

CREACIÓN SANBOX WINDOWS 10

Versión 1.0

MAIK.ES

05/03/2025



Índice

Introducción:	1
Consideraciones antes de crear la máquina virtual	2
Creación de un usuario local aleatorio.....	2
Evitar el uso de una cuenta personal de Microsoft	2
Creación de máquina virtual	2
Crear instantánea INICIAL de la máquina.....	2
Configurar tipo de red	3
Instalación Guest Additions Virtualbox	3
Deshabilitar Microsoft defender	4
Desinstalar Microsoft defender	6
Segunda instantánea de la máquina en VirtualBox.....	9
Instalación de herramientas	9
Autoruns.....	9
TCPView.....	10
ProcExp (Process Explorer).....	11
Conclusión	12
Agradecimientos.....	13

Introducción:

Bienvenido a esta guía didáctica y ética sobre la creación y uso de una **sandbox** en una máquina virtual con **VirtualBox**. En este documento, aprenderás a configurar un entorno controlado con **Windows 10** diseñado específicamente para el análisis de software malicioso.

Es importante destacar que esta guía tiene **finés exclusivamente educativos y de investigación**, orientados al análisis de malware en un entorno seguro. **No se fomenta ni se respalda el uso indebido de los conocimientos adquiridos.**

Para garantizar que el análisis no se vea afectado por medidas de seguridad automatizadas, **se deshabilitará completamente Windows Defender**, evitando así la eliminación o alteración de los archivos en estudio. Además, utilizaremos herramientas clave para la inspección del sistema y la identificación de cambios provocados por el malware, tales como:

- **Autoruns:** Para examinar los programas y servicios que se inician automáticamente con el sistema.
- **TCPView:** Para monitorear conexiones de red y detectar comunicaciones sospechosas.
- **Process Explorer (ProcExp):** Para analizar procesos en ejecución y evaluar su comportamiento.

Siguiendo esta guía paso a paso, podrás configurar un entorno seguro donde analizar el comportamiento de software potencialmente malicioso sin poner en riesgo tu sistema principal. **Recuerda siempre manejar este conocimiento con responsabilidad y en entornos controlados.** ¡Comencemos!



Consideraciones antes de crear la máquina virtual

Antes de proceder con la creación de la máquina virtual, es fundamental tener en cuenta algunos aspectos clave para garantizar la seguridad y la efectividad de nuestra **Sandbox**.

Creación de un usuario local aleatorio

Durante la instalación de **Windows 10**, será necesario crear un usuario local en la máquina virtual. **Es importante que el nombre de usuario, la contraseña y las preguntas de seguridad sean completamente aleatorios y no tengan relación con nosotros.** Esto se debe a que la **Sandbox** será un entorno donde instalaremos y analizaremos diferentes tipos de malware, por lo que **no debe contener información personal ni datos reutilizables.**

Para generar credenciales seguras y aleatorias, puedes utilizar herramientas en línea de generación de contraseñas o simplemente escribir datos al azar que no recuerdes ni uses en ningún otro sistema.

Evitar el uso de una cuenta personal de Microsoft

Windows 10 puede solicitar el inicio de sesión con una cuenta de **Microsoft**. **No uses una cuenta personal ni ninguna vinculada a información real.** En su lugar, elige la opción de **crear un usuario local** o, si deseas usar una cuenta de Microsoft, crea una nueva dentro de la máquina virtual exclusivamente para este propósito.

Esto es crucial para evitar que cualquier malware acceda a información privada o vincule la Sandbox a tu cuenta principal.

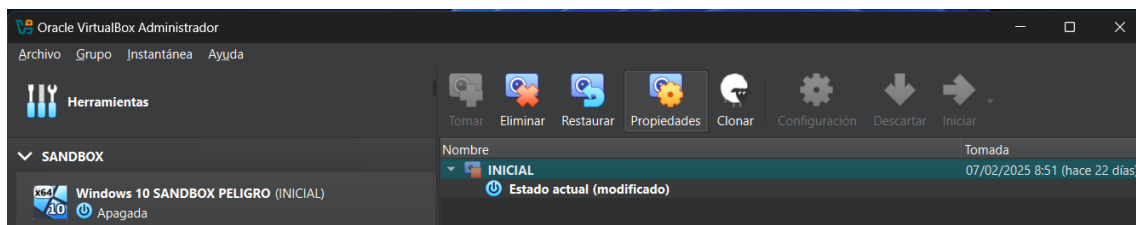
Creación de máquina virtual

Configuraciones previas de la máquina virtual:

- Núcleos de procesador: 4
- RAM: 4GB
- Almacenamiento: 50GB

Crear instantánea INICIAL de la máquina

Una vez creada la máquina virtual antes de comenzar con el proceso de creación de la Sandbox crearemos una instantánea INICIAL (MV limpia sin ninguna modificación).



