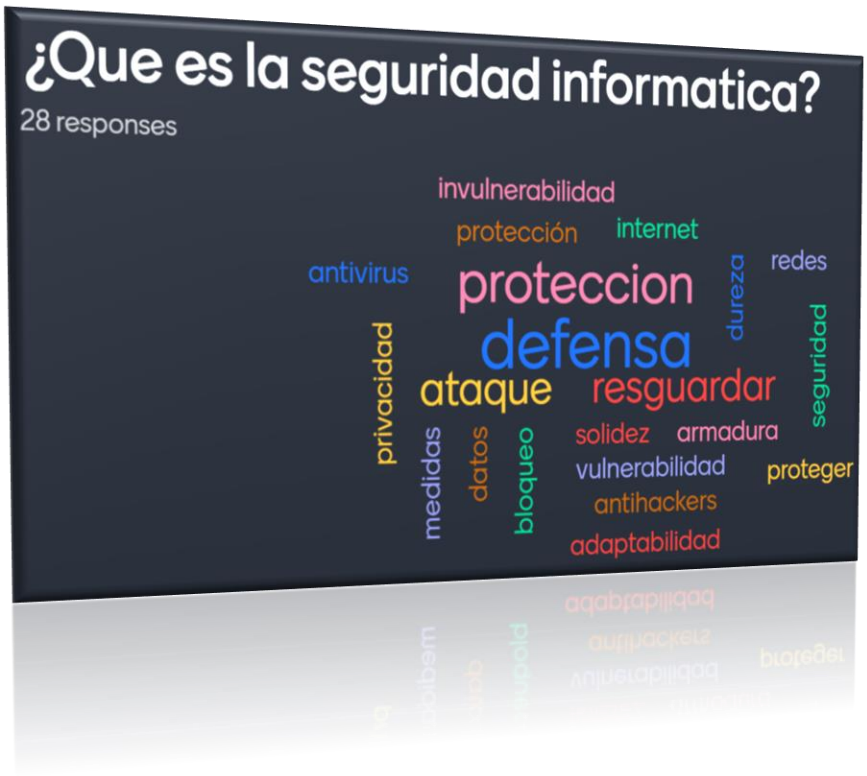
Universidad Paraguayo Alemana

UNIVERSIDAD PARAGUAYO ALEMANA
HEIDELBERG - ASUNCIÓN



Seguridad TICs

Prof.: Chrystian Ruiz Diaz

Contenido

Nota de Uso Académico

Este documento ha sido preparado exclusivamente para el uso académico del docente. Este documento no puede ser distribuido a ninguna otra parte ni utilizado para ningún otro propósito, diferente al establecido como alcance en el proyecto académico de la **UNIVERSIDAD PARAGUAYO ALEMANA**. El uso indebido del material fuera del ámbito académico no representa ninguna responsabilidad del docente.

Análisis Forense con Herramientas de Kali Linux

Objetivo

Los alumnos aprenderán a utilizar herramientas de análisis forense disponibles en Kali Linux para investigar y extraer información relevante de archivos, sistemas y redes.

Consideraciones

I. **Compatibilidad de Módulos y Librerías:** Este material es una guía referencial para la instalación y pruebas a realizarse. Es responsabilidad del usuario verificar e instalar las versiones de los módulos, librerías y dependencias que sean compatibles con el entorno de trabajo.

II. **Manejo de Copia y Pegado de Código entre PC Física y VM:** Al copiar y pegar sentencias desde la PC física a la máquina virtual (VM), es común que se copien caracteres no visibles (como saltos de línea `\r\n` u otros). Para evitar problemas, se recomienda pegar el código en un editor de texto dentro de la VM y ajustar manualmente los espacios, tabulaciones y saltos de línea según sea necesario para cada sentencia.

III. **Corrección de Errores:** Detectar, investigar y corregir errores de sintaxis es una parte integral del trabajo. Los estudiantes deben estar preparados para identificar y solucionar estos problemas como parte del proceso de aprendizaje y desarrollo.

Parte 1: Análisis de Metadatos con ExifTool

Herramienta: ExifTool

Ejercicio

1. **Instalación**:

```
sudo apt-get install exiftool
```

2. **Análisis de una Imagen**:
   - Descarga una imagen de ejemplo o usa una imagen propia.
   - Ejecuta el siguiente comando para extraer metadatos:

```
exiftool /ruta/a/tu/imagen.jpg
```

3. **Tareas**:
   - Documenta la información obtenida, incluyendo:

- Fecha y hora de creación.
- Dispositivo utilizado.
- Coordenadas GPS (si están presentes).

4. **Preguntas**:
   - ¿Qué información puedes inferir sobre la imagen a partir de los metadatos?
   - ¿Cómo podrían estos datos ser útiles en una investigación forense?

Parte 2: Análisis de Volcado de Memoria con Volatility

Herramienta: Volatility

Ejercicio

1. **Instalación**:

```
sudo apt-get install volatility
```

2. **Captura de un Volcado de Memoria**:
   - Usa un volcado de memoria de ejemplo o captura uno (en sistemas Linux, se pueden usar herramientas específicas como LiME).
3. **Análisis**:
   - Lista los procesos activos en el volcado de memoria:

```
volatility -f /ruta/a/tu/memory.dmp --profile=Win7SP1x64
pslist
```

4. **Tareas**:
   - Identifica procesos sospechosos o desconocidos.
   - Investiga los módulos cargados en la memoria.
5. **Preguntas**:
   - ¿Qué procesos se están ejecutando en el sistema?
   - ¿Puedes identificar algún proceso que parezca malicioso o fuera de lugar?

Parte 3: Captura y Análisis de Tráfico de Red con Wireshark

Herramienta: Wireshark

Ejercicio

1. **Instalación**:

```
sudo apt-get install wireshark
```


2. **Captura de Tráfico**:
   - Abre Wireshark y selecciona tu interfaz de red.
   - Inicia la captura y navega por algunos sitios web.
3. **Análisis**:
   - Filtra el tráfico HTTP:

```
http
```

4. **Tareas**:
   - Identifica las solicitudes GET y POST.
   - Examina los paquetes capturados para encontrar información relevante, como credenciales no cifradas.
5. **Preguntas**:
   - ¿Qué tipos de datos sensibles puedes identificar en el tráfico capturado?
   - ¿Cómo podrías proteger esta información en un entorno real?

Parte 4: Análisis de Sistemas de Archivos con Autopsy

Herramienta: Autopsy

Ejercicio

1. **Instalación**:

```
sudo apt-get install autopsy sleuthkit
```

2. **Creación de un Caso**:
   - Abre Autopsy y crea un nuevo caso.
   - Añade una imagen de disco o una carpeta con archivos para analizar.
3. **Análisis**:
   - Busca archivos borrados y recupera información de interés.
   - Analiza los registros de actividad.
4. **Tareas**:
   - Documenta los hallazgos, como archivos recuperados y registros importantes.
   - Realiza un análisis de línea de tiempo de las actividades en el sistema.
5. **Preguntas**:
   - ¿Qué archivos borrados pudiste recuperar?
   - ¿Qué información importante encontraste en los registros de actividad?

Conclusión

Cada una de estas actividades proporciona una oportunidad práctica para que los alumnos se familiaricen con las herramientas de análisis forense disponibles en Kali Linux. Al completar estos ejercicios, los estudiantes ganarán experiencia en el uso de estas herramientas y comprenderán mejor cómo se aplican en investigaciones forenses reales.

