ANÁLISIS FORENSE

Unidad 1. Actividad 4

20 DE NOVIEMBRE DE 2023

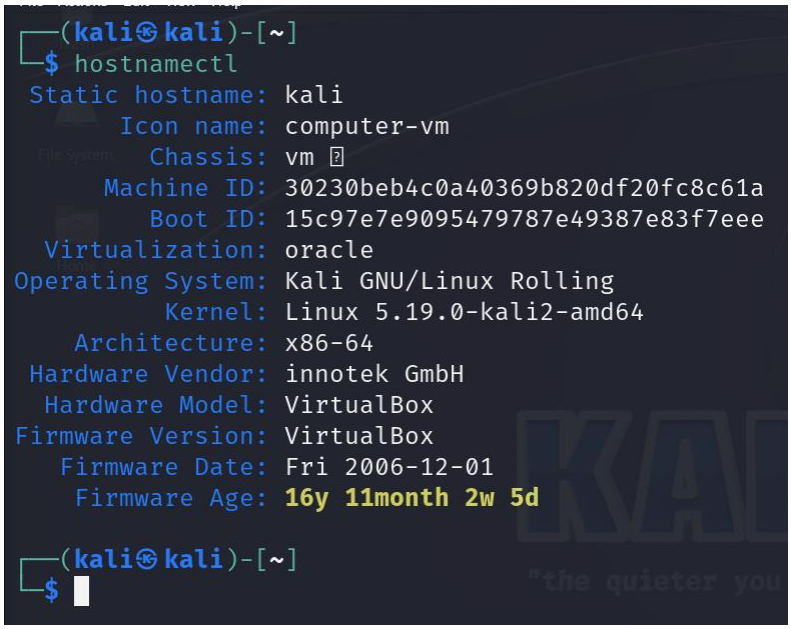
CARLOS DÍAZ MONTES
ESPECIALIZACIÓN DE CIBERSEGURIDAD

Índice

Ejercicios

Caso 1

1. ¿Cuál es el nombre del equipo?



2. El usuario tenía establecida una conexión FTP con un organismo público. ¿Cuál es?

3. Hay por lo menos un proceso que contiene malware. ¿Cuál es su nombre y su PID? Deberás justificar que está infectado.

4. Hay un proceso infectado que tiene establecida una conexión HTTPS. ¿Cuál es la dirección IP a la que está conectado? Deberás justificar que es un proceso infectado.

5. Hay una contraseña de un fichero comprimido escrita en el bloc de notas. ¿Cuál es?

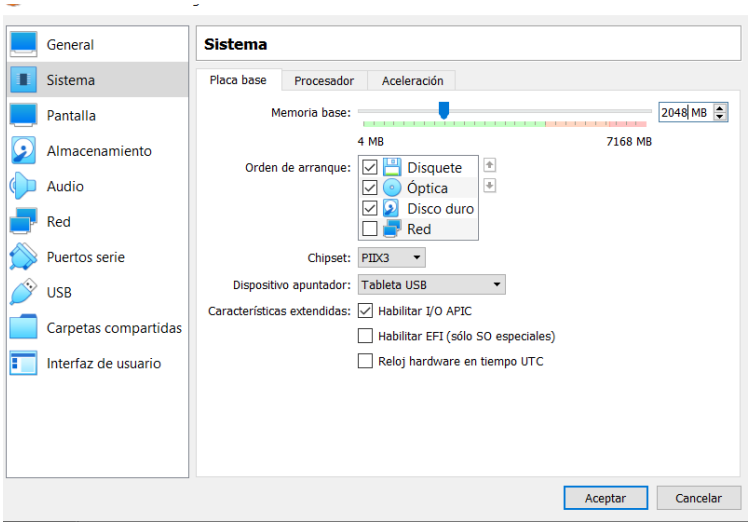
6. Existe un fichero ZIP accesible en la memoria RAM. ¿Qué animal se encuentra dentro?

Caso 2.

