ANÁLISIS DE DOMINIOS CON **FOCA**

Mauro de los Santos Nodar mauro.delossantos@udc.es

fic

UNIVERSIDADE DA CORUÑA

ÍNDICE

1. Introducción....2

2. Metadatos....3
Análisis de metadatos con FOCA....3
Pervirtiendo los metadatos....6

3. Descubrimiento de red....7
WebSearch....7
DNS....7
Bing IP....8
Shodan....8
Network Discovery con FOCA....8
Más....9

4. Vulnerabilidades....10
Juicy files....10
Backups....11
Fugas de información con Subversion....11
DNS Cache Snooping....12
Métodos HTTP inseguros....13
Data Leaks....13
IIS URL Short Name....13
Conclusiones y ataque ejemplo....14

5. Potenciación de FOCA....14
Plugins....14
SVN Downloader....14
SQLi....14
Have I Been Pwned....15
Más....15
Integración de FOCA con otras herramientas y posibles ataques....15
FOCA + Herramientas Spidering como Burp Suite....15
FOCA Intruder: *FOCA* + Burp Suite + Intruder....15
Malware vía actualizaciones: *FOCA* + Evilgrade....15
Ataques Spear Phising: *FOCA* + Metasploit....15
URL's desde el pasado: *FOCA* + Archive.org....15
FOCA + Maltego....16

6. Bonus....16
Análisis de metadatos de un documento....16
Eliminación de metadatos....17

1. Introducción

En el siguiente report analizaremos varios dominios con la herramienta *FOCA*, dividiendo nuestro trabajo de 'auditoría' en varias fases: una primera fase dedicada a los metadatos, posteriormente haremos un descubrimiento de red, seguido de un análisis de vulnerabilidades y finalmente tocaremos una parte de 'potenciación' de *FOCA* al integrarla con diferentes herramientas y usar sus plugins para sacarle el máximo partido.

Pero, primero de todo, ***¿qué es FOCA?*** *FOCA* (*Fingerprinting Organizations with Collected Archives*) es una herramienta orientada al pentesting. Aunque en un principio nace para ser utilizada principalmente para encontrar metadatos e información oculta en los documentos que examina, con el paso de los años se le han ido añadiendo nuevas funcionalidades y mejoras que la hacen mucho más potente.

También se han creado '*FOCAs* alternativas' como la '*Evil FOCA*', especializada en ataques de red, o la '*Forensic FOCA*', orientada al ámbito forense.

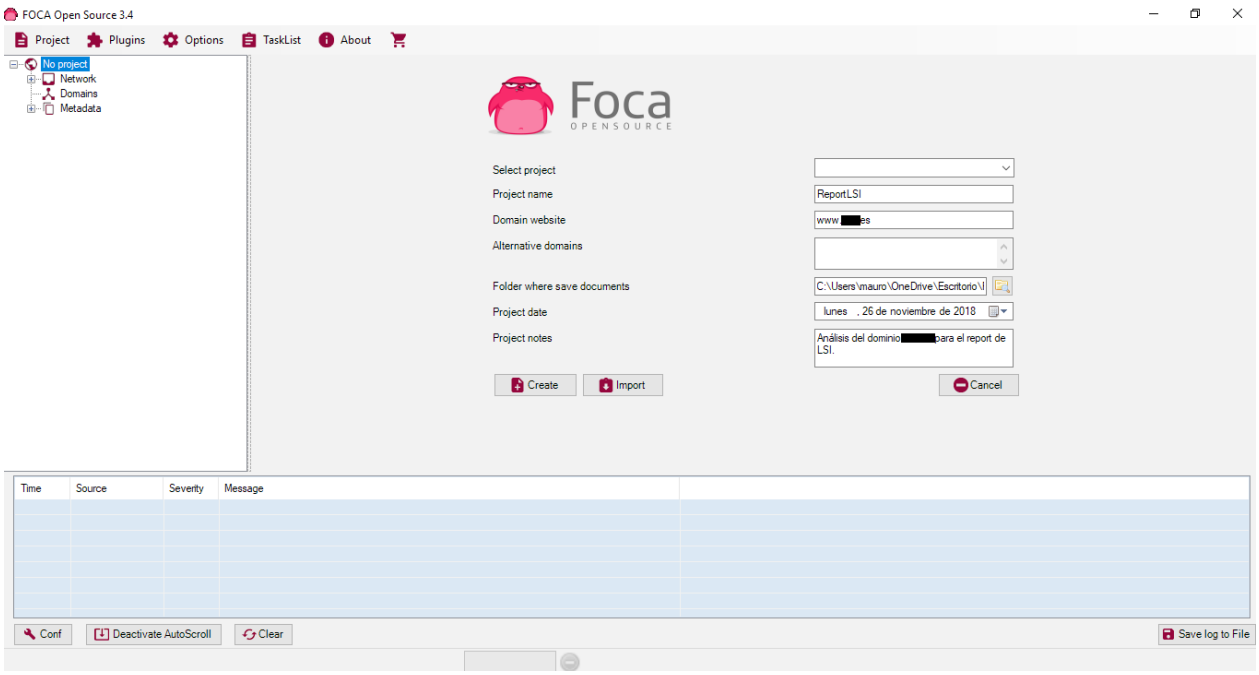
Como culmen a esta herramienta, en 2017, nace '*FOCA Open Source*', una *FOCA* ampliada, donde se recogen todas las mejoras aplicadas desde su nacimiento en 2008, y además, se libera el código. Con esta *FOCA* será con la que llevaremos a cabo el siguiente análisis de dominios.

2. Metadatos

Los metadatos son datos que contienen información relativa a un documento o fichero concreto. Por ejemplo, un archivo de texto podría contener información sobre el usuario que lo ha hecho, cuantas modificaciones ha sufrido o el software que ha sido utilizado. Una foto, podría sin embargo, tener información sobre las coordenadas GPS donde ha sido tomada o la marca y modelo de la cámara que la hizo.

Los metadatos, son muy útiles, ya que facilitan la búsqueda de documentos, catalogan su información y son usados por los motores de búsqueda de Internet, pero, si hacemos una mala gestión de ellos, pueden ser muy perjudiciales ya que pueden revelar información que no queremos que sea pública.

Análisis de metadatos con FOCA



FOCA es una herramienta muy potente en cuánto al análisis de metadatos, así que vamos a ver como sacarle partido:

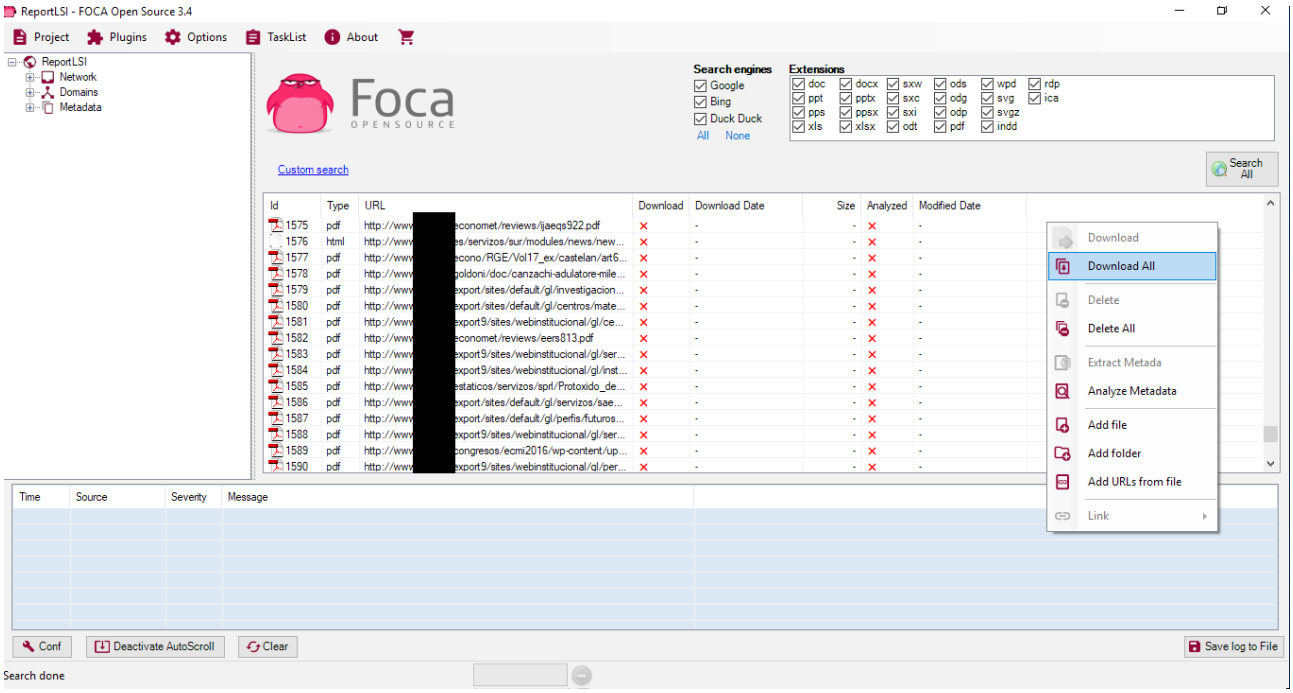
Primero de todo, seleccionaríamos Project → New Project y rellenaríamos los datos requeridos. Fundamentales, serán el 'Domain Website' a auditar (un dominio de una universidad española, en nuestro caso) y la carpeta donde queremos guardar toda la información obtenida. Una vez rellenadas las casillas oportunas, le damos a 'Create'.

