PRAKTIKUM KEAMANAN INFORMASI DAN JARINGAN

PERTEMUAN 6

1. Apa itu Framework Metasploit ?

2. Modul Metasploit

3. Instalasi Metasploit di Kalilinux

4. Metasploit di Kalilinux

Pembahasan :

1. **Apa itu Framework Metasploit?**

   Metasploit Framework merupakan framework yang paling umum dipakai untuk menguji sebuah exploit. Mengapa dibutuhkan framework dalam membuat kode program exploit? Biasanya kode program exploit memiliki operasi yang umum seperti mengirim request HTTP, membuat server web sebagai pancingan bagi korban, dan sebagainya. Dengan adanya sebuah framework yang universal dan lengkap, tugas membuat kode program exploit menjadi lebih mudah. Selain itu, hal ini juga mempermudah pihak lain untuk menguji exploit yang telah ditulis dengan mudah.

   Berdasarkan situs resminya, Metasploit terdiri atas beberapa versi, yaitu **Framework**, **Community, Express, dan Pro**. Seluruh versi selain versi Framework memiliki interface berbasis web yang dapat dipakai dengan mudah. Dari seluruh versi yang ada, hanya versi Framework dan Community yang gratis. Selain itu, pengguna versi Community perlu melakukan registrasi terlebih dahulu. Versi Framework yang hanya menyediakan CLI (tampilan berbasis teks). Untuk menjalankannya, memilih menu Kali Linux, Exploitation Tools, Metasploit, metasploit framework.

2. **Modul Metasploit**

   Modul pada Metasploit dikategorikan menjadi **encoder, nop generator, exploit, payload**, dan **auxiliary**:

   a. Modul exploit mewakili sebuah celah keamanan yang akan diujikan. Celah keamanan ini memungkinkan penyerang untuk mengakses sistem yang diserang. Untuk itu dibutuhkan modul payload yang akan dikerjakan bila modul exploit berhasil menjalankan tugasnya, biasanya berupa shell.

   b. Modul auxiliary adalah sesuatu yang mirip seperti exploit tetapi tidak memiliki payload sehingga penyerang tidak dapat bermain-main dengan sistem sasaran secara leluasa (setidaknya untuk saat tersebut ;). Contohnya adalah operasi scanning, serangan yang

hanya melumpuhkan server, membuat server palsu atau melakukan password cracking secara offline.

c. Modul nop generator dan encoder dipakai untuk mengelabui sistem pertahanan milik sasaran (seperti antivirus dan IDS/IPS) sehingga sasaran tidak mengetahui bahwa dirinya sedang diserang.

3. Instalasi Metasploit di Kalilinux

Langkah-langkah dalam intalasi dan konfigurasi kalilinux, sebagai berikut :

a. Yaitu dengan menjalankan servcie postgresql dan service metasploit seperti di bawah ini :

service metasploit start

```
kali@kali:~$ service postgresql start
bash: service: command not found
kali@kali:~$ sudo su
root@kali:/home/kali#
```

Jika muncul peringatan diatas, maka harus terlebih dahulu masuk ke root@kali. Dengan perintah sudo su.

Pesan error di atas sudah menjelaskan bahwa: Gagal untuk memulai metasploit.service: Unit metasploit.service gagal di buka: tidak ada file atau direktori.

b. Seperti yang di jelaskan pada website www.kali.org, karena terdapat perubahan dalam paket metasploit-framework yang ada di dalam Kali Linux 2.0. ada beberapa perubahan kecil dalam cara memulai Metasploit di Kali Linux 2.0. nah di bawah ini saya berikan cara untuk menjalankan Metasploit di Kali 2.0, sebagai berikut :

