DÍA D - EJERCICIO FINAL - CTF ANÁLISIS DE MALWARE

Prerrequisitos

Accede a la plataforma: https://tryhackme.com

Una vez identificado en tu cuenta, utiliza el buscador y escribe: "Malware Introductory".

Selecciona el CTF y accede al contenido.

Escenario

El malware es un tema muy frecuente dentro de la ciberseguridad y, lamentablemente, también un elemento recurrente en las noticias a nivel mundial en la

actualidad.

El análisis de malware no solo es una forma de respuesta ante incidentes, sino que también resulta útil para comprender cómo los comportamientos de las

distintas variantes de malware dan lugar a su correspondiente categorización. Esta sala será una introducción práctica a las técnicas y herramientas

utilizadas en el análisis de malware; aunque breve, espero poder ampliar estas técnicas en mayor profundidad en el futuro.

Al analizar malware, es importante tener en cuenta lo siguiente:

Punto de entrada (PoE): Es decir, ¿fue a través de correo no deseado que nuestro filtrado de e-mail no detectó y el usuario abrió el archivo adjunto?

¡Revisemos nuestros filtros de spam y formemos mejor a nuestros usuarios para futuras medidas de prevención!

Indicadores de ejecución: ¿Cuáles son los indicios de que el malware siquiera se ha ejecutado en una máquina? ¿Hay archivos, procesos o quizás algún

intento de comunicación “no ordinaria”?

Comportamiento del malware: ¿Cómo actúa el malware? ¿Intenta infectar otros dispositivos? ¿Cifra archivos o instala algo como una puerta trasera /

herramienta de acceso remoto (RAT)?

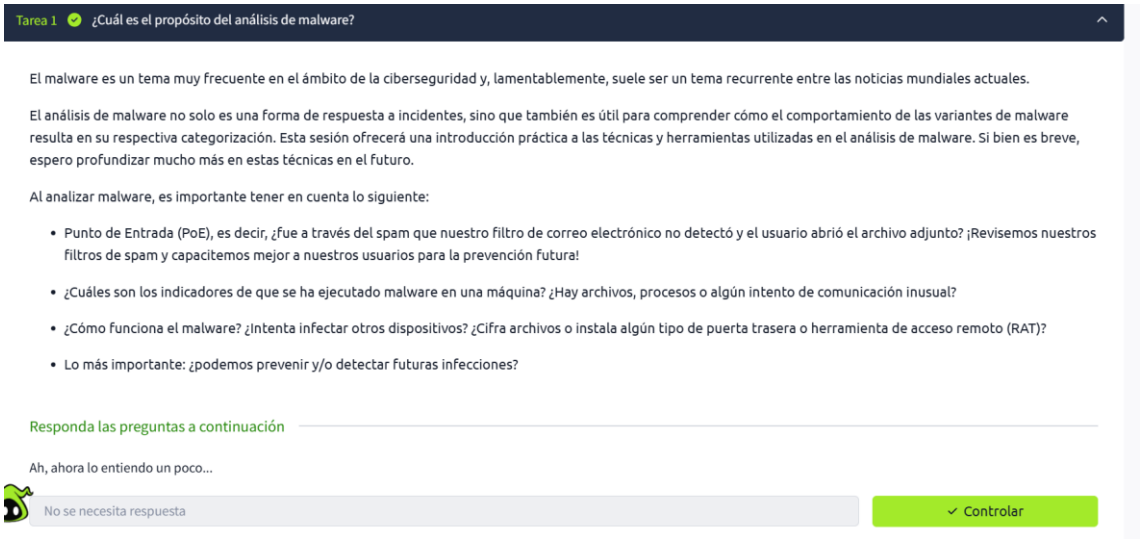
Y lo más importante: ¿Podemos, en última instancia, prevenir y/o detectar nuevas infecciones?

Malware Introductory

El reto consiste en completar las siguientes tareas:

Tarea 1. ¿Cuál es el propósito del análisis de malware?

La finalidad de esta tarea es entender el propósito del análisis del malware.



Tarea 2. Comprender las campañas de malware.

A "Targeted" attack is just that - targeted. In most cases, malware attacks that occur this way are created for a specific purpose against a specific target. A great example of this type of purpose could be the DarkHotel malware, whom is designed to steal information such as authentication details from government officials.

Mass Campaign

On the other hand, the "Mass Campaign" classification can be akin to many real life examples, and is the most common type of attacks. The entire purpose of this type of Malware is to infect as many devices as possible and perform whatever it may - regardless of target.

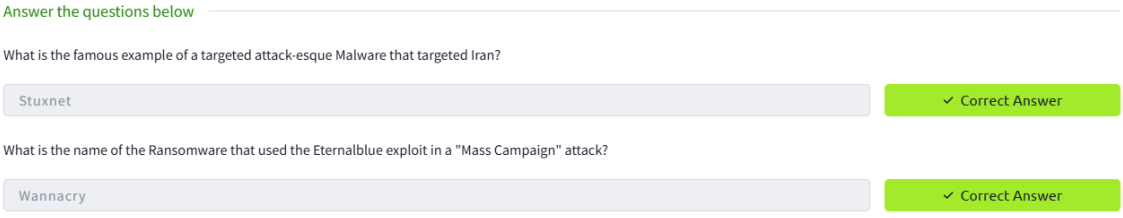
Companies such as Kaspersky to name one, track these campaigns (known as Advanced Persistent Threats (APTs) and often report on their infection rate and indicators, much akin to the real-life spread of a virus from the World Health Organisation (WHO).

Kaspersky report on the "Crouching Yeti (Energetic Bear)" campaign, this campaign specifically targets the following:

- Industrial/machinery
- Manufacturing
- Pharmaceutical
- Construction
- Education
- Information technology

(Kaspersky)

Whilst it this variant is *technically targeted*, there is a rather large scope of this variant of malware, and as such, can be considered as a "Mass Campaign" attack.



Tarea 3. Identificar si se ha producido un ataque de malware.

Aquí se pueden visualizar los pasos:

The ultimate process of a malware attack can be broken down into a few broad steps:

1. Delivery
2. Execution
3. Maintaining persistence (not always the case!)
4. Propagation (not always!)

Y mas abajo se encuentran las dos firmas que el malware puede dejar en un host después de un ataque.

Firmas basadas en el host

En términos generales, estos son los resultados de la ejecución y cualquier persistencia realizada por el malware. Por ejemplo, ¿se ha cifrado un archivo? ¿Se ha instala algún software adicional? Estas son dos de las muchas firmas basadas en el host que es útil conocer para prevenir y evitar futuras infecciones

Firmas basadas en red

En resumen, esta clasificación de firmas es la observación de cualquier comunicación de red que tenga lugar durante la entrega, ejecución y propagación. Por ejemplo el ransomware, ¿dónde ha contactado el malware para los pagos de Bitcoin?

Aquí se muestra la evidencia de la superación del nivel.

These are generally speaking the results of execution and any persistence performed by the Malware. For example, has a file been encrypted? Has any additional software been installed? These are two of many, many host-based signatures that are useful to know to prevent and check against further infection.

Network-Based Signatures

At an overview, this classification of signatures are the observation of any networking communication taking place during delivery, execution and propagation. For example, in Ransomware, where has the Malware contacted for Bitcoin payments?

Such as in the case of Wannacry, looking for a large amount of "Samba" Protocol communication attempts is a great indication of infection due to its use of "Eternalblue".

Answer the questions below

Name the first essential step of a Malware Attack?

Delivery — ✓ Correct Answer

Now name the second essential step of a Malware Attack?

Execution — ✓ Correct Answer

What type of signature is used to classify remnants of infection on a host?

Host-Based Signatures — ✓ Correct Answer

What is the name of the other classification of signature used after a Malware attack?

Network-Based Signatures — ✓ Correct Answer

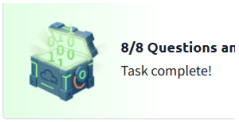
Tarea 4. Estático vs. Análisis dinámico.

En esta tarea no hay que hacer nada, únicamente comprender las categorías que se utilizan a la hora de analizar el malware.

Existen dos categorías que se utilizan al analizar malware:

1. Análisis estático

2. Análisis dinámico



Si bien los métodos y herramientas utilizados para estas dos categorías son muy diferentes, son esenciales para comprender cómo se comporta un malware.

Análisis estático .

En resumen, el " Análisis Estático " se utiliza para obtener una abstracción de alto nivel de la muestra. Con este método, puede ser bastante sencillo determinar si un fragmento de código es "malicioso" (aunque no siempre, ya que se tratará más adelante). En esencia, este método consiste en analizar la muestra en su estado actual, sin ejecutar el código.

El uso de técnicas como el análisis de firmas mediante sumas de comprobación permite realizar un análisis de malware rápido, eficaz (aunque extremadamente breve) y seguro.

Análisis dinámico

Este paso es mucho más complejo y es donde se basa en gran medida la abstracción de la muestra. El « análisis dinámico » implica esencialmente ejecutar la muestra y observar lo que sucede. Por supuesto, esto no es seguro. Si la muestra resulta ser «ransomware», ha perdido sus archivos. Si es capaz de propagarse atravesando una red, genial... Acaba de infectar su red de área local (LAN).

Tenga en cuenta que estas son explicaciones extremadamente simplistas de estas técnicas ; hay mucho más involucrado que abordaremos a lo largo de esta serie.

