



Laboratorio 3.1

Contraseñas

Ing. Alex Araya Rojas, MT
CISSP, CISM

Enero 2022

Lab 3.1

Contraseñas

01

Descargar el instalador

02

Proceso de instalación

03

Utilización de la herramienta



Procedimiento

Descargar el instalador

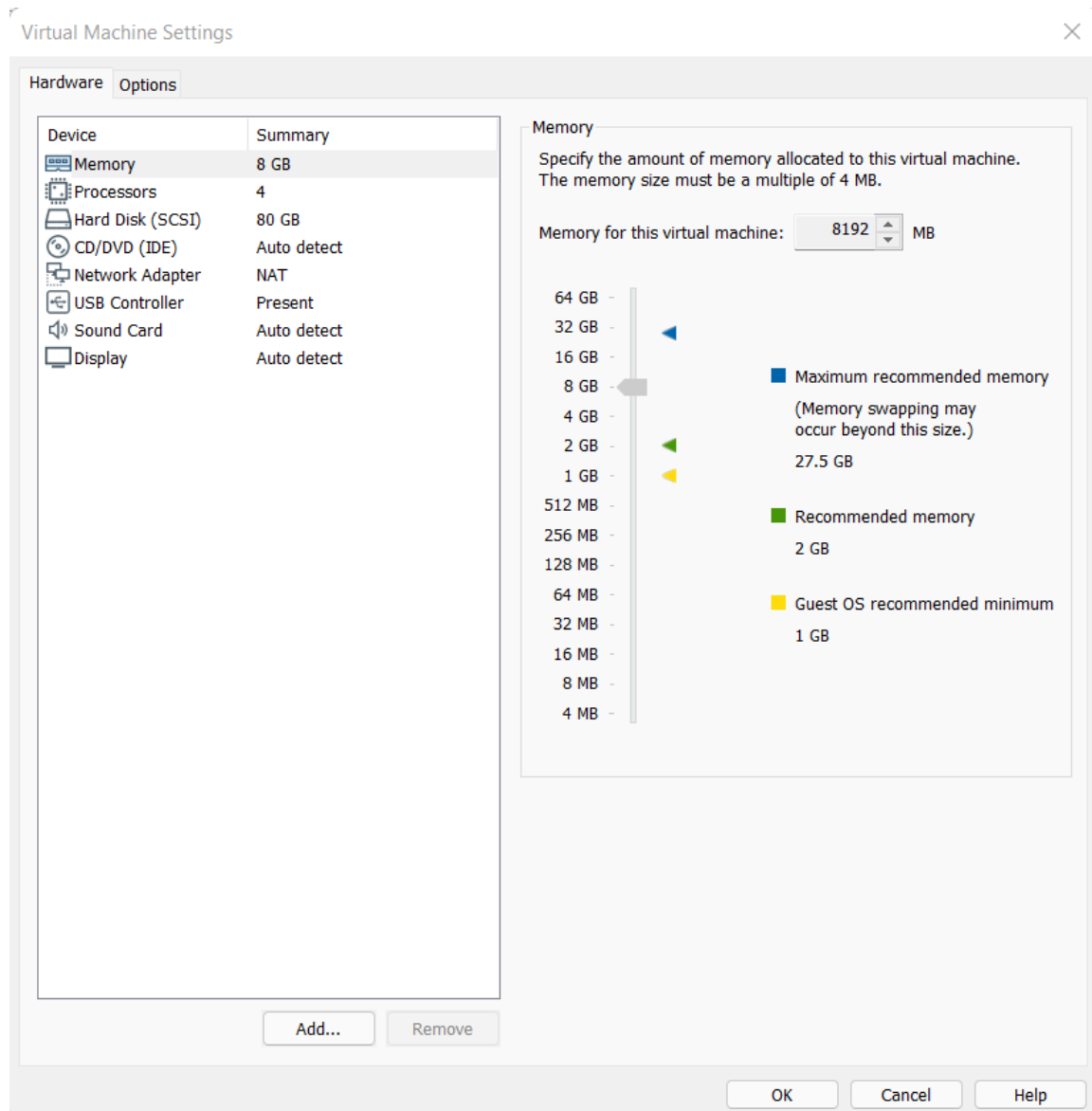
01. Es recomendable que realice estas pruebas en un equipo virtual para no comprometer la seguridad de su equipo de cómputo.
02. Descargue la ultima versión de Kali Linux, al momento de la liberación de este laboratorio es la 2021.4a. Este archivo es un archivo que pesa aprox. 2,5 GB (<https://kali.download/virtual-images/kali-2021.4a/kali-linux-2021.4a-vmware-amd64.7z>)
03. Requerimos también un equipo con Windows 10, puede conseguirlo en la siguiente url: <https://www.microsoft.com/es-es/software-download/windows10>
Este archivo lo utilizaremos para el Laboratorio 3.2 pero puede irlo descargando para ganar tiempo.
04. Sino cuenta con el software para instalar máquinas virtuales, puede descargar VMware Player en la carpeta de herramientas del Teams del curso Forense.

