IFCT0109. SEGURIDAD INFORMÁTICA

MF0487_3 AUDITORÍA DE SEGURIDAD INFORMÁTICA

ANEXO

HACKING ÉTICO RECONOCIMIENTO

DOCENTE: BENITO MANUEL GONZÁLEZ RODRÍGUEZ

CONTENIDOS

- **INTRODUCCIÓN**
- OSINT/RECONOCIMIENTO PASIVO
- RECONOCIMIENTO ACTIVO
- OTRAS HERRAMIENTAS DE RECONOCIMIENTO
- ANÁLISIS DE METADATOS

INTRODUCCIÓN

LA FASE DE RECONOCIMIENTO *COMENZARÁ UNA VEZ QUE SE FINALICE LA DEFINICIÓN DEL ALCANCE, SE FIRMEN LOS DOCUMENTOS NECESARIOS Y SE ELABORE UN PLAN PARA LA PRUEBA DE PENETRACIÓN*.

DE ESTA FORMA, *AUNQUE LA PRUEBA A REALIZAR SEA DE CAJA NEGRA, SE TENDRÁ AL MENOS UN MÍNIMO DE INFORMACIÓN QUE SERVIRÁ COMO PUNTO DE PARTIDA* A PARTIR DEL CUAL OBTENER MÁS INFORMACIÓN RELACIONADA CON LA ORGANIZACIÓN OBJETIVO.

INTRODUCCIÓN

ESTE **PUNTO DE PARTIDA INICIAL** PUEDE SER SIMPLEMENTE **EL NOMBRE DE LA ORGANIZACIÓN**, QUE SERÁ GENERALMENTE EL PUNTO DE PARTIDA DE UN ATACANTE, **O BIEN** SE **PUEDE COMENZAR CON MÁS INFORMACIÓN**, COMO:

NOMBRE DEL DOMINIO; RANGO DE DIRECCIONES IP, O NOMBRES DE ALGUNAS PERSONAS PERTENECIENTES A LA ORGANIZACIÓN

ESTA FASE **ES MUY IMPORTANTE,** YA QUE **PERMITIRÁ CONOCER LA ORGANIZACIÓN** LO SUFICIENTE COMO PARA LLEVAR A CABO LAS FASES POSTERIORES.

INTRODUCCIÓN

ANTES DE COMENZAR EL ATAQUE ***ES NECESARIO HACER UN ESTUDIO PROFUNDO SOBRE LA ORGANIZACIÓN*** *PARA CONOCERLA LO MEJOR POSIBLE Y ESTUDIARLA EN BÚSQUEDA DE POSIBLES VULNERABILIDADES E INFORMACIÓN QUE PERMITA LLEVAR A CABO EL ATAQUE.*

COMO RESULTADO DEL RECONOCIMIENTO, UNO DE LOS PRODUCTOS QUE SE OBTENDRÁ ES **UNA RELACIÓN DE POSIBLES OBJETIVOS**, QUE DEBERÁ SER CUIDADOSAMENTE VERIFICADA ANTES DE PROSEGUIR CON LAS SIGUIENTES FASES PARA CONFIRMAR QUE DICHOS OBJETIVOS ENTRAN DENTRO DEL ALCANCE.

INTRODUCCIÓN

ES POSIBLE QUE ALGUNOS DE LOS OBJETIVOS ENCONTRADOS NO SEAN NI SIQUIERA CONOCIDOS POR PERSONAL DE LA ORGANIZACIÓN.

EN EL CASO DE UN TEST DE PENETRACIÓN ES CONVENIENTE VERIFICAR LOS OBJETIVOS CON EL REPRESENTANTE DE ÉSTA.

DURANTE EL RECONOCIMIENTO **SE EVITARÁ EN LA MEDIDA DE LO POSIBLE INTERACTUAR CON EL OBJETIVO**, O SE INTERACTUARÁ CON EL DE UNA MANERA *NORMAL*.

VEAMOS CÓMO OBTENER INFORMACIÓN DE LA ORGANIZACIÓN A PARTIR DE FUENTES ABIERTAS, **RECONOCIMIENTO PASIVO** U **OSINT (OPEN SOURCE INTELLIGENCE).**

CONTENIDOS

- INTRODUCCIÓN
- **OSINT/RECONOCIMIENTO PASIVO**
- RECONOCIMIENTO ACTIVO
- OTRAS HERRAMIENTAS DE RECONOCIMIENTO
- ANÁLISIS DE METADATOS

OSINT/RECONOCIMIENTO PASIVO

CON EL **RECONOCIMIENTO PASIVO**:

SE BUSCARÁ TODA LA INFORMACIÓN POSIBLE SOBRE LA RED Y LOS SISTEMAS DEL OBJETIVO SIN ESTABLECER CONEXIÓN DIRECTA CON EL MISMO

INTERNET PROPORCIONA UNA GRAN AYUDA A LA HORA DE BUSCAR INFORMACIÓN EN FUENTES ABIERTAS, POR LO QUE SERÁ LA BASE PARA REALIZAR ESTE RECONOCIMIENTO.

DURANTE EL RECONOCIMIENTO PASIVO **SE BUSCARÁ INFORMACIÓN RELATIVA A**:

NOMBRES DE DOMINIO; DIRECCIONES IP; ORGANIZACIONES CON LAS QUE SE RELACIONA; TECNOLOGÍAS EMPLEADAS; INFRAESTRUCTURA DE RED; DIRECCIONES DE CORREO; NOMBRES DE EMPLEADOS, SUS CARGOS E INFORMACIÓN PERSONAL DE LOS MISMOS.

OSINT/RECONOCIMIENTO PASIVO

ES **NECESARIO OBTENER CUANTA INFORMACIÓN SEA POSIBLE DE** CÓMO FUNCIONA **LA ORGANIZACIÓN**, *SUS UBICACIONES FÍSICAS* (SI EL TEST DE PENETRACIÓN INCLUYE UNA PARTE FÍSICA), *SU ESTRUCTURA JERÁRQUICA, EL ÁREA DE NEGOCIO DE LA ORGANIZACIÓN, LA TERMINOLOGÍA EMPLEADA POR PERSONAL DE LA ORGANIZACIÓN*.

LAS **HERRAMIENTAS** QUE SE UTILIZARÁN SERÁN **COMUNES Y AL ALCANCE DE CUALQUIERA:**

- *BUSCADORES WEB*
- *REDES SOCIALES*
- *FOROS*
- *OFERTAS DE EMPLEO*
- *BASES DE DATOS ONLINE*
- *BÚSQUEDA DE METADATOS EN ARCHIVOS*

OSINT/RECONOCIMIENTO PASIVO

EXISTE UNA TÉCNICA QUE, AUNQUE PAREZCA ANTIGUA, HOY EN DÍA PUEDE SEGUIR PROPORCIONANDO INFORMACIÓN INTERESANTE.

SE HA ADOPTADO EL TÉRMINO **DUMPSTER DIVING** PARA DEFINIR ALGO QUE SE HA REALIZADO TODA LA VIDA:

BUSCAR EN LA BASURA PARA OBTENER INFORMACIÓN ÚTIL SOBRE LA ORGANIZACIÓN O SOBRE EL PERSONAL DE LA MISMA O SUS CLIENTES.

OSINT/RECONOCIMIENTO PASIVO

REDES SOCIALES

LAS REDES SOCIALES **REQUIEREN UN REGISTRO PREVIO** PARA PODER VER INFORMACIÓN. TAMBIÉN **SERÁ NECESARIO INTERACTUAR CON LAS CUENTAS** SOBRE LAS QUE SE ESTÁ OBTENIENDO INFORMACIÓN. PUEDE MERECER LA PENA UTILIZARLAS PARA OBTENER INFORMACIÓN.

LA UTILIZACIÓN DE REDES SOCIALES **IMPLICA UN TRABAJO PREVIO DE CREACIÓN DE PERFILES** EN DIVERSAS REDES SOCIALES Y DARLES VIDA, DE MODO QUE PAREZCAN CUENTAS LEGÍTIMAS.

OSINT/RECONOCIMIENTO PASIVO

REDES SOCIALES

HAY QUE TENER EN CUENTA QUE **LA INTERACCIÓN CON USUARIOS DE LAS MISMAS SUPONE UNA ACCIÓN DE INGENIERÍA SOCIAL**, POR LO QUE SE DEBERÁ **LLEVAR A CABO CON TOTAL PRECAUCIÓN** Y PROTEGIENDO LA INFORMACIÓN OBTENIDA.

PARA UN ATACANTE REAL ESTO ES MÁS SENCILLO, DADO QUE NO TIENE MIRAMIENTOS A LA HORA DE CREAR CUENTAS FALSAS NI VULNERAR LA LEGISLACIÓN RELATIVA A LA PROTECCIÓN DE DATOS PERSONAL.

OSINT/RECONOCIMIENTO PASIVO

FOROS

EXISTEN NUMEROSOS **FOROS DONDE SE TRATAN TEMAS TÉCNICOS** DONDE *LOS ADMINISTRADORES DE LOS SISTEMAS SUELEN HACER PREGUNTAS ACERCA DE CONFIGURACIONES O PROBLEMAS QUE SE ENCUENTRAN EN SU TRABAJO DIARIO* Y ES POSIBLE QUE REVELEN EL NOMBRE DE SU ORGANIZACIÓN DE MANERA INADVERTIDA O INTENCIONADAMENTE, O QUE SE LES PUEDA RELACIONAR DE ALGUNA MANERA CON LA MISMA.

EN ESTE CASO, **A TRAVÉS DE LOS FOROS SE PUEDE OBTENER INFORMACIÓN ACERCA DE LAS TECNOLOGÍAS EMPLEADAS POR UNA ORGANIZACIÓN, E IDENTIFICAR ALGUNA VULNERABILIDAD O MALA CONFIGURACIÓN.**

OSINT/RECONOCIMIENTO PASIVO

OFERTAS DE EMPLEO

EN LAS **OFERTAS DE EMPLEO PARA PERSONAL INFORMÁTICO** LAS ORGANIZACIONES SUELEN RELACIONAR LAS TECNOLOGÍAS QUE DEBEN CONOCER LOS FUTUROS EMPLEADOS.

SON UNA BUENA FUENTE DE INFORMACIÓN PARA UN ATACANTE, QUE ÚNICAMENTE TIENE QUE LEERLAS PARA HACER UNA RELACIÓN INICIAL DE POSIBLES TECNOLOGÍAS Y HERRAMIENTAS, AUNQUE DEBERÁ CONFIRMARLA Y AMPLIARLA POSTERIORMENTE.

OSINT/RECONOCIMIENTO PASIVO

BÚSQUEDAS EN INTERNET

LAS PERSONAS Y LAS ORGANIZACIONES TIENDEN A REVELAR INFORMACIÓN DE MANERA INADVERTIDA O INTENCIONADA. POR EJEMPLO, EN REDES SOCIALES O A TRAVÉS DE CAMPAÑAS DE PUBLICIDAD EN INTERNET.

SE PUEDE OBTENER MUCHA INFORMACIÓN INTERESANTE Y ÚTIL A TRAVÉS DE DIFERENTES BUSCADORES REALIZANDO UNA SERIE DE BÚSQUEDAS CON UNA SINTAXIS ADECUADA.

LOS BUSCADORES PROPORCIONAN UNA SERIE DE **OPERADORES DE BÚSQUEDA** QUE SE PUEDEN UTILIZAR PARA AYUDAR A CENTRAR LAS BÚSQUEDAS EN DETALLES ESPECÍFICOS.

ESTO SE DEFINE COMO **GOOGLE HACKING** Y **BING HACKING.**

OSINT/RECONOCIMIENTO PASIVO

GOOGLE HACKING

SE TRATA DE UNA **TÉCNICA DE BÚSQUEDA** BASADA EN LA **COMBINACIÓN DE DIFERENTES OPERADORES DE BÚSQUEDA PARA OBTENER RESULTADOS SENSIBLES** QUE AFECTEN A UN OBJETIVO Y QUE PUEDAN SER UTILIZADOS POR UN ATACANTE.

LOS **OPERADORES DE GOOGLE** PERMITEN HACER *BÚSQUEDAS SOBRE SITIOS Y DOMINIOS ESPECÍFICOS*, ASÍ COMO *PÁGINAS QUE CONTENGAN CONTENIDO RELACIONADO*, TAMBIÉN PERMITEN *BUSCAR EN FUNCIÓN DE TEXTO* QUE SE PUEDA ENCONTRAR *EN EL TÍTULO DE LAS PÁGINAS, DE LAS URL O EN EL CONTENIDO DE LA PÁGINA*.