Una vez creado el proyecto, procederemos a conseguir los documentos del dominio a auditar, para ello podremos usar tres motores de búsqueda diferentes: Los gigantes *Bing* y *Google* y el menos conocido pero muy útil *DuckDuckGo*. Marcamos los tres para extraer todos los documentos posibles del dominio.

También podemos ver como podemos elegir que extensiones de documentos queremos, para así descartar los archivos con las extensiones no deseadas. Las marcaremos todas.

FOCA, aquí lo que hace es hacer una búsqueda personalizada en los tres motores de búsqueda, buscando ficheros con las extensiones indicadas en el dominio establecido. Si queremos ver o modificar a nuestro gusto la sintaxis concreta solo tendríamos que hacer click en '*Custom Search*', en la parte superior izquierda, debajo del logo.

Una vez elegidos motores de búsqueda y extensiones de documentos, le daremos a '*Search All*' y veremos como empiezan a aparecer los archivos y a colocarse en la hoja de cálculo en el centro de la pantalla. Vemos como en esto caso, *FOCA* ha conseguido 1686 documentos para analizar.



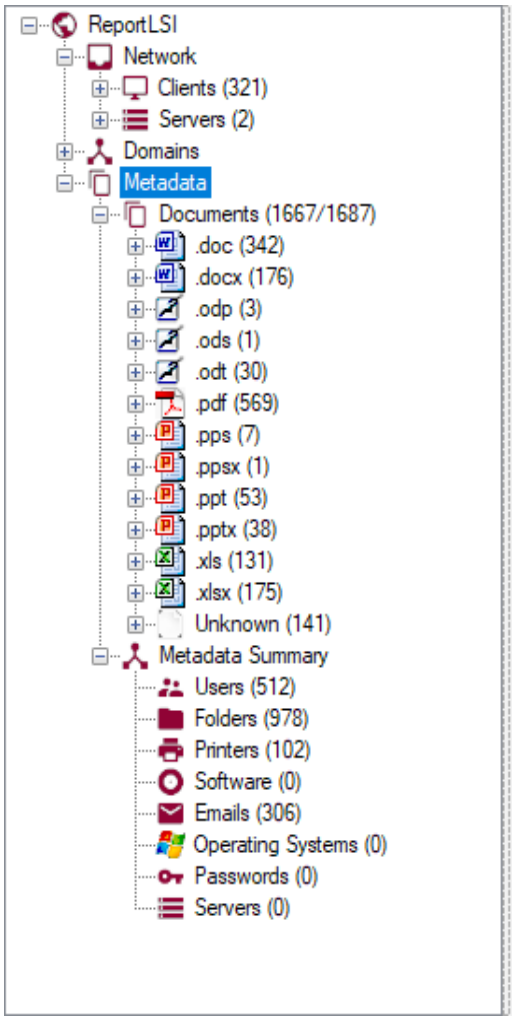
Seguido a esto, simplemente tendríamos que hacer click derecho encima de la hoja de cálculo con los documentos, '*Download All*'. Una vez descargados, procederíamos a '*Extract Metadata*' y '*Analyze Metadata*' obteniendo así todos los metadatos de todos los ficheros del dominio.

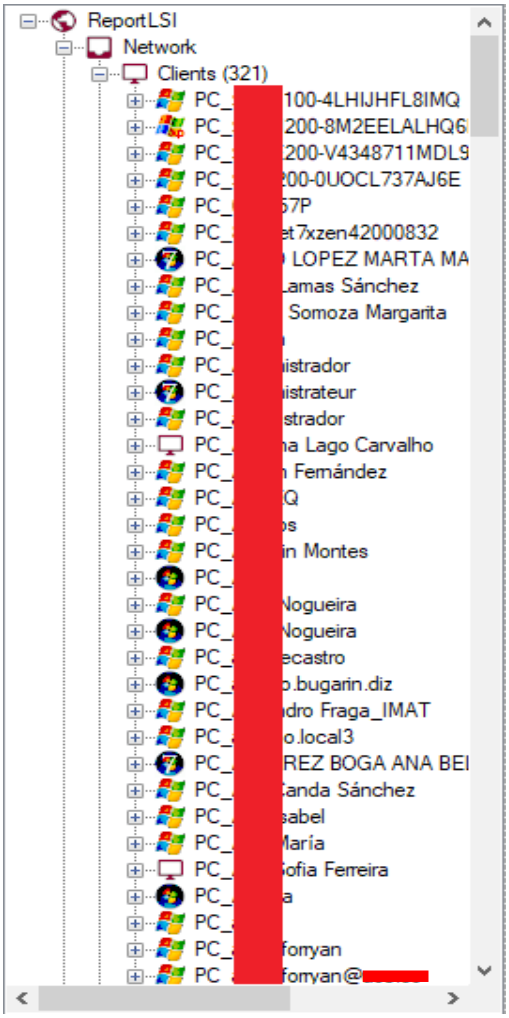
Una vez analizados, vemos como en muy poco tiempo ya hemos conseguido información jugosa de una organización como son Nombres de Usuario (512!) o emails (306!). Hemos sacado también los sistemas operativos en las máquinas de los trabajadores (vemos SO anticuados como Windows Vista o 7 en varios equipos, incluso algún XP), a priori los objetivos más débiles contra un posible ataque, carpetas de ficheros en la organización, impresoras (102), software utilizado para elaborar los

