Informe.

Miembros del equipo:
Jesus Alejandro Ramírez Baltazar.
Angel Gabriel Cruz Velazquez.
Ana Naybeth Medina Perez.

Modulo 1. Extracción de eventos relevantes del Visor de eventos (registros de eventos)

El módulo 1 tiene como finalidad **automatizar la extracción y exportación de eventos de los registros de Windows**. El script principal importa el módulo “Modulo.psm1” mediante el “Manifiesto.psd1”. Al ingresar el usuario el script solicita que elegir una de las tres opciones (Security, System, Application), luego tiene que ingresar la fecha de inicio y fin, también el tipo de formato del archivo (CSV, HTML o XML) y al final el nombre del archivo sin la extensión, si uno de los datos no está correctamente le saldrá un mensaje de error y le solicitará ingresar de nuevo hasta que estén bien.

Casi al final el código mandara un mensaje que se generó correctamente el archivo, si no sale el mensaje puede significar que no se está ejecutando como administrador ya que en la parte de Security necesita permisos que solo lo tiene si se ejecuta en PowerShell administrador.

Modulo 2. Correlación de procesos activos con conexiones de red

Se realizó un análisis del sistema utilizando PowerShell para correlacionar procesos activos con sus respectivas conexiones de red. Primero se enumeraron los procesos en ejecución junto con sus rutas, filtrando aquellos con ubicación conocida para facilitar la identificación. Posteriormente, se obtuvieron todas las conexiones TCP activas y se relacionaron con los procesos que las generaron, mostrando detalles como puertos abiertos, direcciones remotas y estado de la conexión. Esta información fue exportada en formatos CSV y XML para su revisión.

Además, se ejecutó una función que detecta procesos potencialmente sospechosos, evaluando si cuentan con firma digital válida y si se ejecutan desde rutas inusuales como carpetas temporales, de descargas o el escritorio. Los procesos que no cumplen con estos criterios fueron marcados como sospechosos y documentados en un archivo HTML.

El análisis permitió identificar procesos legítimos del sistema y de aplicaciones comunes, así como algunos ejecutables sin firma digital que mantenían conexiones activas con direcciones IP externas. Se recomienda revisar manualmente estos procesos, restringir la ejecución desde rutas vulnerables y automatizar este tipo de auditorías para mantener la seguridad del entorno.

Modulo 3. Investigación de direcciones IP remotas mediante AbuseIPDB

El script lo que hace es extraer las IP remotas del módulo 2 primero comprobando que dicho formato con las IP exista en formato CSV para posteriormente comprobar su reputación dando datos como el país de origen, el ISP, el nombre del dominio y el tipo de uso. Esto datos los recolecta usando el API AbuseIPDB, adicional a esto también te proporciona el nivel de riesgo de la información recolectada por dicho API de la IP, El script te muestra en pantalla todos los datos anteriormente mencionados incluyendo el nivel de riesgo para finalmente generarlos en formato CSV.