**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 03 Scanning Network.**

**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**

Anteriormente, reunió toda la información posible sobre el destino, como el rango de direcciones IP y la topología de la red.

Ahora, como hacker ético, o probador de penetracion, su próximo paso será realizar el escaneo de puertos, escaneo de red y escaneo de vulnerabilidades en la dirección IP que obtuvo en la fase de recopilación de información. Esto le ayudará a identificar la IP / nombre de host, puertos, servicios, hosts en vivo, vulnerabilidades y servicios que se ejecutan en la red de destino.

El escaneo de puertos lo ayudará a identificar los puertos abiertos y los servicios que se ejecutan en puertos específicos, lo que implica la conexión a puertos de sistema TCP y UDP. El escaneo de puertos se utiliza para descubrir las vulnerabilidades en los servicios que se ejecutan en un puerto.

La exploración de vulnerabilidades determina la posibilidad de ataques a la seguridad de la red. Evalúa los sistemas y la red de la organización en busca de vulnerabilidades, como parches faltantes, servicios innecesarios, autenticación débil y cifrado débil. El escaneo de vulnerabilidades es un componente crítico de cualquier asignación de pruebas de penetración.

Los laboratorios de este módulo le brindarán experiencia en tiempo real en el escaneo de redes y el escaneo de vulnerabilidades.

**Objetivos de Laboratorio**

El objetivo de este laboratorio es ayudar a los estudiantes a realizar escaneo de redes, escanear puertos, analizar las vulnerabilidades de la red, etc.

Necesita realizar un escaneo de red para:

- Compruebar los sistemas en vivo y los puertos abiertos.

- Realizar la captura de banners y huellas del sistema operativo.

- Identificar las vulnerabilidades de la red.

- Dibuje diagramas de red de hosts vulnerables.

**Descripción general del escano de red**

El escaneo en red es un procedimiento para identificar hosts activos en una red, ya sea con el propósito de atacarlos o para evaluar la seguridad de la red. Los procedimientos de exploración, como los barridos de ping y las exploraciones de puertos, recopilan información sobre qué. Las direcciones IP se asignan a los hosts activos que están activos en las redes, y los servicios que se ejecutan en él. El análisis de vulnerabilidades es un proceso de identificación de vulnerabilidades de seguridad de los sistemas en una red para determinar si se puede explotar un sistema y dónde.

**Laboratorio 1**

**Técnicas de creación de paquetes UDP y TCP utilizando HPING3**

**Escenario**

En el escaneo de la red, su primer procedimiento será escanear la red de destino para determinar todos los puertos abiertos posibles, hosts en vivo y servicios en ejecución. El conocimiento de las técnicas de creación de paquetes puede ayudarlo a escanear la red más allá del firewall o IDS.

**Objetivo de Laboratorio**

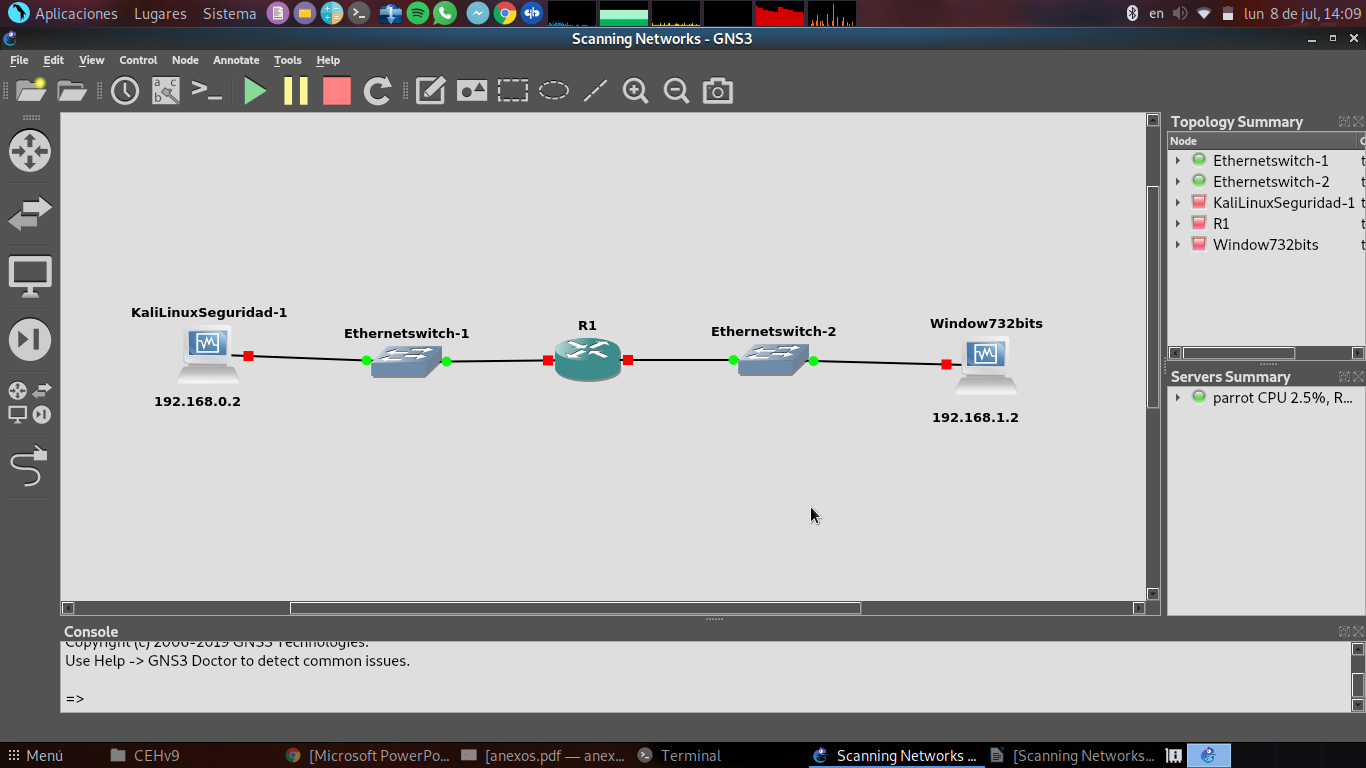
Este laboratorio le ayudará a comprender cómo realizar el escaneo de la red y la creación de paquetes utilizando hping3.

**Entorno de Laboratorio**

Para llevar a cabo el laboratorio, necesitas:

- Una computadora que ejecuta Kali Linux (Attacker Machine)

- Una computadora corriendo windows

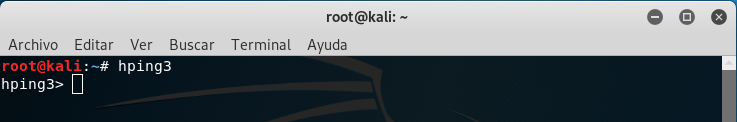


**Descripción general de la elaboración de paquetes**

La creación de paquetes es una técnica que le permite probar conjuntos de reglas de firewall y encontrar puntos de entrada en un sistema o red específicos. Esto se hace generando paquetes manualmente para probar los dispositivos y el comportamiento de la red, en lugar de utilizar el tráfico de red existente.

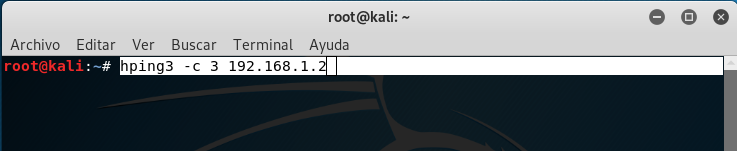
**Tareas de Laboratorio**

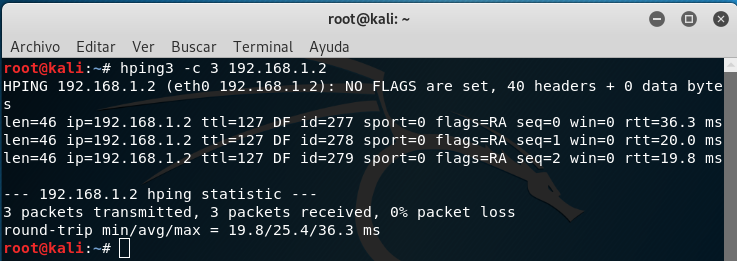
1. Para iniciar HPING3 en kali Linux, vaya a Aplicaciones -> Kali Linux -> Recopilación de información -> Identificación de host en vivo -> hping3.

****

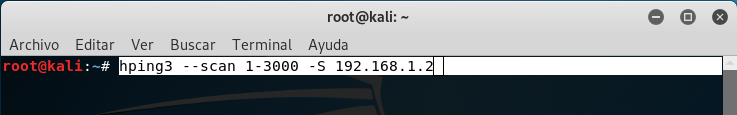
2. Ahora escriba hping3 -c 3 <Dirección IP de la máquina de destino> y presione Entrar. En este laboratorio, estamos usando una dirección IP de la máquina de Windows 7 (192.168.1.2).

Aquí, -c 3 significa que solo queremos enviar tres paquetes a la máquina de destino.

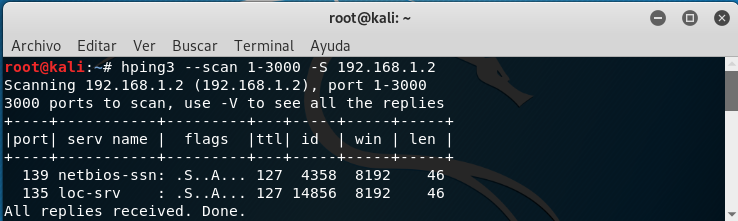
- Desde el comando anterior, la salida muestra que se recibieron y enviaron tres paquetes.

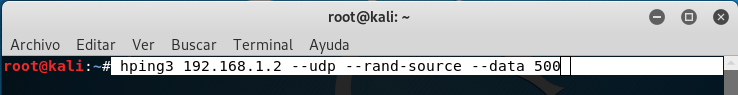


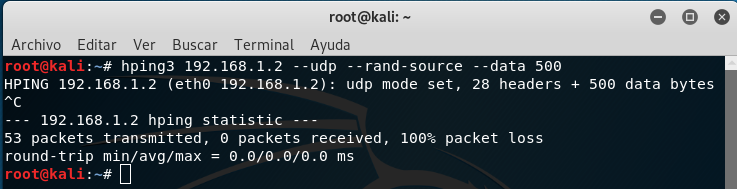
3. Ahora escriba hping3 -sean 1-3000 -S <Dirección IP de destino> y presione Entrar.

- Aquí, el parámetro -sean define el rango de puertos a escanear y -S representa el indicador SYN.

- La salida muestra los puertos abiertos en la máquina de destino, es decir, windows 7.

4.Ahora, para realizar la creación del paquete UDP, escriba hping3 <dirección IP de la máquina de destino> -udp -rand-source -data 500 y presione Entrar.

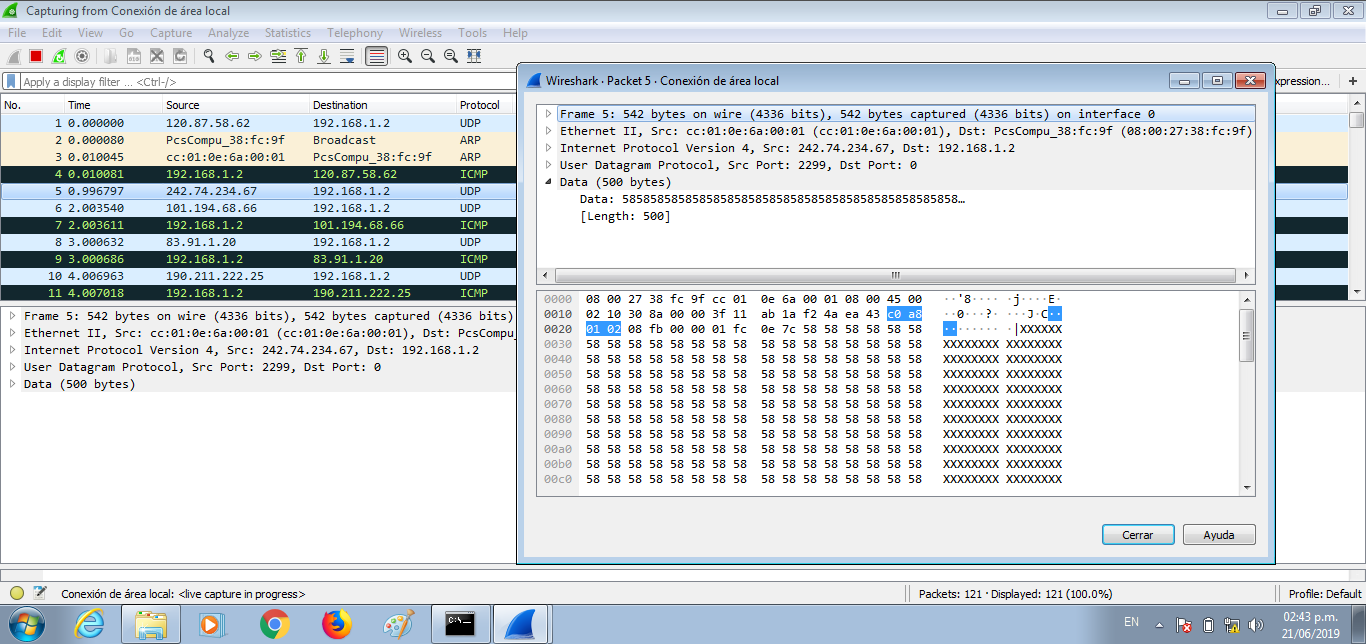




5. Ahora, inicie sesión en la máquina virtual de Windows 7 e inicie Wireshark para comenzar a capturar los paquetes. Observe los paquetes UDP en Wireshark.

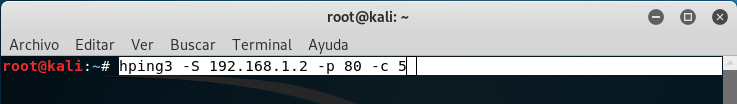
- Haga doble clic en cualquier paquete UDP y observe los detalles.

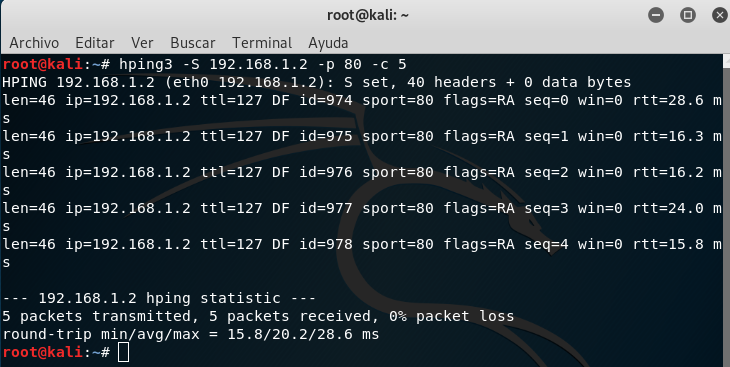
- El paquete UDP es capturado por Wireshark en la máquina de destino.

- Cierre todas las ventanas de wirehark. Cuando se le solicite guardar, haga clic en Salir sin guardar para cerrar. Wireshark sin guardar la captura de tráfico.

- Antes de realizar esta tarea, inicie de nuevo Wireshark en la máquina con Windows 7 (Máquina de destino) y déjela en funcionamiento.

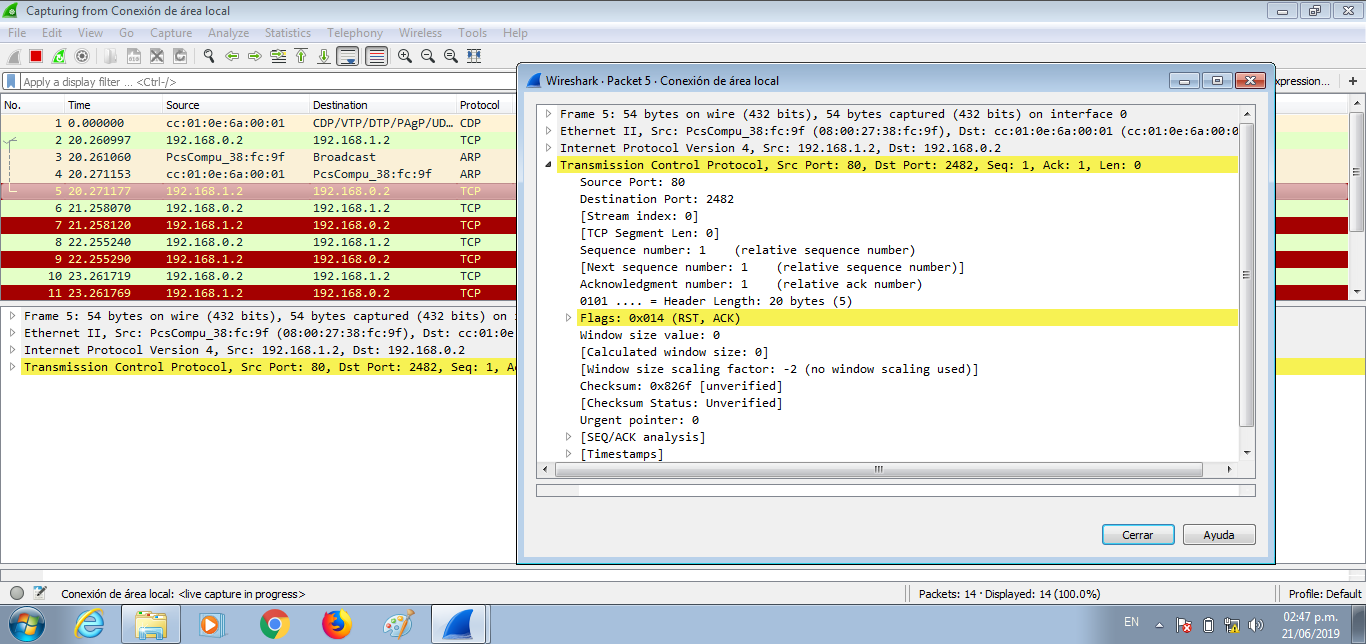
6. Envíe una solicitud TCP SYN a la máquina de destino, escriba hping3 -S <Dirección IP de la máquina de destino> -p 80 -c 5 y presione Entrar.



- -S realizará la solicitud TCP SYN en la máquina de destino, -p pasará el tráfico que se asigna a través del puerto asignado, y -c es el recuento de los paquetes enviados a la máquina de destino.

- La captura de pantalla anterior muestra que se enviaron cinco paquetes TCP a través del puerto 80 a la máquina de destino.

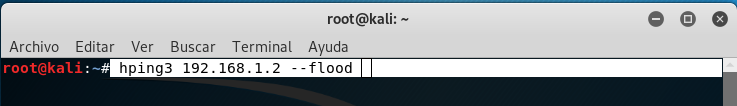
7. Ahora cambie a la máquina de destino (es decir, Windows 7) y observe los paquetes TCP capturados a través de Wireshark.



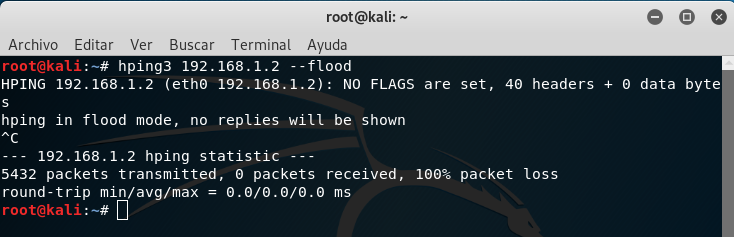
- Ahora reinicie las ventanas de Wireshark en Windows 7 para iniciar la nueva captura.

