Laboratorio 1: Análisis de Amenazas en Entorno Virtualizado

Enunciado para el Campista

Objetivo del laboratorio:
Aprender a identificar amenazas comunes en entornos digitales mediante el análisis de un archivo sospechoso en un entorno controlado. Este laboratorio te permitirá familiarizarte con herramientas básicas de virtualización y análisis de malware.

Herramientas necesarias

1. **VirtualBox o VMware Workstation Player** (gratuitos y fáciles de usar).
2. **Sistema operativo virtualizado**: Una máquina virtual con Windows 10 (versión trial) o Linux (por ejemplo, Ubuntu).
3. **Herramientas de análisis de malware:**
    - **VirusTotal** (plataforma en línea).
    - **Process Explorer** (de Sysinternals para Windows).
    - **Wireshark** (para analizar tráfico de red).
    - **Sandbox segura:** Opcional, si se desea usar **Cuckoo Sandbox** para profundizar.

Configuraciones previas al laboratorio

1. Instalación y configuración de VirtualBox o VMware Workstation Player

1. Descarga e instala VirtualBox o VMware desde su sitio oficial.
2. Crea una nueva máquina virtual:
    - Asigna 2 GB de RAM y 20 GB de almacenamiento.
    - Configura el adaptador de red en modo NAT.
    - Instala el sistema operativo (Windows 10 o Linux).

2. Configuración del sistema operativo virtualizado

1. Instala las siguientes herramientas dentro de la máquina virtual:
    - **Process Explorer**: Descárgalo desde la página de Sysinternals.
    - **Wireshark**: Descárgalo e instálalo desde su página oficial.
2. Configura el sistema operativo:
    - Aísla la máquina virtual deshabilitando las conexiones compartidas con el host.
    - Asegúrate de que el firewall del sistema operativo esté habilitado.

3. Preparación de un archivo sospechoso

Visita virustotal y descarga un archivo inofensivo simulado (simulando malware). Este archivo estará en un entorno seguro para evitar riesgos reales.

Instrucciones Paso a Paso

Parte 1: Configuración del entorno virtualizado

1. Abre VirtualBox o VMware y ejecuta la máquina virtual creada.
2. Verifica que todas las herramientas (Process Explorer, Wireshark) estén instaladas y funcionando correctamente.
3. Desconecta la máquina virtual de internet para evitar interacciones externas durante el análisis.

Parte 2: Identificación de amenazas comunes

1. Familiarízate con las herramientas instaladas:
    - Usa **Process Explorer** para observar procesos activos en el sistema operativo.
    - Configura **Wireshark** para monitorear tráfico de red local.

Parte 3: Análisis del archivo sospechoso

1. Carga el archivo proporcionado en **VirusTotal** (desde el navegador en el host, no dentro de la máquina virtual).
    - Documenta si el archivo es detectado como malicioso y qué amenazas son reportadas.
2. Ejecuta el archivo en la máquina virtual y monitorea los procesos usando **Process Explorer**:
    - Identifica procesos desconocidos o sospechosos iniciados por el archivo.
3. Analiza el tráfico de red con **Wireshark**:
    - Captura paquetes mientras el archivo se ejecuta y busca comportamientos anómalos (por ejemplo, conexiones no autorizadas o repetitivas).

Parte 4: Documentación de hallazgos

1. Crea un informe donde detalles:
    - Las observaciones realizadas con VirusTotal.
    - Procesos sospechosos detectados con Process Explorer.
    - Cualquier tráfico anómalo capturado con Wireshark.
2. Incluye capturas de pantalla y una breve descripción de cada hallazgo.

Resultados de aprendizaje

Criterios:

1. **Preparación del entorno virtualizado:** Verificación de que las configuraciones sean correctas y seguras.
2. **Uso de herramientas:** Capacidad para utilizar VirusTotal, Process Explorer y Wireshark de manera adecuada.
3. **Identificación de amenazas:** Habilidad para reconocer procesos y tráfico anómalo.
4. **Documentación:** Calidad del informe presentado, claridad y detalle de los hallazgos.

Este laboratorio te permitirá adquirir habilidades iniciales para analizar amenazas en un entorno controlado, una de las competencias fundamentales en ciberseguridad. ¡Buena suerte!