

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

<b>Nombre y Apellidos:</b>	JHONATAN RODRIGUEZ FERREIRA	<b>Firma del Alumno:</b>	
<b>DNI:</b>	78644010h	<b>Firma del Profesor:</b>	

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

<b>PRÁCTICA : E5 – Instalar un ordenador Bastionado Windows o Linux</b> <b>MF0486_3 : Seguridad en Equipos Informáticos</b>		<b>Fecha</b>	14 / 03 / 2022
		Página 2 de 4	
<b>Curso</b>	7.1. MF0486_3 Seguridad en equipos informáticos	<b>Plan de Formación</b>	FC- 2021.1/II.000/1914256

## 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\\_\(computing\)](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.

<b>PRÁCTICA : E5 – Instalar un ordenador Bastionado Windows o Linux</b> <b>MF0486_3 : Seguridad en Equipos Informáticos</b>		<b>Fecha</b>	14 / 03 / 2022
		Página 3 de 4	
<b>Curso</b>	7.1. MF0486_3 Seguridad en equipos informáticos	<b>Plan de Formación</b>	FC- 2021.1/II.000/1914256

## 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.

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



### Windows Bastionados

[http://wiki.intrusos.info/doku.php/seguridad:asegurar\\_windows](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-securechek>



### Linux Bastionados

<http://www.linuxsecurity.com/>

[http://www.softpanorama.org/Commercial\\_linuxes/Security/hardening.shtml](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>

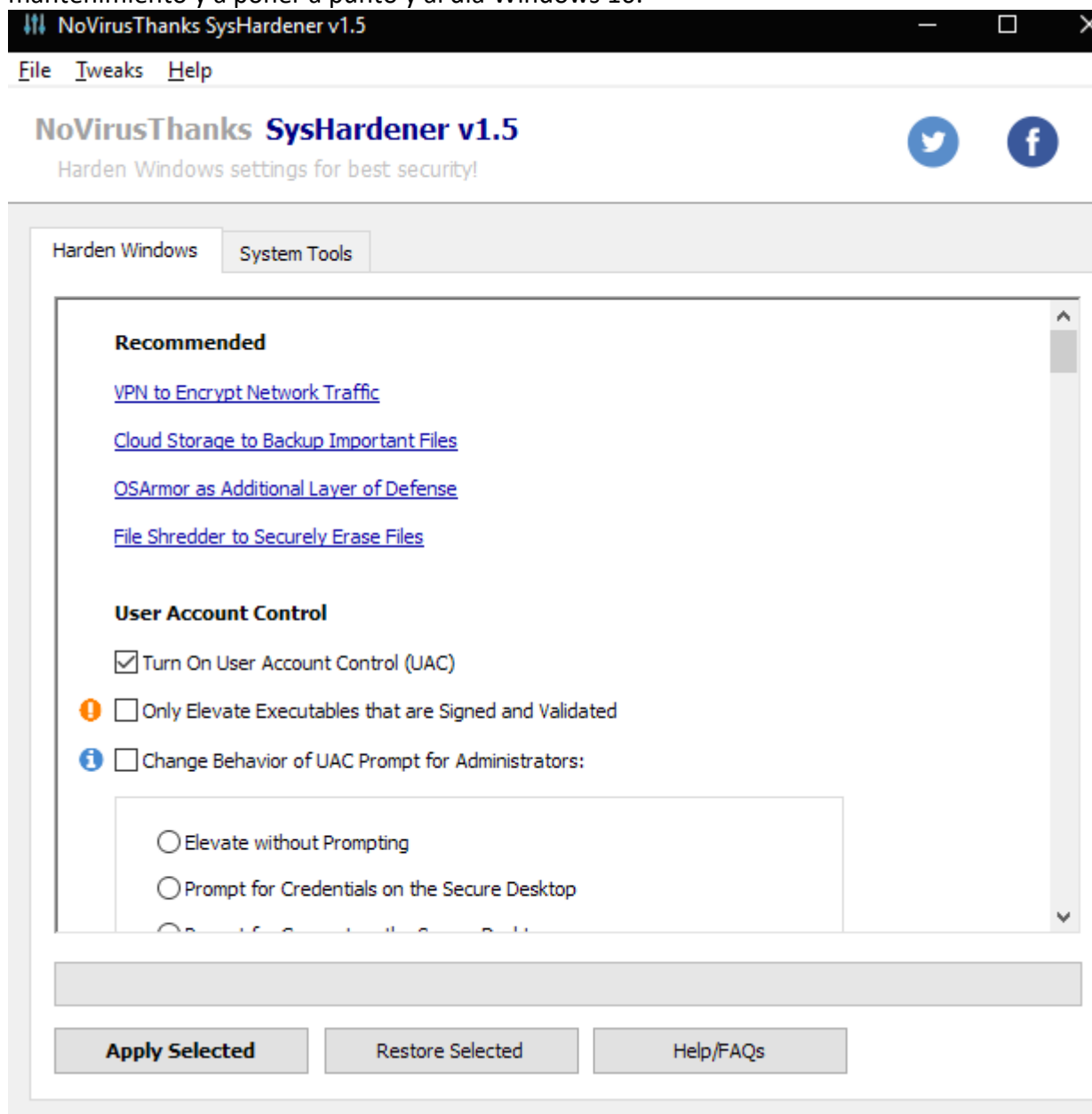
<http://www.cyberciti.biz/faq/linux-bastion-host/>

