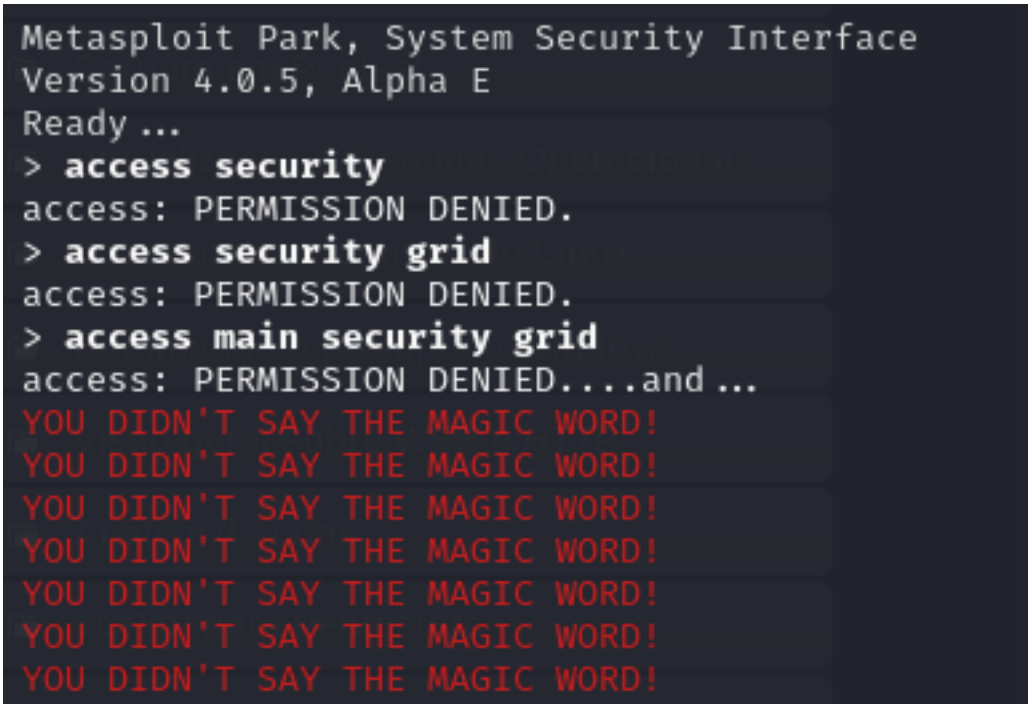
Módulos Auxiliares

+ Se ficarmos dando o comando banner, ele vai exibir sempre novos banners



+ Funciona basicamente igual nosso terminal linux

+ Se dermos o

```
show -h
```

Ele mostra os encoders, os payloads, os módulos de exploração etc

+ Para visualizar todos os módulos auxiliares,

```
show auxiliary
```

+ Para usar algum módulo, vamos usar o use
+ Ao usarmos use auxiliary/ e dermos um tab duplo, ele vai nos mostrar as outras opções.
+ No caso, se quisermos um portscan, fazemos

```
use auxiliary/scanner/portscan + tab tab
```

```
msf6 > use auxiliary/scanner/portscan/
use auxiliary/scanner/portscan/ack        use auxiliary/scanner/portscan/syn        use auxiliary/scanner/portscan/xmas
use auxiliary/scanner/portscan/ftpbounce  use auxiliary/scanner/portscan/tcp
```

+ Quando ele ficar vermelho é por que iniciou o módulo

```
msf6 > use auxiliary/scanner/portscan/tcp
msf6 auxiliary(scanner/portscan/tcp) >
```

+ Pra visualizar, podemos dar um info
+ Para ver as opções, show options

```
msf6 auxiliary(scanner/portscan/tcp) > info

       Name: TCP Port Scanner
     Module: auxiliary/scanner/portscan/tcp
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  hdm <x@hdm.io>
  kris katterjohn <katterjohn@gmail.com>

Check supported:
  No

Basic options:
  Name         Current Setting  Required  Description
  ----         ---------------  --------  -----------
  CONCURRENCY  10               yes       The number of concurrent p
  DELAY        0                yes       The delay between connecti
  JITTER       0                yes       The delay jitter factor (m
  PORTS        1-10000          yes       Ports to scan (e.g. 22-25,
  RHOSTS                        yes       The target host(s), see ht
  THREADS      1                yes       The number of concurrent t
  TIMEOUT      1000             yes       The socket connect timeout

Description:
  Enumerate open TCP services by performing a full TCP connect on ea
  This does not need administrative privileges on the source machine
  may be useful if pivoting.


View the full module info with the info -d command.

msf6 auxiliary(scanner/portscan/tcp) > show options

Module options (auxiliary/scanner/portscan/tcp):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   CONCURRENCY  10               yes       The number of concurrent
```

+ Para setar um endereço de IP nesse RHOSTS é muito simples:

```
set RHOSTS 172.16.1.7
```

+ Pra que o script comece a rodar, adivinha:

```
run
```

+ Para ver tudo o que ele pode buscar, executamos

```
search -h
```

+ Podemos fazer uma pesquisa do seguinte tipo:

```
search type:auxiliary smnp
```
ou rdp, ou smp, ou portscan e assim vai

+ Poderíamos também fazer a busca por exploits ao invés de módulos auxiliares

```
search type:exploits smnp
```

+ Com o comando back, a gente volta.