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:	JAVIER PRUNELL ACOSTA	Firma del Alumno:	
DNI:	5405600W	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 qué sistema operativo cree que es el más apropiado para utilizarlo como bastión en una red. ¿Por qué?
Vamos a utilizar el sistema operativo Linux. Con ello, vamos a utilizar la distro Linux Mint o cualquier distribución que tenga actualizado de manera estable los repositorios. No se recomienda utilizar una distribución de Linux que no tenga un soporte de seguridad o ayuda asentado. El tener un kernel más cerrado, a nivel de seguridad y al estar compuesto por módulos, podemos personalizar mejor la seguridad del mismo.

2ª Parte: El alumno tendrá que realizar un esquema de como quedaría su elección de la primera parte.

Para el sistema operativo Linux, utilizaremos Kali Linux:

- Arranque
- Usuarios y grupos
- Acceso
- Configuración sudo
- Servicios
- Sistemas de ficheros
- Red
- Firewall

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.

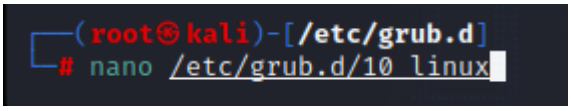
HARDENING LINUX: Kali Linux

Primeramente, la distro seleccionada para Linux, será Kali Linux ya que tenemos herramientas preinstaladas que nos pueden beneficiar para endurecer el sistema de una forma más segura. Tenemos que tener en cuenta que vamos a configurar las siguientes partes dentro del sistema:

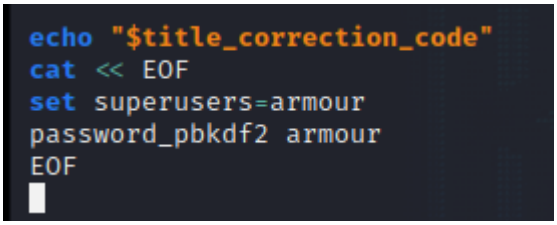
- Arranque
- Usuarios y grupos
- Acceso
- Configuración sudo
- Servicios
- Sistemas de ficheros
- Red
- Firewall

CONFIGURACIÓN DEL ARRANQUE

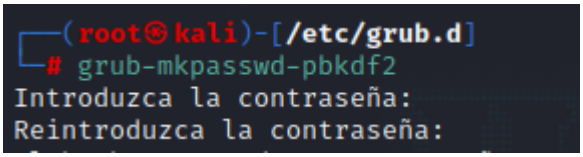
Introducimos una contraseña en el arranque del sistema, de esta forma, estamos fortaleciendo el acceso al sistema. **CONFIGURAR EL GRUB**



Accedemos al archivo, nos dirigimos al final y añadimos:

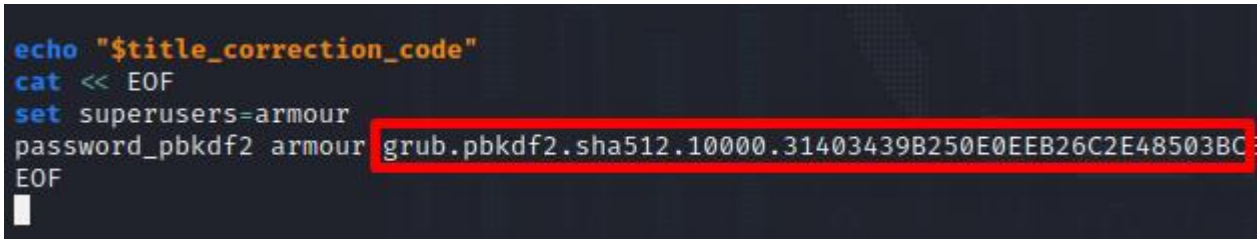


Posteriormente, guardamos el documento (CTRL + O) y después salimos. Introducimos el siguiente comando, y ponemos la contraseña “armour”, de esta forma, copiamos el hash generado:



A continuación, en el mismo archivo, pegamos el hash, guardamos y actualizamos grub

update-grub



Finalmente, configuramos directamente el grub desde la terminal:

grub-mkconfig -o /boot/grub/grub.cfg

Recordamos que debemos darle solo permisos de lectura al fichero de arranque:

Chmod 400 /boot/grub/grub.cfg

Ahora procedemos a la configuración para usuarios, forzando que el usuario acceda solamente a través de un **SINGLE USER.** Pondremos como contraseña “palmera”

```
┌──(root㉿kali)-[/etc/grub.d]
└─# passwd
Nueva contraseña:
Vuelva a escribir la nueva contraseña:
passwd: contraseña actualizada correctamente
```