Pertama ketikkan

/etc/init.d/postgresql start

/etc/init.d/postgresql start

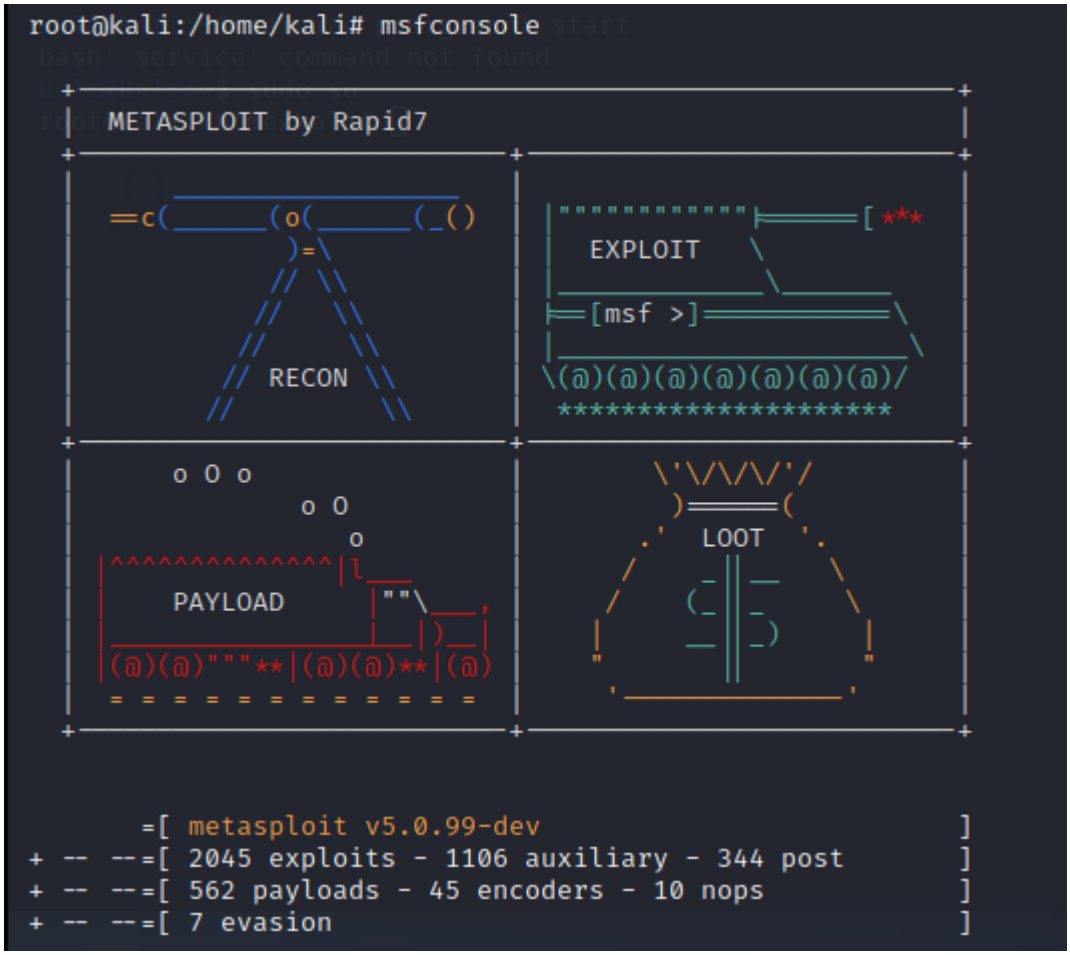
```
File  Actions  Edit  View  Help

root@kali:/home/kali# /etc/init.d/postgresql start
Starting postgresql (via systemctl): postgresql.service.
```

Perintah diatas adalah untuk menjalankan postgresql server

c. Perintah diatas digunakan untuk menginisialisai database metasploit framework. perintah ini cukup diketikkan ketika pertama kali kita menjalankan metasploit. msfdb init

```
root@kali:/home/kali# msfdb init
[i] Database already started
[+] Creating database user 'msf'
[+] Creating databases 'msf'
[+] Creating databases 'msf_test'
[+] Creating configuration file '/usr/share/metasploit-framework/config/database.yml'
[+] Creating initial database schema
```

d. Selanjutnya tinggal jalankan metasploit console : ketik : msfconsole



msfconsole terbuka tanpa error apapun, untuk mengecek status database gunakan perintah berikut

db_status

poststgresql connectec to msf

```
msf5 > db_status
[*] Connected to msf. Connection type: postgresql.
msf5 >
```

4. Contoh penggunaan metasploit untuk melakukan ip / port scanner.
Berikut langkah-langkah dalam melakukan ip / port scanner menggunakan metasploit :

a. Untuk melihat seluruh modul yang ada, saya dapat memberikan perintah **show all** seperti:

```
msf5 > show all
Encoders
========

   #   Name                          Disclosure Date  Rank    Check  Description
   -   ----                          ---------------  ----    -----  -----------
   0   cmd/brace                                      manual  No     Bash Brace Expansion Comma
nd Encoder
   1   cmd/echo                                       manual  No     Echo Command Encoder
   2   cmd/generic_sh                                 manual  No     Generic Shell Variable Sub
stitution Command Encoder
   3   cmd/ifs                                        manual  No     Bourne ${IFS} Substitution
 Command Encoder
   4   cmd/perl                                       manual  No     Perl Command Encoder
   5   cmd/powershell_base64                          manual  No     Powershell Base64 Command
Encoder
   6   cmd/printf_php_mq                              manual  No     printf(1) via PHP magic_qu
otes Utility Command Encoder
   7   generic/eicar                                  manual  No     The EICAR Encoder
   8   generic/none                                   manual  No     The "none" Encoder
   9   mipsbe/byte_xori                               manual  No     Byte XORi Encoder
   10  mipsbe/longxor                                 manual  No     XOR Encoder
   11  mipsle/byte_xori                               manual  No     Byte XORi Encoder
   12  mipsle/longxor                                 manual  No     XOR Encoder
   13  php/base64                                     manual  No     PHP Base64 Encoder
   14  ppc/longxor                                    manual  No     PPC LongXOR Encoder
   15  ppc/longxor_tag                                manual  No     PPC LongXOR Encoder
   16  ruby/base64                                    manual  No     Ruby Base64 Encoder
```

```
[*] Available Framework plugins:
    * aggregator
    * alias
    * auto_add_route
    * beholder
    * db_credcollect
    * db_tracker
    * event_tester
    * ffautoregen
    * ips_filter
    * lab
    * libnotify
    * msfd
    * msgrpc
    * nessus
    * nexpose
    * openvas
    * pcap_log
    * request
    * rssfeed
    * sample
    * session_notifier
    * session_tagger
    * socket_logger
    * sounds
    * sqlmap
    * thread
    * token_adduser
    * token_hunter
    * wiki
```