Configurar tipo de red

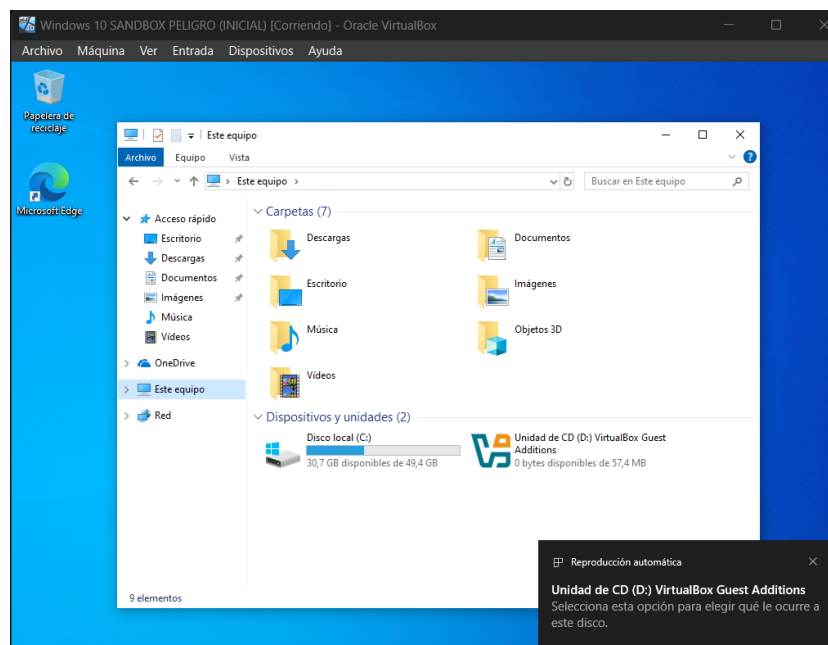
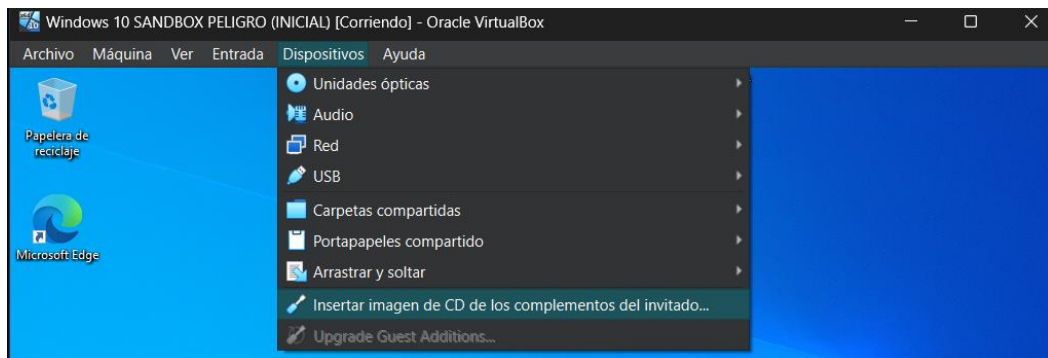
Para lograr que la máquina virtual tenga **acceso a Internet**, pero **no pueda comunicarse ni con la máquina anfitriona ni con otras máquinas**, la mejor opción es utilizar la configuración "NAT".

¿Por qué NAT?

- **NAT (Network Address Translation)** permite que la máquina virtual acceda a Internet a través de la máquina anfitriona, pero no permite que la VM se comunique con la anfitriona ni con otras máquinas en la red local.
- La máquina virtual tendrá acceso a Internet, pero su comunicación será limitada solo a esa red externa (Internet), sin acceso ni visibilidad desde la red local ni desde la máquina anfitriona.

Instalación Guest Additions Virtualbox

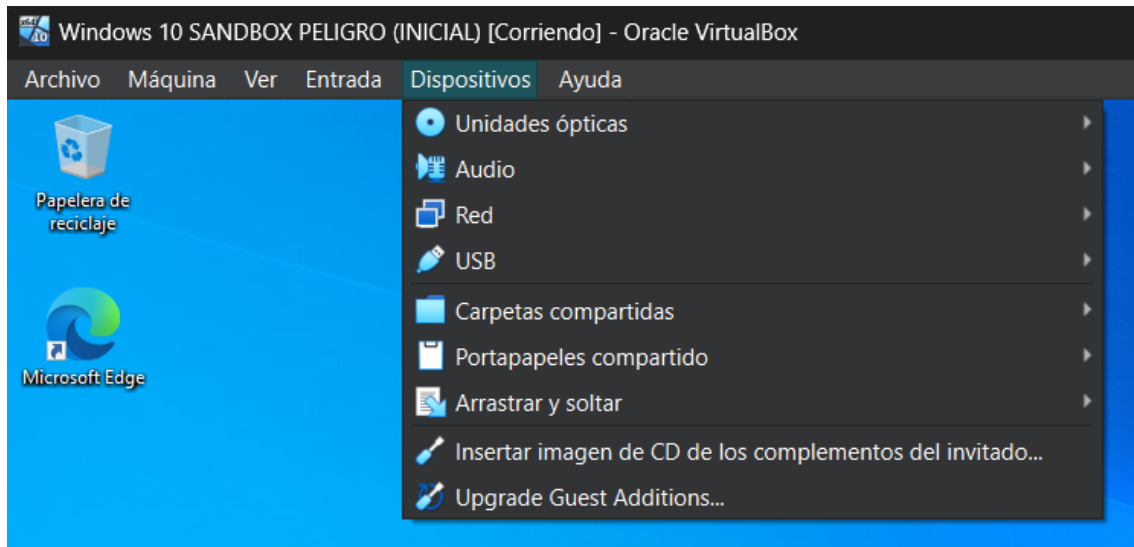
El siguiente paso será la instalación de las guest additions de virtualbox.