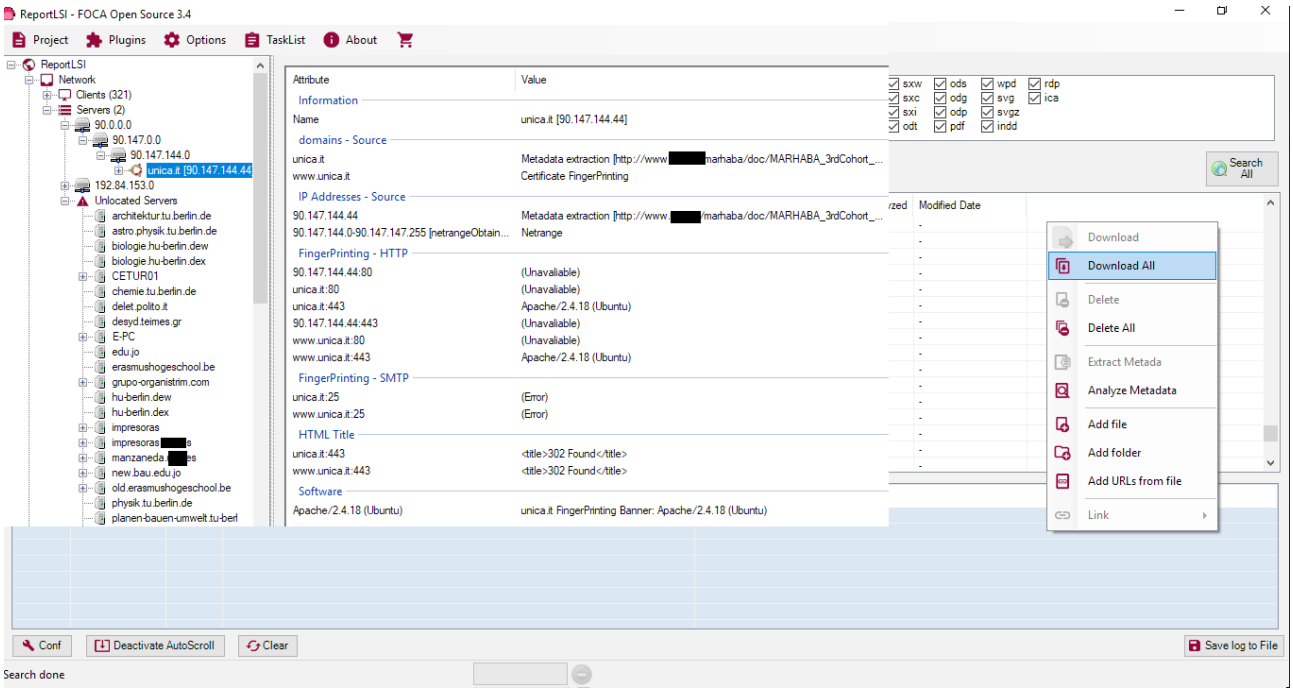
documentos (aunque no aparezca en *Software*, haciendo click en cualquier documento o máquina, vemos qué software se ha usado en él), etcétera.
En la parte de '*Network*', vemos 321 máquinas con sus nombres (bastante significativos), sistemas operativos, software y demás. Y en '*Servers*', vemos como ya conocemos dos IP's con información apetecible (que corre un Apache/2.4.18 o el netrange entre otras) y múltiples *Unlocated Servers*.

En conclusión, vemos como en pocos minutos, y solo examinando los documentos públicos en un dominio, *FOCA* nos da un montón de información, en teoría, oculta o privada de una organización.

Todos estos datos, como vemos en la imagen inferior, se sitúan en el apartado '*Metadata Summary*' y en '*Network*'. Buceando un poco por las máquinas ('*Clients*'), usuarios, servers, etc. conseguimos más información.





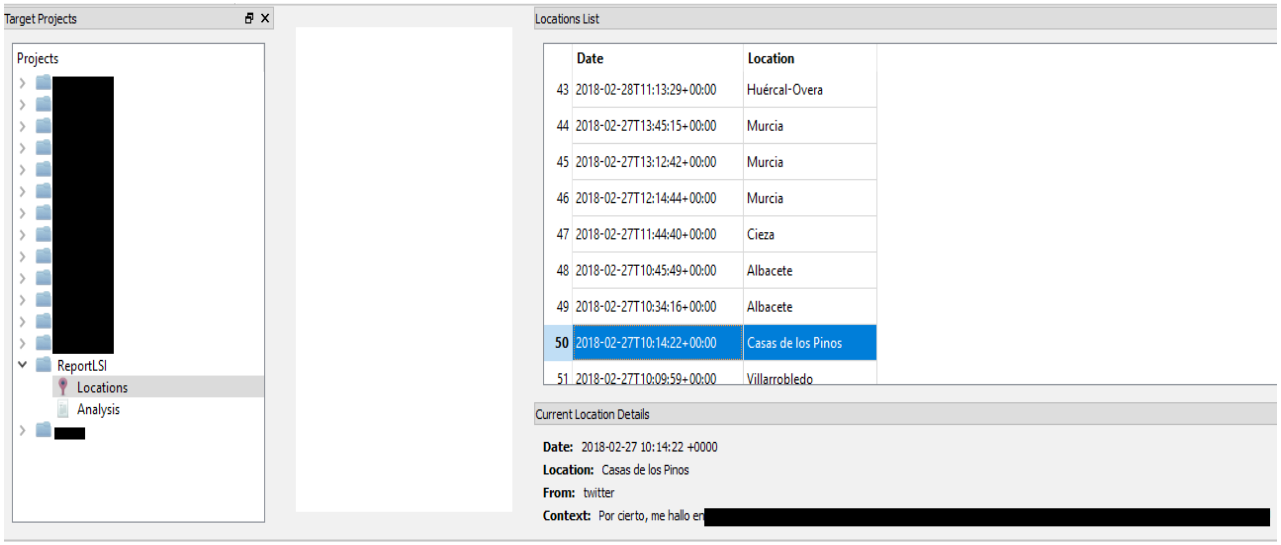


Pervirtiendo los metadatos

Una vez hecho esto, ya tenemos información mucho más valiosa de lo que imaginamos para tener una primera toma de contacto y un primer análisis general de la organización. Para dar uno de los miles de ejemplos interesantes donde hacemos uso de ella, vamos a coger un nombre de usuario que *FOCA* nos ha revelado, preferiblemente que tenga acceso a varias carpetas, y que estas carpetas sean carpetas con muchos archivos y usuarios vinculados (podemos averiguarlo fácilmente viendo los accesos a las carpetas descubiertas, los documentos extraídos de las mismas, etc).

Buscamos su nombre y apellidos o su email en *Google* y, rápidamente nos encontramos con su cuenta de twitter.

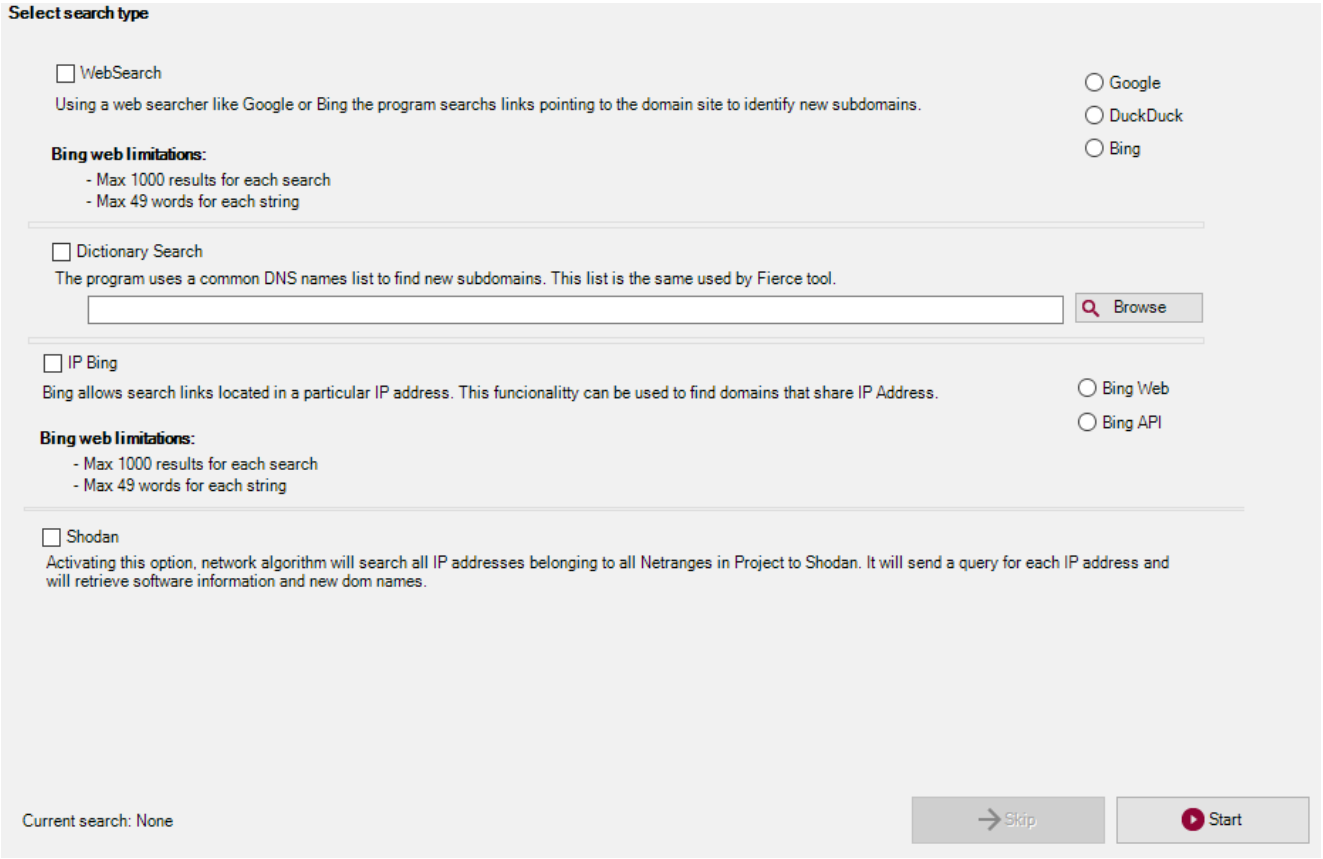
Llevando esto de los metadatos un poco más allá y aprovechando lo anterior, podemos utilizar otra herramienta (de las muchísimas que existen), que es **Creepy**, para analizar su cuenta de twitter y sacar un perfil de sus últimas y más frecuentes geolocalizaciones. Pudiendo así, sacar por ejemplo, a parte de datos privados como su dirección, o los sitios a donde se va de vacaciones, que a priori, si no tenemos nada en contra de ese pobre trabajador, son inservibles, datos más relevantes, como por ejemplo, si trabaja por las mañanas o por las tardes, la ubicación de su despacho, etcétera. En la imagen inferior podemos ver un ejemplo de esto, donde se nos muestra la localización geográfica de los tweets de la cuenta indicada, acompañados por su fecha y hora:



3. Descubrimiento de red

En este apartado se van a estudiar las funcionalidades de footprinting y fingerprinting que *FOCA* lleva a cabo para hacer un proceso de '*Network Discovery*', para así localizar servidores internos, direccionamiento IP de equipos y segmentos de red, descubrimiento DNS, nombres de equipos, SO, software..y mucho más.

Si vamos a la opcion '*Network*', arriba a la izquierda en FOCA, vemos como tenemos 4 casillas para marcar. Estas son 4 técnicas que usa FOCA en su proceso de descubrimiento de red. Vamos a comentarlas brevemente:



WebSearch

Busca nombres de hosts y dominios a través de URLs asociadas al dominio principal, en *Google*, *Bing* o *DuckDuckGo* de forma que cada link se analiza para buscar nuevos nombres de dominio y hosts. *FOCA* maximiza la ventana de 1000 resultados máximos haciendo todo tipo de búsquedas y eliminando URLs ya obtenidas.

DNS

Es una opción muy amplia. La información de los recursos de un dominio que mantiene un servidor DNS se organiza en unos ficheros llamados mapas de dominios, que se componen de registros, con valioso contenido. Por ejemplo, los registros NS (contienen la dirección IP y nombre de los servidores DNS), los MX (los datos de servidores de correo), las direcciones IP de máquinas están en los registros A (IPv4) y AAAA (IPv6), y así muchos más (SOA, SPF, DKIM, IM, LDAP…). *FOCA* consultará más de 70 tipos de registros para intentar obtener nombres y roles de equipos, subdominios, y más datos valiosos.

En cuanto al DNS, comentar tres cosas más:

- *FOCA* intentará hacer una transferencia de zona de todos los servidores DNS que encuentre para intentar obtener todos los registros del dominio de forma global. Aunque no se debería poder hacer, si está mal configurado y se consigue, esta técnica entrega todo el mapa de dominio de la empresa, con servidores externos e internos.

- *FOCA*, lee también de un fichero (por defecto el mismo que utiliza la herramienta *Fierce*) nombres de host comunes (FTP, pc01, pc02, intranet, etcétera) y trata de resolverlos contra los dominios principales del proyecto.

- Y por último, *FOCA* tiene una funcionalidad llamada *DNS Prediction*, que pretende predecir nombres de servidores DNS cuando se detecta un patrón en la forma de nombrarlos. Por ejemplo, si encontramos un server llamado DNS-S-1, sería sensato pensar que podría existir un DNS-S-2,3,4,5... Esta herramienta genera diferentes combinaciones respecto a un nombre de servidor base y las usa para descubrir nuevos servidores.

Bing IP

Por cada IP que tenemos, *FOCA* usará *Bing* para encontrar todos los nombres de dominios alojados en esa misma IP (hoy en día esto es posible gracias al hosting compartido y a los virtual hosts). Saber esta información nos ayuda para tener más y quizás mejores vectores de ataque. Esto, puede paralizar el proyecto si encontramos una IP con miles de dominios asociados, por lo que tenemos la opción '*Skip*', que saltará a la siguiente IP, para así no eternizar el proyecto.

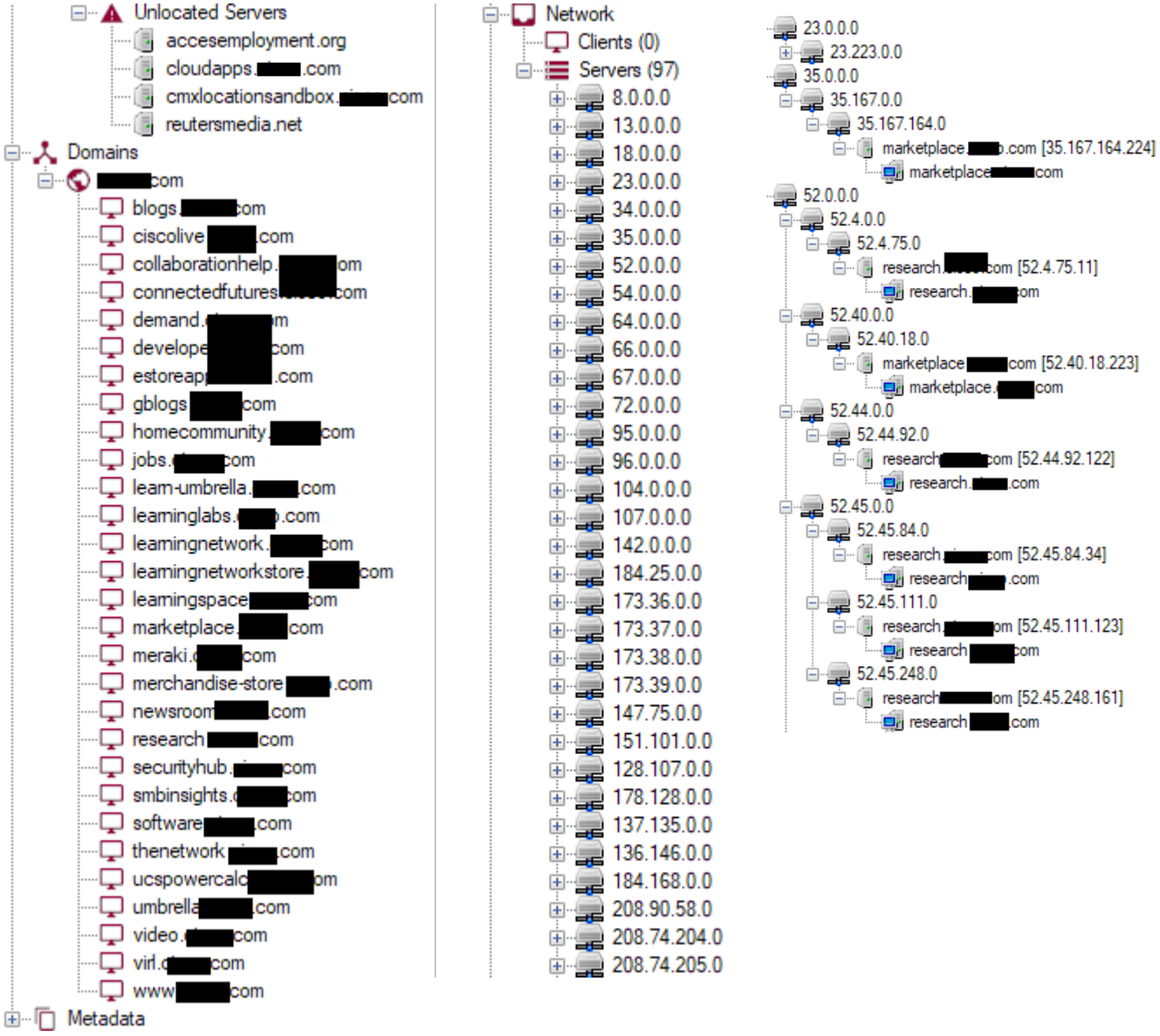
Shodan

Es un buscador que permite hacer búsquedas basadas en equipos para obtener gran información de dispositivos conectados a Internet. A diferencia de los buscadores tradicionales, las arañas de *Shodan* no indexan documentos si no que rastrean cabeceras. *FOCA* lo utiliza para obtener información de las IP´s recolectadas como sistemas operativos, nombre de host, servicios ofrecidos...Los resultados que ofrece *Shodan* pueden ser muy interesantes ya que analizan millones de puertos de las direcciones de internet obteniendo información HTTP[S], FTP, SNMP, etcétera.