<b>PRÁCTICA : E5 – Instalar un ordenador Bastionado Windows o Linux</b> <b>MF0486_3 : Seguridad en Equipos Informáticos</b>		Fecha	14 / 03 / 2022
		Página 5 de 4	
Curso	7.1. MF0486_3 Seguridad en equipos informáticos	Plan de Formación	FC- 2021.1/II.000/1914256

Para Bastionar nuestro equipo utilizaremos sistema **Windows 10** y usaremos una aplicación llamada **SYSHARDENER**.

Paso 1: Descargaremos la herramienta de la página <https://www.novirusthanks.org/products/syshardener/> y procedemos a su instalación.

Paso 2: Abrimos la aplicación y veremos 2 pestañas, la **Harden Windows** donde nos muestra una especie de listado por el cual uno puede marcar o desmarcar dependiendo de que tan fuerte o no quiere uno tener el equipo y la pestaña **System Tools** el cual con conocimientos técnicos podremos de la misma manera activar o desactivar funciones del Windows 10 e incluso hacer mantenimiento y a poner a punto y al día Windows 10.



<b>PRÁCTICA : E5 – Instalar un ordenador Bastionado Windows o Linux</b> <b>MF0486_3 : Seguridad en Equipos Informáticos</b>		<b>Fecha</b>	14 / 03 / 2022
		Página 6 de 4	
<b>Curso</b>	7.1. MF0486_3 Seguridad en equipos informáticos	<b>Plan de Formación</b>	FC- 2021.1/II.000/1914256

Paso 3: Procedemos a Hardenisar nuestro equipo

Por no tener recursos en el ordenador de casa y no poder crear una maquina virtual utilizaré en mi sistema actual el procedimiento de hardenin realizando una lista de check muy pequeña para comprobar las virtudes de la aplicación pero no las aplicaré.

The screenshot shows the 'Harden Windows' application window. It has two tabs: 'Harden Windows' (selected) and 'System Tools'. Under the 'Harden Windows' tab, there is a section titled 'User Account Control'. It contains the following settings:

- ☐ Turn On User Account Control (UAC)
- ☒ Only Elevate Executables that are Signed and Validated
- ☒ Change Behavior of UAC Prompt for Administrators:
  - ☐ Elevate without Prompting
  - ☐ Prompt for Credentials on the Secure Desktop
  - ☐ Prompt for Consent on the Secure Desktop
  - ☐ Prompt for Credentials
  - ☐ Prompt for Consent
  - ☒ Prompt for Consent for non-Windows Binaries (Default)
- ☐ Change Behavior of UAC Prompt for Users:

At the bottom of the window, there are three buttons: 'Apply Selected', 'Restore Selected', and 'Help/FAQs'.