8. Cambie a la máquina Kali Linux e intente inundar los paquetes TCP a Windows 8.1 (máquina de destino).

- Para inundar los paquetes TCP, escriba hping3 <dirección IP de la máquina de destino> -flood y presione Entrar.



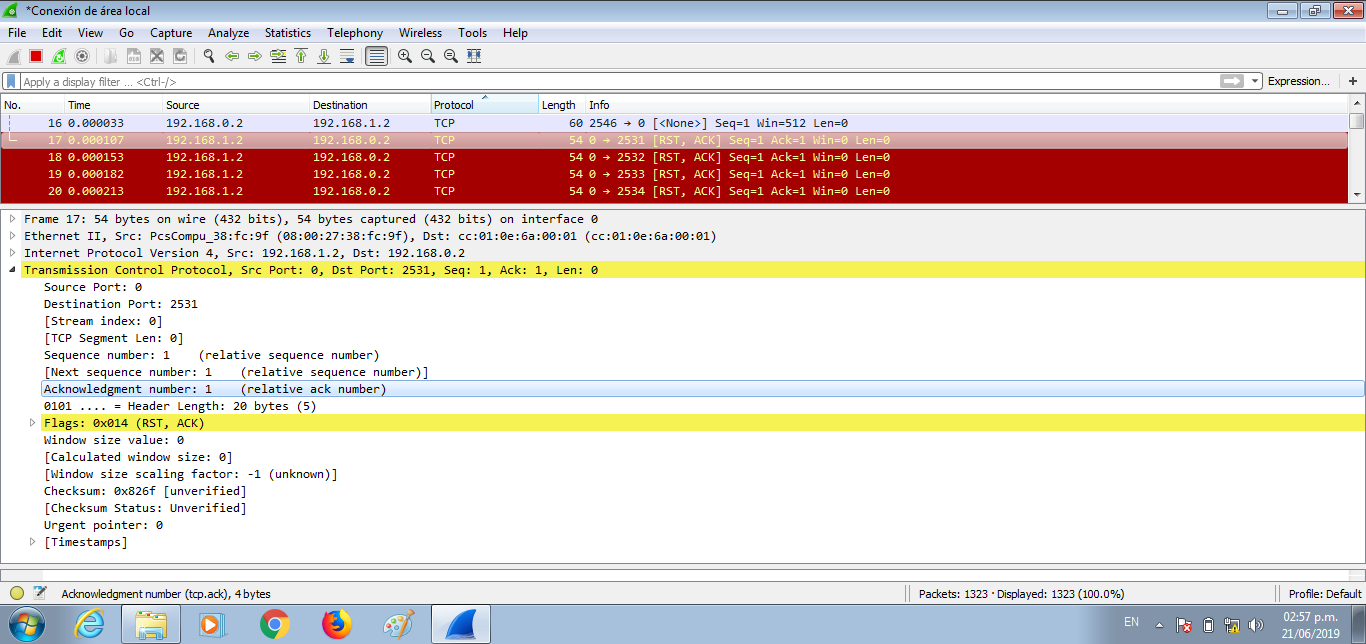
- Una vez que inunde el tráfico a la máquina de destino, responderá en la terminal hping3.



9 Cambie a Windows 7 y observe la ventana de Wireshark, que muestra la inundación de paquetes TCP desde la máquina atacante.

- Haga doble clic en la secuencia de paquetes TCP para observar la información del paquete TCP.





- La secuencia de paquetes TCP muestra la información completa de los paquetes TCP transmitidos a la máquina atacante y los paquetes del receptor.

**Laboratorio 2**

**Escanear la red utilizando el generador de paquetes colasoft.**

**Escenario**

Durante la fase de escaneo de la red, debe realizar un escaneo de la red para detectar hosts en vivo en la red. Como experto en piratas informáticos o probador de penetración, debe conocer las diferentes exploraciones de red utilizando las técnicas de exploración de ping ARP.

**Objetivos de Laboratorio**

El objetivo de este laboratorio es cómo detectar hosts en vivo en la red usando el generador de paquetes Colasoft.

**Entorno de Laboratorio**

En este laboratorio, necesitas:

- Generador de paquetes Colasoft ubicado en D:\CEH-Tools\CEHv9 Module 03 Scanning Networks\Create\ Custom Packet Using TCP Flags\Colasoft Packet Builder

- Una computadora con Windows 7 como máquina anfitriona

- También puede descargar la última versión de colasoft packet builder desde <http://www.colasoft.com/download/products/download_packet_builder.php>

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

- Un navegador web con una conexión a Internet que se ejecuta en la máquina host.

**Descripción general de ARP Ping Scanning**

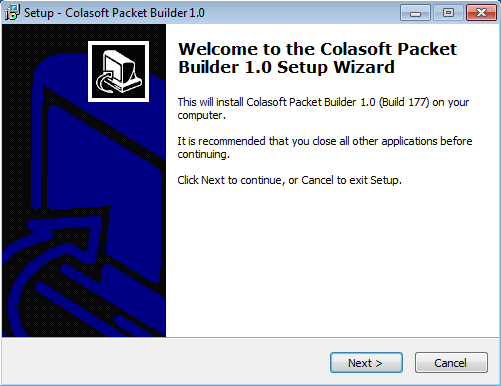
El escaneo ARP ping implica enviar un paquete ARP a los hosts en la red y observar las respuestas que se reciben del host que están activas o activas en la red.

**Tareas de Laboratorio**

1. Navegue a D:\CEH-Tools\CEHv9 Module 03 Scanning Networks\Create Custom Packet Using TCP Flags\Colasoft\ Packet Builder and double-click pktbuilder-1.01.177.exe.

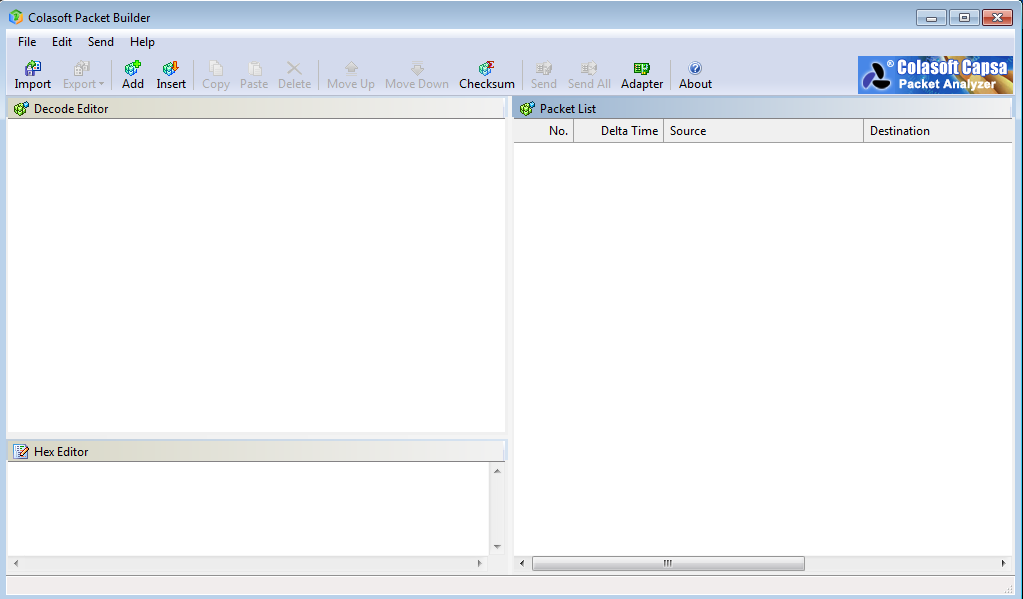
Nota: Si aparece una ventana emergente Abrir archivo - Advertencia de seguridad, haga clic en Ejecutar.

- Siga los pasos de instalación guiados por el asistente para instalar Colasoft Packet Builder.



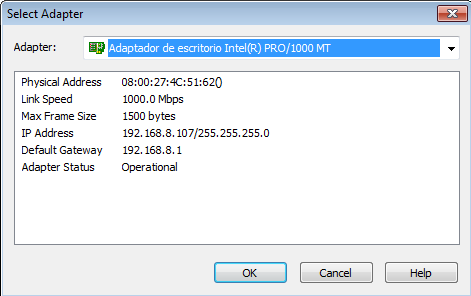
2. Al completar la instalación, inicie la aplicación Colasoft Packet Builder 1.0 desde la pantalla de aplicaciones.

- La GUI del constructor de paquetes colasoft aparece como se muestra en la captura de pantalla.



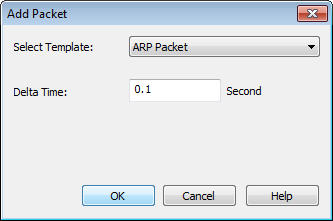
- Antes de comenzar su tarea, haga clic en el icono del adaptador.

- Cuando aparezca la ventana de selección de adaptador, verifique la configuración del adaptador y haga clic en Aceptar.

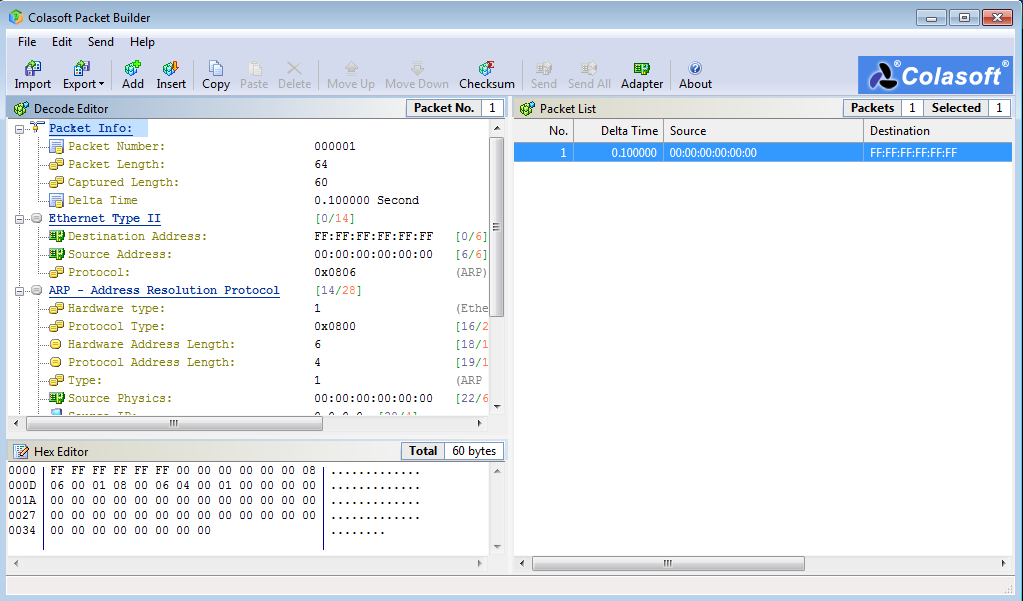


- Para agregar o crear un paquete, haga clic en Agregar icono en la sección del menú.

- En el cuadro de diálogo Agregar paquete, seleccione la plantilla de paquete ARP, establezca el tiempo de Delta en 0,1 segundos y haga clic en Aceptar.

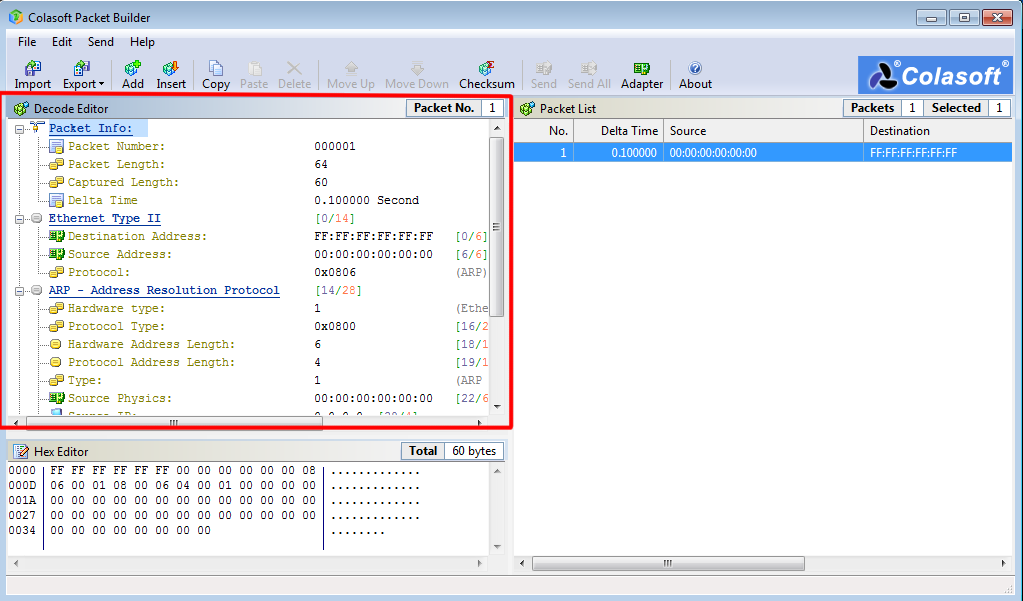


- Puede ver la lista de paquetes agregados en el lado derecho de la ventana, debajo de la Lista de paquetes.

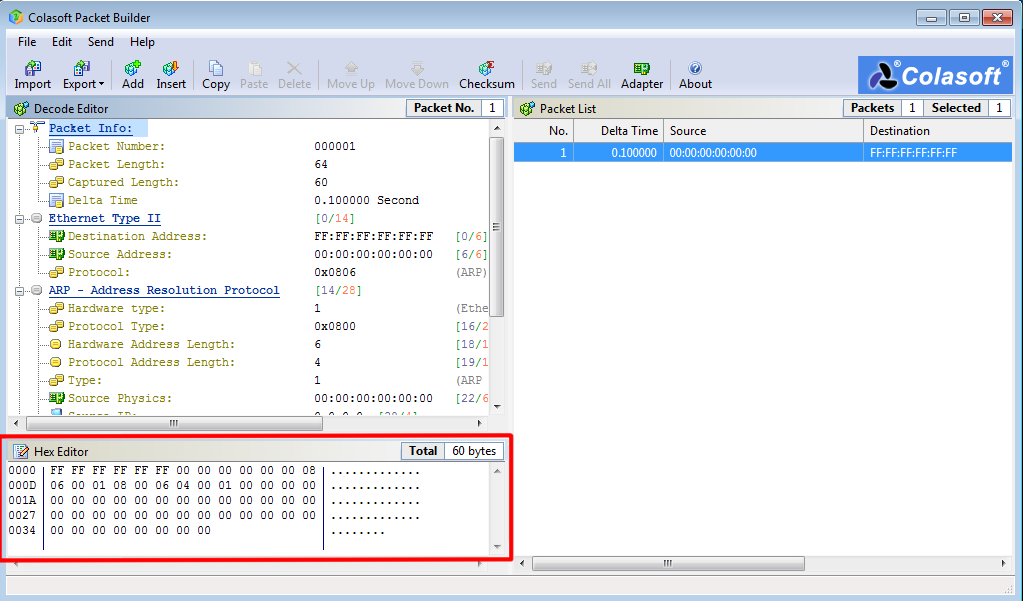


- Colasoft Packet Builder le permite editar la información de decodificación en los dos editores: editor de decodificación y editor hexadecimal, ubicado en el panel izquierdo de la ventana

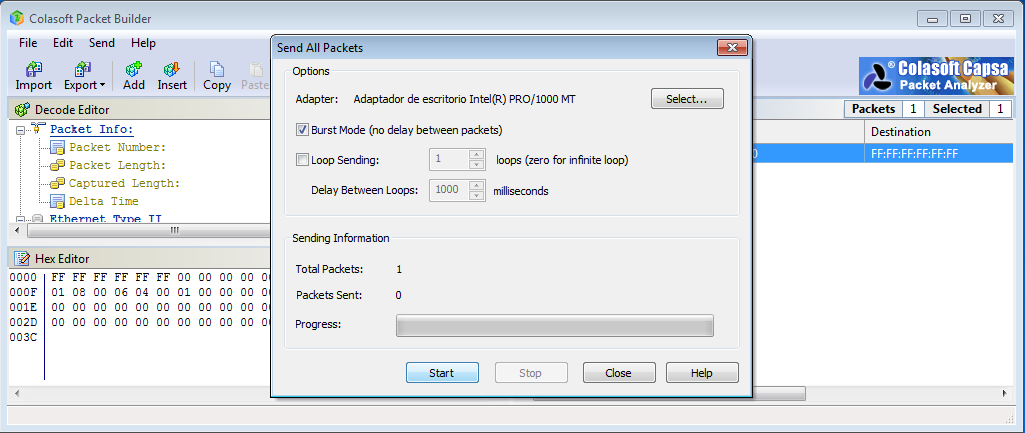
- La sección del editor de decodificación le permite editar la información de decodificación de paquetes haciendo doble clic en el elemento que desea decodificar.



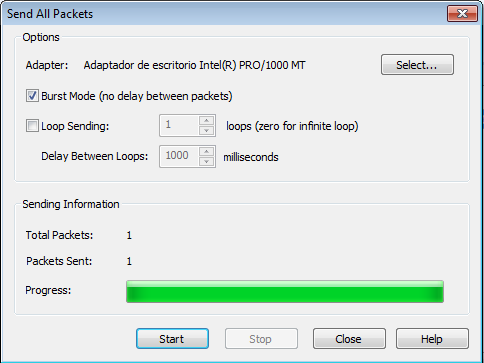
12. El editor Hex muestra el contenido del paquete real en valor hexadecimal sin procesar a la izquierda y su equivalente ASCII.

- Para enviar todos los paquetes a la vez, haga clic en enviar todos desde la barra de menú.

- En la ventana enviar todos los paquetes, marque la opción de modo de ráfaga y luego haga clic en iniciar.



- Cerrar la ventana



- Ahora, cuando este paquete ARP se transmite en la red, las máquinas activas reciben el paquete y algunas de ellas comienzan a responder con una respuesta ARP. Para observar qué máquina está respondiendo al paquete ARP, también debe realizar una aplicación de monitoreo de paquetes como Wireshark o Colasoft Packet capture simultáneamente. Estas aplicaciones registran todos los paquetes que se transmiten en la red.

- Para exportar los paquetes enviados desde el menú de archivo, haga clic en Exportar -> Todos los paquetes.

- En la ventana Guardar como, seleccione una carpeta de destino en el campo Guardar en, especifique el nombre y tipo de archivo y haga clic en Guardar.



- Este archivo guardado puede ser usado para futuras referencias.

**Laboratorio 3**

**Solución de problemas básicos de red utilizando megaping**

**Escenario**

Durante la fase de escaneo de la evaluación de seguridad, no debe limitar sus intentos de escaneo por número o tipo. Es importante probar diferentes herramientas y técnicas para detectar el host de línea y abrir los puertos del sistema. Este laboratorio demostrará cómo detectar hosts en vivo y abrir puertos en la red de destino.

**Objetivos de Laboratorio**

El objetivo de este laboratorio es usar MegaPing para detectar hosts en vivo y abrir puertos de sistemas en la red.