Responda las preguntas a continuación

¡Entiendo las dos amplias categorías que se emplean al analizar malware potencial!

No se necesita respuesta

✓ Respuesta correcta

Tarea 5. Discusión sobre las herramientas proporcionadas y sus usos.

Lo único que se hace en esta tarea es comprender las herramientas de análisis estático.

Verá que algunas herramientas se superpondrán entre el análisis estático y dinámico :

Herramientas de análisis estático proporcionadas :

C:\Usuarios\Análisis\Escritorio\ **Herramientas\Estático\ Herramientas PE**

- Dependency Walker (depende)
- ID de PE
- **Explorador de PE**
- PEview
- ResourceHacker

C:\Usuarios\Análisis\Escritorio\ **Herramientas\Estático\Desmontaje**

- IDA Freeware
- WinDbg

C:\Usuarios\Análisis\Escritorio\ **Herramientas\Sysinternalsuite**

- ResourceHacker

C:\Usuarios\Análisis\Escritorio **\Herramientas\Dinámica**

Las herramientas enumeradas aquí se utilizarán para tareas futuras, ya que implican depuración, que actualmente está fuera del alcance de esta sala... Sin embargo, se explorarán más adelante en la serie

Responda las preguntas a continuación

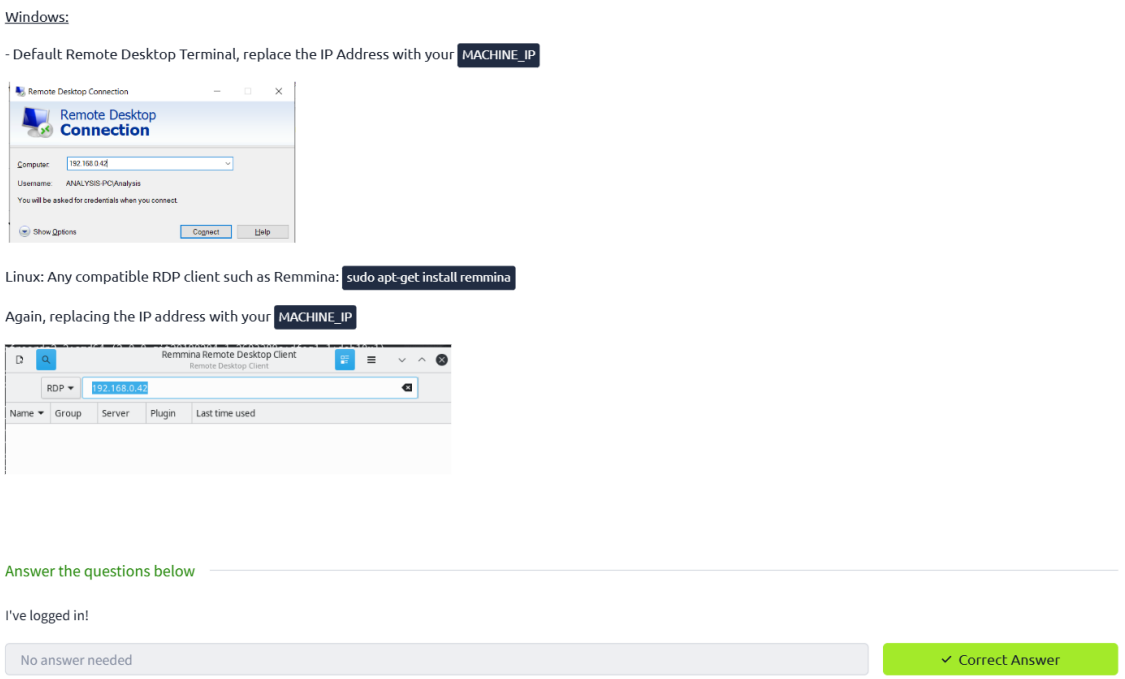
Vamos a proceder

No se necesita respuesta

✓ Respuesta correcta

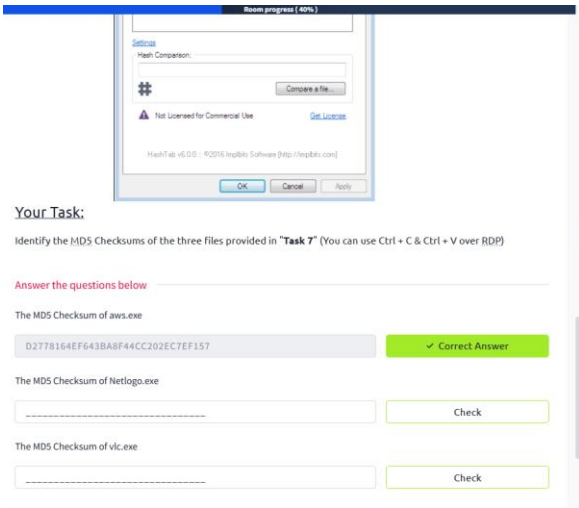
Tarea 6. Conexión al entorno de análisis de Windows (despliegue).

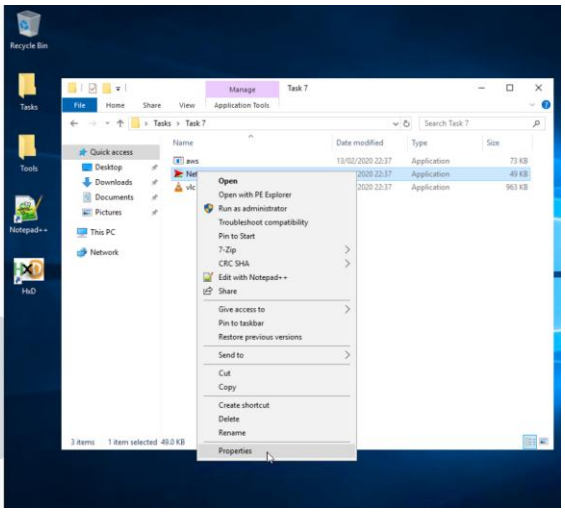
En esta tarea se inicializa la Maquina Virtual que vamos a utilizar para las próximas tareas.

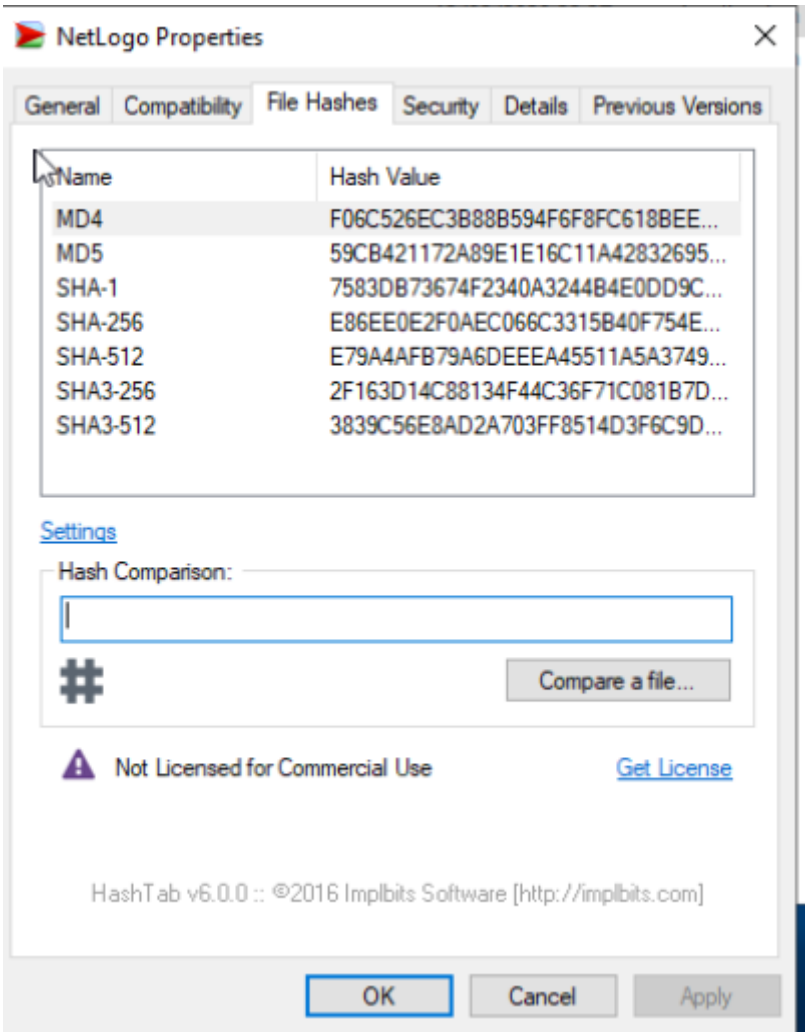


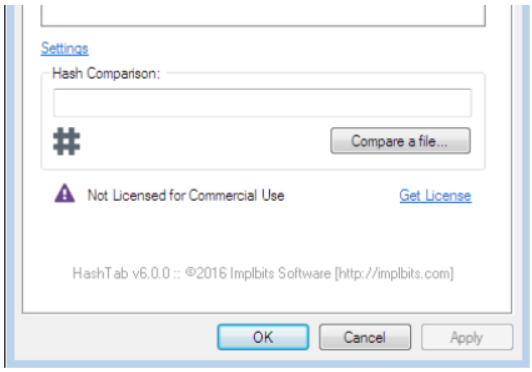
Tarea 7. Obtención de sumas de comprobación MD5 de los archivos proporcionados.