Con esta opción nos aseguramos que solamente se puedan instalar programas y aplicaciones que solamente esten validadas y firmadas por windows 10, sin embargo nos da la opción de si tenemos cuenta de administrador podamos elegir si queremos instalar o no.

<b>PRÁCTICA : E5 – Instalar un ordenador Bastionado Windows o Linux</b> <b>MF0486_3 : Seguridad en Equipos Informáticos</b>		Fecha	14 / 03 / 2022
		Página 7 de 4	
Curso	7.1. MF0486_3 Seguridad en equipos informáticos	Plan de Formación	FC- 2021.1/II.000/1914256

#### Windows Security Tweaks

- ☒ Turn On Windows File Protection
- ☒ Turn On Driver Signing\Integrity Check
- ☒ Show File Extensions for Known Files
- ☐ Show Hidden and System Files
- ☒ Turn Off Support for 16-bit Processes

En la parte de **seguridad** le indicamos que nos active la protección para archivos de windows y que revise la integridad de nuestros controladores para que así nos indique cualquier cambio y no de origen a instalar un posible malware. Le indicamos también que podamos ver las extensiones y que no nos deje ejecutar procesos de 16 bits.


#### PowerShell Hardening

- ☐ Change PowerShell Execution Policy for Current User

- ☐ Restricted (Default) - No script either local or remote can be executed
- ☒ AllSigned - All scripts need to be signed to be executed
- ☐ RemoteSigned - All remote or downloaded scripts must be signed
- ☐ Unrestricted - Prompt if unsigned remote scripts are executed
- ☐ Bypass - Nothing is blocked and there are no warnings or prompts
- ☐ Undefined - Remove the execution policy for the current user

En la parte de **Powershell** le indicaremos que solo nos deje ejecutar aquellos scripts que sean firmados, dándonos una mayor seguridad de que únicamente podrán ejecutar scripts solo los administradores o aquellos usuarios que se les pueda validar su firma.

<b>PRÁCTICA : E5 – Instalar un ordenador Bastionado Windows o Linux</b> <b>MF0486_3 : Seguridad en Equipos Informáticos</b>		<b>Fecha</b>	14 / 03 / 2022
		Página 8 de 4	
<b>Curso</b>	7.1. MF0486_3 Seguridad en equipos informáticos	<b>Plan de Formación</b>	FC- 2021.1/II.000/1914256

 ☒ Disable PowerShell v2.0 Engine

**File Type Associations**

☒ Unassociate .VBS File Extension

☒ Unassociate .VBE File Extension

☒ Unassociate .JS File Extension

☒ Unassociate .JSE File Extension

☒ Unassociate .WSF File Extension

☒ Unassociate .WSH File Extension

☒ Unassociate .HTA File Extension

☒ Unassociate .SCR File Extension

☒ Unassociate .PTE File Extension

☐ Unassociate .BAT File Extension

☐ Unassociate .PS1 File Extension

También le indicamos que no se pueda ejecutar versiones antiguas de Powershell y que unicamente se podrá ejecutar archivos solo con extension .Bat y .PS1

#### Vulnerable Software Tweaks

- ☒ Turn Off JavaScript in Adobe Reader
- ☒ Turn On Protected View in Adobe Reader
- ☒ Turn Off Opening of non-PDF Files in Adobe Reader
- ☒ Turn On Enhanced Security in Adobe Reader
- ☒ Turn On Check for Updates at Startup in Adobe Reader
- ☒ Turn Off Macros in Microsoft Office
- ☒ Turn Off DDEAUTO in Microsoft Office
- ☒ Turn Off ActiveX in Microsoft Office
- ☒ Turn Off OLE Objects in Microsoft Office
- ☒ Set Macros Security to "Very High" in Kingsoft WPS Office
- ☒ Turn Off JavaScript Actions in Foxit Reader