OSINT/RECONOCIMIENTO PASIVO

GOOGLE HACKING

SITE

ESTE OPERADOR PERMITE INDICAR EL NOMBRE DE UN SITIO O UN DOMINIO SOBRE EL QUE SE LIMITARÁN LAS BÚSQUEDAS. POR EJEMPLO:

site:sitioejemplo.es

RELATED

PARA BUSCAR PÁGINAS CON UN CONTENIDO SIMILAR AL SITIO SOBRE EL QUE SE BUSCA. PUEDE SERVIR PARA ENCONTRAR ALGUNA RELACIÓN ENTRE ORGANIZACIONES EN FUNCIÓN DEL CONTENIDO DE SUS SITIOS WEB O LOS HIPERVÍNCULOS EXISTENTES. POR EJEMPLO:

related:bancoejemplo.es

OSINT/RECONOCIMIENTO PASIVO

GOOGLE HACKING

LINK

BUSCA ÚNICAMENTE EN PÁGINAS QUE TIENEN UN ENLACE A UN SITIO WEB:

link:sitioejemplo.es

INTITLE

SE RESTRINGEN LAS BÚSQUEDAS AL TÍTULO DE LA PÁGINA. RESULTA MUY ÚTIL PARA *LOCALIZAR SITIOS WEB QUE MUESTREN EL ÍNDICE DE ARCHIVOS* Y CARPETAS UBICADOS EN UN DIRECTORIO, LO QUE PERMITIRÁ A UN ATACANTE ACCEDER A INFORMACIÓN SENSIBLE. POR EJEMPLO:

intitle:index of parent directory

OSINT/RECONOCIMIENTO PASIVO

GOOGLE HACKING

INURL

BUSCA DIRECCIONES URL QUE CONTENGAN UN TEXTO DETERMINADO. SE PUEDE UTILIZAR PARA BUSCAR SCRIPTS CORRESPONDIENTES A IMPLEMENTACIONES DE SITIOS WEB CON VULNERABILIDADES CONOCIDAS. POR EJEMPLO:

inurl:wp-content/plugins/my-calendar changelog

INTEXT

BUSCA EXCLUSIVAMENTE EN EL TEXTO DE LA PÁGINA. POR EJEMPLO:

intext:Windows

OSINT/RECONOCIMIENTO PASIVO

GOOGLE HACKING

SE PUEDEN **COMBINAR DIFERENTES OPERADORES** PARA ACOTAR MÁS LA BÚSQUEDA. LOS RESULTADOS DE LA BÚSQUEDA TAMBIÉN CAMBIARÁN SEGÚN SE UTILICEN O NO COMILLAS, POR LO QUE PUEDE RESULTAR INTERESANTE PROBAR DISTINTAS FORMAS DE BUSCAR. POR EJEMPLO:

site:sitioejemplo.es intext:windows

OSINT/RECONOCIMIENTO PASIVO

GOOGLE HACKING

UNO DE LOS **ELEMENTOS MÁS INTERESANTES A BUSCAR** DURANTE LA FASE DE RECONOCIMIENTO **SON ARCHIVOS**, **POR SU CONTENIDO**, Y **POR LOS METADATOS** QUE PUEDAN CONTENER.

FILETYPE

PERMITE BUSCAR ARCHIVOS POR SU EXTENSIÓN. EL OPERADOR **SITE:** ES UNO DE LOS OPERADORES QUE SE SUELEN COMBINAR CON ESTE, PUESTO QUE PERMITE BUSCAR ARCHIVOS CONCRETOS EN UN SITIO ESPECÍFICO. POR EJEMPLO:

Filetype:xlsx site:empresa.es

OSINT/RECONOCIMIENTO PASIVO

GOOGLE HACKING

EXISTEN MULTITUD DE OPERADORES QUE SE PUEDEN COMBINAR PRÁCTICAMENTE DE MANERA ILIMITADA PARA REALIZAR BÚSQUEDAS DE VULNERABILIDADES O SITIOS Y PÁGINAS DE INTERÉS.

SE PUEDEN ENCONTRAR NUMEROSOS EJEMPLOS EN LA **GOOGLE HACKING DATABASE:**

https://www.exploit-db.com/google-hacking-database

ES UN SITIO WEB MANTENIDO POR **OFFENSIVE SECURITY** DONDE *SE RECOPILAN TÉRMINOS DE BÚSQUEDA ESPECÍFICOS*, DENOMINADOS **DORKS**, CATEGORIZADOS EN FUNCIÓN DE LOS OBJETIVOS PERSEGUIDOS CON LOS MISMOS.

OSINT/RECONOCIMIENTO PASIVO

OTROS MOTORES DE BÚSQUEDA

ADEMÁS DE LAS BÚSQUEDAS DE QUE SE PUEDEN HACER CON BUSCADORES COMO GOOGLE O BING, **EXISTEN MOTORES DE BÚSQUEDA QUE PERMITEN ENCONTRAR DISPOSITIVOS CONECTADOS**, LO QUE PUEDE RESULTAR DE INTERÉS A LA HORA DE LOCALIZAR DIRECCIONES IP CORRESPONDIENTES A ROUTERS O IDENTIFICAR E INCLUSO CONTROLAR CÁMARAS DE VIGILANCIA, ENTRE MUCHAS OTRAS POSIBILIDADES.

LOS DOS MÁS CONOCIDOS SON **SHODAN** Y **ZOOMEYE**, PERO EXISTEN OTROS QUE PUEDEN RESULTAR INTERESANTES, COMO **GREYNOISE, CENSYS, ONYPHE O BYNARYEDGE**.

OSINT/RECONOCIMIENTO PASIVO

OTROS MOTORES DE BÚSQUEDA

SHODAN

SE CENTRA **EN ENCONTRAR TODO TIPO DE DISPOSITIVOS CONECTADOS A INTERNET**, QUE PUEDEN SER *ROUTERS*, *SERVIDORES WEB*, *CÁMARAS DE VIGILANCIA*, *OBJETOS DE LA "INTERNET DE LAS COSAS" (IOT)* O CUALQUIER OTRO ELEMENTO QUE SE PUEDA CONECTAR.

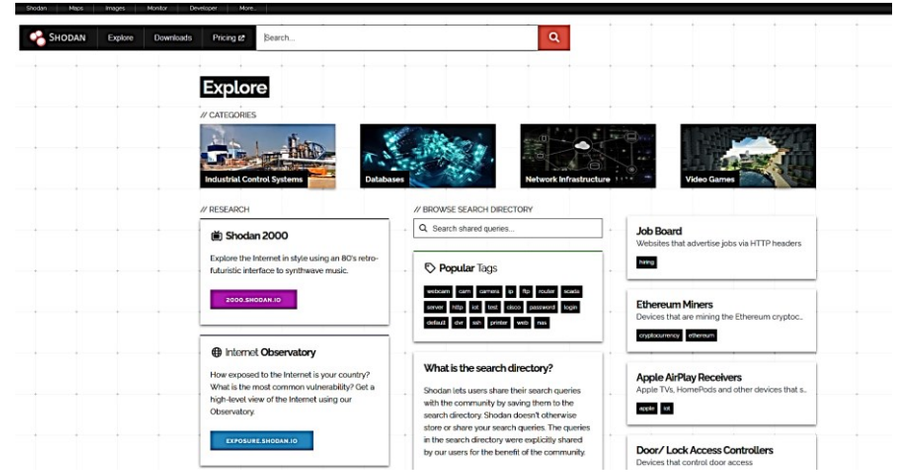
SE PUEDE UTILIZAR DE FORMA GRATUITA, SI BIEN PARA UTILIZAR TODO SU POTENCIAL ES NECESARIO REGISTRARSE Y SUSCRIBIRSE PAGANDO.

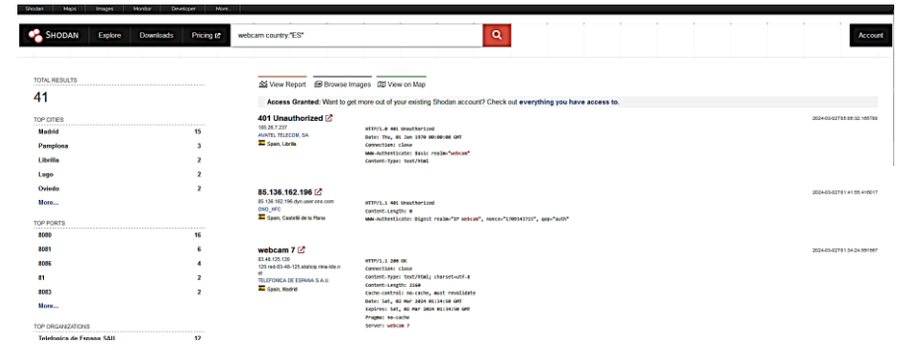
OSINT/RECONOCIMIENTO PASIVO

OTROS MOTORES DE BÚSQUEDA

SHODAN

SI SE SELECCIONA ALGUNA DE LAS CATEGORÍAS SE MOSTRARÁN LAS DIRECCIONES IP Y MÁS INFORMACIÓN DE LOS ELEMENTOS CORRESPONDIENTES, QUE A SU VEZ SE PODRÁN SELECCIONAR PARA OBTENER MÁS INFORMACIÓN, COMO SU UBICACIÓN, TECNOLOGÍAS UTILIZADAS, VULNERABILIDADES CONOCIDAS O PUERTOS ABIERTOS, ENTRE OTRAS COSAS.





OSINT/RECONOCIMIENTO PASIVO

OTROS MOTORES DE BÚSQUEDA

ZOOMEYE

ESTE MOTOR DE BÚSQUEDA, DE ORIGEN CHINO, OFRECE UNA FUNCIONALIDAD SIMILAR A LA DE SHODAN Y PERMITE REALIZAR UNA SERIE DE BÚSQUEDAS GRATUITAS Y OFRECE MÁS POSIBILIDADES EN CASO DE ESTAR REGISTRADOS Y SUSCRITOS.

AL IGUAL QUE EN SHODAN, SE PUEDEN REALIZAR BÚSQUEDAS PROPIAS O UTILIZAR LAS OPCIONES QUE PROPORCIONA LA HERRAMIENTA A TRAVÉS DE BÚSQUEDAS PREDEFINIDAS.

OSINT/RECONOCIMIENTO PASIVO

BASES DE DATOS WHOIS

CUALQUIER DISPOSITIVO CONECTADO A INTERNET PUEDE SER LOCALIZADO A TRAVÉS DE SU DIRECCIÓN IP PÚBLICA. A UNA PERSONA NO LE SUELE RESULTAR SENCILLO RECORDAR ESTAS DIRECCIONES Y, ADEMÁS, ESTAS DIRECCIONES PUEDEN CAMBIAR.

PARA RESOLVERLO SE USAN LOS **NOMBRES DE DOMINIO** UTILIZANDO **NOMBRES COMPRENSIBLES Y FÁCILES DE RECORDAR.**

UN NOMBRE DE DOMINIO PERMITE **ASOCIAR DIRECCIONES IP CON RECURSOS EN INTERNET**, LO QUE PERMITE QUE LAS ORGANIZACIONES OFREZCAN SERVICIOS O INFORMACIÓN Y QUE SU ACCESO SEA MÁS SENCILLO POR PARTE DEL PÚBLICO GENERAL.

OSINT/RECONOCIMIENTO PASIVO

BASES DE DATOS WHOIS

EL **NOMBRE DE DOMINIO** DE UNA ORGANIZACIÓN TIENE UNA **ESTRUCTURA FORMADA POR VARIAS PARTES.** GENERALMENTE SE COMPONDRÁ DE:

- **NOMBRE DEL DOMINIO RAÍZ.**
- **PUNTO DEL DOMINIO DE NIVEL SUPERIOR (TLD),** (LOS HABITUALES **.COM, .ES, .ORG**).
- **VARIOS SUBDOMINIOS** QUE SE PUEDEN EMPLEAR PARA IDENTIFICAR DIFERENTES SERVICIOS. SE ANTEPONEN AL NOMBRE DEL DOMINIO, TAMBIÉN SEPARADOS POR UN PUNTO.

ESTRUCTURA DE UN NOMBRE DE DOMINIO

OSINT/RECONOCIMIENTO PASIVO

BASES DE DATOS WHOIS

CUANDO UNA ORGANIZACIÓN **REGISTRA UN NOMBRE DE DOMINIO** TIENE QUE **PROPORCIONAR CIERTA INFORMACIÓN DE LA EMPRESA.**

ESTA INFORMACIÓN **SE REGISTRA A TRAVÉS DE ENTIDADES** DENOMINADAS **REGISTRADORES**, QUE LA ALMACENAN EN BASES DE DATOS.

ESTA INFORMACIÓN PÚBLICA ERA ACCESIBLE A TRAVÉS DEL PROTOCOLO **WHOIS**, Y SE PODÍA CONSULTAR CON NAVEGADORES O LÍNEA DE COMANDOS, SALVO QUE EL PROPIETARIO DEL DOMINIO PAGARA UNA CUOTA PARA OCULTARLO.

OSINT/RECONOCIMIENTO PASIVO

BASES DE DATOS WHOIS

ESTO **HA CAMBIADO** CON LA ENTRADA EN VIGOR DEL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS (**RGPD**) EN **2018.**

LA **ICANN** (ORGANISMO QUE COORDINA LOS NOMBRES DE DOMINIO A NIVEL MUNDIAL Y ES LA RESPONSABLE DE **WHOIS**) SE VIO OBLIGADA A REALIZAR CIERTAS MODIFICACIONES.

