Mayo 28 2019

FOCA (Fingerprinting Organizations with Collected Archives)

By mar10

FOCA (Fingerprinting Organizations with Collected Archives) es una herramienta utilizada principalmente para encontrar metadatos e información oculta en los documentos que examina. Estos documentos pueden estar en páginas web, y con FOCA se pueden descargar y analizar. OS Windows

Los documentos que es capaz de analizar son muy variados, siendo los más comunes los archivos de Microsoft Office, Open Office, o ficheros PDF, aunque también analiza ficheros de Adobe InDesign, o svg por ejemplo.

Estos documentos se buscan utilizando tres posibles buscadores que son Google, Bing y DuckDuckGo. La suma de los tres buscadores hace que se consigan un gran número de documentos. También existe la posibilidad de añadir ficheros locales para extraer la información EXIF de archivos gráficos, y antes incluso de descargar el fichero se ha realizado un análisis completo de la información descubierta a través de la URL.

Con todos los datos extraídos de todos los ficheros, FOCA va a unir la información, tratando de reconocer qué documentos han sido creados desde el mismo equipo, y qué servidores y clientes se pueden inferir de ellos.

Download:https://www.elevenpaths.com/es/labstools/foca-2/index.html#

FOCA comenzó siendo una herramienta de análisis de metadatos para dibujar una red a partir de los mismos, y en la actualidad se ha convertido en un referente en el ámbito de la seguridad informática, gracias a las numerosas opciones que incorpora. Gracias a dichas opciones con FOCA es posible realizar múltiples ataques y técnicas de análisis como:

- Extracción de metadatos.
- Análisis de red.
- DNS Snooping.
- Búsqueda de ficheros comunes.
- Juicy files.
- Búsqueda de proxys.
- Reconocimiento de tecnologías.
- Fingerprinting.
- Leaks.
- Búsqueda de backups.
- Forzado de errores.
- Búsqueda de directorios abiertos

Además FOCA tiene una serie de plugins para aumentar la funcionalidad o el número de ataques que se pueden realizar a los elementos obtenidos durante el análisis que pueden ser descargados desde el Market.

FOCA incluye un módulo de descubrimiento de servidores, cuyo objetivo es automatizar el proceso de

búsqueda de los mismos usando técnicas enlazadas recursivamente. Las técnicas utilizadas en este sentido son:

Web Search
Busca nombres de hosts y dominios a través de la búsqueda de URLs asociadas al dominio principal, cada link es analizado para extraer de él nuevos nombres de hosts y nombres de domino.

DNS Search
A cada dominio se le consultará cuáles son los hostnames configurados en los servidores NS, MX y SPF para descubrir nuevos nombres de hosts y nombres de dominios.

Resolución IP
Cada nombre de host se resolverá contra el DNS para obtener la dirección IP asociada a ese nombre de servidor. Para que esta tarea sea lo más certera posible, la consulta se realiza contra un DNS interno de la organización.

PTR Scanning
Para encontrar más servidores en el mismo segmento de una determinada dirección IP FOCA realizará un escaneo de registros PTR.

Bing IP
Por cada dirección IP descubierta se lanzará un proceso de búsqueda de nuevos nombres de dominio asociados a esa dirección IP.

Common names
Este módulo está pensado para realizar ataques de diccionario contra el DNS. Utiliza un fichero de texto donde se añade una lista de nombres de host comunes como ftp, pc01, pc02, intranet, extranet, internal, test, etcétera.

DNS Prediction
Utilizado para aquellos entornos en los que se haya descubierto un nombre de equipo que pueda dar pie a pensar que se está utilizando un patrón en el sistema de nombres.

Robtex
El servicio Robtex es uno de los múltiples servicios que hay en Internet para analizar las direcciones IP y los dominios, FOCA lo utiliza para intentar descubrir nuevos dominios buscando en la información que Robtext posee de ella.

FUENTE ORIGINAL : https://www.elevenpaths.com/es/labstools/foca-2/index.html

Tags:
FOCA
Hacking
Windows
Windows 10
hacking-windows
Cracking