Encendemos la maquina virtual desde el ejercicio 6 y nos vamos a la carpeta Tasks luego a Task 7 y ahí en cada uno de los archivos se procede a acceder a sus propiedades luego se procede a entrar a la ventana “File Hashes” y ahí se pueden visualizar los hashes necesarios para superar la prueba.






NetLogo Properties
General
Compatibility
File Hashes
Security
Details
Previous Versions
Name
Hash Value
MD4
F06C526EC3B88B594F6F8FC618BEE...
MD5
59CB421172A89E1E16C11A42832695...
SHA-1
7583DB73674F2340A3244B4E0DD9C...
SHA-256
E86EE0E2F0AEC066C3315B40F754E...
SHA-512
E79A4AFB79A6DEEEA45511A5A3749...
SHA3-256
2F163D14C88134F44C36F71C081B7D...
SHA3-512
3839C56E8AD2A703FF8514D3F6C9D...
Settings
Hash Comparison:
Compare a file...
Not Licensed for Commercial Use
Get License
HashTab v6.0.0 :: ©2016 Implbits Software [http://implbits.com]
OK
Cancel
Apply



Your Task:

Identify the MD5 Checksums of the three files provided in "**Task 7**" (You can use Ctrl + C & Ctrl + V over RDP)

Answer the questions below

The MD5 Checksum of aws.exe

D2778164EF643BA8F44CC202EC7EF157 ✓ Correct Answer

The MD5 Checksum of Netlogo.exe

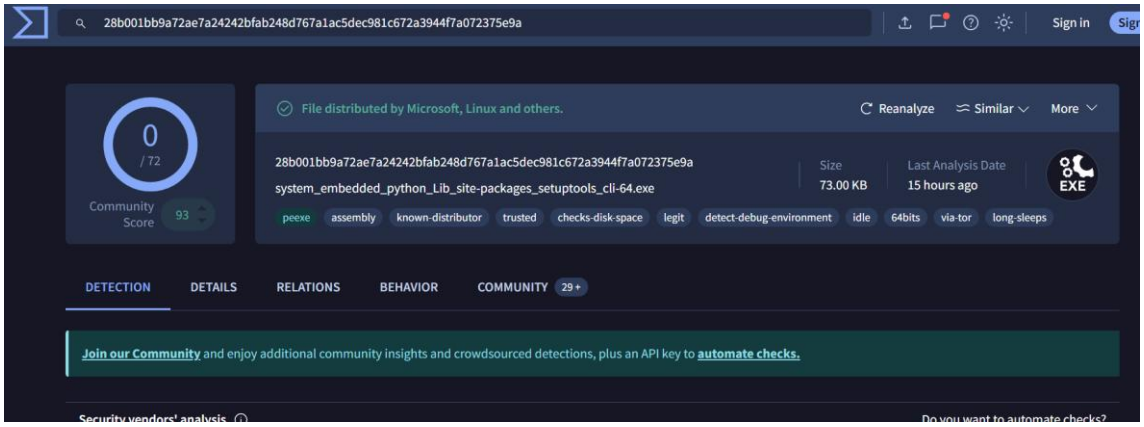
59CB421172A89E1E16C11A428326952C ✓ Correct Answer

The MD5 Checksum of vlc.exe

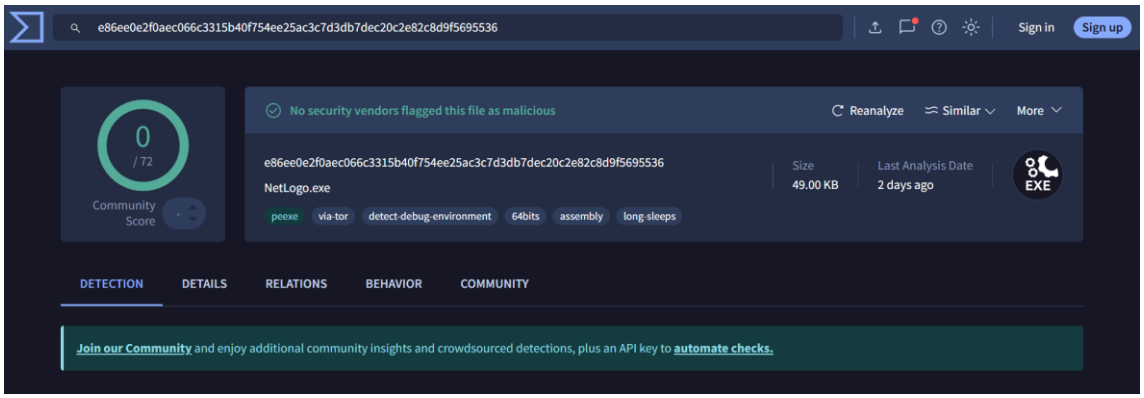
5416BE1B8B04B1681CB39CF0E2CAAD9F ✓ Correct Answer

Tarea 8. Ahora veamos si las sumas de comprobación MD5 se han analizado antes.

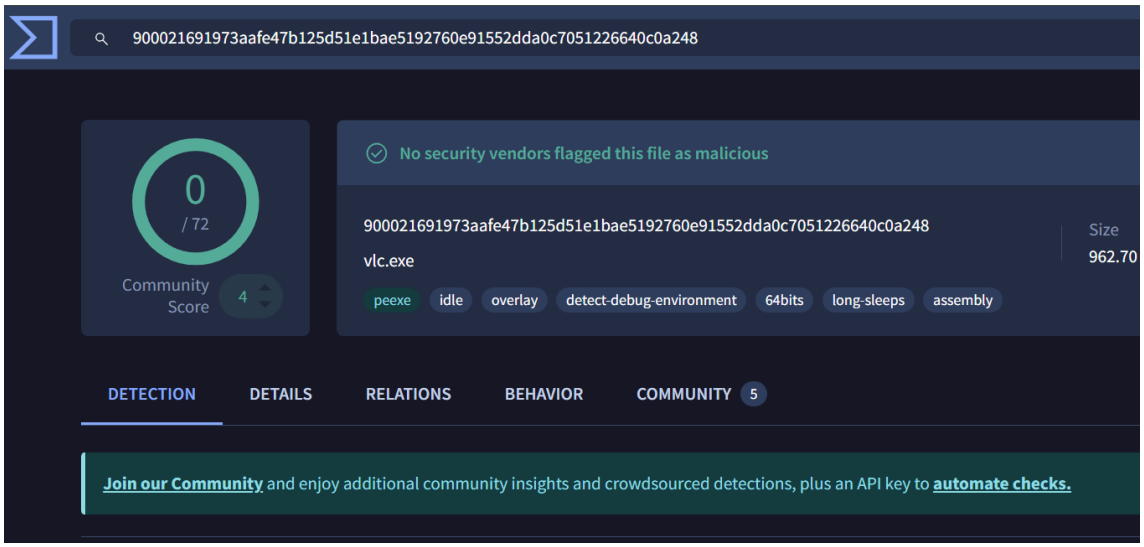
Aws.exe no lo califica como malicioso



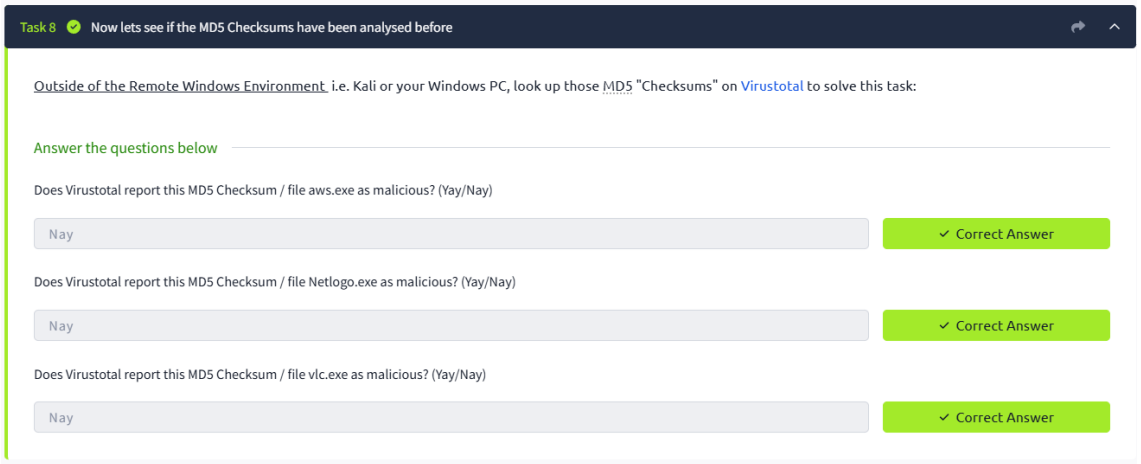
Netlogo.exe tampoco lo detecta como malicioso