Network Discovery con FOCA

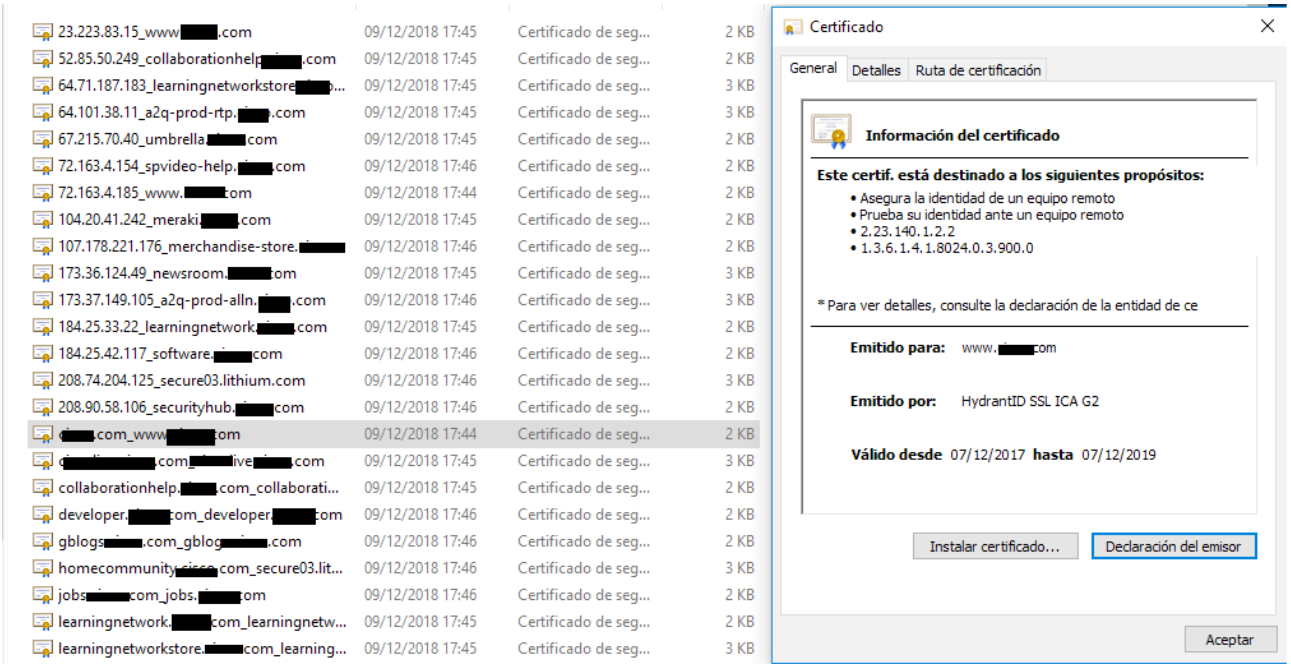
En nuestro ejemplo de auditoría, cambiaremos de dominio esta vez para analizar a una de las grandes empresas informáticas de hoy en día. Marcaremos las cuatro opciones y le daremos a Start. Cuando *FOCA* haya acabado, tendremos toda la información del descubrimiento de red tanto en los *Servers* de la Pestaña *Network* como en *Domains*. Si se encuentra nueva información de cuentas, equipos, software, SO, etcétera se actualizarán debidamente en sus campos correspondientes.

En este caso, hemos hallado alrededor de 100 servidores en el dominio indicado así como un gran número de dominios extra y 'Unlocated Servers'. Por lo tanto, vemos cuán exitoso puede ser hacer un descubrimiento de red a un sitio web, de hecho, muchas veces se suele tomar como el primer paso para obtener un primer mapa de organización, para después proceder a un análisis de metadatos y un estudio más intensivo de las IP's descubiertas seleccionadas.



Más

Para finalizar este apartado, comentar que aunque sólo se nos den a elegir cuatro tácticas para hacer *Network Discovery*, *FOCA* utiliza muchos otros métodos y trucos por detrás. Cabe mencionar alguno de ellos como puede ser el *Google Slash Trick*, que nos permite que Google nos muestre URLs con puertos extraños, el *PTR Scanning*, donde *FOCA* busca los registros ptr, usados para resolver consultas DNS inversas y por último, destacar que en la carpeta donde al crear el proyecto hemos decidido guardar los archivos, tenemos una carpeta llamada *Certificates*, con todos los certificados digitales de las conexiones HTTPS. *FOCA* los usa para obtener nuevos dominios y extraer datos. Esta carpeta es muy valiosa ya que podremos acceder a las CRL (*Certificate Revocation List*) y, al fin y al cabo, a toda la información disponible de los certificados (número de serie, Autoridad Certificadora, periodo de validez…).



4. Vulnerabilidades

FOCA incorpora una gran cantidad de funcionalidades para la búsqueda automática de vulnerabilidades en los servidores del dominio auditado. A continuación listaremos algunas de estas vulnerabilidades analizadas por *FOCA*, haremos una breve explicación de ellas y las contrastaremos con ejemplos.

Juicy files

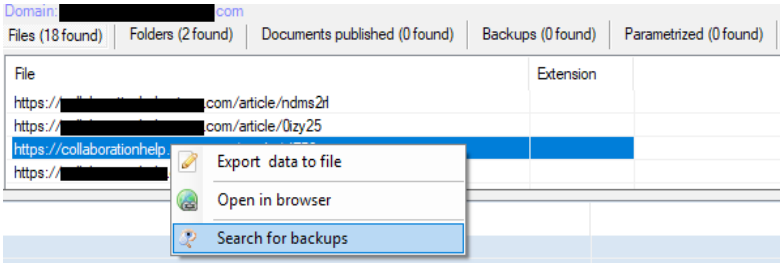
Son archivos 'jugosos' todos aquellos archivos de los que se puede extraer mucha información. *FOCA*, hará un descubrimiento de ellos de muchas maneras:

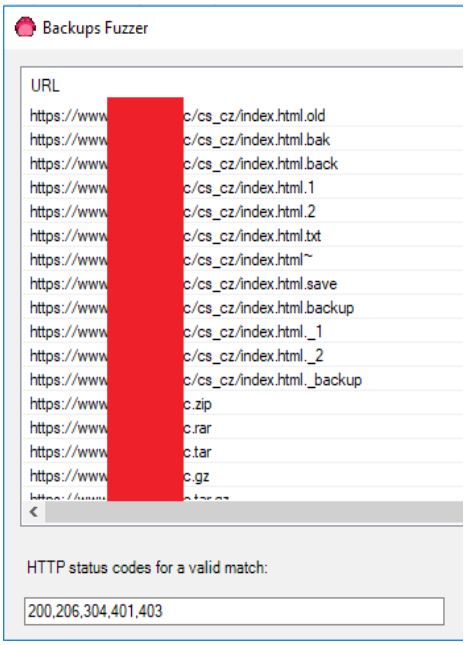
- Analizando extensiones sospechosas (.bak, .old).
- Buscando puertos inusuales (con el Google Slash Trick mencionado anteriormente).
- Utilizando los ficheros .listing (ficheros creados por wget al hacer conexiones ftp, que contienen en texto plano, el listado del directorio enviado por el servidor ftp).
- Examinando los ficheros .DS_Store (encargados de almacenar los metadatos que indican como debe ser abierto el directorio en el que está contenido).
- Haciendo Google/Bing/DuckDuckGo Crawling.
- Estudiando los ficheros robots.txt (ficheros de texto donde se suele indicar a los rastreadores y arañas de los buscadores que parte o partes no deben entrar a rastrear ni indexar).
- Sacando partido de los servidores Apache con:
  (1) El modulo mod_negotiation (que básicamente hace un ls en el servidor de un fichero indicado pero sin su extensión, sacando así ficheros interesantes como pueden ser copias de seguridad, versiones descartadas, etc.).
  (2) El módulo mod_user_dir (que permite generar una carpeta en el servicio web para cada usuario, colgando de la URL que se indica un carácter tilde o virgulilla seguido del nombre de usuario)
  (3) La posible falla de que al solicitar un directorio directamente, este no cuente con un fichero por defecto a mostrar cuando esto pase, y que liste todo el contenido del mismo.