Proceso de instalación

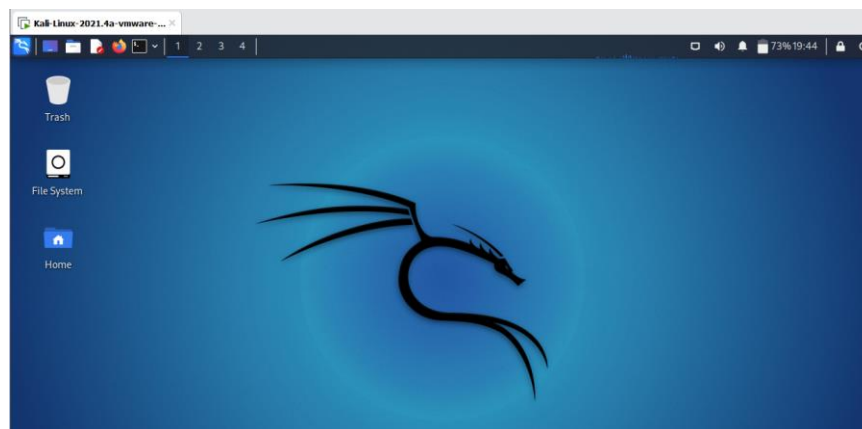
01. Para este laboratorio es necesario contar con un virtualizador instalado, si tiene problemas en para lograrlo, puede esperar a las sesiones semanales para apoyarle en el proceso o buscar tutoriales de VMware Player.
02. Vamos a trabajar en el aprovisionamiento de la máquina virtual con Linux Kali.
03. Descomprima el archivo descargado en la ubicación en donde se ejecutará el Kali Linux.
04. En VMware player, siga los siguientes pasos:
05. Haga clic en abrir y busque el archivo dentro de la carpeta que recientemente acaba de descomprimir.

Name	Date modified	Type	Size
 Kali-Linux-2021.4a-vmware-amd64.vmx.7z	4/2/2022 18:29	File folder	
 Kali-Linux-2021.4a-vmware-amd64	20/1/2022 15:14	VMware virtual machine...	4 KB

06. Configure los parámetros de la máquina virtual para que queden iguales a los siguientes, especialmente el valor de la tarjeta de red que debe estar en modo NAT. Si no cumple con la memoria RAM o CPU no hay problema.