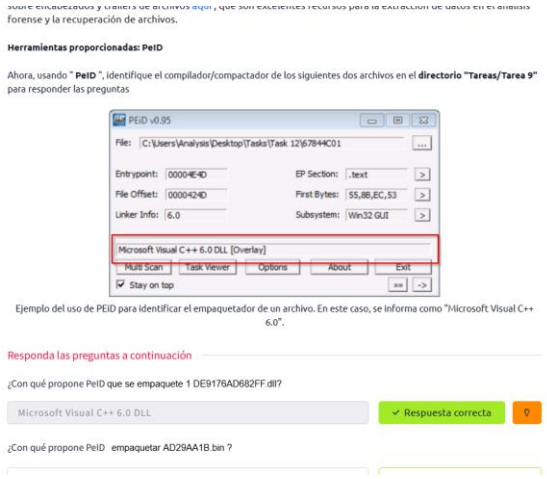
Vlc.exe tampoco lo muestra como malicioso

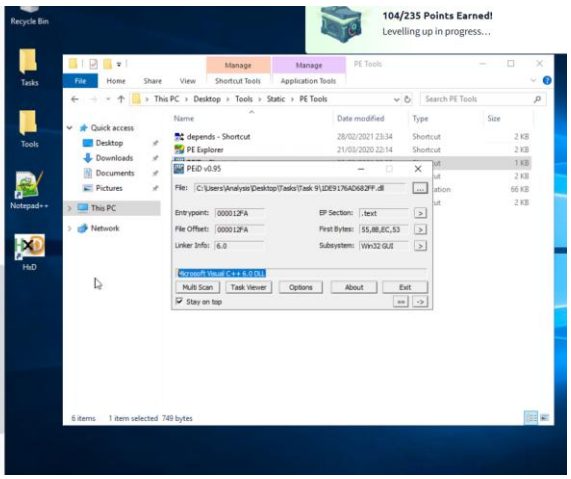


Aquí se ve como se ha superado el reto.

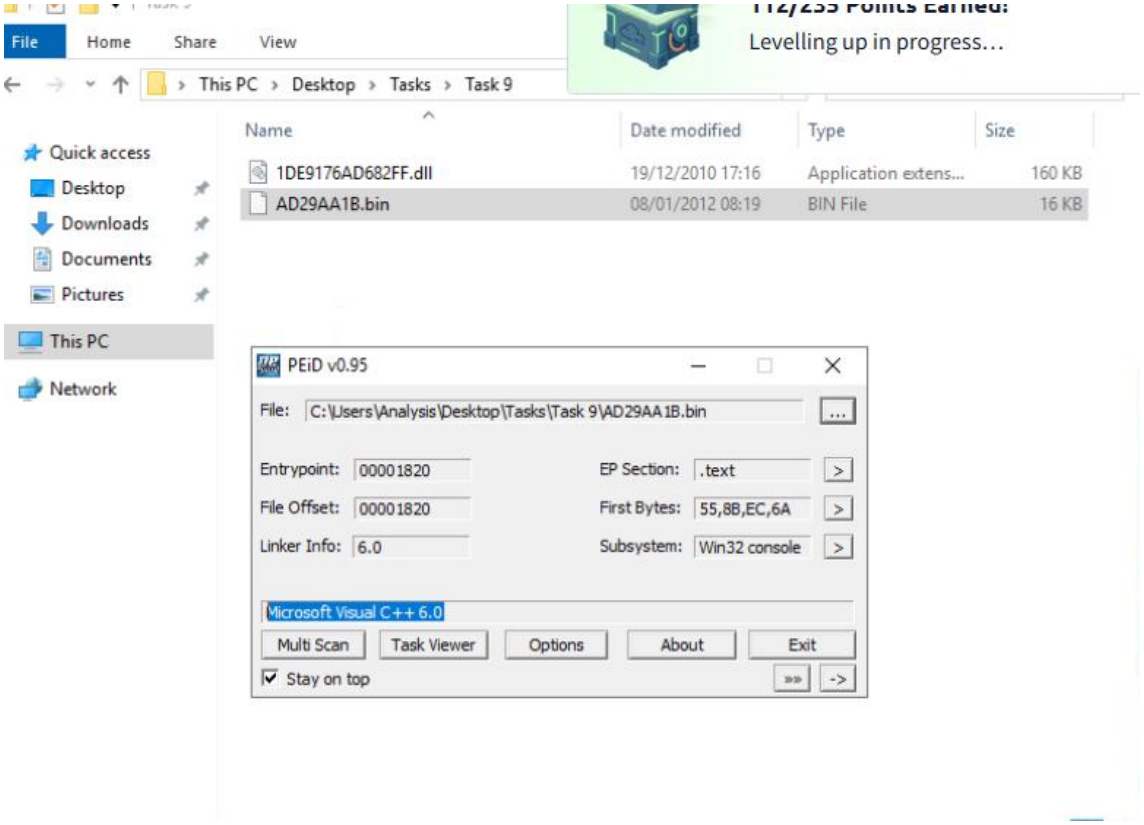


Tarea 9. Identificar si los ejecutables están ofuscados/empaquetados.

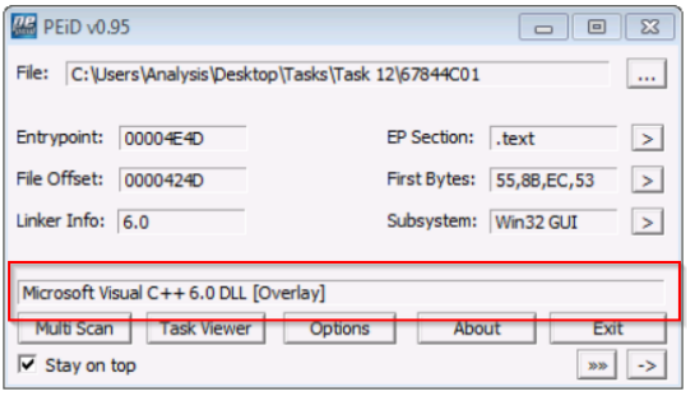




Para la segunda respuesta al abrir la herramienta esta por defecto filtrando por ejecutables hay que cambiarlo a filtrar por todos para que aparezca el archivo.



Evidencia de superación de los niveles.



Ejemplo del uso de PEiD para identificar el empaquetador de un archivo. En este caso, se informa como "Microsoft Visual C++ 6.0".

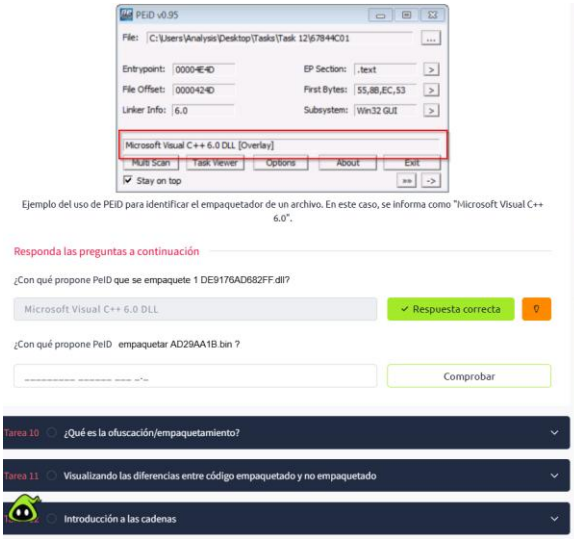
Responda las preguntas a continuación

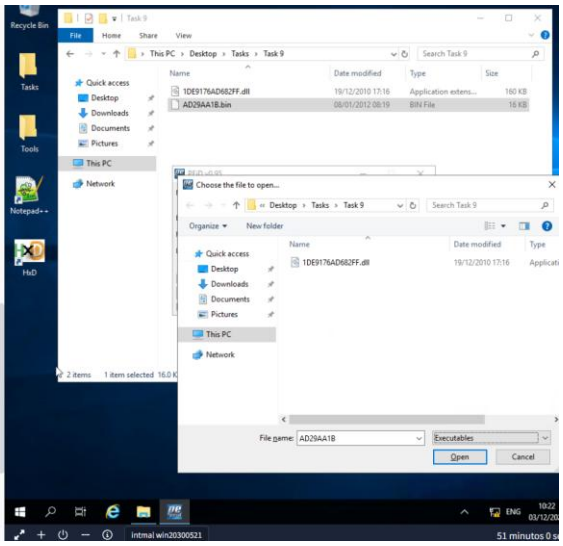
¿Con qué propone PeID que se empaquete 1 DE9176AD682FF.dll?

Microsoft Visual C++ 6.0 DLL ✓ Respuesta correcta

¿Con qué propone PeID empaquetar AD29AA1B.bin ?

