

Técnicas OSINT y *Exploiting*. FOCA, Maltego y Kali Linux.

RODRIGO IGLESIAS GORRÓN

SRCX08

RAÚL VELASCO CAMINERO

09/12/2015

A solid orange horizontal bar at the bottom of the slide.

Índice

1. **Introducción.**
2. Técnicas OSINT. Herramientas.
3. Metadatos.
4. FOCA y Maltego.
5. *Pestesting* e intrusión.
6. ¿Qué es Kali? Principales herramientas.
7. Ataques a redes *Wireless*.
8. Ataques a contraseñas.
9. Ataque *Man In The Middle* (MITM).
10. Vulnerabilidades Web y *SQL Injection*.
11. Algunos ejemplos con Kali.
12. Referencias.

Introducción

A la hora de vulnerar un sistema, hay diferentes medios para aproximarse:

- **OSINT:** *open-source intelligence*. Localizar todos los rastros que hayan podido dejarse en Internet en registros de direcciones IP, cuentas de redes sociales, correos electrónicos, cuentas de registro de servidores, **documentos... Información pública.**
- **Doxing:** encontrar la identidad real detrás de una ciber-identidad. Es decir, poder responder preguntas como quién controla una web o una cuenta de una red social.
- **Exploiting:** hackear páginas web, servidores, robo de datos, bases de datos, insertar troyanos... **Información privada.**

Índice

1. Introducción.
2. **Técnicas OSINT. Herramientas.**
3. Metadatos.
4. FOCA y Maltego.
5. *Pestesting* e intrusión.
6. ¿Qué es Kali? Principales herramientas.
7. Ataques a redes *Wireless*.
8. Ataques a contraseñas.
9. Ataque *Man In The Middle* (MITM).
10. Vulnerabilidades Web y *SQL Injection*.
11. Algunos ejemplos con Kali.
12. Referencias.

Técnicas OSINT

Técnicas que tratan de hallar información a partir de fuentes públicas. Muy relacionado con *Big Data*.

Algunos ejemplos:

- **Medios de comunicación:** periódicos, televisiones.
- **Sitios web:** contenido generado por **usuarios**, comunidades, foros, **redes sociales**.
- **Documentos:** informes, estadísticas y datos oficiales, presupuestos, comunicados, boletines oficiales, contratos.
- **Profesional y académica:** conferencias, tesis, artículos y trabajos de expertos.
- **Otros recursos:** registros de localización con Google Maps.

Herramientas OSINT

- **Spokeo:** página web que cuenta con una base de datos de gente estadounidense, incluyendo datos como nombre, dirección, email, fotos, ingresos, familia...
- <http://www.spokeo.com>

PERSON

Enrique J Iglesias

AGE

57






LOCATIONS

Dexter, NM
Roswell, NM
Fredonia, WI
Cleveland, WI

RELATIVES

Angelita Iglesias
Sonia Iglesias
Anna Iglesias
Rita Iglesias
Irma Iglesias

INCLUDES

SEE RESULTS NOW >

FUN FACTS

Rodrigo Iglesias

STATISTICS FOR ALL 29 PEOPLE NAMED RODRIGO IGLESIAS

\$139k

INCOME AVERAGE

Our wealth data indicates income average is \$139k.

79%

MARRIED

78.6% of these people are married, and 21.4% are single or divorced.

41 yrs

AVERAGE AGE

53% are in their 30s, while the average age is 41.

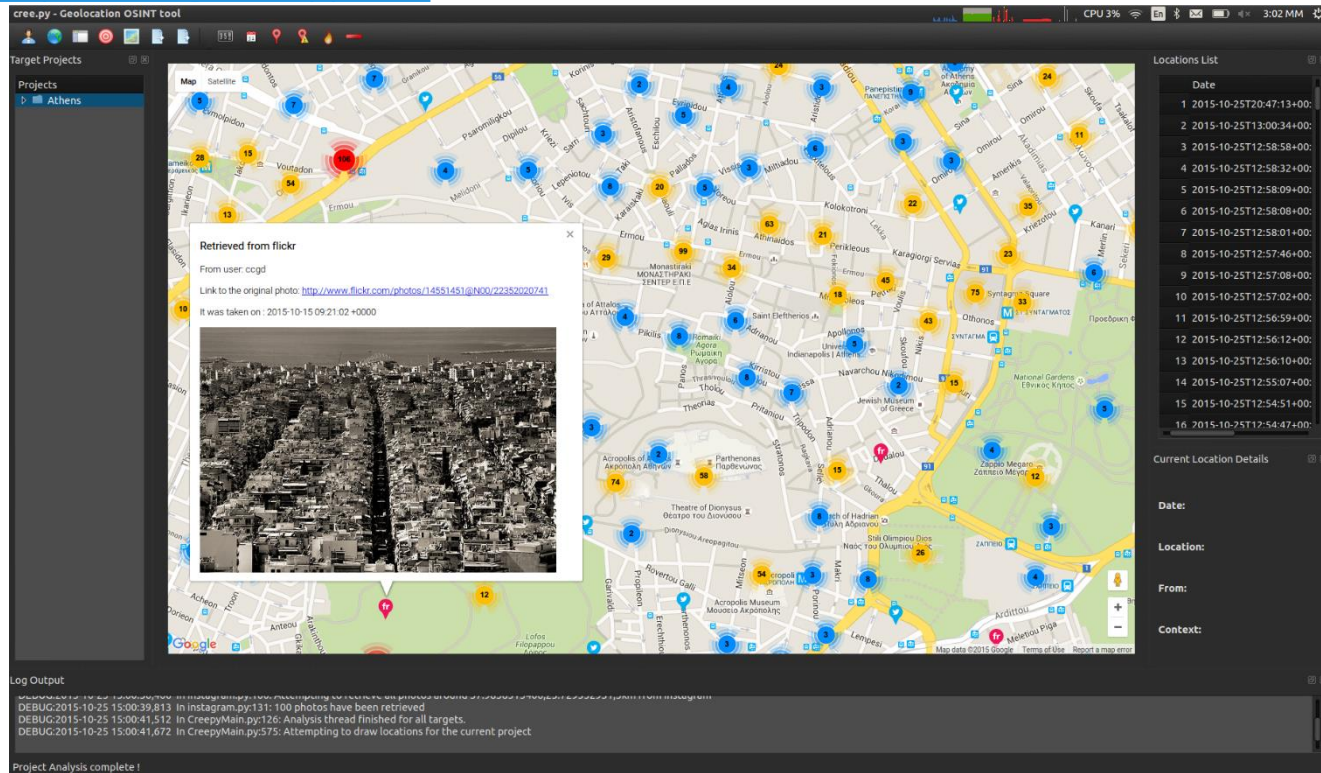
100%

HISPANIC

Our ethnicity data indicates the majority is Hispanic.