Ejecutamos Virtualbox Guest Additions y le damos siguiente hasta finalizar el proceso. Tras finalizar elegimos la opción de reinicio de la máquina.

Tras reiniciar la máquina nos dirigimos a la opción “Dispositivos” de VirtualBox y configuramos las siguientes opciones:

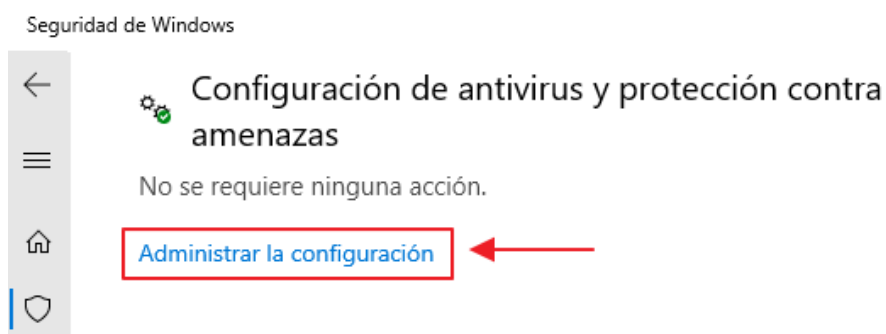
- Portapapeles compartido: Anfitrión (host) a invitado (máquina virtual).
- Arrastrar y soltar: Anfitrión (host) a invitado (máquina virtual).



Es muy importante que no se elijan las opciones “Invitado a anfitrión” ni “bidireccional” ya que estas opciones permiten transmitir archivos de la máquina virtual a la máquina host, lo lógico es que ningún archivo de la Sandbox se cuele a la máquina host evitando así la propagación de malware a nuestro equipo personal.

Deshabilitar Microsoft defender


Nos dirigimos a la opción “**Configuración de antivirus y protección contra amenazas**” y elegimos “**Administrar la configuración**”




Deshabilitamos las siguientes opciones:

Protección en tiempo real


Busca malware e impide que se instale o ejecute en tu dispositivo. Puedes desactivar esta opción durante un breve período de tiempo antes de que se vuelva a activar automáticamente.

 La protección en tiempo real está desactivada, lo que hace que tu dispositivo sea vulnerable.

 Desactivado

Protección basada en la nube


Proporciona una protección mayor y más rápida con acceso a los datos más recientes de protección en la nube. Funciona mejor cuando el envío automático de muestras está activado.

 La protección basada en la nube está desactivada. El dispositivo podría ser vulnerable. [Descartar](#)

 Desactivado

Envío de muestras automático

Envía archivos de muestra a Microsoft para ayudar a protegerte a ti y a otras personas de posibles amenazas. Te preguntaremos si el archivo que necesitamos podría contener información personal.


 El envío de muestras automático está desactivado. El dispositivo puede estar en peligro. [Descartar](#)

 Desactivado

[Enviar una muestra manualmente](#)

Protección contra alteraciones

Impide que otras personas alteren características de seguridad importantes.

 La protección contra alteraciones está desactivada. El dispositivo podría estar en peligro. [Descartar](#)

