Manual de Prácticas – Apto V

Información general

- **Materia:** SEMINARIO DE ACTUALIZACION TECNOLOGICA PERMANENTE PARA INGENIERO EN TELEINFORMATICA POR OPERACION VIRTUAL V
- **Duración del curso:** Inicio 16-01-2025 Fin 01-06-2025
- **Docente:** José Guadalupe Alvarado Ornelas
- **Número de prácticas:** 3 + Proyecto Final

- **Objetivo general:** Capacitar al estudiante en el análisis, recuperación, preservación e interpretación de evidencia digital mediante herramientas especializadas.**Práctica 1: Forense Digital con Autopsy**

Objetivo: Utilizar las herramientas de **Autopsy** para realizar un análisis forense básico, incluyendo la recuperación de archivos eliminados, análisis del historial web, extracción de metadatos de imágenes y búsqueda de palabras clave.

Materiales Necesarios

- **Autopsy** (descargable desde https://www.autopsy.com/)
- **Imagen forense de prueba** (puedes usar una imagen de disco como **"Evidencia.img"** o descargar una de repositorios forenses como Digital Corpora), o utilizar alguna prfoporcionada en clases.
- **Dispositivo de almacenamiento** (USB o disco duro con datos eliminados para práctica).

Procedimiento

1. Configuración del Caso en Autopsy

1. Abre **Autopsy** y crea un nuevo caso.
2. Asigna un nombre (ej: **"Practica_Forense"**) y una descripción.
3. Selecciona la **imagen forense** (o un disco/USB real si lo estás analizando).
4. Configura los módulos de análisis (selecciona todos los disponibles para un análisis completo).

2. Recuperación de Archivos Eliminados

1. Ve a la pestaña **"File Analysis"**.
2. Busca en **"Deleted Files"** para ver archivos eliminados.
3. Selecciona uno (ej: un documento .docx o una imagen .jpg) y examina su contenido.
4. Exporta el archivo para verificar su recuperación.

3. Análisis del Historial Web

1. Navega a **"Web History"** en el panel de resultados.
2. Revisa las URLs visitadas, cookies y caché del navegador.
3. Filtra por dominios sospechosos (ej: sitios de descargas o phishing).
4. Exporta el historial en formato CSV para su revisión.

4. Extracción de Metadatos de Imágenes

1. Localiza una imagen (ej: foto.jpg) en el sistema de archivos.
2. Haz clic derecho y selecciona **"View File Metadata"**.
3. Analiza datos como:
    - **Fecha de creación/modificación**
    - **Geolocalización** (si está disponible en EXIF).
    - **Modelo de cámara** (si fue tomada con un smartphone).
4. Compara con otras imágenes para detectar inconsistencias.

5. Búsqueda de Palabras Clave (Keyword Search)

1. Ve a **"Keyword Search"** e ingresa términos relevantes (ej: "confidencial", "contraseña").
2. Autopsy buscará en archivos, registros y contenido oculto.
3. Examina los resultados para identificar información sensible.

6. Análisis de Eventos (Timeline Analysis)

1. Abre **"Timeline"** para ver una línea de tiempo de actividad.
2. Filtra por fechas sospechosas (ej: día de un incidente).
3. Identifica archivos creados, modificados o eliminados en ese período.

Resultados Esperados

- Recuperación exitosa de al menos **5 archivos eliminado**.
- Identificación de **sitios web visitados** en el historial.
- Extracción de **metadatos** (fecha, ubicación, modelo de cámara).
- Detección de **palabras clave** relevantes en archivos.
- Generación de un **informe forense** con hallazgos.

Aprendizaje obtenido:

Esta práctica permite familiarizarse con las funciones esenciales de **Autopsy** en un entorno forense, desde la recuperación de datos hasta el análisis de metadatos. Se recomienda experimentar con diferentes imágenes forenses para profundizar en el uso de la herramienta.

Nota: Si no tienes una imagen forense, puedes crear una con **FTK Imager** o **dd** en Linux copiando un USB con archivos eliminados previamente.

¿Necesitas una imagen de prueba? Puedes usar **"Defense Advanced Research Projects Agency (DARPA) datasets"** o descargar muestras de CFReDS

Practica 2: Identificación de Vulnerabilidades Utilizando Shodan

Objetivo:

El objetivo de esta tarea es que los estudiantes adquieran habilidades prácticas en el uso de Shodan para identificar dispositivos vulnerables y evaluar posibles riesgos de seguridad en un entorno controlado.

Instrucciones:

1. **Registro y Acceso a Shodan**:
    - Si aún no tienes una cuenta en Shodan, regístrate en Shodan.io y familiarízate con la plataforma. Asegúrate de entender las políticas de uso y las limitaciones del servicio gratuito.