ACTUALMENTE, CUANDO SE REGISTRA UN DOMINIO, SE PIDE CONSENTIMIENTO PARA MOSTRAR LOS DATOS PERSONALES EN LAS BÚSQUEDAS, Y EN CASO DE NO DARSE EL CONSENTIMIENTO, ESTOS DATOS NO SE MOSTRARÁN EN BÚSQUEDAS **WHOIS.**

OSINT/RECONOCIMIENTO PASIVO

BASES DE DATOS WHOIS

CONSULTAS WHOIS A TRAVÉS DEL NAVEGADOR

PARA REALIZAR LAS CONSULTAS SE PUEDE ACUDIR:

- HTTPS://LOOKUP.ICANN.ORG/. SE PUEDE UTILIZAR PARA BÚSQUEDAS SOBRE DISTINTOS DOMINIOS.
- HTTPS://WWW.DOMINIOS.ES/DOMINIOS/. PARA DOMINIOS .ES.
- HTTPS://WHOIS.DOMAINTOOLS.COM/. PERMITE BUSCAR DIFERENTES DOMINIOS, INCLUIDOS AQUELLOS EN QUE LOS TLD SON .ES.

EN FUNCIÓN DE LA PÁGINA QUE SE UTILICE SE OBTENDRÁN UNOS RESULTADOS MÁS O MENOS DETALLADOS, POR LO QUE RESULTARÁ INTERESANTE UTILIZAR LAS DIFERENTES ALTERNATIVAS.

OSINT/RECONOCIMIENTO PASIVO

BASES DE DATOS WHOIS

CONSULTAS WHOIS A TRAVÉS DEL NAVEGADOR

EXISTEN APLICACIONES DE LÍNEAS DE COMANDOS QUE PERMITEN REALIZAR CONSULTAS **WHOIS**.

ESTA HERRAMIENTA SE ENCUENTRA POR DEFECTO EN LAS DISTRIBUCIONES LINUX Y LA MAYOR PARTE DE SISTEMAS UNIX-LIKE,

PERO PARA WINDOWS ES NECESARIO DESCARGAR ALGUNA HERRAMIENTA.

```
Th1@hacking:~$ whois [redacted].es
This TLD has no whois server, but you can access the whois database at
https://www.nic.es/
Th1@hacking:~$
```

OSINT/RECONOCIMIENTO PASIVO

BASES DE DATOS WHOIS

CONSULTAS WHOIS A TRAVÉS DEL NAVEGADOR

EN LINUX SE PUEDE UTILIZAR EL PARÁMETRO **-I**

EN PRIMER LUGAR CONSULTARÁ A **WHOIS.IANA.ORG.**

A CONTINUACIÓN, CONSULTARÁ AL SERVIDOR WHOIS QUE SE INDIQUE COMO AUTORITATIVO PARA ESA PETICIÓN.

```
Th1@hacking:~$ whois -I [redacted].es
% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object

refer:        whois.nic.es

domain:       ES

organisation: Red.es
address:      Edificio Bronce
address:      Plaza Manuel Gomez Moreno
address:      Madrid  28020
address:      Spain

contact:      administrative
name:         Alberto Martinez Lacambra
organisation: Red.es
address:      Edificio Bronce
address:      Plaza Manuel Gomez Moreno
address:      Madrid  28020
address:      Spain
phone:        +34 91 212 76 24
fax-no:       +34 91 555 76 64
e-mail:       esnic-admin@red.es
```

CONTENIDOS

- INTRODUCCIÓN
- OSINT/RECONOCIMIENTO PASIVO
- **RECONOCIMIENTO ACTIVO**
- OTRAS HERRAMIENTAS DE RECONOCIMIENTO
- ANÁLISIS DE METADATOS

RECONOCIMIENTO ACTIVO

DNS

CON LAS TÉCNICAS ANTERIORES NO SE INTERACTÚA CON EL OBJETIVO, PERO EXISTEN OTRAS **TÉCNICAS Y HERRAMIENTAS DE RECONOCIMIENTO ACTIVO**, QUE YA **IMPLICAN UN CONTACTO MÁS DIRECTO CON EL OBJETIVO**.

DNS

ES UN PROTOCOLO QUE SE UTILIZA PARA **ASOCIAR NOMBRES DE DOMINIO CON LAS DIRECCIONES IP** CORRESPONDIENTES.

ESTA INFORMACIÓN SE ALMACENA EN UNA **BASE DE DATOS JERÁRQUICA DISTRIBUIDA.** EN CADA NIVEL SE ENCUENTRAN DIFERENTES SERVIDORES, QUE RESUELVEN LOS NOMBRES Y RESPONDEN A LAS PETICIONES, DENTRO DE SU ESPACIO DE NOMBRES.

RECONOCIMIENTO ACTIVO

DNS

EN EL CASO DE ENCONTRAR ALGÚN **SERVIDOR DNS** DURANTE LAS BÚSQUEDAS **WHOIS**, SE PUEDEN HACER CONSULTAS A LOS MISMOS Y ENCONTRAR EQUIPOS RELACIONADOS CON LA ORGANIZACIÓN.

ES POSIBLE QUE ALGUNO DE LOS EQUIPOS QUE SE IDENTIFIQUEN EN ESTE PUNTO NO PERTENEZCA A LA ORGANIZACIÓN OBJETIVO O QUEDE FUERA DEL ALCANCE, POR LO QUE RESULTARÁ NECESARIO VERIFICARLO CONVENIENTEMENTE.

PARA QUE UN **SERVIDOR DNS** PROPORCIONE INFORMACIÓN ACERCA DE UN DOMINIO HAY **HACER LAS CONSULTAS ADECUADAS** PARA LOS **DISTINTOS TIPOS DE REGISTROS**.

RECONOCIMIENTO ACTIVO

DNS

NS (*NAMESERVER*)

CONTIENE EL NOMBRE DE LOS SERVIDORES DE NOMBRES ASOCIADOS A UN DOMINIO CONCRETO.

A (*ADDRESS/HOST*)

RELACIONA LA DIRECCIÓN IPV4 DE UN DOMINIO. EL EQUIVALENTE PARA IPV6 ES EL AAAA (QUAD-A).

MX (*MAIL EXCHANGE*)

IDENTIFICA LOS SERVIDORES DE CORREO DE UN DOMINIO.

TXT (*TEXT*)

PERMITE INCLUIR CUALQUIER CADENA DE TEXTO, QUE SE PUEDE UTILIZAR PARA DISTINTOS PROPÓSITOS, COMO ALMACENAR INFORMACIÓN DEL PROPIETARIO.

RECONOCIMIENTO ACTIVO

DNS

CNAME (*CANONICAL NAME*)

PERMITE INDICAR NOMBRES ALTERNATIVOS (ALIAS) PARA UN HOST.

PTR (POINTER/REVERSE)

PARA BÚSQUEDAS INVERSAS, LO QUE PERMITE ENCONTRAR LOS REGISTROS CORRESPONDIENTES A UNA DIRECCIÓN IP.

SOA (*START OF AUTHORITY)*

INDICA QUE UN SERVIDOR ES AUTORITATIVO PARA UNA ZONA. ESTOS REGISTROS CONTIENEN INFORMACIÓN ADMINISTRATIVA SOBRE LA ZONA Y TIENEN UNA GRAN IMPORTANCIA PARA LAS TRANSFERENCIAS DE ZONA, SOBRE LAS QUE SE HABLARÁ POSTERIORMENTE.

RECONOCIMIENTO ACTIVO

DNS

SPF (*SENDER POLICY FRAMEWORK*)

ES UN REGISTRO TXT QUE INDICA LOS NOMBRES DE SERVIDORES O DIRECCIONES IP AUTORIZADAS PARA ENVIAR CORREOS ELECTRÓNICOS EN NOMBRE DEL DOMINIO.

RP (*RESPONSIBLE PERSON*)

ESTE ES UN REGISTRO MERAMENTE INFORMATIVO QUE NO SE USA HABITUALMENTE, PERO EN CASO DE USARSE CONTENDRÁ INFORMACIÓN DE LA PERSONA RESPONSABLE DE UN DOMINIO.

SRV (*SERVICE LOCATION*)

AUNQUE TAMPOCO SE USA HABITUALMENTE, SIRVE PARA INDICAR QUÉ SERVICIOS ESTÁN DISPONIBLES EN EL DOMINIO, EL NOMBRE DEL EQUIPO Y EL PUERTO EN EL QUE SE ENCUENTRA CADA SERVICIO.

RECONOCIMIENTO ACTIVO

DNS

HERRAMIENTAS PARA OBTENER INFORMACIÓN DE UN SERVIDOR DNS

PARA OBTENER INFORMACIÓN DE UN SERVIDOR DNS SE PUEDEN UTILIZAR DIFERENTES HERRAMIENTAS E INSTRUCCIONES DE LÍNEA DE COMANDOS.

ALGUNAS DE ELLAS ESTÁN DISPONIBLES POR DEFECTO EN PRÁCTICAMENTE CUALQUIER SISTEMA OPERATIVO O, AL MENOS, EN CASI TODAS LAS DISTRIBUCIONES LINUX, MIENTRAS QUE OTRAS ES PRECISO DESCARGARLAS EN EL EQUIPO EN EL QUE SE VAN A EJECUTAR:

- **NSLOOKUP**
- **HOST**
- **DIG**

RECONOCIMIENTO ACTIVO

DNS

HERRAMIENTAS PARA OBTENER INFORMACIÓN DE UN SERVIDOR DNS

NSLOOKUP

ESTA INSTRUCCIÓN ESTÁ DISPONIBLE POR DEFECTO EN **WINDOWS** Y EN CASI CUALQUIER DISTRIBUCIÓN DE **LINUX** Y **UNIX-LIKE**.

LA EJECUCIÓN BÁSICA ES SENCILLA: BASTA CON EJECUTAR EL COMANDO E INDICAR EL DOMINIO O UN NOMBRE DE HOST COMO PARÁMETRO.

```
pru@pru-VirtualBox:~$ nslookup www.google.es
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   www.google.es
Address: 142.250.200.131
Name:   www.google.es
Address: 2a00:1450:4003:80d::2003
```

RECONOCIMIENTO ACTIVO

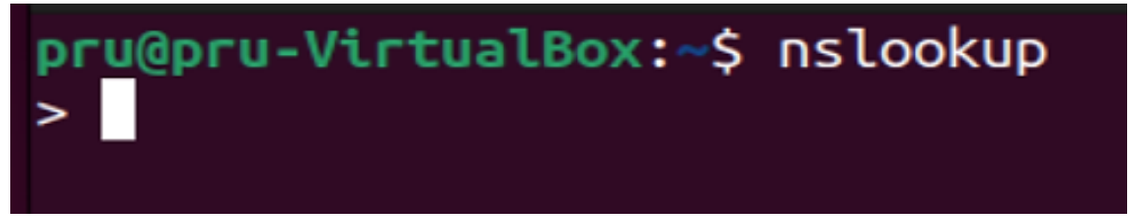
DNS

HERRAMIENTAS PARA OBTENER INFORMACIÓN DE UN SERVIDOR DNS

NSLOOKUP

PERMITE ESPECIFICAR DIFERENTES PARÁMETROS PARA EJECUTAR CONSULTAS MÁS COMPLEJAS.

UNA DE LAS CARACTERÍSTICAS QUE LA HACEN INTERESANTE ES QUE **PERMITE TRABAJAR DE MANERA INTERACTIVA.** PARA ELLO SE EJECUTARÁ EL COMANDO **NSLOOKUP SIN INDICAR NINGÚN PARÁMETRO NI EL DOMINIO**, DE ESTA FORMA SE ABRIRÁ UN PROMPT DESDE EL QUE SE PODRÁN REALIZAR CONSULTAS MÁS COMPLEJAS.



RECONOCIMIENTO ACTIVO

DNS

HERRAMIENTAS PARA OBTENER INFORMACIÓN DE UN SERVIDOR DNS

NSLOOKUP

NSLOOKUP PERMITE INDICAR QUÉ SERVIDOR DNS SE QUIERE UTILIZAR LA RESOLUCIÓN DE NOMBRES, LO QUE PERMITE UTILIZAR LOS SERVIDORES QUE SE HAYAN PODIDO OBTENER AL HACER LAS BÚSQUEDAS **WHOIS**. EN CASO DE QUE NO SE DISPONGA DE NINGÚN SERVIDOR DNS PERO SE CONOZCA EL DOMINIO DE LA ORGANIZACIÓN, SE PUEDE UTILIZAR NSLOOKUP PARA OBTENER INFORMACIÓN DE LOS SERVIDORES DNS.

```
pru@pru-VirtualBox:~$ nslookup
> milaulas.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   milaulas.com
Address: 167.114.128.84
```

RECONOCIMIENTO ACTIVO

DNS

HERRAMIENTAS PARA OBTENER INFORMACIÓN DE UN SERVIDOR DNS

NSLOOKUP

PARA INDICAR UN SERVIDOR DNS DIFERENTE SE UTILIZA LA INSTRUCCIÓN **SERVER**, SEGUIDA DE LA DIRECCIÓN IP O DEL NOMBRE DEL SERVIDOR.

```
pru@pru-VirtualBox:~$ nslookup
> server ns1.luadns.net
Default server: ns1.luadns.net
Address: 185.142.218.1#53
Default server: ns1.luadns.net
Address: 2001:67c:25a0::1#53
>
```

POR DEFECTO, **NSLOOKUP** BUSCARÁ LOS REGISTROS **A.**

RECONOCIMIENTO ACTIVO

DNS

HERRAMIENTAS PARA OBTENER INFORMACIÓN DE UN SERVIDOR DNS

NSLOOKUP

SI SE QUIERE OBTENER INFORMACIÓN DE OTROS REGISTROS, SE PUEDE INDICAR EL TIPO DE REGISTRO SOBRE EL QUE SE QUIERE PREGUNTAR CON LA INSTRUCCIÓN **SET TYPE=**, SEGUIDO DEL TIPO DE REGISTRO DESEADO (**SET TYPE=MX** O **ANY**).