Ahora vamos a toca la CONFIGURACIÓN DE ACCESO con el SSH
Instalaremos un SSH Server.

apt install openssh-server
chmod 600 /etc/ssh/sshd_config

Accedemos al archivo y habilitamos las siguientes opciones. Ya está por defecto, activado el SSH PAM (UsePAM yes).

```
ClientAliveInterval 300
ClientAliveCountMax 0
#UseDNS no
#PidFile /run/sshd.pid
MaxStartups 10:30:100
#PermitTunnel no
```

```
# Authentication:

LoginGraceTime 1m
PermitRootLogin no
#StrictModes yes
MaxAuthTries 4
MaxSessions 4
#PubkeyAuthentication yes
#AuthorizedKeysFile     .ssh/authori
#AuthorizedPrincipalsFile none
#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody
HostbasedAuthentication no
#IgnoreUserKnownHosts no
IgnoreRhosts yes
#PasswordAuthentication yes
PermitEmptyPasswords no
```

Vamos a trabajar ahora con la CONFIGURACIÓN DE RED. Para evitar ataques por MAN IN THE MIDDLE y para evitar estos accesos indeseados, deshabilitamos todas las redirecciones de paquetes:

```
┌──(root㉿kali)-[/etc/grub.d]
└─# sysctl -w net.ipv4.conf.all.send_redirects=0
net.ipv4.conf.all.send_redirects = 0

┌──(root㉿kali)-[/etc/grub.d]
└─# sysctl -w net.ipv4.conf.default.send_redirects=0
net.ipv4.conf.default.send_redirects = 0

┌──(root㉿kali)-[/etc/grub.d]
└─# sysctl -w net.ipv4.route.flush=1
net.ipv4.route.flush = 1
```

Como hemos podido comprobar, el sistema de hardening de Linux podría ser interminable, por ello, debemos tener siempre un checklist para comprobar algunas de las opciones (o todas) de las que nos podamos encontrar dentro de la configuración de cualquier distribución.
PARA ELLO, PODEMOS GUIARNOS CON ESTE DOCUMENTO: Linux Checklist

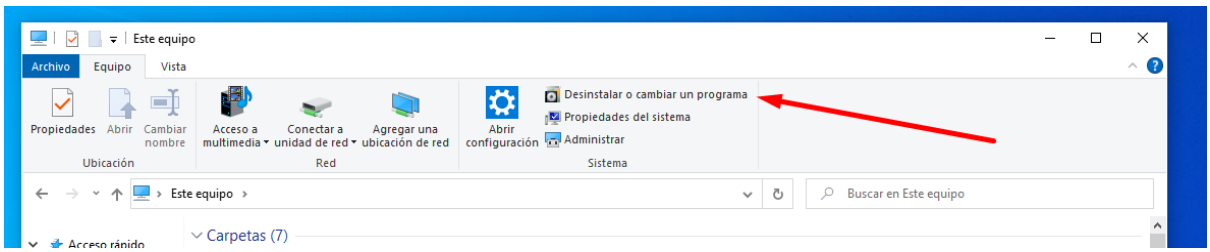
HARDENING en Windows 10

Dentro de la configuración de Windows 10, podemos seguir un cheklist más simple, ya que el mismo sistema operativo, a través de sus actualizaciones, sistemas de seguridad propios de la misma, nos indican que el sistema ya es seguro de por sí. Vamos a verificar de forma simple los siguientes puntos.

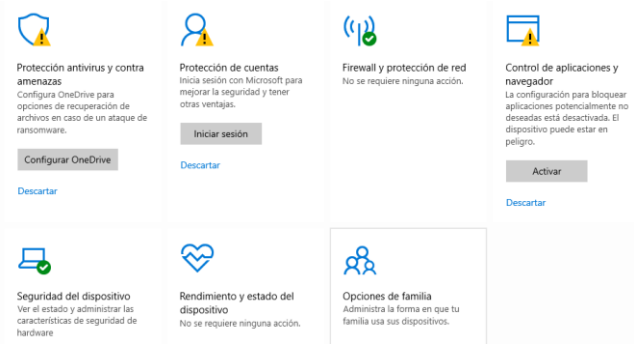
- Desinstalar programas que no estemos usando
- Utilizar Seguridad de Windows
- Protección contra ransomware
- Cifrado de SSD, discos duros o particiones
- Autenticación segura de vuestros inicios de sesión
- Gestionar alternativas de inicios de sesión

Todas estas opciones, se pueden comprobar en la configuración interna de Windows (Windows+I) y a partir de aquí, todo lo demás debemos depender de programas a terceros para aumentar la capacidad de protección de los mismos sistemas operativos.