Herramientas OSINT

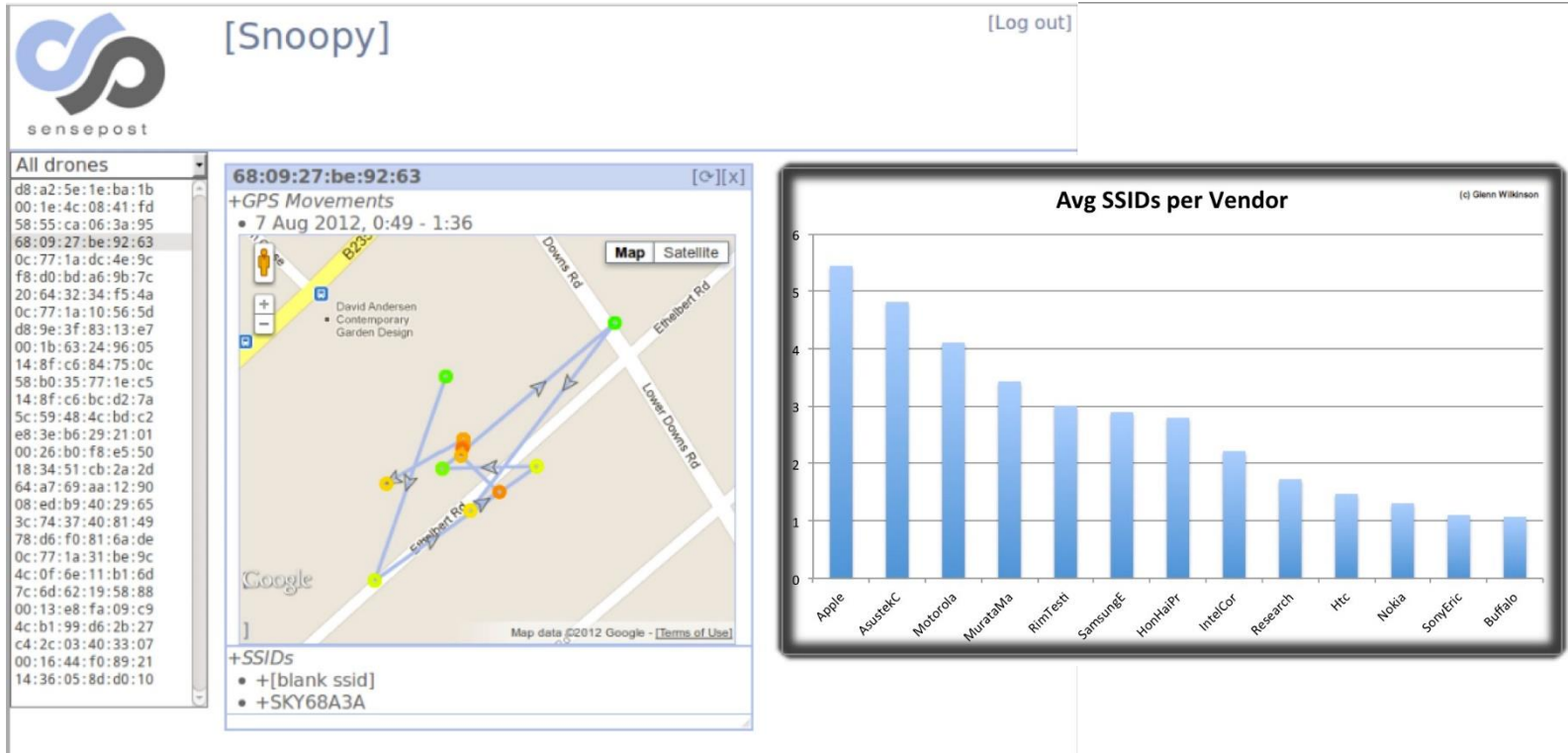
- **Creepy:** herramienta que nos ofrece información de geolocalización basada en la información pública de las redes sociales.
- <http://www.geocreepy.com/>



Herramientas OSINT

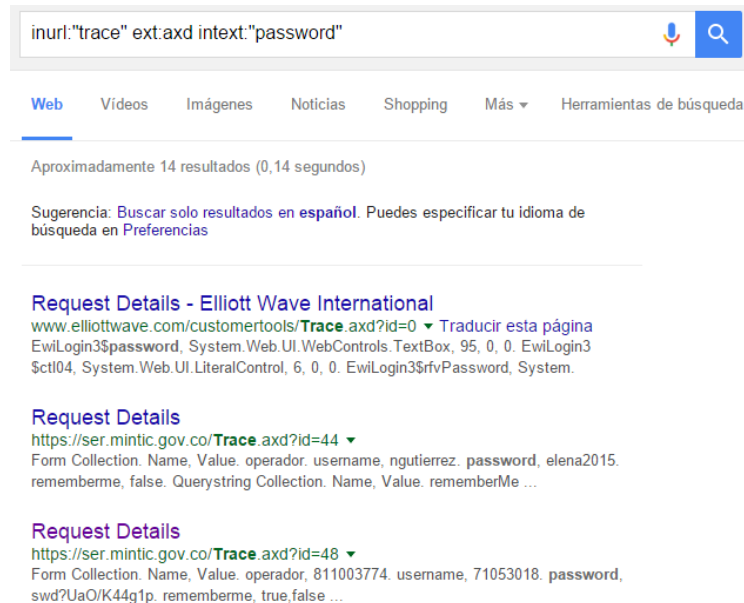
- **Snoopy**: herramienta de rastreo y análisis de perfiles. Se instala en un dispositivo y realiza diferentes usos de los paquetes que captura.
- 1. **Legal**: puede utilizarse para obtener estadísticas anónimas. Por ejemplo, podemos poner un dispositivo en cada puerta de un establecimiento para ver por dónde entra o sale más gente, y ampliar la seguridad en esa zona.
- 2. **Borderline**: puede analizarse el tipo de dispositivo (Android, iPhone...) que entra en una tienda, y hacer una campaña hacia este tipo de gente. Otro ejemplo sería que un ayuntamiento decidiese llenar la ciudad con dispositivos de este tipo para poder tener información de criminales a partir de su teléfono: Localización, patrones, rutinas...
- 3. **Ilegal**: podríamos acercarnos mucho a una persona en diferentes situaciones para analizar qué tipo de dispositivo usa e incluso capturar información enviada por este. Una vez hecho esto, podríamos preparar algún ataque específico para él (*Rogue AP, Botnet, anuncios...*)
- <https://www.sensepost.com/blog/2012/snoopy-a-distributed-tracking-and-profiling-framework/>

Herramientas OSINT



Herramientas OSINT

- **Google Hacking DB:** base de datos con diferentes búsquedas que se pueden hacer en Google para obtener información confidencial, como contraseñas, accesos a bases de datos...
- <https://www.exploit-db.com/google-hacking-database/>



Índice

1. Introducción.
2. Técnicas OSINT. Herramientas.
3. **Metadatos.**
4. FOCA y Maltego.
5. *Pestesting* e intrusión.
6. ¿Qué es Kali? Principales herramientas.
7. Ataques a redes *Wireless*.
8. Ataques a contraseñas.
9. Ataque *Man In The Middle* (MITM).
10. Vulnerabilidades Web y *SQL Injection*.
11. Algunos ejemplos con Kali.
12. Referencias.

