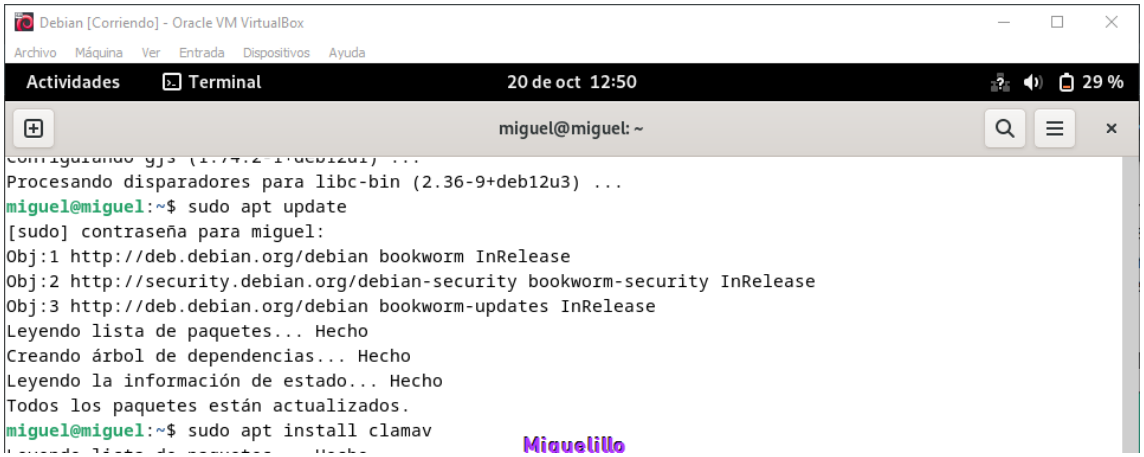
Índice:

Ejercicio 1

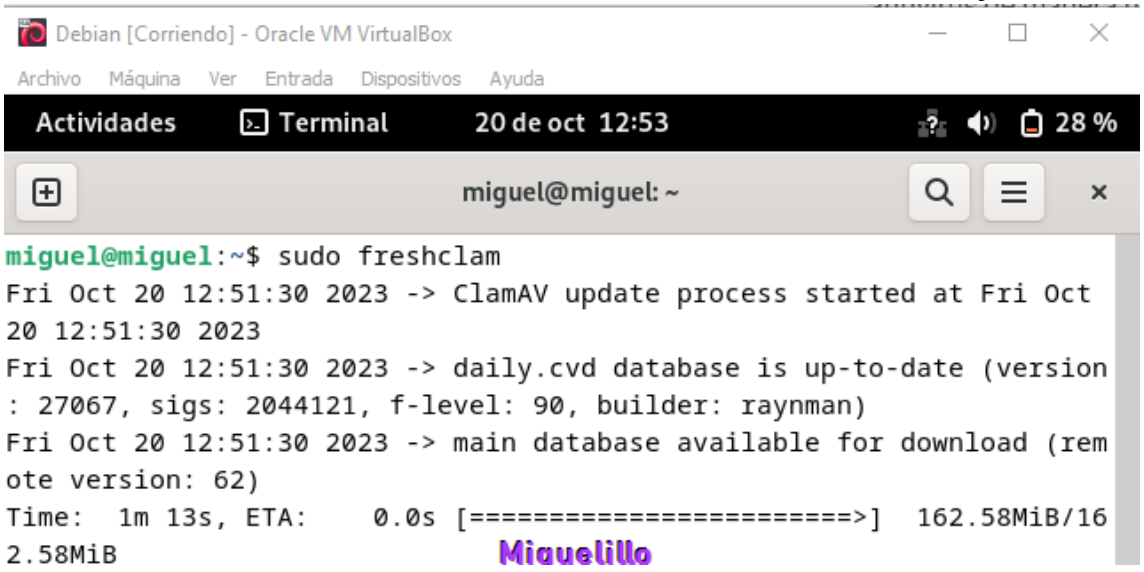
a) Instala en GNU/Linux el antivirus ClamAV, y su versión gráfica Clamtk

Solución:

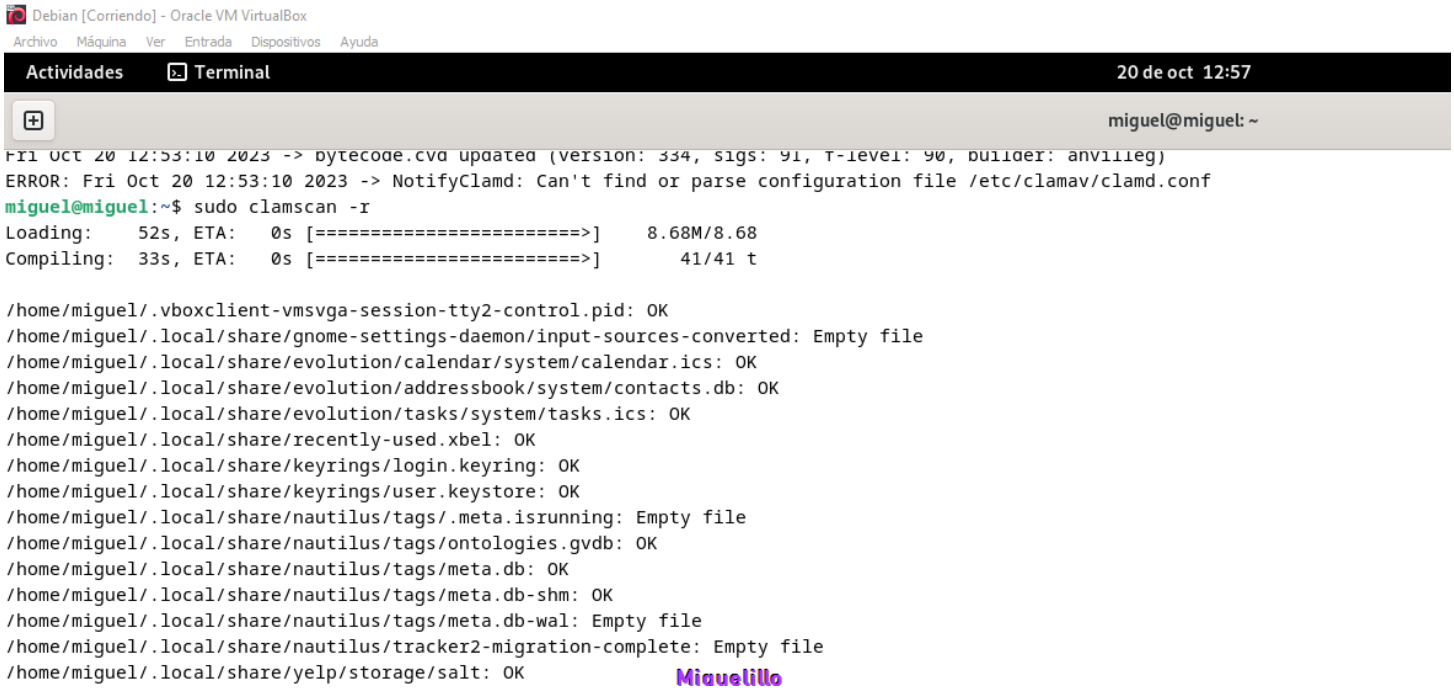
Hacemos un *sudo apt update* y un *sudo apt upgrade* para instalarlo sudo apt install clamav



