|  |  |  |  |
| --- | --- | --- | --- |
| **Nombre y Apellidos:** |  | **Firma del Alumno:** |  |
| **DNI:** |  | **Firma del Profesor:** |  |

|  |  |  |
| --- | --- | --- |
| **Apto:** | **No Apto:** | **Calificación:** |

**Instrucciones Generales**

La puntuación máxima será de 10 puntos.

Esta prueba tendrá una duración máxima de 100 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\_E3**
* 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 )
* **SFC :** Sistema operativo Windows ( Virtualizado )
* **Rootkit Hunter :** Sistema operativo Linux ( virtualizado )
* Pendrive.

**Descripción de la práctica**

**Instrucciones específicas**

El objetivo de esta práctica guiada será como se puede asegurar la **integridad** de los datos en sistemas Windows y Linux.

**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 100 minutos para realizar la práctica.

Se podrá realizar en cuatro partes con una duración cada una de 25 minutos.

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

**Páginas webs :**

**SFC ( System File Check)**

<https://en.wikipedia.org/wiki/System_File_Checker>

<https://neosmart.net/wiki/sfc/>

<https://support.microsoft.com/es-es/kb/929833>

**rootkit**

<https://es.wikipedia.org/wiki/Rootkit>

<https://es.wikipedia.org/wiki/Rkhunter>

<https://rootkit.nl/projects/rootkit_hunter.html>

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.

Se instalo Desde el Rootkit, un sotfware en repositorio llamado LINYS, una **herramienta de seguridad** muy completa para **realizar una auditoría de nuestro sistema Linux**.

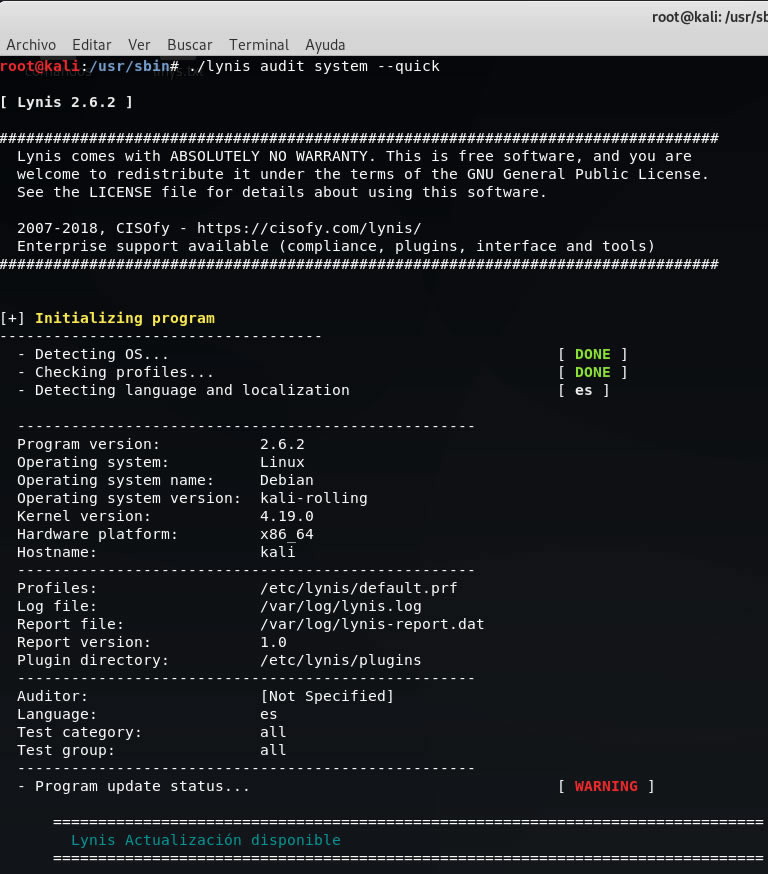
Se instalo desde el terminal en la plataforma de Kali-Linux con el comando:

$ apt-get install lynis

Una vez instalado se ejecutó con el comando:

$ lynis audit system --quick

**Al ejecutarse,** éste Analizó el software instalado en el sistema para detectar problemas de seguridad. Junto a la información relacionada con la seguridad. También buscó información general del sistema, en archivos y los paquetes instalados. Realizando un scanner corto al sistema y archivos por si presentaban algún problema. El proceso tardó unos 5 minutos y arrojó como resultados los siguientes listados de diagnóstico:



Auditando para el caso que nos interesa; el sistema de archivos.



Posteriormente, como resultado final, arrojó todo un diagnostico completo para el resto de componentes del sistema. Verificando que todo el sistema y sus carpetas estaban activos y óptimos ante cualquier amenaza.

