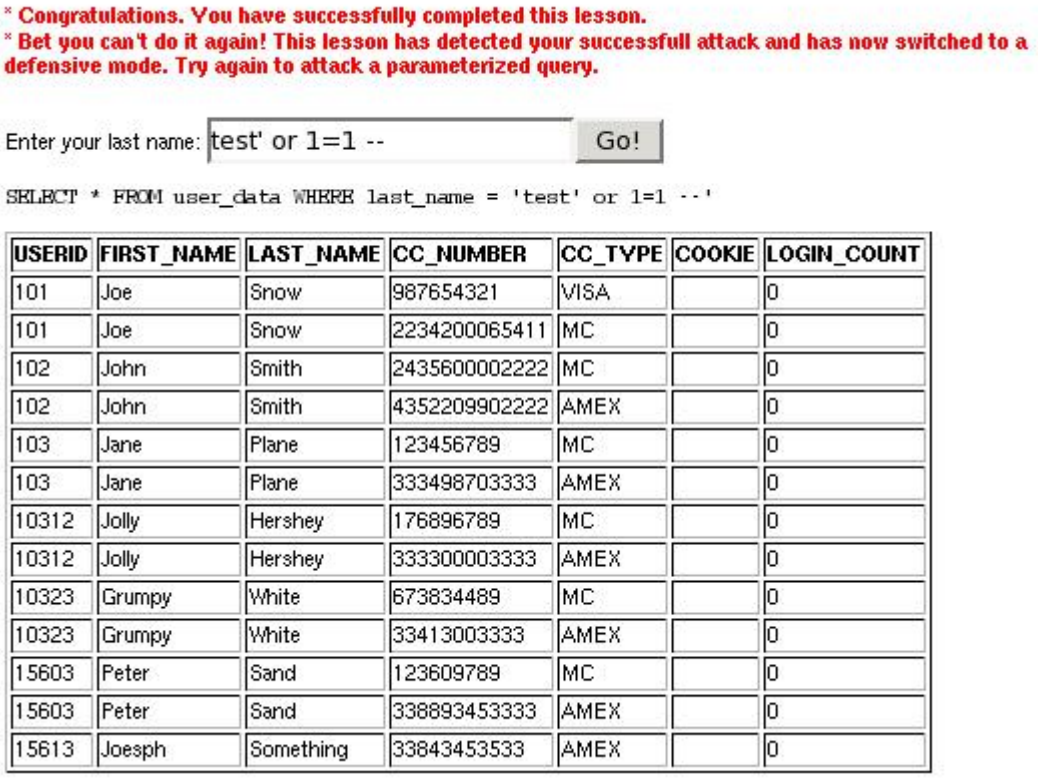
Tugas 5 Keamanan Jaringan



Tampilan Page String SQL Injection



Tampilan hasil pencarian nama smith



* 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

Hasil Penggunaan SQL injection

Analisa:

Dari praktikum kali ini tujuannya adalah untuk mengetahui kelemahan dari sistem yang akan menjadi target kita dan dengan mengetahui kelemahan-kelemahan itu kita dapat menutupi kelemahan itu. Kegiatan pertama yaitu mencari password dan username target. Kelemahan dari sistem ini adalah mudahnya password yang di gunakan oleh sistem. Penggunaan kombinasi karakter angka huruf dan simbol perlu di lakukan untuk membuat password lebih aman.

Hal kedua yang dilakukan yaitu Injection adalah untuk menampilkan seluruh data yang terdapat pada database sistem, ini terjadi karena lemahnya sistem sehingga terdapat celah pada program karena tidak melakukan filter terlebih dahulu terhadap inputan yang di berikan kepada sistem

Tugas 5 Keamanan Jaringan