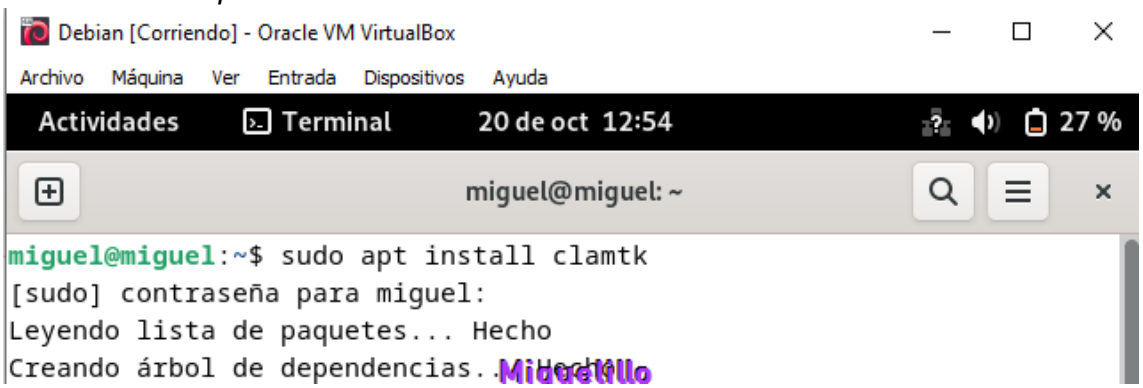
Para actualizar la base de datos de clamv hacemos un *sudo freshclam*

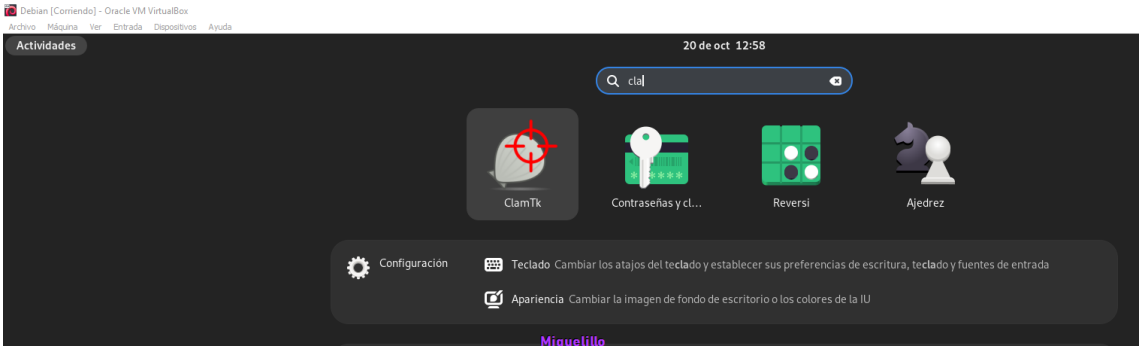


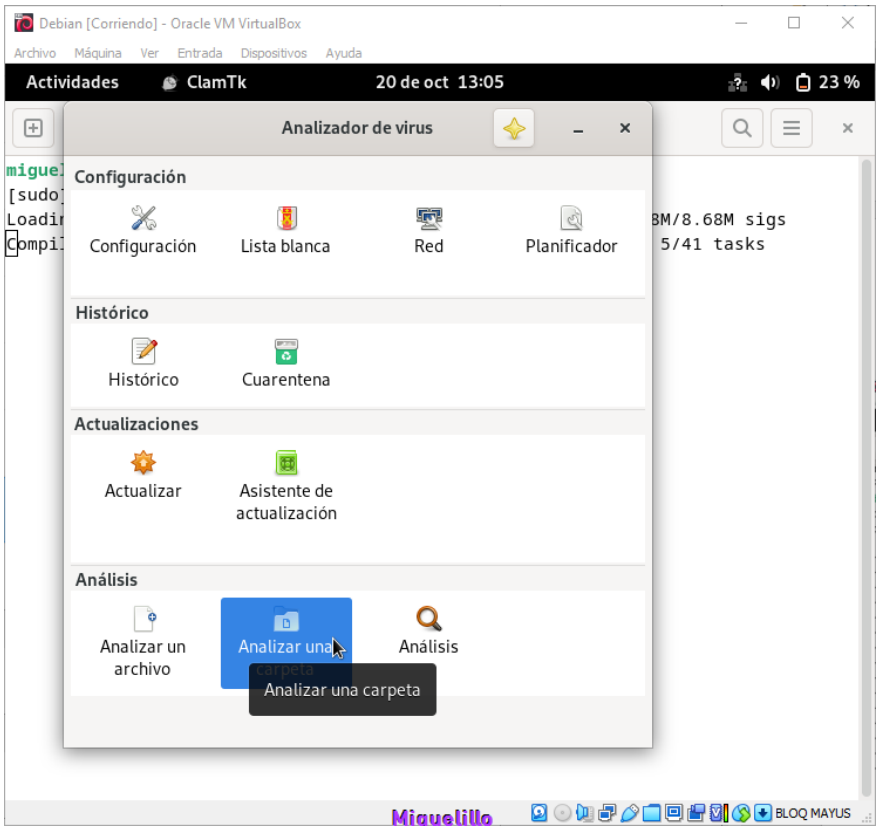
Para hacer un escaneo hacemos *sudo clamscan -r /*



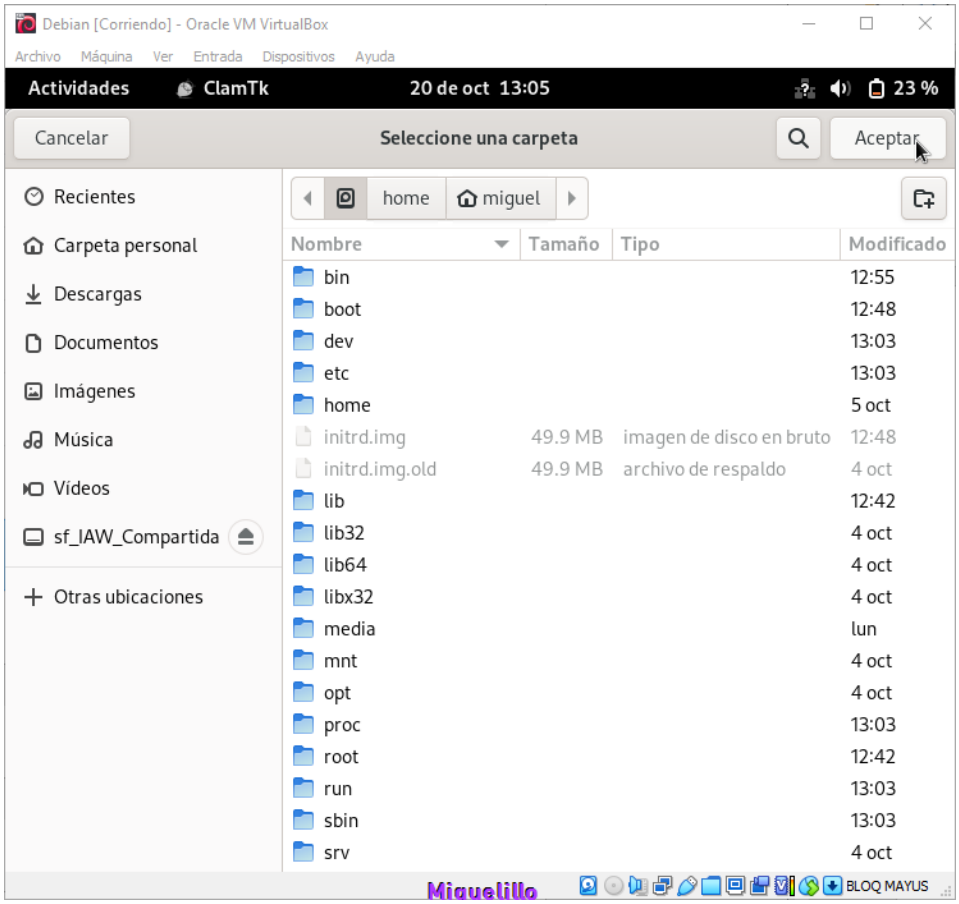
Hacemos un *sudo apt update* y un *sudo apt upgrade* para instalarlo Clamtk *sudo apt install clamtk*