UNA VEZ QUE YA SE HAYA CONFIGURADO **NSLOOKUP** PARA HACER LAS BÚSQUEDAS SOBRE EL SERVIDOR Y LOS REGISTROS DESEADOS, SE INDICARÁ EL DOMINIO DIRECTAMENTE EN EL PROMPT.

```
pru@pru-VirtualBox:~$ nslookup
> server ns1.luadns.net
Default server: ns1.luadns.net
Address: 185.142.218.1#53
Default server: ns1.luadns.net
Address: 2001:67c:25a0::1#53
> set type=any
```

RECONOCIMIENTO ACTIVO

DNS

HERRAMIENTAS PARA OBTENER INFORMACIÓN DE UN SERVIDOR DNS

NSLOOKUP

```
Th1@hacking:~$ nslookup
> server ns1.[redacted].es
Default server: ns1.[redacted].es
Address: 217.18.16[redacted]#53
> set type=any
> [redacted].es
Server:         ns1.[redacted].es
Address:        217.18.16[redacted]#53

[redacted].es   mail exchanger = 10 mail.[redacted].es.
[redacted].es   text = "v=spf1 +a +mx ip4:217.18.16[redacted]/20 -all"
Name:   [redacted].es
Address: 217.18.16[redacted]
ra-ma.es
        origin = ns2.[redacted].es
        mail addr = jesus[redacted].com
        serial = 2019111201
        refresh = 86400
        retry = 7200
        expire = 1209600
        minimum = 7200
[redacted].es   nameserver = ns2.[redacted].es.
[redacted].es   nameserver = ns1.[redacted].es.
>
```

RECONOCIMIENTO ACTIVO

DNS

HERRAMIENTAS PARA OBTENER INFORMACIÓN DE UN SERVIDOR DNS

NSLOOKUP

EN LA RESPUESTA SE IDENTIFICAN LOS SIGUIENTES ELEMENTOS:

1. **SERVER** Y **ADDRESS:** SE CORRESPONDE CON EL NOMBRE DEL SERVIDOR DNS QUE SE HA INDICADO, ASÍ COMO SU DIRECCIÓN IP.
2. **MAIL EXCHANGER**: INDICA EL REGISTRO MX.
3. **V=SPF1**: INDICA EL REGISTRO SPF. EN ESTE CASO SE INDICA QUE LOS SERVIDORES QUE PUEDEN ENVIAR MENSAJES CON EL DOMINIO SE CORRESPONDEN CON LAS IP ASOCIADAS A LOS REGISTROS “A” Y “MX” SEGÚN ESTÁN CONFIGURADOS EN EL SERVIDOR. TAMBIÉN SE INDICA EL RANGO DE DIRECCIONES IP QUE PUEDEN ENVIAR CORREOS EN NOMBRE DEL DOMINIO.
4. EL SIGUIENTE REGISTRO QUE SE INDICA ES EL SOA, QUE PROPORCIONA LA SIGUIENTE INFORMACIÓN.
   - NOMBRE DEL DOMINIO, QUE ES EL QUE SE HA PREGUNTADO.
   - **ORIGIN.** SERVIDOR DE NOMBRES DEL DOMINIO. EN ESTE CASO ES NS2.RA-MA.ES
   - **MAIL ADDR.** ES LA DIRECCIÓN DE CORREO ELECTRÓNICO DEL ADMINISTRADOR DEL DOMINIO. LA @ SE SUSTITUYE POR UN PUNTO.
   - **SERIAL.** SE UTILIZA A MODO DE VERSIONADO, EN UN FORMATO AÑO-MES DÍA SEGUIDO DE UN NÚMERO EN FUNCIÓN DE CUANTAS VECES SE HAYA EDITADO ESE DÍA: “AAAAMMDDXX”.
   - **REFRESH.** INTERVALO (EN SEGUNDOS) QUE TARDARÁ EL SERVIDOR DNS SECUNDARIO EN COMPROBAR CON EL PRIMARIO SI SE HA MODIFICADO LA VERSIÓN, DESDE LA ANTERIOR COMPROBACIÓN.
   - **RETRY.** INTERVALO DE RECONEXIÓN CON EL SERVIDOR PRIMARIO, EN CASO DE FALLO EN EL INTENTO ANTERIOR.
   - **EXPIRE.** TIEMPO QUE EL SERVIDOR DNS SECUNDARIO CONSIDERA QUE LA INFORMACIÓN DE LA ZONA QUE MANTIENE EN CACHÉ ES VÁLIDA, SI NO PUEDE CONECTARSE CON EL PRIMARIO.
   - **MINIMUM.** TIEMPO QUE UN NOMBRE DE DOMINIO SE GUARDA EN CACHÉ, TRANSCURRIDO EL CUAL EL SERVIDOR DEBE ACTUALIZAR LA INFORMACIÓN PROCEDENTE DE UN SERVIDOR AUTORITATIVO.

RECONOCIMIENTO ACTIVO

DNS

HERRAMIENTAS PARA OBTENER INFORMACIÓN DE UN SERVIDOR DNS

HOST

DESDE LA LÍNEA DE COMANDOS DE **LINUX** SE PUEDE EJECUTAR EL COMANDO **HOST**, PARA REALIZAR BÚSQUEDAS **DNS** TANTO DIRECTAS COMO INVERSAS, ASÍ COMO PARA MOSTRAR EL RESULTADO DE DISTINTOS REGISTROS Y REALIZAR UNA TRANSFERENCIA DE ZONA.

LA CONSULTA MÁS BÁSICA CON EL COMANDO **HOST** CONSISTE EN INDICAR ÚNICAMENTE EL DOMINIO, CON LO QUE POR DEFECTO SE MOSTRARÁ LA INFORMACIÓN DEL REGISTRO **A**.

```
pru@pru-VirtualBox:~$ host www.google.es
www.google.es has address 142.250.184.3
www.google.es has IPv6 address 2a00:1450:4003:808::2003
pru@pru-VirtualBox:~$
```

RECONOCIMIENTO ACTIVO

DNS

HERRAMIENTAS PARA OBTENER INFORMACIÓN DE UN SERVIDOR DNS

HOST

TAMBIÉN ES POSIBLE INDICAR LOS TIPOS DE REGISTROS QUE SE QUIEREN CONSULTAR, UTILIZANDO EL PARÁMETRO **-T**.

```
pru@pru-VirtualBox:~$ host -t MX www.milaulas.com
www.milaulas.com is an alias for proxy.gnomio.com.
pru@pru-VirtualBox:~$
```

RECONOCIMIENTO ACTIVO

DNS

HERRAMIENTAS PARA OBTENER INFORMACIÓN DE UN SERVIDOR DNS

DIG

PERMITE REALIZAR CONSULTAS A LOS SERVIDORES **DNS**. EN LA EJECUCIÓN DE **DIG** SE PUEDE INDICAR EL DOMINIO, EL TIPO DE REGISTRO A CONSULTAR, Y EL SERVIDOR **DNS** QUE SE QUIERE UTILIZAR. PARA INDICAR LOS REGISTROS SE PUEDE UTILIZAR O EL PARÁMETRO **-T**.

DE IGUAL MANERA QUE CON **NSLOOKUP** Y CON **HOST**, ES POSIBLE OBTENER LOS SERVIDORES DNS HACIENDO UNA CONSULTA DE LOS REGISTROS **NS**.

RECONOCIMIENTO ACTIVO

DNS

HERRAMIENTAS PARA OBTENER INFORMACIÓN DE UN SERVIDOR DNS

DIG

```
pru@pru-VirtualBox:~$ dig www.ull.es -t ns

; <<>> DiG 9.18.18-0ubuntu0.22.04.2-Ubuntu <<>> www.ull.es -t ns
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22268
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.ull.es.                    IN      NS

;; ANSWER SECTION:
www.ull.es.             600     IN      CNAME   w4.stic.ull.es.

;; AUTHORITY SECTION:
stic.ull.es.            600     IN      SOA     dns1.ull.es. hostmaster.stic.ull.es. 1708947259 120
0 300 1209600 3600

;; Query time: 163 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Sun Mar 03 04:54:28 WET 2024
;; MSG SIZE  rcvd: 113
```

RECONOCIMIENTO ACTIVO

DNS

HERRAMIENTAS PARA OBTENER INFORMACIÓN DE UN SERVIDOR DNS

OTRAS HERRAMIENTAS

EXISTEN HERRAMIENTAS DESARROLLADAS ESPECÍFICAMENTE PARA RECONOCIMIENTO, ASÍ COMO OTRAS MULTIPROPÓSITO QUE PERMITEN OBTENER INFORMACIÓN A PARTIR DE LOS **DNS**. ALGUNAS DE LAS MÁS DESTACABLES SON LAS SIGUIENTES:

- **DNSENUM** DISPONIBLE EN DISTRIBUCIONES. SE PUEDE DESCARGAR DE: HTTPS://GITHUB.COM/FWAEYTENS/DNSENUM
- **DNSRECON** INSTALADA EN DISTRIBUCIONES DE SEGURIDAD. SE PUEDE ENCONTRAR EN: HTTPS://GITHUB.COM/DARKOPERATOR/DNSRECON

RECONOCIMIENTO ACTIVO

DNS

HERRAMIENTAS PARA OBTENER INFORMACIÓN DE UN SERVIDOR DNS

TRANSFERENCIAS DE ZONA

ESTÁN PENSADAS PARA ACTUALIZAR LA INFORMACIÓN DE LOS **SERVIDORES DNS SECUNDARIOS** A PARTIR DE LA INFORMACIÓN QUE TIENEN LOS **PRIMARIOS**.

SE LLEVAN A CABO EN EL PUERTO **TCP 53** Y, GENERALMENTE, LOS SERVIDORES DNS BIEN CONFIGURADOS BLOQUEARÁN TODAS LAS TRANSFERENCIAS DE ZONA QUE SE EJECUTEN DESDE INTERNET DESDE DIRECCIONES IP NO AUTORIZADAS, POR LO QUE DURANTE ESTA FASE SERÁ IMPROBABLE QUE SE OBTENGAN RESULTADOS.

RECONOCIMIENTO ACTIVO

DNS

HERRAMIENTAS PARA OBTENER INFORMACIÓN DE UN SERVIDOR DNS

TRANSFERENCIAS DE ZONA

PUEDEN SER DE UTILIDAD DURANTE LA POST-EXPLOTACIÓN. UNA VEZ QUE SE LOGRE ACCESO A REDES INTERNAS CABE LA POSIBILIDAD DE TENER ACCESO A SERVIDORES DNS INTERNOS DE LA ORGANIZACIÓN Y TAL VEZ SE PUEDA REALIZAR UNA TRANSFERENCIA DE ZONA DESDE UN EQUIPO COMPROMETIDO.

RECONOCIMIENTO ACTIVO

INGENIERÍA SOCIAL

LA INGENIERÍA SOCIAL **SE SUSTENTA EN LA PREMISA DE QUE EL SER HUMANO ES EL ESLABÓN MÁS DÉBIL EN LA CADENA DE LA CIBERSEGURIDAD**, POR LO QUE UTILIZA DISTINTAS TÉCNICAS DE MANIPULACIÓN PARA CONSEGUIR QUE LOS USUARIOS REALICEN ALGUNA ACCIÓN O REVELEN INFORMACIÓN SENSIBLE. ES DE GRAN IMPORTANCIA DURANTE EL RECONOCIMIENTO.

GENERALMENTE, TODAS LAS ACCIONES DE INGENIERÍA SOCIAL IRÁN PRECEDIDAS DE UN RECONOCIMIENTO MÁS O MENOS PROFUNDO QUE HAYA PERMITIDO, AL MENOS, IDENTIFICAR ALGUNOS EMPLEADOS DE UNA ORGANIZACIÓN, TRAS LO CUAL SE EMPLEARÁN UNA SERIE DE TÉCNICAS CON EL FIN DE OBTENER INFORMACIÓN.

RECONOCIMIENTO ACTIVO

INGENIERÍA SOCIAL

ALGUNAS DE ESTAS TÉCNICAS SON LAS SIGUIENTES:

PHISHING/VISHING/SMISHING

CORREOS ELECTRÓNICOS, LLAMADAS DE TELÉFONO O MENSAJES DE TEXTO FALSOS QUE SIMULAN PROCEDER DE UNA FUENTE LEGÍTIMA Y QUE SE UTILIZAN PARA QUE CONSEGUIR EXTRAER INFORMACIÓN PERSONAL, FINANCIERA O DE LA ORGANIZACIÓN.

REDES SOCIALES

OBTENER INFORMACIÓN DE MANERA PASIVA, EN MUCHOS CASOS, ESTO NO SERÁ POSIBLE O SE NECESITARÁ DE UNA INTERACCIÓN DIRECTA CON LA VÍCTIMA. EN ESTE ÚLTIMO CASO, UN ATACANTE BUSCARÁ ESTABLECER UNA RELACIÓN CON LA VÍCTIMA Y GANARSE SU CONFIANZA PARA CONSEGUIR QUE REVELE INFORMACIÓN.