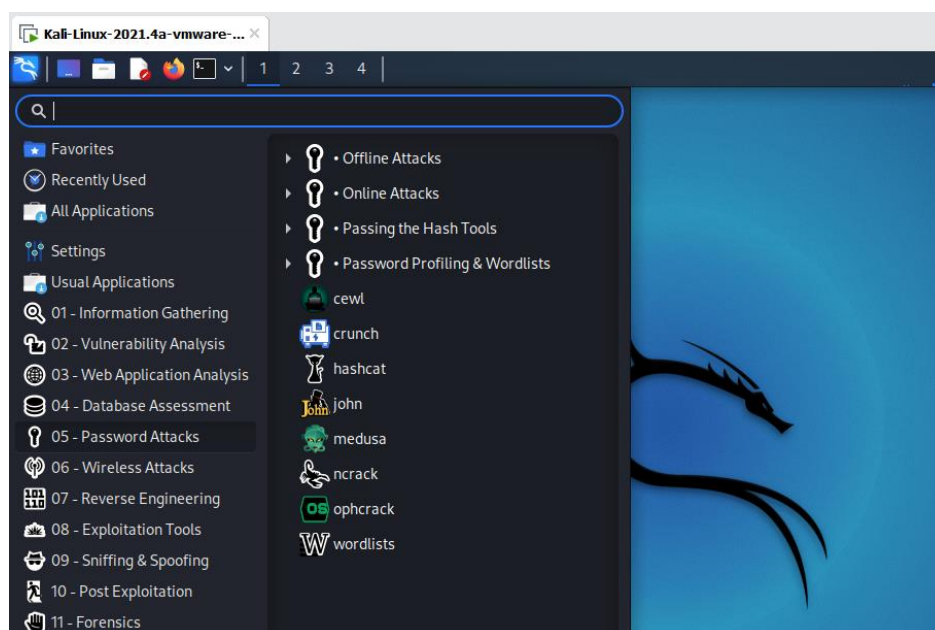


07. Inicie la máquina virtual de Kali Linux y deberá verse similar a esta imagen:

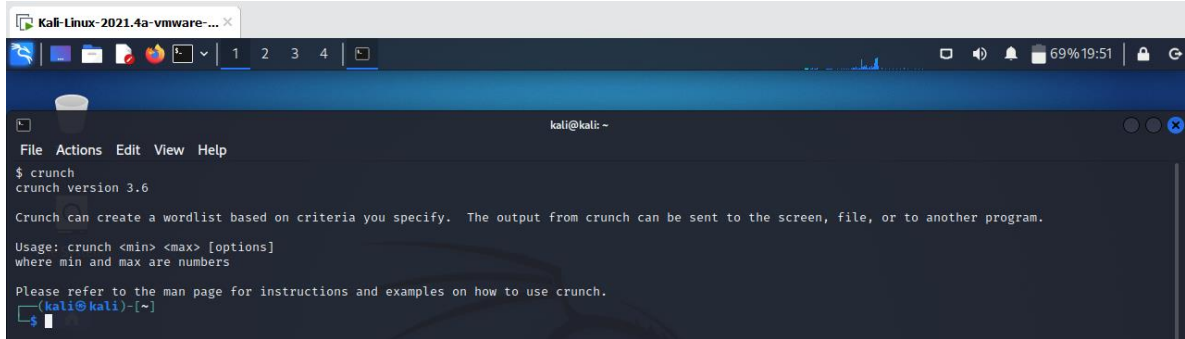


Utilización de la herramienta

01. Uno de los pasos más importantes a la hora de tratar de dar con una contraseña, es tener la capacidad de generar tus propios archivos que serán utilizados para ir probando opciones contra el servicio que intentaremos romper.
02. Para este laboratorio, utilizaremos una herramienta que viene instalada en Kali Linux llamada “Crunch”
03. Abra un terminal en Kali Linux y digite Crunch o busque la herramienta en el menú de Kali Linux.

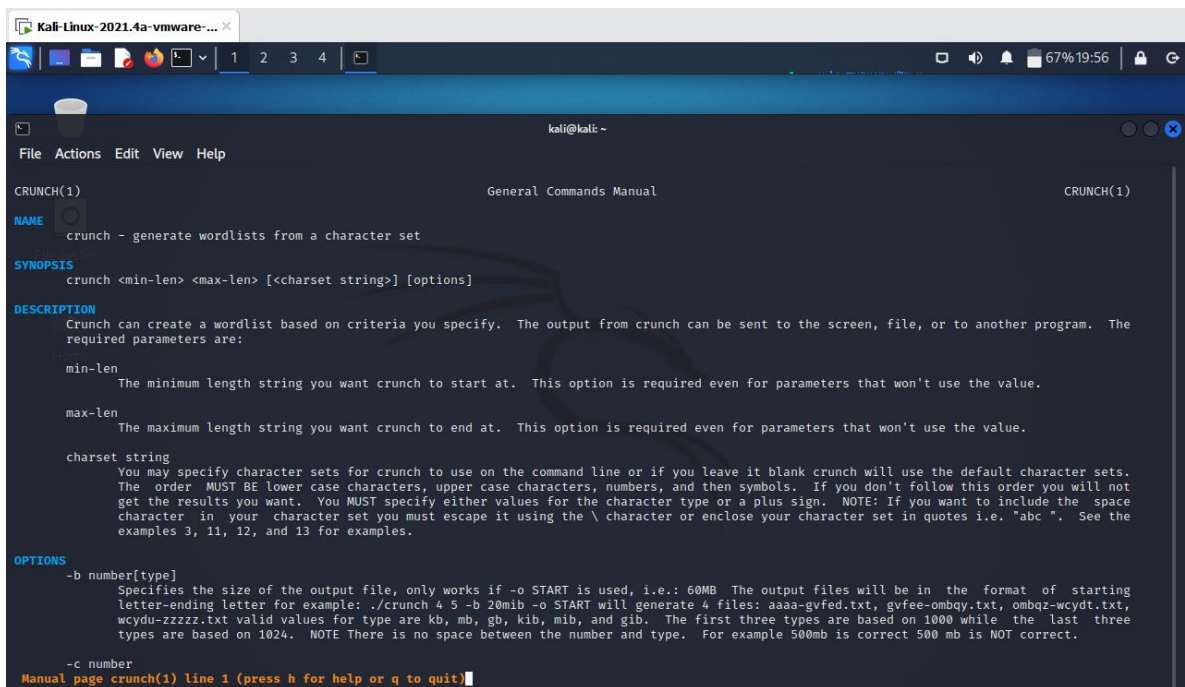


04. Deberá ver algo similar a esta imagen:



```
Kali-Linux-2021.4a-vmware-...  
kali@kali: ~  
$ crunch  
crunch version 3.6  
  
Crunch can create a wordlist based on criteria you specify. The output from crunch can be sent to the screen, file, or to another program.  
  
Usage: crunch <min> <max> [options]  
where min and max are numbers  
  
Please refer to the man page for instructions and examples on how to use crunch.  
(kali@kali)~  
$
```