También le indicaremos que no se pueda **ejecutar ningún tipo de código** como javascript, activex y otros que es por donde se aprovechan los ciberdelicuentes realizando pequeñas sentencias en SQL injection o pequeños script ya que nuestro ordenador necesita ejecutar esos archivos



<b>PRÁCTICA : E5 – Instalar un ordenador Bastionado Windows o Linux</b> <b>MF0486_3 : Seguridad en Equipos Informáticos</b>		Fecha	14 / 03 / 2022
		Página 9 de 4	
Curso	7.1. MF0486_3 Seguridad en equipos informáticos	Plan de Formación	FC- 2021.1/II.000/1914256

mayoriamente para poder trabajar con sistemas mas que todo por internet. Desactivando todo este tipo de software blindaremos mucho nuestro equipo a tal punto que podría ser incomodo es por ello que hay que saber elegir bien que se pueda o no ejecutar.

#### Windows Firewall (Outbound)

- ☒ Block Outbound Connections for Attrib.exe
 ☒ Block Outbound Connections for Dwm.exe  
☒ Block Outbound Connections for AtBroker.exe
 ☒ Block Outbound Connections for Excel.exe

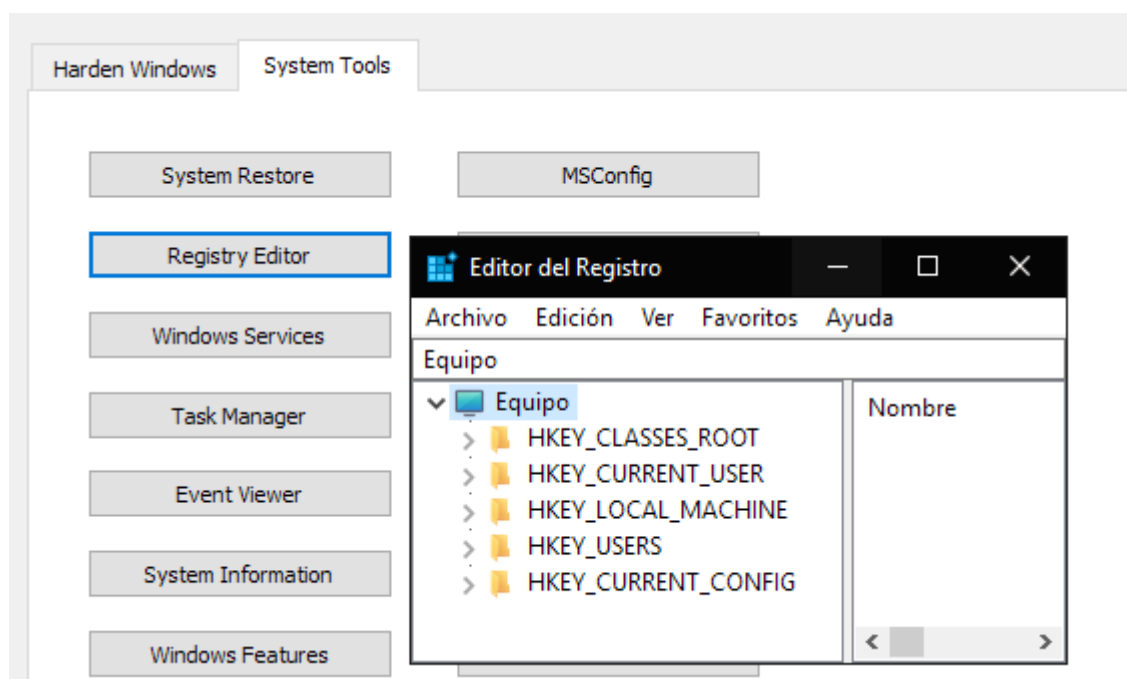
- ☒ Block Outbound Connections for ScriptRunner.exe