RECONOCIMIENTO ACTIVO

INGENIERÍA SOCIAL

DUMPSTER DIVING

QUE CONSISTE EN REBUSCAR EN LA BASURA DE LA VÍCTIMA DE MODO QUE SE PUEDA OBTENER INFORMACIÓN PERSONAL O DE LA ORGANIZACIÓN.

CONTENIDOS

- INTRODUCCIÓN
- OSINT/RECONOCIMIENTO PASIVO
- RECONOCIMIENTO ACTIVO
- **OTRAS HERRAMIENTAS DE RECONOCIMIENTO**
- ANÁLISIS DE METADATOS

OTRAS HERRAMIENTAS DE RECONOCIMIENTO ACTIVO

EXISTEN OTRAS HERRAMIENTAS QUE PROPORCIONAN EN UN MISMO ENTORNO MUCHAS DE LAS FUNCIONALIDADES MENCIONADAS ANTERIORMENTE Y GENERAN INFORMES CON LA INFORMACIÓN RECOPILADA DE MANERA COHERENTE Y ORDENADA.

NO OBSTANTE, NO SE DEBE PERDER DE VISTA QUE LAS HERRAMIENTAS NO LLEGARÁN A TODOS LOS SITIOS Y TAMBIÉN PUEDEN GENERAR MUCHA INFORMACIÓN NO RELACIONADA CON EL OBJETIVO, POR LO QUE SIEMPRE RESULTARÁ NECESARIA UNA REVISIÓN DE LA MISMA, ASÍ COMO COMPLEMENTARLA CON LA INFORMACIÓN QUE SE PUEDA OBTENER DE ACCIONES MANUALES.

OTRAS HERRAMIENTAS DE RECONOCIMIENTO ACTIVO

RECON-NG

ES UN **FRAMEWORK DESARROLLADO EN PYTHON** POR *TIM TOMES* (*LANMASTER53*). DISPONIBLE DE MANERA GRATUITA EN GITHUB:

HTTPS://GITHUB.COM/LANMASTER53/RECON-NG

AUNQUE **SE MANEJA CON COMANDOS**, PROPORCIONA UN **ENTORNO UNIFICADO** DESDE EL QUE **LLEVAR ACCIONES DE RECONOCIMIENTO DE MANERA INTERACTIVA.**

ESTÁ DISEÑADO PARA REALIZAR UN **RECONOCIMIENTO BASADO EN LA WEB** Y **ALMACENAR LOS RESULTADOS EN UNA BASE DE DATOS**, QUE SE PUEDE **CONSULTAR** Y EXPORTAR LOS DATOS.

SE BASA EN **MÓDULOS ORGANIZADOS POR CATEGORÍAS** ORIENTADAS A LAS DISTINTAS ACCIONES QUE SE PUEDEN REALIZAR.

OTRAS HERRAMIENTAS DE RECONOCIMIENTO ACTIVO

RECON-NG

SE PUEDE **UTILIZAR** EN CUALQUIER SISTEMA OPERATIVO QUE TENGA **PYTHON INSTALADO EN SU VERSIÓN 3.7.6 O SUPERIOR**.

LAS DISTRIBUCIONES ORIENTADAS A SEGURIDAD LA TENDRÁN DISPONIBLE EN SUS REPOSITORIOS, POR LO QUE SE INSTALARÁ COMO CUALQUIER OTRO PAQUETE, MIENTRAS QUE PARA OTRAS DISTRIBUCIONES SERÁ NECESARIO CLONAR EL REPOSITORIO DE GITHUB E INSTALAR LAS DEPENDENCIAS.

LA INSTALACIÓN DESDE LOS REPOSITORIOS DE UNA DISTRIBUCIÓN BASADA EN DEBIAN ES IGUAL A LA DE CUALQUIER PAQUETE:

```
SUDO APT INSTALL RECON-NG
```

OTRAS HERRAMIENTAS DE RECONOCIMIENTO ACTIVO

RECON-NG

LA INSTALACIÓN DESDE EL REPOSITORIO DE GITHUB REQUIERE TENER INSTALADO PREVIAMENTE **PIP O PIP3**:

```
SUDO APT INSTALL PYTHON-PIP [SUDO APT INSTALL PYTHON3-PIP]
GIT CLONE HTTPS://GITHUB.COM/LANMASTER53/RECON-NG.GIT CD RECON-NG
SUDO PIP INSTALL -R REQUIREMENTS [PIP3 INSTALL -R REQUIREMENTS]
SUDO PIP INSTALL LXML [PIP3 INSTALL IXML]
```

ES PRECISO TENER EN CUENTA QUE LAS DEPENDENCIAS QUE SE INSTALAN SON LAS NECESARIAS PARA EJECUTAR EL FRAMEWORK, NO LAS REQUERIDAS POR LOS DIFERENTES MÓDULOS. UNA VEZ INSTALADAS LAS DEPENDENCIAS SE PUEDE EJECUTAR LA HERRAMIENTA

OTRAS HERRAMIENTAS DE RECONOCIMIENTO ACTIVO

RECON-NG

LA HERRAMIENTA NO ES EXCESIVAMENTE COMPLICADA DE MANEJAR, SIN EMBARGO, AL DISPONER DE NUMEROSOS MÓDULOS, REQUIERE UN PERIODO DE FAMILIARIZACIÓN MÁS O MENOS EXTENSO ANTES DE EMPLEARLA EN ENTORNOS REALES.

AL INICIAR LA HERRAMIENTA POR PRIMERA VEZ SE MUESTRA EL MENSAJE ***NO MODULES ENABLED/INSTALLED***.

CON EL COMANDO **HELP** SE MUESTRA AYUDA DE LOS COMANDOS QUE SE PUEDEN EJECUTAR.

OTRAS HERRAMIENTAS DE RECONOCIMIENTO ACTIVO

RECON-NG

OTRAS HERRAMIENTAS DE RECONOCIMIENTO ACTIVO

RECON-NG

```
[recon-ng][default] > help

Commands (type [help|?] <topic>):
---------------------------------
back            Exits the current context
dashboard       Displays a summary of activity
db              Interfaces with the workspace's database
exit            Exits the framework
help            Displays this menu
index           Creates a module index (dev only)
keys            Manages third party resource credentials
marketplace     Interfaces with the module marketplace
modules         Interfaces with installed modules
options         Manages the current context options
pdb             Starts a Python Debugger session (dev only)
script          Records and executes command scripts
shell           Executes shell commands
show            Shows various framework items
snapshots       Manages workspace snapshots
spool           Spools output to a file
workspaces      Manages workspaces

[recon-ng][default] >
```

OTRAS HERRAMIENTAS DE RECONOCIMIENTO ACTIVO

RECON-NG

ANTES DE HACER NADA SERÁ NECESARIO CARGAR LOS MÓDULOS.

PARA LISTAR LOS MÓDULOS DISPONIBLES SE PUEDE UTILIZAR EL COMANDO **MARKETPLACE SEARCH**, CON LO QUE SE MOSTRARÁ UNA LISTA DE MÓDULOS QUE INDICARÁ, PARA CADA UNO DE ELLOS, INFORMACIÓN ACERCA DE LA VERSIÓN, FECHA DE ACTUALIZACIÓN, SI ESTÁ INSTALADO Y SI TIENE DEPENDENCIAS (***COLUMNA D***) O REQUIERE CLAVES API (***COLUMNA K***).

EL FRAMEWORK DISPONE DE DIFERENTES CATEGORÍAS EN LOS QUE SE AGRUPAN LOS MÓDULOS SEGÚN SU PROPÓSITO:

OTRAS HERRAMIENTAS DE RECONOCIMIENTO ACTIVO

RECON-NG

ANTES DE HACER NADA SERÁ NECESARIO CARGAR LOS MÓDULOS.

PARA LISTAR LOS MÓDULOS DISPONIBLES SE PUEDE UTILIZAR EL COMANDO **MARKETPLACE SEARCH**, CON LO QUE SE MOSTRARÁ UNA LISTA DE MÓDULOS QUE INDICARÁ, PARA CADA UNO DE ELLOS, INFORMACIÓN ACERCA DE LA VERSIÓN, FECHA DE ACTUALIZACIÓN, SI ESTÁ INSTALADO Y SI TIENE DEPENDENCIAS (***COLUMNA D***) O REQUIERE CLAVES API (***COLUMNA K***).

EL FRAMEWORK **DISPONE DE DIFERENTES CATEGORÍAS** EN LOS QUE SE AGRUPAN LOS **MÓDULOS SEGÚN SU PROPÓSITO**:

OTRAS HERRAMIENTAS DE RECONOCIMIENTO ACTIVO

RECON-NG

- **DISCOVERY.** TIENE DOS MÓDULOS QUE PERMITE OBTENER INFORMACIÓN INTERACTUANDO DIRECTAMENTE CON EL ENTORNO DEL OBJETIVO. INCLUYE UN MÓDULO PARA BUSCAR ARCHIVOS EN LA WEB INDICADA Y OTRO MÓDULO PARA BUSCAR EN LA CACHÉ DEL DNS LOS DOMINIOS VISITADOS, CON EL FIN DE INTENTAR DETERMINAR EL ANTIVIRUS UTILIZADO POR LA ORGANIZACIÓN.
- **EXPLOITATION.** CONTIENE DOS MÓDULOS PENSADOS PARA EXPLOTAR VULNERABILIDADES EN LA WEB.

OTRAS HERRAMIENTAS DE RECONOCIMIENTO ACTIVO

RECON-NG

- **RECON.** ES LA CATEGORÍA QUE ENGLOBA MÁS MÓDULOS, DEDICADOS AL PROPÓSITO PRINCIPAL DE LA HERRAMIENTA, QUE ES EL RECONOCIMIENTO DE DIFERENTES ASPECTOS. DISPONE DE **MÓDULOS** DE *RESOLUCIÓN DE NOMBRES Y DIRECCIONES IP*, MÓDULOS *PARA HACER BÚSQUEDAS EN DIFERENTES MOTORES DE BÚSQUEDA*, *ACCESOS BASES DE DATOS DE CREDENCIALES EXPUESTAS EN INTERNET*, ETC.

  ES NECESARIO TENER EN CUENTA QUE PARA MUCHOS DE ELLOS SERÁ NECESARIO CONFIGURAR UNA **API KEY**, POR LO QUE PREVIAMENTE SERÁ NECESARIO UN REGISTRO EN LOS SITIOS CORRESPONDIENTES.

OTRAS HERRAMIENTAS DE RECONOCIMIENTO ACTIVO

RECON-NG

- **REPORTING.** LA HERRAMIENTA PROPORCIONA LA POSIBILIDAD DE EXPORTAR INFORMACIÓN EN DIFERENTES FORMATOS.
- **IMPORT,** PENSADO PARA IMPORTAR ARCHIVOS DE TEXTO CON INFORMACIÓN RELACIONADA CON HOSTS Y CON PUERTOS, PARA COMPLETAR LA BASE DE DATOS. LA HERRAMIENTA TAMBIÉN PERMITE CREAR Y UTILIZAR MÓDULOS CREADOS POR LOS USUARIOS.

OTRAS HERRAMIENTAS DE RECONOCIMIENTO ACTIVO

RECON-NG

LA INSTALACIÓN DE LOS MÓDULOS SE PUEDE HACER: **DE MANERA INDIVIDUAL**, INDICANDO EL PATH COMPLETO O EL NOMBRE, **INDICANDO EL TIPO** PARA INSTALAR TODOS LOS MÓDULOS DE ESE TIPO, O **HACER UNA CARGA MASIVA DE TODOS LOS MÓDULOS.**

```
marketplace install path_módulo
marketplace install nombre
marketplace install tipo_módulos
marketplace install all
```

OTRAS HERRAMIENTAS DE RECONOCIMIENTO ACTIVO

RECON-NG

SI SE QUIEREN CONOCER LOS MÓDULOS INSTALADOS SE UTILIZARÁ EL COMANDO **MODULES**.

PARA PODER EJECUTAR UN MÓDULO ES NECESARIO CARGARLO USANDO EL COMANDO **MODULES** Y CONFIGURAR LAS OPCIONES CON EL COMANDO **OPTIONS**.

PARA OBTENER MÁS INFORMACIÓN DEL MÓDULO Y CONOCER LAS OPCIONES QUE SE PUEDEN CONFIGURAR SE RECURRIRÁ AL COMANDO **INFO**.