**Entorno de Laboratorio**

Para llevar a cabo este laboratorio, necesitas:

- El megaping se encuentra en D:\CEH-Tools\CEHv9\ Module 03 Scanning Networks\Scanning Tools\MegaPing

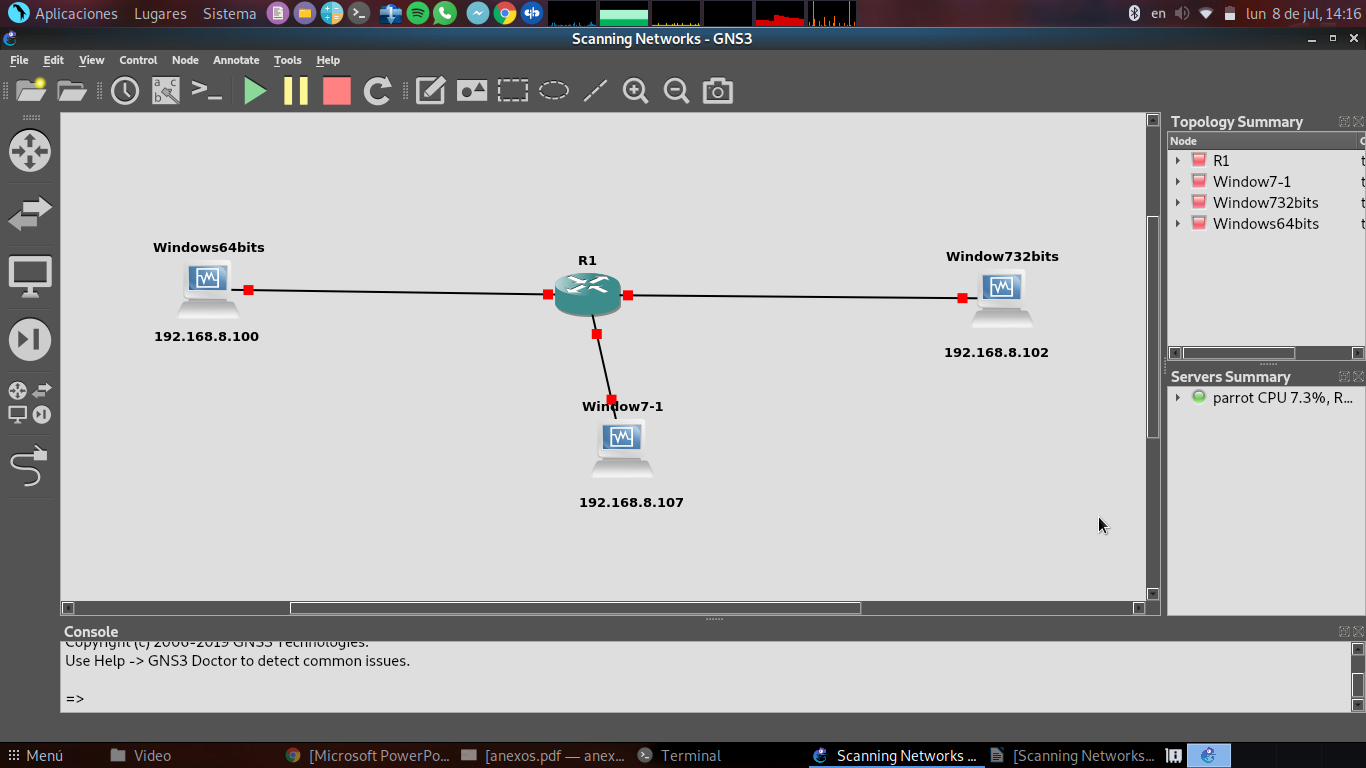
- También puede descargar la última versión de MegaPing desde el enlace <http://www.magnetosoft.com/>

- Si su dispositivo descarga la última versión, las capturas de pantalla que se muestran en el laboratorio pueden diferir.

- Privilegios administrativos para ejecutar herramientas

- Configuración TCP / IP correctamente configurada y un servidor DNS accesible

- Este laboratorio funcionará en el entorno de laboratorio CEH en Windows Server 2012, Windows 2008 y Windows 7



**Resumen de MegaPing**

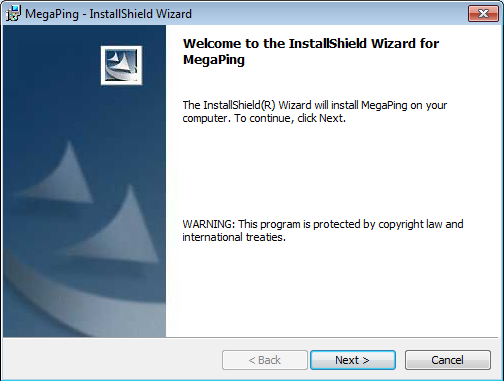
Con la utilidad MegaPing, puede detectar hosts en vivo, abrir puertos del sistema en la red. También puede realizar varias actividades de solución de problemas de red con la ayuda de las utilidades de red integradas, como el nombre de búsqueda de DNS, los hosts de la lista de DNS, Finger, el monitor de host, el escáner de IP, el escáner de NetBios, el sincronizador de tiempo de red, el ping, el escáner de puertos, el escáner de recursos compartidos , traceroute, y WHOIS.

**Tareas de Laboratorio**

1. Antes de comenzar esta práctica de laboratorio, asegúrese de haber iniciado sesión en la máquina virtual de Windows 7.

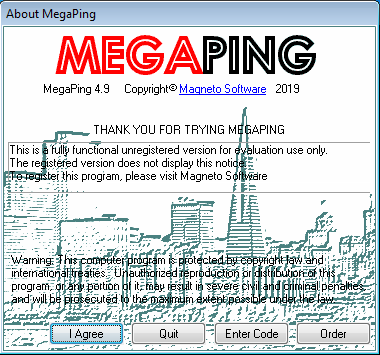
- Vuelva a la máquina host (servidor de Windows 2012), navegue a D: \ CEH-Tools \ CEHv9 Module 03 Scanning Tools\MegaPing y haga doble clic en megaping\_setup.exe

- Siga los pasos de la instalación guiada por el asistente para instalar MegaPing.

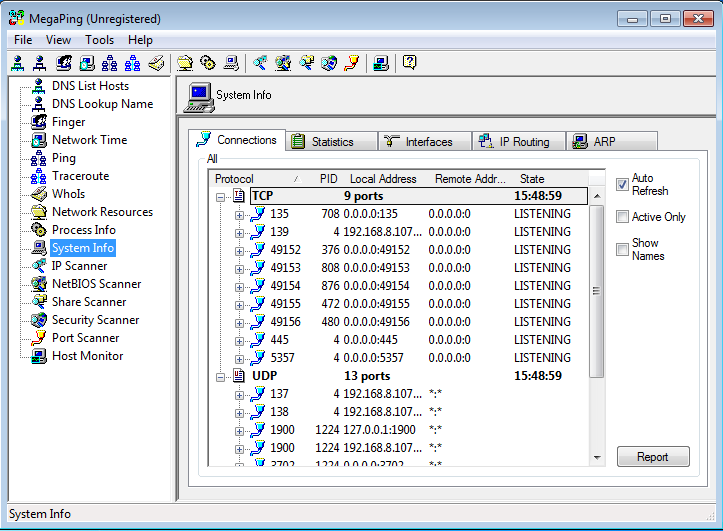


2. Al finalizar la instalación, inicie MegaPing desde la pantalla de aplicaciones.

- Aparece la ventana emergente Acerca de Megaping. Espere hasta que aparezca el botón Acepto y luego haga clic en el botón.



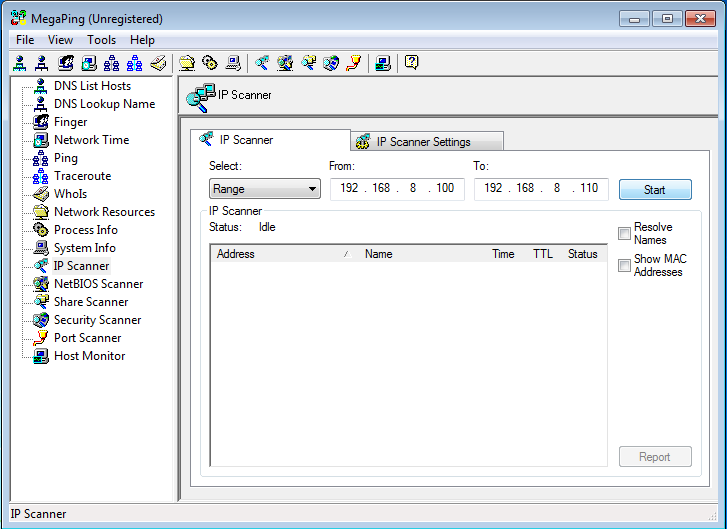
- Aparece la GUI de Megaping (sin registrar) que muestra la información del sistema como se muestra en la siguiente captura de pantalla.

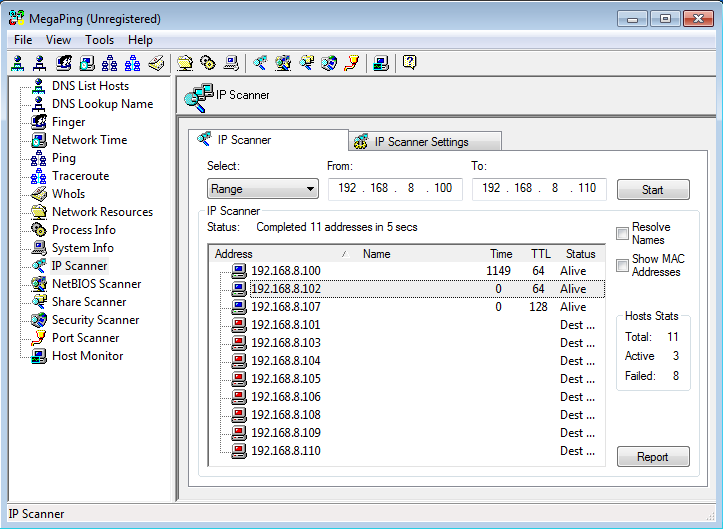
****

- Seleccione cualquiera de las opciones del panel izquierdo de la ventana.

- Por ejemplo, seleccione el escáner de IP, especifique el rango de IP en los campos Desde y hasta, en esta práctica de laboratorio, la IP es de 192.168.8.100 a 192.168.8.10. Haga clic en Inicio.

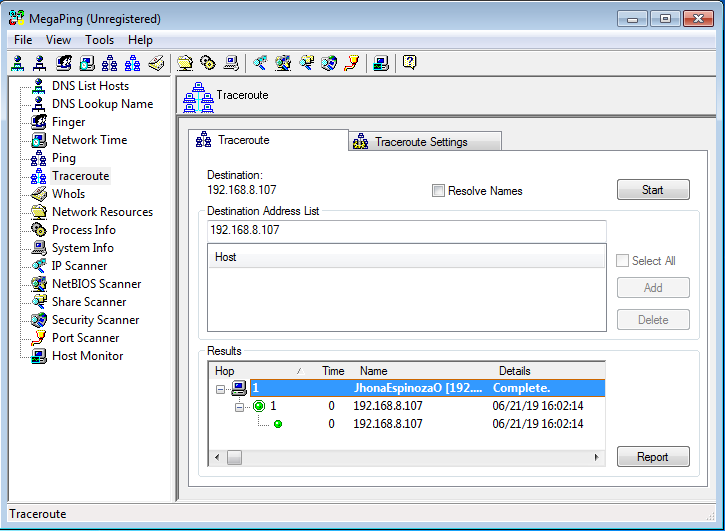
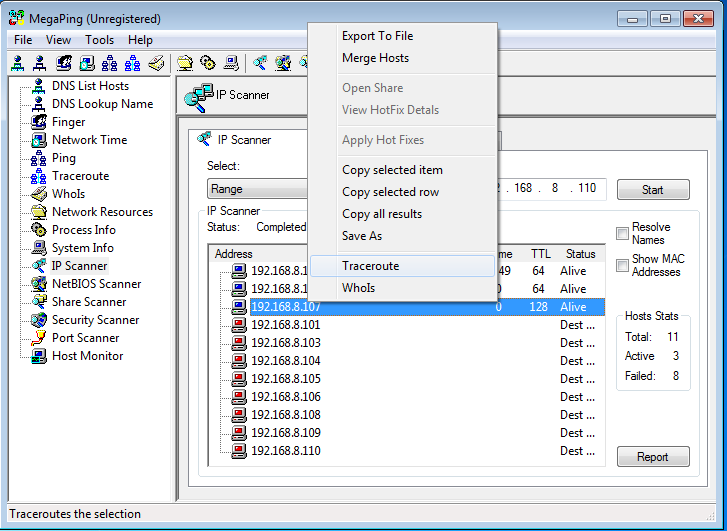
Nota: Puede especificar el rango de IP, dependiendo de su red.



- Megaping enumera todas las direcciones IP dentro del rango objetivo especificado con su TTL (Time-to-Live), Status (muerto o vivo) y estadísticas de los hosts vivos y muertos

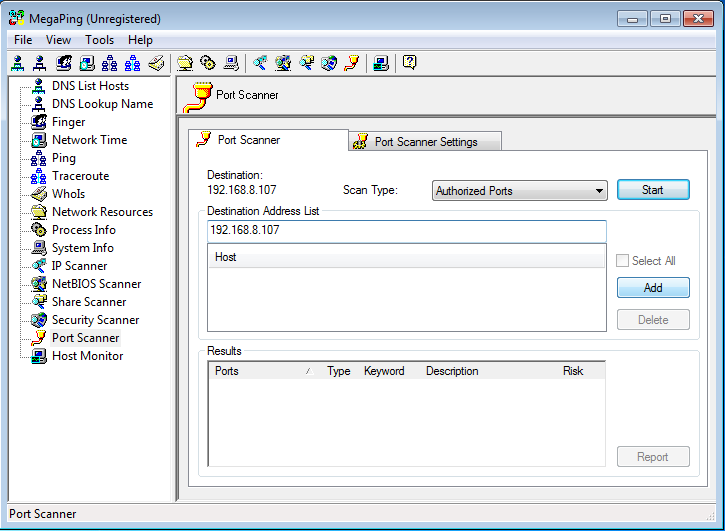
- Haga clic derecho en una dirección IP, y haga clic en traceroute

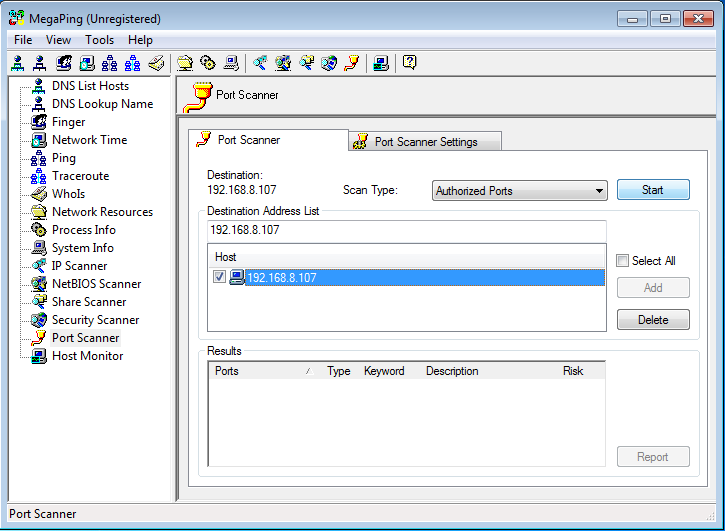
- En esta práctica de laboratorio, se selecciona la dirección IP de Windows 7 (192.168.8.107).

- MegaPing lo redirecciona a la sección Traceroute, mostrando la cantidad de saltos tomados por la máquina host para alcanzar la máquina virtual de Windows 7.

- Seleccione el escáner de puertos en el panel izquierdo.

- Ingrese la dirección IP de la máquina de Windows 7 en la sección de la lista de direcciones de destino y haga clic en agregar. La dirección IP que se indica a continuación puede variar en su entorno de laboratorio.

- Verifique la dirección IP y haga clic en el botón Iniciar para comenzar a escuchar el tráfico el 192.168.8.107.



- MegaPing enumera los puertos asociados con Windows 7, junto con el tipo de puerto, la palabra clave, el número de puerto de riesgo y la descripción, como se muestra en la siguiente captura de pantalla

**Laboratorio 4**

**Entendiendo el escaneo en red usando Nmap**

**Escenario**

Nmap es una utilidad de escaneo en red que la mayoría de los profesionales de seguridad utiliza durante su tarea de evaluación de seguridad. Es compatible con varios tipos de técnicas de escaneo de red. Durante su evaluación de seguridad, se le pedirá que realice una exploración de red utilizando Nmap. Por lo tanto, como hacker ético profesional o probador de penetración, debería poder realizar un escaneo de red utilizando Nmap. Este laboratorio le mostrará cómo realizar el escaneo en red usando Nmap.

**Objetivos de Laboratorio**

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

- Escanear una subred entera.

- Rastrea todos los paquetes enviados y recibidos.

- Realizar una exploración completa lenta.

- Crear un nuevo perfil para realizar un escaneo nulo.

- Escanear puertos TCP y UDP.

- Analizar los detalles del host y su topología.

**Entorno de laboratorio**

Para realizar el laboratorio, necesitas:

- Nmap, ubicado en: D:\CEH-Tools\CEHv9 Module 03 Scanning Networks\Scanning Tools\Nmap. Tu puedes descargar la version mas actual de Nmap en el enlace [http://nmap.org](http://nmap.org/). Si decide descargar la última versión, las capturas de pantalla que se muestran en el laboratorio pueden diferir.

- Una computadora que ejecuta Windows como máquina host.

- Windows ejecutándose en una máquina virtual.

- Ubuntu ejecutándose en una máquina virtual

- Un navegador web con acceso a internet.

- Privilegios administrativos para ejecutar la herramienta Nmap

**Resumen de Nmap**

Nmap es una utilidad utilizada para el descubrimiento de redes, la administración y la auditoría de seguridad. También se utiliza para tareas como el inventario de la red, la administración de los programas de actualización del servicio y el monitoreo del tiempo de actividad del host o del servidor.

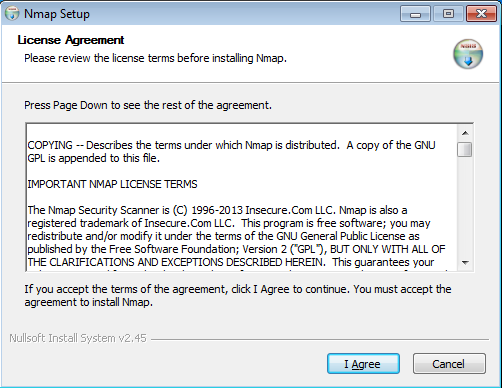
**Tareas de Laboratorio**

1. Inicie sesión en una o más máquinas virtuales. En esta tarea de laboratorio, hemos utilizado Windows 8 y Windows server 2008.

