FLUJO DE DATOS NTFS

NTFS Alternate Data Stream (ADS) es un flujo oculto de Windows, que contiene metadatos del archivo, como atributos, número de palabras, nombre del autor y acceso, y hora de modificación de los archivos.

ADS puede bifurcar datos en archivos existentes sin cambiar ni alterar su funcionalidad, tamaño o visualización a las utilidades de navegación de archivos.

ADS permite a un atacante inyectar código malicioso en archivos de un sistema accesible y ejecutarlos sin ser detectados por el usuario.

PASOS PARA CREAR STREAMS NTFS

Paso 1 en CMD inicie c:\>notepad miarchivo.txt:leon.txt y haga clic en 'Sí' para crear el nuevo archivo, introduce algunos datos y guárdalo.

Paso 2 Inicie c:>notepad miarchivo.txt:tigre.txt y haga clic en 'Sí' para para crear el nuevo archivo, introducir algunos datos y guardar el archivo.

Paso 3 Vea el tamaño del archivo miarchivo.txt (Debería ser cero)

Paso 4 Los siguientes comandos se pueden utilizar para ver o modificar los datos ocultos en los pasos 1 y 2, respectivamente:

```
notepad miarchivo.txt:leon.txt
```

```
notepad miarchivo.txt:tigre.txt
```

Nota: El Bloc de notas es una aplicación compatible con el flujo. No debe utilizar flujos alternativos para almacenar información crítica

PASOS PARA MANIPULAR FLUJOS NTFS

Puede manipular flujos NTFS para ocultar un archivo malicioso en otros archivos, como archivos de texto.

Paso 1 Ocultar Trojan.exe (programa malicioso) en Readme.txt (flujo)

```
c:\>type c:\Trojan.exe >c:\Readme.txt:Trojan.exe
```

El comando "type" oculta un archivo en un flujo de datos (ADS) detrás de un archivo existente. Los dos puntos (:) indica el comando para crear o utilizar ADS.

Paso 2 Crear un enlace al flujo Trojan.exe dentro del archivo Readme.txt

Después de ocultar el archivo Trojan.exe detrás del archivo Readme.txt es necesario crear un enlace para ejecutar el archivo Trojan.exe desde el flujo. Esto crea un acceso directo para Trojan.exe en el stream.

```
C:>mklink backdoor.exe Readme.txt:Trojan.exe
```

Paso 3 Ejecutar el troyano

Escriba C:\>backdoor para ejecutar el troyano que ha escondido detrás de Readme.txt. Aquí, el backdoor es el acceso directo creado en el paso anterior, que ejecuta el troyano.

Nota: Utilice el Bloc de notas para leer el archivo oculto. Por ejemplo, el comando C:\>notepad sample.txt:secret.txt crea el flujo secret.txt detrás del archivo archivo sample.txt