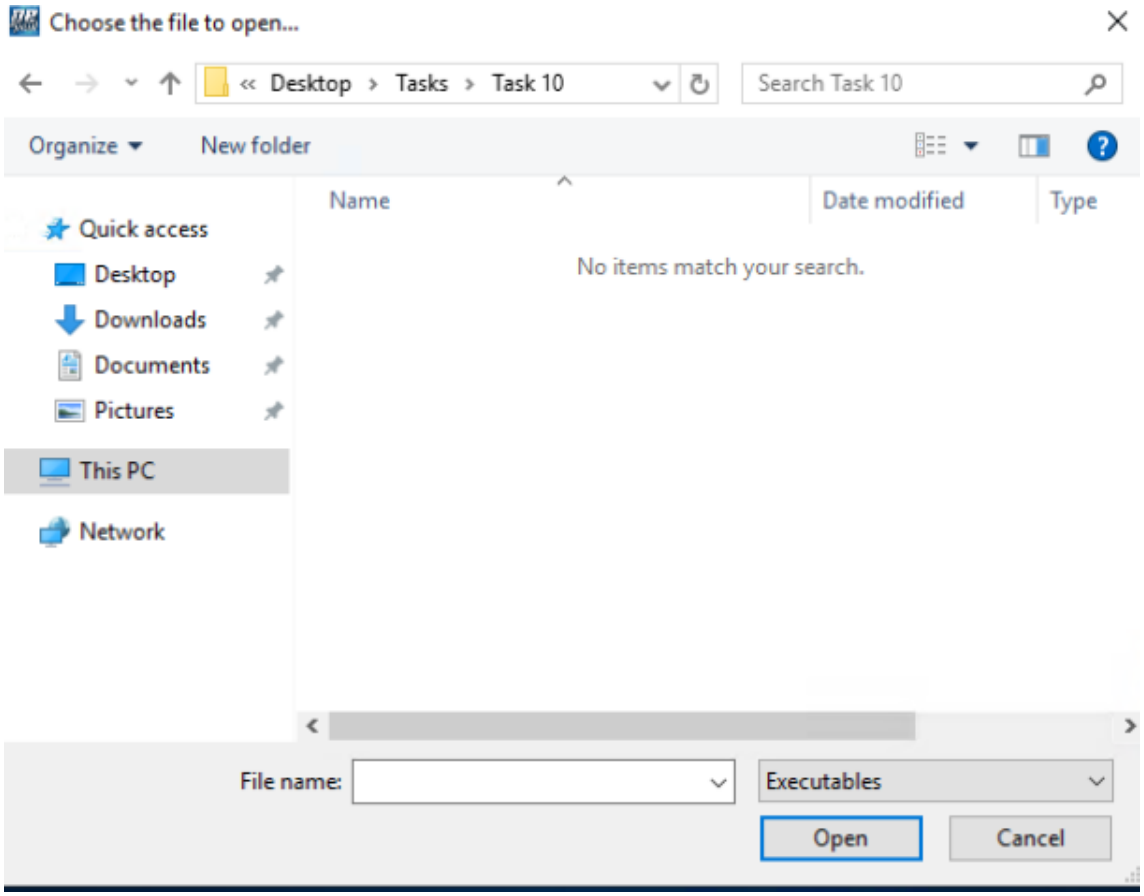
Microsoft Visual C++ 6.0 ✓ Respuesta correcta



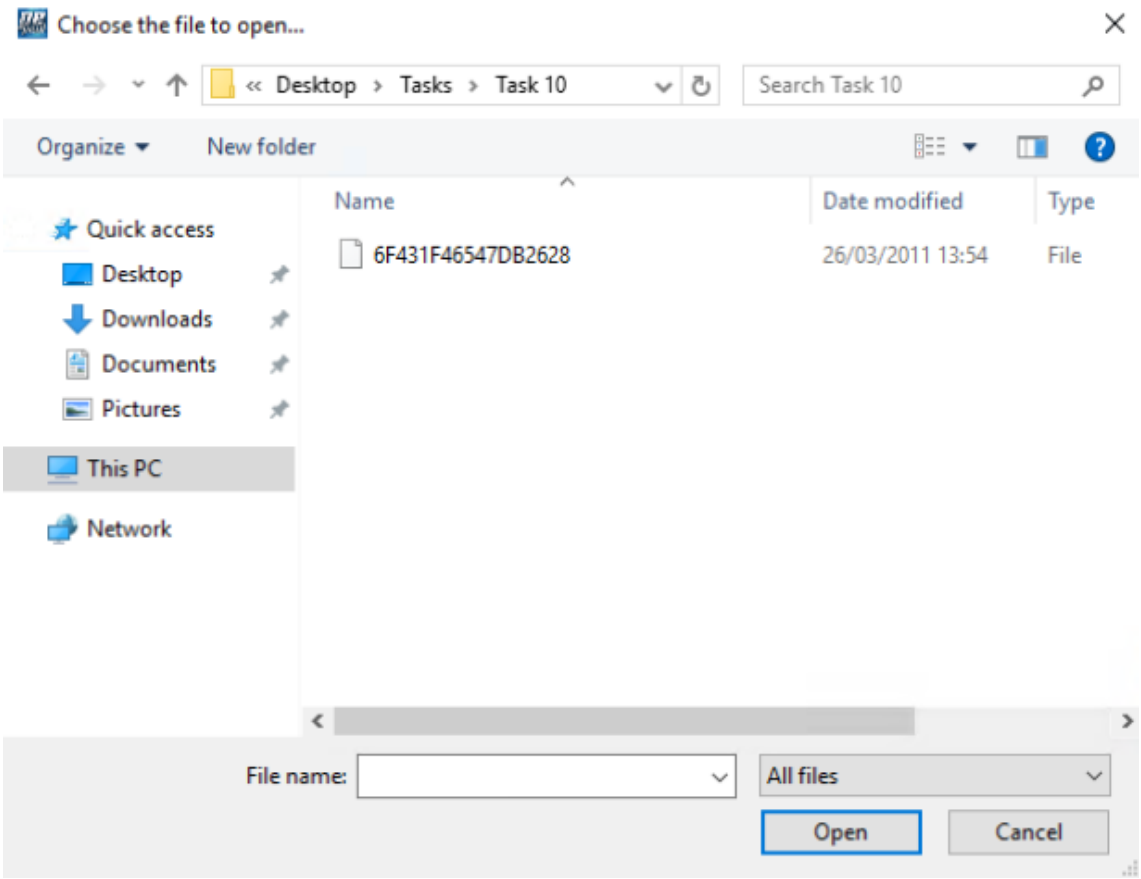


Tarea 10. ¿Qué es la ofuscación/empaquetado?.

Abro la herramienta y veo que no aparece ningún archivo en la carpeta de Task 10 y es por el mismo tema de que esta filtrando solo por archivo ejecutables.



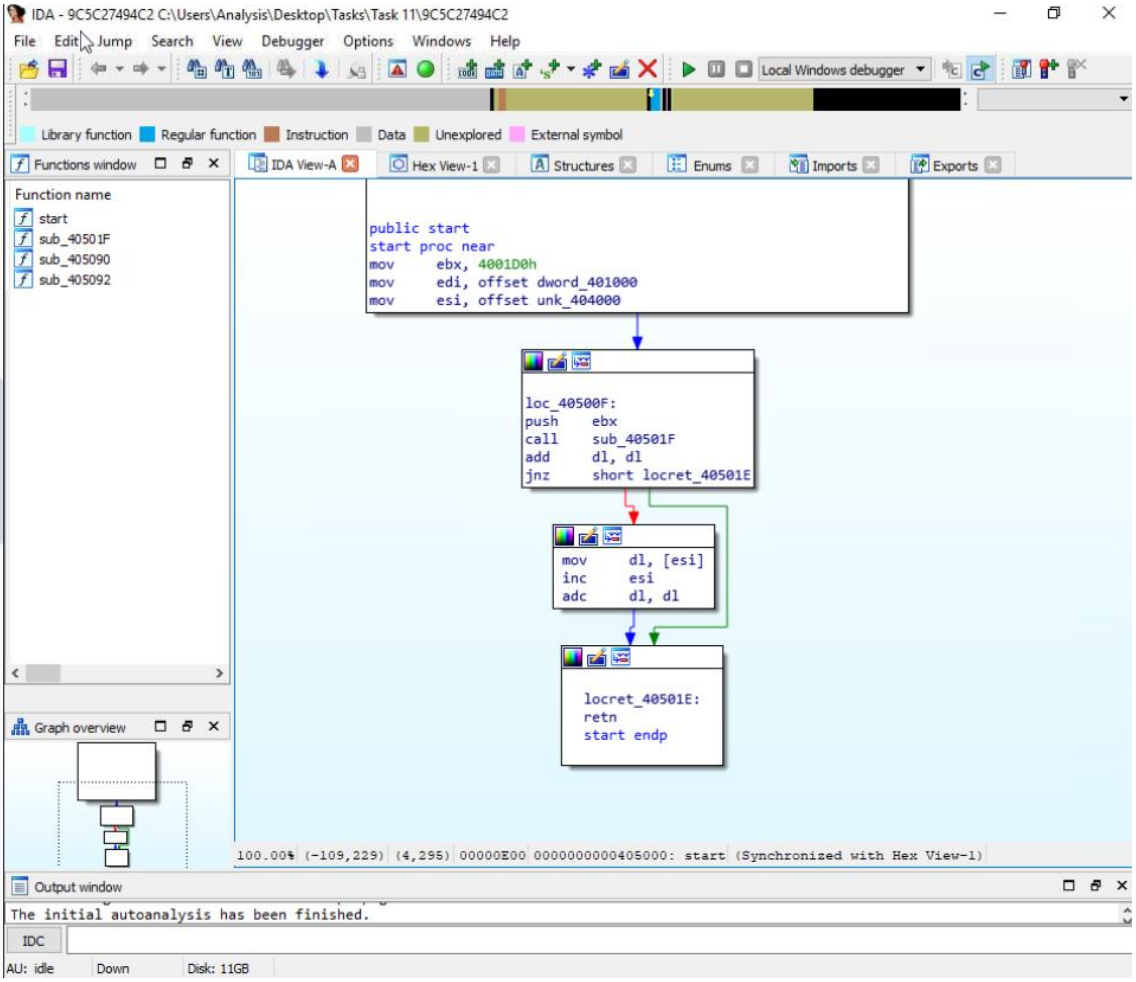
Una vez cambiado el filtrado se ve como aparece el archivo que estamos buscando.