- Cambie a la máquina host de Windows Server 2012 y navegue a D:\CEH-Tools\CEHv9 Module 03 Scanning Networks\Scanning Tools\Nmap; luego haga doble click nmap-6.40-setup.exe

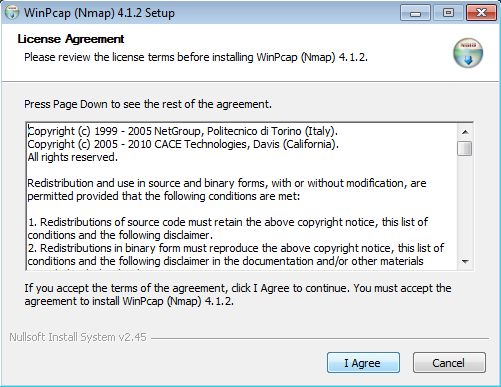
- Si aparece un archivo abierto -> emergente de advertencia de seguridad, haga clic en ejecutar.

- En la ventana de configuración de Nmap, haga clic en Acepto y siga los pasos de instalación para instalar Nmap utilizando todos los valores predeterminados.



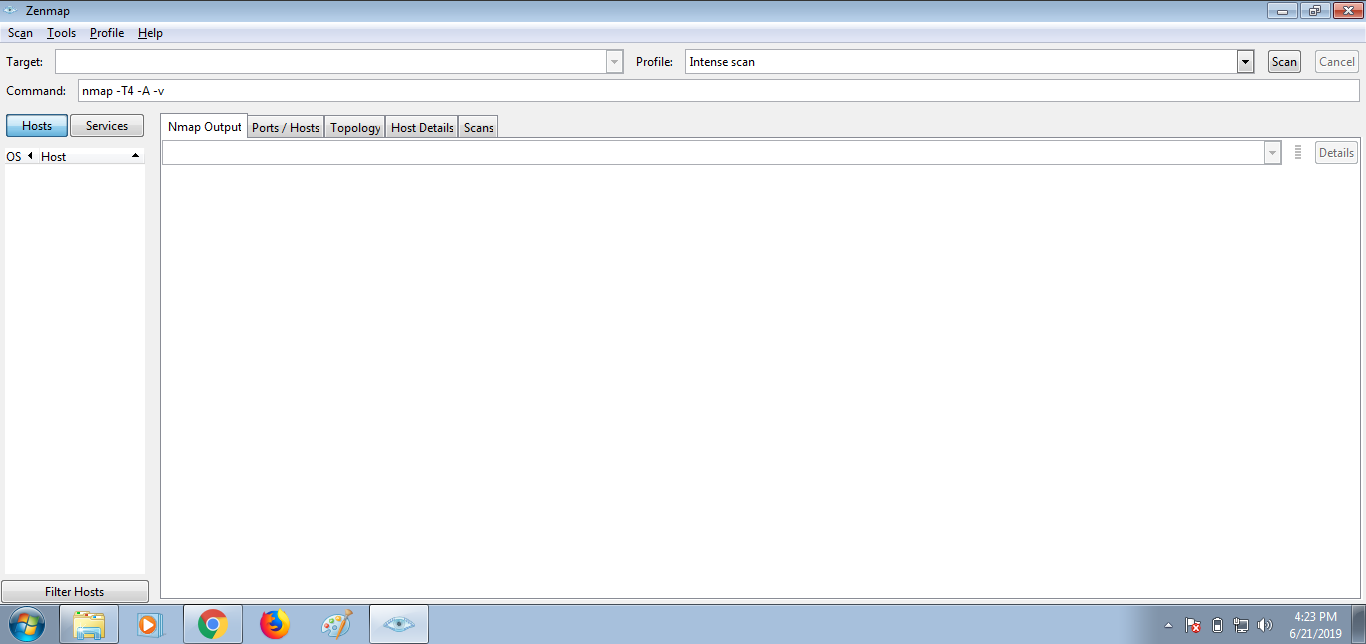
- En el momento de la instalación, aparece una ventana emergente de configuración de WinPcap. Si ya está instalada una versión superior de WinPcap, haga clic en no y siga los pasos de instalación guiados por el asistente para instalar Nmap.

Nota: Si instaló WinPcap anteriormente, haga clic en Sí para instalarlo.

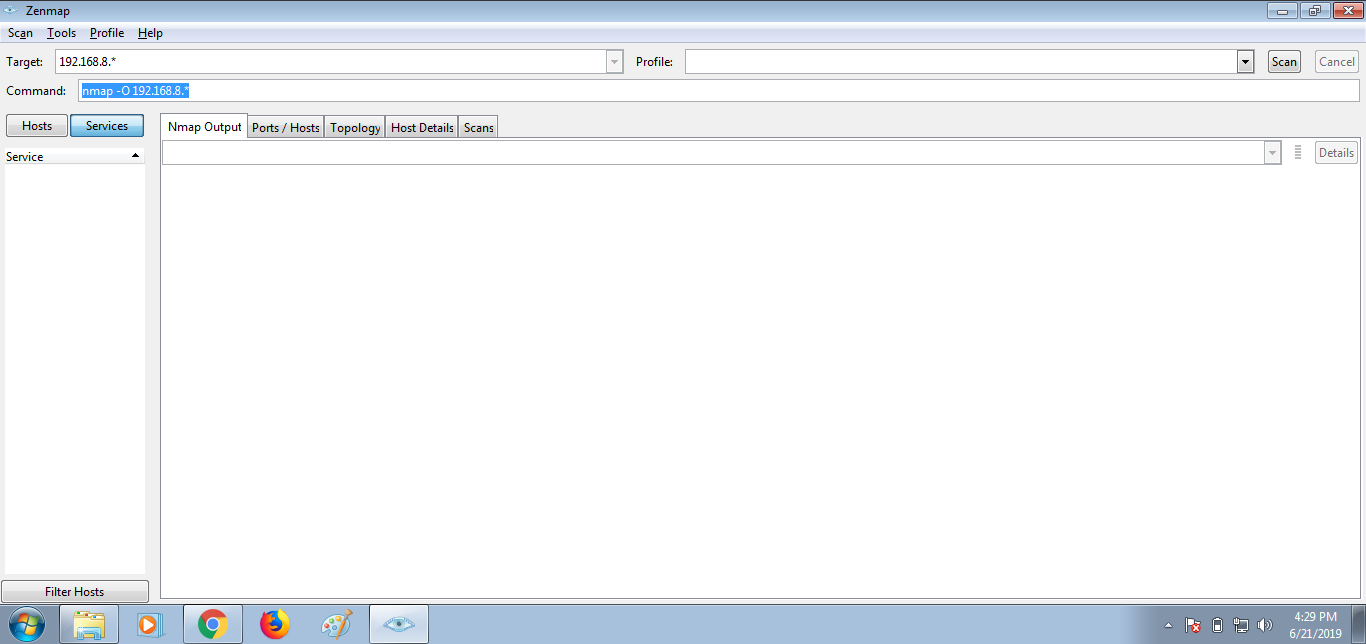


- Al finalizar la instalación, inicie la aplicación GUI de Nmap-Zenmap desde la pantalla de aplicaciones. Puede presionar la tecla "Windows" para acceder a la pantalla principal de Windows para el servidor 2012.

2. La GUI de Nmap-Zenmap aparece con el perfil Intense sean configurado de forma predeterminada.

- En el campo de comando, escriba el comando nmap -O seguido del rango de direcciones IP. En esta práctica de laboratorio, es 192.168.8. \*. Al proporcionar el comodín '\*' (asterisco), puede escanear una subred completa o rango de IP con Nmap para descubrir hosts activos.

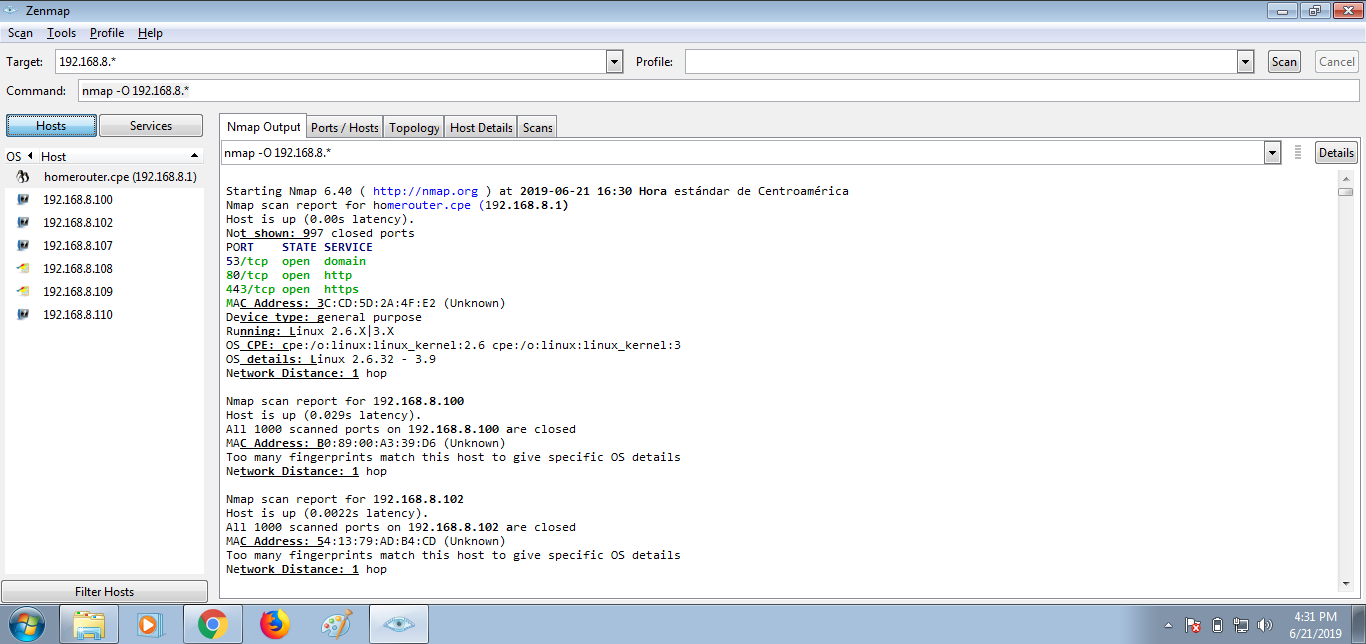
Nota: Este rango puede diferir en su entorno de laboratorio.

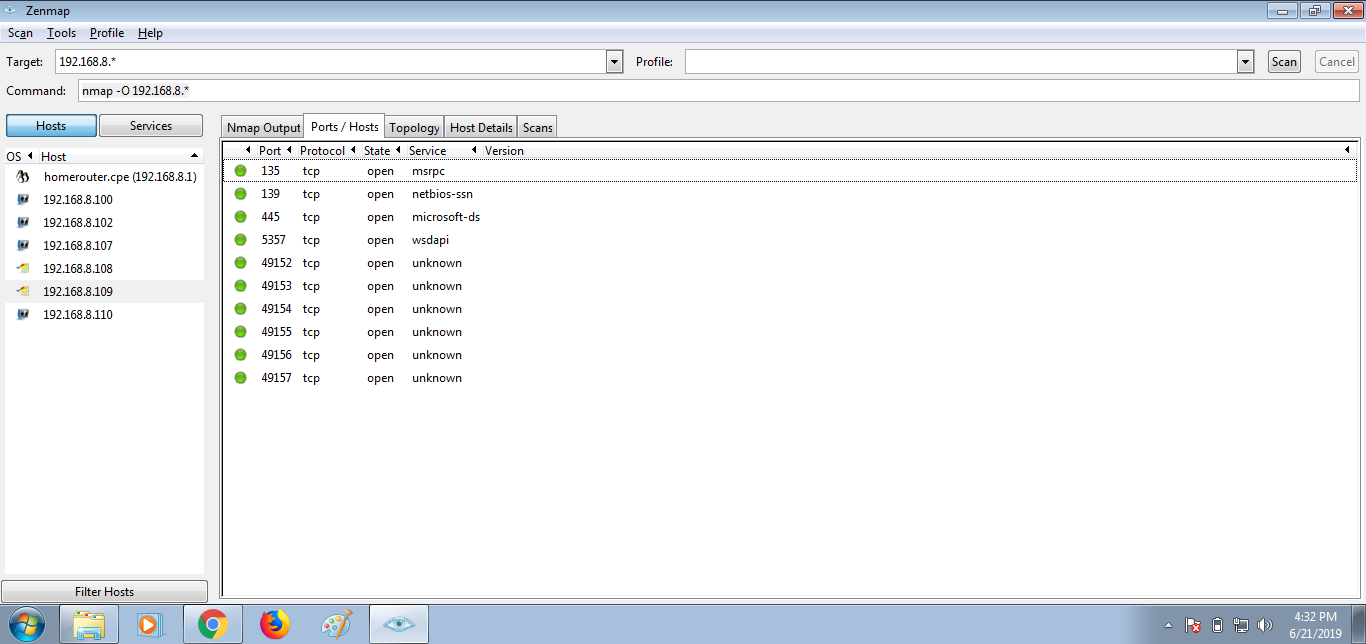
- Haga clic en Escanear para comenzar a escanear las máquinas virtuales.

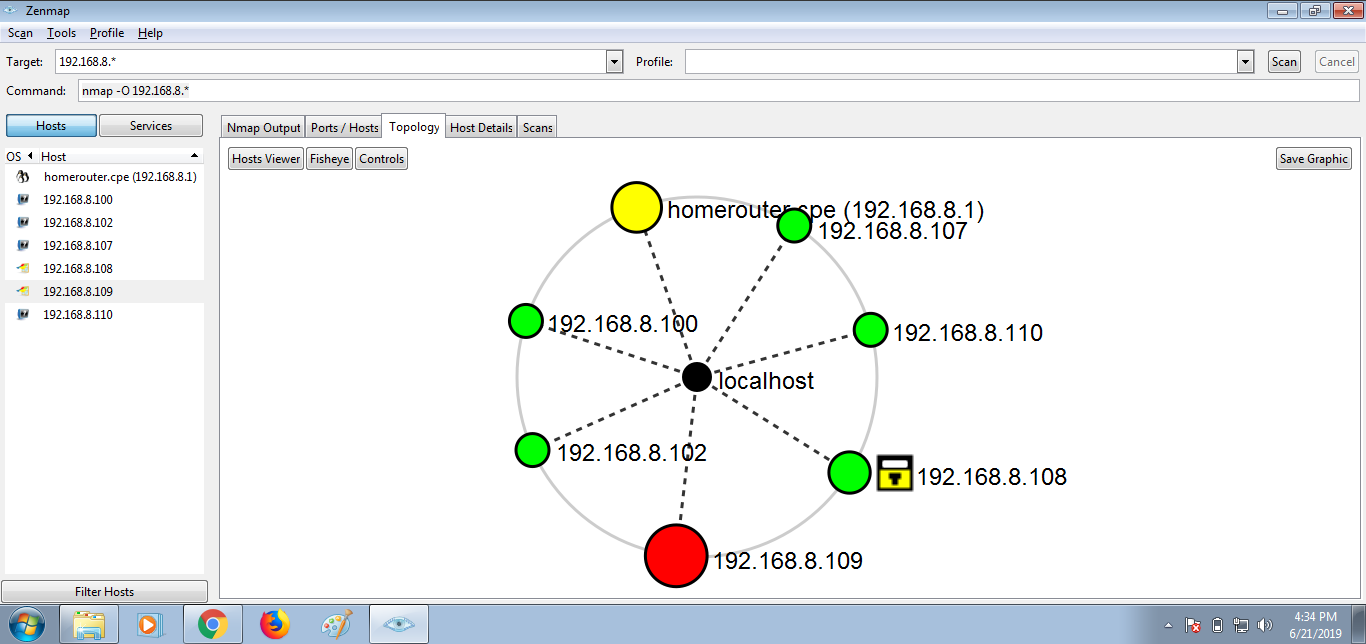
- Nmap escanea toda la red y muestra información de todos los hosts que se escanearon, junto con los puertos abiertos, el tipo de dispositivo, los detalles del sistema operativo, etc.

Nota: Los resultados devueltos por Nmap pueden variar en su entorno de laboratorio.

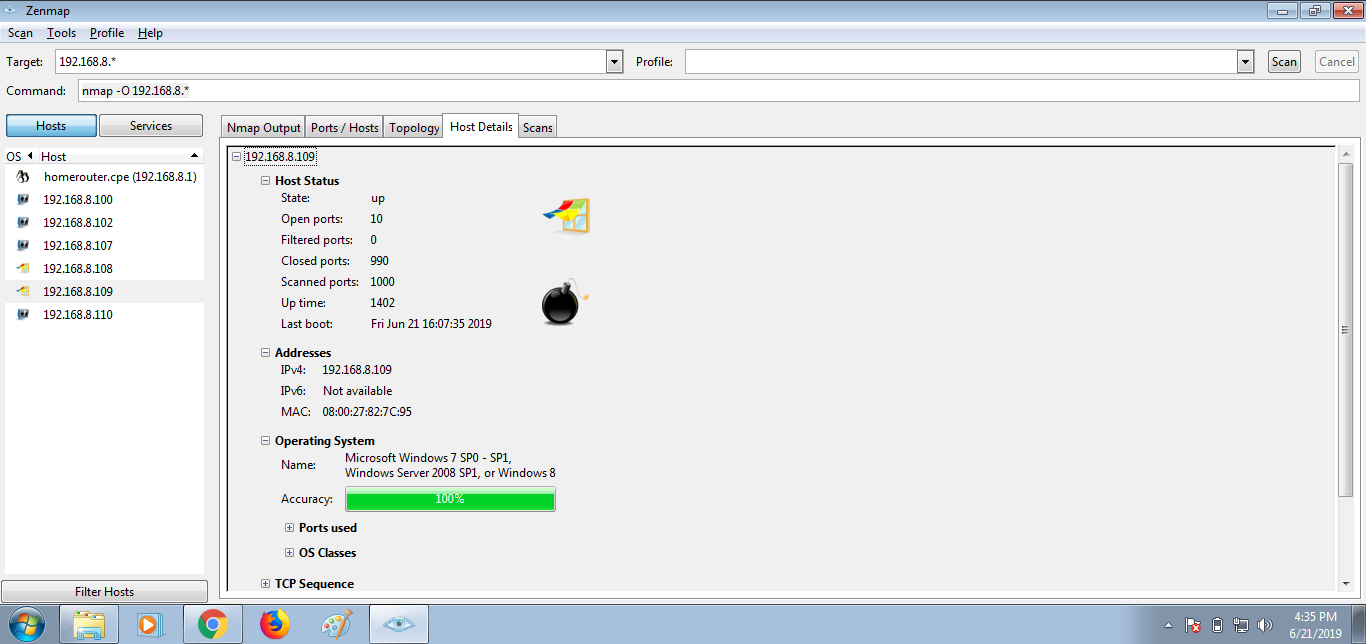
- Desplácese hacia abajo en la ventana o seleccione la dirección IP de un host de la lista de hosts en el panel izquierdo para ver sus detalles.