2. **Búsqueda de Dispositivos Vulnerables**:
    - Utiliza Shodan para buscar dispositivos vulnerables en Internet basándote en las siguientes consultas. Para cada consulta, captura al menos tres resultados que consideres relevantes y analiza la información proporcionada por Shodan.

Consultas:

- Encuentra servidores MySQL que están expuestos directamente a Internet, lo que podría ser un riesgo si no están protegidos adecuadamente**.**

```
port:3306
```

- Buscar dispositivos vulnerables a la vulnerabilidad Log4Shell (CVE-2021-44228):

```
vuln:CVE-2021-44228
```

- Identificar cámaras IP expuestas con contraseñas por defecto:

```
http.title:"webcam" "default password"
```

- Buscar routers con puertos de administración abiertos:

```
port:8080 "router"
```

- Buscar servidores FTP que permiten acceso anónimo:

```
ftp anon
```

Entrega:

- Un reporte que incluya capturas de pantalla de los resultados obtenidos y una explicación breve (1-2 párrafos) para cada consulta sobre por qué los dispositivos encontrados son vulnerables y qué medidas podrían tomarse para protegerlos.

3. **Reflexión Ética**:
    - Escribe una reflexión corta (1-2 párrafos) sobre las implicaciones éticas y legales de usar herramientas como Shodan. Considera cómo estas herramientas pueden ser utilizadas tanto para proteger como para explotar sistemas.

Formato de Entrega:

- Un documento en formato PDF que incluya todos los resultados de las búsquedas, capturas de pantalla, análisis y reflexiones.
- El reporte debe ser claro y bien estructurado, con secciones tituladas para cada consulta y análisis. Todas las capturas de pantalla deben estar acompañadas de una breve explicación.

Practica 3: Investigación de una persona utilizando OSINT

Objetivo:

Aplicar técnicas de Open Source Intelligence (OSINT) para recolectar y analizar información pública de diversas fuentes abiertas, demostrando las habilidades de investigación y análisis en el ámbito de la ciberseguridad.

Instrucciones:

1. **Selecciona una empresa o persona pública:**
   - Elige una empresa, organización o figura pública que sea accesible para realizar una investigación. **No** se permite investigar personas privadas ni realizar actividades que comprometan la ética o la privacidad.

2. **Recopila información utilizando las siguientes técnicas y herramientas OSINT:**
   - **Motores de búsqueda avanzados**: Utiliza Google Dorks para encontrar información relevante (como documentos, bases de datos, configuraciones de servidores).
   - **Redes sociales**: Analiza los perfiles públicos en redes como Facebook, Twitter, LinkedIn, etc.
   - **Whois**: Utiliza esta herramienta para obtener información sobre los dominios asociados con la organización o figura pública.
   - **Shodan**: Busca dispositivos conectados a Internet asociados con la empresa o el objetivo seleccionado.
   - **theHarvester**: Realiza una búsqueda para obtener correos electrónicos, nombres de dominio, y otra información relevante.
   - Otras herramientas de tu elección, como Maltego, Recon-ng o SpiderFoot.

3. **Organiza los resultados de tu investigación:**
   - **Información básica**: Describe los datos principales del objetivo (ubicación, dominios, correos electrónicos, etc.).
   - **Redes sociales**: ¿Qué tipo de información puedes obtener de sus perfiles públicos? (publicaciones, conexiones, imágenes, etc.).
   - **Dispositivos y servidores**: Detalla cualquier información obtenida de Shodan o similar (IP, servicios abiertos, versiones de software).
   - **Vulnerabilidades potenciales**: Identifica posibles riesgos o vulnerabilidades en la infraestructura digital de la organización o figura pública basada en tu investigación.

4. **Análisis y conclusiones:**
   - **Resumen de hallazgos:** Describe tus descubrimientos más importantes y relevantes.
   - **Implicaciones de seguridad:** Reflexiona sobre cómo la información obtenida puede ser utilizada para mejorar la ciberseguridad del objetivo.

- **Recomendaciones:** Sugiere al menos 3 medidas que la empresa o persona pública debería tomar para proteger mejor su información pública.

5. **Informe final:**
   - Escribe un informe detallado de 3 a 5 páginas con la información obtenida, el análisis realizado y las recomendaciones propuestas.
   - Incluye capturas de pantalla de las herramientas utilizadas y de los hallazgos relevantes.
   - Asegúrate de utilizar un lenguaje formal y estructurar tu informe de manera clara.

Entrega:

- El trabajo debe ser entregado en formato PDF a través de la plataforma
- Cualquier hallazgo debe respetar las leyes locales y principios éticos. No se permite la recolección de información mediante métodos intrusivos o ilegales.