Metadatos

- Conjunto de datos que contienen información relativa a un documento o un fichero concreto.
 - Procedencia, datos del autor, fecha de creación y modificación, software usado en la redacción...
- En fotografía, el Exif guardado en el formato JPEG o TIFF nos da información sobre la marca y modelo de la cámara, profundidad de color, resolución, o incluso coordenadas GPS desde donde se realizó dicha fotografía.
- Muy útiles para catalogar información y facilitar la localización, optimizando las búsquedas.
- **Riesgo si no son gestionados de manera adecuada.**



Measurement Flare - 0.999%
Measurement Illuminant - D65
DCTEncode Version - 100
APP14 Flags0 - [14], Encoded with Blend=1 downsampling
APP14 Flags1 - (none)
Color Transform - YCbCr
Camera ID - 72157624637608383

Keywords - Fotos Terminadas
Date Created - 2015:08:22
Time Created - 09:54:19
Digital Creation Date - 2015:08:22
Digital Creation Time - 09:54:19
City - Sydney
Country- Primary Location Name - Australia
Viewing Cond Illuminant - 19.6445 20.3718 16.8089
Viewing Cond Surround - 3.92889 4.07439 3.36179
Viewing Conditions Illuminant Type - D50
Measurement Observer - CIE 1931

Metadatos – Casos y ejemplos

- En 2003, un documento fue publicado por el gobierno británico (Bajo el gobierno de Toni Blair), que contenía información sobre Irak, Saddam Hussein y armas de destrucción masiva para justificar su entrada en la guerra de Irak.
- Estaba en formato **Word**, por lo que contenía metadatos de Office, como el *log* de las revisiones y últimos cambios. Se presentó el documento como que no había sido editado, mientras que los metadatos dieron información de que se había editado, copiado, etcétera.
- En 2011, el programa electoral del PP lo publica un becario de las FAES.
- Se analizó el PDF en el que habían quedado rastro de metadatos, y se vio que se había generado con **Word 2007**, que lo había hecho un tal Javier Vidueria, y que el documento base re-aprovechado se llamaba “Viaje de Javier Arenas a San Sebastián”.
- Piratería de software en una empresa.
- Cuanto hay mucha versión de software, se puede sospechar que se está recurriendo a la piratería como medio de obtención. Ejemplo: SGAE.

Software	Versiones	Usuarios	Documentos
QuarkXPress	1.0 - 4.01 - 5 - 6.5 - 8.0 - 8.01 - 8.02	Carlos Caso - joseluis - Sergio - Pipo - El estudio - iMAC - G5 Jose	52
FreeHand	MX - 1.5	Olga - Ordenador G5 - Pixel Pan	4
Ghostsript	7.05 - 8.15 - 8.54 - 8.61	fernandod - funsmg - recepcion - barbag - Richard	12
PDFCreator	0.9.3 - 0.9.5	barbag - Richard	9
Adobe Acrobat	7.0 - 8.0 Paper Capture Plug-in - 8.1		5
Adobe Reader	8.1		1
Adobe Acrobat PDF Writer	3.0.1 para Power Macintosh - 4.0 - 4.05	iMAC - Pipo - EL ESTUDIO - richard - frosales	41
Adobe Distilier	3.02 - 4.0 - 4.05 - 5.0 - 6.0 - 7.0 - 7.0.5 - 8.0 - 8.1 - 8.2	SGAE - ASEIAF - Benjamín Yópez (yepes) - Pipo - G4 - Albert Sánchez Graells - FUNDACION - fernandod - Juani - Pixel Pan - José Luis - G5 José - ACMMOL - Susana Tello - Olga - markgr - Carlos Caso - Ordenador G5 - Paco Rosales - FUNARF - COMMGR - Sergio - COMCRG - commgr - funcnj - seccpg	91
MS Office	95 - 97 - 2000 - XP - 2003 - 2007		85
Solid Converter PDF	v4		18
Snagit by TechSmith		Snagit user	1

Metadatos – Casos y ejemplos

- Uso de la geolocalización en una foto para detener contrabandistas:
 - En el caso de la foto inferior, se supo que la fotografía a un alijo de drogas estaba hecho con un iPhone, y podíamos ver exactamente las coordenadas GPS de dónde se hizo:



- Otros ejemplos: <http://www.elladodelmal.com/2012/04/analisis-forense-de-metadatos-15.html>

Índice

1. Introducción.
2. Técnicas OSINT. Herramientas.
3. Metadatos.
4. **FOCA y Maltego.**
5. *Pestesting* e intrusión.
6. ¿Qué es Kali? Principales herramientas.
7. Ataques a redes *Wireless*.
8. Ataques a contraseñas.
9. Ataque *Man In The Middle* (MITM).
10. Vulnerabilidades Web y *SQL Injection*.
11. Algunos ejemplos con Kali.
12. Referencias.

Análisis de metadatos -



- Tras *OOMetaExtractor*, herramienta utilizada para extraer los metadatos de ficheros OpenOffice, *ElevenPaths* desarrolló una nueva herramienta de análisis de metadatos y huella digital: FOCA (*Fingerprinting Organizations with Collected Archives*).
- Sirve para encontrar metadatos e información oculta en los documentos que examina. Estos pueden estar en páginas web, y la herramienta se encarga ella misma de descargarlos y analizarlos.
- Es capaz de analizar documentos muy variados, desde archivos de Microsoft Office, Open Office o PDF, hasta ficheros de Adobe InDesign o Adobe Photoshop.
- Para la búsqueda de documentos, se utilizan 3 buscadores, consiguiendo un gran número de documentos. Además, se pueden añadir documentos locales.

Análisis de metadatos -



- Además, FOCA incluye diferentes módulos para descubrir servidores y automatizar el proceso de búsqueda de estos. Las técnicas entrelazadas recursivamente usadas son:
 - **Web Search:** se busca nombres de hosts y dominios a través de la búsqueda de URLs asociadas al dominio principal, y a su vez cada link es analizado para extraer de él nuevos nombres de hosts y nombres de dominio.
 - **DNS Search:** a cada dominio se le consulta cuales 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 interno de la organización para obtener la dirección IP asociada.
 - **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, se lanzará un proceso de búsqueda de nombres de dominio asociados a esa dirección IP.
 - **Common names:** ataque de diccionario al DNS, con nombres de *host* comunes.
 - **DNS Prediction:** usado para aquellos entornos en los que se siga un patrón a la hora de asignar nombres de dominio.