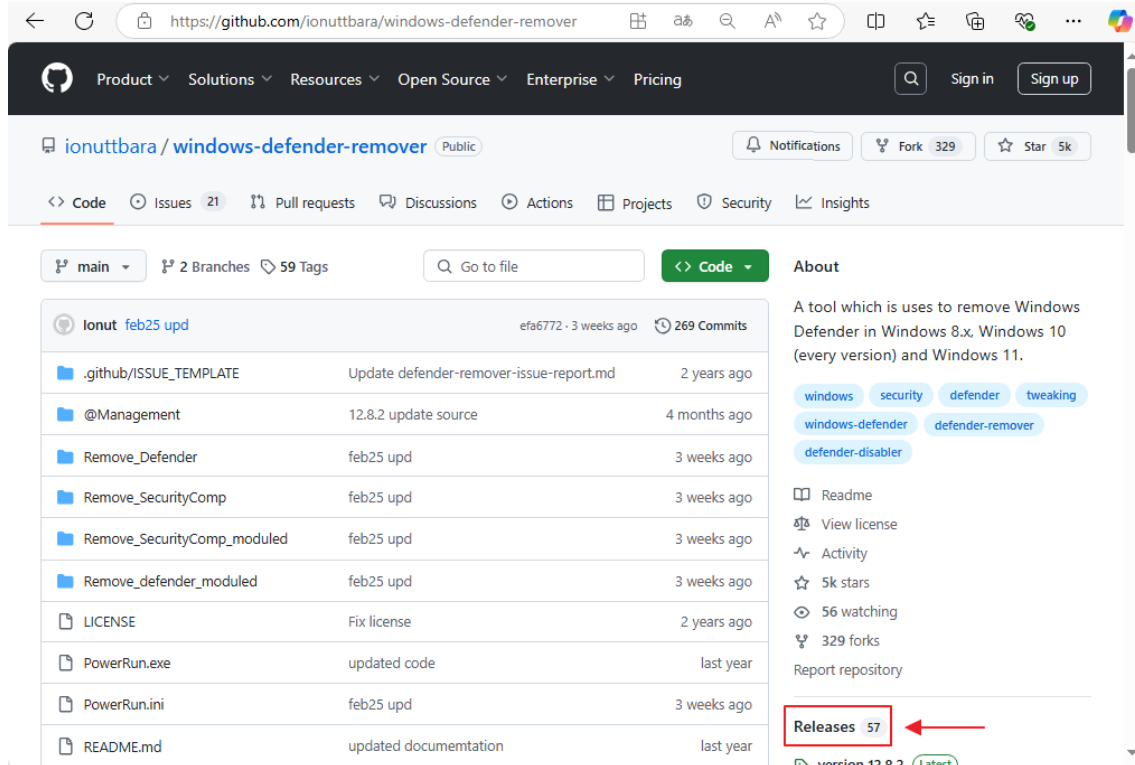
 Desactivado

[Más información](#)

Desinstalar Microsoft defender

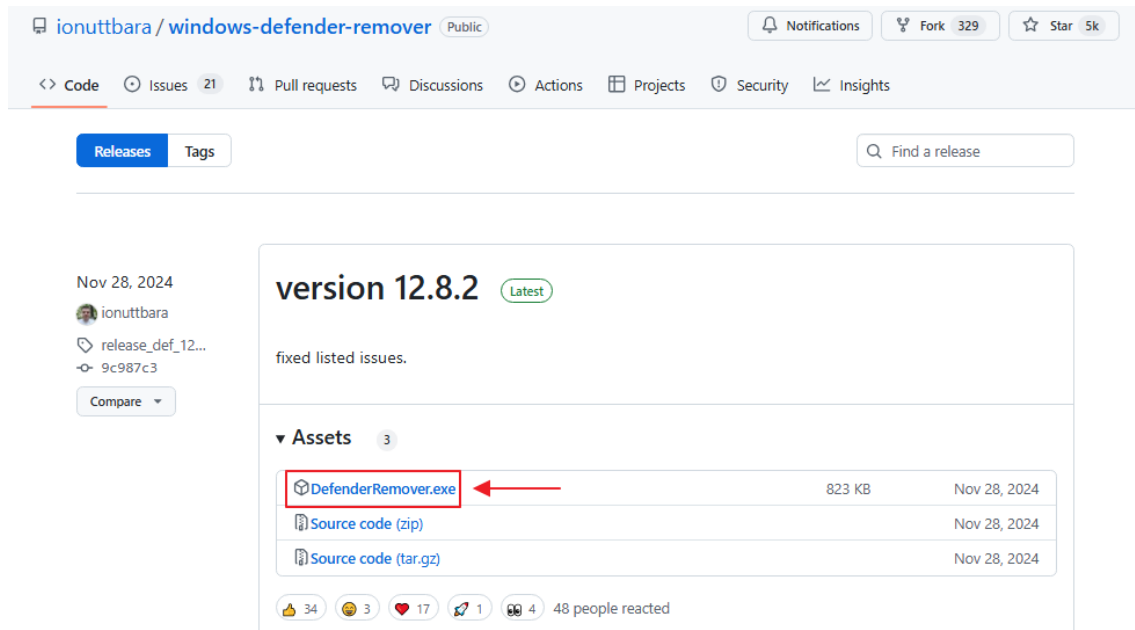
Para desinstalar por completo Microsoft Defender nos bajaremos de GitHub la herramienta **DefenderRemover.exe**

Link: <https://github.com/ionuttbara/windows-defender-remover>



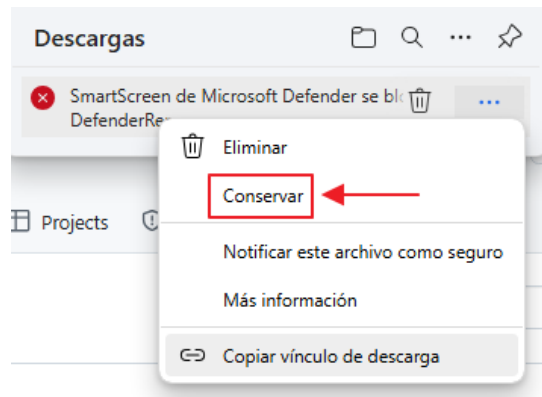
The screenshot shows the GitHub repository page for `ionuttbara/windows-defender-remover`. The repository is public and has 329 forks and 5k stars. The 'Releases' section in the right sidebar is highlighted with a red box and a red arrow, indicating the location to download the tool.