Crea una máquina virtual Windows 7. Durante el proceso de instalación de Windows es recomendable que le des bastantes recursos para que vaya más rápido.

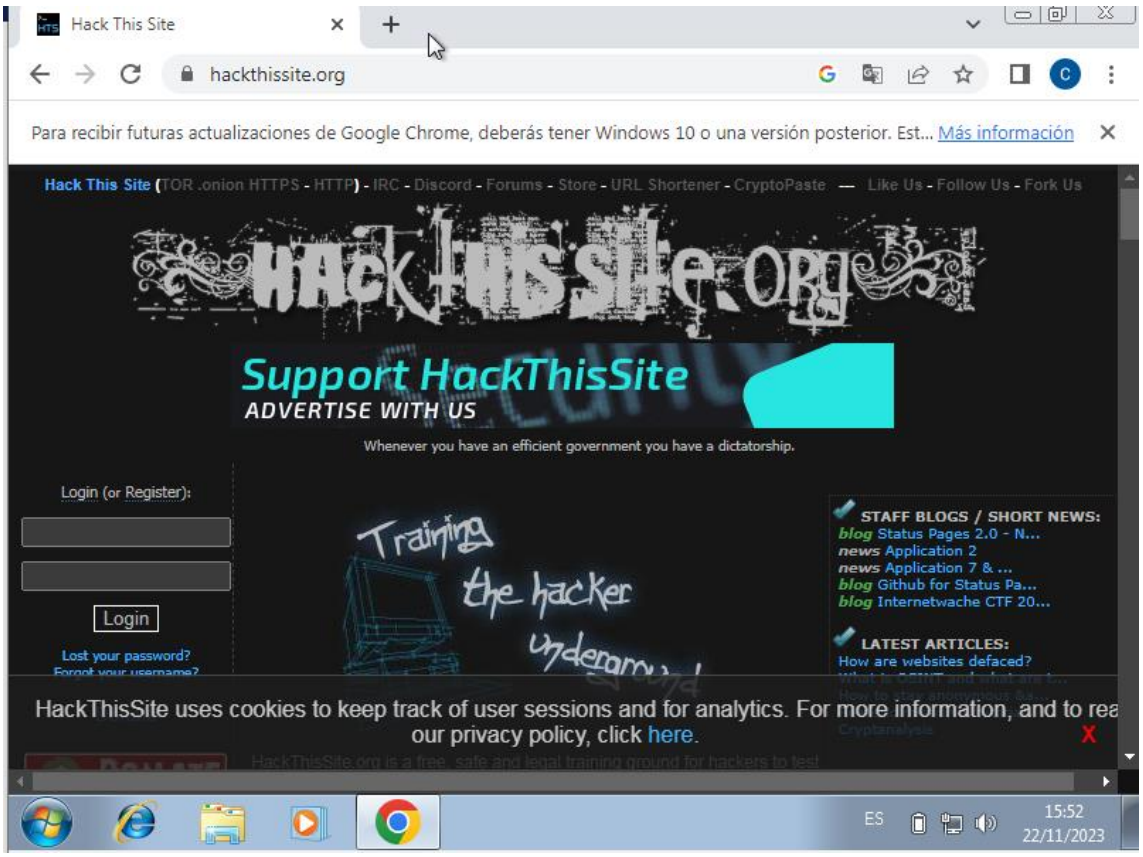
2. Para la máquina. Asígnale una cantidad no muy grande de RAM (<= 2GB). Vuelve a arrancarla.

