

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:	
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

PRÁCTICA : E5 – Instalar un ordenador Bastionado Windows o Linux MF0486_3 : Seguridad en Equipos Informáticos			Fecha	14 / 03 / 2022
			Página 2 de 4	
Curso	7.1. MF0486_3 Seguridad en equipos informáticos	Plan de Formación	FC-2021.I/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.

PRÁCTICA : E5 – Instalar un ordenador Bastionado Windows o Linux MF0486_3 : Seguridad en Equipos Informáticos			Fecha	14 / 03 / 2022
			Página 3 de 4	
Curso	7.1. MF0486_3 Seguridad en equipos informáticos	Plan de Formación	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.

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



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-securechek>



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/>

PRÁCTICA : E5 – Instalar un ordenador Bastionado Windows o Linux MF0486_3 : Seguridad en Equipos Informáticos			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	

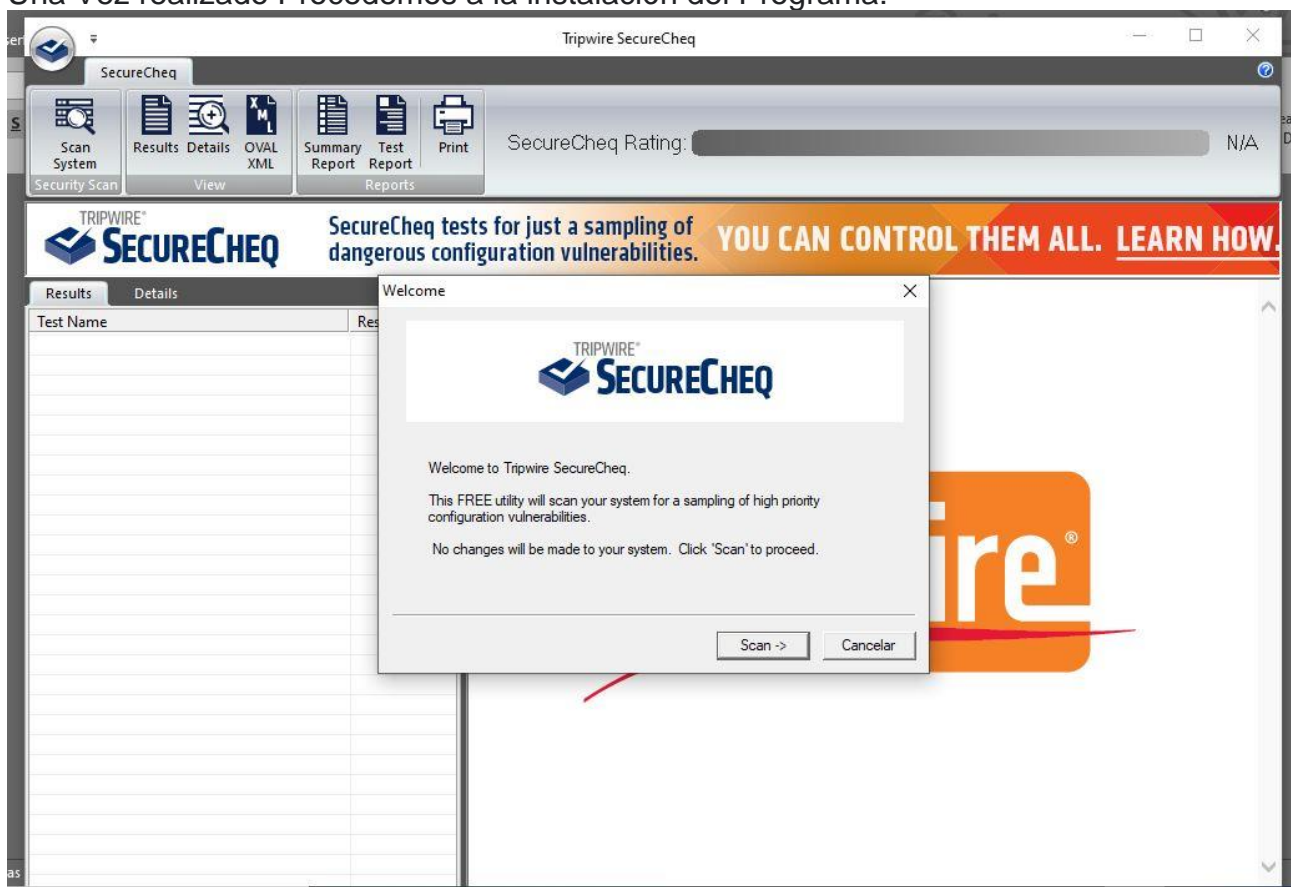
1ª Parte :