- Llevando a cabo una búsqueda de los servidores Proxy del dominio tanto por análisis de puertos (3128, puerto que habitualmente usa Squid Porxy) como haciendo una conexión al servidor de Google a través de un servicio Proxy descubierto en la máquina objetivo.

Backups

Consiste en encontrarse que la copia de seguridad de un directorio ha sido directamente creada en el servidor de ficheros del servidor web. Muchas veces,cuando tenemos un directorio de la forma http://www.server.com/carpeta1/carpeta2, se produce una copia de seguridad de carpeta 2 que se hace directamente desde carpeta1, por lo que encontramos un archivo .zip o .tgz, .rar etc, directamente publicado en el servidor con la misma.





Para localizarlas, bastaría con ir al nodo del servidor web, acceder a la información de URLs localizadas y ahí pulsar sobre '*Search for Backups*', seleccionando una o varias URL.

Fugas de información con Subversion

FOCA intentará buscar el fichero *.svn/entries*, un archivo donde se encuentra la información de las últimas actualizaciones que se han realizado en un proyecto que usa SVN como gestor de código.

Tenemos también el fichero *wc.db*, que es la base de datos de Subversion, es decir, un fichero con información de todos los ficheros subidos al servidor.

Por último, tenemos la carpeta *Pristine*, donde se guarda una copia de todos los archivos originales subidos al servidor, se guardan de la forma pristine/SHA1(nombre fichero descubierto).svn-base, por lo que al conocer el nombre de algún archivo del servidor, podemos pedir la copia que se encuentra en Pristine.

Con lo que respecta a las vulnerabilidades SVN, *FOCA* cuenta con un plugin específico, y existen un montón de herramientas que integradas con *FOCA* nos pueden dar muchísima información valiosa, como por ejemplo **Svnpristine**.

DNS Cache Snooping

Los servidores DNS pueden tener una Caché, que utilizan para resolver nombres de dominio ya resueltos previamente. Esto, puede dar información muy jugosa, ya que si configuramos nuestras consultas DNS a modo solo caché, y le preguntamos al servidor, podemos ver si la página por la que le hemos preguntado, ya ha sido buscada previamente por alguna máquina de esa empresa.

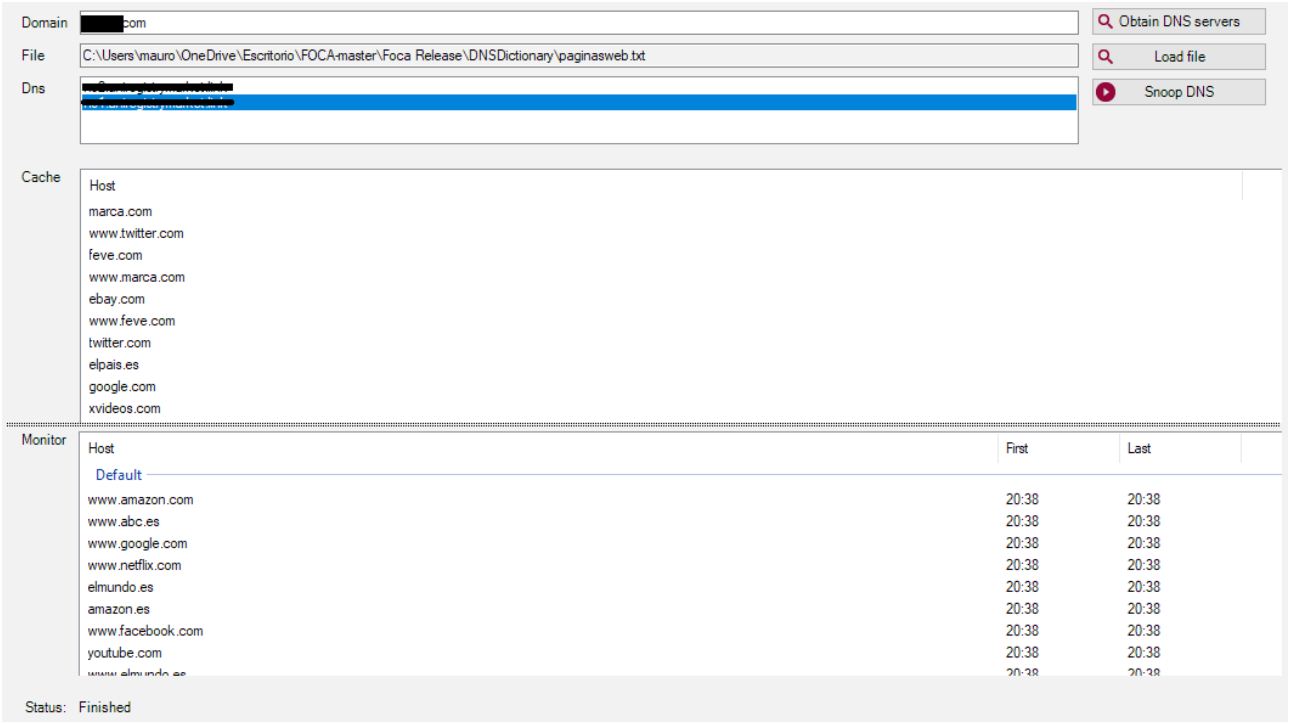
Aunque pueda parecer una vulnerabilidad débil, hay múltiples escenarios donde esto es muy útil, como pueden ser:

- El descubrimiento de software usado dentro de la organización, comprobando que páginas de actualizaciones se visitan (sistemas operativos, paquetes ofimáticos, **antivirus**...).

- Podemos sacar perfiles ideológicos de los trabajadores de la empresa, ver visitas a sitios web comprometidos, ver cuales son las páginas web más visitadas para después intentar un ataque falsificando actualizaciones, emails, logins..etc de esas páginas.

Es una vulnerabilidad muy potente, y a la cual *FOCA* dedica un plugin. Solo tendremos que meter el dominio al que queremos estudiar en '*Domain*' y cargar un archivo .txt con páginas web con las que probar para ver si han sido o no solicitadas. Cuando la respuesta sea afirmativa, aparecerán en la página Cache.

Probando un poco, vemos como para este dominio (oculto por razones obvias), han sido resueltas consultas a páginas de períodicos deportivos, redes sociales e incluso a una página pornográfica.



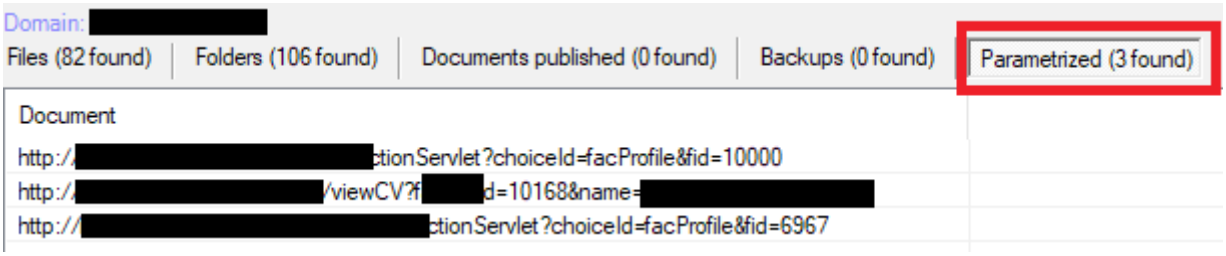
Métodos HTTP inseguros

A veces, algunas aplicaciones webs tienen habilitados métodos para la manipulación de ficheros como pueden ser *DELETE*, *PUT*, *COPY* etcétera.