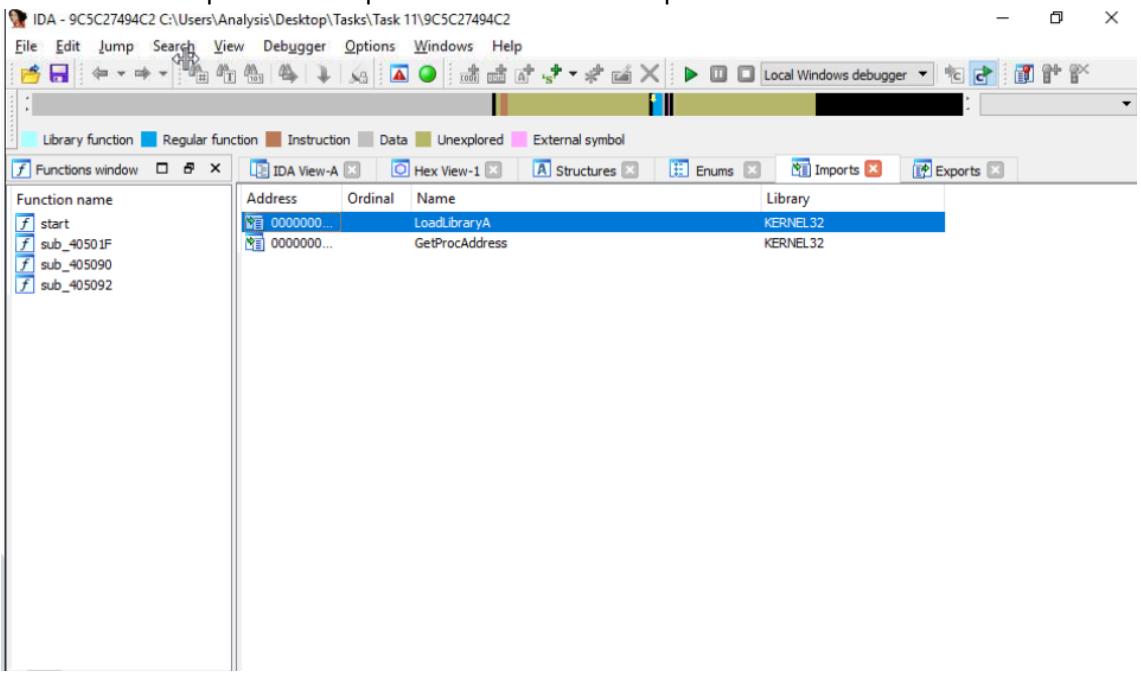
Dentro del mismo tenemos la respuesta.

Tarea 11. Visualizando las diferencias entre código empaquetado y no empaquetado.

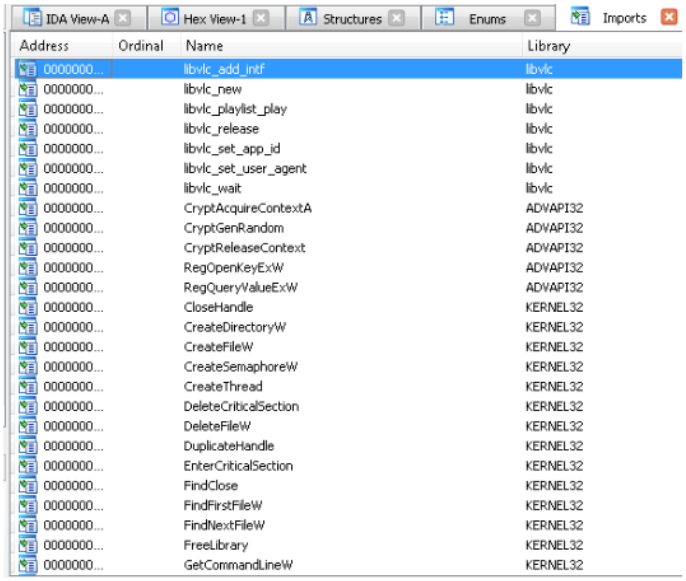
Abrimos la herramienta iIDA con el archivo del task 11



En la sección Imports se ve que se han intentado importar dos archivos lo cual es extraño



Evidencia de superación del nivel.



¿Ves cuánta información hay aquí? El código ofuscado es mucho más difícil de analizar, al menos a nivel estático, ya que se nos presenta muy poca información.

Responda las preguntas a continuación

¡Maldita ofuscación!

No se necesita respuesta

✓ Respuesta correcta

Tarea 12. Introducción a las cadenas ("strings").

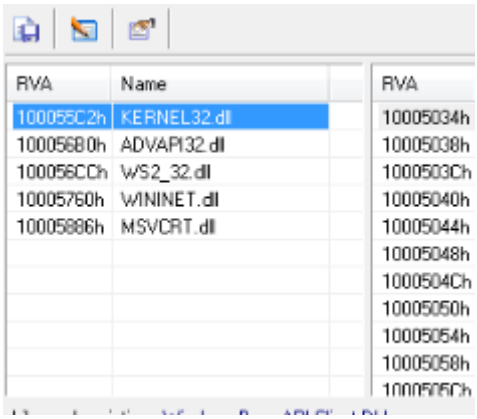
Primero abrimos el cmd, vamos a la ruta: cd C:\Users\Analysis\Desktop\Tools\SysinternalsSuite y ejecutamos la herramienta de strings.

```
C:\Users\Analysis\Desktop\Tools\SysinternalsSuite>strings "C:\Users\Analysis\Desktop\Tasks\Task 12\67844C01"

Strings v2.53 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

!This program cannot be run in DOS mode.
Rich
.text
`.rdata
@.data
.reloc
QQSUVW3
_^]
[YY
```

Y vemos que nos sale la URL que nos pide la respuesta 1

```
Y29ubmVjdA==
practicalmalwareanalysis.com
serve.html
dW5zdXBwb3J0
```

Para la respuesta 2, aquí se puede observar como son 5 las importaciones únicas que hay.



RVA	Name	RVA
100055C2h	KERNEL32.dll	10005034h
10005680h	ADVAPI32.dll	10005038h
100056CCh	WS2_32.dll	1000503Ch
10005760h	WININET.dll	10005040h
10005886h	MSVCRT.dll	10005044h
		10005048h
		1000504Ch
		10005050h
		10005054h
		10005058h
		1000505Ch

Evidencia de como se ha superado el nivel.

¿Cuál es la URL que se muestra después de usar "strings"?

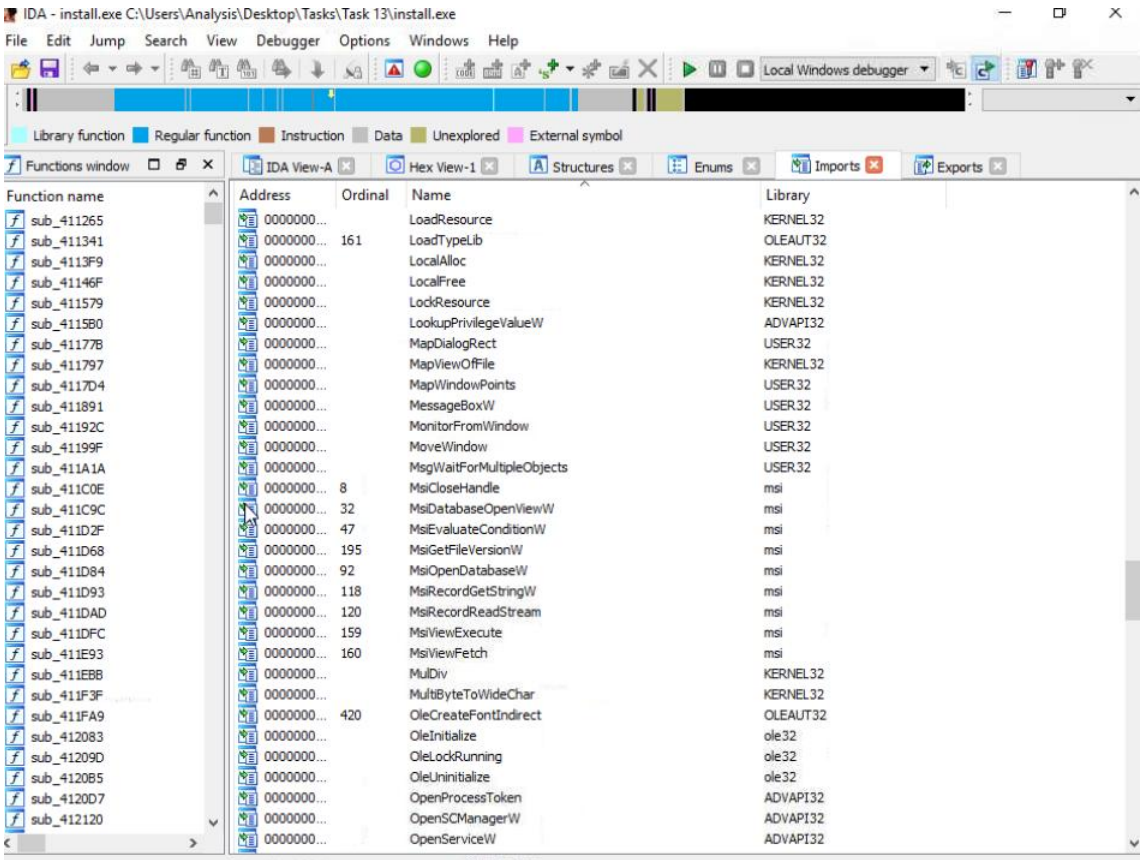
practicalmalwareanalysis.com ✓ Respuesta correcta

¿Cuántas "Importaciones" **únicas** hay?

