PRÁCTICA : E5 – Instalar un ordenador Bastionado Windows o Linux MF0486_3 : Seguridad en Equipos Informáticos			Fecha	14 / 03 / 2022
			Página 1 de 4	
Curso	7.1. MF0486_3 Seguridad en equipos informáticos	Plan de Formación	FC-2021.1/II.000/1914256	

Nombre y Apellidos:	ALEXIS VENTURA MEDINA	Firma del Alumno:	Firmado por VENTURA MEDINA
DNI:	49946563Q	Firma del Profesor:	

Apto: ☐ **No Apto:** ☐ **Calificación:** ☐

Instrucciones Generales

La puntuación máxima será de 10 puntos.
Esta prueba tendrá una duración máxima de 1260 minutos
(Temporalizados durante la Unidad de Aprendizaje)

El alumno/a deberá acatar las siguientes normas durante la duración de la práctica :

- Rellene el encabezado con su nombre, apellidos y D.N.I.
- Firme en todas y cada una de las hojas entregadas, incluidas las que estén en blanco.
- Usar exclusivamente bolígrafo azul o negro
- Guardar los ficheros generados en una carpeta con nombre **MF0486_E5**
- El docente le indicará al final como entregar el contenido de dicha carpeta
- Al finalizar el ejercicio y antes de entregarlo **comprueba tus respuestas**, en caso de duda consulta al docente.

Equipo y material

- Bolígrafo azul.
- Folios.
- Ordenadores.
- Conexión a Internet. (Para buscar información a modo de ayuda)
- Pendrive.
- Bibliografía empleada en el Módulo.
- Sistema operativo Windows
- Sistema operativo Linux

Instrucciones específicas

El objetivo de esta práctica guiada será que el alumno elabore un Plan de seguridad de una empresa ficticia o real, en el cual se plasmen diversas políticas de seguridad vistas durante el módulo formativo.

Condiciones de realización:

La actividad se llevará a cabo en el aula y el alumnado contará en todo momento supervisión del docente.

El alumnado contará con una duración de 1260 minutos para realizar la práctica.
Se podrá realizar en varias partes con una duración cada una de 60 minutos.

El alumno podrá hacer uso de internet para su realización, y se detallan a continuación algunas webs de ayuda.

Páginas webs : https://en.wikipedia.org/wiki/Hardening_(computing)

Hardening :

> En informática, el hardening o endurecimiento, es el proceso de garantizar un sistema mediante la reducción de servicios que pudieran extender sus vulnerabilidades.

En ella se valorará la utilización de herramientas para la gestión del tiempo y secuenciación del uso de las aplicaciones necesarias. Y se observará especialmente la autonomía del alumnado a la hora de ejecutar y tomar decisiones. Como también la estructuración del ejercicio en donde se solicitará, orden, coherencia y limpieza.

Una vez terminado la práctica se le notificará al docente y pasará a su evaluación.

Descripción de la práctica

1ª Parte :

El alumno tendrá que elegir que sistema operativo cree que es el más apropiado para utilizarlo como bastión en una red. ¿ Por qué?

2ª Parte :

El alumno tendrá que realizar un esquema de como quedaría su elección de la primera parte.

3ª Parte :

El alumno tendrá que elegir un sistema operativo ya sea en Windows o Linux, virtualizarlo y bastionarlo, describiendo los pasos que ha seguido para ello en un documento en Word.

Windows Bastionados

http://wiki.intrusos.info/doku.php/seguridad:asegurar_windows

http://seguridad-en-redes-mimi.blogspot.com.es/2012/05/hardening-windows.html

https://protegermipc.net/2018/03/20/apps-hardening-en-windows/

https://www.securitywizardry.com/scanning-products/host-scanners/tripwire-securecheq