FOCA hará un estudio de todos los verbos potencialmente peligrosos permitidos en todos los directorios (mediante peticiones *OPTIONS*) y nos alertará de ellos.
Que uno de estos métodos estén permitidos no quiere decir que podamos borrar y actualizar a la ligera ficheros de ese servidor, es más, aunque estén habilitados su uso debería estar restringido, pero nunca está de más comprobarlo debido a la infinidad de servidores que presentan esta vulnerabilidad.
Para aprovecharnos de ella, podemos destacar la subida de WebShells con métodos *PUT*, que harían posible que un atacante comenzara a escribir en el código fuente, el borrado de archivos con *DELETE*, o el *HIJACKING* de cookies usando *TRACE* (Desde *FOCA* podríamos realizar los dos primeros ataques, el *TRACE* podríamos sacarle partido con herramientas como *Burp*, por ejemplo).

Data Leaks

FOCA, para descubrirlas, hará principalmente dos cosas, una, enviar peticiones erróneas (de muy diversos tipos, aprovechándose de la inyección de parámetros en las URL) para obtener respuestas y analizarlas en busca de información valiosa, y otra, aprovecharse del mod_security, analizando el código fuente de una página buscando las expresiones regulares del fichero de reglas anti fuga de información del módulo Mod_Security, que precisamente se encarga de detener el envío de páginas respuesta que contienen las expresiones anteriores.



IIS URL Short Name

Esta es otra vulnerabilidad a la que *FOCA* dedica un plugin. Consiste básicamente que para todos los servidores *Internet Information Services* (*IIS*) descubiertos por *FOCA* se comprueba la característica *IIS Short Name*, que permite realizar un descubrimiento de ficheros por medio del sistema de nombres acortados que aún incorpora el sistema de ficheros de Windows.

La herencia de los 8:3 caracteres en el nombre de los ficheros (8 de nombre + 3 de extensión) hace que hoy en día todavía se pueda acceder a un archivo mediante su nombre acortado, aun así, esto en *IIS* no es posible ya que encuentre el archivo o no, dará un error, pero lo curioso es que si intentamos llegar a un archivo mediante su nombre acortado en un *IIS*, obtendremos dependiendo de si existe o no, un 404 o un 400.

Por lo que, jugando con los errores y con el ingenio, podemos descubrir la existencia de ficheros así como sus primeros 6 caracteres de nombre. Evidentemente, esto no siempre es posible, tenemos que contar con un servidor que los mensajes de Error 400 y 404 sean diferentes y en las que no se filtre el carácter *, el cual usaremos como carácter comodín.

Un ejemplo para descubrir si existe un fichero o no, usando el símbolo de acortamiento de nombre ~1, * como carácter comodín y el 404 como true y el 400 como false, vemos que con una prueba del siguiente estilo podemos ver si un fichero existe (Valid) o no (Invalid).

IIS Version	URL	Server Message
IIS 6	*/Valid*~1*/*.aspx	HTTP 404 – File not found
	/Invalid~1*/.aspx*	HTTP 400 – Bad Request

Tenemos un plugin en *FOCA* que se encarga de analizar y estudiar al completo esta vulnerabilidad, y que la hace más sencilla e intuitiva.

Conclusiones y ataque ejemplo

Una vez hemos visto toda la parte de análisis de metadatos, descubrimiento de red y detección y análisis de vulnerabilidades, vemos que tras aplicar todas estas opciones a un dominio, tenemos información muy valiosa sobre él. Ahora, es tiempo para que el pentester, una vez la tiene en su poder, decida que hacer con ella. Hay multitud de opciones y ataques que hacer. Por ejemplo, una vez que tenemos el nombre de un usuario (obtenido en análisis de metadatos), que tenga acceso a un buen número de carpetas compartidas en la red de la institución (metadatos + descubrimiento de red) y que conozcamos su *antimalware* (mediante *DNS Cache Snooping*, una vulnerabilidad y un plugin), será muy fácil hacer un ataque a la organización, simplemente entregándole un pendrive con malware específico a la victima y esperando que lo conecte a su equipo, o aún más facil, troyanizando una de sus páginas más visitadas o falsificando una actualización de software instalado en su equipo (como veremos más adelante).

5. Potenciación de FOCA

Por último, veremos que mediante el uso de los plugins de *FOCA*, o de la integración de esta con otras herramientas, podemos hacer auténticas virguerías. En este apartado, más que entrar en detalle o explicar detenidamente que hacer, vamos a mencionar unas cuantas posibilidades, definirlas de una forma rápida y sencilla y dejar en poder de la imaginación y curiosidad del lector los detalles de cada posible ataque.

Plugins

A parte de los plugins de *DNS Cache Snooping* y *IIS Shortname* explicados más en detalle en apartados anteriores, tenemos más en el repositorio oficial de *FOCA Open Source*:

SVN Downloader

Sacará máximo partido a las vulnerabilidades SVN mencionadas anteriormente (svn.entries, wc.db, Pristine) y a otras muchas, como análisis de logs, deteccion de shells internos..etcétera con el fin de averiguar lo máximo posible sobre la estructura interna de un servidor.

SQLi

Permite automatizar la extracción de datos de una aplicación web de la que se ha determinado que es vulnerable a un ataque SQL Injection.

Have I Been Pwned

Permite preguntarle a *havelbeenpwned.com* por los emails encontrados en la fase de extracción de metadatos con un sólo click. Esta página comprueba si los emails que le pasamos han sido vulnerados alguna vez.

Más

Puedes comprobar por ti mismo el resto de plugins en:
https://www.elevenpaths.com/focamarket/index.html

La nueva *FOCA* contiene la opción de creación de plugins, es decir, podemos crear desde 0 un plugin que satisfaga todas nuestras necesidades.

Integración de FOCA con otras herramientas y posibles ataques

FOCA + Herramientas Spidering como Burp Suite

Nos permite llegar a URL's no indexadas, que a priori *FOCA* no puede llegar, por lo que no puede analizar su contenido, mediante el uso de *Spidering*. Así conseguimos todo lo posible referente a un dominio.

FOCA Intruder: *FOCA* + Burp Suite + Intruder

Se pretende obtener un informe inicial de las vulnerabilidades más genéricas detectadas de manera eficiente por FOCA y Burp Suite combinados, para lanzar a continuación el módulo *Intruder* en función de los resultados obtenidos.

Malware vía actualizaciones: *FOCA* + Evilgrade

Es una opción muy interesante. Aprovechándonos del robo del trafico DNS (mediante las vulnerabilidades previamente comentadas), suplantamos los servidores que son comprobados por los clientes para descargarse actualizaciones. De manera que, la próxima vez que un usuario víctima se descargue una actualización, se estará descargando nuestro malware. Aunque requiere de una complejidad mayor que las anteriores, teniendo que manipular el trafico DNS (con DNS Caché Poisining, DNS Tempering o ARP Spoofing), combinando *FOCA* y *Evilgrade* este ataque se hace un poco más sencillo.

Ataques Spear Phising: *FOCA* + Metasploit

Es un ataque muy sencillo pero a la vez muy efectivo. Se basa en el envío de un correo electrónico con un fichero adjunto modificado o un enlace a un sitio web malicioso confiando en que la víctima lo abra. Una posibilidad sería obteniendo mediante *FOCA* los emails y antimalwares de los usuarios de la empresa que utilizaran Microsoft Office, para después diseñar un ataque aprovechando la vulnerabilidad Microsoft Office RTF Parsing Stack Overflow, creando con *Metasploit* un archivo RTF malicioso. Una vez tenemos este fichero creado y el email de las víctimas, bastaría con cambiarle el nombre por *'modificacion_fechas_vacaciones.rtf'*, por ejemplo, enviárselo y confiar en que alguno lo fuera a abrir. Una vez abierto, tendríamos una shell inversa con conectividad a nuestro equipo.

URL's desde el pasado: *FOCA* + Archive.org

Mediante esta herramienta podremos acceder a las diferentes versiones web que han ido pasando por una URL. Estas, que a priori no son accesibles, pueden contener los motivos o fallos por los cuales fueron actualizadas, y normalmente son mucho más vulnerables que las versiones más recientes y actualizadas. Bastaría con hacer un script, que a partir de una URL, nos saque todo su historial, y

después analizar los resultados con *FOCA*, haciendo así un análisis exhaustivo de metadatos, red y vulnerabilidades de versiones antiguas de páginas web, lo cual suele dar mucha información.

FOCA + Maltego

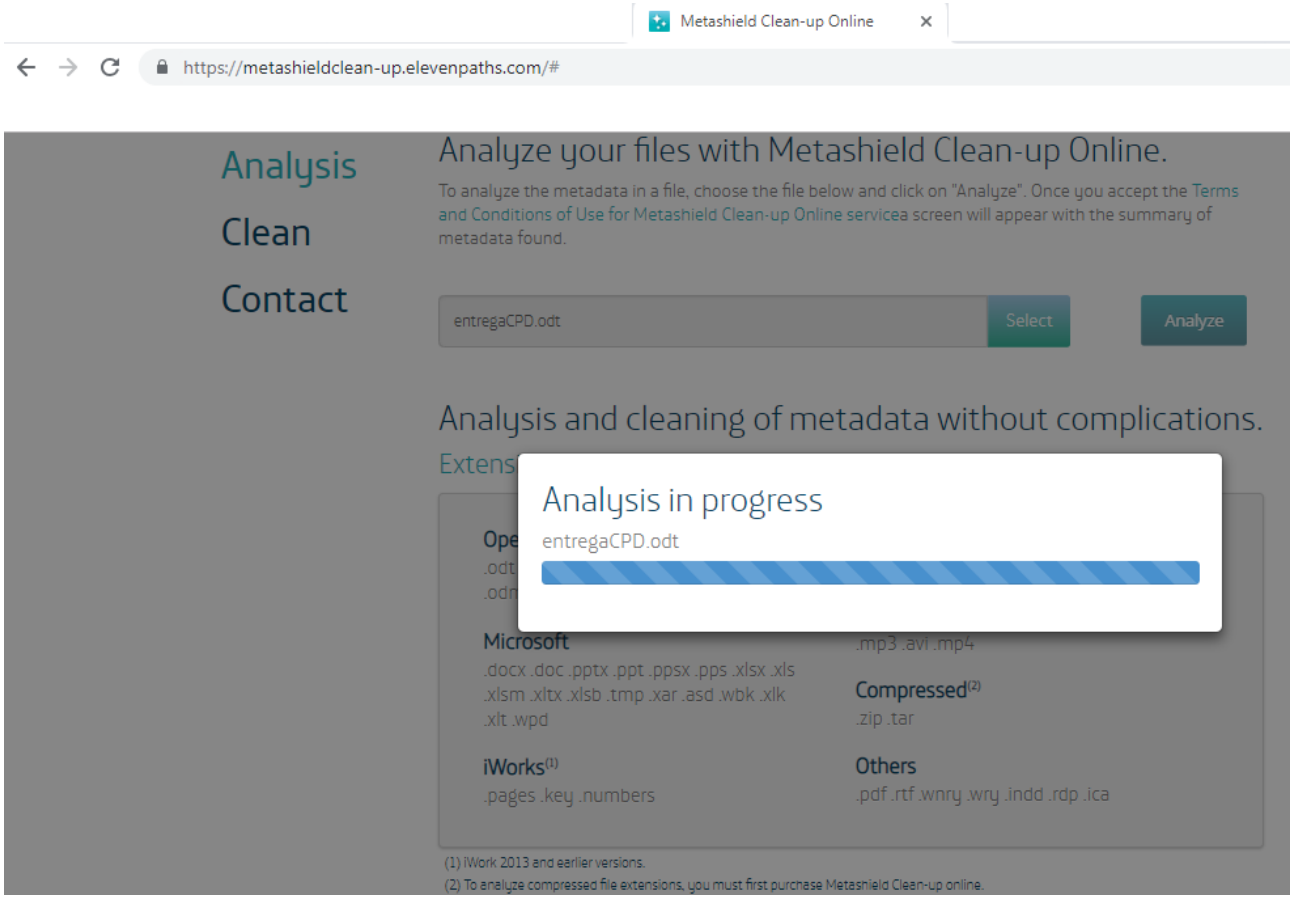
Otra opción sería, tras lanzar FOCA y obtener todos la información posible, exportar los datos a *Maltego* para tener una representación gráfica dinámica de todos los activos descubiertos.

Estos son unos de los pocos ejemplos que existen, hay millones de opciones para sacarle el máximo partido a *FOCA* y hacer cosas realmente interesantes. Por lo que, los límites a la hora de utilizar la *FOCA* son infinitos.

6. Bonus

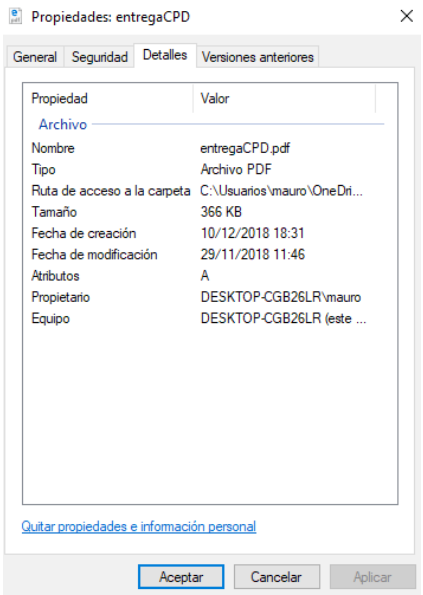
Análisis de metadatos de un documento

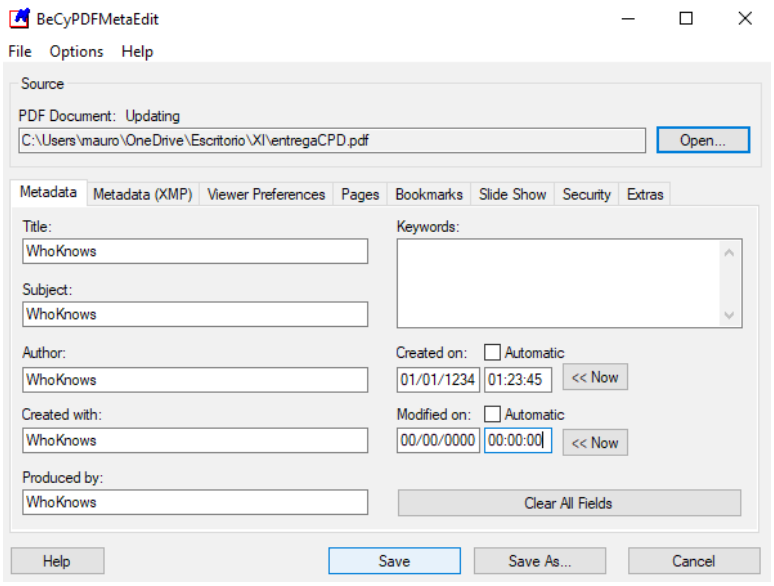
Si lo que quieres es analizar puntualmente los metadatos de un documento y no puedes, tienes o quieres tener instalado *FOCA Open Source*, existe una herramienta llamada *FOCA Online* o *MetaShield Clean-Up*, que permite de forma muy rápida e intuitiva, subir un documento y analizar todos sus metadatos.



Eliminación de metadatos

Sería curioso que después de este report, cualquiera de vosotros se descargara este pdf, lo analizara y viera que está repleto de información, no? Ya sabemos todos de la importancia de los metadatos, así que una parte importante es la de eliminarlos, y aunque *FOCA* no la haga, nosotros tenemos que encargarnos de ello. Para esto, podemos hacerlo de forma manual, eliminando los metadatos de nuestro documento desde el propio programa donde lo hayamos escrito (Writer, Word, AdobeAcrobat...), los datos EXIFs de las imágenes y vídeos del documento con herramientas como ExIfTool, y revisando y eliminando cada posible fuga de información que pueda ser relevante.
Otras opciones a probar son las de eliminar el archivo meta.xml de nuestro documento definitivo tras abrirlo ,por ejemplo, con WinRar, o más facil aún, haciendo click derecho sobre el documento a limpiar, Propiedades → Quitar Propiedades.
Y por supuesto, también existen multitud de herramientas que lo hacen de forma automática como son Edit PDF Metadata, **BeCyPDFMetaEdit**, exiv2, o MetaShield for Client.





Y ya para finalizar, recomendar al máximo el libro gracias al que este report es posible y a través del cuál he sacado la mayoría de la información: *Pentesting con FOCA*, de Chema Alonso. A parte de ser el 99% de la bibliografía del trabajo, es también una lectura imprescindible si quieres iniciarte o ampliar conocimientos en el mundo del pentesting y de los metadatos.