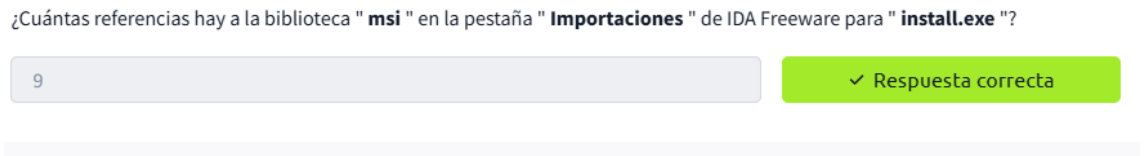
5 ✓ Respuesta correcta

Tarea 13. Introducción a las importaciones.

Utilizando la herramienta IDA y abriendo el ejecutable install.exe voy a la sección de importaciones y se ve como la librería con nombre msi solo aparece 9 veces.

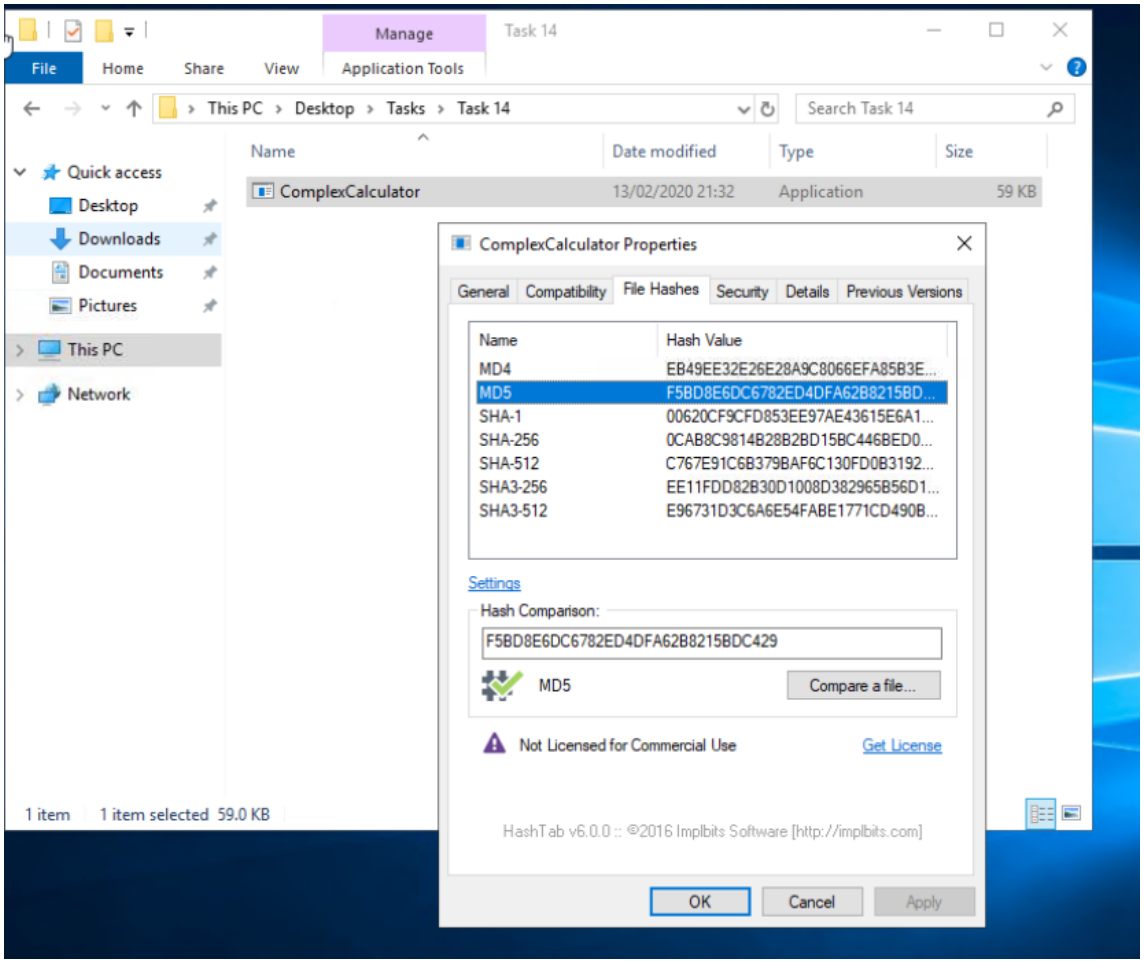


Evidencia de superación del ejercicio.

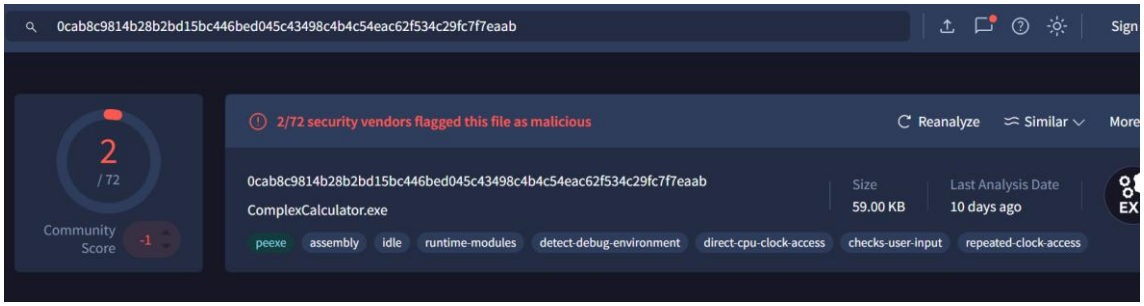


Tarea 14. Resumen práctico.

Primero me voy a la carpeta 14 al archivo que estamos buscando le hacemos click derecho propiedades y vamos a las secciones de File Hashes y nos aparece el MD5 que estamos buscando.



Después, para la segunda respuesta, vamos a virustotal y pegamos ese MD5 y obtenemos:



Con lo cual si detecta que es malicioso.

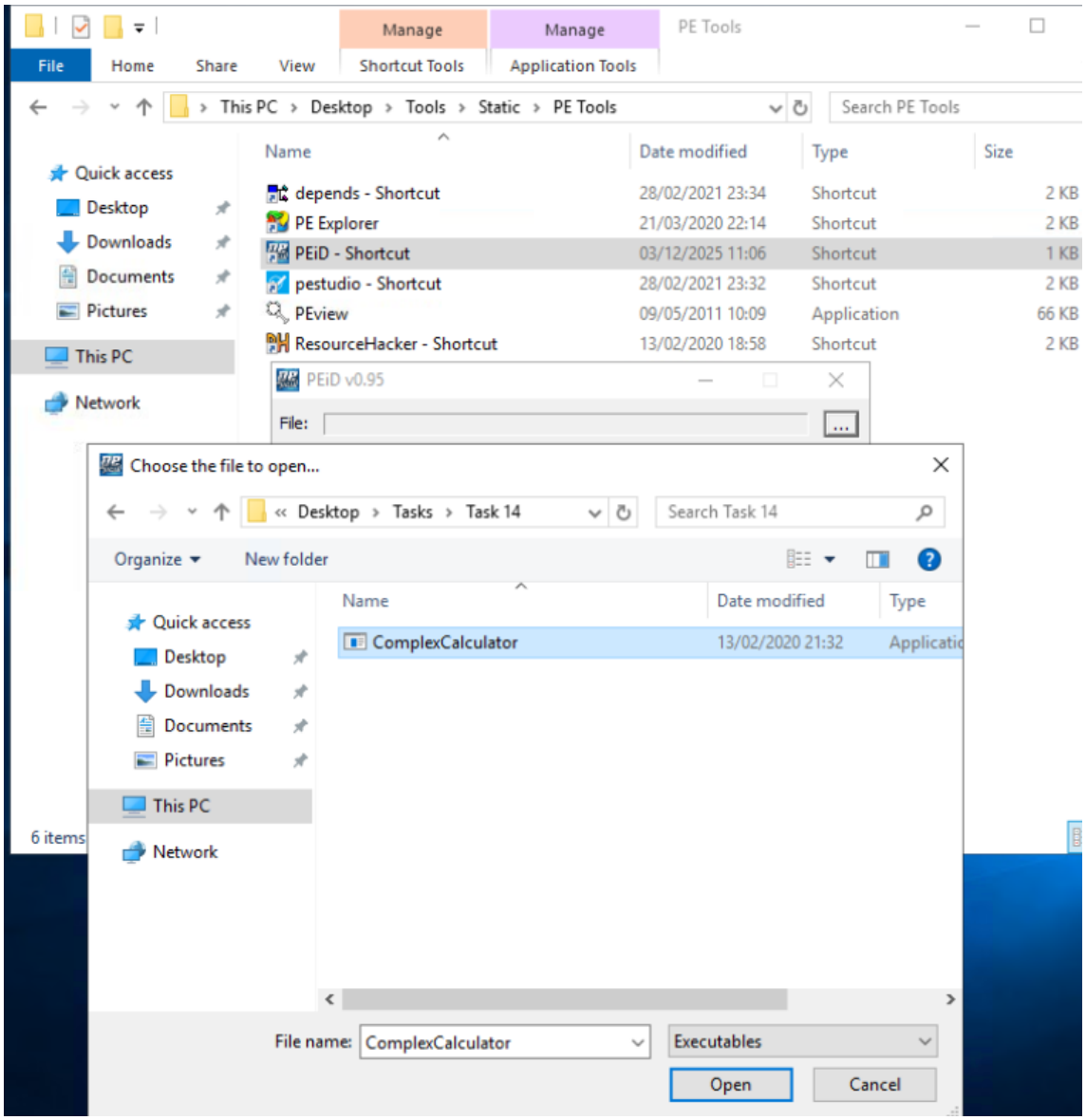
Para la siguiente respuesta utilizamos la herramienta strings desde cmd:

```
C:\Users\Analysis\Desktop\Tools\SysinternalsSuite>strings "C:\Users\Analysis\Desktop\Tasks\Task 14\ComplexCalculat
or.exe"

Strings v2.53 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

!This program cannot be run in DOS mode.
a`A
od.
Vc.
od*
od,
```

