Desarrollar habilidades en el uso de comandos básicos de Linux para procesar y analizar datos contenidos en un archivo de texto. El archivo a trabajar es vulnerables.txt.

Cada práctica debe ser ejecutada en linux, editada con vim y agrupada en un script individual, es decir, se entregarán 8 scripts junto a este informe.

Cada ejercicio debe adjuntar una captura de pantalla de la salida del script y el código fuente del script en **UNA SOLA CAPTURA DE PANTALLA O FOTO**.

Ejercicio:

1. Filtrar las líneas que contengan el texto COERCE_PLUS.
2. Mostrar solo las líneas que incluyan STATUS_LOGON_FAILURE.
3. Seleccionar todas las líneas donde el puerto sea 445.

Ejercicio:

1. Obtener todas las direcciones IP de los sistemas vulnerables.
2. Extraer los nombres de las máquinas asociadas con el dominio cooperativa.fin.ec.
3. Crear una lista única de las vulnerabilidades explotadas por efsrpc.

Ejercicio:

1. Contar cuántos sistemas diferentes están utilizando Windows 11.

2. Generar una lista única de las vulnerabilidades asociadas con el exploit PrinterBug.
3. Identificar cuántos sistemas tienen credenciales asociadas con el usuario si.testing.

Ejercicio:

1. Calcular cuántas veces aparece cada tipo de servicio (SMB, COERCE_PLUS) en el archivo.
2. Generar un reporte que contenga la cantidad total de líneas agrupadas por sistema operativo.
3. Identificar qué direcciones IP tienen múltiples vulnerabilidades asociadas.

Ejercicio:

1. Extraer los nombres de las máquinas y los sistemas operativos en un formato de dos columnas separados por tabulación.
2. Crear un listado de todos los sistemas que tienen firmas digitales deshabilitadas (signing:False) junto con sus direcciones IP.
3. Identificar cuáles máquinas tienen tanto VULNERABLE como Exploit Success en el mismo registro.

Ejercicio:

1. Comparar la cantidad de sistemas vulnerables entre Windows 10 y Windows 11.
2. Listar los sistemas que tienen credenciales válidas pero están marcados como STATUS_LOGON_FAILURE.
3. Identificar las direcciones IP asociadas con más de un tipo de exploit, separadas por el nombre del exploit.

Ejercicio:

1. Contar cuántas líneas tienen exactamente cinco palabras antes de la primera aparición de un paréntesis (.
2. Calcular el porcentaje de sistemas que tienen SMBv1 deshabilitado (SMBv1:False).
3. Crear un archivo nuevo que contenga solo los registros donde el dominio no sea cooperativa.fin.ec, ordenado alfabéticamente por el nombre de la máquina.

Ejercicio:

1. Crear un reporte agrupado por tipo de servicio (SMB o COERCE_PLUS) que muestre el número total de vulnerabilidades detectadas por grupo.
2. Generar un archivo que contenga todas las direcciones IP vulnerables y sus sistemas operativos en un formato CSV.
3. Identificar las líneas duplicadas en el archivo original y contar cuántas veces se repiten.