Descargar el .exe

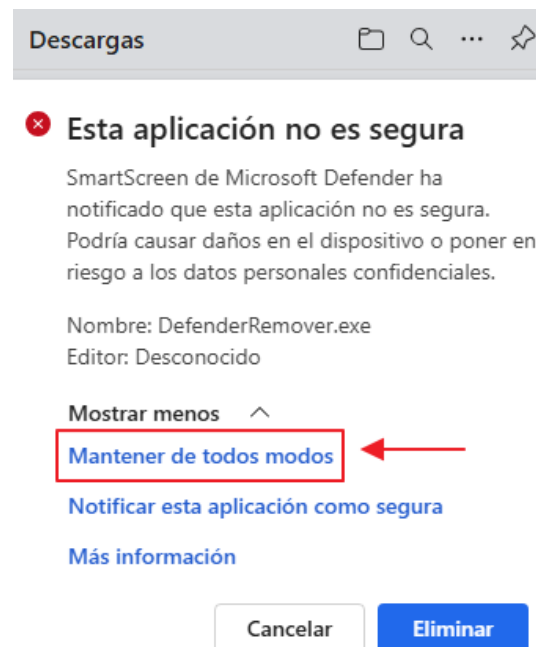


The screenshot shows the GitHub release page for version 12.8.2 of the `windows-defender-remover`. The release is labeled 'Latest' and includes a description: 'fixed listed issues.' The 'Assets' section lists three files: `DefenderRemover.exe` (823 KB, Nov 28, 2024), `Source code (zip)` (Nov 28, 2024), and `Source code (tar.gz)` (Nov 28, 2024). The `DefenderRemover.exe` file is highlighted with a red box and a red arrow.

Nos saltará el aviso el cual Microsoft Defender nos indica que se trata de un archivo no seguro.
Para continuar con la descarga seleccionar los 3 puntos y elegir conservar el archivo:

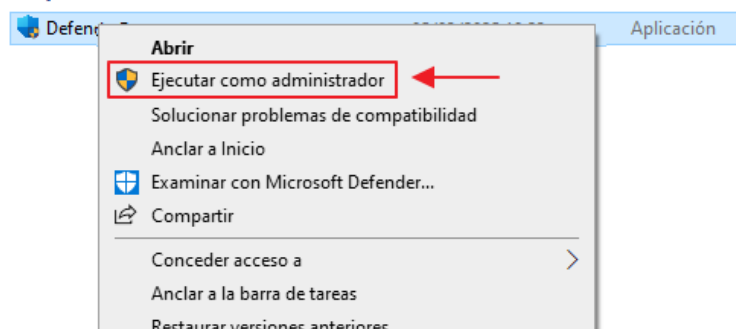


Nos saltará una segunda ventana de alerta y seleccionamos “Mostrar más” eligiendo la opción “Mantener de todos modos”:



Una vez hecho esto por fin tendremos descargado el archivo DefenderRemove.exe

Ahora procedemos a ejecutar el archivo como administrador:



Y se nos abrirá la siguiente ventana:



Para continuar con la instalación del programa deberemos seleccionar “Más información” y elegir la opción “ejecútalo de todos modos”:



Una vez abierto el ejecutable elegiremos la opción “Y” eliminar Windows Defender Antivirus y deshabilitar todas las notificaciones de seguridad.

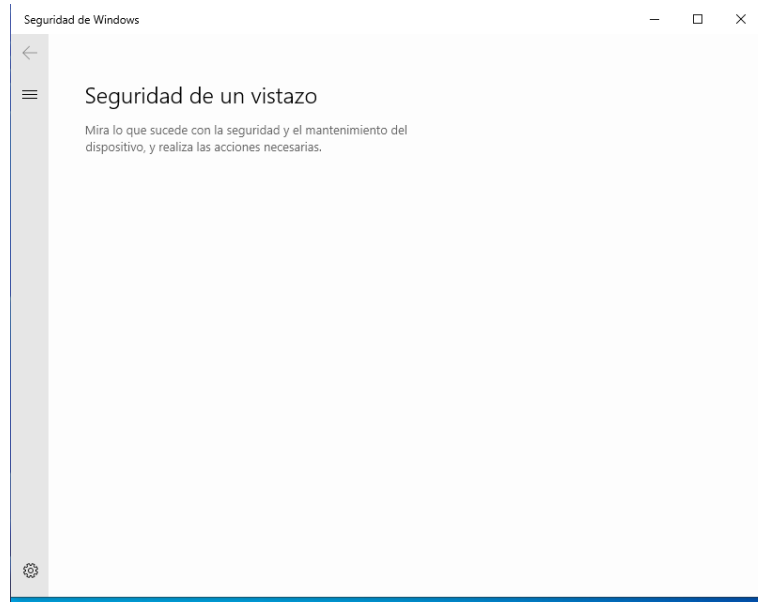
```

C:\Windows\system32\cmd.exe
----- Defender Remover Script , version 12.8.2 -----
Select an option:

Do you want to remove Windows Defender and alongside components? After this you'll need to reboot.
If you PC have a Microsoft Pluton Chip, you can disable from BIOS anytime. (This script removes the integration of Pluton
Chip Support and Processing from Windows.)
After confirmation of Removal, your Device will RESTART!!
A backup and/or System Restore point is recommended.
[Y] Remove Windows Defender Antivirus + Disable All Security Mitigations
[A] Remove Windows Defender only, but keep UAC Enabled
[S] Disable All Security Mitigations
  
```

El ejecutable empezará con el proceso de eliminación de Windows Defender y una vez finalizado la máquina se reiniciará.

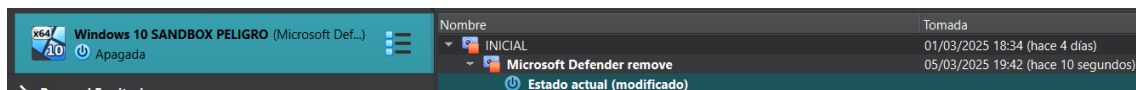
Una vez reiniciada la máquina nos dirigimos a Privacidad y seguridad en Windows y podemos observar que la opción de seguridad ya no aparece.