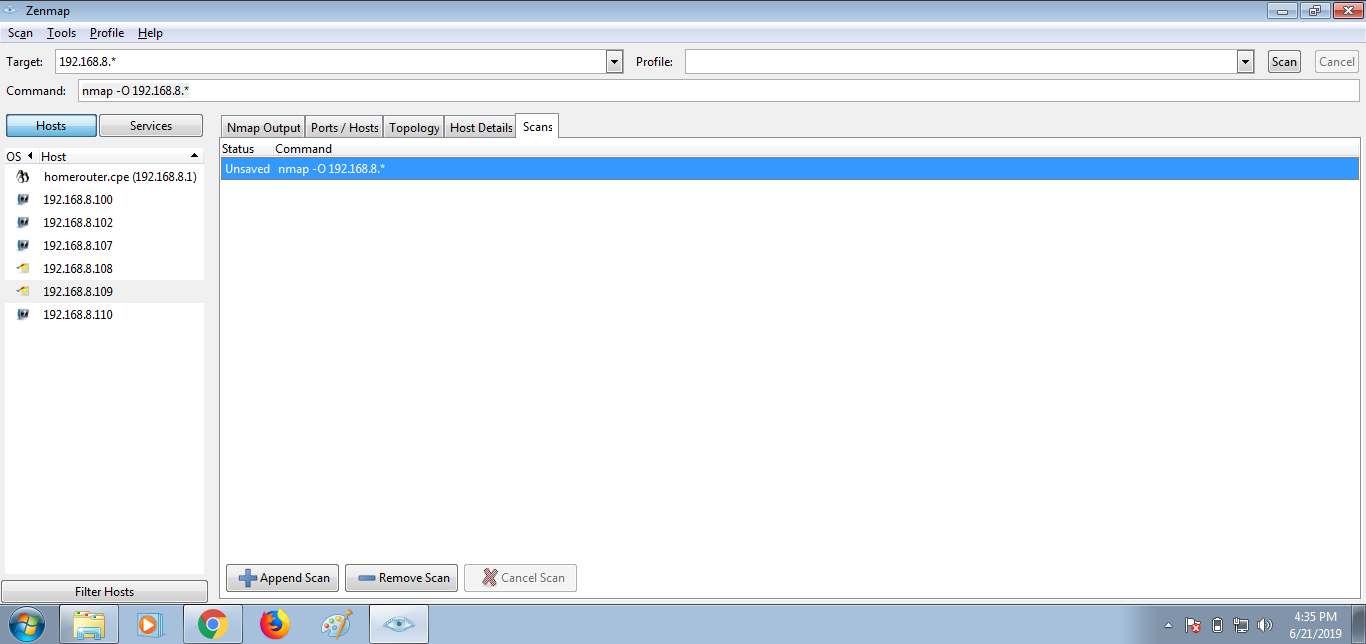
- Haga clic en la pestaña puertos / hosts y elija la dirección IP de un host (aquí se ha seleccionado 192.168.8.109) en el panel izquierdo para ver todos los puertos abiertos asociados con el host seleccionado.

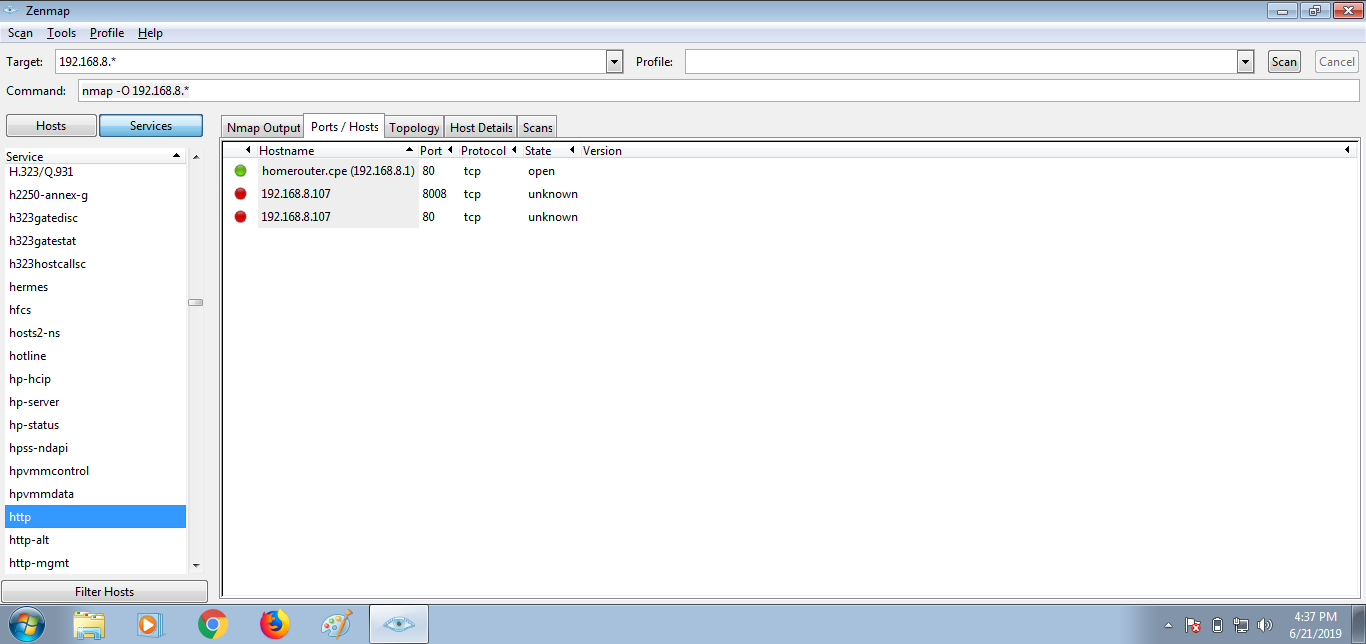
- Un atacante podría intentar establecer una conexión a través de cualquiera de estos puertos abiertos explotando cualquier vulnerabilidad (si se encuentra) en un servicio en ejecución.

- Haga clic en la pestaña de topología para ver la topología de la red de destino que contiene la dirección IP de destino.

- Haga clic en el extremo de la pestaña de detalles del host y seleccione la dirección IP de un host (aquí 10.0.0.10) para ver los detalles del host que se descubrió durante el análisis.

- Haga clic en la pestaña de escaneos para ver el estado del escaneo.

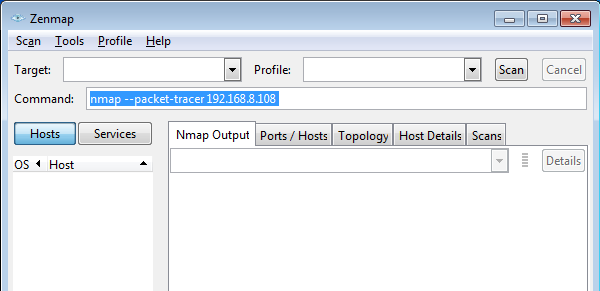
- Haga clic en la pestaña de servicio y seleccione cada servicio (aquí se ha elegido http) para enumerar todos los puertos en los que se está ejecutando el servicio, su estado (abierto / cerrado / desconocido), versión, etc.



- Una vez que se realiza la exploración, finalice la exploración y salga de la aplicación Nmap.

3. Inicia Nmap desde la pantalla de aplicaciones.

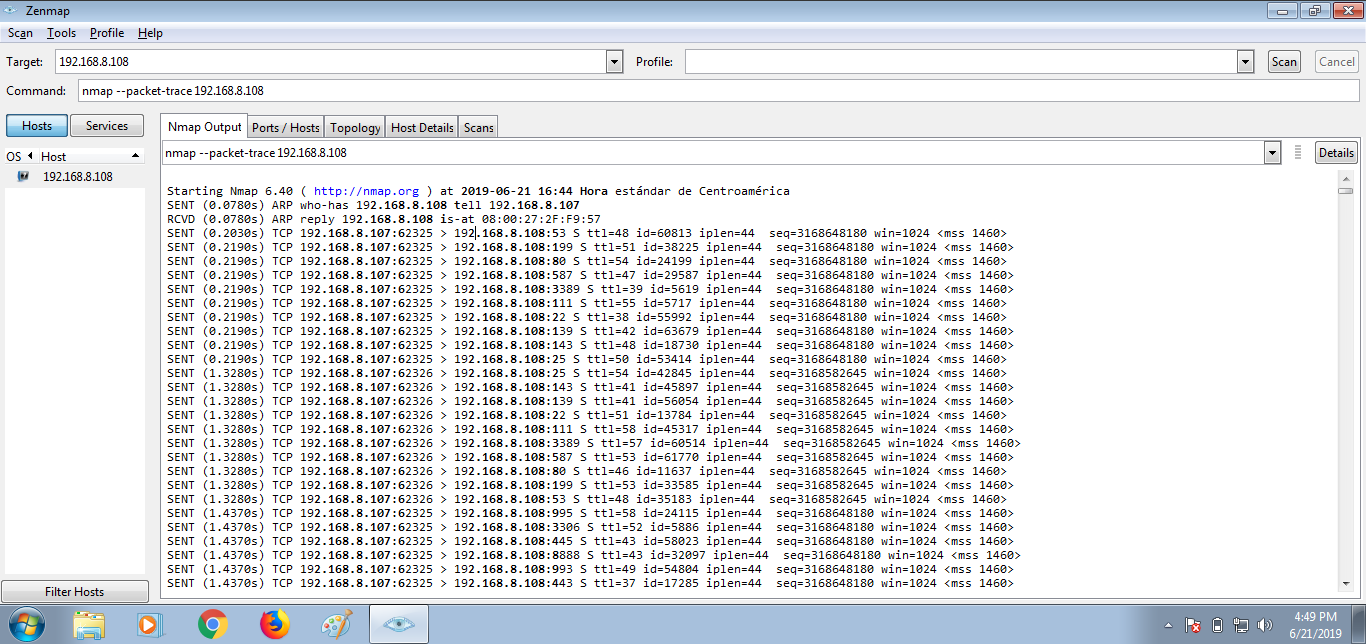
- En el campo de comando, escriba el comando nmap -packet-trace seguido de la dirección IP de la máquina de destino (es decir, 192.168.8.108).

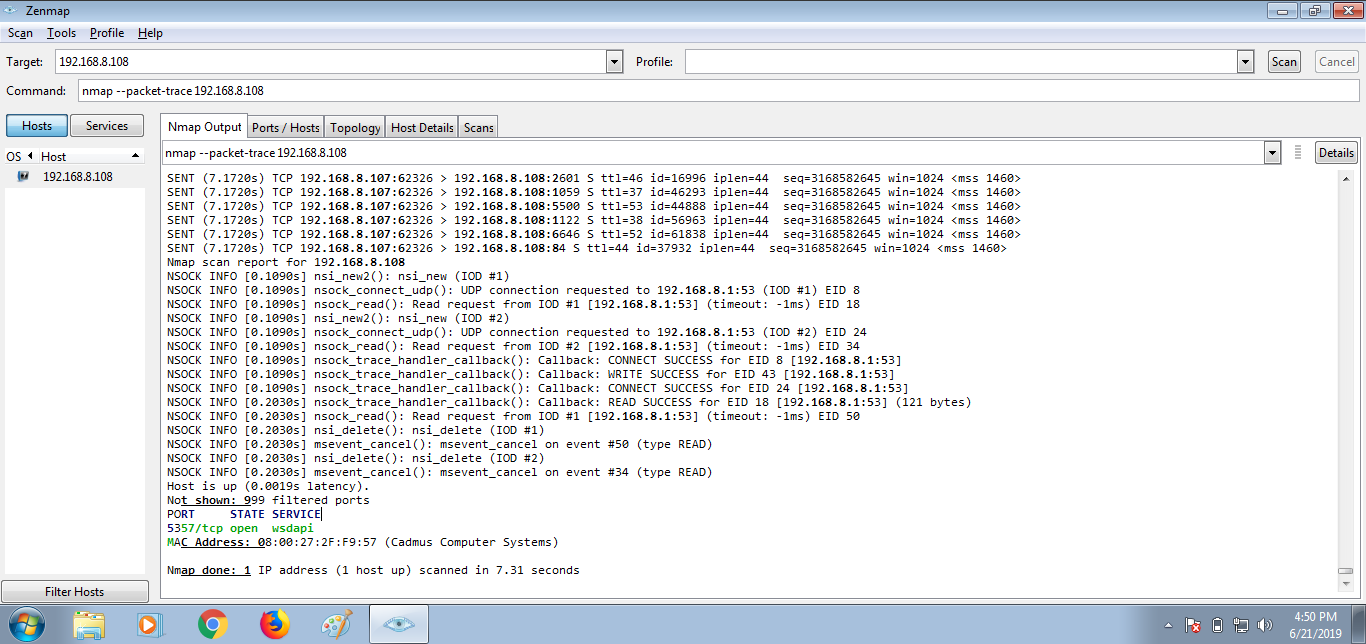


- Está realizando un inventario de red para la máquina virtual.

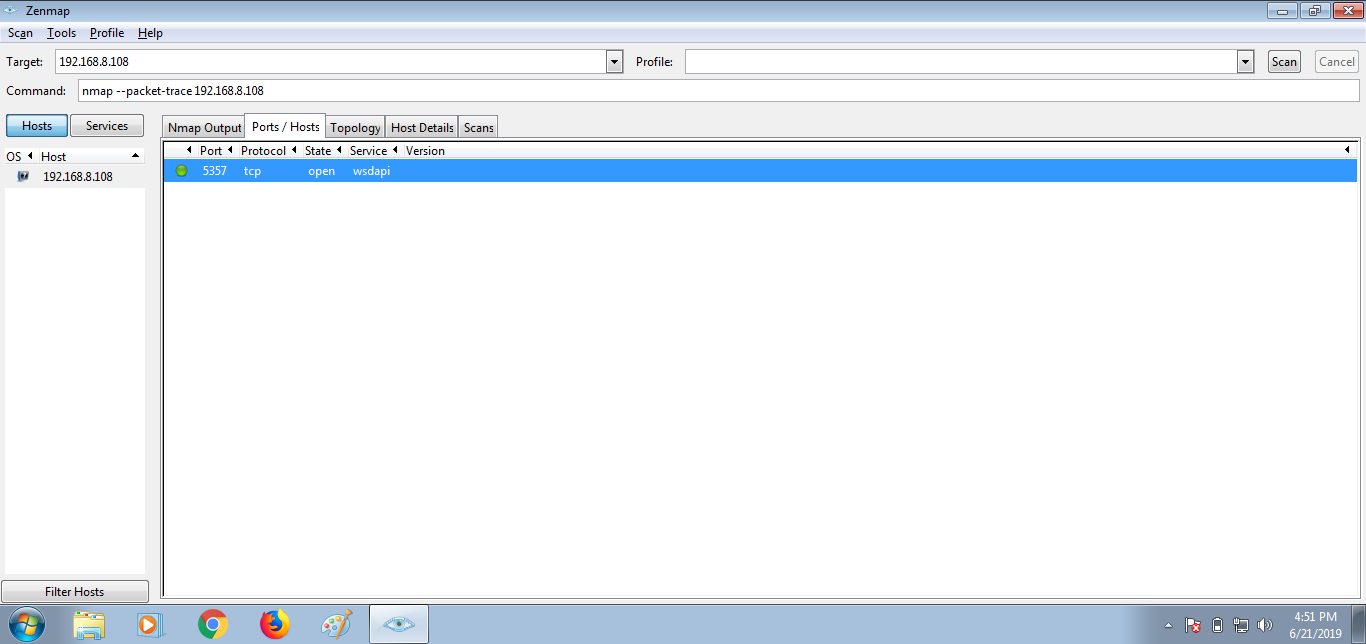
- Haga clic en escanear para comenzar a escanear la máquina virtual.

- Al emitir el comando packet-trace, Nmap envía algunos paquetes a la máquina intencionada y recibe paquetes en respuesta a los paquetes enviados. Imprime un resumen de cada paquete que envía y recibe.

- La siguiente captura de pantalla muestra los paquetes enviados desde el host al destino y los paquetes recibidos del destino al host que se muestran en la pestaña Salida de Nmap en Nmap:

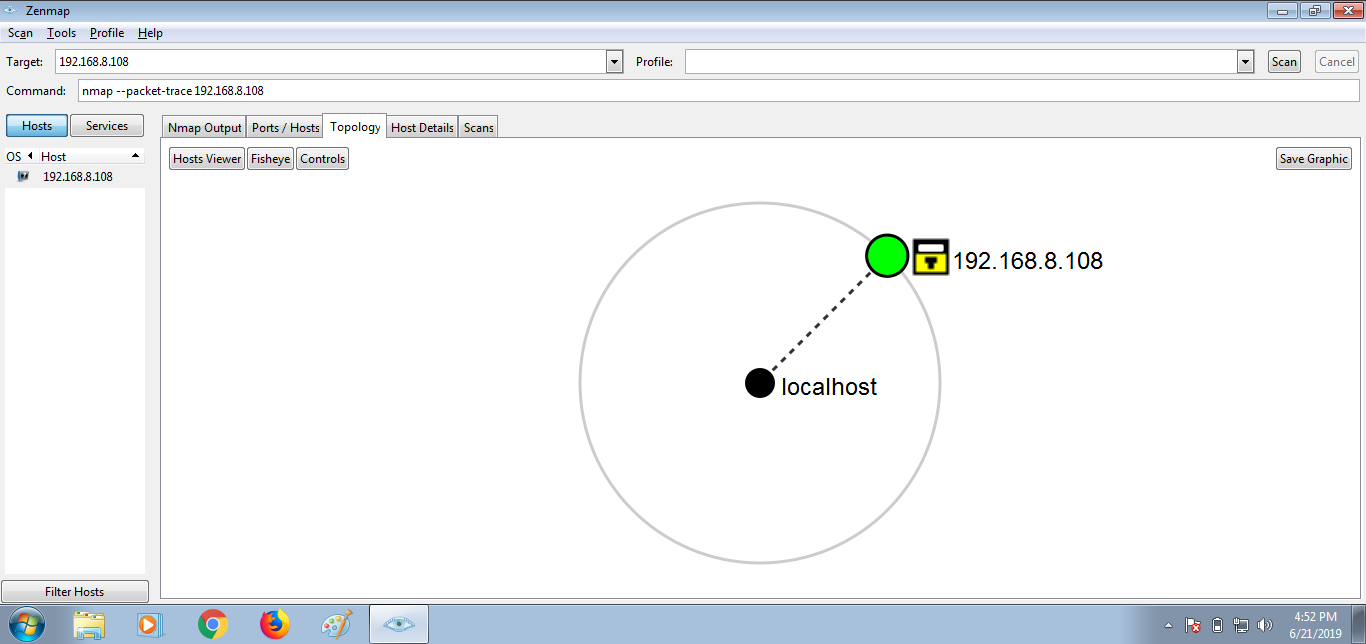
- Desplácese hacia abajo de la ventana para ver los puertos TCP abiertos.

- Haga clic en la pestaña Puertos / Hosts para mostrar más información sobre los resultados del análisis.