Análisis de la red con



Select search type

☒ WebSearch ☒ Also, improve results with Robtex

Using a web searcher like Google or Bing the program searches links pointing to the domain site to identify new subdomains.

Google Web limitations

- Max 1000 results for each search
- Max 32 words in a search string

☒ Google Web

☐ Google API

☐ Bing Web

☐ Bing API

☒ DNS Search

DNS Search performs queries to DNS Servers searching for well-known records. The following queries will be done:

NS, SOA, Primary, Master, MX, SPF, Domainkeys Records, DKIM Records, SRV Records for VoiP, IM and Active Directory, Kerberos, LDAP and Web Proxy Autodiscovery.

☒ ZoneTransfer

☒ Dictionary Search

The program uses a common DNS names list to find new subdomains. This list is the same used by Fierce tool.

☒ IP Bing

Bing allows search links located in a particular IP address. This functionality can be used to find domains that share IP Address.

☒ Bing Web

☐ Bing API

Bing Web limitations

- Max 1000 results for each search
- Max 49 words in a search string

☒ PTR Scan

When the program discovers an IP address, it can make a reverse resolution over the entire IP range in DNS internal. Just reserve resolution contained in the domain will be added.

It's very slow.

☒ Shodan & Robtex

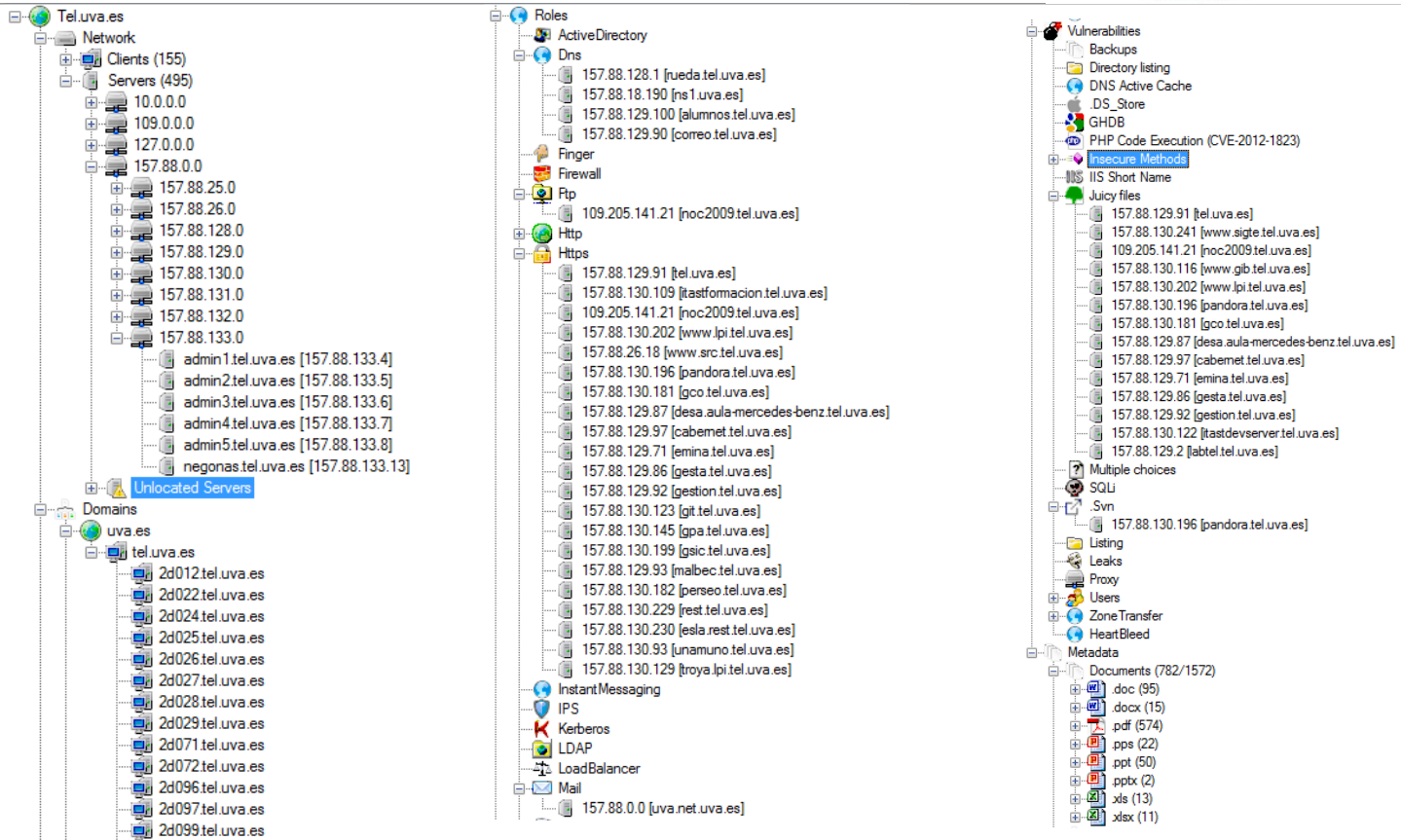
Activating this option, network algorithm will search all IP addresses belonging to all Netranges in Project to Shodan. It will send a query for each IP address and will retrieve software information and new domain names.