Segunda instantánea de la máquina en VirtualBox

En este momento una vez eliminado Microsoft Defender procedemos a realizar una segunda instantánea del equipo para tener un punto de guardado y no perder el progreso anterior en el caso de que queramos probar otro malware.

Importante: realizar la instantánea del equipo con la máquina apagada para que pese menos.



Instalación de herramientas

Autoruns

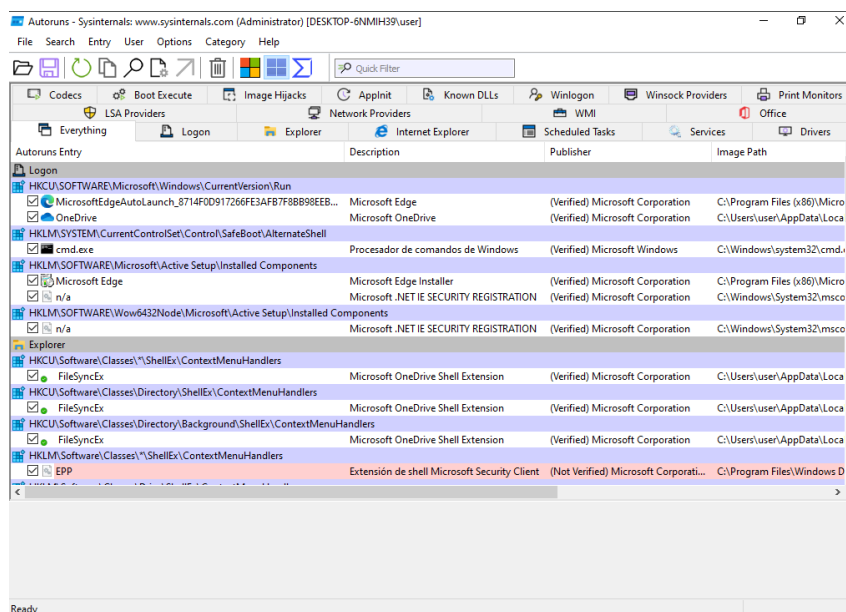
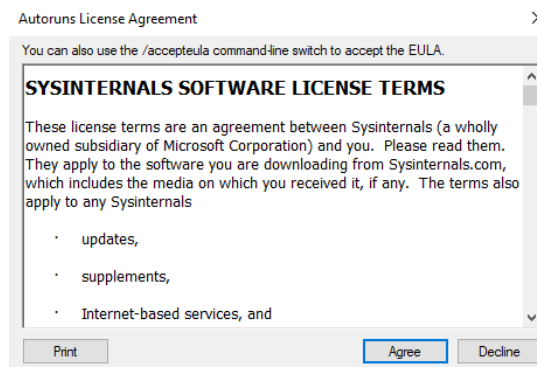
Esta herramienta de Sysinternals permite ver y gestionar todos los programas que se ejecutan automáticamente al iniciar Windows. Muestra las aplicaciones, controladores y servicios que se inician con el sistema operativo, tanto en el registro como en otros lugares. Es útil para deshabilitar programas no deseados o para analizar posibles malware que se inicie automáticamente.

Link: <https://download.sysinternals.com/files/Autoruns.zip>

Nos descargará un fichero .Zip el cual podremos ubicar donde queramos y ejecutaremos el archivo .exe para iniciar la herramienta.

Nombre	Fecha de modificación	Tipo	Tamaño
autoruns	05/03/2025 19:50	Archivo de Ayuda ...	25 KB
Autoruns	05/03/2025 19:50	Aplicación	1.718 KB
Autoruns64	05/03/2025 19:50	Aplicación	1.910 KB
Autoruns64a	05/03/2025 19:51	Aplicación	2.030 KB
autorunsc	05/03/2025 19:50	Aplicación	702 KB
autorunsc64	05/03/2025 19:50	Aplicación	786 KB
autorunsc64a	05/03/2025 19:51	Aplicación	808 KB
Eula	05/03/2025 19:51	Documento de te...	8 KB

En la primera ejecución seleccionamos “Agree” aceptando los términos uso y licencia.



TCPView

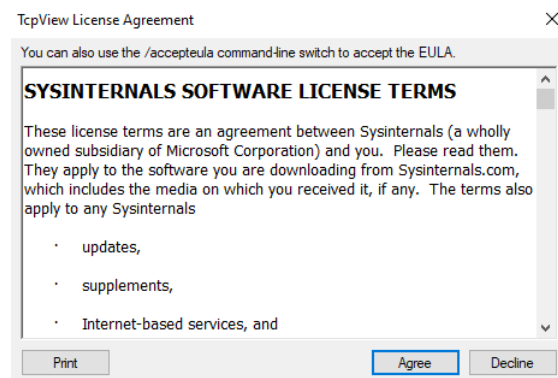
Esta herramienta muestra todas las conexiones TCP y UDP activas en tu equipo. Ofrece información sobre las direcciones IP locales y remotas, puertos y el estado de cada conexión. Es útil para monitorear la actividad de red, detectar conexiones sospechosas o verificar el tráfico de datos.