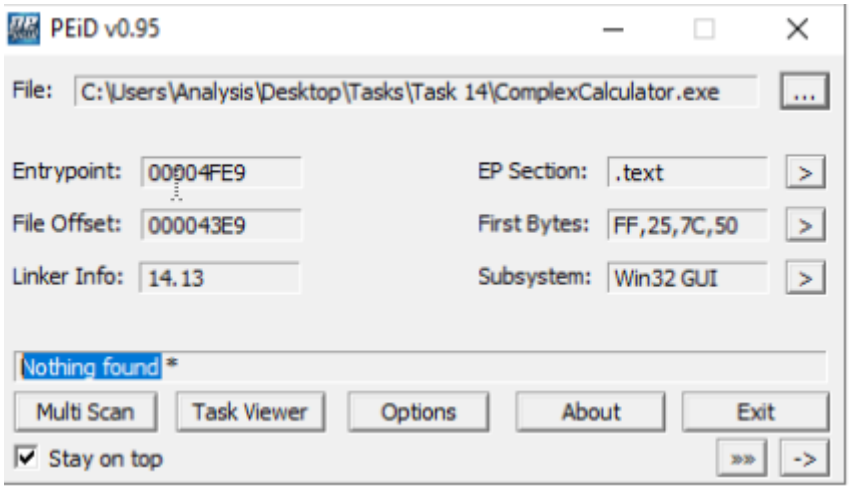
La última cadena usada es: “d:h:” cómo se puede apreciar en la captura.

```
1 1&1,12181>1D1J1P1
12282>2
2&3.3B3U3
565_5n5
6w6
7-7;7V7a7
8B8V8]8
:':h:n:
:;;@;e;m;w;
<'</<;<D<I<O<Y<c<s<
=&=.=6=A=F=L=V=`=s=X=
>&>P>_>
?9?H?Q?^?v?
0h1l1p1t1
2 2
d:h:

C:\Users\Analysis\Desktop\Tools\SysinternalsSuite>_
```

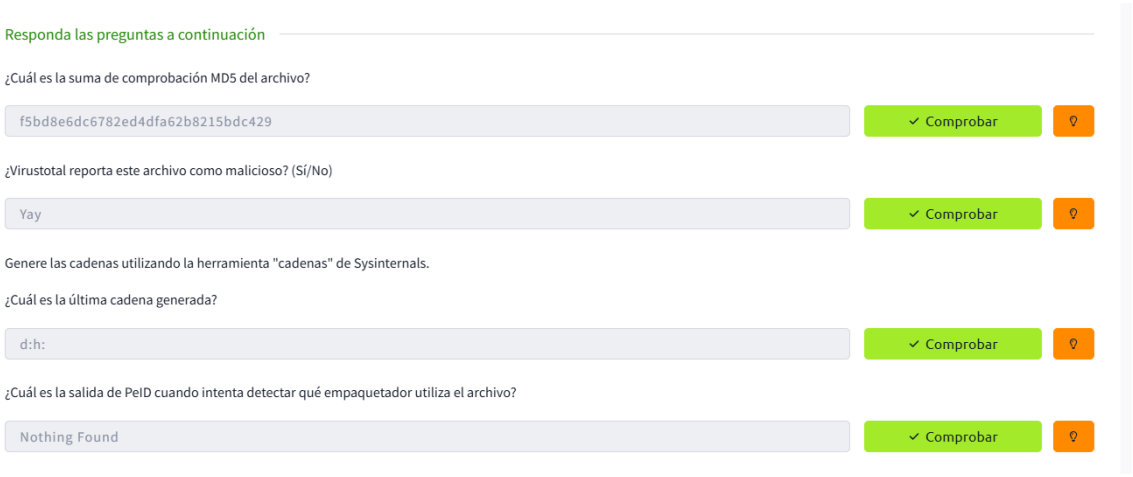
Para la siguiente pregunta, abrimos el archivo 14 desde PeID



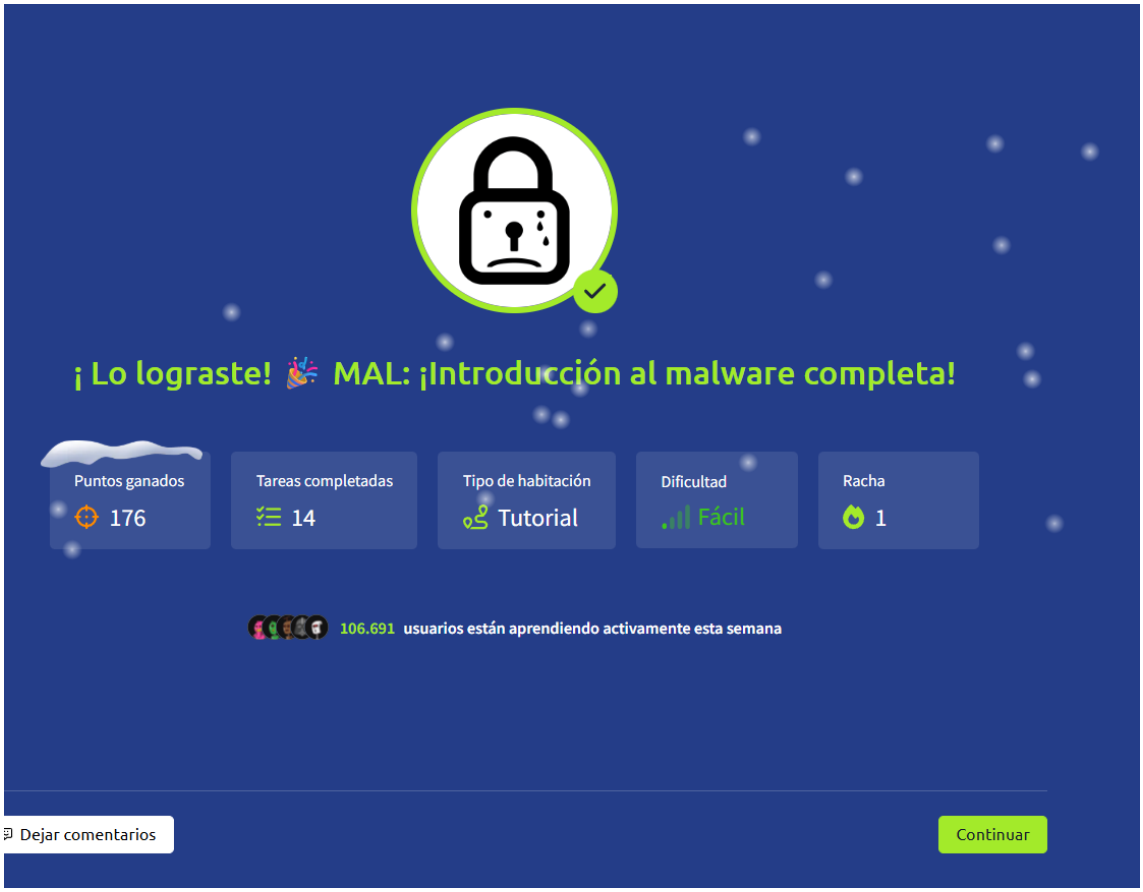
Se ve la salida de cuando intenta detectar que empaquetador utiliza el archivo.



Evidencia de superación del nivel 14.



Aquí se puede visualizar la flag del CTF FINAL.



Hay que documentar el CTF para realizar la entrega individual en moodle. Este debe incluir como mínimo:

Respuesta a cada pregunta formulada.

Explicación de como se ha superado cada prueba y/o nivel.

Capturas de pantalla que evidencien como se ha superado cada prueba y/o nivel.

Otros retos

Si te ha gustado Análisis de Malware, y quieres más retos para seguir practicando, puedes realizar los siguientes CTF:

TryHackMe Basic Malware RE:

https://tryhackme.com/r/room/basicmalwarere

TryHackMe Carnage:

https://tryhackme.com/r/room/c2carnage

TryHAckMe Dunkle Materie:

https://tryhackme.com/r/room/dunklematerieptxc9