- Si partimos de una **instalación** desde 0 de un sistema operativo, podemos presupones que no hace falta desinstalar ningún programa "sospechoso", de todas formas, y por seguridad, siempre debemos supervisar que no haya instalaciones de programas "no permitidos" en nuestro SO. En este equipo, podemos acceder y eliminar todos los programas "indeseables".



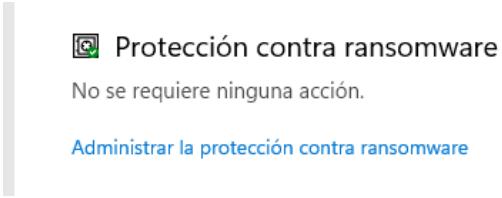
Utilizar la seguridad de Windows 10. Aunque la mayoría de técnicos no podemos "confiarnos" plenamente en ello, como podemos ver en la siguiente imagen, Windows nos está avisando de que hay ciertos riesgos que el detecta. En este caso, deberíamos instalar un antivirus, proteger las cuentas internas y proteger más



específicamente los navegadores (actualizados, limitando accesos por administrador, etc)

La **protección** contra ransomware, puede ser muy compleja, ya que podemos gestionar una red completa para evitar el acceso a los ordenadores, pero también podemos instalar programas antimalware para evitar ataques como por ejemplo el AppCheck Anti-Ransomware o el Trend Micro RansomBuster. Pero en este caso, vamos a revisar la seguridad de Windows 10 enfocada al ransomware.

Seguridad de Windows > Inicio > protección contra ransomware:



En la configuración del ransomware, nos encontramos con:

Como podemos ver, la configuración del OneDrive es una posibilidad para mantener seguros los archivos directamente en la nube.

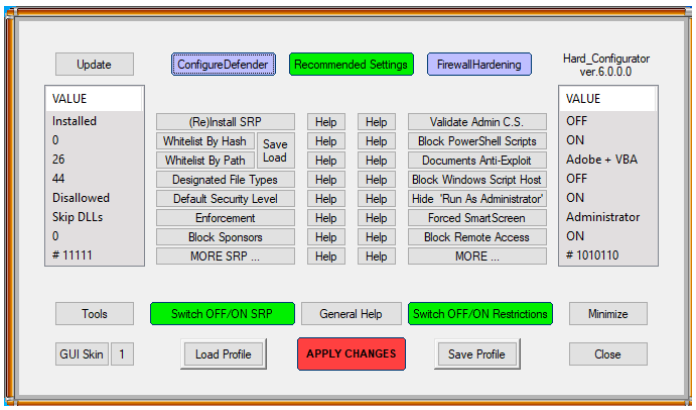
- Cifrado de los discos duros SSD y HDD. Esta opción siempre es opcional, aunque es recomendable, y también tenemos que tener en cuenta que los SSD, a la larga con el cifrado, se vuelven menos óptimos y su tiempo de vida disminuye por la cantidad de veces que el disco se escribe y lee. Aunque, la actualización con la build 18317 de Windows 10, y a partir de Windows 10 19H1, el cifrado por defecto del sistema operativo será a través de software con BitLocker.

El hardening de un sistema operativo puede ser un trabajo muy tedioso y casi sin límites, por ello, vamos a aplicar a Windows un programa específico llamado **HARD_CONFIGURATOR**. Cuanto más tiempo se le dedique a cerrar un sistema operativo, más seguro podría ser, aunque no lo asegura al 100%.