Link: <https://download.sysinternals.com/files/TCPView.zip>

Nos descargará un fichero .Zip el cual podremos ubicar donde queramos y ejecutaremos el archivo .exe para iniciar la herramienta.

Eula	05/03/2025 19:59	Documento de te...	8 KB
tcpvcon	05/03/2025 19:59	Aplicación	198 KB
tcpvcon64	05/03/2025 19:59	Aplicación	245 KB
tcpvcon64a	05/03/2025 19:59	Aplicación	232 KB
tcpview	05/03/2025 19:59	Archivo de Ayuda ...	16 KB
tcpview	05/03/2025 19:59	Aplicación	923 KB
tcpview64	05/03/2025 19:59	Aplicación	1.062 KB
tcpview64a	05/03/2025 19:59	Aplicación	1.020 KB

En la primera ejecución seleccionamos “Agree” aceptando los términos uso y licencia.



TCPView - Sysinternals: www.sysinternals.com

File Edit View Process Connection Options Help

Process Name Process ID Protocol State Local Address Local Port Remote Address Remote Port Create Time

svchost.exe	948	TCP	Listen	0.0.0.0	135	0.0.0.0	0	05/03/2025 19:4
System	4	TCP	Listen	10.0.2.15	139	0.0.0.0	0	05/03/2025 19:4
svchost.exe	4164	TCP	Listen	0.0.0.0	5040	0.0.0.0	0	05/03/2025 19:4
lsass.exe	716	TCP	Listen	0.0.0.0	49664	0.0.0.0	0	05/03/2025 19:4
wininit.exe	548	TCP	Listen	0.0.0.0	49665	0.0.0.0	0	05/03/2025 19:4
svchost.exe	1188	TCP	Listen	0.0.0.0	49666	0.0.0.0	0	05/03/2025 19:4
svchost.exe	1196	TCP	Listen	0.0.0.0	49667	0.0.0.0	0	05/03/2025 19:4
spoolsv.exe	2632	TCP	Listen	0.0.0.0	49668	0.0.0.0	0	05/03/2025 19:4
services.exe	692	TCP	Listen	0.0.0.0	49669	0.0.0.0	0	05/03/2025 19:4
svchost.exe	3028	TCP	Established	10.0.2.15	49675	4.207.247.139	443	05/03/2025 19:4
svchost.exe	3028	TCP	Established	10.0.2.15	49726	4.207.247.139	443	05/03/2025 19:4
msedge.exe	4212	TCP	Established	10.0.2.15	49821	4.209.164.61	443	05/03/2025 19:5
msedge.exe	4212	TCP	Established	10.0.2.15	49824	172.205.80.42	443	05/03/2025 19:5
msedge.exe	4212	TCP	Established	10.0.2.15	49825	4.231.66.184	443	05/03/2025 19:5
[Time Wait]		TCP	Time Wait	10.0.2.15	49828	151.101.134.172	80	
SearchApp.exe	6956	TCP	Established	10.0.2.15	49829	204.79.197.203	443	05/03/2025 20:0
[Time Wait]		TCP	Time Wait	10.0.2.15	49830	204.79.197.203	443	
[Time Wait]		TCP	Time Wait	10.0.2.15	49835	108.157.96.79	443	
msedgeview2.exe	8168	TCP	Established	10.0.2.15	49839	13.74.129.1	443	05/03/2025 20:0
msedgeview2.exe	8168	TCP	Established	10.0.2.15	49840	204.79.197.203	443	05/03/2025 20:0
msedgeview2.exe	8168	TCP	Established	10.0.2.15	49842	52.182.143.209	443	05/03/2025 20:0
msedgeview2.exe	8168	TCP	Close Wait	10.0.2.15	49844	2.20.187.32	443	05/03/2025 20:0
msedgeview2.exe	8168	TCP	Close Wait	10.0.2.15	49846	23.62.180.221	443	05/03/2025 20:0
msedgeview2.exe	8168	TCP	Established	10.0.2.15	49847	150.171.27.10	443	05/03/2025 20:0
msedgeview2.exe	8168	TCP	Established	10.0.2.15	49849	150.171.27.10	443	05/03/2025 20:0
msedgeview2.exe	8168	TCP	Established	10.0.2.15	49851	2.23.28.182	443	05/03/2025 20:0
msedgeview2.exe	8168	TCP	Close Wait	10.0.2.15	49852	2.23.28.182	443	05/03/2025 20:0
[Time Wait]		TCP	Time Wait	10.0.2.15	49853	151.101.134.172	80	
System	4	TCP	Listen	0.0.0.0	445	0.0.0.0	0	05/03/2025 19:4
svchost.exe	4768	TCP	Listen	0.0.0.0	7680	0.0.0.0	0	05/03/2025 19:4

Endpoints: 66 Established: 12 Listening: 20 Time Wait: 4 Close Wait: 3 Update: 2 sec States: (All)

ProcExp (Process Explorer)

