**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 04 Enumeration**

**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**

Con el desarrollo de tecnologías y aplicaciones de red, los ataques a la red aumentan considerablemente tanto en número como en gravedad. Los atacantes siempre buscan vulnerabilidades de servicio: vulnerabilidades de la aplicación en una red o servidores. Si los atacantes encuentran una falla o un resquicio en un servicio que se ejecuta en Internet, lo usarán de inmediato para comprometer todo el sistema y otros datos encontrados y, por lo tanto, para comprometer otros sistemas de red. Del mismo modo, si encuentran una estación de trabajo con privilegios administrativos con fallas en las aplicaciones de esa estación de trabajo, pueden ejecutar un código arbitrario o implantar virus para intensificar el daño a la red.

Como técnica clave en el dominio de seguridad de la red, un sistema de detección de intrusión (IDS) desempeña un papel vital en la detección de diversos tipos de ataques y la protección de las redes. Por lo tanto, como administrador, debe asegurarse de que los servicios no se ejecuten como usuario root, y debe tener cuidado con los parches y las actualizaciones de las aplicaciones de proveedores u organizaciones de seguridad como CERT y CVE. Se pueden implementar protecciones para que el software de cliente de correo electrónico no abra o ejecute automáticamente los archivos adjuntos.

En el primer paso de una evaluación de seguridad y pruebas de penetración de su organización, ha recopilado información de código abierto sobre su organización. Ahora, necesita realizar la enumeración en la red. En este paso, debe explorar más la red de destino para recopilar más detalles, como máquinas de red, usuarios y carpetas compartidas. Como experto hacker ético y probador de penetración, debe saber cómo enumerar redes de destino y extraer nombres, recursos de red y servicios, utilizando diversas técnicas de enumeración.

**Objetivos de Laboratorio**

El objetivo de este laboratorio es proporcionar conocimiento experto sobre la enumeración de redes y otras responsabilidades que incluyen:

- Nombres de Usuarios y de Grupos

- Lista de computadoras, sus sistemas operativos y puertos

- Nombre de maquinas, recursos de red, y servicios

- Listas de recursos compartidos en hosts individuales en la red

- Politicas y contrasñas

**Vision de general de Enumeracion**

La enumeración es el proceso de extracción de nombres de usuarios, nombres de máquinas, recursos de red, recursos compartidos y servicios de un sistema, y se realiza en un entorno de intranet.

**Laboratorio 3**

**Realización de la enumeración de la red usando SuperScan**

**Escenario**

Durante la enumeración, la información se recopila sistemáticamente y se identifican los sistemas individuales. Los evaluadores de la pluma examinan los sistemas en su totalidad para evaluar las debilidades de seguridad. En esta práctica de laboratorio, extraemos información de NetBIOS, cuenta de usuario y grupo, recursos compartidos de red y dominios y servicios de confianza (en ejecución o detenidos). SuperScan detecta los puertos TCP y UDP abiertos en las máquinas de destino y determina qué servicios se ejecutan en ellos, lo que permite a los atacantes explotar estos puertos abiertos y piratear las máquinas de destino. Como experto hacker ético y probador de penetración, puede utilizar SuperScan para enumerar las redes de destino y extraer listas de computadoras, nombres de usuarios, grupos de usuarios, nombres de máquinas, recursos de red y servicios.

**Objetivos de Laboratorio**

El objetivo de esto es ayudar a los estudiantes a aprender y realizar la enumeración de NetBIOS, que se lleva a cabo para obtener:

- Listas de equipos que pertenecen a un dominio.

- Listas de recursos compartidos en los hosts individuales en la red.

- Políticas y contraseñas.

**Entorno de Laboratorio**

Para completar este laboratorio, necesitarás:

- SuperScan se encuentra en D: \ CEH-Tools \ CEHv9 Module 04 Enumeration\NetBIOS Enumeration Tools\SuperScan

- También puede descargar la última versión de SuperScan desde este enlace <http://www.mcafee.com/us/downloads/free-tools/superscan.aspx>

- Una computadora que ejecuta Windows Server 2012 como máquina host.

- Windows 8.1 se ejecuta en una máquina virtual como máquina de destino.

- Privilegios administrativos para instalar y ejecutar herramientas.

- Un navegador web con conexión a internet.

**Descripción general de SuperScan**

1. El propósito de SuperScan es recopilar información como:

a. Umbral de bloqueo de cuenta.

b. Grupos locales y cuentas de usuario.

c. Grupos globales y cuentas de usuario.

2. Restrinja la rutina de anulación anónima y también la verificación de contraseña:

a. Cheques para cuentas de usuario con contraseñas en blanco

b. Comprueba las cuentas de usuario con contraseñas que sean iguales a los nombres de usuario en minúsculas.

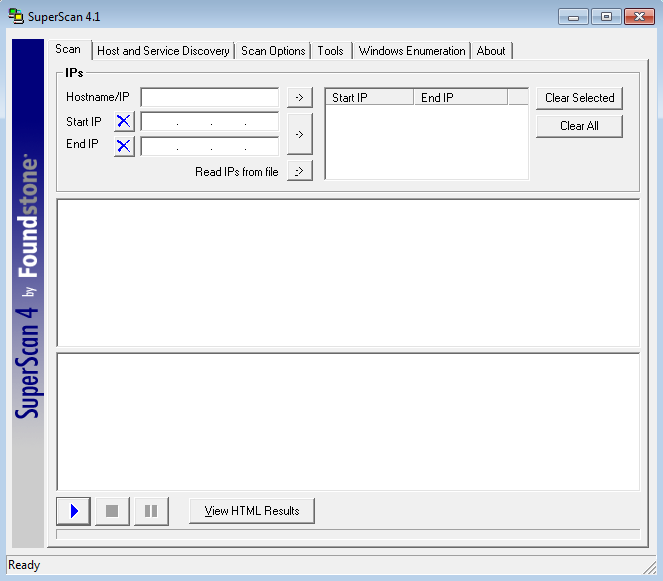
**Tareas de Laboratorio**

1 Inicie la máquina virtual de Windows 8.1 a partir de este laboratorio.

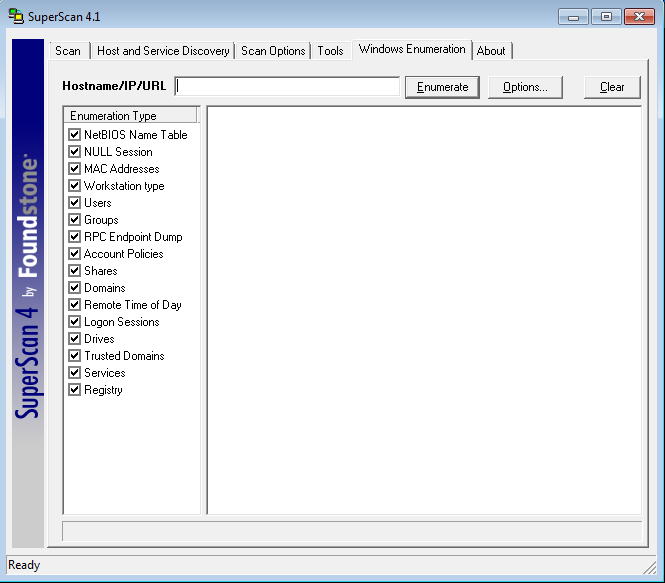
- Vuelva a la máquina host (Windows Server 2012), navegue a D: \ CEH-Tools \ CEHv9 Module 04 Enumeration\NetBios Enumeration Tools\SuperScan, y hacer doble click en SuperScan4.1.exe

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

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



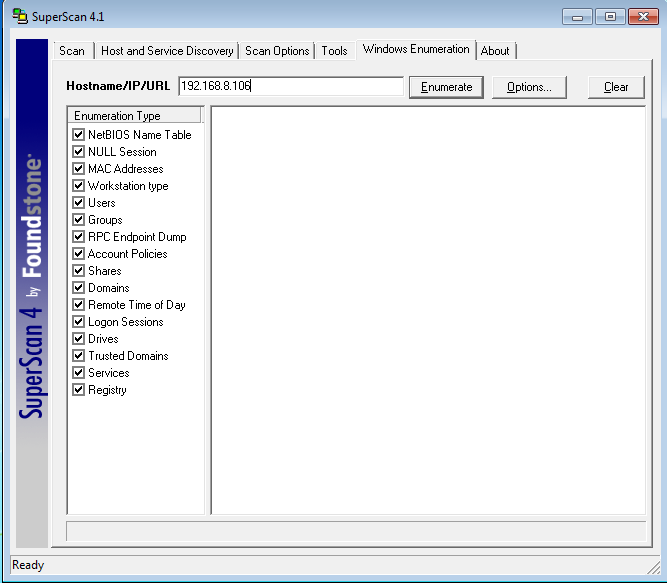
2. Haga clic en la pestaña Enumerar de Windows.