Current search: None

Pasos para realizar el análisis

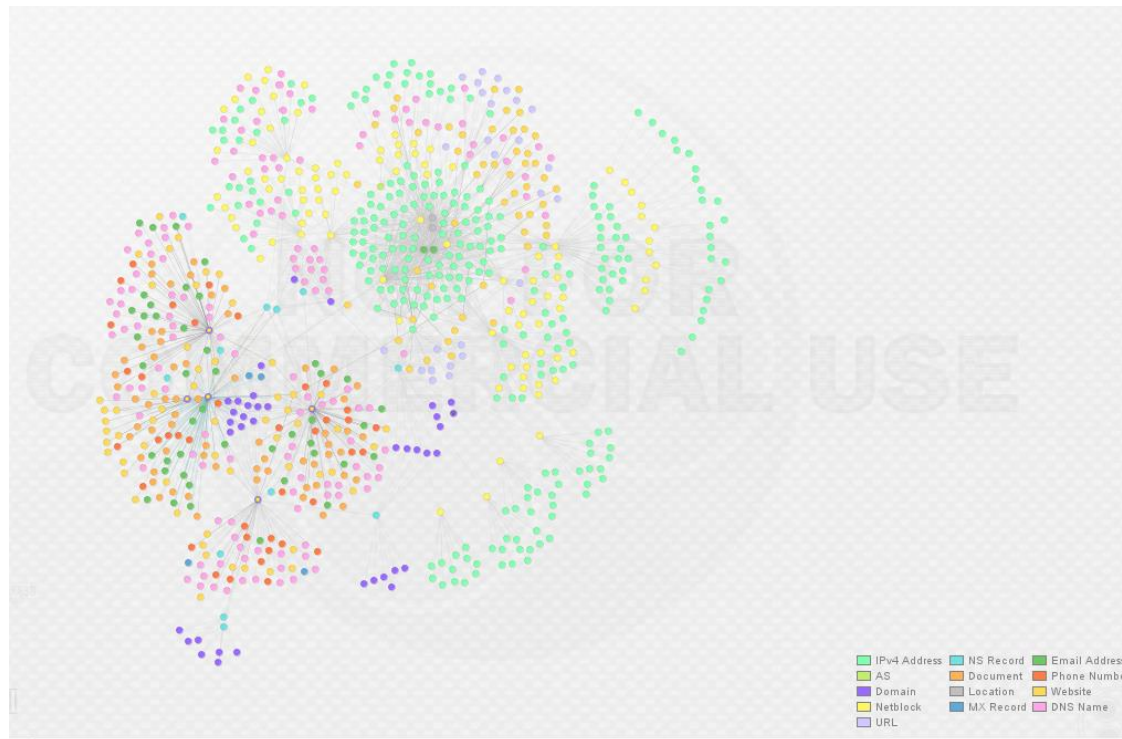
1. Realizar un análisis exhaustivo de la red.
2. Descargar todos los ficheros posibles.
3. Extraer metadatos.
4. Analizar metadatos.
5. Detectar posibles vulnerabilidades u objetivos.
6. Corregir vulnerabilidades.

Análisis de tel.uva.es con



Análisis alternativos - Maltego

- Herramienta muy potente de análisis de redes y metadatos.
- Funcionalidades similares a FOCA, limitadas en la versión gratuita y extendidas en la versión de pago.



Índice

1. Introducción.
2. Técnicas OSINT. Herramientas.
3. Metadatos.
4. FOCA y Maltego.
5. ***Pestesting* e intrusión.**
6. ¿Qué es Kali? Principales herramientas.
7. Ataques a redes *Wireless*.
8. Ataques a contraseñas.
9. Ataque *Man In The Middle* (MITM).
10. Vulnerabilidades Web y *SQL Injection*.
11. Algunos ejemplos con Kali.
12. Referencias.

Pestesting e intrusión

- **Pentesting:** evaluar los niveles de seguridad de un sistema informático o red mediante la simulación.
- Pasos para realizar un test de intrusión:
 - Reglas del juego: alcance y términos del test de intrusión.
 - Recolección de información.
 - Análisis de las vulnerabilidades.
 - Explotación de las vulnerabilidades.
 - Post-explotación del sistema.
 - Generación de informes.

Índice

1. Introducción.
2. Técnicas OSINT. Herramientas.
3. Metadatos.
4. FOCA y Maltego.
5. *Pestesting* e intrusión.
6. **¿Qué es Kali? Principales herramientas.**
7. Ataques a redes *Wireless*.
8. Ataques a contraseñas.
9. Ataque *Man In The Middle* (MITM).
10. Vulnerabilidades Web y *SQL Injection*.
11. Algunos ejemplos con Kali.
12. Referencias.

¿Qué es Kali?



- Sucesor de la herramienta *BackTrack*.
- Utilizada para realizar auditorías tanto internas como externas.
- Principales usos de Kali:
 - Análisis de vulnerabilidades.
 - Ataques a contraseñas.
 - *Exploits*.
 - Vulnerabilidades Web.
 - Ataques a redes inalámbricas.
 - Análisis forense.
 - Ataque a redes: envenenamiento de redes y *Man In The Middle*.

Principales herramientas



Principales herramientas

- **Aircrack-ng:** se trata de un conjunto de software de seguridad inalámbrica que incluye un analizador de paquetes de redes, un *crackeador* de redes WEP y WPA/WPA2 y otro conjunto de herramientas de auditoría inalámbrica.
- **Burpsuite:** es una herramienta escrita íntegramente en Java que permite realizar test de intrusión en aplicaciones web, permitiendo combinar técnicas manuales y automáticas para analizar, detectar, atacar y explotar aplicaciones web.
- **Hydra:** es un *crackeador* de contraseñas multihilo por fuerza bruta en base a diccionarios. Puede crackear prácticamente cualquier servicio (Telnet, POP3, SMTP, IMAP, SMB, SSHv1 y SSHv2...) usando una conexión directa o *proxys*, con o sin SSL.
- **John:** hace referencia a *John The Ripper*, una herramienta muy popular que permite comprobar que las contraseñas de los usuarios son lo suficientemente seguras.
 - Aplica fuerza bruta para descifrar contraseñas, siendo capaz de romper varios algoritmos de cifrado como DES y SHA-1 entre otros.

Principales herramientas

- **Maltego:** es una aplicación de minería y recolección de información utilizada durante la fase de *Data Gathering*, proceso por el cual se trata de obtener el mayor número de información posible sobre un objetivo. Esta información se muestra de forma gráfica. Es una herramienta muy potente, llena de opciones que pueden ser muy útiles para investigar empresas, sitios, personas...
- **Metasploit Framework:** es la herramienta más útil y potente que ofrece Kali. Se trata de una herramienta para desarrollar y ejecutar *exploits* contra un equipo remoto. Sin embargo esta herramienta dispone de gran cantidad de funcionalidades las cuales son muy utilizadas por los auditores de seguridad.
- **NMAP:** programa por consola de comandos que sirve para efectuar un rastreo de puertos. Utilidades:
 - Identifica puertos abiertos y servicios que se están ejecutando en una máquina.
 - Características del hardware de red.
 - Identifica equipos en una red.
 - Determina el sistema operativo y versión de una máquina.

Principales herramientas

- **SQLMap:** es una herramienta muy útil en los test de intrusión que automatiza el proceso de detección y explotación de fallos de tipo *SQL Injection* y, de esta forma, obtener toda la información contenida dentro de los servidores de bases de datos.
- **Wireshark:** esta aplicación es un analizador de paquetes que permite examinar datos de una red viva o de un archivo capturado salvado en el disco. Analiza a información capturada, a través de los detalles y sumarios por cada paquete. Es una herramienta profesional imprescindible para los auditores informáticos.
- **Zaproxy:** es una herramienta fácil de usar y que forma parte de las aplicaciones de uso habitual en el proceso de *pentesting* para encontrar vulnerabilidades en aplicaciones web.