#### Windows Firewall (Inbound)

- ☒ Block Outbound Connections for Services.exe
 ☒ Block Inbound Connections

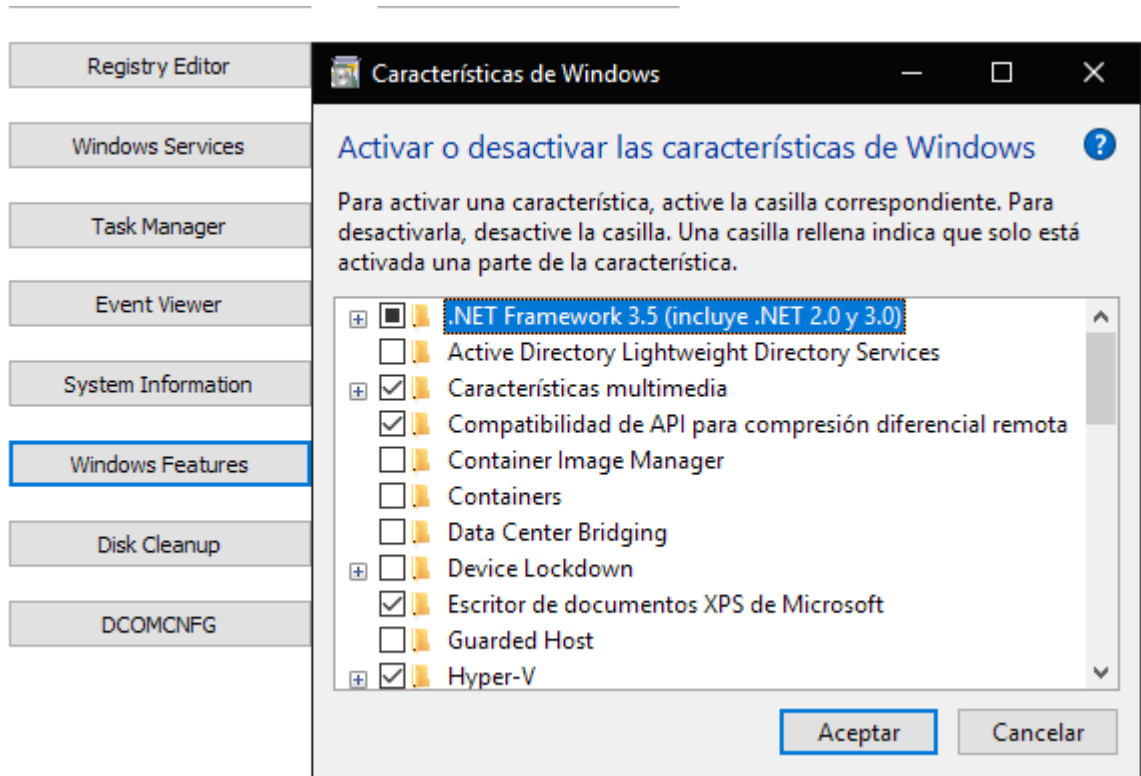
También podremos configurar la parte de **Firewall de salida** indicándole que nos bloquee aquellas aplicaciones o servicios que se puedan conectar a internet y no nos interese como también se le puede indicar que no nos permita entrar ningún tipo de conexión a nuestro ordenador hardninsandolo por completo.

Le daríamos al botón aplicar cambios y el automáticamente tomaría toda nuestra configuración y la ejecutaria.