- Introduzca la dirección IP de la máquina de destino en el cuadro de texto Nombre de host / IP / URL. En esta práctica de laboratorio, ingresamos la dirección IP de la máquina virtual de Windows 8.1.

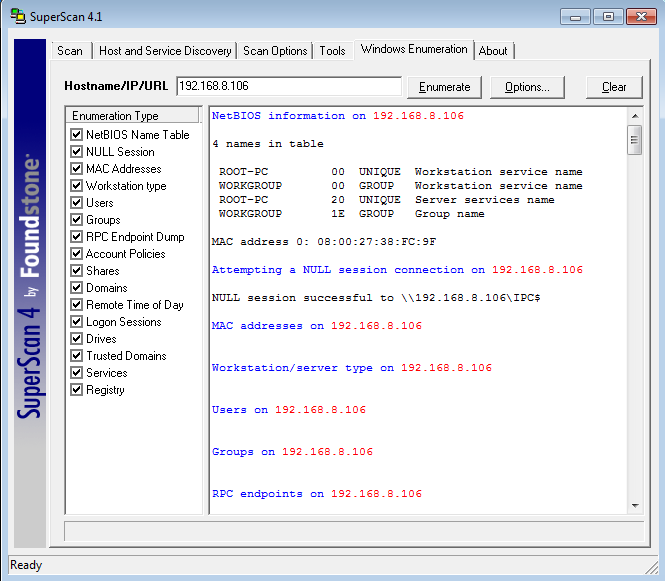
- Marque los tipos de enumeración que desea realizar.

- Ahora, haga clic en Enumerar

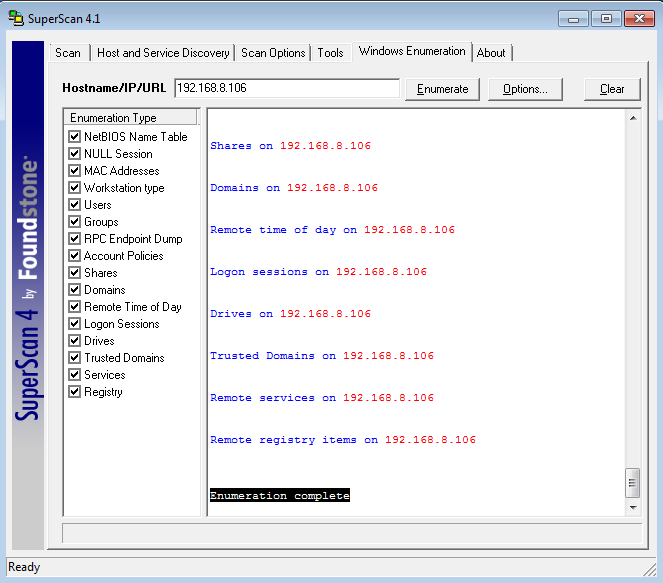


- SuperScan comienza a enumerar el nombre de host proporcionado y muestra los resultados

como se muestra en la siguiente captura de pantalla.



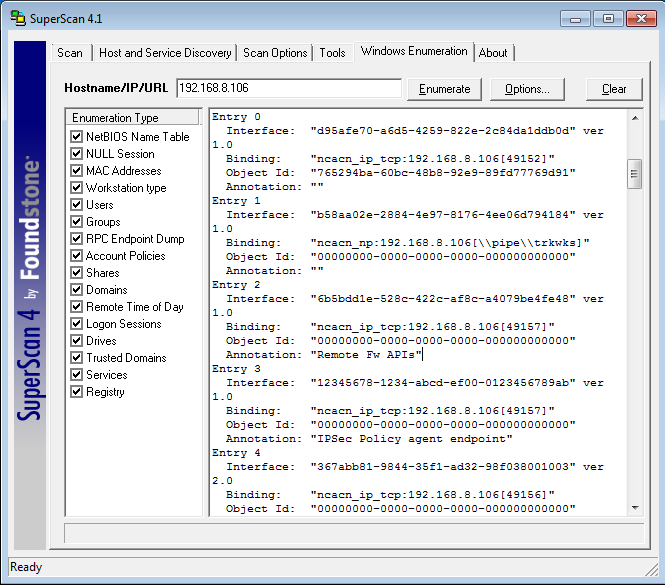
- Espera a que se complete el proceso de enumeración



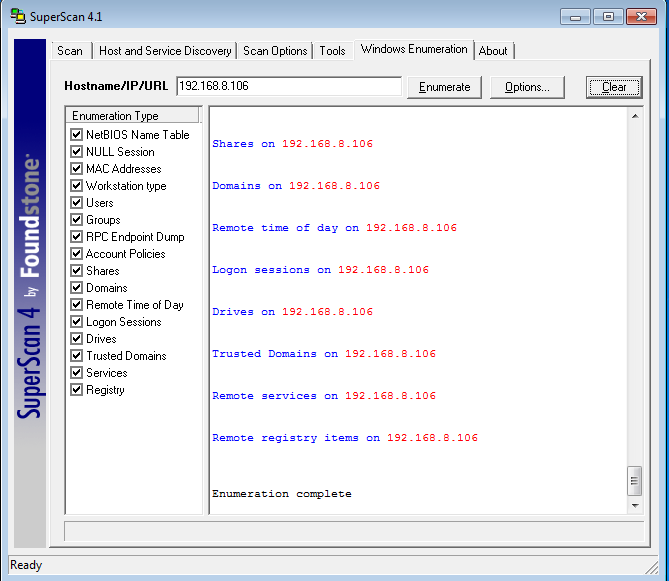
- Una vez finalizado el proceso de enumeración, el botón de detención cambia a Enumerar.

- Desplácese por la ventana. Se mostrará un mensaje de enumeración completa al final de la ventana de resultados de la enumeración.

- Ahora, desplácese por la ventana para ver los resultados de la enumeración.



14. Para realizar una nueva enumeración en otro nombre de host, haga clic en el botón Borrar en la parte superior derecha de la ventana. La opción borra todos los resultados anteriores.

**Analisis de Laboratorio**

Analizar y documentar los resultados relacionados con este ejercicio. Proporcione su opinión sobre la postura y la exposición de seguridad de su objetivo.

**Laboratorio 4**

**Enumerar recursos en una máquina local usando hyena**

**Escenario**

Los piratas informáticos enumeran aplicaciones y banners además de identificar cuentas de usuario y recursos compartidos. En esta práctica de laboratorio, Hyena utiliza una interfaz de estilo Explorer para todas las operaciones, servicios, dispositivos, eventos, archivos, impresoras y trabajos de impresión, sesiones, archivos abiertos, espacio en disco, derechos de usuario, mensajes, exportación, programación de trabajos, procesos e impresión. todos son compatibles Para ser un experto en piratería ética y un probador de penetración, debe tener un conocimiento sólido de enumeración, lo que requiere una conexión activa a la máquina que está siendo atacada.

**Objetivos de Laboratorio**

El objetivo de esto es ayudar a los estudiantes a aprender y realizar la enumeración de la red de:

- Información del usuario del sistema.

- Ejecución de servicios del sistema.

**Entorno de Laboratorio**

Para realizar este laboratorio, necesitas:

- Una computadora con Windows Server 2012

- Privilegios administrativos para instalar y ejecutar herramientas.

- También puedes descargar esta herramienta desde el siguiente enlace <http://systemtools.com/hyena/download.com>

- Si su dispositivo descarga la última versión de esta herramienta, las capturas de pantalla pueden diferir.