Índice

1. Introducción.
2. Técnicas OSINT. Herramientas.
3. Metadatos.
4. FOCA y Maltego.
5. *Pestesting* e intrusión.
6. ¿Qué es Kali? Principales herramientas.
7. **Ataques a redes *Wireless*.**
8. Ataques a contraseñas.
9. Ataque *Man In The Middle* (MITM).
10. Vulnerabilidades Web y *SQL Injection*.
11. Algunos ejemplos con Kali.
12. Referencias.

Ataques a redes *Wireless*

- Kali dispone de numerosas herramientas para realizar ataques a redes inalámbricas.
- No solo existen ataques a redes WLAN (más normales):
 - Ataques a redes *Bluetooth*: *BTScanner*.
 - Ataques a la tecnología RFID:
 - **Tres categorías:** RFIDiot ACG, RFIDiot FROSCH y RFIDiot PSCSC.
 - Ataques a la tecnología NFC: *Mfcuk*.
- Nosotros nos vamos a centrar en el ataque a redes WLAN.

Ataques a redes *Wireless*

- La *suite* de herramientas *air* proporciona todo lo necesario para llevar a cabo auditorías a redes *Wireless* en Kali.
- Para realizar este tipo de ataques lo primero es poder poner la tarjeta de red en modo monitor (capturar todo el tráfico que hay en el aire).
 - Herramienta *airmon-ng* (`airmon-ng start <interfaz wlan>`).
- También se necesita un Sniffer de tráfico.
 - Herramienta *airodump-ng*.
- Herramientas interesantes que proporciona esta *suite*:
 - **Airbase-ng**: habilitar el adaptador inalámbrico como si fuese un punto de acceso normal. De este modo se podría engañar a un usuario para que se conectase a un punto de acceso falso.
 - **Aireplay-ng**: permite realizar operaciones o ataques sobre los puntos de acceso y clientes asociados a estos. Herramienta que se utilizará posteriormente.
 - **Aircrack-ng**: permite realizar ataques de fuerza bruta, diccionario o estadísticos a capturas de tráfico *Wireless*. En función del tipo de cifrado de la red que se quiera crackear, se realizará un tipo de ataque u otro.

Ataques a redes *Wireless*

Ataque	Descripción
-0 Desautenticación	Este ataque permite al atacante desautenticar a uno o varios clientes de un punto de acceso.
-1 Autenticación falsa	Este ataque permite asociarse a un punto de acceso, siempre y cuando el AP lo permita.
-2 Selección interactiva	Este ataque permite elegir un paquete y reenviarlo. Puede dar mejores resultados que el ataque 3.
-3 Reinyección de paquetes	Este ataque permite capturar un paquete ARP y reinyectarlo contra el AP, generando gran volumen de tráfico.
-4 Ataque ChopChop	Este ataque no recupera la clave WEP en sí misma, sino que revela meramente el texto plano.
-5 Fragmentación	Este ataque intenta generar una <i>keystream</i> .
-6 Caffè-Latte	Los clientes asociados serán quienes aporten más IVs para <i>crackear</i> la red.

Tabla 06.02: Resumen y descripción de los tipos de ataques en *aireplay*.

Tipos de ataque con la herramienta *aireplay-ng*.

Índice

1. Introducción.
2. Técnicas OSINT. Herramientas.
3. Metadatos.
4. FOCA y Maltego.
5. *Pestesting* e intrusión.
6. ¿Qué es Kali? Principales herramientas.
7. Ataques a redes *Wireless*.
8. **Ataques a contraseñas.**
9. Ataque *Man In The Middle* (MITM).
10. Vulnerabilidades Web y *SQL Injection*.
11. Algunos ejemplos con Kali.
12. Referencias.

Ataques a contraseñas

- Los ataques a contraseñas o *password cracking* no son más que todas aquellas técnicas orientadas a romper o descifrar contraseñas utilizadas para proteger sistemas, aplicaciones o documentos.
- Todo mecanismo de autenticación por contraseñas lo que realiza es una comparación del *hash* de las contraseñas establecidas para protegerlos, con lo generado por la contraseña utilizada.
- *Hash* más utilizados:
 - **MD5**: problema de las colisiones. Dos entradas distintas a una función de Hash da la misma salida.
 - **SHA**: elimina el problema de las colisiones a medida que se aumenta la representación hexadecimal.
 - **LM**: primer *Hash* de los sistemas Windows. Obsoleto.
 - **NTLM**: sucesor de LM. Proceso costoso en tiempo al realizar un ataque de *hash*.

Ataques a contraseñas

- La imagen inferior muestra como se almacenan las contraseñas en un sistema GNU/Linux.
- Contenido de cada línea:
 1. Nombre del usuario.
 2. Algoritmo de resumen utilizado.
 3. El *salt* de la contraseña.
 4. La contraseña cifrada.
 5. Días transcurridos desde el 1 de Enero de 1970 hasta el día en que la contraseña fue cambiada por primera vez.
 6. Número mínimo de días para poder cambiar la contraseña.
 7. Número máximo de días que la contraseña es válida.
 8. Número de días antes de que expire la contraseña.
 9. Número de días para que la cuenta sea deshabilitada desde la caducidad de la contraseña.
 10. Número de días desde el 1 de Enero de 1970 para que la cuenta sea deshabilitada.

```
Ricardo:$6$ky2RlnaX$04lNuS.7w2Q6mougB.3j8ec3t0xKmh2ENUY.Gxe2K/STEbLJQHZNy2z48i4jrgyX4V7Ce7rvHlpFaYNSILmK1:15810:0:99999:7:::
```

Imagen 03.05: Almacenamiento de *hash* en sistemas GNU/LINUX.

Ataques a contraseñas

Métodos de ataque:

- **Ataques de fuerza bruta:** consiste en probar todas las combinaciones posibles hasta encontrar aquella que permita el acceso, usando distintos patrones (números, caracteres, mayúsculas...).
- **Ataques de diccionario:** son muy similares a los “ataques de fuerza bruta”. La diferencia radica en que las combinaciones suelen ser palabras de un diccionario.
- **Ataques de *Rainbow Table*:** son ataques basados en una tabla que almacena una relación de pares de palabras en texto plano (palabra inicial-palabra final). La relación que vincula estas palabras es que ambas son utilizadas en la función de resumen y reducción que representa la *Rainbow Table*. Proceso de creación:
 - Sobre la palabra inicial se aplica un algoritmo de resumen y se obtiene el *hash* de esa palabras.
 - Sobre ese *hash* se aplica un algoritmo de reducción y se obtiene la nueva palabra en texto plano.