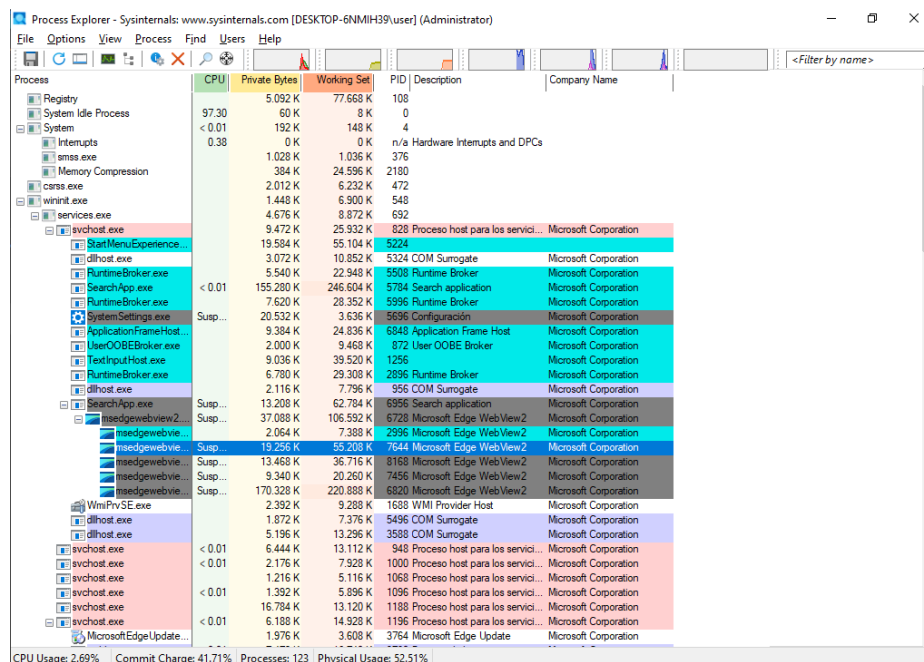
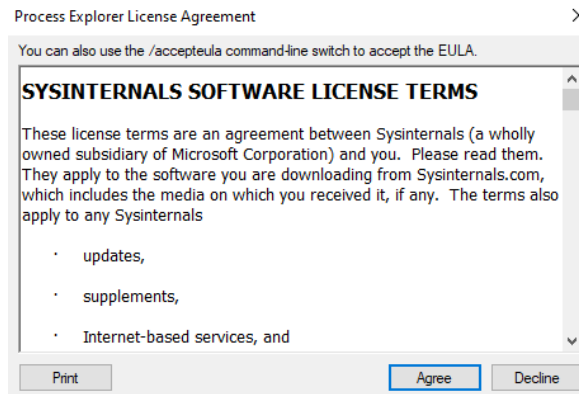
Esta herramienta avanzada permite ver y gestionar todos los procesos en ejecución en tu computadora, ofreciendo detalles más completos que el Administrador de tareas. Muestra qué archivos y claves de registro están siendo utilizados por cada proceso, lo que facilita la identificación de procesos maliciosos o no deseados.

Link: <https://download.sysinternals.com/files/ProcessExplorer.zip>

Nos descargará un fichero .Zip el cual podremos ubicar donde queramos y ejecutaremos el archivo .exe para iniciar la herramienta.

Eula	05/03/2025 20:04	Documento de te...	8 KB
procexp	05/03/2025 20:04	Aplicación	4.425 KB
procexp64	05/03/2025 20:04	Aplicación	2.326 KB
procexp64a	05/03/2025 20:04	Aplicación	2.334 KB

En la primera ejecución seleccionamos “Agree” aceptando los términos uso y licencia.



Conclusión

En esta guía hemos aprendido cómo configurar un entorno seguro y controlado en una máquina virtual utilizando VirtualBox para el análisis de software malicioso. A lo largo de los pasos, se ha hecho énfasis en la importancia de proteger la máquina anfitriona y evitar cualquier posible propagación de malware. La creación de una Sandbox adecuada implica el uso de configuraciones cuidadosas, como la generación de credenciales aleatorias y el uso de una cuenta local, además de deshabilitar medidas de seguridad como Microsoft Defender para prevenir interferencias durante el análisis.

Asimismo, hemos instalado y configurado herramientas esenciales como Autoruns, TCPView y Process Explorer, que permiten monitorear y gestionar el comportamiento del sistema durante el análisis. Al tomar precauciones adicionales, como la creación de instantáneas antes y después de realizar cambios importantes, aseguramos que siempre podamos revertir cualquier alteración indeseada y mantener un entorno limpio para futuros estudios.

Este proceso es una excelente manera de analizar malware de forma segura y responsable, sin comprometer los sistemas principales. No obstante, siempre debemos ser conscientes de la responsabilidad que implica manejar este tipo de conocimiento y utilizarlo exclusivamente con fines educativos y éticos.

Agradecimientos

Quiero agradecer a:

- **Mark Russinovich**, autor de la suite Sysinternals, cuyas herramientas como Autoruns, TCPView y Process Explorer son esenciales para el análisis de sistemas.
- **Nate Gentile**, youtuber especializado en tecnología, por su contenido educativo y accesible que ha sido de gran ayuda en el aprendizaje del sector.
- **Marc Rivero López**, experto en ciberseguridad, por su experiencia y enfoque en la protección de sistemas y redes, enriqueciendo nuestra comprensión de la ciberseguridad.