**Resumen de la enumeración**

La enumeración es el proceso de extracción de nombres de usuarios, nombres de máquinas, recursos de red, recursos compartidos y servicios de un sistema. Las técnicas de enumeración se realizan en un entorno de intranet.

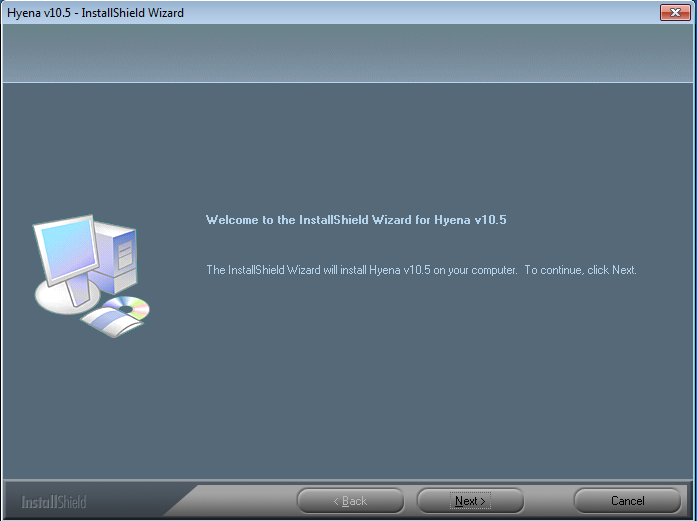
**Tareas de Laboratorio**

1. Navegue a D: \ CEH-Tools \ CEHv9 Module 04 Enumeration\NetBIOS\Enumeration Tools\Hyena y hacer doble click Hyena\_English\_x64.exe.

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

- Aparece el asistente de instalación de Hyena, haga clic en Siguiente.

Nota: Si se le pide que instale C ++ Redistribute, haga clic en instalar. Después de la instalación, si requiere un reinicio del sistema, haga clic en Sí para reiniciar la máquina.

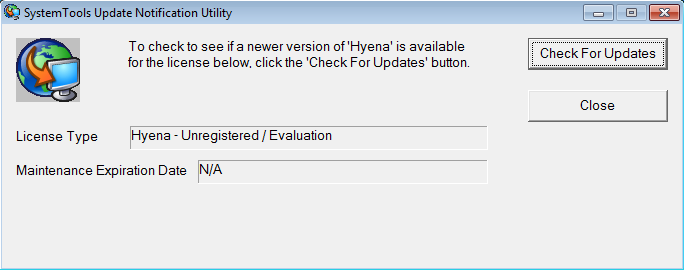


- Sigue los pasos para instalar Hyena.

- Al finalizar la instalación, aparece la sección de InstallShield Wizard completado; Haga clic en Finalizar para completar la instalación.

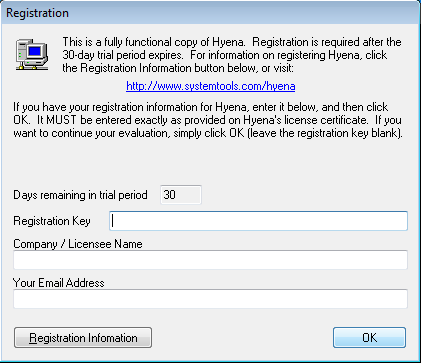
- Al finalizar la instalación, inicie la aplicación Hyena desde la pantalla de aplicaciones.

- Si aparece la utilidad de notificación de actualización de herramientas de sistema, haga clic en cerrar.

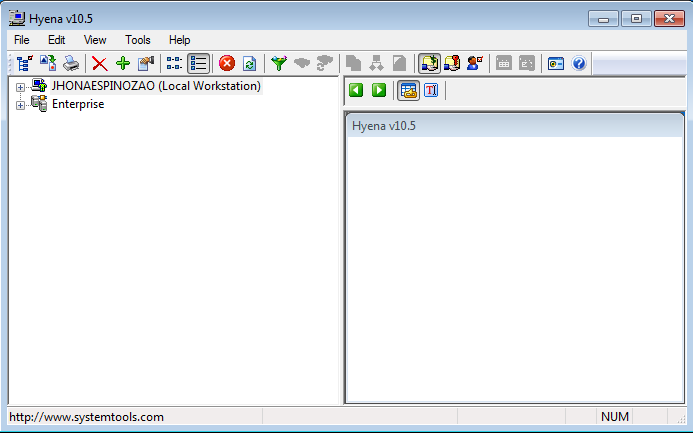


- Si aparece la ventana de registro, solicitándole que registre la aplicación, haga clic en No.

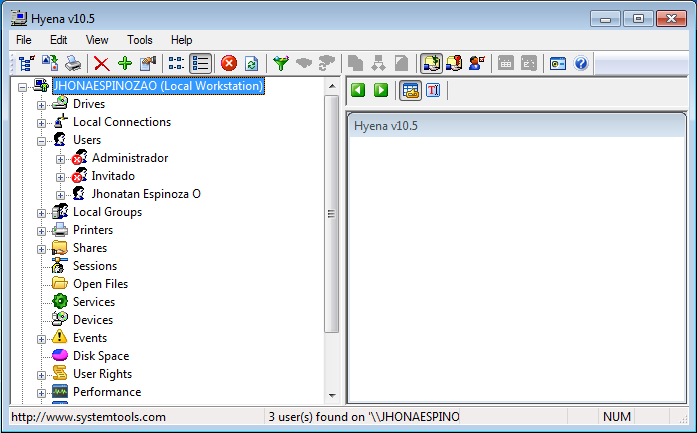
- Si aparece el cuadro de diálogo Hiena, que le solicita que registre la aplicación, haga clic en No.