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,
- Windows 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:



PRÁCTICA : E5 – Instalar un ordenador Bastionado Windows o Linux MF0486_3 : Seguridad en Equipos Informáticos		Fecha	14 / 03 / 2022
		Página 6 de 4	
Curso	7.1. MF0486_3 Seguridad en equipos informáticos	Plan de Formación	FC-2021.I/II.000/1914256

Al correr el programa arroja el siguiente resultado:

The screenshot shows the Tripwire SecureCheq application window. The interface includes a top navigation bar with icons for Scan System, Results, Details, OVAL XML, Summary Report, Test Report, and Print. A progress bar indicates a 'SecureCheq Rating' of 18%. Below this is a banner for 'TRIPWIRE SECURECHEQ' with the text 'SecureCheq tests for just a sampling of dangerous configuration vulnerabilities. YOU CAN CONTROL THEM ALL. LEARN HOW.' The main content area displays a 'SecureCheq Summary Report' for computer 'DESKTOP-LVS1S31' scanned on '2022-04-17 09:11:27'. It lists two IP addresses: 192.168.56.1 and 192.168.1.36. A detailed list of 22 tests is shown on the left, with results ranging from 'Passed' to 'FAILED'. A large red bar indicates '18% Passing (for 22 tests)'. The 'OS HARDENING' section at the bottom provides advice on securing OS configurations.

Ahora vamos resolviendo uno a uno los problemas indicados.

PRÁCTICA : E5 – Instalar un ordenador Bastionado Windows o Linux MF0486_3 : Seguridad en Equipos Informáticos		Fecha	14 / 03 / 2022
		Página 7 de 4	
Curso	7.1. MF0486_3 Seguridad en equipos informáticos	Plan de Formación	FC-2021.I/II.000/1914256

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.

SecureCheq Rating: 18%

SecureCheq tests for just a sampling of dangerous configuration vulnerabilities. YOU CAN CONTROL THEM ALL.

Test Name	Result
Logging for Successful and Failed Logon At...	FAILED
Logging of Successful System Change Even...	FAILED
Security Event Log is Configured to a Suffici...	FAILED
Latest Security Patch	
Network Access: Shares That Can Be Access...	
Windows Firewall: Apply Local Firewall Rule...	
Windows Guest Account: Disabled	
Wireless Configuration Service: Disabled	
Remote Administration Service Permission	
Allow Logon through Remote Desktop Serv...	
Allow Logon through Terminal Services: No...	
Access: Trust All Installed Add-ins and Tem...	
Account Lockout Threshold Is Less than or ...	
All Remote Sessions Will Be Encrypted	
Allow Users to Connect Remotely Using Ter...	
Always Install with Elevated Privileges: Disa...	
Reset Account Lockout Counter after at Lea...	
Password History Memory Is Greater than o...	
Prevent IIS Installation: Enabled	
Audit Configuration	
Audit Database Object Access: Captured	
Audit for Unsuccessful Attempts	
Audit Object Access: Success and Failure	
Audit Policy Change: Success	
Audit Schema Object Management: Captur...	
Auto Creation of Admin Shares: Disabled	
Built-in Guest Account Renamed	

DETAILS

This test ensures that the event log is at least 80 megabytes. This provides ample opportunity for log data retention.

REMEDIATION

To remediate failure of this policy test, set the maximum size of the security event log to 81920 KB or greater.