Aprendizaje obtenido:

Esta tarea les permitirá a los estudiantes practicar técnicas OSINT de manera ética y responsable, al mismo tiempo que desarrollan habilidades analíticas en ciberseguridad.

Proyecto Final de Ciberseguridad: Auditoría de Seguridad en un Entorno de Trabajo

Objetivo:

Realizar un análisis integral de seguridad en un entorno de trabajo, evaluando la red, el cuarto de telecomunicaciones, el acceso físico y los controles de seguridad más comunes. El estudiante deberá identificar vulnerabilidades informáticas y físicas, documentarlas en un reporte detallado y proponer recomendaciones para mitigar los riesgos encontrados.

Fases del Proyecto:

1. Análisis de Red y Seguridad Informática

- **Escaneo de Red:**
  - Utilizar herramientas como **Nmap, Wireshark o Nessus** para identificar dispositivos conectados, puertos abiertos y servicios en ejecución.
  - Detectar posibles equipos con configuraciones inseguras (ej.: contraseñas por defecto, servicios obsoletos).
- **Evaluación de Vulnerabilidades:**
  - Analizar posibles fallos en la red (ej.: falta de segmentación VLAN, tráfico no cifrado, SNMP público).
  - Revisar políticas de firewall y filtrado de tráfico.

2. Inspección del Cuarto de Telecomunicaciones

- **Infraestructura Física:**

- Verificar condiciones ambientales (temperatura, humedad, ventilación).
- Revisar cableado estructurado (UTP, fibra óptica) y etiquetado correcto.
- Comprobar redundancia eléctrica (UPS, generadores).

- **Seguridad del Cuarto:**
  - Confirmar controles de acceso (biométricos, tarjetas RFID, llaves).
  - Evaluar sistemas de videovigilancia y registros de acceso.

3. Revisión del Acceso Físico

- **Controles de Entrada/Salida:**
  - Verificar si existen políticas de identificación (badges, listas de acceso).
  - Detectar posibles puntos ciegos en cámaras de seguridad.
- **Protección de Equipos:**
  - Revisar si hay computadoras o servidores sin bloqueo físico (Kensington locks).
  - Confirmar que no hay documentos sensibles a la vista.

4. Evaluación de Controles Comunes de Seguridad

- **Políticas de Autenticación:**
  - Verificar si se utiliza autenticación multifactor (MFA).
  - Revisar políticas de contraseñas (longitud, complejidad, caducidad).
- **Copias de Seguridad (Backups):**
  - Confirmar que existan respaldos automatizados y cifrados.
  - Validar que se realicen pruebas de restauración.

Entregables (Reporte en PDF):

1. Portada

- Nombre del proyecto, alumno, grupo y fecha.

2. Introducción

- Objetivo del proyecto y metodología utilizada.

3. Hallazgos de Vulnerabilidades

- **Red y Sistemas:**
  - Lista de puertos abiertos innecesarios.
  - Servicios sin parches o con configuraciones débiles.
- **Cuarto de Telecomunicaciones:**
  - Falta de control de acceso o monitoreo ambiental.
- **Acceso Físico:**
  - Puntos de entrada sin supervisión adecuada.
- **Controles de Seguridad:**
  - Contraseñas débiles, falta de MFA o backups no verificados.

4. Recomendaciones de Mitigación

- **Red:**
  - Implementar segmentación VLAN, actualizar firmware y cerrar puertos no utilizados.
- **Cuarto de Telecomunicaciones:**
  - Instalar sistemas de control de acceso y monitoreo ambiental.
- **Acceso Físico:**

  - Añadir cámaras en zonas críticas y políticas de identificación estrictas.
- **Controles de Seguridad:**
  - Forzar MFA, mejorar políticas de contraseñas y automatizar backups.

5. Conclusiones

- Impacto de las vulnerabilidades encontradas.
- Lecciones aprendidas durante el análisis.

6. Anexos (Opcional)

- Capturas de pantalla de escaneos (Nmap, Nessus).
- Fotos del entorno evaluado (sin exponer información sensible).
- Diagramas de red propuestos para mejoras.

Criterios de Evaluación:

Aspecto	Puntaje
Profundidad del análisis (Herramientas usadas, detección de vulnerabilidades)	30%
Reporte de Vulnerabilidades (Claridad, documentación de riesgos)	25%
Recomendaciones (Soluciones técnicas y físicas viables)	25%
Presentación (Formato PDF profesional, estructura, evidencias)	20%

Notas Adicionales:

- El proyecto puede realizarse en un entorno simulado (ej.: VirtualBox, redes de laboratorio) o en una empresa real (con autorización).
- Se debe mantener confidencialidad si se trabaja con datos reales.