Hard_Configurator

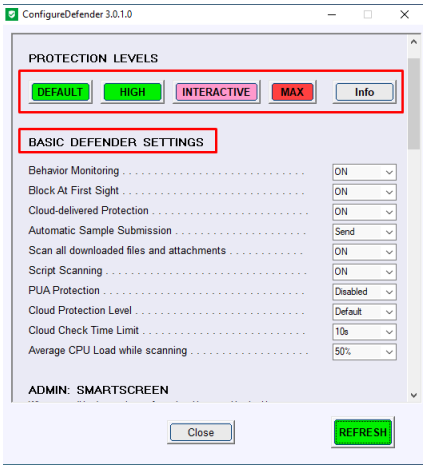
CONFIGURACIÓN DEL PROGRAMA

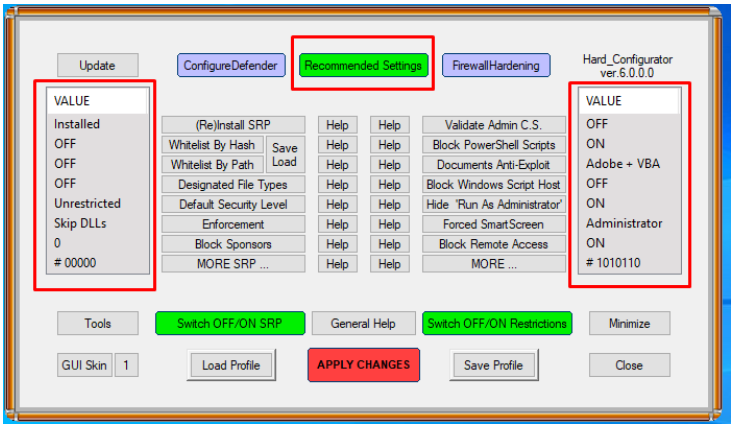
En favor de este software que no he podido observar en otro de los programas de seguridad, es que antes de iniciar el programa y configurarlo, nos recomienda hacer una copia de seguridad del sistema, por si las restricciones de seguridad son demasiado fuertes. Vamos a hacer un recorrido desde dentro de todas las opciones que tiene el programa. En este caso, tenemos un panel con bastantes opciones. Configuración, opciones recomendadas y un hardening al Firewall.



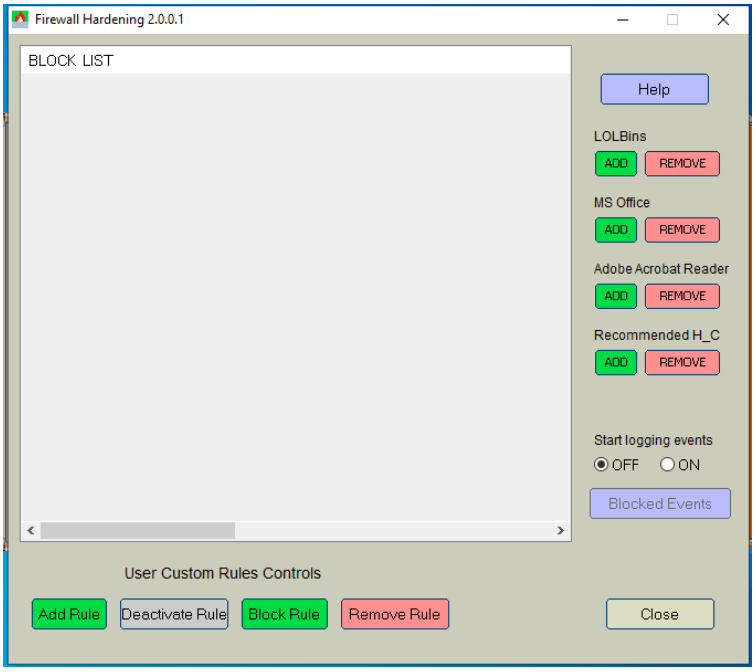
CONFIGURE DEFENDER Y RECOMMENDED SETTINGS

En esta sección, podemos seleccionar la complejidad de la protección, desde por defecto hasta una protección máxima. Al volver al panel principal, podemos ver las recomendaciones (bajo el arranque del programa como administrador) que se nos encuentra a la derecha y a la izquierda de los paneles. En este caso, por ejemplos, se nos ha deshabilitado la lista blanca del PATH y del HASH, o los bloqueos de Windows bajo un Script Host.





También, una herramienta muy potente que tiene el programa es la integración y configuración de un sistema de Firewall donde limitar puertos y programas. Que, a su vez, se puede empatar con la actividad E6 relacionada con el Firewall. Podemos añadir reglas, eliminarlas, desactivarlas, etc.



Finalmente, podemos guardar el perfil de la configuración, cargar un perfil ya guardado o simplemente aplicar la configuración. Es también muy interesante, que dentro de las herramientas que nos encontramos en el programa, tenemos manager de imagen de backup. De esta forma, también podríamos empatar con la práctica E2 refiriéndonos a la confidencialidad de la información y teniendo esta segura.