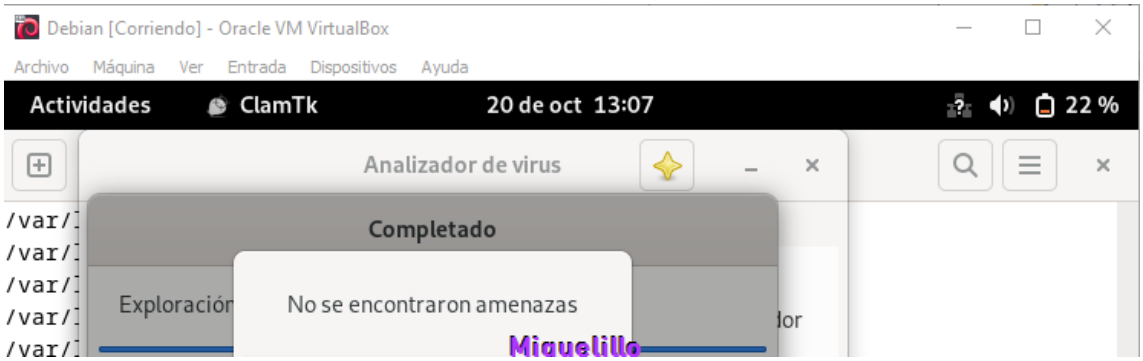




Nos vamos a / y le damos a Aceptar



Se finalizany no hay amenaza



b) Investiga en Internet el término: Spyware

Solución:

El spyware es un malware que se instala en un ordenador sin el conocimiento o el consentimiento del usuario. Su función principal es recopilar información personal o de navegación del usuario de manera secreta.

El spyware puede hacer que valla más lento el ordenador ya que consume recursos de ordenador, puede abrir puertos y dejar puertas traseras, recopilar información personal y sensible yalgunas veces incluyen addware.

Para eliminar el spyware escanear con software anti-spyware, actualiza tu software de seguridad, elimina extensiones sospechosas del navegador, en situaciones extremas restauramos el sistema

Podemos utilizar la extensión AdBlock, Windows Defender, malwarebytes:

c) Investiga en Internet el término Adware

Solución:

El "adware" es un tipo de malware que, a menudo, se instala en un ordenador sin el consentimiento del usuario y muestra anuncios publicitarios no deseados en forma de ventanas emergentes, banners, o redirecciones de navegador. El propósito principal del adware es generar ingresos para los desarrolladores al mostrar anuncios a los usuarios, pero puede ser molesto y perjudicial.

Los anuncios no deseados pueden interrumpir la experiencia del usuario y dificultar la navegación en línea, el adware puede consumir recursos del sistema y ralentizar el ordenador. adware pueden rastrear la actividad en línea del usuario, puede redirigir el tráfico web a sitios no deseados, potencialmente peligrosos.

Para eliminarlo podemos usar software anti-malware, actualiza tu software, elimina extensiones y programas no deseados, restaura la configuración del navegador, revisa las tareas programadas.

Aplicaciones antiadware

AdBlock Plus una extensión para un navegador , AdwCleaner eliminar adware y te previene de él también

d) Investiga en Internet el término : Hijacking

Solución:

Hijacking" se refiere a tomar control de un sistema sin permiso.los "Browser Hijackers" son malware que modifican tu navegador sin permiso.esto puede cambiar la página de inicio, redirigirte a sitios no deseados y afectar tu privacidad.

Efectos sobre el sistema cambios no deseados modifican la configuración del navegador sin consentimiento, lo que puede ser molesto y dificultar la navegación en línea, redirección de direcciones no deseadas: Pueden redirigir al usuario a sitios web no deseados, incluyendo sitios maliciosos. Al cambiar la configuración del navegador, los browser hijackers pueden poner en riesgo la privacidad y la seguridad del usuario.

Para eliminar Pharming podemos usar software como OpenDNS o Norton 360 y Norton Internet Security. Cosas como verificar el DNS y usar uno confiable como el 8.8.8.8 ayuda a evitarlos.

Para prevenir Hijacking podemos usar Bitdefender, Kaspersky, Norton y Malwarebytes. extensiones de navegador, como "NoScript" o "HTTPS Everywhere",

e) Investiga en Internet los términos: Keyloggers y Stealers

Solución:

Los keyloggers son programas maliciosos diseñados para registrar todas las pulsaciones de teclado de un usuario sin su conocimiento. Los stealers son tipos de malware diseñados para robar contraseñas almacenadas en un sistema. Esto incluye contraseñas guardadas en navegadores web, programas de correo electrónico y otros servicios.

Sobre el sistema

Los keyloggers pueden registrar credenciales de inicio de sesión, números de tarjeta de crédito y otra información personal, lo que puede dar lugar a robos de identidad y fraudes. El uso de keyloggers compromete la privacidad del usuario, ya que todo lo que se escribe en el teclado puede ser registrado y utilizado en su contra.

Sobre el sistema

Pueden robar contraseñas almacenadas en tu sistema, lo que puede dar a los atacantes acceso a tus cuentas en línea.

Los atacantes pueden acceder a tu información personal y datos sensibles.

Software para detectarlos Malwarebytes, SpyShelter, BitDefender y AVG

f) Investiga en Internet los términos: Botnets, Rogue, y Criptovirus

Solución:

Un botnet es una red de dispositivos infectados por malware que son controlados de manera remota por un atacante.

El término "Rogue" se utiliza para describir programas o aplicaciones falsas que se hacen pasar por software legítimo pero en realidad son maliciosos.

Los criptovirus son un tipo de malware que cifra los archivos del usuario y exige un rescate para desbloquearlos.

Para eliminar un botnet, es importante desinfectar todos los dispositivos infectados. Esto suele requerir la ejecución de un software antivirus actualizado y la eliminación de archivos y procesos maliciosos. En casos muy extremos formatear el equipo.