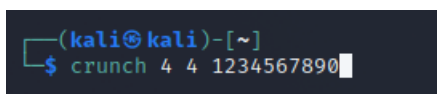
05. Puede utilizar el comando “man crunch” para ver toda la lista de opciones y descripciones del comando.



```
Kali-Linux-2021.4a-vmware-...  
kali@kali: ~  
$ man crunch  
CRUNCH(1)                                General Commands Manual                                CRUNCH(1)  
  
NAME  
crunch - generate wordlists from a character set  
  
SYNOPSIS  
crunch <min-len> <max-len> [<charset string>] [options]  
  
DESCRIPTION  
Crunch can create a wordlist based on criteria you specify. The output from crunch can be sent to the screen, file, or to another program. The required parameters are:  
  
min-len  
The minimum length string you want crunch to start at. This option is required even for parameters that won't use the value.  
  
max-len  
The maximum length string you want crunch to end at. This option is required even for parameters that won't use the value.  
  
charset string  
You may specify character sets for crunch to use on the command line or if you leave it blank crunch will use the default character sets. The order MUST BE lower case characters, upper case characters, numbers, and then symbols. If you don't follow this order you will not get the results you want. You MUST specify either values for the character type or a plus sign. NOTE: If you want to include the space character in your character set you must escape it using the \ character or enclose your character set in quotes i.e. "abc ". See the examples 3, 11, 12, and 13 for examples.  
  
OPTIONS  
-b number[type]  
Specifies the size of the output file, only works if -o START is used, i.e.: 60MB. The output files will be in the format of starting letter-ending letter for example: ./crunch 4 5 -b 20mib -o START will generate 4 files: aaaa-gvfed.txt, gvfee-ombqy.txt, ombqz-wcydt.txt, wcydu-zzzzz.txt valid values for type are kb, mb, gb, kib, mib, and gib. The first three types are based on 1000 while the last three types are based on 1024. NOTE There is no space between the number and type. For example 500mb is correct 500 mb is NOT correct.  
  
-c number  
Manual page crunch(1) line 1 (press h for help or q to quit)
```

06. Vamos a generar un listado de contraseñas numéricas, incluyendo dígitos del 0 al 9 y con una longitud de 4 caracteres, por ejemplo los pines de una tarjeta de crédito.

07. Escriba el siguiente comando: “Crunch 4 4 1234567890”



```
(kali@kali)~  
$ crunch 4 4 1234567890
```

08. El resultado será visible en pantalla solamente, si desea que dicho resultado se almacene en un archivo de texto para ser utilizado posteriormente, puede escribir el siguiente comando:

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ crunch 4 4 1234567890 -o /home/kali/archivo.txt  
Crunch will now generate the following amount of data: 50000 bytes  
0 MB  
0 GB  
0 TB  
0 PB  
Crunch will now generate the following number of lines: 10000  
crunch: 100% completed generating output  
  
(kali@kali)-[~]  
$ ls  
archivo.txt Desktop Downloads FDL Pictures scipag_vulscan Videos  
bCAuosaa.jpeg Documents faraday-server_amd64.deb Music Public Templates ysoserial-0.0.6-SNAPSHOT-BETA-all.jar  
  
(kali@kali)-[~]  
$
```

09. Genere un listado (no guarde el archivo!!!) de contraseñas de 3 a 6 caracteres de longitud, utilizando los caracteres: “123abc”

```
(kali@kali)-[~]  
$ crunch 3 6 123abc  
Crunch will now generate the following amount of data: 380592 bytes  
0 MB  
0 GB  
0 TB  
0 PB
```

10. Podemos generar las contraseñas siguiendo un patrón específico, por ejemplo generar una contraseña de 6 dígitos, en las cuales se tengan 3 números, 1 carácter especial y 2 caracteres.

```
(kali@kali)-[~]  
$ crunch 6 6 -t %%%^@00
```

11. Como parte de su prueba de realización del laboratorio, arme los siguientes escenarios:

12. Genere un listado de archivos que combine mayúsculas y minúsculas más números, con una longitud de 8 caracteres.

13. Investigue opciones adicionales de esta herramienta.