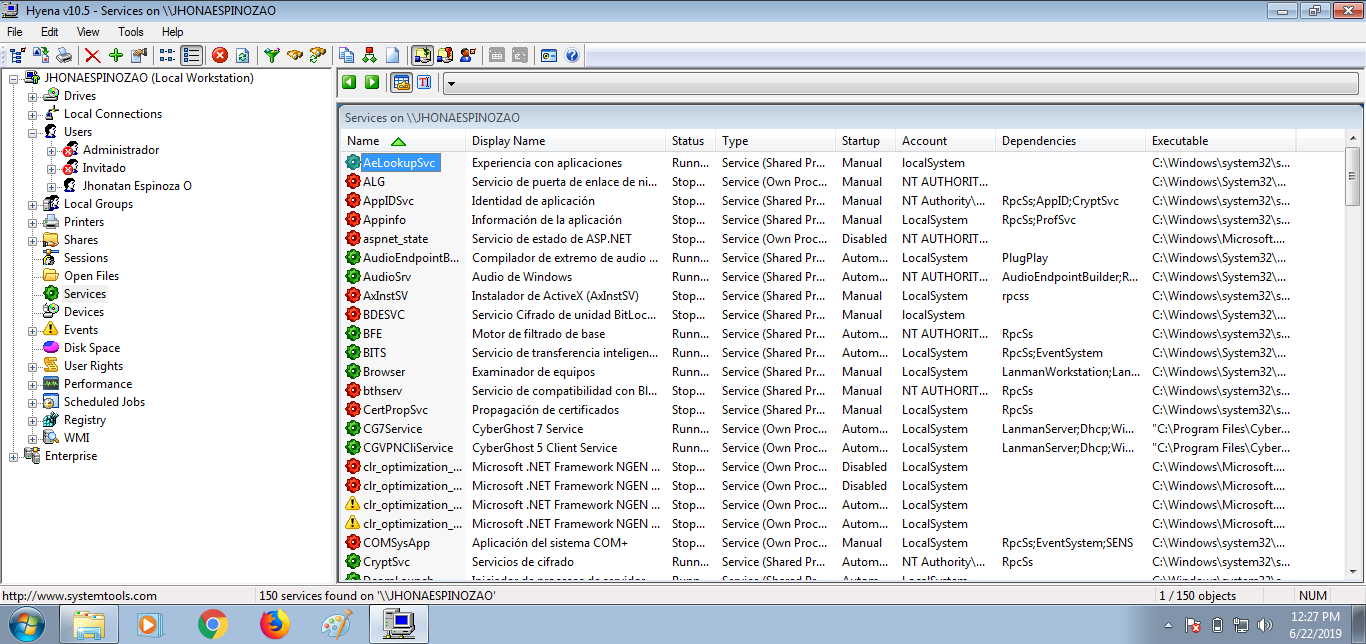


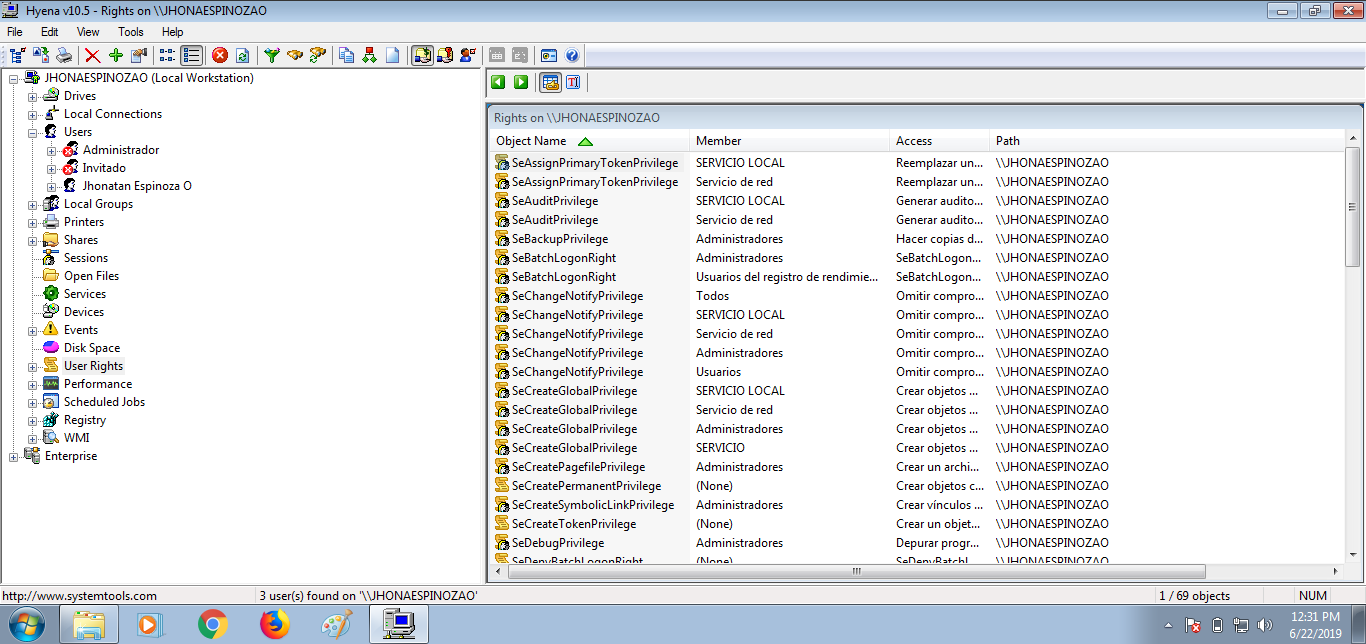
2. Aparece la ventana principal de Hyena, como se muestra en la captura de pantalla.

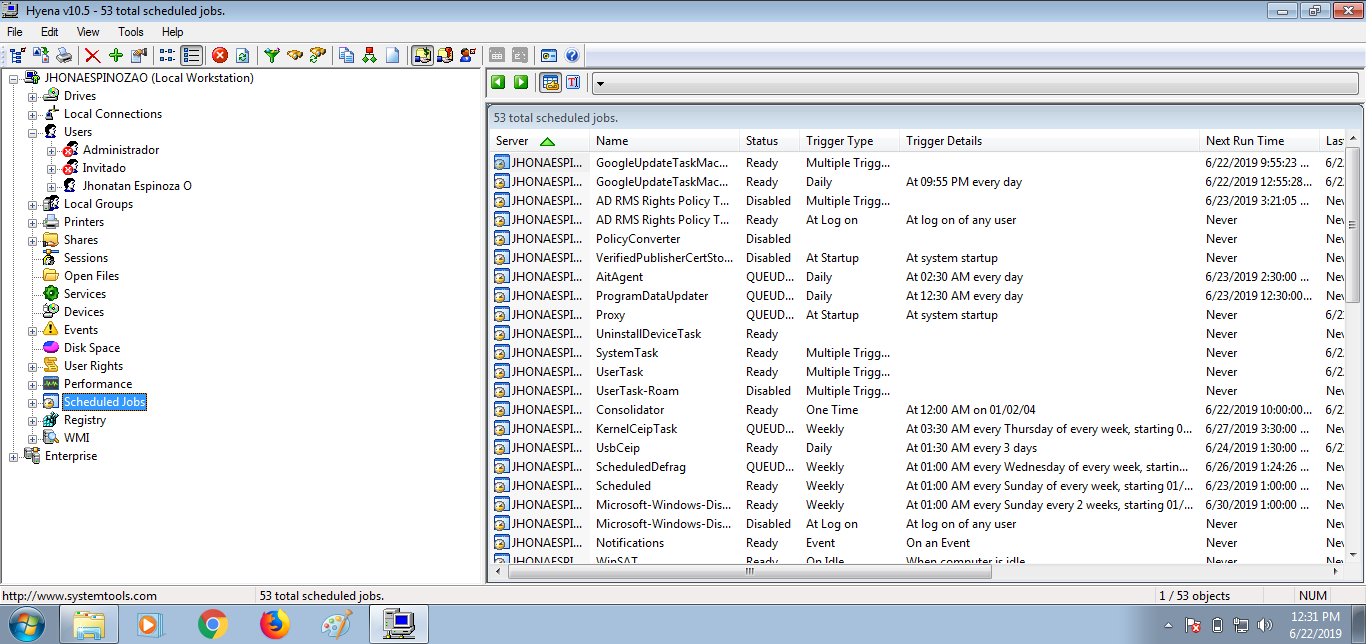


- Haga clic en el nodo "+" de la estación de trabajo local para expandir la sección, luego expanda el nodo Usuarios para ver todos los usuarios en la máquina local.

- Para verificar los servicios que se ejecutan en el sistema, haga doble clic en Servicios.

- Haga doble clic en Derechos de usuario para enumerar los Derechos de usuario.

- Haga doble clic en Trabajos programados para examinar los trabajos programados.



- Al observar todas estas opciones, puede verificar cualquier información razonable descubierta por Hyena que le indique tomar las medidas de seguridad adecuadas para proteger el sistema.

**Analisis de Laboratorio**

Analizar y documentar los resultados relacionados con este ejercicio de laboratorio. Proporcione su opinión sobre la seguridad y la exposición de su objetivo.

**Laboratorio 5**

**Realización de la enumeración de red utilizando el enumerador de NetBIOS**

**Escenario**

La enumeración es el primer ataque en una red objetivo, que se utiliza para recopilar la información de forma activa. Debe tener un conocimiento sólido de enumeración, un proceso que requiere una conexión activa a la máquina que está siendo atacada. Un hacker enumera aplicaciones y banners además de identificar cuentas de usuario y recursos compartidos. En esta práctica de laboratorio, enumeramos el nombre de usuario, la dirección MAC y el grupo de dominio de un objetivo.

**Objetivos de Laboratorio**

El objetivo de este laboratorio es ayudar a los estudiantes a aprender y realizar la enumeración de NetBIOS.

El propósito de la enumeración de NetBIOS es recopilar la siguiente información:

- Umbral de bloqueo de cuenta.

- Grupos locales y cuentas de usuario.

- Grupos globales y cuentas de usuario.

**Entorno de Laboratorio**

Para completar este laboratorio, necesitarás:

- La herramienta de enumerador NetBIOS se encuentra en D: \ CEH-Tools \ CEHv9 Module 04 Enumeration\NetBIOS Enumeration Tools\NetBIOS Enumerator

- También puede descargar la última versión del enumerador NetBIOS desde el enlace [http://nbtenum.sourceforge.net](http://nbtenum.sourceforge.net/)

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

- Una máquina que ejecuta Windows Server 2012 como una máquina atacante.