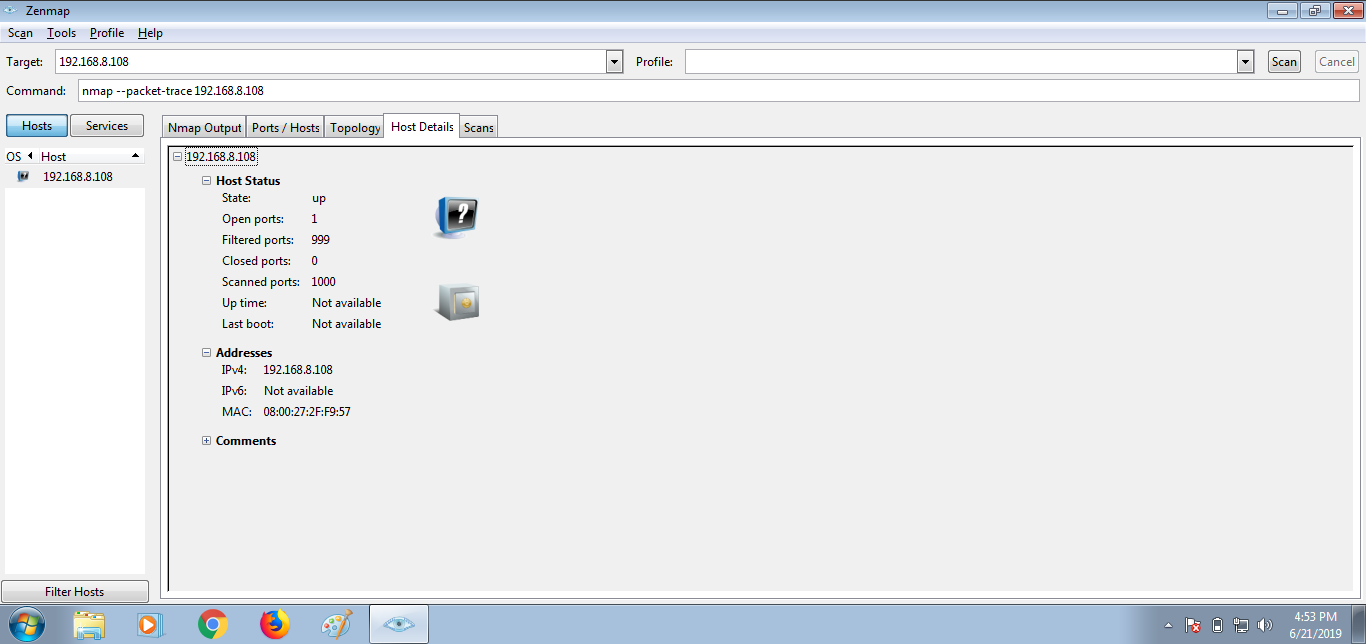


- Nmap muestra el puerto, el protocolo, el estado, el servicio y la versión del escaneo. Aquí, como puede observar, se ha encontrado más número de puertos abiertos en comparación con el análisis anterior.

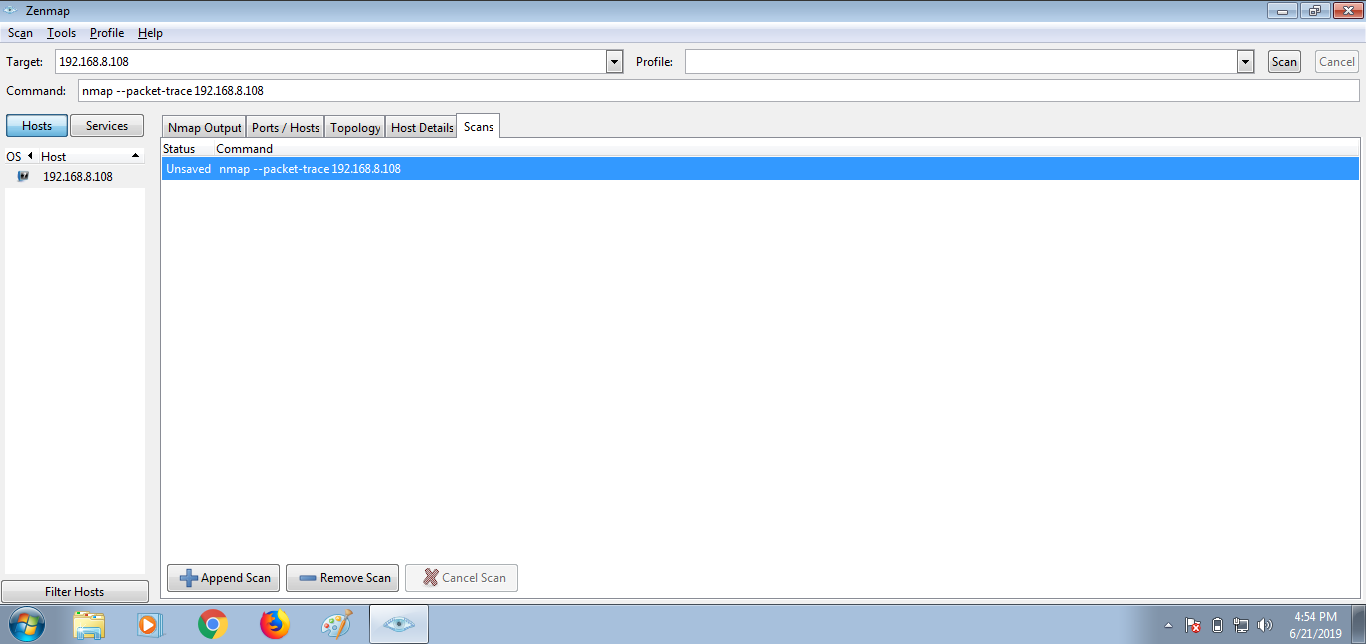
- Haga clic en la pestaña Topología para ver la topología de la red de destino que contiene la dirección IP proporcionada.

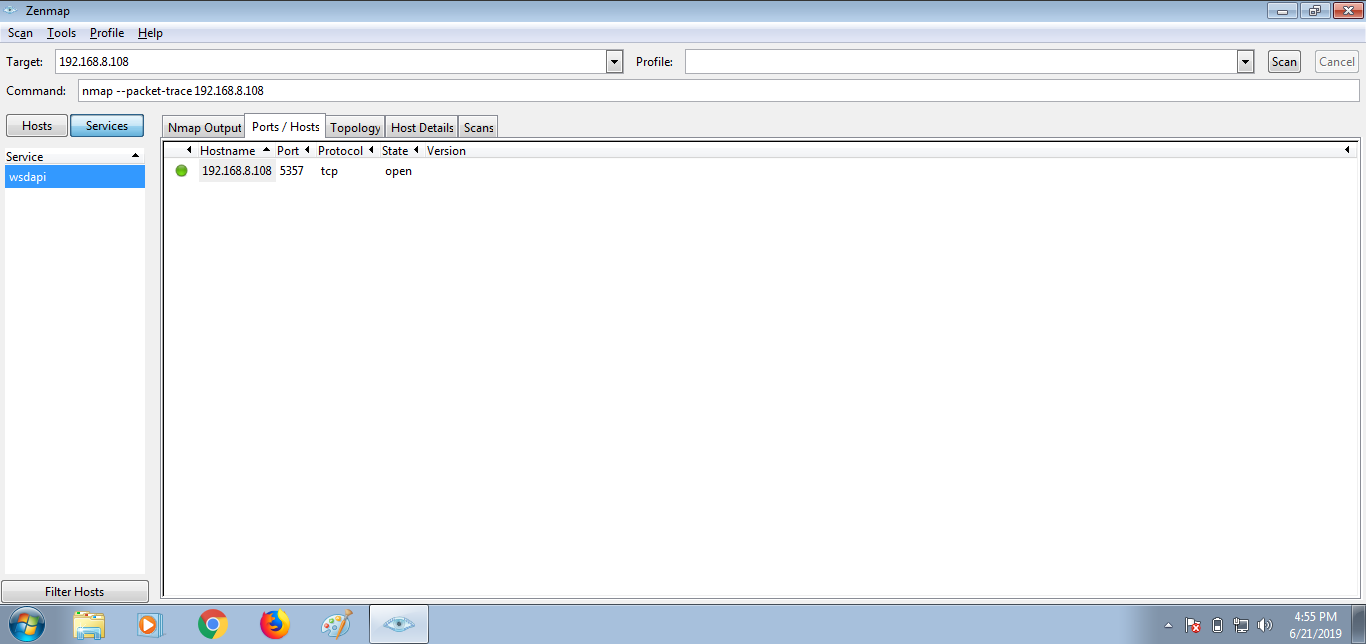


- De la misma manera, haga clic en la pestaña de detalles del host para ver los detalles de todos los hosts descubiertos durante el perfil intenso.



- Haga clic en la pestaña de escaneados para ver el estado del escaneo y el comando utilizado.

- Haga clic en la pestaña de servicios ubicada en el panel derecho de las ventanas. Esta pestaña muestra la lista de servicios.



- Un atacante usa cualquiera de estos servicios y sus puertos abiertos para ingresar a la red / host objetivo y establecer una conexión.

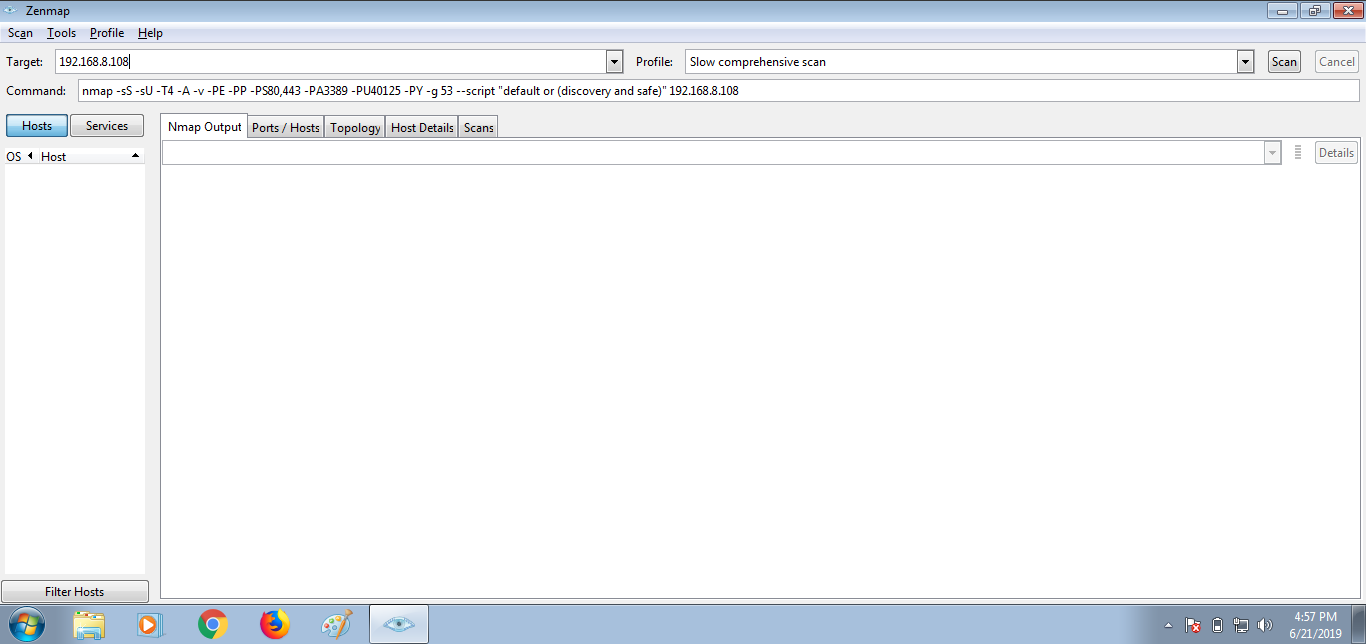
- Una vez que se realiza la exploración, puede terminar Nmap.

4. La exploración completa y lenta utiliza tres protocolos diferentes, TCP, UDP y SCTP, y ayuda a determinar qué sistema operativo, servicios y versiones está ejecutando el host de acuerdo con los servicios TCP y UDP más comunes.

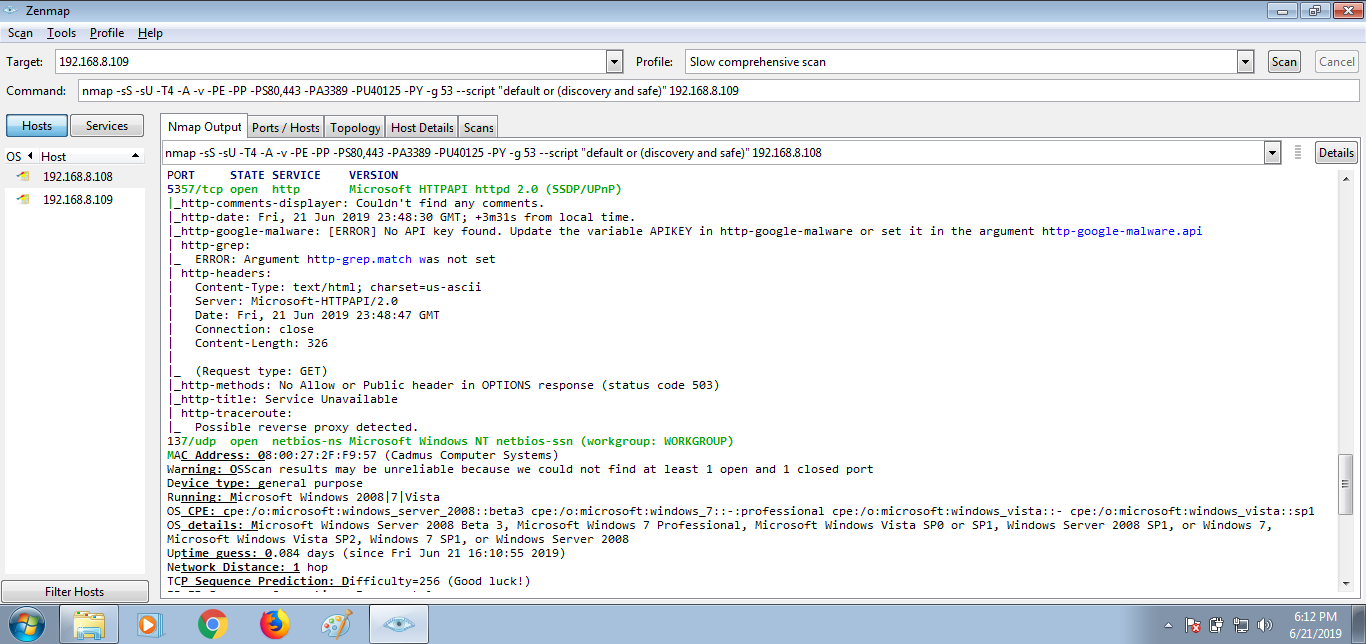
- Es simplemente un escaneo intenso que utiliza el protocolo UDP además de algunas opciones de escaneo más. Esta exploración se realiza en un intento de rastrear las máquinas en una red, incluso si están configuradas para bloquear. Peticiones de ping.

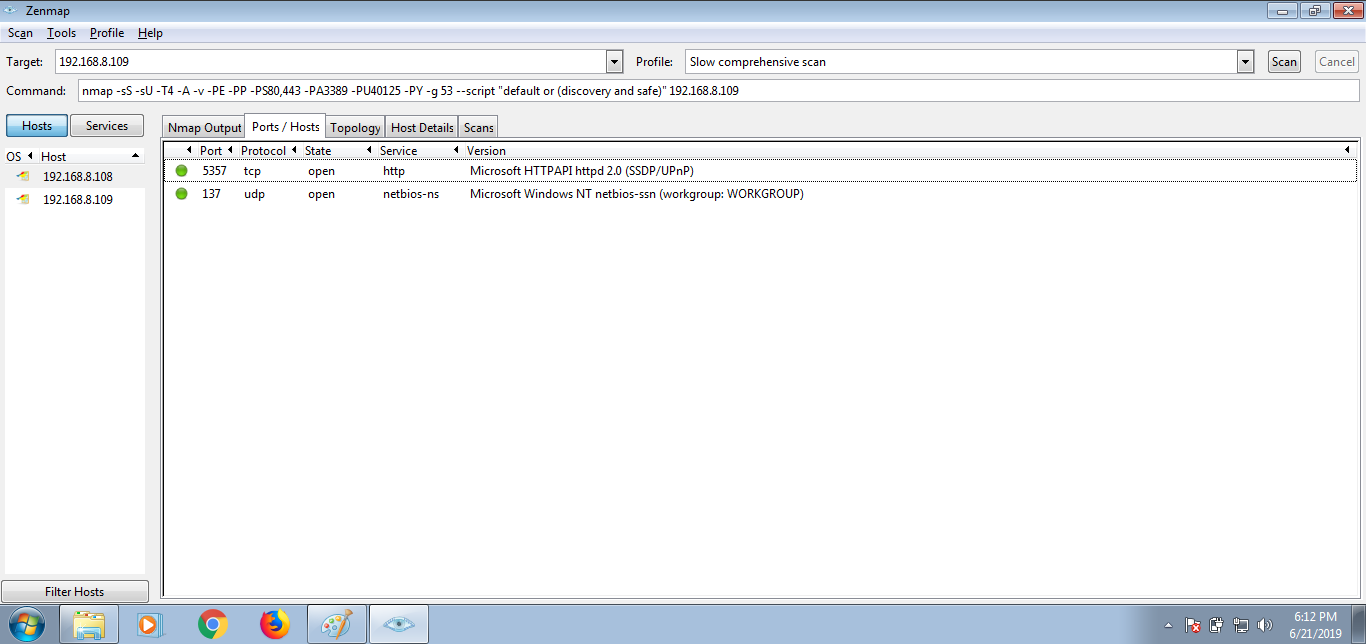
- Inicia Nmap desde la pantalla de aplicaciones.

- Ingrese la dirección IP de Windows 8.1 (192.168.8.108) en el campo Destino, seleccione Exploración exhaustiva lenta en la lista desplegable del perfil y haga clic en Explorar.