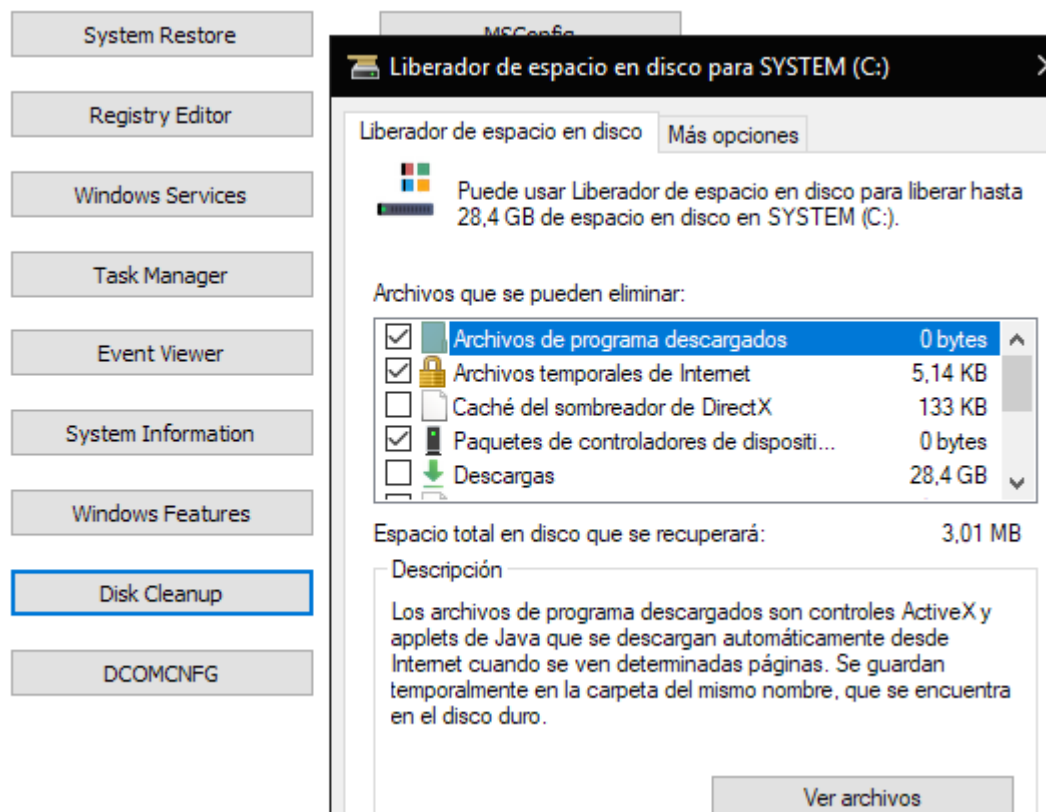
Luego paraa laa parte de optimización podremos entrar en la pestaña Systms Tools y con conocimientos técnicos podremos entrar por ejemplo a la parte de registro y modificar lo que querramos.

<b>PRÁCTICA : E5 – Instalar un ordenador Bastionado Windows o Linux MF0486_3 : Seguridad en Equipos Informáticos</b>		<b>Fecha</b>	14 / 03 / 2022
		Página 10 de 4	
<b>Curso</b>	7.1. MF0486_3 Seguridad en equipos informáticos	<b>Plan de Formación</b>	FC- 2021.1/II.000/1914256



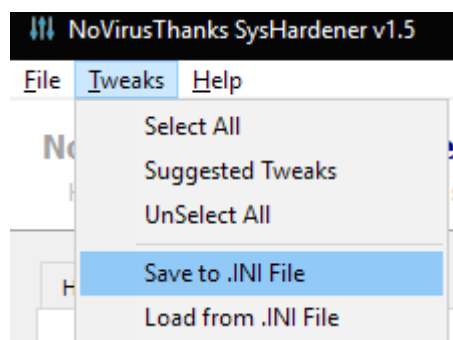
Podremos activar o desactivar características de Windows o incluso liberar espacio en disco de ser necesario.

<b>PRÁCTICA : E5 – Instalar un ordenador Bastionado Windows o Linux</b> <b>MF0486_3 : Seguridad en Equipos Informáticos</b>		<b>Fecha</b>	14 / 03 / 2022
		Página 11 de 4	
<b>Curso</b>	7.1. MF0486_3 Seguridad en equipos informáticos	<b>Plan de Formación</b>	FC- 2021.1/II.000/1914256



Y por ultimo si queremos que esta misma configuración de Hardening funcione en otros equipos podemos pinchar en la opción Tweaks y grabar un archivo .INI. Lo único que necesitaremos en otro equipo es tener la misma aplicación y pinchar donde dice Load from INI.file y asi tendríamos más equipos con la misma configuración

Y si damos un paso más alla podremos mediante consola replicar ese archivo a todos los equipos en la red y mediante script que se ejecute automáticamente y asi podre hardenizar todos los equipos de una red de manera rapida y sencilla.



FIN.