OTRAS HERRAMIENTAS DE RECONOCIMIENTO ACTIVO

RECON-NG

```
[recon-ng][default] > modules load recon/domains-contacts/metacrawler
[recon-ng][default][metacrawler] > info

      Name: Meta Data Extractor
    Author: Tim Tomes (@lanmaster53)
   Version: 1.1

Description:
  Searches for files associated with the provided domain(s) and extracts any contact related metadata.

Options:
  Name     Current Value  Required  Description
  -------  -------------  --------  -----------
  EXTRACT  False          yes       extract metadata from discovered files
  SOURCE   default        yes       source of input (see 'info' for details)

Source Options:
  default        SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
  <string>       string representing a single input
  <path>         path to a file containing a list of inputs
  query <sql>    database query returning one column of inputs

Comments:
  * Currently supports doc, docx, xls, xlsx, ppt, pptx, and pdf file types.
```

OTRAS HERRAMIENTAS DE RECONOCIMIENTO ACTIVO

RECON-NG

```
[recon-ng][default] > modules load recon/domains-contacts/metacrawler
[recon-ng][default][metacrawler] > info

      Name: Meta Data Extractor
    Author: Tim Tomes (@lanmaster53)
   Version: 1.1

Description:
  Searches for files associated with the provided domain(s) and extracts any contact related metadata.

Options:
  Name     Current Value  Required  Description
  -------  -------------  --------  -----------
  EXTRACT  False          yes       extract metadata from discovered files
  SOURCE   default        yes       source of input (see 'info' for details)

Source Options:
  default        SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
  <string>       string representing a single input
  <path>         path to a file containing a list of inputs
  query <sql>    database query returning one column of inputs

Comments:
  * Currently supports doc, docx, xls, xlsx, ppt, pptx, and pdf file types.
```

OTRAS HERRAMIENTAS DE RECONOCIMIENTO ACTIVO

RECON-NG. EJEMPLO

```
[recon-ng][default] > marketplace install hackertarget
[*] Module installed: recon/domains-hosts/hackertarget
[*] Reloading modules...
[recon-ng][default] > modules load hackertarget
[recon-ng][default][hackertarget] > options set SOURCE ull.es
SOURCE ⇒ ull.es
[recon-ng][default][hackertarget] > run
```

OTRAS HERRAMIENTAS DE RECONOCIMIENTO ACTIVO

RECON-NG. EJEMPLO

```
______
ULL.ES
______
[*] Country: None
[*] Host: appserver.saii.ull.es
[*] Ip_Address: 193.145.111.242
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------------------
[*] Country: None
[*] Host: campusingenieriaytecnologia.ull.es
[*] Ip_Address: 193.145.118.202
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------------------
```

```
[*] ------------------------------------------------------------
[*] Country: None
[*] Host: 0075-balbpub5-correo.com.stic.ull.es
[*] Ip_Address: 193.145.118.161
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------------------
[*] Country: None
[*] Host: beowulf.pcg.ull.es
[*] Ip_Address: 193.145.101.115
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------------------

_______
SUMMARY
_______
[*] 500 total (0 new) hosts found.
```

OTRAS HERRAMIENTAS DE RECONOCIMIENTO ACTIVO

RECON-NG. EJEMPLO

```
[recon-ng][default] > modules load xssed
[recon-ng][default][xssed] > options set SOURCE ull.es
SOURCE => ull.es
[recon-ng][default][xssed] > run

------
ULL.ES
------
[*] No vulnerabilites found.
[recon-ng][default][xssed] > options set SOURCE ulpgc.es
SOURCE => ulpgc.es
[recon-ng][default][xssed] > run

--------
ULPGC.ES
--------
[*] Category: XSS
[*] Example: http://www.ulpgc.es/index.php?pagina=buscadorrapido&ver=inicio&codigo_buscador=3&B='><script
>alert(1<br>);</script>test&accion=Buscar
[*] Host: www.ulpgc.es
[*] Notes: None
[*] Publish_Date: 2010-07-09 00:00:00
[*] Reference: http://xssed.com/mirror/55417/
[*] Status: unfixed
[*] ---------------------------------------------------

-------
SUMMARY
-------
[*] 1 total (0 new) vulnerabilities found.
```

OTRAS HERRAMIENTAS DE RECONOCIMIENTO ACTIVO

RECON-NG. EJEMPLO

```
[recon-ng][default] > marketplace load module recon/hosts-hosts/resolve
Interfaces with the module marketplace

Usage: marketplace <info|install|refresh|remove|search> [...]

[recon-ng][default] > modules load recon/hosts-hosts/resolve
[recon-ng][default][resolve] > options
Manages the current context options

Usage: options <list|set|unset> [...]

[recon-ng][default][resolve] > options set SOURCE ull.es
SOURCE => ull.es
[recon-ng][default][resolve] > run
[*] ull.es => 193.145.118.52
[recon-ng][default][resolve] >
```

OTRAS HERRAMIENTAS DE RECONOCIMIENTO ACTIVO

theHarvester

SE TRATA DE OTRA HERRAMIENTA QUE PERMITE OBTENER INFORMACIÓN PROCEDENTE DE DIVERSAS FUENTES. EN ESTE CASO, ESTÁ DESARROLLADA POR **CHRISTIAN MARTORELLA** Y TAMBIÉN ESTÁ DISPONIBLE DE MANERA GRATUITA EN UN REPOSITORIO DE GITHUB:

HTTPS://GITHUB.COM/LARAMIES/THEHARVESTER

EL PROCESO DE INSTALACIÓN ES SIMILAR AL QUE SE HA DESCRITO PARA **RECON-NG**, Y EN EL PROPIO GIT DE LA HERRAMIENTA DISPONE DE UN ENLACE EN EL QUE SE INDICAN LOS PASOS PARA INSTALARLO DE DIVERSAS FORMAS.

OTRAS HERRAMIENTAS DE RECONOCIMIENTO ACTIVO

theHarvester

LA HERRAMIENTA **PERMITE HACER RECONOCIMIENTO PASIVO Y ACTIVO**, Y **BUSCA EN DIVERSAS FUENTES** PARA *RECOPILAR NOMBRES*, *DIRECCIONES DE CORREO ELECTRÓNICO*, *DOMINIOS*, *DIRECCIONES IP, Y DIRECCIONES WEB*.

ENTRE EL RECONOCIMIENTO ACTIVO, PERMITE SACAR CAPTURAS DE PANTALLA AUTOMÁTICAS DE LOS SUBDOMINIOS QUE SE ENCUENTRE, ASÍ COMO REALIZAR UNA ENUMERACIÓN POR FUERZA BRUTA DEL DNS.

SERÁ PRECISO INDICAR LA BÚSQUEDA A REALIZAR A TRAVÉS DE PARÁMETROS.

OTRAS HERRAMIENTAS DE RECONOCIMIENTO ACTIVO

theHarvester

PARA VER TODAS LAS OPCIONES QUE OFRECE EJECUTA EL COMANDO:

```
theHarvester -h
```

```
└─$ theHarvester -h
Read proxies.yaml from /home/kali/.theHarvester/proxies.yaml
*******************************************************************
*  _   _                                            _             *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __| '_ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* theHarvester 4.5.1                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************
usage: theHarvester [-h] -d DOMAIN [-l LIMIT] [-S START] [-p] [-s] [--screenshot SCREENSHOT] [-v] [-e DNS_SERVER] [-t] [-r [DNS_RESOLVE]] [-n] [-c]
                    [-f FILENAME] [-b SOURCE]

theHarvester is used to gather open source intelligence (OSINT) on a company or domain.

options:
  -h, --help            show this help message and exit
  -d DOMAIN, --domain DOMAIN
                        Company name or domain to search.
  -l LIMIT, --limit LIMIT
                        Limit the number of search results, default=500.
  -S START, --start START
                        Start with result number X, default=0.
  -p, --proxies         Use proxies for requests, enter proxies in proxies.yaml.
  -s, --shodan          Use Shodan to query discovered hosts.
  --screenshot SCREENSHOT
                        Take screenshots of resolved domains specify output directory: --screenshot output_directory
  -v, --virtual-host    Verify host name via DNS resolution and search for virtual hosts.
  -e DNS_SERVER, --dns-server DNS_SERVER
                        DNS server to use for lookup.
  -t, --take-over       Check for takeovers.
  -r [DNS_RESOLVE], --dns-resolve [DNS_RESOLVE]
                        Perform DNS resolution on subdomains with a resolver list or passed in resolvers, default False.
  -n, --dns-lookup      Enable DNS server lookup, default False.
  -c, --dns-brute       Perform a DNS brute force on the domain.
  -f FILENAME, --filename FILENAME
                        Save the results to an XML and JSON file.
  -b SOURCE, --source SOURCE
                        anubis, baidu, bevigil, binaryedge, bing, bingapi, bufferoverun, brave, censys, certspotter, criminalip, crtsh, dnsdumpster,
                        duckduckgo, fullhunt, github-code, hackertarget, hunter, hunterhow, intelx, netlas, onyphe, otx, pentesttools, projectdiscovery,
                        rapiddns, rocketreach, securityTrails, sitedossier, subdomaincenter, subdomainfinderc99, threatminer, tomba, urlscan, virustotal,
                        yahoo, zoomeye
```

OTRAS HERRAMIENTAS DE RECONOCIMIENTO ACTIVO

theHarvester

PUEDES VISUALIZAR LOS PRINCIPALES COMANDOS:

-d: DOMINIO OBJETIVO SOBRE EL QUE SE QUIERE REALIZAR EL ANÁLISIS. POR EJEMPLO, OSI.ES.

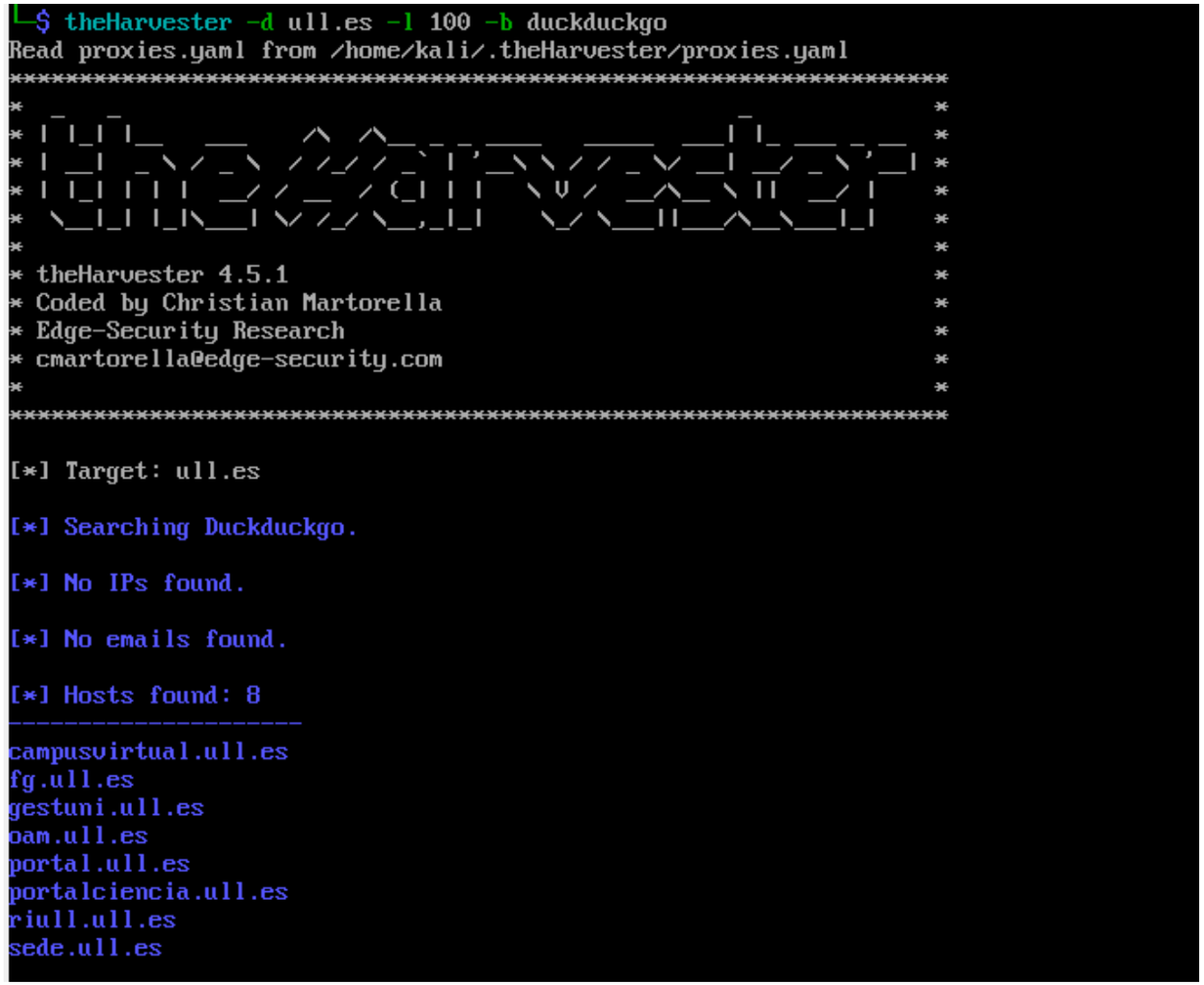
-l: LÍMITE PARA EVITAR QUE LA BÚSQUEDA COLAPSE. SE PUEDE LIMITAR A UN NÚMERO DETERMINADO DE RESULTADOS, POR EJEMPLO, AL LÍMITE -L 100.

-f: ARCHIVO. SI SE QUIERE EXPORTAR LOS RESULTADOS A UN ARCHIVO, LOS FORMATOS MÁS HABITUALES SON .XMLO .JSON, POR EJEMPLO, -F RESULTADOS.XML.

-b: FUENTE. SE PUEDEN ESPECIFICAR UNO O VARIOS MOTORES DE BÚSQUEDA CON LOS QUE SE REALIZARÁ EL ANÁLISIS. POR EJEMPLO, -B BING.