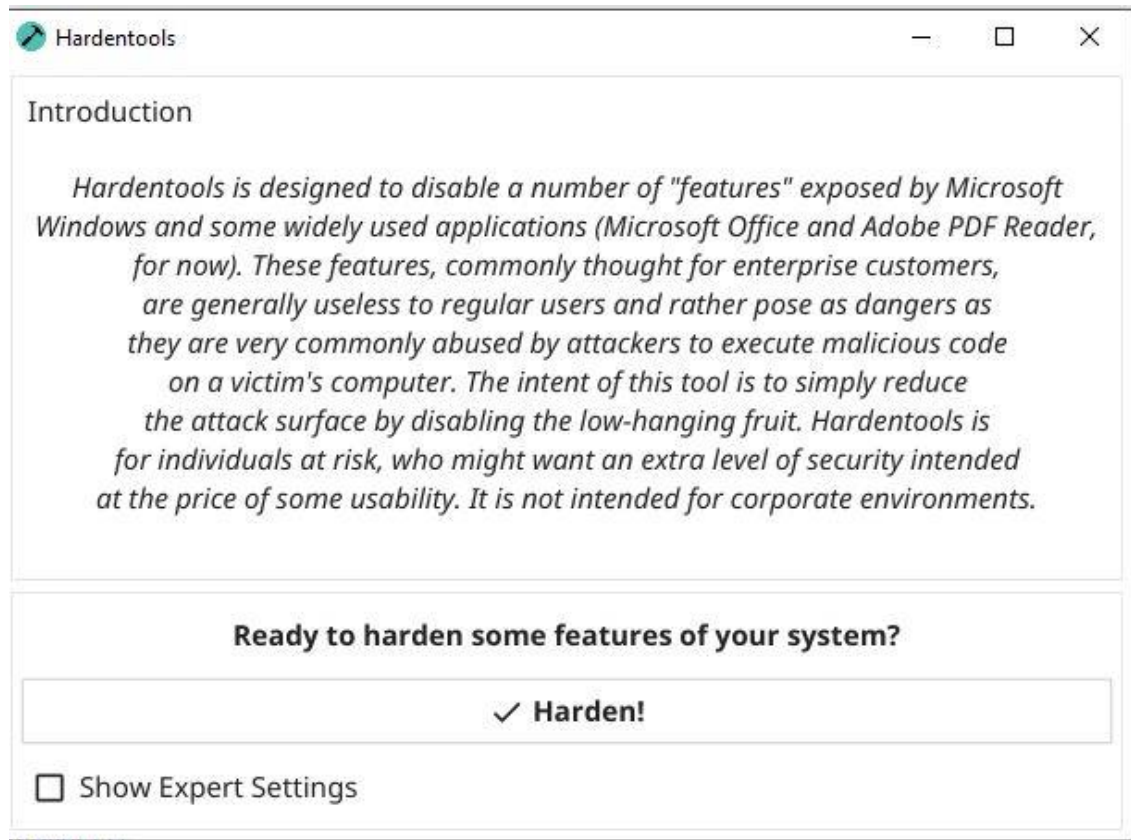
Setting the maximum size of the security event log to 81920 KB or greater on Windows 2008 R2, Windows 7:

1. Select a group policy object to edit within the **Microsoft Management Console**.
2. Select **Computer Configuration > Policies > Administrative Templates: Policy definitions (ADMX files) retrieved from the local machine > Windows Components > Event Log Service > Security**.
3. Right-click **Maximum Log Size (KB)** and select **Edit**.
4. Select **Enabled** and enter an integer value that is greater than or equal to **81920** then click **OK**.

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

Ahora vamos a probar con otro programa:

Hardentools



PRÁCTICA : E5 – Instalar un ordenador Bastionado Windows o Linux MF0486_3 : Seguridad en Equipos Informáticos			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	

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.



Operation in progress...

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

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

A continuación vemos que está Hardenizado.



Done! Risky features have been hardened!
For all changes to take effect please restart Windows.

Close		
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.