Linux Bastionados

http://www.linuxsecurity.com/

http://www.softpanorama.org/Commercial_linuxes/Security/hardening.shtml

http://linux-com.blogspot.com.es/2012/03/linux-bastion-host-checklist.html

http://www.cyberciti.biz/tips/linux-security.html

http://www.cyberciti.biz/faq/linux-bastion-host/

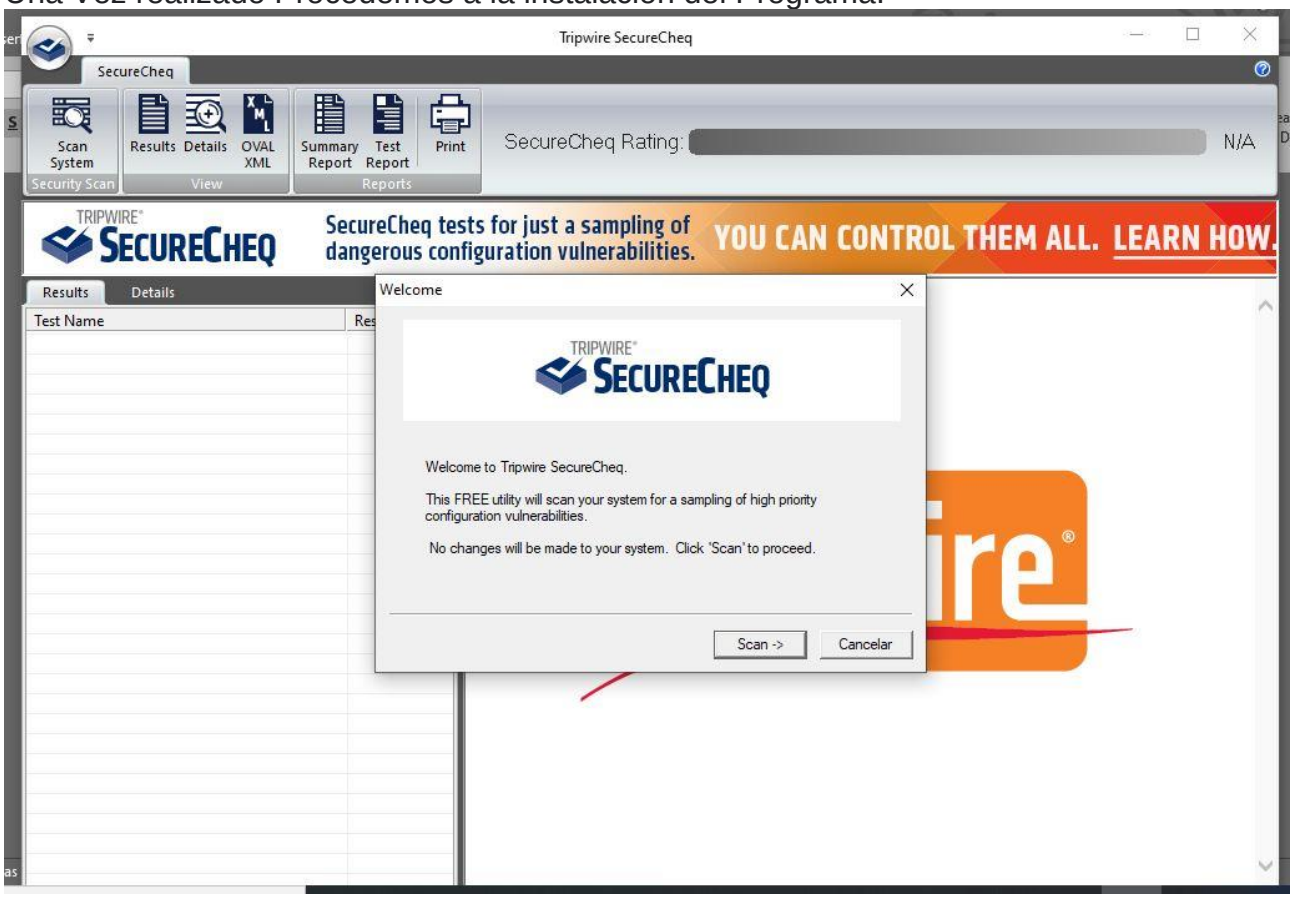
1ª Parte :

Para Bastionado, por ser de facilidad su manipulación, ser versátil y no se necesita conocer de códigos para su puesta en funcionamiento el Sistema Operativo de Microsoft Windows es el más usado actualmente.