Para eliminar software Rogue, se recomienda el uso de un programa antivirus o antimalware confiable

La eliminación de criptovirus puede ser complicada. Lo ideal es prevenir la infección mediante la adopción de buenas prácticas de seguridad, como realizar copias de seguridad regulares. Si ya estás infectado, es importante no pagar el rescate y buscar herramientas de desencriptación gratuitas si están disponibles. También puedes utilizar programas antimalware para eliminar el ransomware.

Para evitar bot net TOTALAV, Bitdefender Windows Defender

Para evitar cripto virus Kaspersky Avast etc.

Para evitar criptovirus panda AVG Norton

g) Investiga en Internet información sobre el fichero autorun.inf que poseen los dispositivos de almacenamiento

Solución:

El archivo llamado autorun.inf se usa en dispositivos extraíbles que se utiliza para indicar al sistema cómo comportarse al insertar el dispositivo. Sin embargo, algunos tipos de malware se camuflan y propagan a través de este archivo.

El malware puede copiar su propio ejecutable en el dispositivo de almacenamiento y modificar el archivo autorun.inf para que ejecute automáticamente el malware cuando se inserta el dispositivo en una computadora.

Eliminar este malware puede ser un proceso delicado, pero desactivar la función "Autorun" en el Panel de control de Windows y utilizar un software antivirus actualizado son pasos clave. Eliminar el archivo autorun.inf También es importante realizar análisis de seguridad en busca de malware.

Efectos en el sistema

- Infección del sistema operativo y robo de información confidencial.
- Ralentización del sistema debido a la carga adicional del malware en segundo plano.
- Bloqueo de acceso a archivos y carpetas.
- Realización de actividades maliciosas, como envío de spam o ataques DDoS.
- Dificultades en la eliminación del malware, ya que puede regenerarse o protegerse a sí mismo.

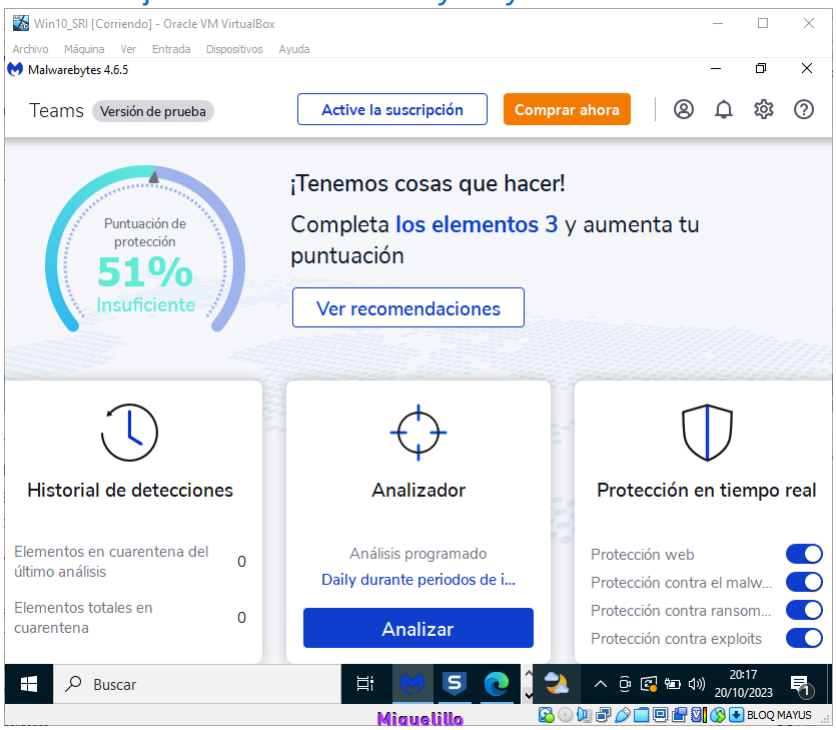
Antivirus o antimalware como Malwarebytes, AVG, Avast y Windows Defender, ofrecen protección en tiempo real y pueden ayudar a prevenir infecciones.

d) Instala y utiliza al menos dos herramientas de análisis antimalware, indicando en un informe que tipo de malware evitas.