Ataques a contraseñas

Tipos de ataque:

- Ataques con conexión.
- Ataques sin conexión.
- **Ataques con conexión:** en este tipo de ataques es necesario que el dispositivo o servicio se encuentre en línea, para de esta forma poder establecer la comunicación con el mismo, en la que se intentan averiguar credenciales válidas estudiando el tipo de respuestas obtenidas por cada una de las peticiones que se le realizan.
- Una herramienta muy conocida: *findmyhash*.
- Comando:
findmyhash {tipo de hash} {parámetro (-h, -g, -f) {hash o dirección del fichero con hashes}}

Ataques a contraseñas

- Herramienta Hydra

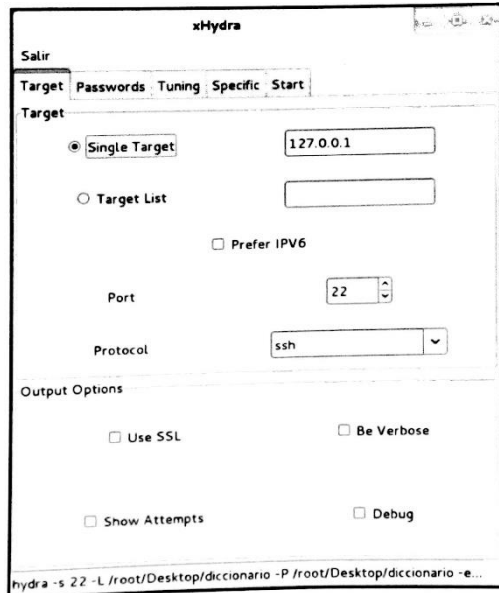


Imagen 03.10: Interfaz visual de Hydra.

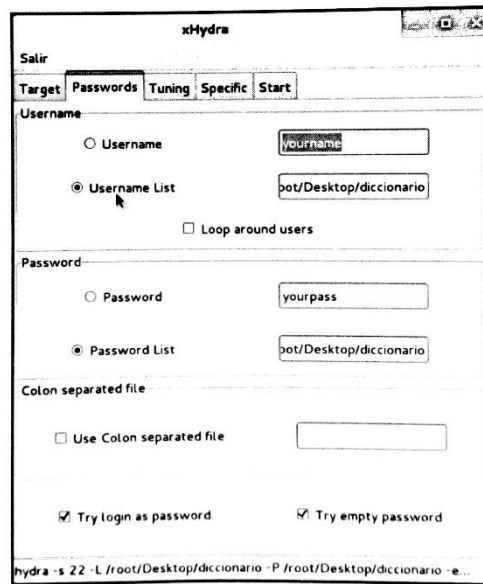


Imagen 03.11: Credenciales en Hydra.

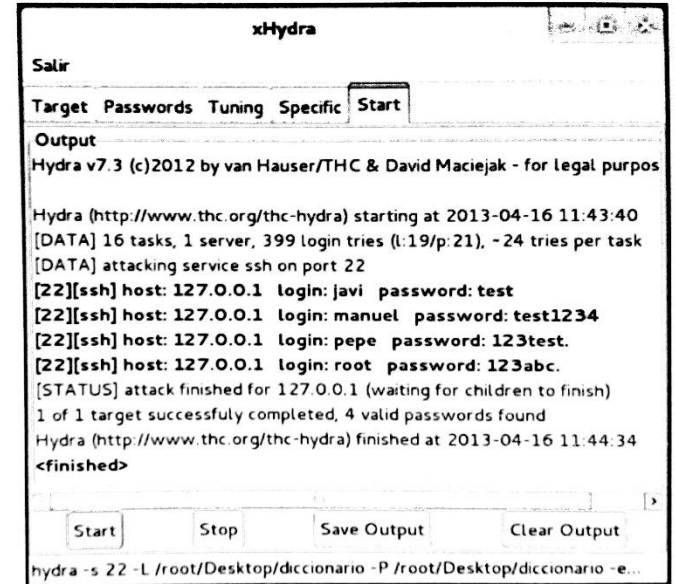


Imagen 03.12: Resultado del estudio con Hydra.

Ataques a contraseñas

- **Ataques sin conexión:** en este tipo de ataques, resulta necesario establecer contacto con el dispositivo o servicio (generalmente una sola ocasión), en la que se establece una comunicación cifrada o se consigue un hash que puede ser almacenado de manera local para posteriormente ser estudiado. Todo se realiza de manera local.
- Herramientas útiles:
 - **Hash-identifier:** identifica un hash sin saber el tipo de hash que se posee.
 - **John the ripper:** herramienta para realizar ataques de fuerza bruta y de diccionario. Modos de ataque:
 - **Single crack:** se prueban contraseñas similares al usuario (*john -single /etc/shadow*)
 - **Wordlist:** ataque por diccionarios (*john -wordlist={fichero con el diccionario} {fichero a estudiar}*).
 - **Incremental:** ataque por fuerza bruta, probando todas las posibilidades existentes (*john -incremental {fichero a estudiar}*).
 - **External:** se puede definir un código propio para generar las contraseñas de prueba.

Índice

1. Introducción.
2. Técnicas OSINT. Herramientas.
3. Metadatos.
4. FOCA y Maltego.
5. *Pestesting* e intrusión.
6. ¿Qué es Kali? Principales herramientas.
7. Ataques a redes *Wireless*.
8. Ataques a contraseñas.
9. **Ataque *Man In The Middle* (MITM).**
10. Vulnerabilidades Web y *SQL Injection*.
11. Algunos ejemplos con Kali.
12. Referencias.

Ataque Man In The Middle (MITM)

- La mayoría asocia la técnica de *Man In the Middle (MITM)* con el *ARP Spoofing*. MITM no es solo este tipo de técnica, sino cualquiera de ellas que permita colocar el rol del atacante en el medio de una comunicación, es decir, interceptar la información entre un emisor y un receptor.
- Consiste en que la información de la víctima circule a través de la máquina del atacante. Con esto se logra que el atacante pueda analizar y procesar el tráfico.
- **ARP Spoofing:** para llevar a cabo esta técnica, el atacante y la víctima deben encontrarse en la misma red y utilizar el protocolo IPv4 para el intercambio de datos (LAN cableada o inalámbrica).

Ataque Man In The Middle (MITM)

- Man In The Middle + ARP Spoofing.
- Pasos para realizar este ataque:
 - Envenenar la tabla ARP de la víctima (*arp spoof -i interfaz red -t IP victima IP Router*).
 - Nuestra máquina como router (*echo 1 > /proc/sys/net/ipv4/ip_forward*).
 - La herramienta *driftnet* muestra las imágenes que la víctima esta visualizando.

