Black System

Seguridad Informática

Seguridad Informática

FPTD/2021/019/2080

Metadatos

Pueden definirse como unos datos que describen a otros datos. Por ejemplo en las propiedades de un documento de Office, se puede encontrar información clasificada como Metadatos.
Algunos ejemplos de Metadatos son:

Creador del Documento
Nombre del equipo donde se creo
Sistema Operativo
Una nombre de una impresora.
Una Ruta (Path)

Existen muchas herramientas para la extracción de los METADATOS, la FOCA es una de ellas. Es una herramienta para el S.O Windows, escrita por el consultor de seguridad español “Chema Alonso”.

Otra opción para poder ver los metadatos de los archivos es: https://metashieldclean-up.elevenpaths.com/
El inconveniente de esta opción es que tenemos que ir de un archivo en uno.

nmap

Nmap nos permitirá obtener una gran cantidad de información sobre los equipos de nuestra red, es capaz de escanear qué hosts están levantados, e incluso comprobar si tienen algún puerto abierto, si están filtrando los puertos (tienen un firewall activado), e incluso saber qué sistema operativo está utilizando un determinado objetivo.

- Hay 65535 puertos en cada IP. Para escanear todos los puetos tendríamos que realizar el siguiente escaneo:

nmap ip -p-

- Para que solo nos muestren los puertos que están abiertos:

nmap ip -p- --open

- Otro parámetro para indicarle que vaya más rápido pero que haga más ruido o que vaya más lento y sigiloso es:

nmap ip -p- --open -T5 (con este iria rápido pero ruidoso)

- Para que no aplique diferencial DNS (para ahorrar tiempo en el escaneo)

nmap ip -p- --open -T5 -n

- Para exportar los resultados a un archivo que podamos grepear

nmap ip -p- --open -T5 -n -oG NombreArchivo

Una vez que sabemos que puertos están abiertos vamos a lanzarle unos scripts básicos para saber la versión y servicio que corren en esos puertos y exportarlo a un tipo de archivo Nmap

- nmap -sC -sV -pPuertosOpen(separados por comas) ip -oN
  ejemplo: nmap -sC -sV -p22,80 192.168.1.190 –oN targeted

nmap

- Comando para hacer UDP SCAN:
  Nmap –sU IP
- Comando para identificar la versión del sistema operativos del equipo que se esta analizando:
  nmap –O –p(Puerto) IP
- Comando nmap usado para escaneo sigiloso y completo:
  Nmap –sS –O –sV ip