- Una máquina virtual que ejecuta Windows Server 2008 como máquina de destino.

- Una máquina virtual que ejecuta Windows 8.1 como una máquina de destino.

- Se requieren privilegios administrativos para ejecutar esta herramienta

**Vision general de Enumeration**

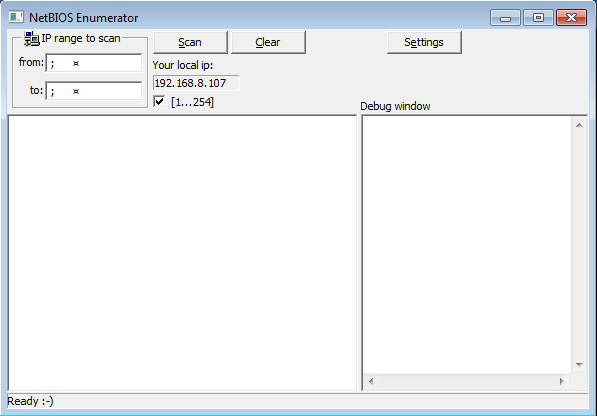
La enumeración implica hacer conexiones activas, de modo que se puedan registrar la información típica que los atacantes buscan en la enumeración e incluye los nombres de las cuentas de usuario para futuros ataques de adivinación de contraseña. El enumerador de NetBIOS es una herramienta de enumeración que muestra cómo utilizar el soporte de red remota y cómo tratar algunas otras técnicas web interesantes, como SMB.

**Tareas de Laboratorio**

1. Para iniciar el enumerador NetBIOS, vaya a D: \ CEH-Tools \ CEHv9 Module 04 Enumeration\NetBIOS Enumeration Tools\NetBIOS Enumerator y hacer doble click NetBIOS Enumerater.exe

- Si aparece la ventana emergente de advertencia de seguridad de archivo abierto, haga clic en Ejecutar.

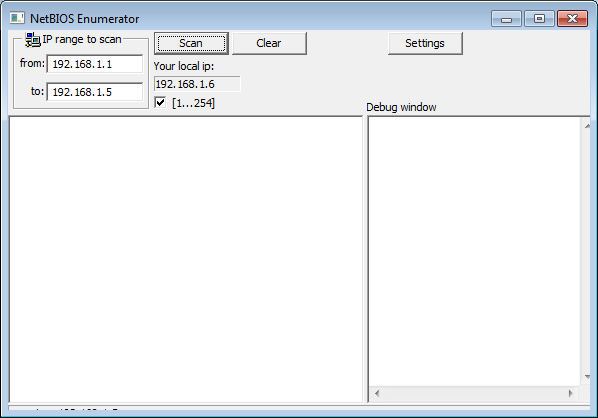
- Aparece la ventana principal de NETBIOS Enumerator, como se muestra en la captura de pantalla.



2. En el rango de IP para escanear, ingrese un rango de IP en los campos desde y hacia.

Nota: el rango de IP puede diferir en su entorno de laboratorio.

- Haga clic en el botón de escaneo para iniciar el escaneo.

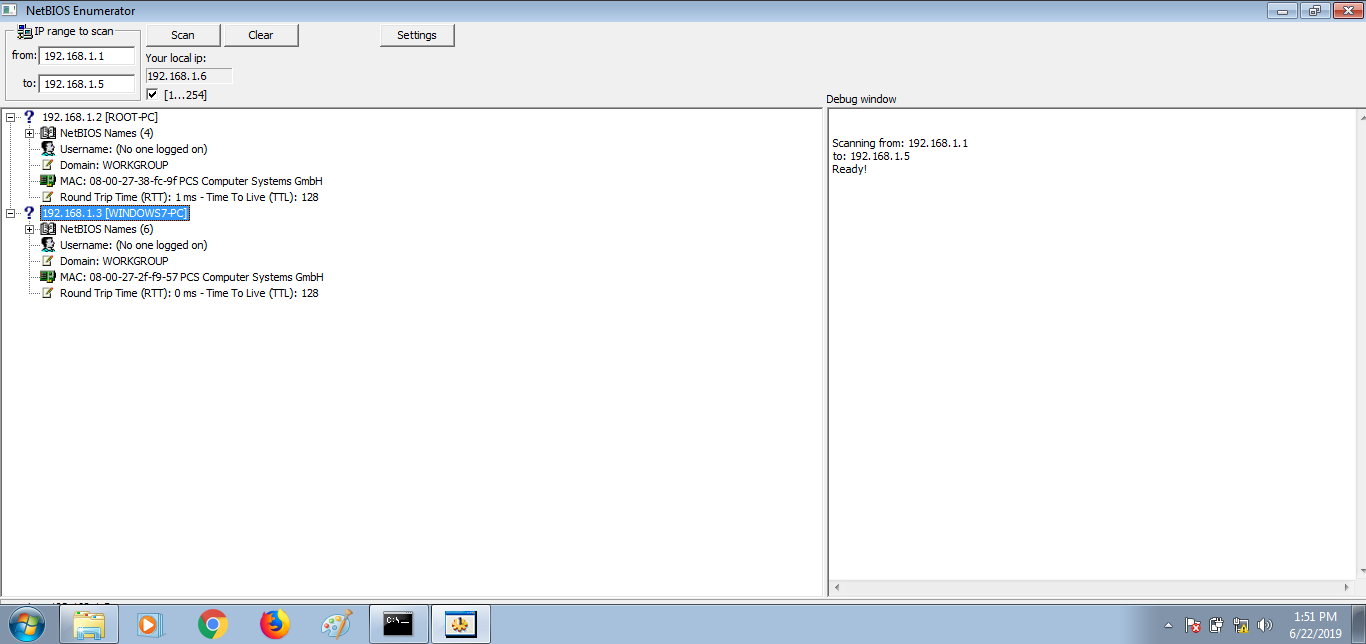


- El enumerador NetBIOS comienza a buscar el rango de direcciones IP proporcionadas.

- Una vez finalizada la exploración, los resultados se muestran en el panel izquierdo.

- La sección de la ventana Depuración en el panel derecho muestra el rango de exploración de direcciones IP y muestra ¡Listo! Después de la finalización de la exploración.

Nota: El resultado del análisis puede diferir en su entorno de laboratorio.

- Los atacantes pueden usar la información obtenida, como nombres de usuario enumerados, y realizar técnicas de adivinación de contraseñas para descifrar una cuenta de usuario.

- Para realizar una nueva exploración o volver a escanear el rango proporcionado de direcciones IP, borre los resultados de la exploración anterior haciendo clic en Borrar.

**Analisis de Laboratorio**

Analizar documentar los resultados relacionados con este ejercicio de laboratorio.

**Laboratorio 6**

**Enumerar una red utilizando un escáner de red SoftPerfect**

**Escenario**

Para ser un hacker ético experto y un probador de penetración, debe tener un conocimiento sólido de enumeración, lo que requiere una conexión activa a la máquina que está siendo atacada. Un hacker enumera aplicaciones y banners además de identificar cuentas de usuario y recursos compartidos. En esta práctica de laboratorio, intentamos resolver los nombres de host y detectar automáticamente su rango de IP local y externo.

**Objetivos de Laboratorio**

El objetivo de este laboratorio es ayudar a los estudiantes a aprender y realizar la enumeración de NetBIOS, que se realiza para detectar:

- Hardware direcciones MAC a través de enrutadores.

- Carpetas compartidas ocultas y escritas.

- Dirección IP interna y externa.

**Entorno de Laboratorio**

Para completar este laboratorio, necesitarás:

- El escáner de red SoftPerfect se encuentra en D: \ CEH-Tools \ CEHv9 Module 04 Enumeration\SNMP Enumeration Tools\SoftPerfect Network Scanner\64 bit

- También puede descargar la última versión de SoftPerfect Network Scanner desde el enlace [http:www.softperfect.com/products/networkscanner](http://www.softperfect.com/products/networkscanner)

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

- Una máquina que ejecuta el servidor Windows 2012.

- Una máquina virtual que ejecuta Windows Server 2008 como máquina de destino.