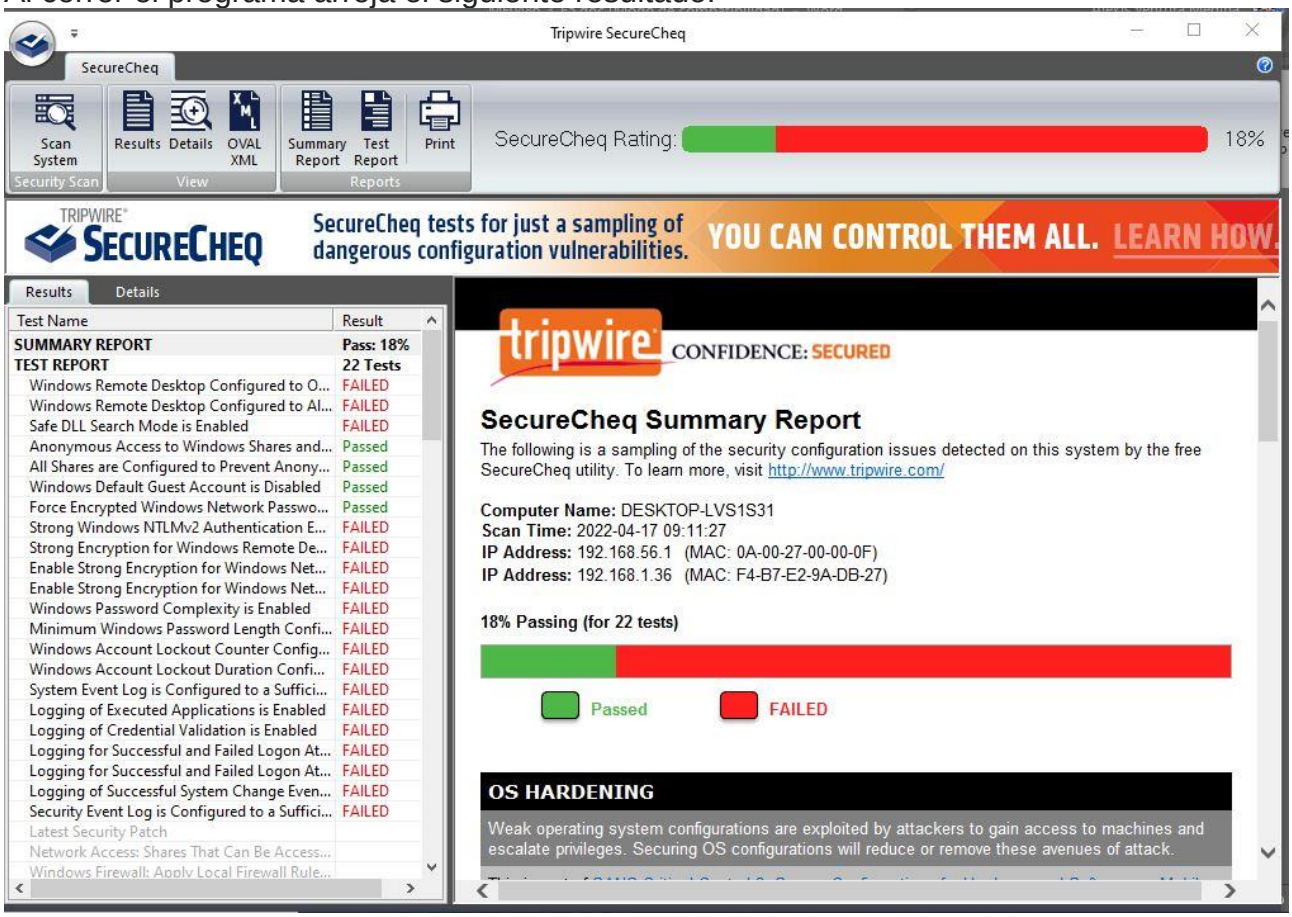
En este caso se realizará sobre Windows 10, ya que se dispone de licencia Original y se puede manipular.