Le ponemos 2048:



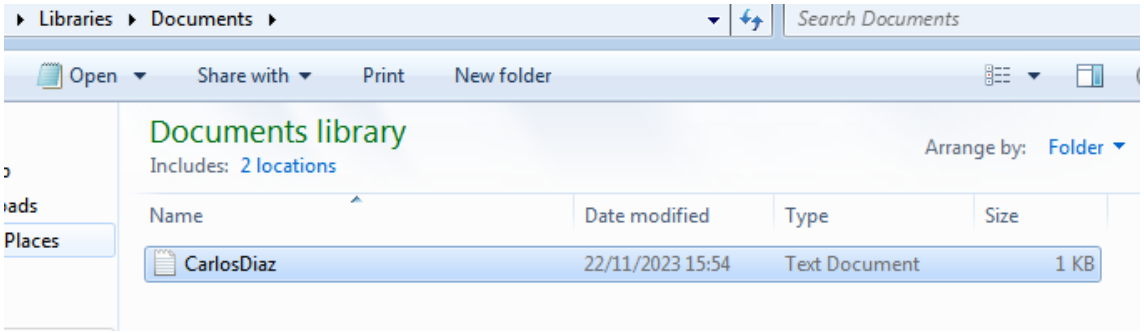
3. Abre un navegador web y conecta con una página relacionada con hacking.

Nos conectamos a la pagina web hack this site:

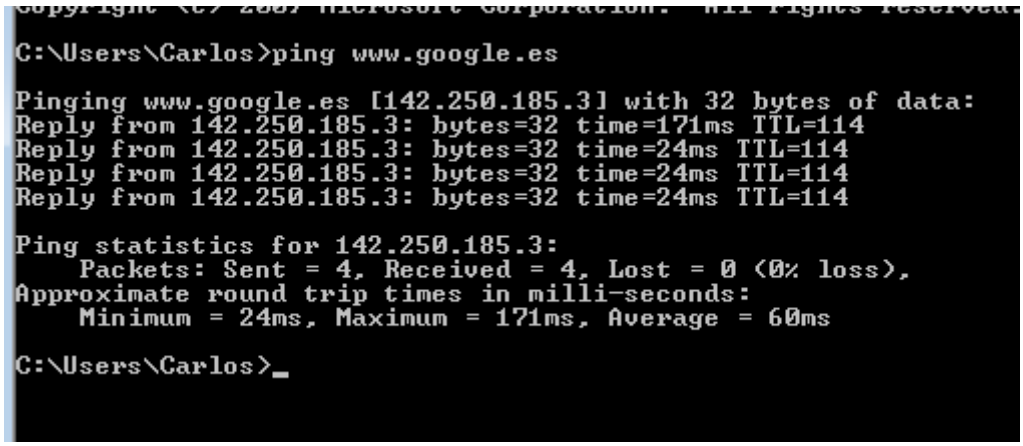


4. Abre un bloc de notas y escribe un mensaje. Guarda el fichero en la carpeta de documentos.

Me creo un documento con mi nombre:

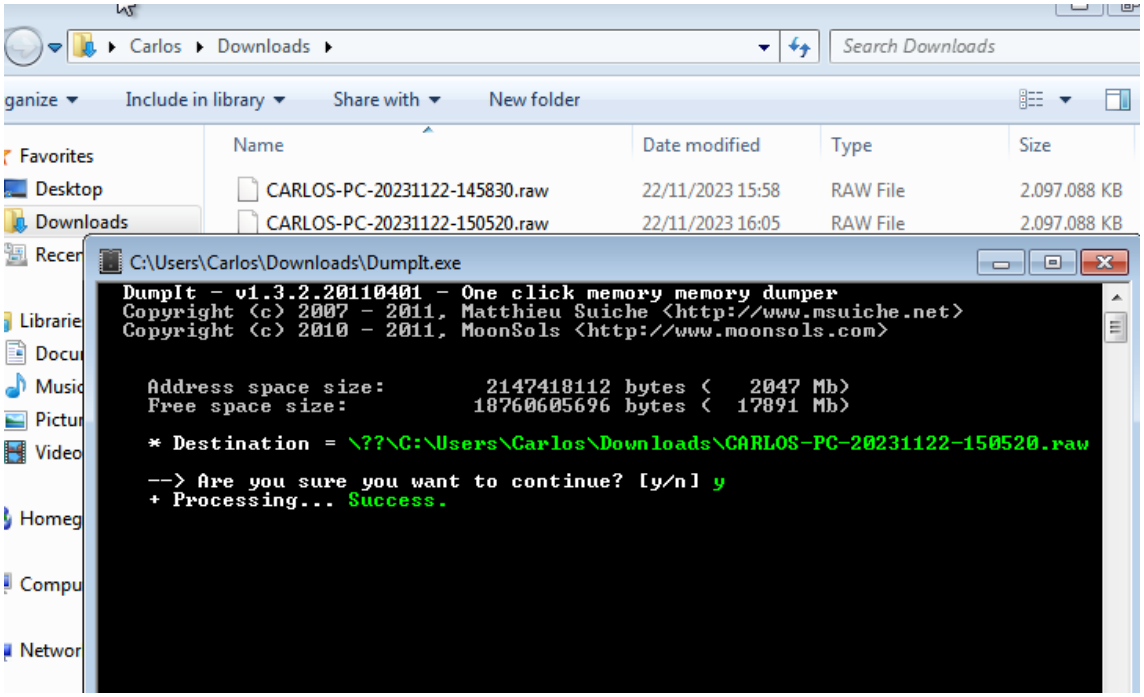


5. Abre una consola y haz ping a www.google.es.



6. Sin cerrar el navegador ni el bloc ni la consola, realiza una adquisición de memoria de la máquina mediante una herramienta como DumpIt o similar.

Nos descargamos Dumplt y una vez lo ejecutamos podemos encontrar un raw:



7. Con Volatility, comprueba que encuentras los procesos del Bloc de Notas, el navegador Web y la consola.

El de la consola:

```
┌──(kali㉿kali)-[~/volatility]
└─$ python2.7 vol.py -f CARLOS-PC-20231122-150520.raw --profile=Win7SP1x64 pslist | grep cmd.exe
Volatility Foundation Volatility Framework 2.6.1
0xfffffa8001b66060 cmd.exe                748   1924      1       19      1      0 2023-11-22 14:54:33 UTC+000
0
```

Los del navegador:

```
┌──(kali㉿kali)-[~/volatility]
└─$ python2.7 vol.py -f CARLOS-PC-20231122-150520.raw --profile=Win7SP1x64 pslist | grep chrome
Volatility Foundation Volatility Framework 2.6.1
0xfffffa8003aed630 chrome.exe            2840   1924     32     1264      1      0 2023-11-22 14:51:05 UTC+000
0
0xfffffa800371b450 chrome.exe             360   2840      8      110      1      0 2023-11-22 14:51:05 UTC+000
0
```

8. Comprueba si puedes averiguar el comando que se estaba ejecutando en la consola.

```
┌──(kali㉿kali)-[~/volatility]
└─$ python2.7 vol.py -f CARLOS-PC-20231122-150520.raw --profile=Win7SP1×64 cmdscan
Volatility Foundation Volatility Framework 2.6.1
**************************************************
CommandProcess: conhost.exe Pid: 2876
CommandHistory: 0×351740 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 1 LastAdded: 0 LastDisplayed: 0
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0×10
Cmd #0 @ 0×34e5c0: ping www.google.es
Cmd #15 @ 0×2f0158: 5
Cmd #16 @ 0×350960: 5
**************************************************
CommandProcess: conhost.exe Pid: 3968
CommandHistory: 0×2f2650 Application: DumpIt.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0×64
Cmd #15 @ 0×290158: /
Cmd #16 @ 0×2f1950: /
```

9. Comprueba si puedes averiguar el texto que estaba en el bloc de notas.

Primero confirmamos que existe el documento:

```
┌──(kali㉿kali)-[~/volatility]
└─$ python2.7 vol.py -f CARLOS-PC-20231122-150520.raw --profile=Win7SP1×64 filescan | grep "CarlosDiaz"
Volatility Foundation Volatility Framework 2.6.1
0×000000007fd26b80     16      0 RW-r-- \Device\HarddiskVolume2\Users\Carlos\Documents\CarlosDiaz.txt
```

Ahora miramos el contenido del documento:

10. Comprueba que encuentras la conexión de red a la página de hacking y la conexión del ping.