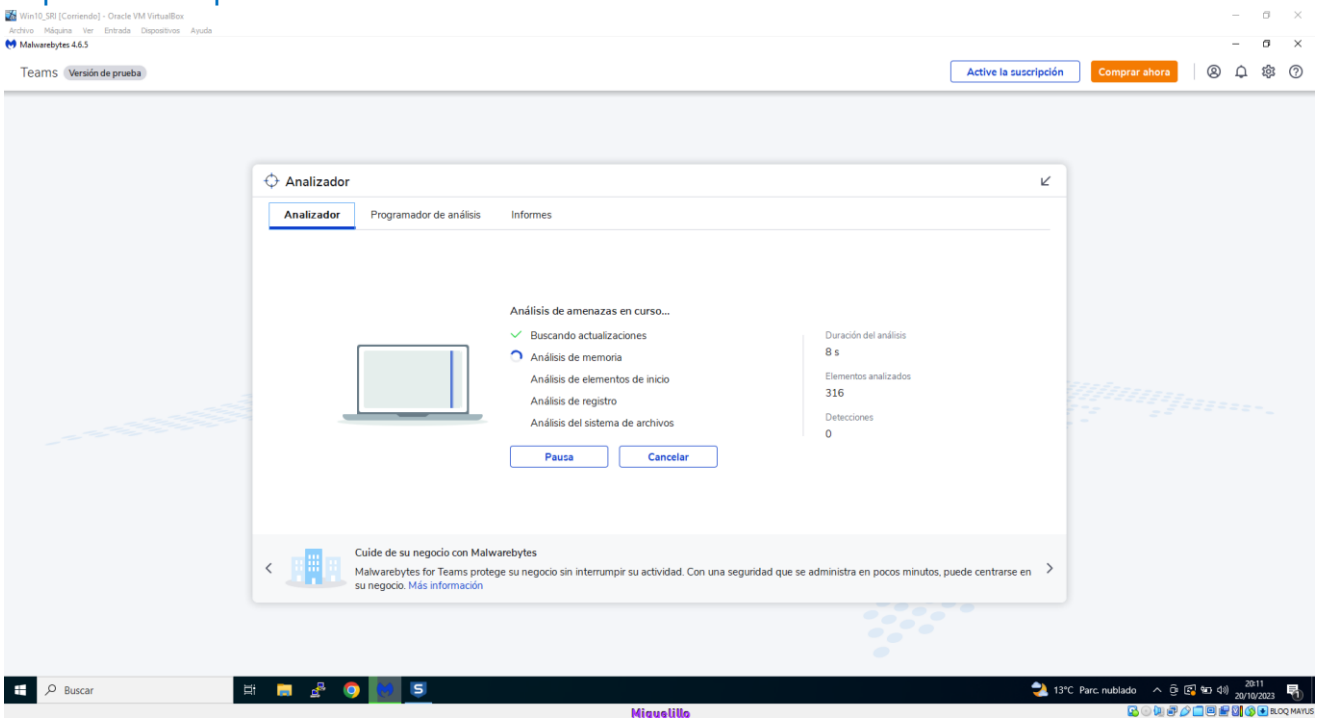
Solución

Malwarebytes

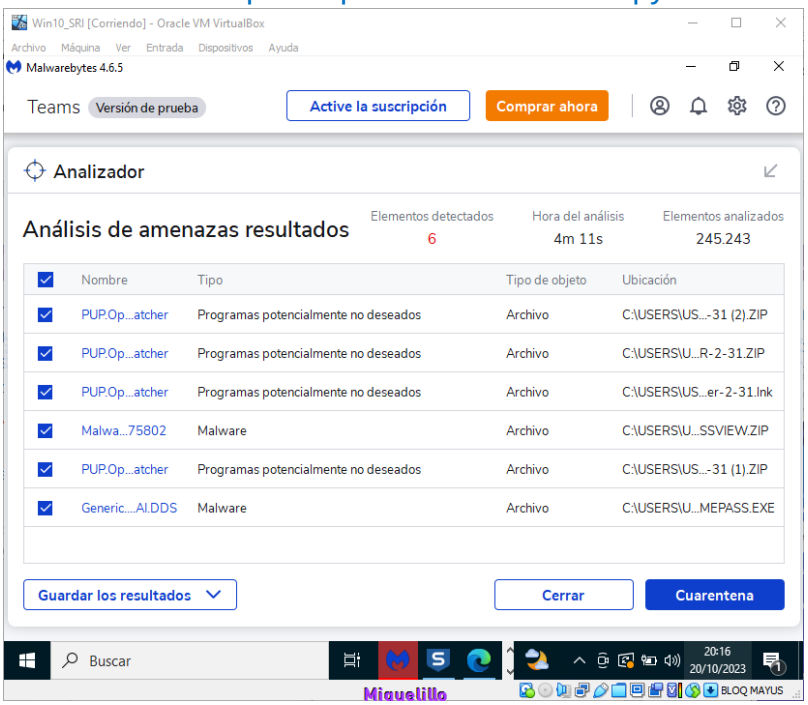
Primero ejecutamos malwarebytes y clicamos en **Escanear**



Esperamos a que se realice el escaneo



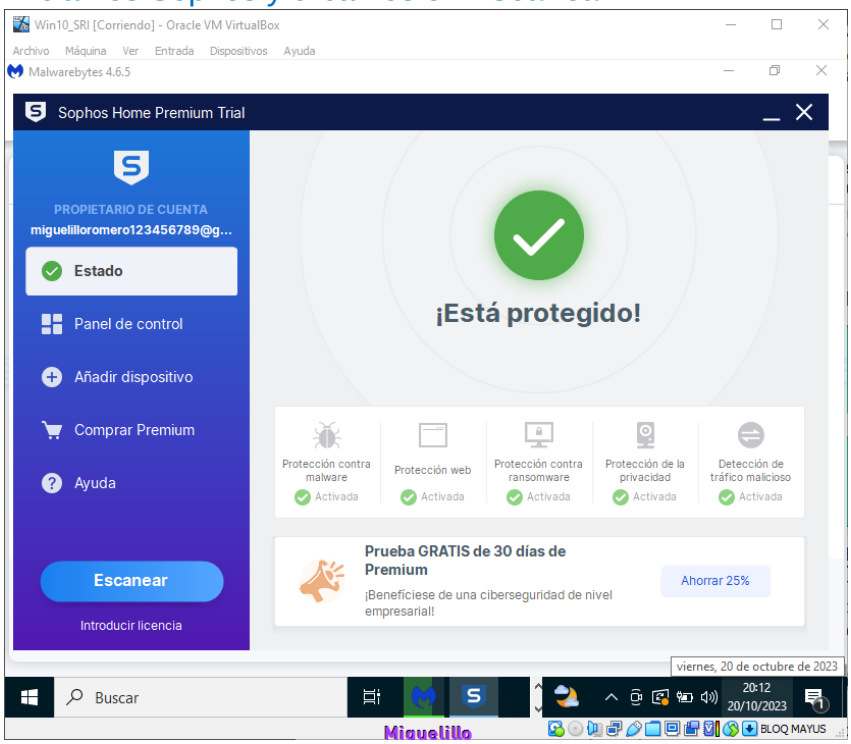
Ha detectado 6 Resultados que se tratan de herramientas muy intrusivas de análisis forense que se podrían usar como spyware en cierto modo.



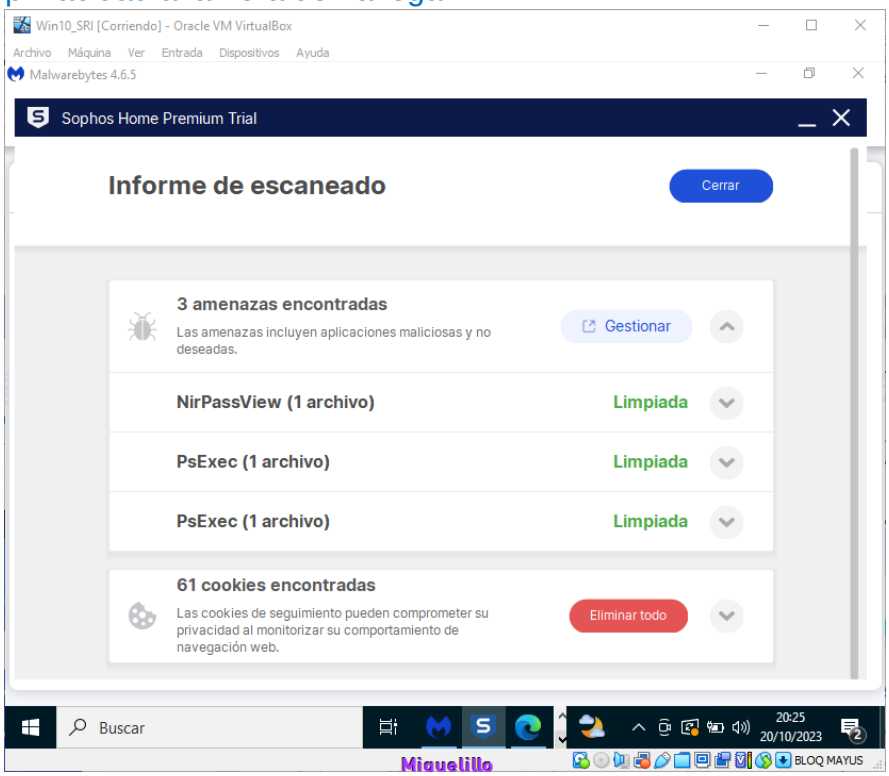
Con malwarebytes podemos evitar spywares, ransomwares, keyloggers y la mayoría de addwares mencionados anteriormente en la práctica ya que es un programa muy completo como hemos comprobado. Con el programa de la compañía “browser guard” añadiríamos una capa adición ya que nos detecta los sitios inseguros y evita Browser hijacker, addwares entre otros.

Sophos

Iniciamos Sophos y clicamos en **Escanear**



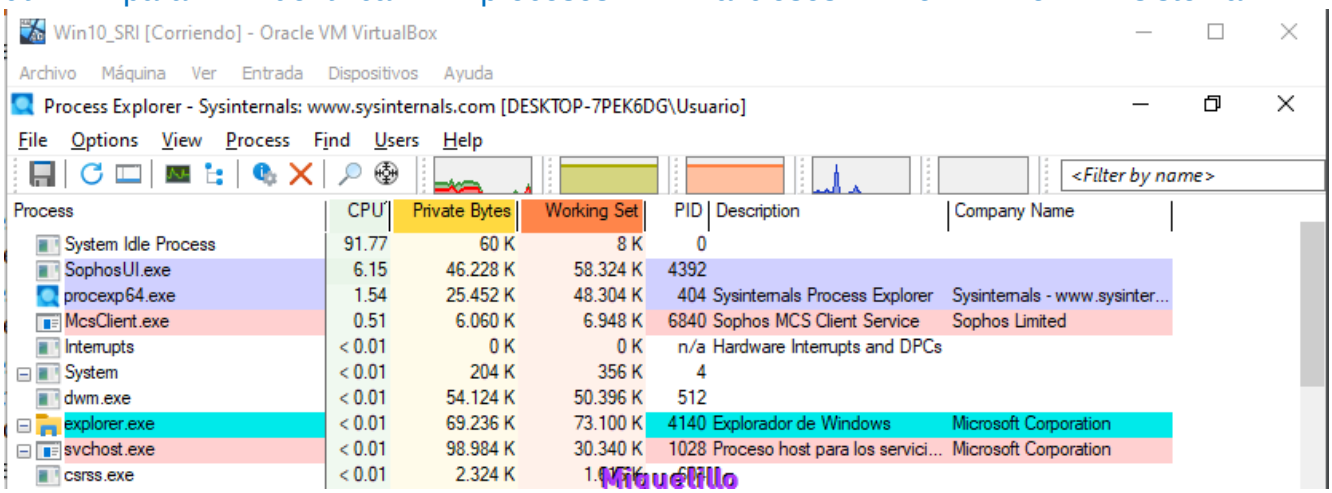
El resultado del análisis que nos ha mostrado las herramientas anteriormente citadas de analisi forense que eran intrusivas pero a diferencia de malware bits no se a metido a los zips, pero si que ha detectado cokies que podrían haberlas habilitado addwares o Browser hijackers que puenden comprometer la privacidad a la hora de navegar



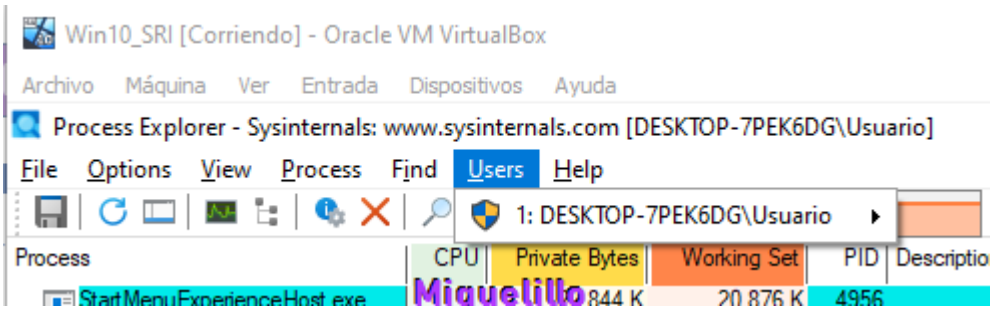
Sophos Home Free es una solución antivirus que ofrece una amplia gama de capacidades de detección y eliminación de malware. Este software puede detectar **Spyware Ransomware Troyanos Adware Rootkits Botnets,** en este caso hemos comprobado que para adwares podría servir bien ya que no ha advertido de esas cookies de seguimiento.

Sysinternals Suite

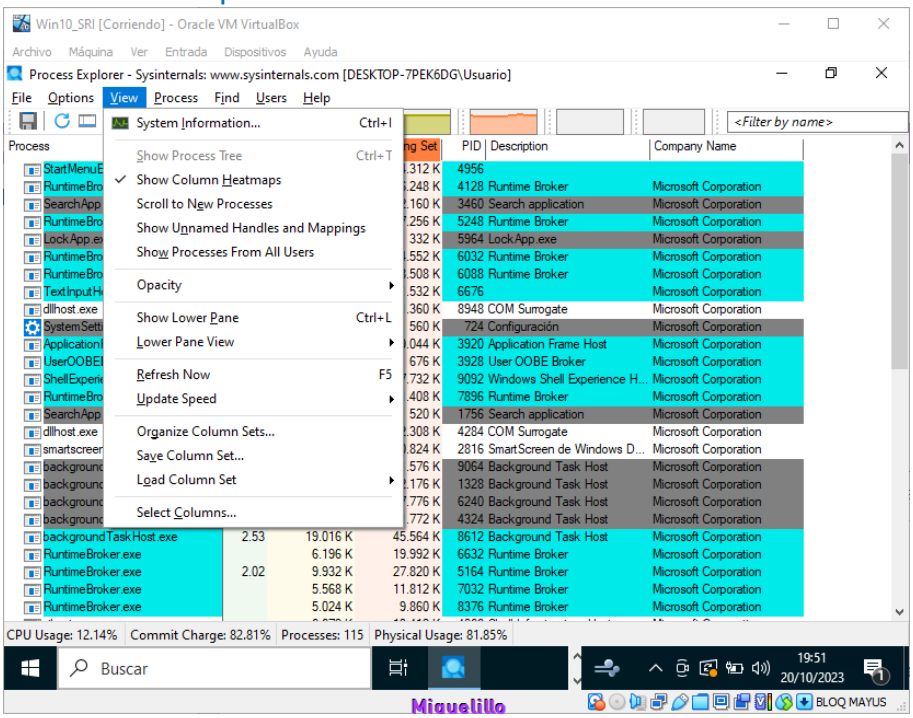
Process Explorer: Proporciona una vista detallada de los procesos en ejecución en el sistema, incluidos los procesos ocultos y los controladores del sistema. Esto puede ser útil para identificar procesos maliciosos en el sistema.



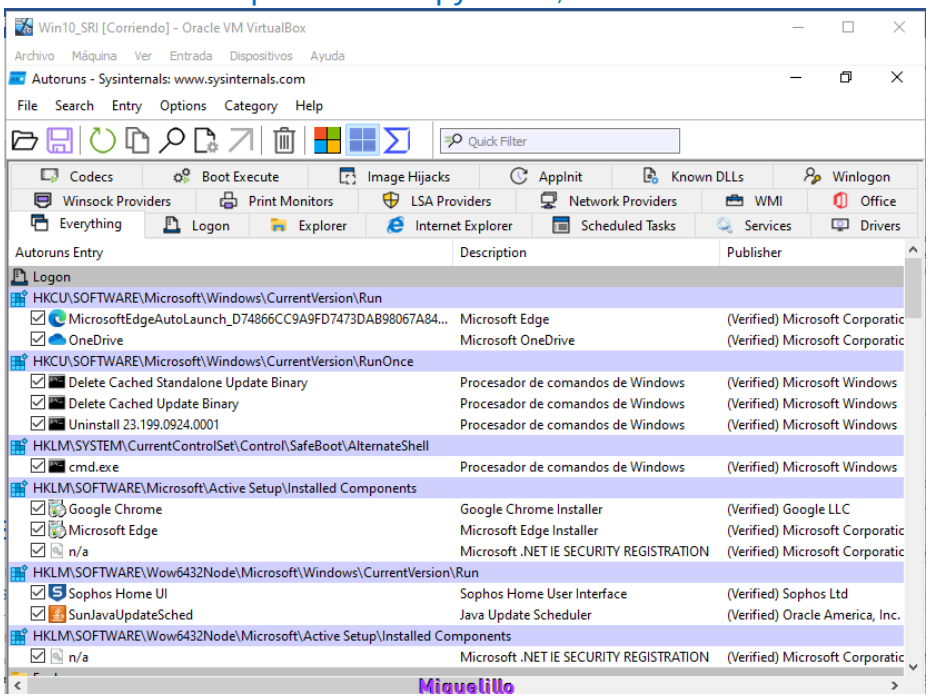
En **Users** podemos ver losusuario que hay actualmente ejecutando tareas



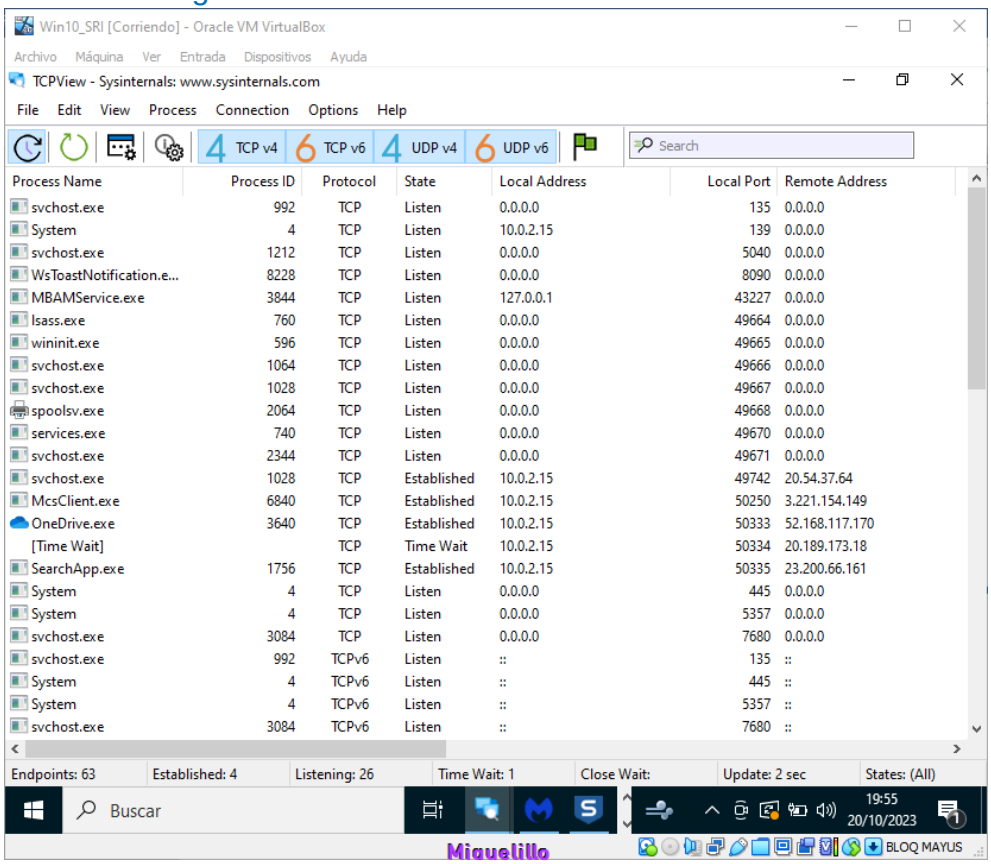
Para modificar podemos ir a **View**



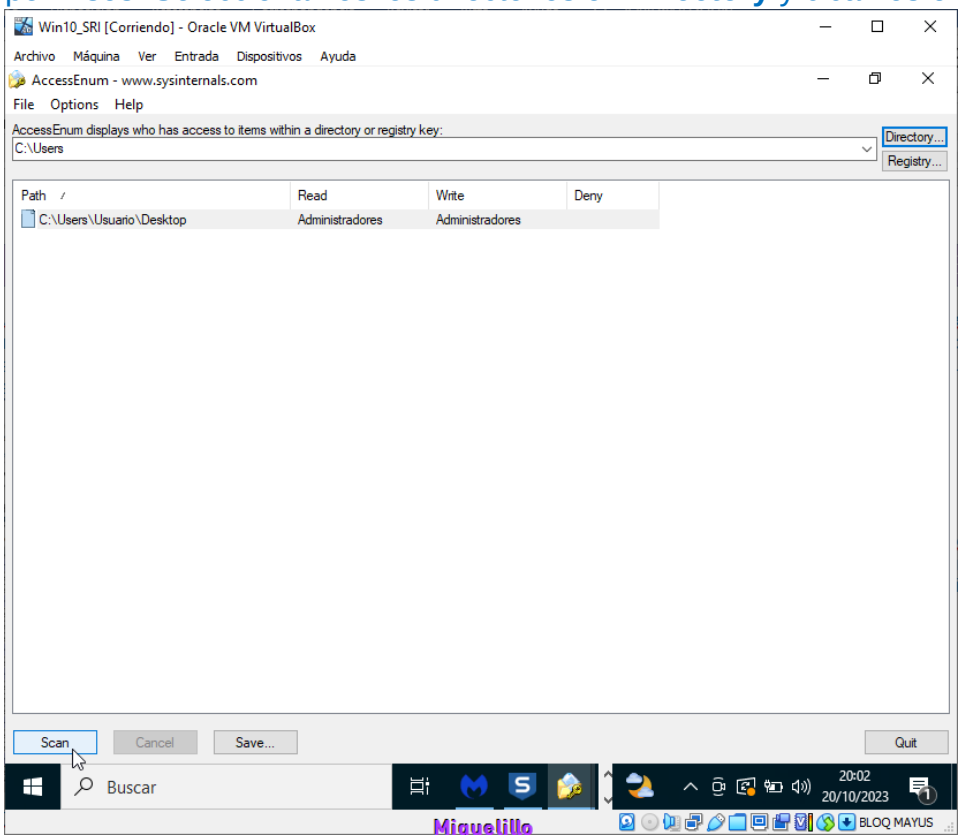
Autoruns: Ayuda a gestionar las aplicaciones y los componentes que se inician **automáticamente** cuando se enciende el sistema. Puede utilizarse para identificar y deshabilitar programas de inicio no deseados o potencialmente maliciosos como pueden ser spywares, addwares etc.



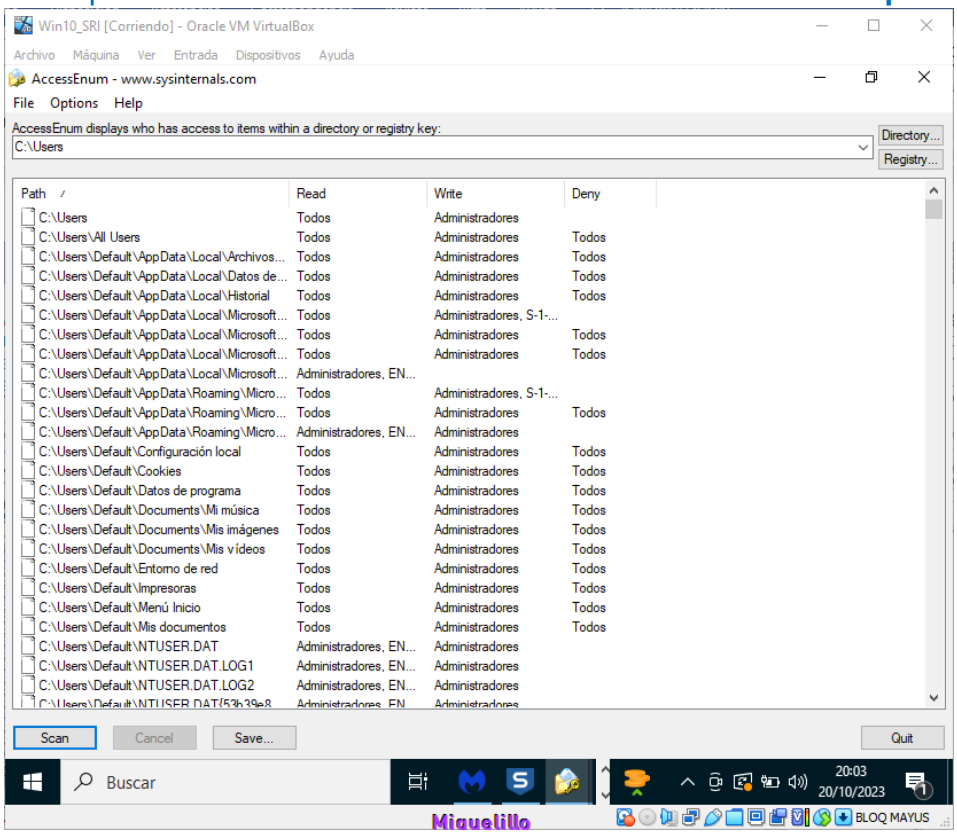
TCPView: Muestra las **conexiones** de **red activas** en el sistema, lo que permite identificar posibles conexiones no autorizadas o sospechosas. Podemos elegir entre **TCP o UDP e IPv6 o IPv4**



AccessEnum: Proporciona una vista **jerárquica** de los n y acceso a los **objetos** en el sistema, lo que ayuda a auditar la seguridad y la configuración de permisos. Seleccionamos los directorios en **Directory** y cicamos en **Scan**

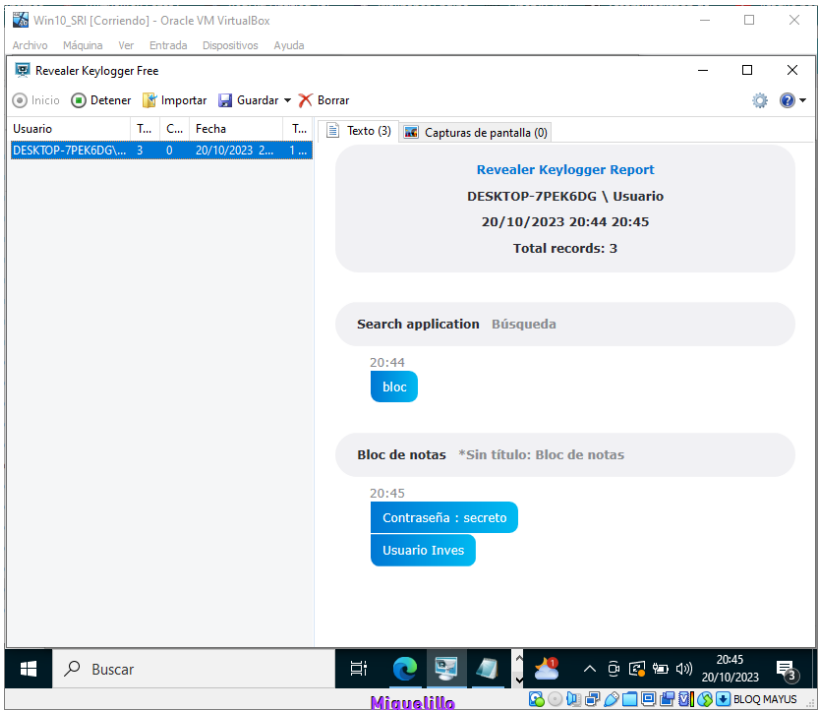


Nos aparece de manera **recursiva** todos los archivos con los **permisos**.



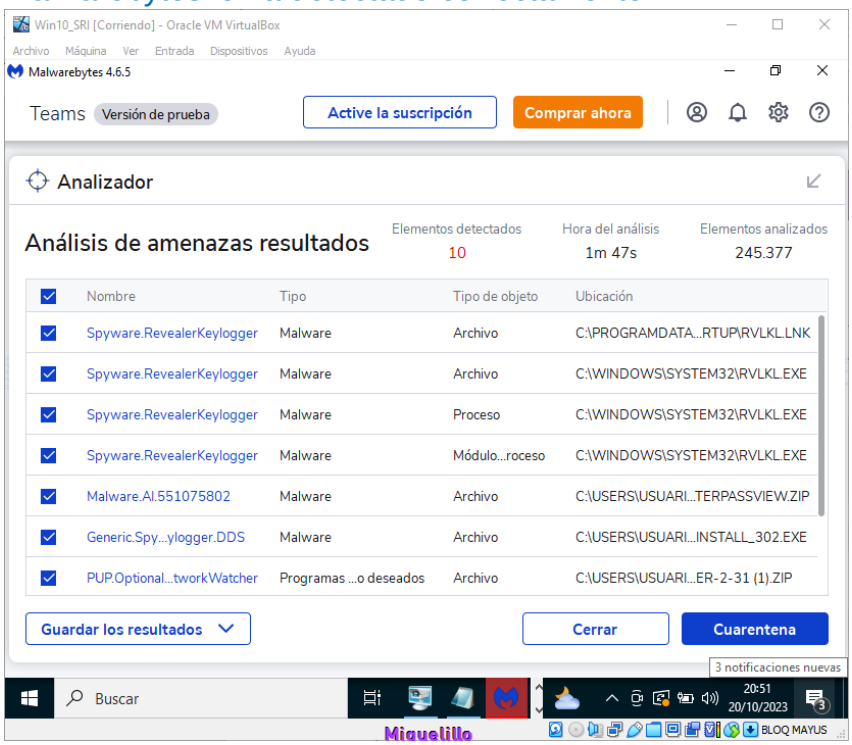
Para evitar un keylogger utilizar autenticación de dos factores, usar teclados softwares a la hora de introducir contraseñas, asegurarse que nadie accede a tu equipo sin tu supervisión para evitar un keylogger hardware

Instalo el keylogger



En primer lugar he tenido que desactivar la protección en tiempo real y el web para que me dejara descargarlo una vez descargado lo ejecuto y lo instalo sin problemas ya que están desactivada la opción de protección en tiempo real

Malwarebytes lo ha detectado correctamente



Sophos también lo ha eliminado no ha sido tan riguroso como Malwarebytes pero lo ha detectado