

Acción financiada por el SCE y por el Servicio Público de Empleo Estatal

PRUEBA OBJETIVA PRÁCTICA FINAL Análisis Forense - Servidor vulnerado : Uso de herramientas forenses MF0488_3 : Gestión de incidentes de seguridad informática			Fecha	07 / 08 / 2019
			Página 1 de 3	
Curso	SEGURIDAD INFORMÁTICA	Código del curso	18-38/000057	

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 120 minutos
(Temporalizados durante el módulo)

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 **MF0488_PRÁCTICA**
- 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.

Acción financiada por el SCE y por el Servicio Público de Empleo Estatal

PRUEBA OBJETIVA PRÁCTICA FINAL Análisis Forense - Servidor vulnerado : Uso de herramientas forenses MF0488_3 : Gestión de incidentes de seguridad informática			Fecha	07 / 08 / 2019
			Página 2 de 3	
Curso	SEGURIDAD INFORMÁTICA	Código del curso	18-38/000057	

Instrucciones específicas



Esta PRUEBA OBJETIVA PRÁCTICA FINAL consiste básicamente en realizar un informe pericial correcto, limpio y que conteste a las interrogantes que se plantean, sin dejar lugar a ambigüedades. Es un reto muy sencillo y que os ayudará a practicar a la hora de iniciaros en los análisis periciales.

Fuente : https://www.flu-project.com/2013/11/fpr9-solucion-al-reto-hacking_463.html

A partir de esta línea TODO ES FICCIÓN para dar contexto a la práctica, ¡así que nadie se alarme! y... ¡a por el reto!

El pasado día 3 de Noviembre ocurrió un trágico accidente al sur de la localidad madrileña de Fuenlabrada. Un avión JKNM-323 procedente de la base aérea de cuatro vientos se estrelló a su paso por el cuadrante oeste, en el barrio de Loranca.

En el suceso fallecieron el piloto y el copiloto, pero milagrosamente sobrevivieron dos miembros de la tripulación. En las declaraciones a los supervivientes por parte de las unidades policiales presentes en el suceso, confirmaron que oyeron una explosión en la cola del avión antes de precipitarse al vacío.

Acción financiada por el SCE y por el Servicio Público de Empleo Estatal

PRUEBA OBJETIVA PRÁCTICA FINAL Análisis Forense - Servidor vulnerado : Uso de herramientas forenses MF0488_3 : Gestión de incidentes de seguridad informática			Fecha	07 / 08 / 2019
			Página 3 de 3	
Curso	SEGURIDAD INFORMÁTICA	Código del curso	18-38/000057	

Instrucciones específicas

Las hipótesis de los expertos encaminan el suceso hacia un posible atentado de un grupo terrorista.

Dos semanas antes del terrible acontecimiento, la empresa aeronáutica JKNM Technologies denunció un robo de información en uno de sus servidores principales, situados en el CPD B de su sede de

Barcelona.

Tú labor como perito judicial informático consistirá en analizar el servidor vulnerado de JKNM Technologies en busca de alguna posible pista que permita a los cuerpos policiales ligar ambos acontecimientos y detener a los culpables.

Puedes pasar a recoger el disco duro a las dependencias de la Guardia Civil.

A continuación encontrarás las firmas del disco duro:

MD5 checksum: 2a0ddfa1b1d34df0b65d5c3ff60e2766SHA1
checksum: 18295c5222d52ec26b0420d5efb2b0868e7ddb91

Dispones de una semana para entregarnos los siguientes documentos:

1. Documento de cadena de custodia
2. Informe pericial documentando las evidencias recopiladas. Necesitamos especialmente que te centres en los archivos localizados en el disco duro que puedan haber sido sustraídos, indicando el cómo, cuándo y por qué. Así como en los ataques que puedan haber sido realizados durante la semana del 21 al 27 de Octubre de 2013, fecha en la que se interpuso la denuncia.

¡¡ Suerte, contamos contigo. ¡!

Acción financiada por el SCE y por el Servicio Público de Empleo Estatal

PRUEBA OBJETIVA PRÁCTICA FINAL Análisis Forense - Servidor vulnerado : Uso de herramientas forenses MF0488_3 : Gestión de incidentes de seguridad informática			Fecha	07 / 08 / 2019
			Página 4 de 3	
Curso	SEGURIDAD INFORMÁTICA	Código del curso	18-38/000057	

Instrucciones específicas



Normalmente en un análisis forense os entregarán una copia física del disco duro a analizar, siempre que no os toque directamente realizarla vosotros mismos. Para la realización de este prueba práctica final se les proporciona directamente el clonado del disco duro de un servidor clonado mediante "dd", y además, se han limpiado todos los archivos que no eran de interés en el pericial, facilitando así la resolución de la práctica.

En ese disco duro se encontraba instalado un servidor web Apache que servía una aplicación web de la empresa JKNM Technologies y desde la que sus empleados descargaban documentos confidenciales de los aviones que fabricaba previa autenticación con un usuario y contraseña válidos.

Los pasos a realizar con dicha clonación del disco duro son :

- 1) Comprobar los hashes del disco duro para verificar que es una clonación del disco duro original. Para ello se puede utilizar por ejemplo las utilidades "md5sum" y "sha1sum"
- 2) Posteriormente habrá que abrirlo con alguna utilidad como FTK Imager o Autopsy, en esta ocasión nosotros se recomienda este segundo, por su posibilidad de parsear y recopilar los archivos localizados en función de su tipología..
- 3) Análisis de las evidencias
- 4) Informe pericial

Acción financiada por el SCE y por el Servicio Público de Empleo Estatal

PRUEBA OBJETIVA PRÁCTICA FINAL Análisis Forense - Servidor vulnerado : Uso de herramientas forenses MF0488_3 : Gestión de incidentes de seguridad informática			Fecha	07 / 08 / 2019
			Página 5 de 3	
Curso	SEGURIDAD INFORMÁTICA	Código del curso	18-38/000057	

Instrucciones específicas

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 120 minutos para realizar la práctica.

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

Páginas webs : https://www.flu-project.com/2013/11/fpr9-solucion-al-reto-hacking_463.html

Análisis Forense : <http://periciales.eu/wp-content/uploads/2014/06/ejemplo-informe-pericial-general.pdf>

Programas Forenses en Windows :

<https://www.incibe.es/jornadas-incibe-espacios-ciberseguridad/estudiantes/programa-forense-windows>

Guía de toma de evidencias :

<https://www.incibe-cert.es/guias-y-estudios/guias/toma-evidencias-windows>

Informe Pericial:

<http://openaccess.uoc.edu/webapps/o2/bitstream/10609/46105/6/fredmorantesTFM0116memoria.pdf>

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.

Acción financiada por el SCE y por el Servicio Público de Empleo Estatal

PRUEBA OBJETIVA PRÁCTICA FINAL Análisis Forense - Servidor vulnerado : Uso de herramientas forenses MF0488_3 : Gestión de incidentes de seguridad informática			Fecha	07 / 08 / 2019
			Página 6 de 3	
Curso	SEGURIDAD INFORMÁTICA	Código del curso	18-38/000057	

Descripción de la práctica