- Una máquina virtual que ejecuta Windows 8.1 como una máquina de destino.

- Se requieren privilegios administrativos para ejecutar esta herramienta

**Vision general de Enumeration**

La enumeración implica una conexión activa para que puedan registrarse. La información típica que los atacantes buscan incluye nombres de cuentas de usuario para futuros ataques de adivinación de contraseñas.

**Tareas de Laboratorio**

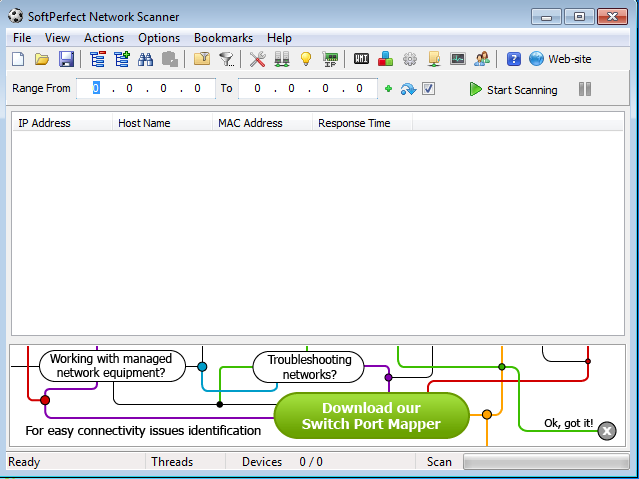
1. Para iniciar el Escáner de red SoftPerfect, vaya a D: \ CEH-Tools \ CEHv9 Module 04 Enumeration\SNMP Enumeration Tools\SoftPerfect Network Scanner\64-bits\y hacer doble click en netscan.exe.

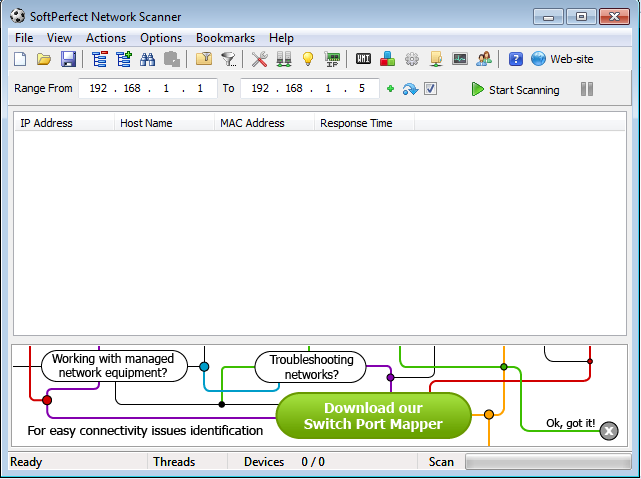
Nota: Si la máquina host (Windows Server 2012) es de 32 bits, debe navegar a D: \ CEH-Tools \ CEHv9 Module 04 Enumeration \ SNMP Enumeration Tools \ SoftPerfect Network Scanner 32 bits y haga clic en netscan.exe

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

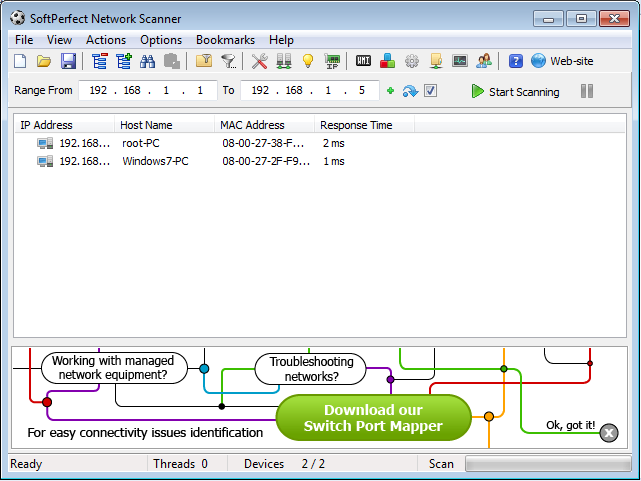
- Si aparece el cuadro de diálogo del escáner de red. haga clic en No.

- La interfaz gráfica de usuario del escáner de red SoftPerfect aparece en la pantalla. Cierre la ventana emergente de anuncios que aparece en el extremo inferior de la GUI.

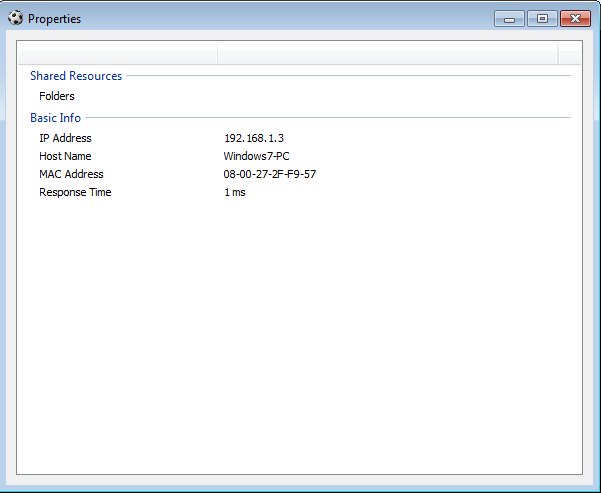
2 Para comenzar a escanear su red, ingrese un rango de IP en los campos desde y hasta, y haga clic en el botón Iniciar escaneo.

 Nota: El rango de IP puede diferir en su entorno de laboratorio.

- La barra de estado muestra el estado del escaneo en la esquina inferior derecha de la GUI.

- Para ver las propiedades de una dirección IP individual, haga clic con el botón derecho en una dirección IP particular y seleccione Propiedades.

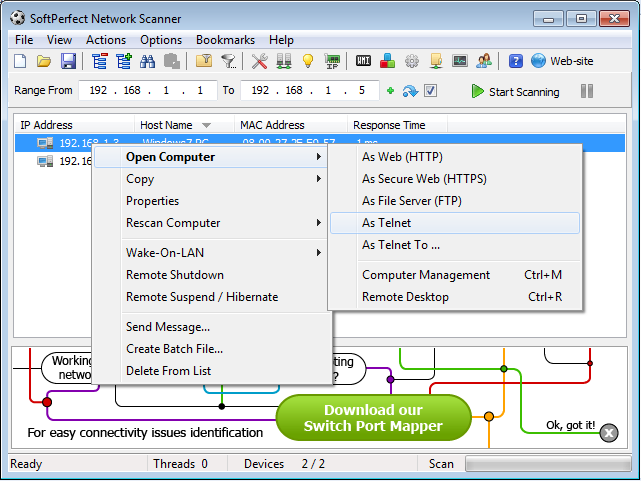
- Aparece la ventana de propiedades. mostrando los recursos compartidos y la información básica de la máquina correspondiente a la dirección IP seleccionada.



- Para ver las carpetas compartidas, observe los hosts escaneados que tienen un nodo + delante de ellos. Expanda el nodo para ver todas las carpetas compartidas.

- Haga clic con el botón derecho en el host seleccionado y haga clic en Abrir computadora. Aparece una lista desplegable, que contiene opciones que le permiten conectarse a la máquina remota como HTTP, HTTPS, Telnet, etc.

- Si el host seleccionado no es lo suficientemente seguro, puede hacer uso de estas opciones para conectarse a las máquinas remotas. También puede realizar actividades como enviar un mensaje, apagar una computadora de manera remota, etc. Estas características solo son aplicables si la máquina seleccionada está construida con una configuración de seguridad deficiente.



**Analisis de Laboratorio**

Analizar y documentar los resultados relacionados con los ejercicios de este laboratorio.

**Laboratorio 11**

**Realización de enumeración de red utilizando varias herramientas de interrogación de DNS**

**Escenario**

Los atacantes aplican varias técnicas de enumeración de DNS como Zone Transfer, Domain and Host Brute-Force y Cache Snooping para obtener información asociada con los servidores DNS y la infraestructura de red de las organizaciones.