- Se realizan las actualizaciones sobre el Sistema Operativo (Windows 10 Pro).
- Desactivar servicios de sistemas que nos son necesarios,
- Widnows Search (WSearch), Archivos sin conexión (CscService)
- Deshabilitar protocolos innecesario ya que no se necesitarían
- Nivel de importancia BAJO
- Utilizar Navegadores Confiables.
- Realizar un Punto de Restauración.

Una Vez realizado Procedemos a la instalación del Programa:

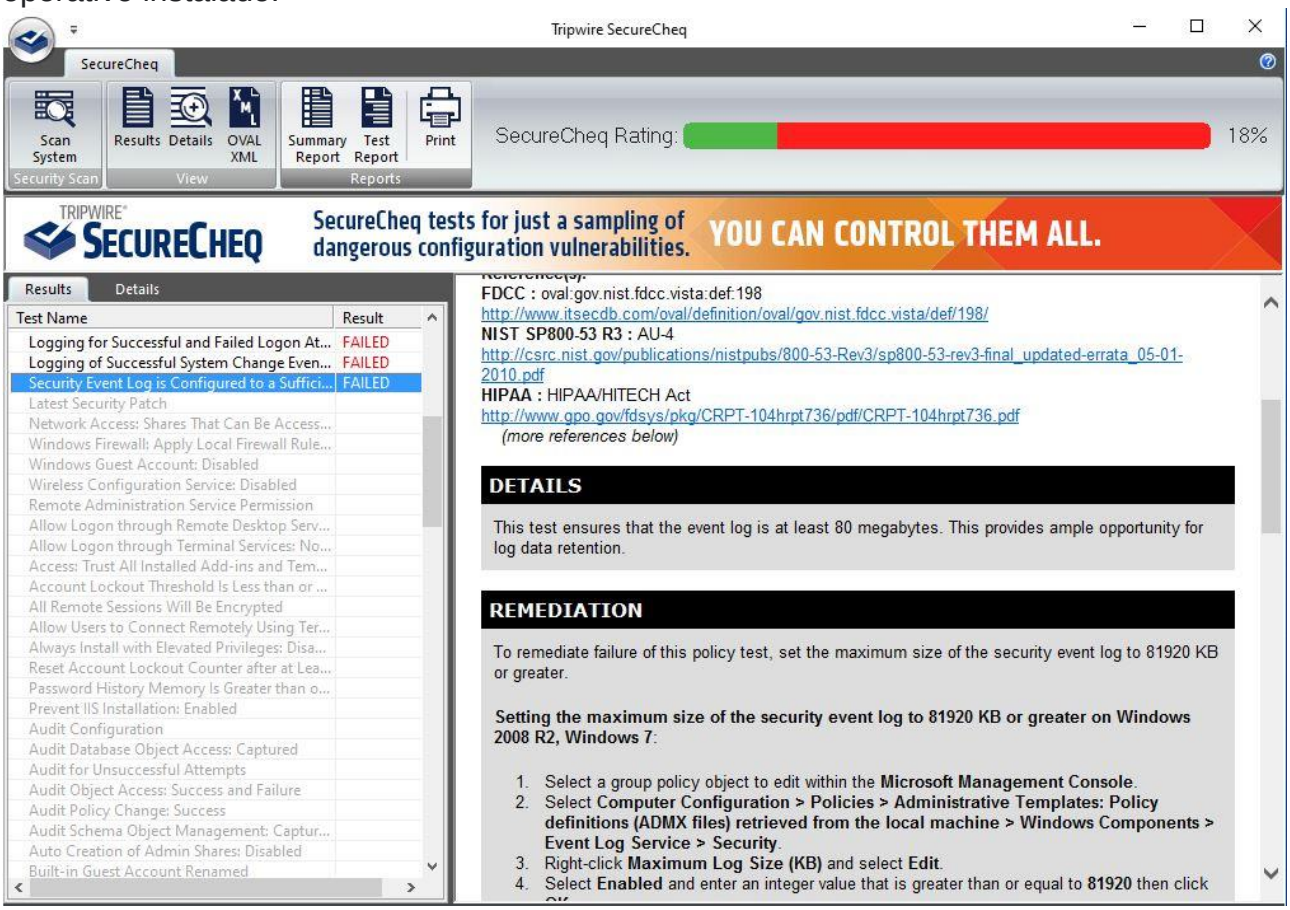


Al correr el programa arroja el siguiente resultado:

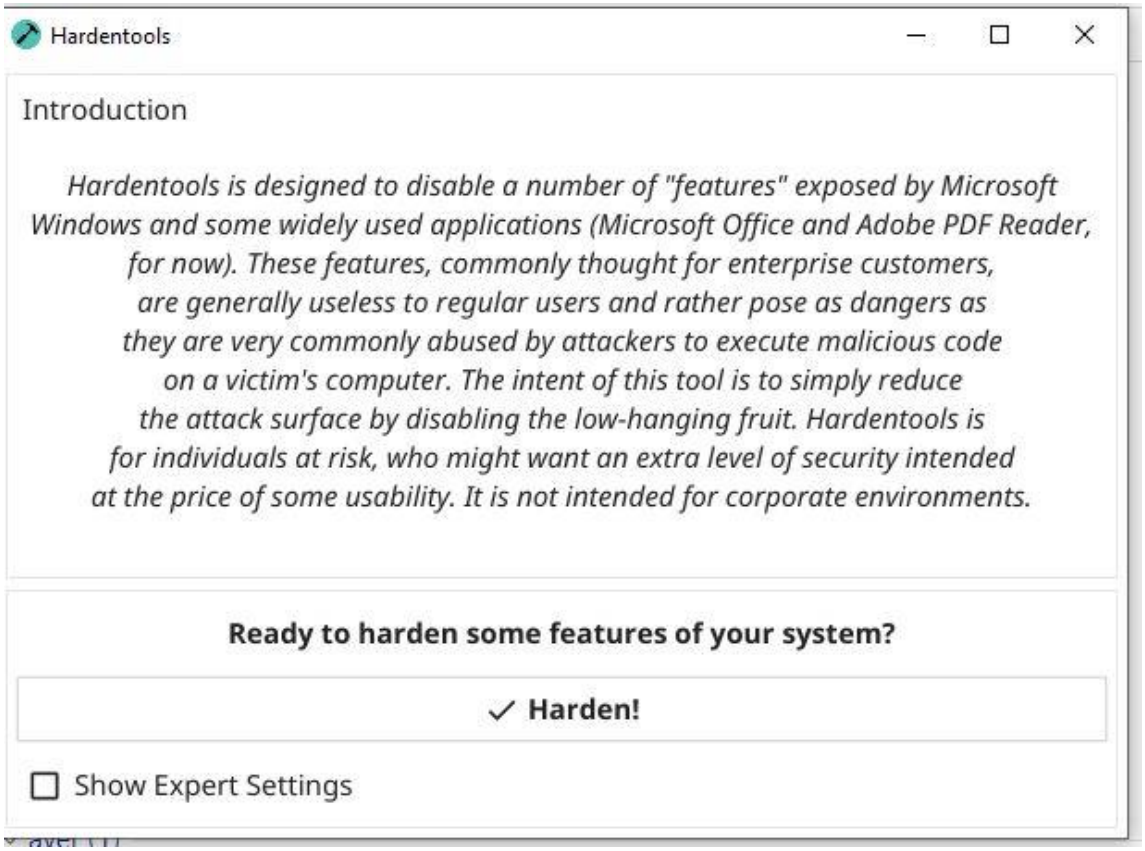


Ahora vamos resolviendo uno a uno los problemas indicados.