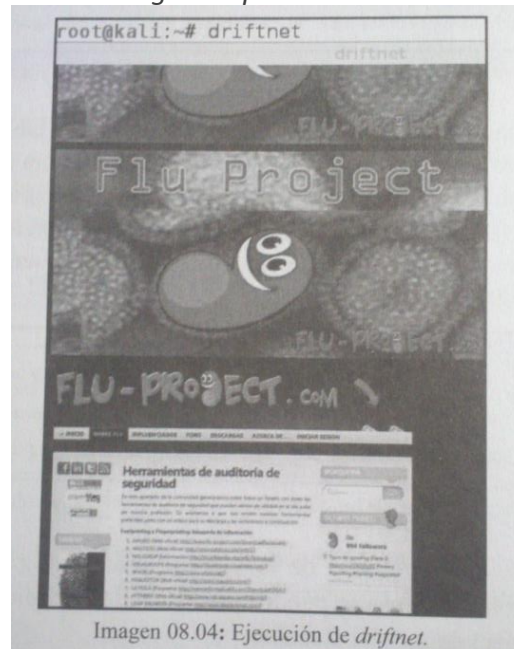


Imagen 08.04: Ejecución de *driftnet*.

Índice

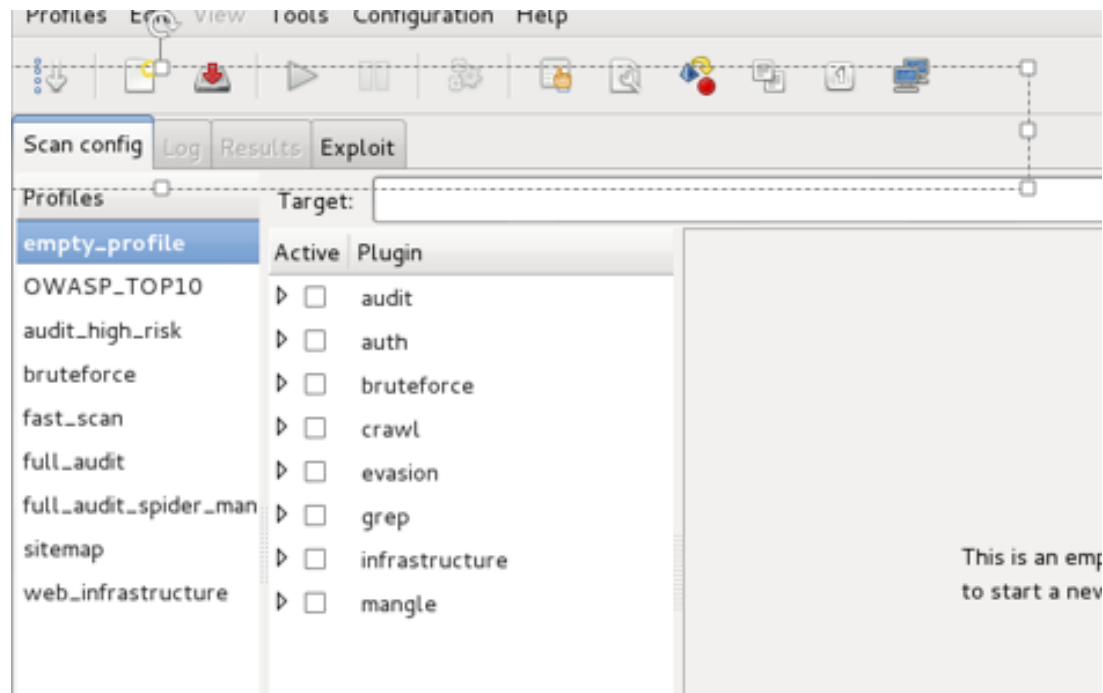
1. Introducción.
2. Técnicas OSINT. Herramientas.
3. Metadatos.
4. FOCA y Maltego.
5. *Pestesting* e intrusión.
6. ¿Qué es Kali? Principales herramientas.
7. Ataques a redes *Wireless*.
8. Ataques a contraseñas.
9. Ataque *Man In The Middle* (MITM).
10. **Vulnerabilidades Web y *SQL Injection*.**
11. Algunos ejemplos con Kali.
12. Referencias.

Vulnerabilidades Web y *SQL Injection*

- En Kali, existen multitud de herramientas para comprobar si una página Web es vulnerable a algún tipo de ataque como puede ser *SQL Injection*.
- ***SQL Injection***: afectan a todas las aplicaciones Web que rescatan información de bases de datos mediante parámetros mal filtrados.
- Para llevar a cabo este tipo de ataques, es conocida la inclusión de una comilla simple en los parámetros a recoger, con el objetivo de forzar un error de sintaxis SQL, y provocar así que la página devuelva algún tipo de error en pantalla.
- Una herramienta muy interesante es *w3af*, con la que es posible explotar vulnerabilidades Web.

Vulnerabilidades Web y *SQL Injection*

- Herramienta w3af:



Índice

1. Introducción.
2. Técnicas OSINT. Herramientas.
3. Metadatos.
4. FOCA y Maltego.
5. *Pestesting* e intrusión.
6. ¿Qué es Kali? Principales herramientas.
7. Ataques a redes *Wireless*.
8. Ataques a contraseñas.
9. Ataque *Man In The Middle* (MITM).
10. Vulnerabilidades Web y *SQL Injection*.
11. **Algunos ejemplos con Kali.**
12. Referencias.

Algunos ejemplos con Kali

- Ataque *Man In The Middle*.
- Ataque a contraseñas con conexión (*findmyhash*).
- Ataque a contraseñas sin conexión (*john*).
- Herramienta w3af.

Índice

1. Introducción.
2. Técnicas OSINT. Herramientas.
3. Metadatos.
4. FOCA y Maltego.
5. *Pestesting* e intrusión.
6. ¿Qué es Kali? Principales herramientas.
7. Ataques a redes *Wireless*.
8. Ataques a contraseñas.
9. Ataque *Man In The Middle* (MITM).
10. Vulnerabilidades Web y *SQL Injection*.
11. Algunos ejemplos con Kali.
12. **Referencias.**

Referencias

- Página oficial FOCA, <https://www.elevenpaths.com/es/labstools/foca-2/index.html>. Último acceso 08/12/2015.
- “*Pentesting con FOCA*”, Chema Alonso, 0xWORD, España, 2013.
- Página oficial Kali Linux, <https://www.kali.org/kali-linux-documentation/>. Último acceso: 08/12/2015.
- “*Pentesting con Kali*”, Pablo González Pérez, Germán Sánchez Garcés, Jose Miguel Soriano de la Cámara, 0xWORD, España, 2013.
- “*Web Penetration Testing with Kali Linux*”, Joseph Muniz, Aamir Lakhani, PACKT publishing, Birmingham, 2013.

Técnicas OSINT y *Exploiting*. FOCA, Maltego y Kali Linux.

RODRIGO IGLESIAS GORRÓN

SRCX08

RAÚL VELASCO CAMINERO

09/12/2015

A solid orange horizontal bar at the bottom of the slide.