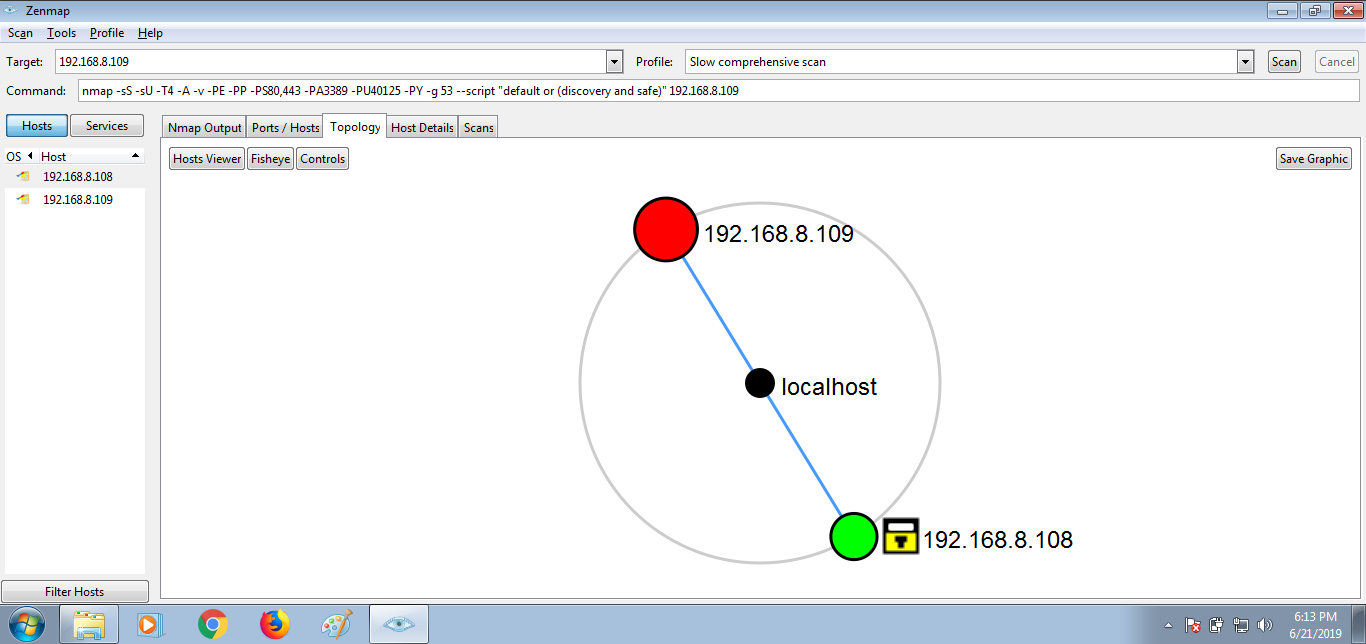


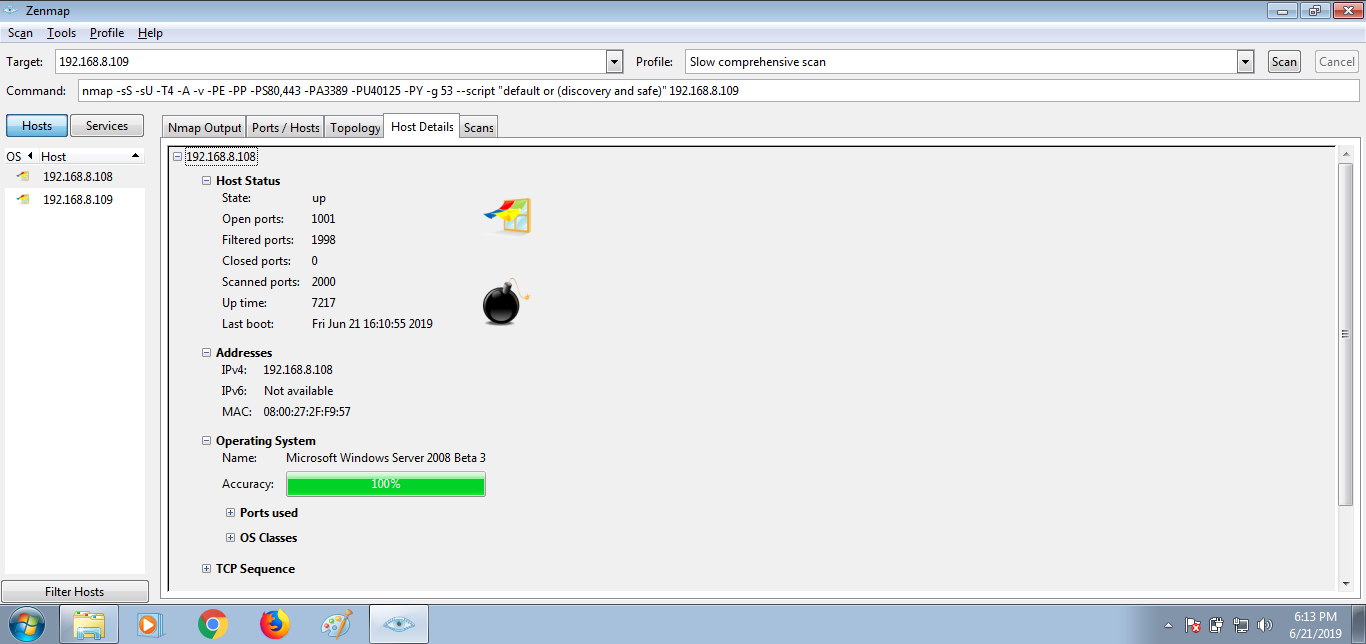
- Nmap escanea la dirección IP de destino con un escaneo lento y completo y muestra los resultados del escaneo en la pestaña de resultados de Nmap.

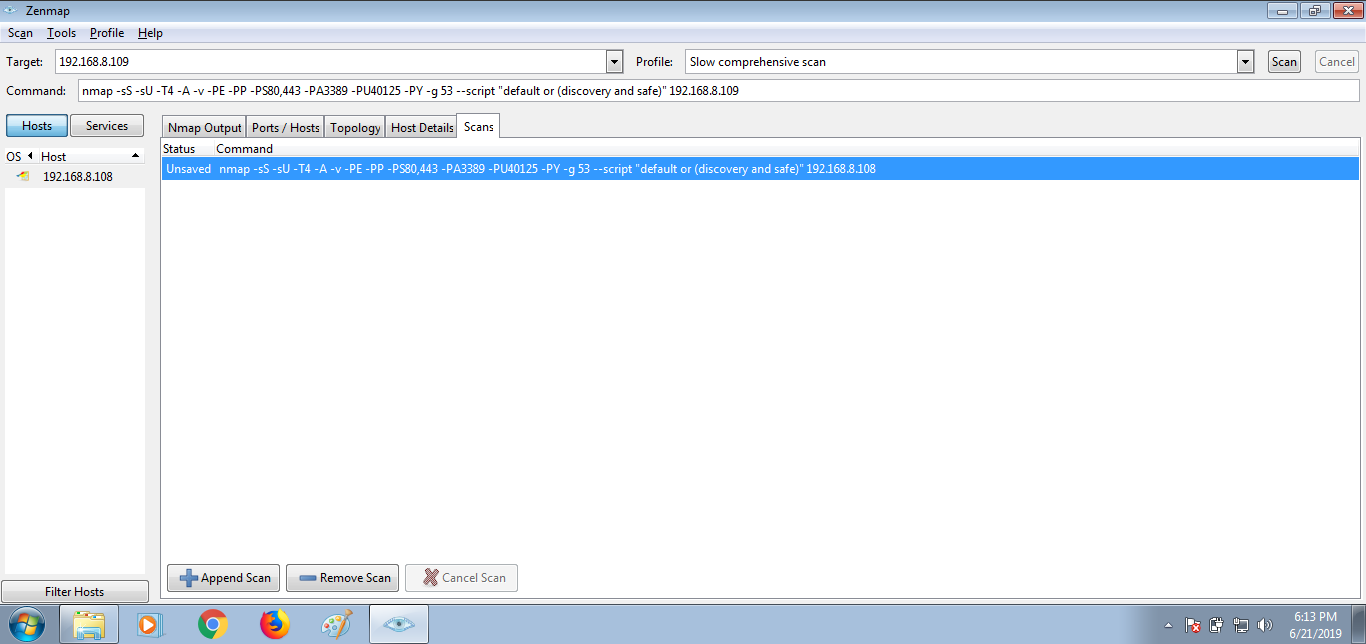
-. Haga clic en la pestaña puertos / hosts para mostrar más información sobre los resultados del análisis. Nmap emplea diversas técnicas de escaneo utilizando el escaneo lento y completo, y muestra más puertos abiertos.

- Nmap muestra el puerto, el protocolo, el estado, el servicio y la versión del escaneo.

- De la misma manera, haga clic en la pestaña de topología para ver la topología de la dirección IP de destino en el perfil de escaneo.

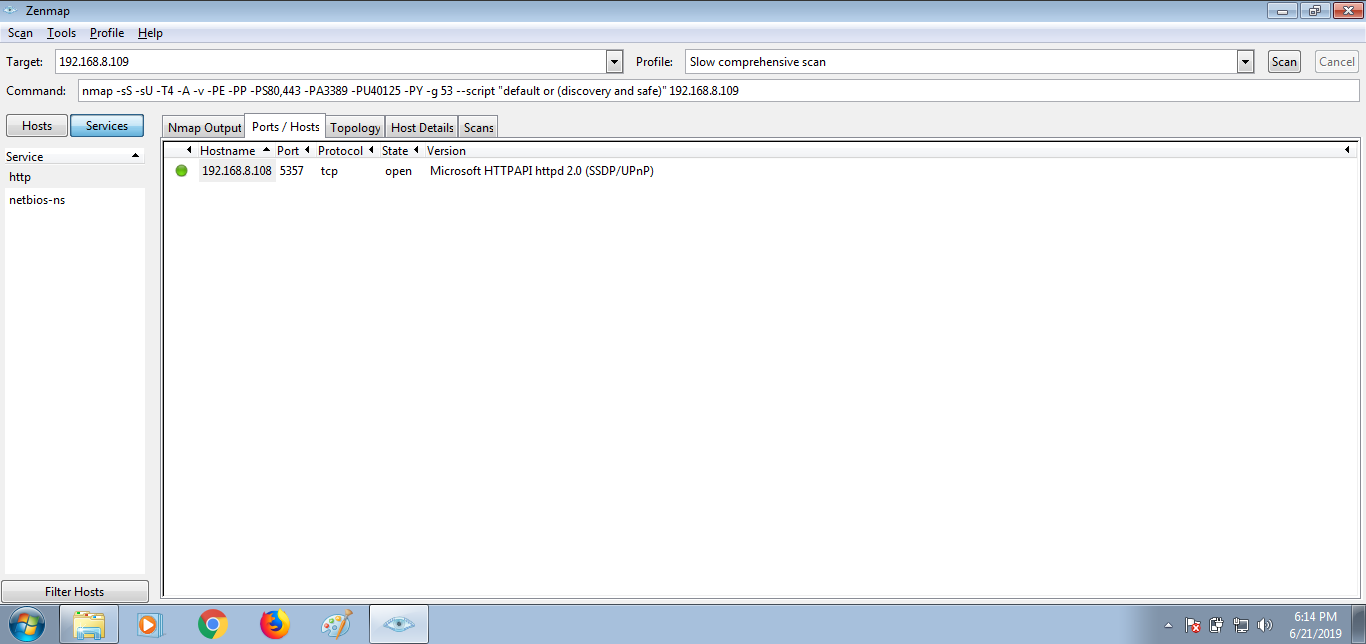
- Haga clic en la pestaña de detalles de hosts para ver los detalles de todos los hosts descubiertos durante el intenso perfil.

- Haga clic en la pestaña de escaneados para ver el estado del escaneo y el comando utilizado.



- Haga clic en la pestaña de servicios ubicada en el panel derecho de las ventanas. Esta

pestaña muestra la lista de servicios.

- Un atacante usa cualquiera de estos servicios y sus puertos abiertos para ingresar a la red / host objetivo y establecer una conexión.

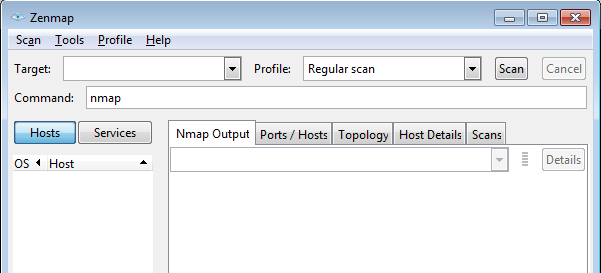
- Una vez, se realiza el escaneo, puede terminar la exploracion

5. Además de las exploraciones presentadas anteriormente, también puede realizar otras exploraciones, como la exploración SYN, la exploración XMAS, la exploración de bandera ACK, etc., en un intento por descubrir máquinas y sus puertos y servicios abiertos en una red.

- También puede elegir los perfiles de escaneo predeterminados disponibles en Nmap para escanear una red.

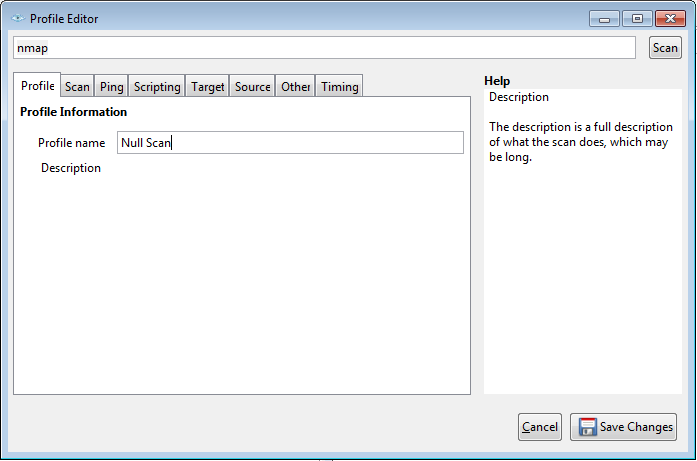
- La exploración nula envía un paquete sin indicadores activados. Solo funciona si la implementación de TCP / IP del sistema operativo se desarrolla de acuerdo con RFC 793. En una exploración nula, los atacantes envían una trama TCP a un host remoto sin indicadores.

- En el campo perfil: seleccione Escaneo regular de la lista desplegable.



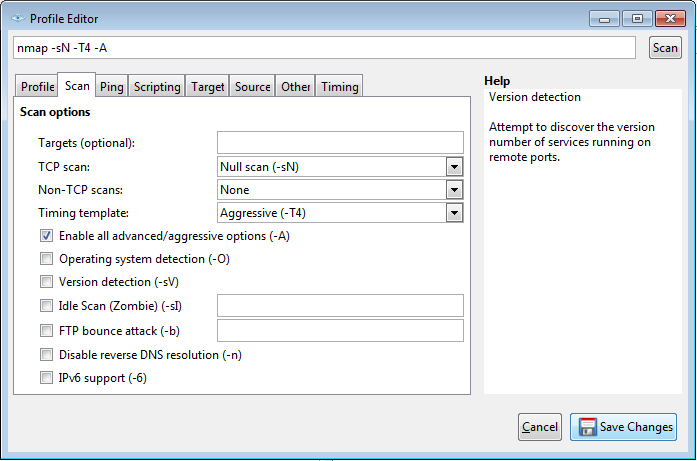
- Para realizar un análisis nulo de una dirección IP de destino, debe crear un nuevo perfil. Haga clic en perfil -> Nuevo perfil o comando CTRL + P

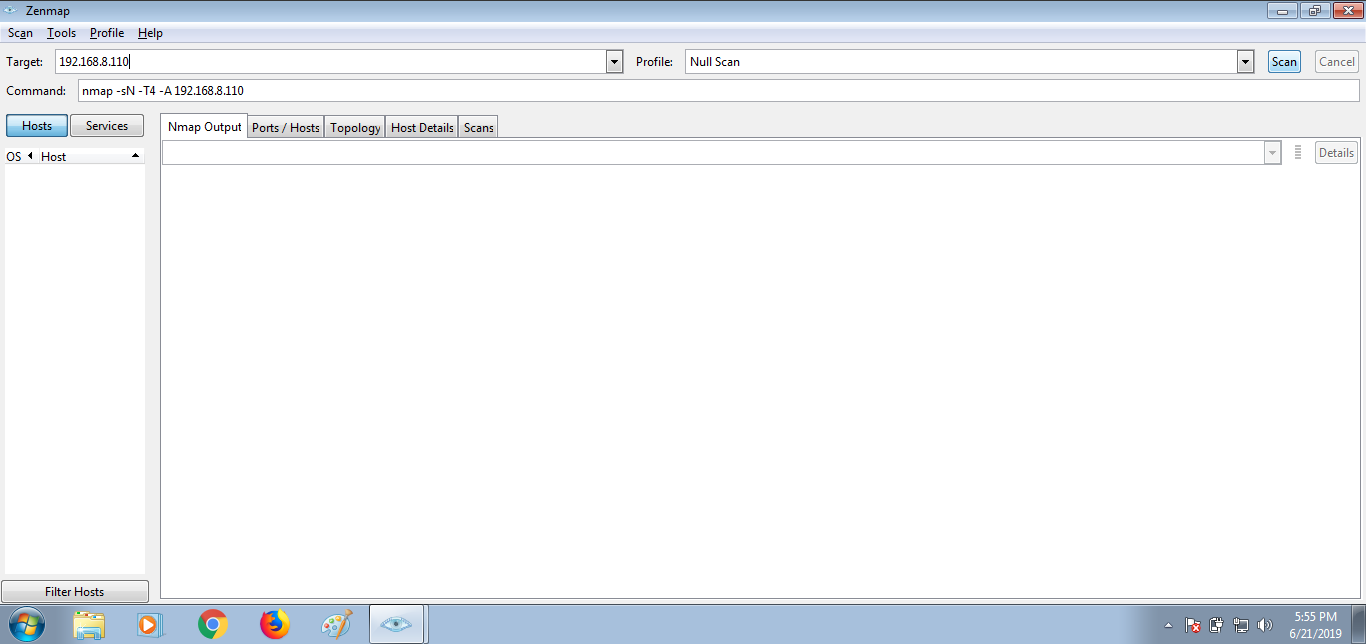
- En la pestaña de perfil, ingrese un nombre de perfil Exploración nula en el campo de nombre de perfil.

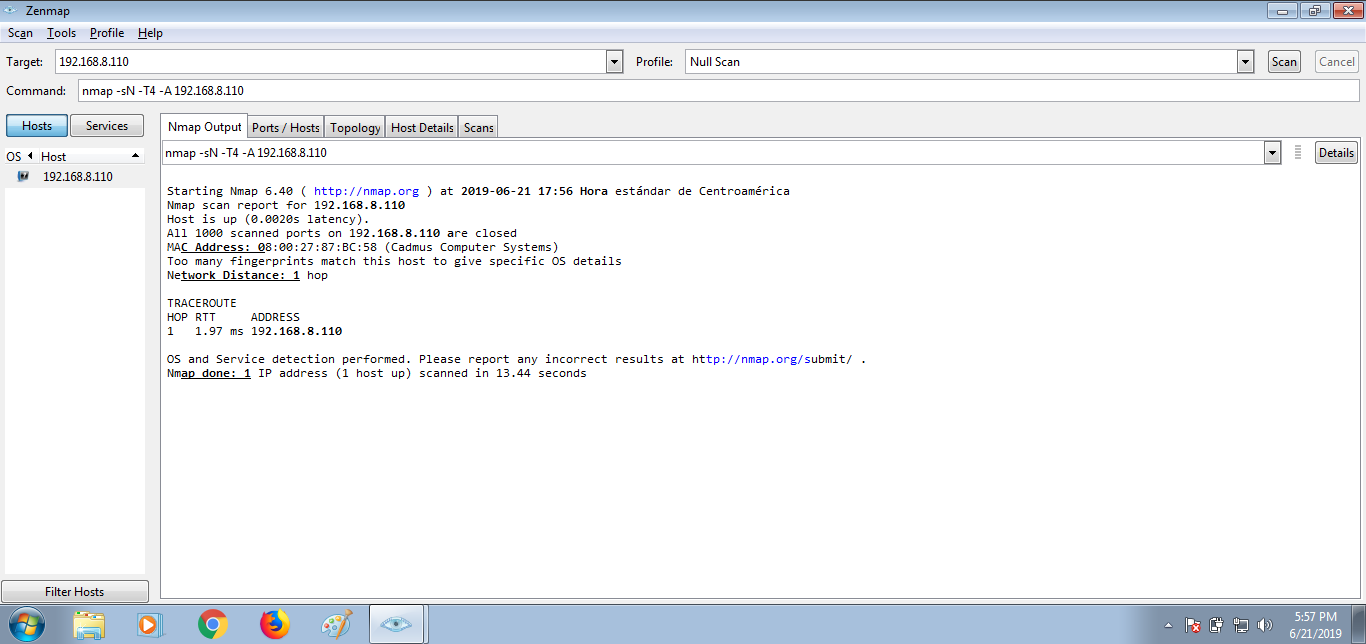
- Haga clic en la pestaña Escanear en la ventana del editor de perfiles. Seleccione la opción Exploración nula (-sN) en la lista desplegable de exploración TCP:

- Seleccione Ninguno en la lista desplegable Exploraciones no TCP: y Agresivo (-T4) en la lista Plantilla de tiempo: Marque la opción Habilitar todas las opciones avanzadas / agresivas (-A) y haga clic en guardar cambios.