OTRAS HERRAMIENTAS DE RECONOCIMIENTO ACTIVO

theHarvester



CONTENIDOS

- INTRODUCCIÓN
- OSINT/RECONOCIMIENTO PASIVO
- RECONOCIMIENTO ACTIVO
- OTRAS HERRAMIENTAS DE RECONOCIMIENTO
- **ANÁLISIS DE METADATOS**

ANÁLISIS DE METADATOS

EL **REAL DECRETO 1708/2011** POR EL QUE SE ESTABLECE EL SISTEMA ESPAÑOL DE ARCHIVOS, DEFINE LOS METADATOS COMO:

> *CUALQUIER DESCRIPCIÓN ESTANDARIZADA DE LAS CARACTERÍSTICAS DE UN CONJUNTO DE DATOS. EN EL CONTEXTO DEL DOCUMENTO ELECTRÓNICO CUALQUIER TIPO DE INFORMACIÓN EN FORMA ELECTRÓNICA ASOCIADA A LOS DOCUMENTOS ELECTRÓNICOS, DE CARÁCTER INSTRUMENTAL E INDEPENDIENTE DE SU CONTENIDO, DESTINADA AL CONOCIMIENTO INMEDIATO Y AUTOMATIZABLE DE ALGUNA DE SUS CARACTERÍSTICAS, CON LA FINALIDAD DE GARANTIZAR LA DISPONIBILIDAD, EL ACCESO, LA CONSERVACIÓN Y LA INTEROPERABILIDAD DEL PROPIO DOCUMENTO*

EN POCAS PALABRAS, **SON DATOS QUE DESCRIBEN OTROS DATOS.**

ANÁLISIS DE METADATOS

LOS ARCHIVOS INFORMÁTICOS SE GENERAN CON DISTINTAS APLICACIONES QUE AÑADEN UNA INFORMACIÓN ADICIONAL ESTRUCTURADA EN FORMA DE METADATOS, QUE NO SE MUESTRAN AL USUARIO DURANTE LA VISUALIZACIÓN DEL DOCUMENTO.

ESTA INFORMACIÓN SE REFIERE A ASPECTOS RELACIONADOS CON FECHAS FORMATOS Y FORMAS DE VISUALIZACIÓN, PERO TAMBIÉN EXISTEN METADATOS QUE PROPORCIONAN MÁS INFORMACIÓN QUE PUEDE RESULTAR MUY ÚTIL PARA UN ATACANTE, POR EJEMPLO:

- **APLICACIÓN UTILIZADA PARA LA GENERACIÓN DEL DOCUMENTO**. NO SOLAMENTE EL NOMBRE, SINO QUE ADEMÁS PUEDE INFORMAR DE LA VERSIÓN UTILIZADA EN EL MOMENTO DE CREAR EL ARCHIVO. ESTO LE SIRVE A UN ATACANTE PARA CONOCER POSIBLES VULNERABILIDADES Y PREPARAR VECTORES DE ATAQUE PARA ATAQUES CLIENT-SIDE.

ANÁLISIS DE METADATOS

- **NOMBRES DE USUARIO**. USUARIOS QUE HAN CREADO Y MODIFICADO EL DOCUMENTO. SEGÚN CÓMO SE GENEREN EN LA ORGANIZACIÓN, PUEDE PROPORCIONAR DIRECTAMENTE EL NOMBRE DE USUARIOS EN EL SISTEMA, O SIMPLEMENTE PUEDE PROPORCIONAR INFORMACIÓN ACERCA DEL NOMBRE Y APELLIDOS DE LOS MISMOS. EN CUALQUIERA DE LOS CASOS, SE TRATA DE UNA INFORMACIÓN VALIOSA PARA UN ATACANTE.
- **DIRECCIONES DE CORREO ELECTRÓNICO**. NUEVAMENTE, UNA INFORMACIÓN MUY ÚTIL PARA UN ATACANTE, QUE LA PUEDE UTILIZAR PARA REALIZAR ATAQUES UTILIZANDO INGENIERÍA SOCIAL.
- **RUTAS EN LAS QUE SE HAN CREADO**. ALGUNOS METADATOS PROPORCIONAN INFORMACIÓN ACERCA DE LA RUTA DEL ARCHIVO CUANDO SE GENERÓ EN EL SISTEMA, LO QUE PUEDE PROPORCIONAR INFORMACIÓN ACERCA DE NOMBRES DE DIRECTORIO QUE PUEDEN RESULTAR DE INTERÉS PARA UN ATACANTE.

ANÁLISIS DE METADATOS

LOS METADATOS DE UNA ORGANIZACIÓN LE **FACILITAN LAS BÚSQUEDAS Y LA INTEGRACIÓN** DE LOS ARCHIVOS EN REPOSITORIOS CENTRALIZADOS.

SIN EMBARGO, UNA EXPOSICIÓN PÚBLICA DE ARCHIVOS CON METADATOS **PUEDE SUPONER UNA FUGA INDESEADA E INCONSCIENTE DE INFORMACIÓN**.

PRÁCTICAMENTE TODOS LOS TIPOS DE ARCHIVOS CONTENDRÁN ALGÚN TIPO DE METADATO. DE MANERA GENERAL, A UN ATACANTE LE INTERESARÁN ARCHIVOS **PDF, HTML**, DE IMAGEN (**JPG, JPEG, ETC.**) Y OFIMÁTICOS (**.DOCX, .DOT, .DOC, .XLSX, .XLS, .PPTX, .PPT, .ODT, .ODF, .ODS, .ODP ETC.**).

PARA PODER EXTRAER LOS METADATOS DE LOS ARCHIVOS ES NECESARIO OBTENER PREVIAMENTE LOS ARCHIVOS. EXISTEN HERRAMIENTAS QUE PERMITEN AUTOMATIZAR LA BÚSQUEDA Y DESCARGA DE ARCHIVOS EN LOS SITIOS WEB DE LA ORGANIZACIÓN E, INCLUSO, PERMITEN AUTOMATIZAR TODO EL PROCESO DE BÚSQUEDA, DESCARGA DE ARCHIVOS Y ANÁLISIS DE METADATOS.

ANÁLISIS DE METADATOS

OBTENCIÓN DE ARCHIVOS CON WGET

AUNQUE **LA FORMA MÁS SIGILOSA PARA DESCARGAR ARCHIVOS ES A TRAVÉS DE UNA NAVEGACIÓN NORMAL** POR LA PÁGINA WEB, **SE TRATA DE UN PROCESO LENTO** Y EN OCASIONES **NO SE ENCONTRARÁN TODOS LOS ARCHIVOS,** POR LO QUE ES E ÚTIL CONOCER TÉCNICAS Y HERRAMIENTAS QUE FACILITEN EL TRABAJO.

UNA HERRAMIENTA ES **WGET.** SE TRATA DE UNA HERRAMIENTA LIBRE Y GRATUITA QUE **PERMITE REALIZAR DESCARGAS DESDE SERVIDORES WEB UTILIZANDO MÚLTIPLES PARÁMETROS** PARA DELIMITAR LAS DESCARGAS, LO QUE PERMITE CONFIGURARLAS PARA PARA ESPECIFICAR LOS TIPOS DE ARCHIVO A BUSCAR E INDICAR QUE LA BÚSQUEDA SE REALICE DE MANERA RECURSIVA.

ANÁLISIS DE METADATOS

OBTENCIÓN DE ARCHIVOS CON WGET

EN EL EJEMPLO SE BUSCAN EN UN DOMINIO I*TODOS LOS ARCHIVOS DE LAS EXTENSIONES INDICADAS* (**-A**), *DE MANERA RECURSIVA* (**-R**) Y SE ALMACENARÁN EN LA RUTA INDICADA (**-P**) Y SIN CREAR SUBDIRECTORIOS (**-ND**):

```
wget -r -l3 -H -t1 -nd -N -np -A.pdf,.docx,.xlsx -
    erobots=off -i -o prueba1/ formacioncip.com
```

CUANDO TERMINE LA EJECUCIÓN SE HABRÁN DESCARGADO EN LA RUTA INDICADA TODOS LOS ARCHIVOS QUE CUMPLAN CON LO INDICADO.

ANÁLISIS DE METADATOS

ANÁLISIS DE METADATOS CON EXIFTOOL

ES UNA HERRAMIENTA GRATUITA MULTIPLATAFORMA DESARROLLADA EN PERL POR *PHIL HARVEY*, **PARA LEER, CREAR Y MODIFICAR METADATOS EN ARCHIVOS DE MÚLTIPLES FORMATOS.**

LA INSTALACIÓN DE **EXIFTOOL** ES MUY SENCILLA, PARA **WINDOWS** Y **MACOS** SE PUEDE ENCONTRAR EN LA WEB DE LA HERRAMIENTA (HTTPS://EXIFTOOL.ORG), Y PARA **LINUX** BASTA CON INSTALAR DESDE LOS REPOSITORIOS EL PAQUETE LIBIMAGE-EXIFTOOL-PERL.

UNA VEZ INSTALADA LA HERRAMIENTA, PARA VISUALIZAR LOS DATOS BASTA CON EJECUTARLA INDICANDO EL NOMBRE DEL ARCHIVO.

ANÁLISIS DE METADATOS

ANÁLISIS DE METADATOS CON FOCA

SE TRATA DE UNA APLICACIÓN PARA **WINDOWS** DESARROLLADA POR **ELEVEN PATHS**, QUE PERMITE LLEVAR A CABO LA DESCARGA DE ARCHIVOS DE UN DOMINIO, ASÍ COMO EL ANÁLISIS DE LOS MISMOS PARA BUSCAR METADATOS.

LA INFORMACIÓN OBTENIDA A PARTIR DE LOS METADATOS SE MUESTRA DE MANERA EN LA HERRAMIENTA DE MANERA ORDENADA Y AGRUPADA POR CATEGORÍAS.

ANÁLISIS DE METADATOS

ANÁLISIS DE METADATOS CON FOCA

LA DESCARGA SE PUEDE REALIZAR A TRAVÉS DEL ENLACE DE DESCARGA DE LA PÁGINA DE LA HERRAMIENTA:

HTTPS://CYBERSECURITYCLOUD.TELEFONICATECH.COM/INNOVACION-LABS/TECNOLOGIAS-INNOVACION/FOCA

QUE REDIRIGE AL GIT DONDE SE PUEDEN ENCONTRAR VARIAS VERSIONES DE LA HERRAMIENTA Y SU CÓDIGO FUENTE.

NO PRECISA INSTALACIÓN Y PARA UTILIZARLA SÓLO **SE REQUIERE DESCARGAR Y DESCOMPRIMIR** UN ARCHIVO .ZIP

ANÁLISIS DE METADATOS

ANÁLISIS DE METADATOS CON FOCA

PERO PARA PODER EJECUTARLA **ES NECESARIO** DISPONER DE UN **SERVIDOR SQL SERVER** AL QUE CONECTARLA.

ESTE SERVIDOR SQL PUEDE SER CUALQUIER VERSIÓN, INCLUIDAS LAS VERSIONES EXPRESS, Y NO TIENE POR QUÉ ESTAR INSTALADO EN EL MISMO EQUIPO EN EL QUE SE EJECUTA LA FOCA, PERO EN ESTE CASO SERÁ PRECISO INDICAR LA CADENA DE CONEXIÓN CUANDO SE INICIE LA HERRAMIENTA.

ANÁLISIS DE METADATOS

ANÁLISIS DE METADATOS CON FOCA

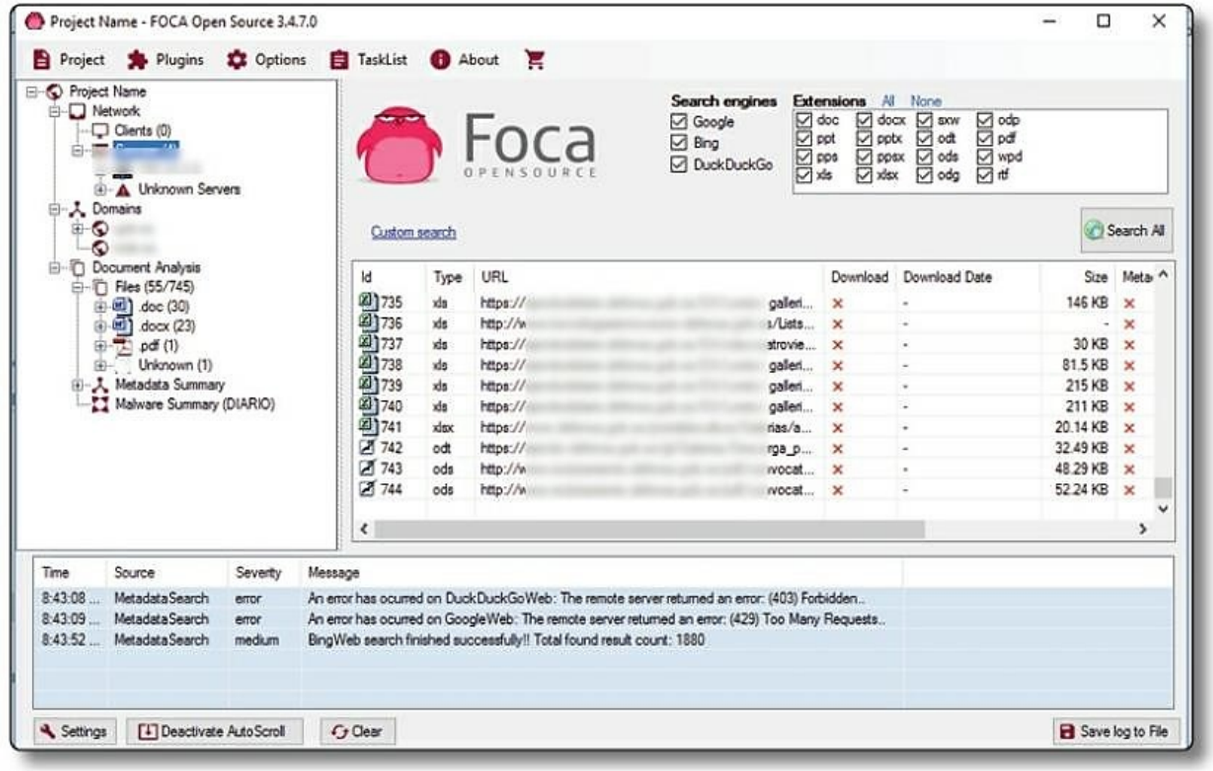
LA PRIMERA ACCIÓN A REALIZAR CUANDO SE EJECUTA LA HERRAMIENTA ES **CREAR UN PROYECTO**.

UNA VEZ INDICADOS EL NOMBRE DEL PROYECTO Y EL DOMINIO, SE PUEDE COMENZAR LA BÚSQUEDA DE ARCHIVOS, PARA LO QUE ES NECESARIO **SELECCIONAR LOS MOTORES DE BÚSQUEDA** QUE SE VAN A UTILIZAR, ASÍ COMO **LOS TIPOS DE ARCHIVO BUSCADOS**.

ANÁLISIS DE METADATOS

ANÁLISIS DE METADATOS CON FOCA

LA HERRAMIENTA IRÁ MOSTRANDO TODOS LOS ARCHIVOS ENCONTRADOS, ASÍ COMO INFORMACIÓN DE LOS SERVIDORES Y DE LOS DOMINIOS.



ANÁLISIS DE METADATOS

ANÁLISIS DE METADATOS CON FOCA

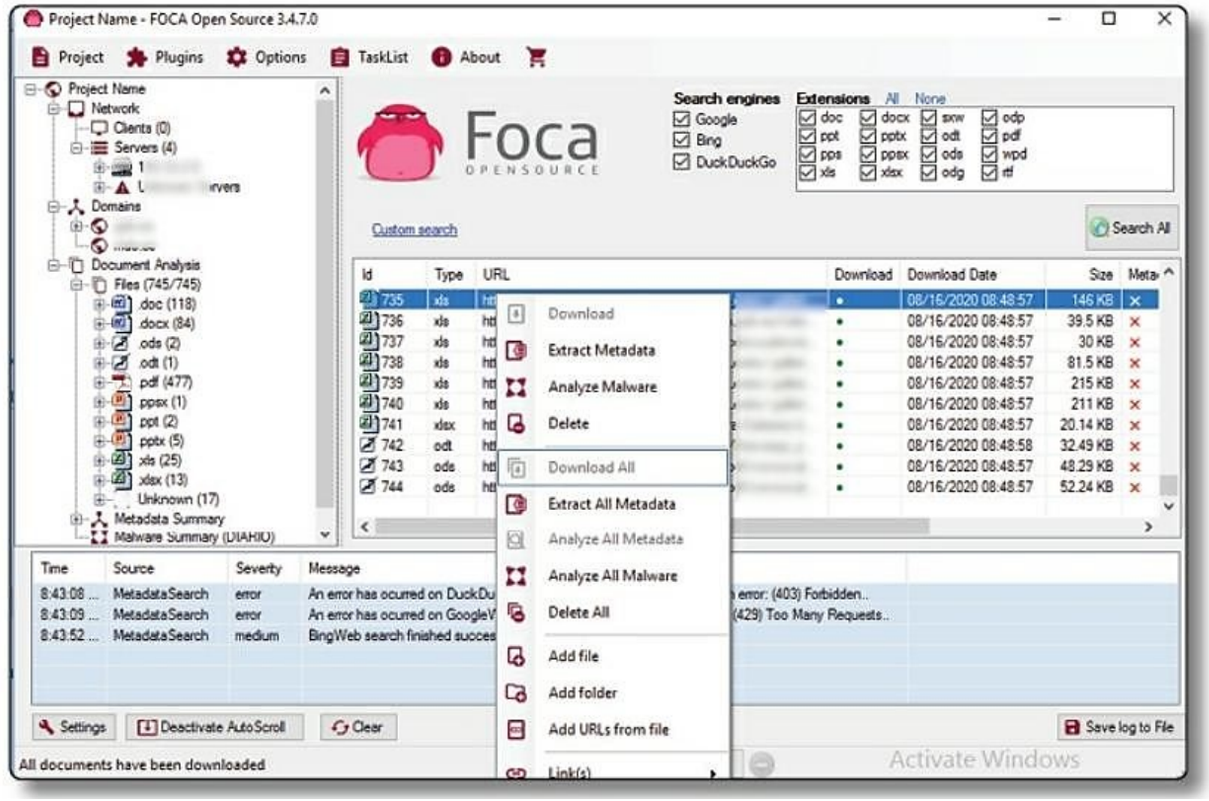
PARA DESCARGAR ARCHIVOS SE PUEDEN SELECCIONAR UNO O VARIOS ARCHIVOS Y **SELECCIONAR LA OPCIÓN DE DESCARGAR** QUE SE MUESTRA EN EL MENÚ CONTEXTUAL.

LOS ARCHIVOS DESCARGADOS SE INDICARÁN CON UN PUNTO VERDE, EN LUGAR DE UNA CRUZ ROJA.

UNA VEZ DESCARGADOS LOS ARCHIVOS, NUEVAMENTE CON EL MENÚ CONTEXTUAL SE PUEDEN EXTRAER LOS METADATOS DE LOS QUE ARCHIVOS SELECCIONADOS O DE TODOS ELLOS.

ANÁLISIS DE METADATOS

ANÁLISIS DE METADATOS CON FOCA



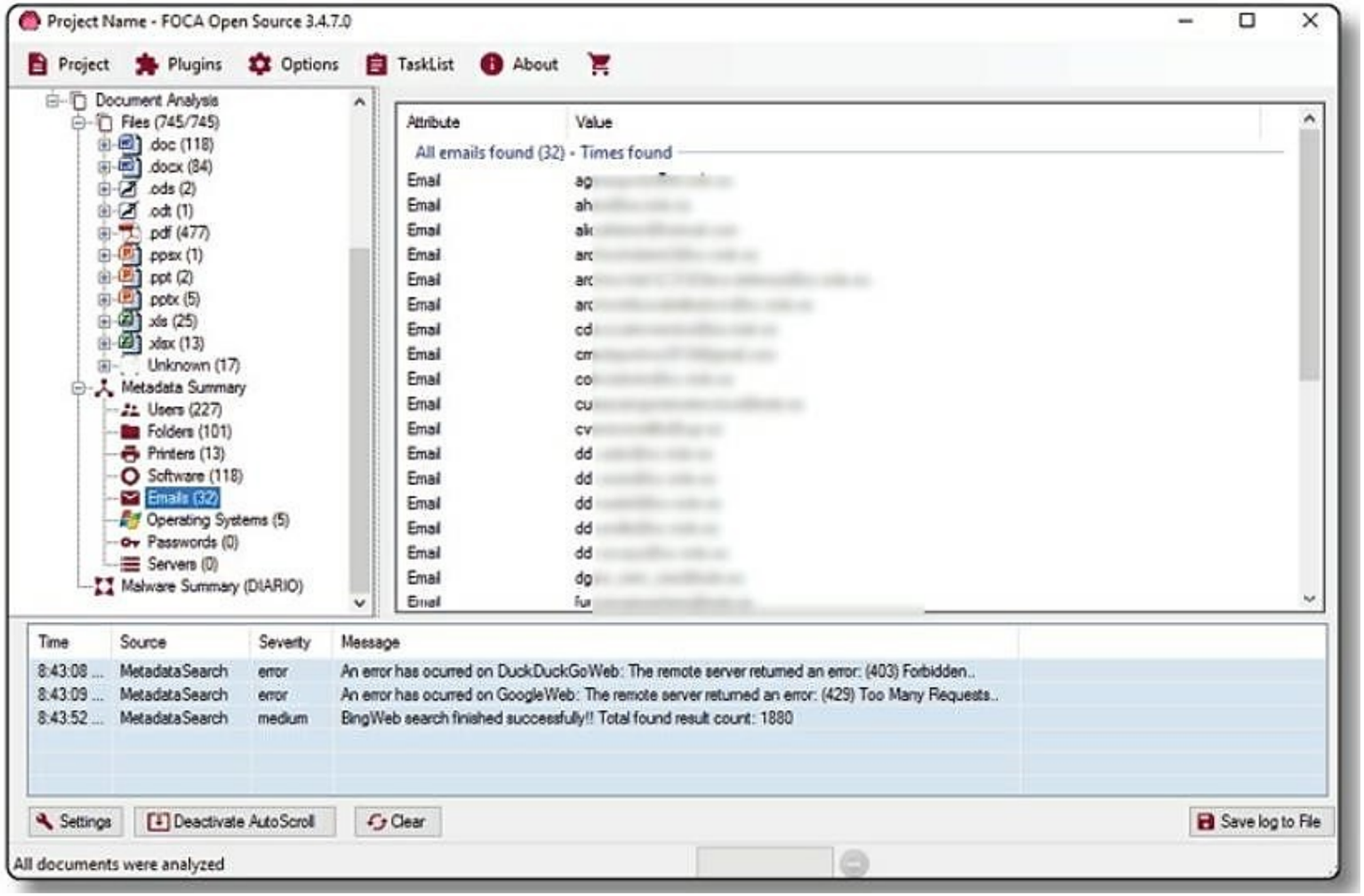
ANÁLISIS DE METADATOS

ANÁLISIS DE METADATOS CON FOCA

A MEDIDA QUE LA EXTRACCIÓN DE METADATOS ENCUENTRA INFORMACIÓN, VA AGRUPÁNDOLA EN LOS DIFERENTES NODOS DEL ÁRBOL DE LA IZQUIERDA. LA CANTIDAD DE INFORMACIÓN ENCONTRADA DEPENDERÁ DE LO CUIDADOSOS QUE HAYAN SIDO EN LA ORGANIZACIÓN A LA HORA DE HACER PÚBLICOS SUS ARCHIVOS.

ANÁLISIS DE METADATOS

ANÁLISIS DE METADATOS CON FOCA



CONTENIDOS

- INTRODUCCIÓN
- OSINT/RECONOCIMIENTO PASIVO
- RECONOCIMIENTO ACTIVO
- OTRAS HERRAMIENTAS DE RECONOCIMIENTO
- ANÁLISIS DE METADATOS

CONCLUSIONES

EL RECONOCIMIENTO SUELE SER UNA FASE QUE **PUEDE PARECER TEDIOSA**, POR LO QUE PUEDE CAER EN LA TENTACIÓN DE PASAR RÁPIDO POR ELLA PARA CENTRARSE EN LAS FASES APARENTEMENTE MÁS INTERESANTES.

SIN EMBARGO, **ESTA FASE RESULTA DE UNA IMPORTANCIA CRUCIAL**, PUESTO QUE UN RECONOCIMIENTO AL QUE NO SE HA DEDICADO EL TIEMPO SUFICIENTE PASARÁ POR ALTO INFORMACIÓN ESENCIAL PARA LAS FASES POSTERIORES.

SE DEBE TENER EN CUENTA QUE UN ATACANTE QUE REALMENTE ESTÉ INTERESADO EN UNA ORGANIZACIÓN CONCRETA DESTINARÁ TODOS SUS MEDIOS A CONOCER A LA MISMA Y A SU PERSONAL ANTES DE INICIAR EL ATAQUE.

CONCLUSIONES

AL FINALIZAR ESTA FASE SE DISPONDRÁ DE BASTANTE INFORMACIÓN Y UNA LISTA DE POTENCIALES OBJETIVOS, QUE DEBERÁ ESTAR PERFECTAMENTE DOCUMENTADA CON LA INFORMACIÓN DESCUBIERTA.

NO SE DEBE CENTRAR ÚNICAMENTE EN LOS ASPECTOS TÉCNICOS Y RELATIVOS AL HARDWARE Y AL SOFTWARE (*DIRECCIONES IP, NOMBRES DE EQUIPOS, SISTEMAS OPERATIVOS, PUERTOS CONOCIDOS, APLICACIONES Y VERSIONES, VULNERABILIDADES CONOCIDAS, CREDENCIALES ENCONTRADAS, ETC.*), SINO QUE SE DEBE **TENER DOCUMENTADA TAMBIÉN LA INFORMACIÓN RELATIVA A LAS PERSONAS E INCLUSO A LOS EDIFICIOS**, PUESTO QUE SEGÚN EL TIPO DE TEST DE PENETRACIÓN SERÁ NECESARIO TAMBIÉN ACTUAR SOBRE ESOS ASPECTOS.

ESTO ES TODO

Extraído de Hacking Ético. Luis Herrero Pérez. Editorial Ra-Ma