Como un pirata informático ético o un oficial de seguridad de la información, debe comprometer la información de la red utilizando técnicas de enumeración de DNS; y luego implementar contramedidas de enumeración de DNS para la protección de datos.

**Objetivos de Laboratorio**

Para completar este laboratorio se necesita:

- Una computadora corriendo Windows Server 2012

- Kali Linux corriendo una maquina virtual

- Conexion a Internet activa

**Vision general de Enumeracion**

La enumeración es el proceso de extracción de nombres de usuarios, nombres de máquinas, recursos de red, recursos compartidos y servicios de un sistema, y se realiza en un entorno de Internet.

**Tareas de Laboratorio**

1. Lanzar la maquina virtual Kali Linux desde Hyper-V manager, e inicie sesion en el.

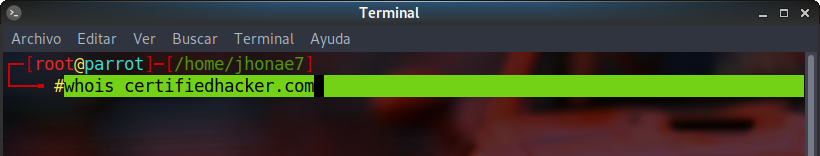
- Aparece kali Linux Desktop, como se muestra en la siguiente captura de pantalla:

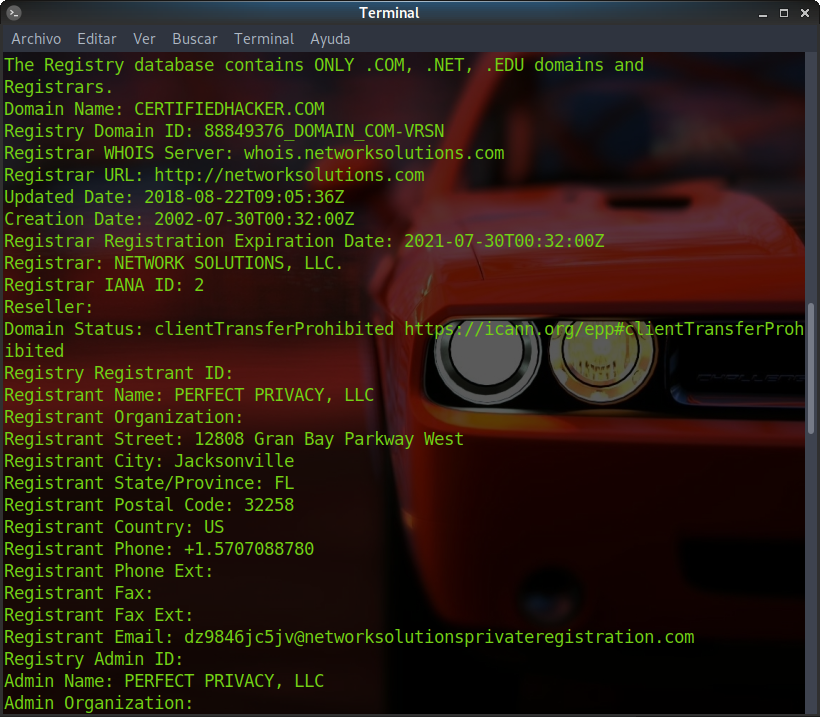
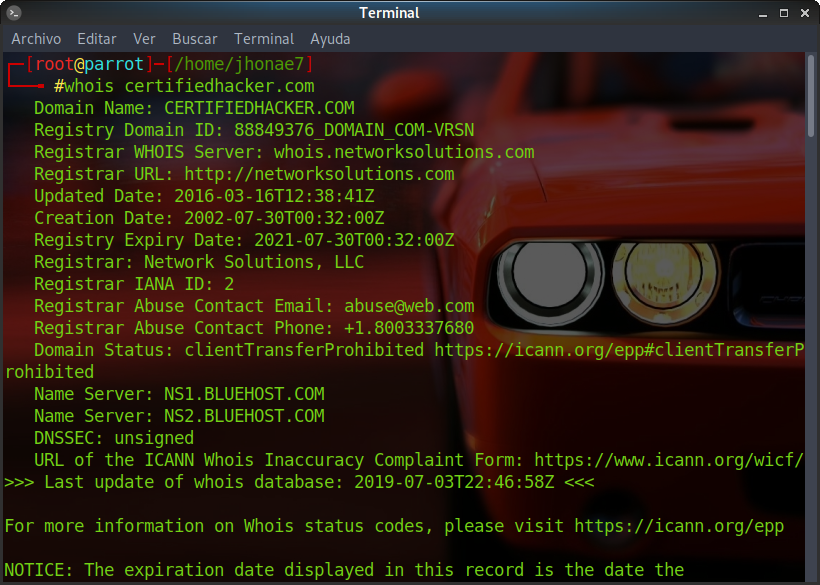
- Seleccione Aplicaciones -> Accesorios -> Terminal para iniciar el terminal de línea de comandos.

- Alternativamente, puede hacer clic en el icono de la línea de comandos, ubicado en la barra de tareas.

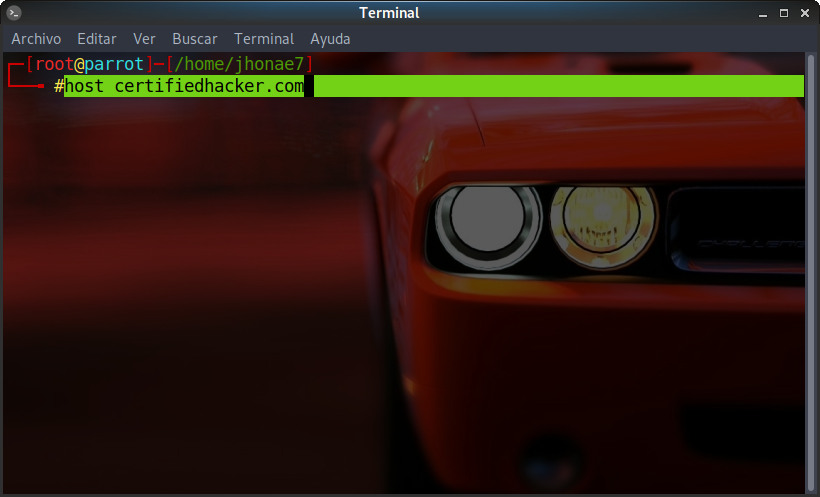
2. El objetivo utilizado en este laboratorio es [www.certicatedhacker.com](http://www.certicatedhacker.com/); su nombre de dominio correspondiente es certifiedhacker.com.

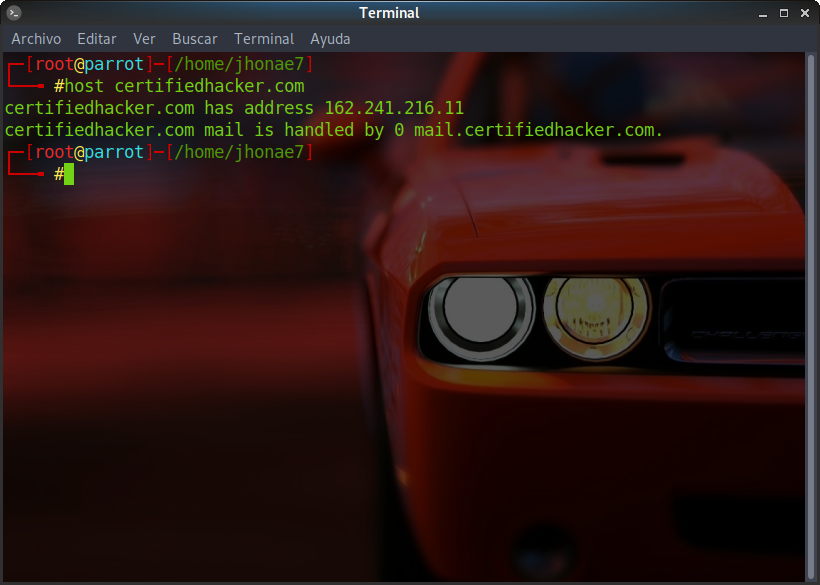
- Escriba whois certifiedhacker.com en el terminal de línea de comandos y presione Entrar.