- Usando esta configuración, estás configurando. Nmap para realizar un escaneo nulo con la plantilla de tiempo como -T4 y todas las opciones agresivas habilitadas.

- En la ventana principal de Zenmap, introduzca la dirección IP de destino (en este caso, 192.168.8.110, que pertenece a la máquina virtual de Ubuntu) para escanear, seleccione el perfil de análisis nulo de la lista desplegable Perfil y, a continuación, haga clic en exploración.

- Al emitir el comando, Nmap envía paquetes TCP sin ninguno de los indicadores TCP establecidos en el paquete. Si la exploración devuelve un paquete RST, significa que el puerto está cerrado; sin embargo, si no se devuelve nada, el puerto está filtrado o abierto.

- Nmap escanea el objetivo y muestra los resultados en la pestaña Salida de Nmap.

Los resultados obtenidos en su laboratorio pueden diferir de los que se muestran en la siguiente captura de pantalla:

- Puede hacer clic en las otras pestañas para examinar los resultados obtenidos por Nmap.

**Navegación anónima usando el Proxy Switcher**

**Escenario**

En el laboratorio anterior, aprendiste cómo hacer que los proxies en cadena de margarita permanezcan indetectables. Del mismo modo, como un experto en piratería ética o un comprobador de penetración, debe conocer todas las formas posibles de usar los servidores proxy para que no se pueda acceder a Internet. Por lo tanto, debería crear proxies para navegar por Internet de forma anónima. Este laboratorio demuestra otra forma de mantener el anonimato de Internet.

**Objetivos de Laboratorio**

Este laboratorio le mostrará cómo usar Proxy Switcher para navegar anónimamente.

**Entorno de Laboratorio**

Para este laboratorio se necesita:

- Proxy switcher, ubicado en D: \ CEH-Tools \ CEHv9 Module 03 Scanning Network \ Proxy Tools \ Proxy Switcher; También puedes descargar la última versión en [http://www.proxyswitcher.com](http://www.proxyswitcher.com/) en cuyo caso las capturas de pantalla que se muestran en el laboratorio pueden diferir.

- Una computadora ejecutando Windows Server 2012

- Un Navegador web con acceso a internet

- Privilegios de administrador para ejecutar las herramientas

**Vision general de Proxy Switcher**

Proxy Switcher le permite ejecutar acciones automáticamente de acuerdo con la conexión de red detectada. En su nombre indica, Proxy Switcher viene con algunas acciones predeterminadas, por ejemplo, la configuración de Internet Explorer, Firefox y Opera.

**Tareas de Laboratorio**

1. Vaya a D: \ CEH-Tools \ CEHv9 Module 03 Scannig Networks \ Proxy Tools \ Proxy Switcher y haga doble clic en ProxySwitcherStandard.exe

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

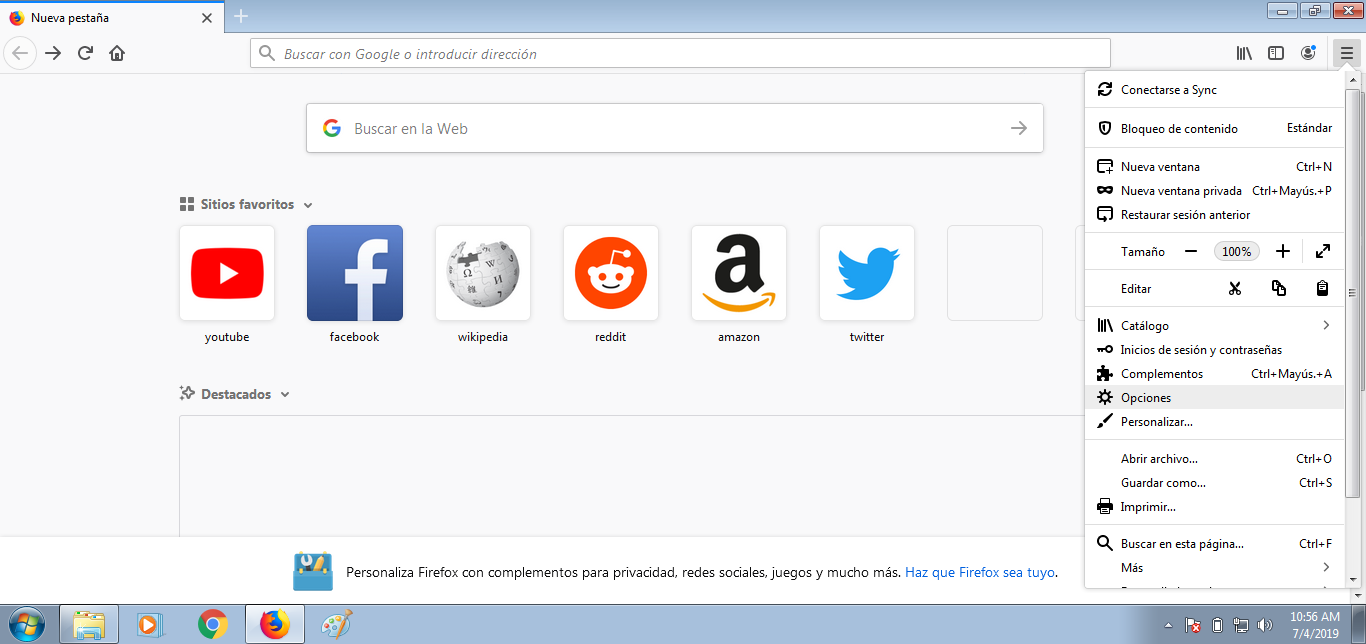
- Siga los pasos de instalación para instalar la aplicación.



- Una vez que se complete la instalación, desmarque todas las opciones en el paso final del asistente y haga clic en Finalizar.



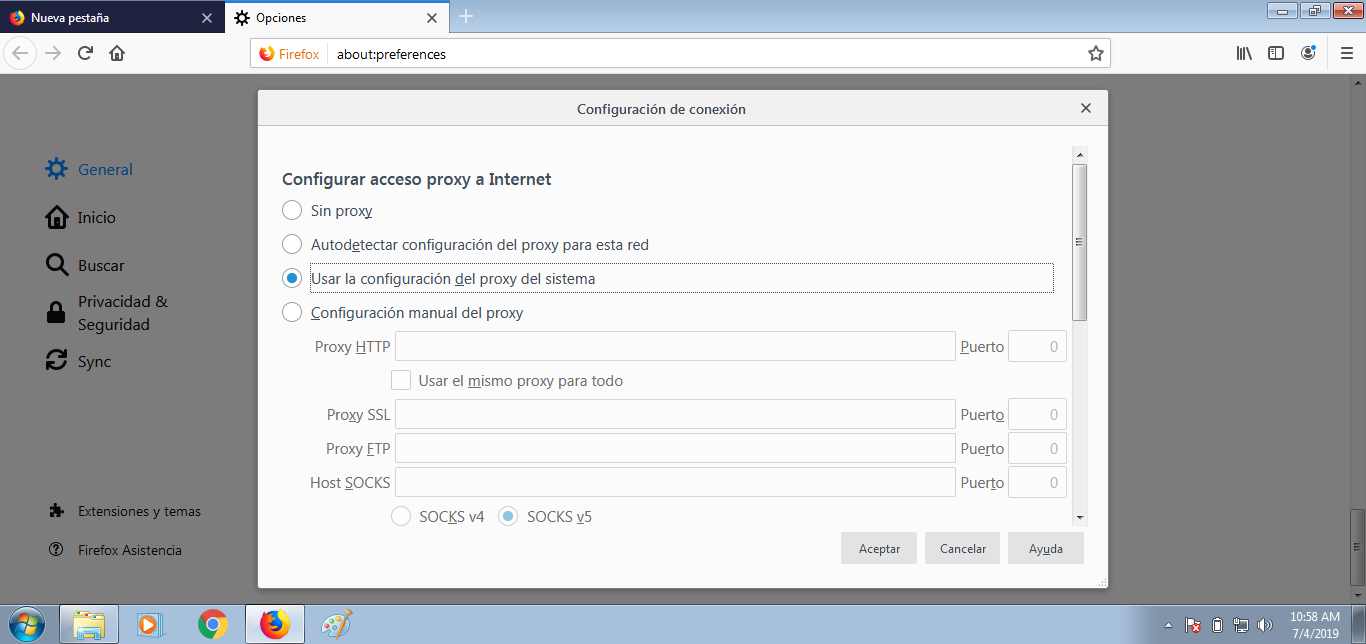
2. Inicie el navegador Firefox en la máquina host.



- Haga clic en el botón desplegable de Firefox en la esquina superior izquierda de la ventana del navegador y haga clic en Opciones.

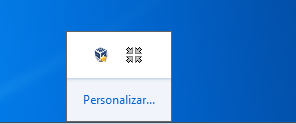
- Abra el perfil Avanzado en el asistente de opciones, haga clic en la pestaña Red y luego haga clic en → Configuración

- Seleccione Usar configuración de proxy del sistema y haga clic en Aceptar.



3. Aparece la pantalla de aplicaciones. Haga clic en el icono de Proxy Switcher Standard

- El icono de ProxySwitcher Standard aparece en la barra de tareas.

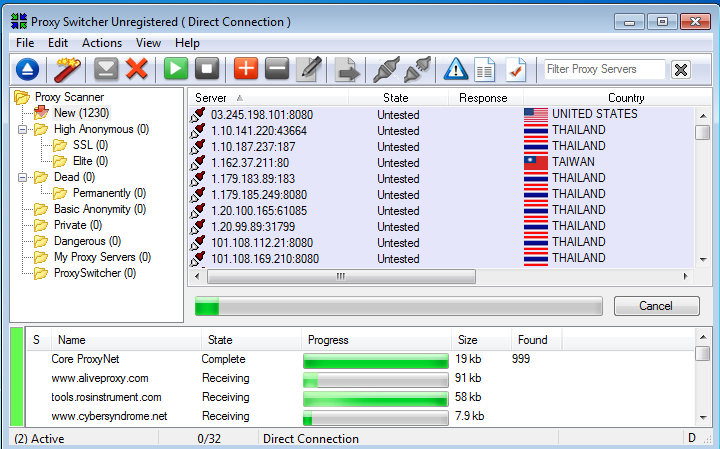


- Haga clic en la barra de tareas y seleccione Proxy Switcher Standard para iniciar la aplicación.

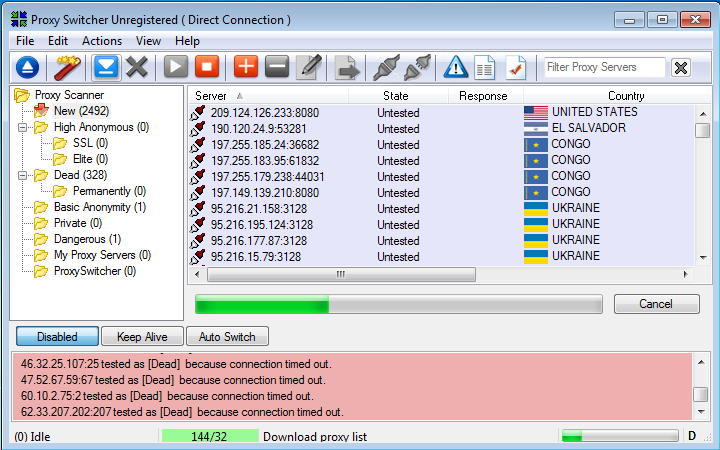
- El Asistente de lista de proxy aparece en la parte superior de la ventana principal de Proxy Switcher. Haga clic en Siguiente.

- Seleccione Buscar nuevo servidor, Volver a analizar el servidor, Volver a verificar el fallecimiento en Tareas comunes y haga clic en Finalizar.

- Aparece una lista de servidores proxy descargados en el panel derecho, como se muestra en la siguiente captura de pantalla:

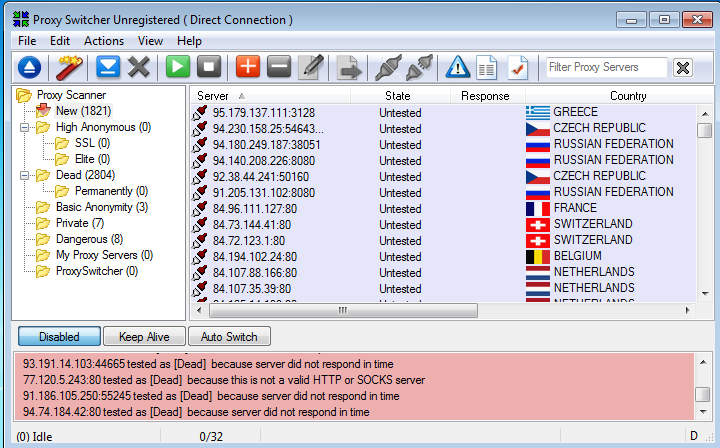
 Nota: La lista de servidores proxy descargados puede variar en su entorno de laboratorio.

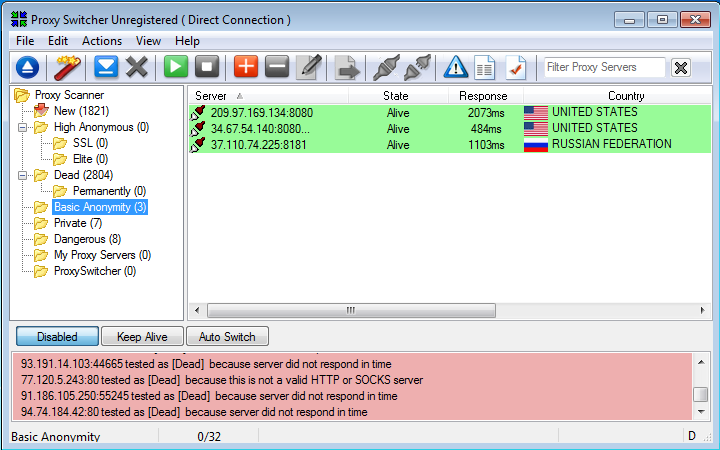
- Para comenzar a descargar la lista de proxy, haga clic en



- Espera hasta que todos los servidores proxy estén descargados. Esto puede llevar una cantidad significativa de tiempo.

Nota: Si tiene suficientes servidores proxy descargados, puede hacer clic en Cancelar para interrumpir la descarga.

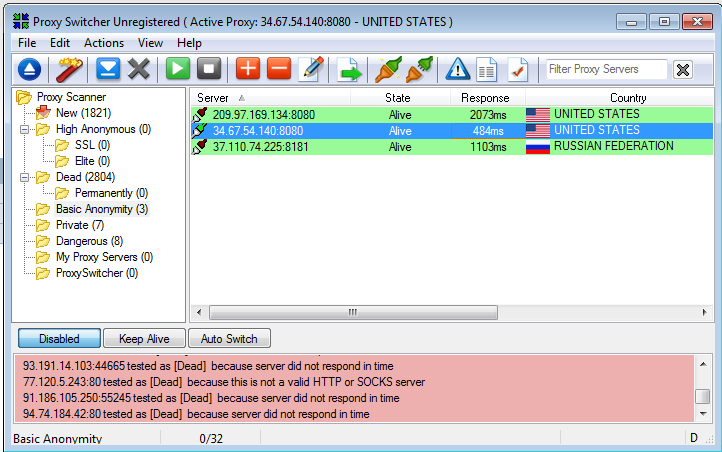
- Haga clic en Basic Anonymity en el panel izquierdo para mostrar una lista de servidores proxy activos.



- Seleccione una dirección IP de servidor proxy en el panel derecho. Para cambiar al servidor proxy seleccionado, haga clic en

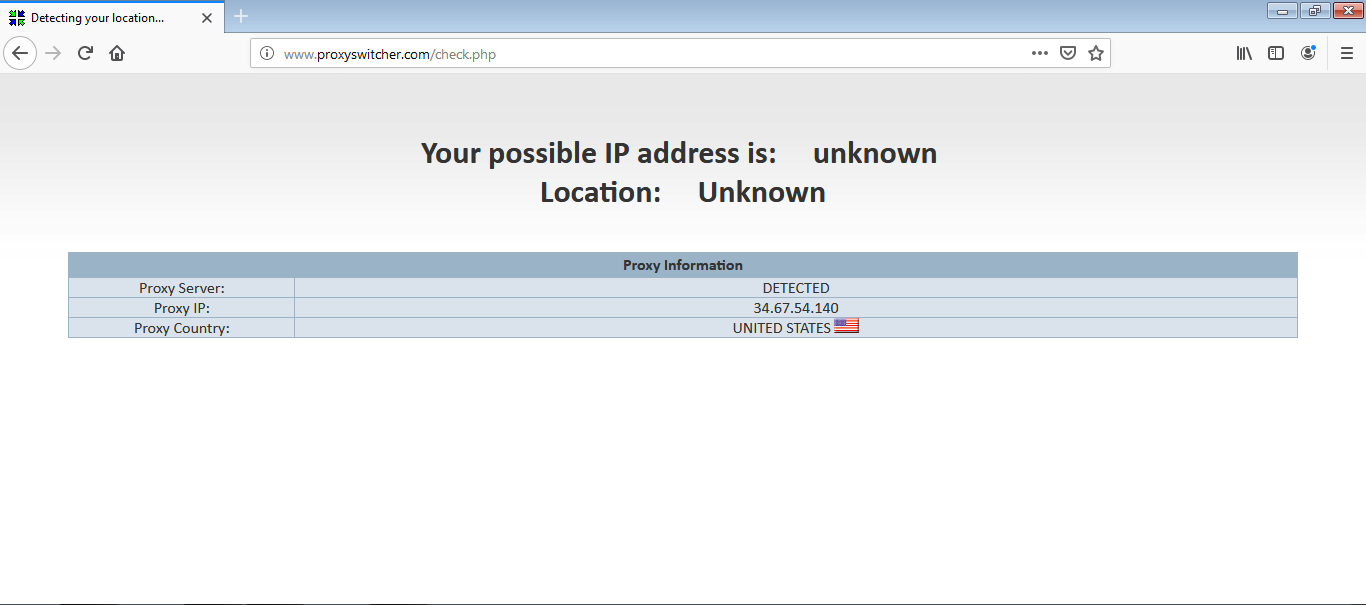
Nota: Seleccione solo aquellos proxies que están en estado Alive-SSL. El proxy seleccionado en este laboratorio puede variar en su entorno de laboratorio.

- Cuando el servidor proxy esté conectado, mostrará el icono de conexión como



- Inicie el navegador web Mozilla Firefox y el navegador e ingrese la URL <http://www.proxyswitcher.com/check.php> para comprobar la conectividad del servidor proxy seleccionado. Si la conexión es exitosa, se muestra la siguiente información que se muestra en el navegador.

Nota: la información que se muestra arriba puede diferir en su entorno de laboratorio.

- Si la conexión no se ha realizado correctamente, intente seleccionar otro proxy de Proxy Switcher y repita el paso 23

- Para asegurarse de que el proxy esté asignado, navegue http://www.google.com y escriba What is my IP en el motor de búsqueda.

- Presione Enter. La dirección IP del proxy se muestra en el SERP (página de resultados del motor de búsqueda), que infiere que la dirección legítima está enmascarada y el proxy está en uso.

Note: La dirección IP mostrada puede diferir en su entorno de laboratorio.

- Abra una nueva pestaña en el navegador web y navegue anónimamente con este proxy.