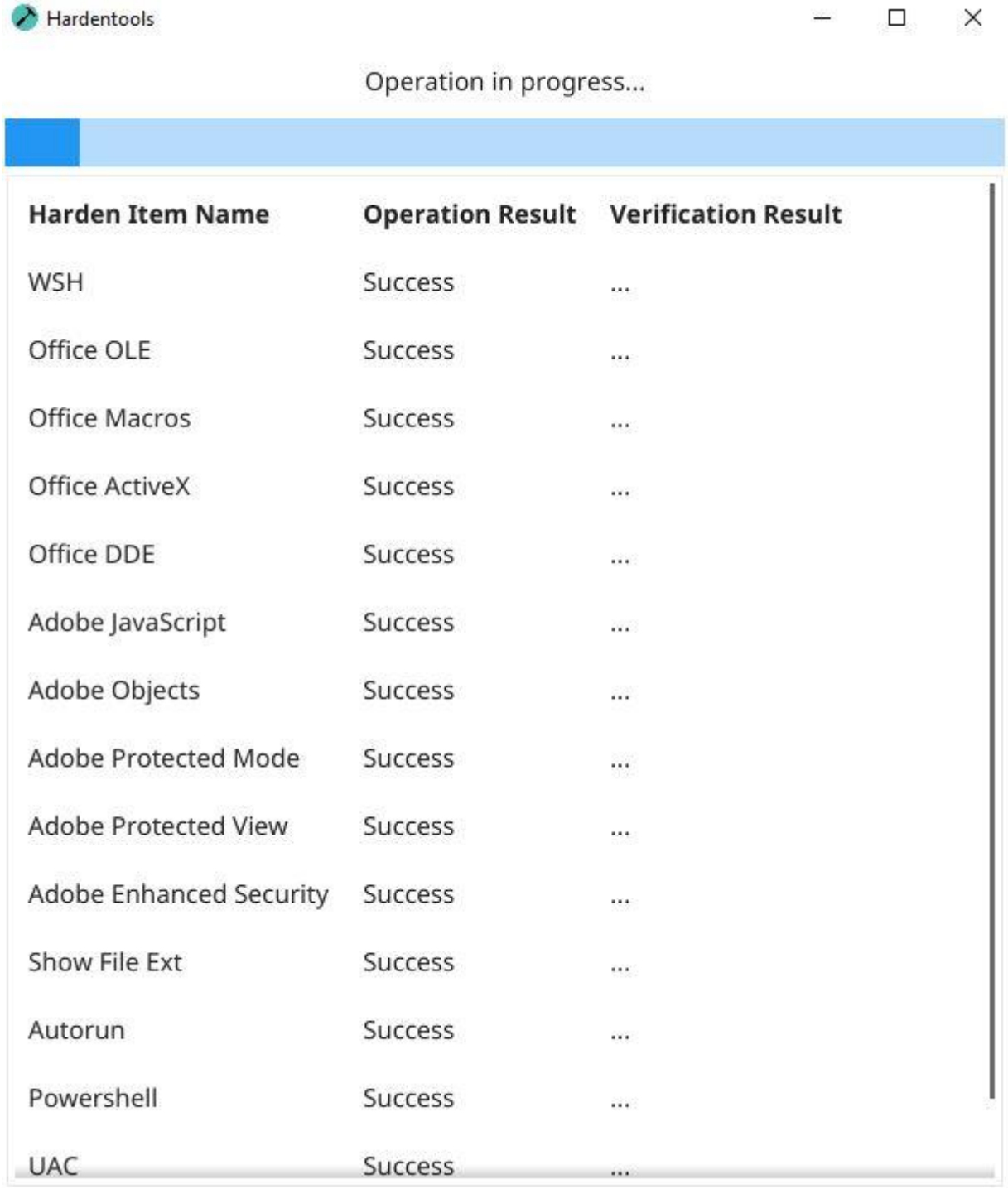
Al ir marcando o pinchando en cada uno de los puntos con fallas, nos indica los problemas que encuentra y nos da las soluciones para repararlos de acuerdo al sistema operativo instalado.



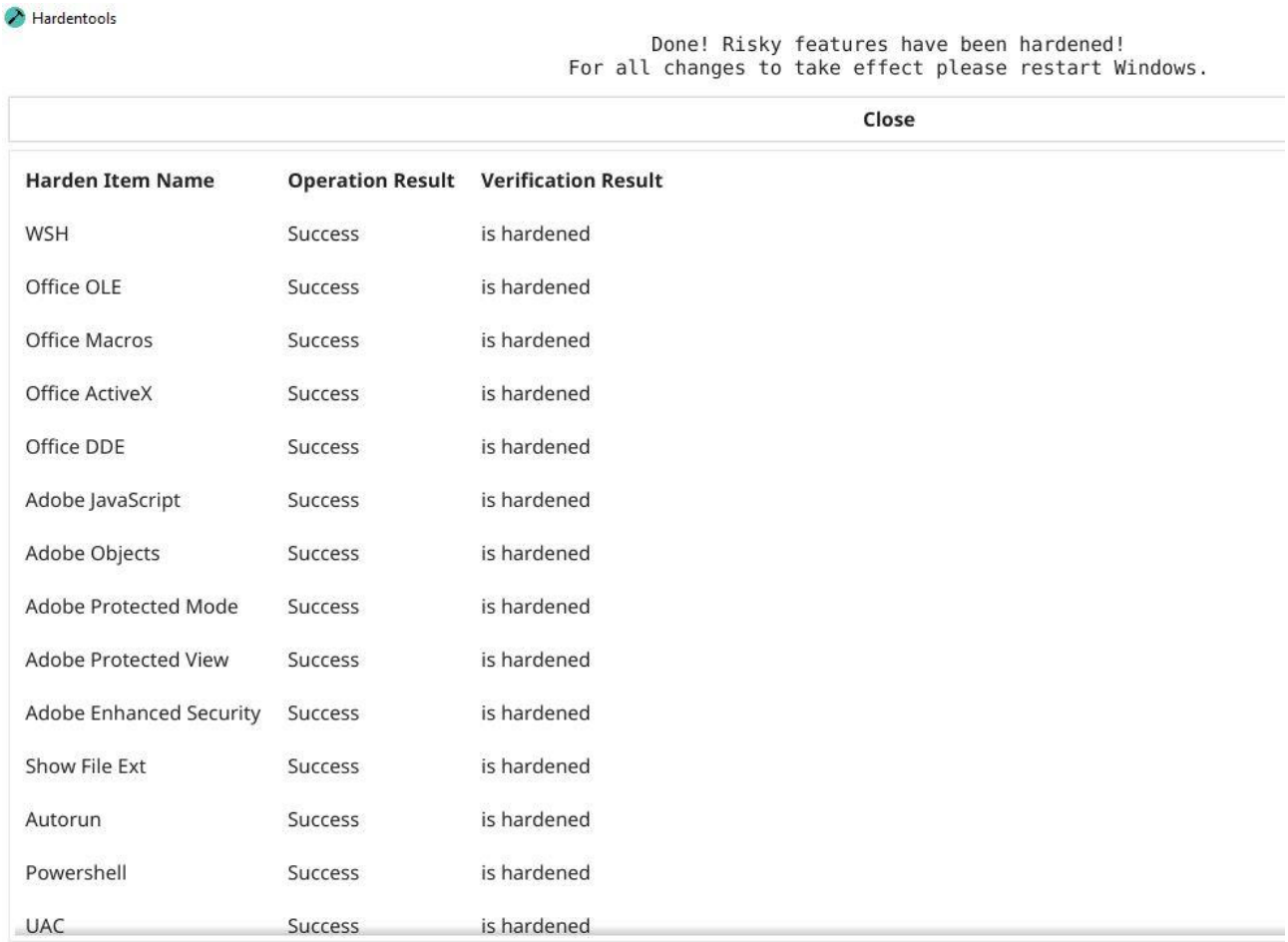
Ahora vamos a probar con otro programa:
Hardentools



Mientras se instala se toma una instantánea para demostrar que el programa tiene una operación en progreso y va harderizando cada uno de las aplicaciones.



A continuación vemos que está Hardenizado.



Harden Item Name	Operation Result	Verification Result
WSH	Success	is hardened
Office OLE	Success	is hardened
Office Macros	Success	is hardened
Office ActiveX	Success	is hardened
Office DDE	Success	is hardened
Adobe JavaScript	Success	is hardened
Adobe Objects	Success	is hardened
Adobe Protected Mode	Success	is hardened
Adobe Protected View	Success	is hardened
Adobe Enhanced Security	Success	is hardened
Show File Ext	Success	is hardened
Autorun	Success	is hardened
Powershell	Success	is hardened
UAC	Success	is hardened

Por último vemos cuales fallaron pero si entramos como expertos podemos cambiarlas.
Debemos reiniciar el equipo a los fines de que hagan efecto.