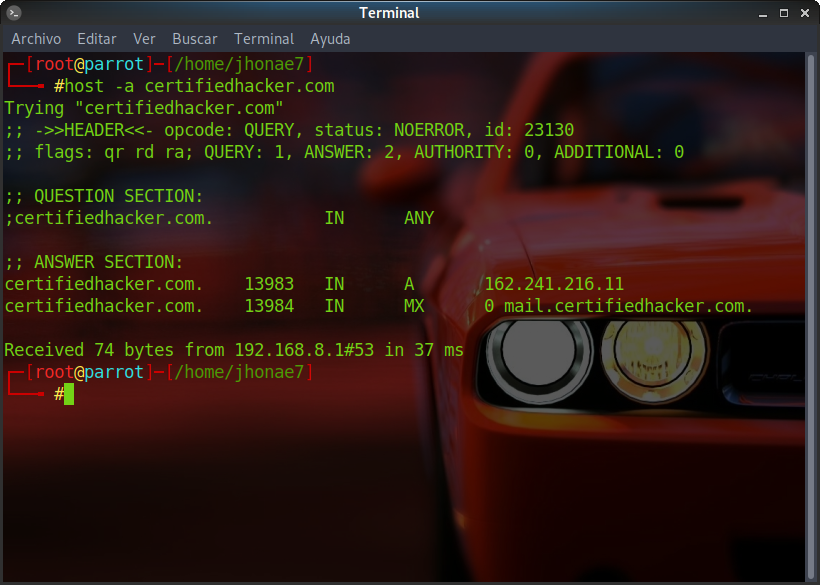
- Esto devuelve información relacionada con whois del dominio certifiedhacker.com.

- Desplácese hacia abajo en la ventana del terminal para ver la información relacionada con el registro:

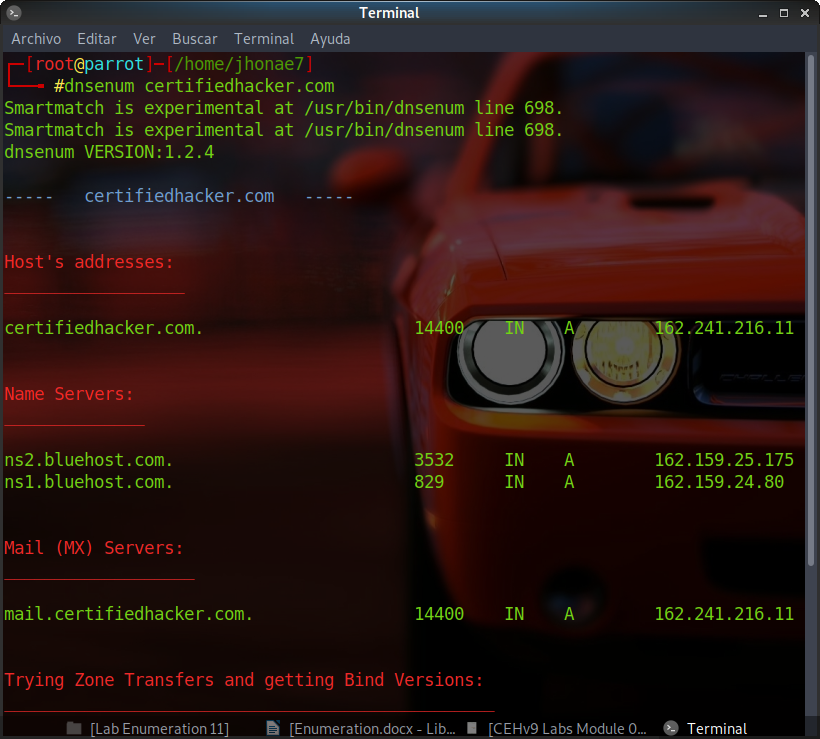
- Escriba host www.certifiedhacker.com para enumerar las direcciones IP del sitio web [www.certifiedhacker.com](http://www.certifiedhacker.com/).

- Se le proporcionarán todas las direcciones IP asociadas con el sitio web de destino, como se muestra en la siguiente captura de pantalla:

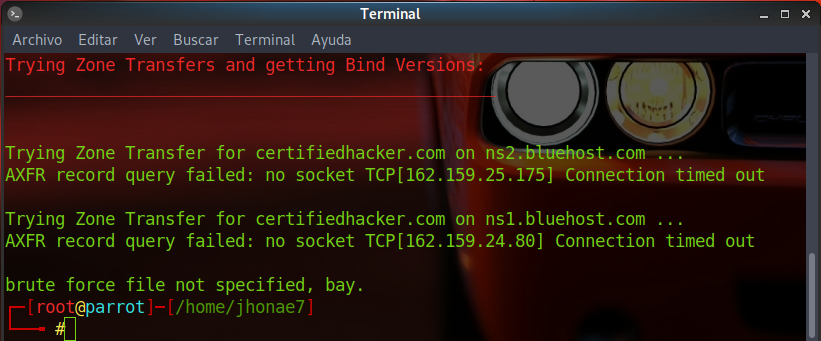
- Escriba host -a certifiedhacker.com y presione Entrar para mostrar los registros DNS asociados con el sitio web, como se muestra en la captura de pantalla:



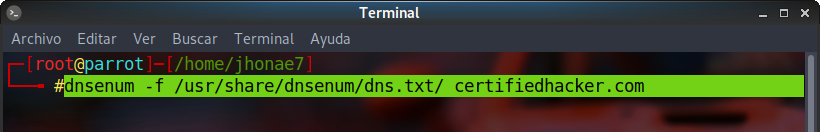
- Escriba dnsenum certifiedhacker.com y presione Entrar para mostrar la dirección IP, los servidores de nombres, los servidores de correo y otros relacionados con el sitio web, como se muestra en la captura de pantalla:



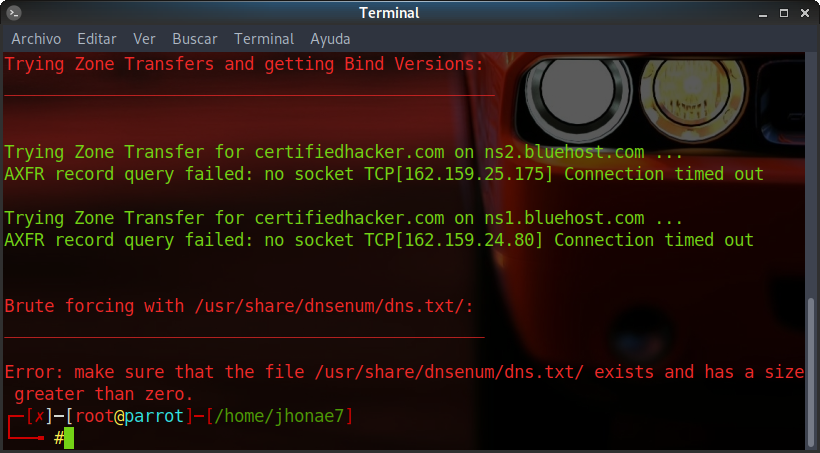
- dnsenum también intenta realizar una transferencia de zona para el dominio en sus servidores de nombres asociados, en un intento de obtener subdominios, como se muestra en la captura de pantalla:



- En caso de que falle una transferencia de zona, puede realizar un ataque de fuerza bruta en el sitio web de destino emitiendo el comando dnsenum -f /usr/share/dnsenum/dns.txt [nombre de dominio del sitio web de destino] y presionando Intro. En esta práctica de laboratorio, el dominio de destino es certifiedhacker.com



- dnsenum intenta imponer una fuerza bruta en el sitio web para extraer su subdominio, la clase de dirección IP, también está asociado con el sitio web.

- Escriba el comando dnsdict6 -d -4 certifiedhacker.com y presione Entrar.

- Esta:

- Enumera los subdominios en certifiedhacker.com asociados con la dirección IPv4.

- Obtiene información relacionada con DNS, como se muestra en la captura de pantalla:

- Escriba fierce -dns certifiedhacker.com y presione Entrar. Esto enumera la información relacionada con el servidor de nombres, junto con los subdominios asociados con el sitio web, como se muestra en la captura de pantalla:

