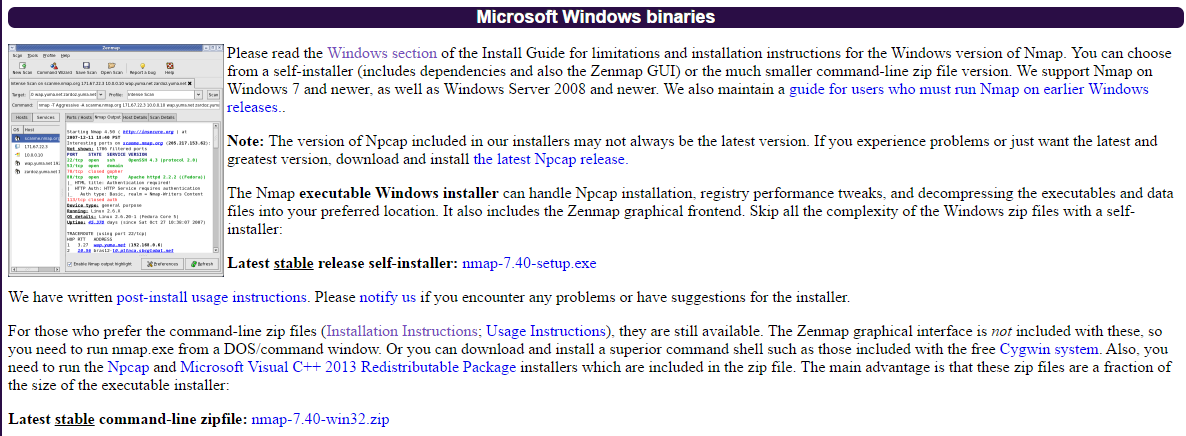
# 5. Proyecto de implementación de un prototipo del sistema utilizando la herramienta Nmap

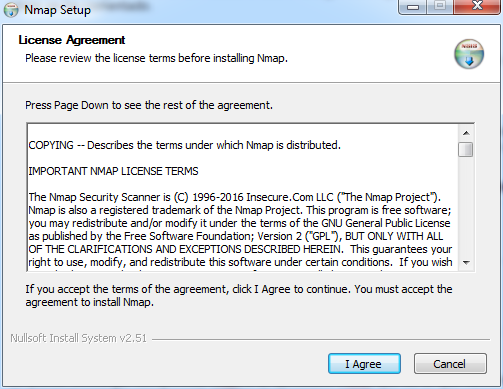
## 5.1 Documentación de la Descarga e Instalación

Nos vamos a la sección de [Descargas](https://nmap.org/download.html) de la página Principal de Nmap y nos descargamos el programa para nuestro sistema operativo (Linux, Mac OS, Windows, AmigaOS, etc), en nuestro caso Microsoft Windows.

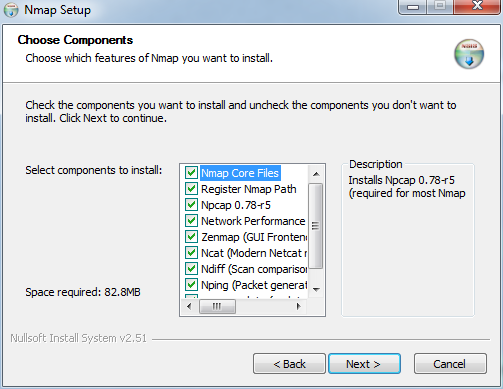


Se puede descargar comprimido (.zip) o el ejecutable (.exe) que es el que hemos descargado para proseguir con la instalación.

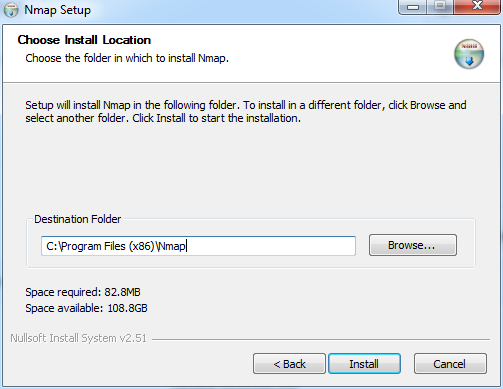
Al empezar la instalación lo primero que nos indica es que tenemos que aceptar los términos y condiciones de la herramienta:



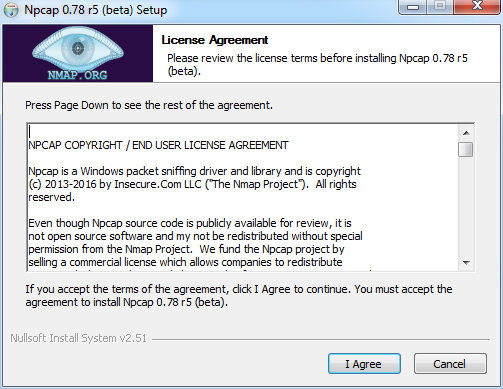
Ahora elegimos todos los componentes que queramos instalar para un profundo análisis de la herramienta:



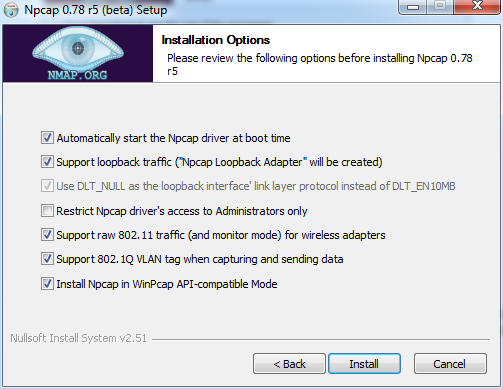
Ahora elegimos el directorio donde se ubicará la instalación:



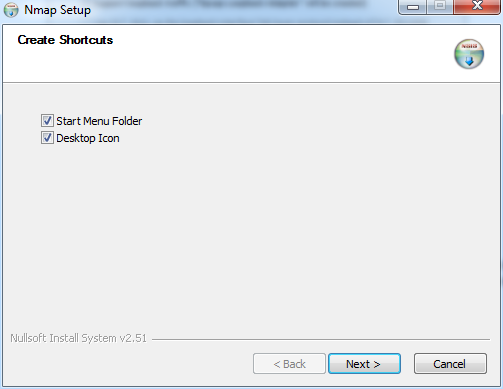
Mientras se instala la herramienta nos ofrecen instalar la función de Npcap:



Lo instalamos con los siguientes requisitos:



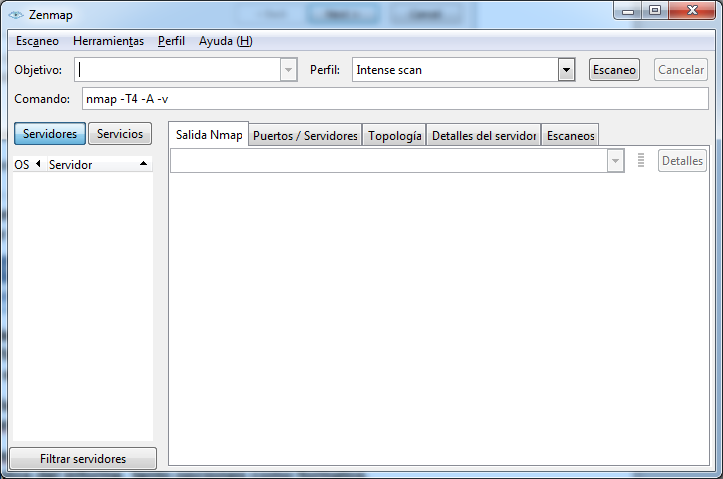
Al finalizar la instalación nos da la opción de crearnos un acceso directo en el Menú de Inicio y/o en el Escritorio:



Al crear los accesos directos que creamos conveniente ya se da por finalizada la instalación.

**4.2 Diseño**

La primera vez que ejecutamos Nmap nos aparece la pantalla principal que nos indica cual es nuestro objetivo a escanear y que comando deseamos introducir para el correcto funcionamiento, aquí le dejamos la muestra de ello:



En la pestaña "Escaneo" podemos encontrar opciones de abrir un nuevo escaneo, guardarlo o salir de la aplicación.

En la pestaña “Herramientas" podemos comparar los resultados obtenidos, buscar los resultados del escaneo o incluso filtrar los servidores.

En la pestaña "Perfil" podemos crear un nuevo perfil o comando, así como editar un perfil seleccionado.

En la pestaña "Ayuda" podemos encontrar la ayuda sobre el uso de esta herramienta, pudiendo reportar cualquier error encontrado y saber acerca de la versión instalada de la herramienta.

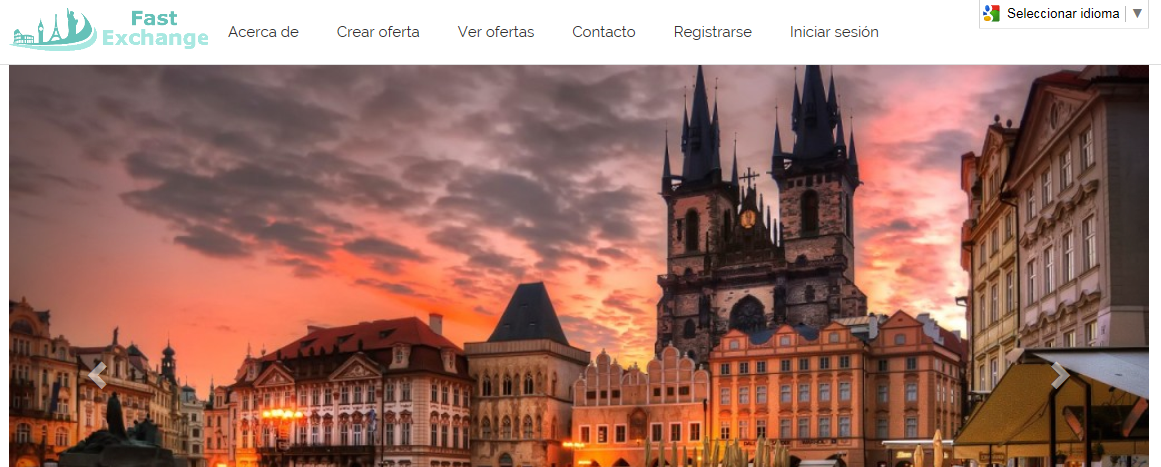
Aparte de estas cuatro pestañas tenemos las siguientes ventanas que nos dará información acerca del escaneo realizado:



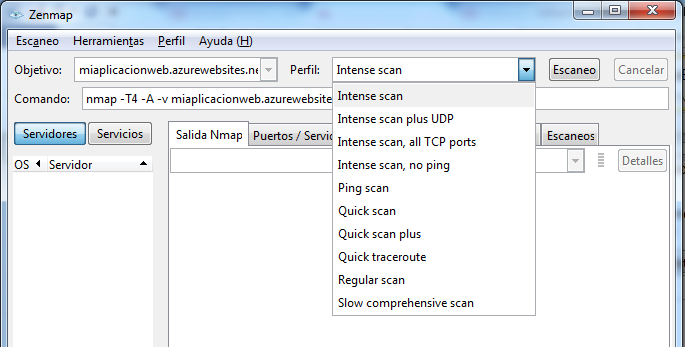
**4.3 Preparación de la ejecución**

Este es el sitio web del prototipo, llamado Fast Exchange, sobre el cual vamos a hacer el análisis de seguridad con la herramienta de Netsparker.

<https://miaplicacionweb.azurewebsites.net/>

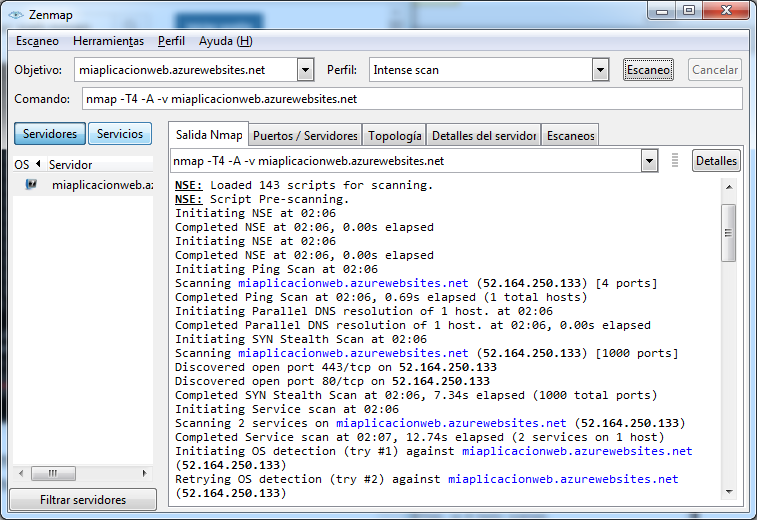


Lo primero que vamos a hacer en Nmap es poner la dirección en el apartado de “Objetivo”, después elegir el Perfil o Comando a ejecutar y clicamos en “Escaneo”. Con ello ya realizaremos la ejecución de la herramienta que solo necesita estos tres campos, ya que el campo de comando se rellena por defecto, si se quisiera realizar una búsqueda personalizada y mucho más completa será necesario usar dicha casilla (Comando):



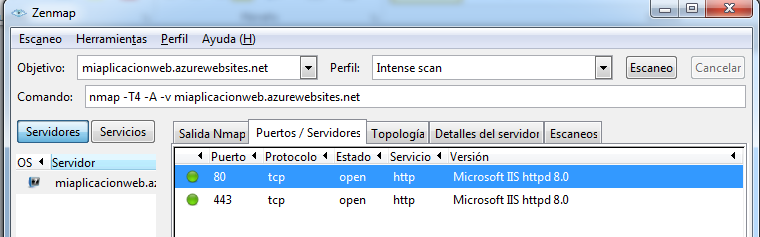
**4.4 Informe de errores**

Si elegimos Intense scan y damos a “Escaneo” para realizar el primer análisis de la web nos reconoce los aspectos generales de la página web:



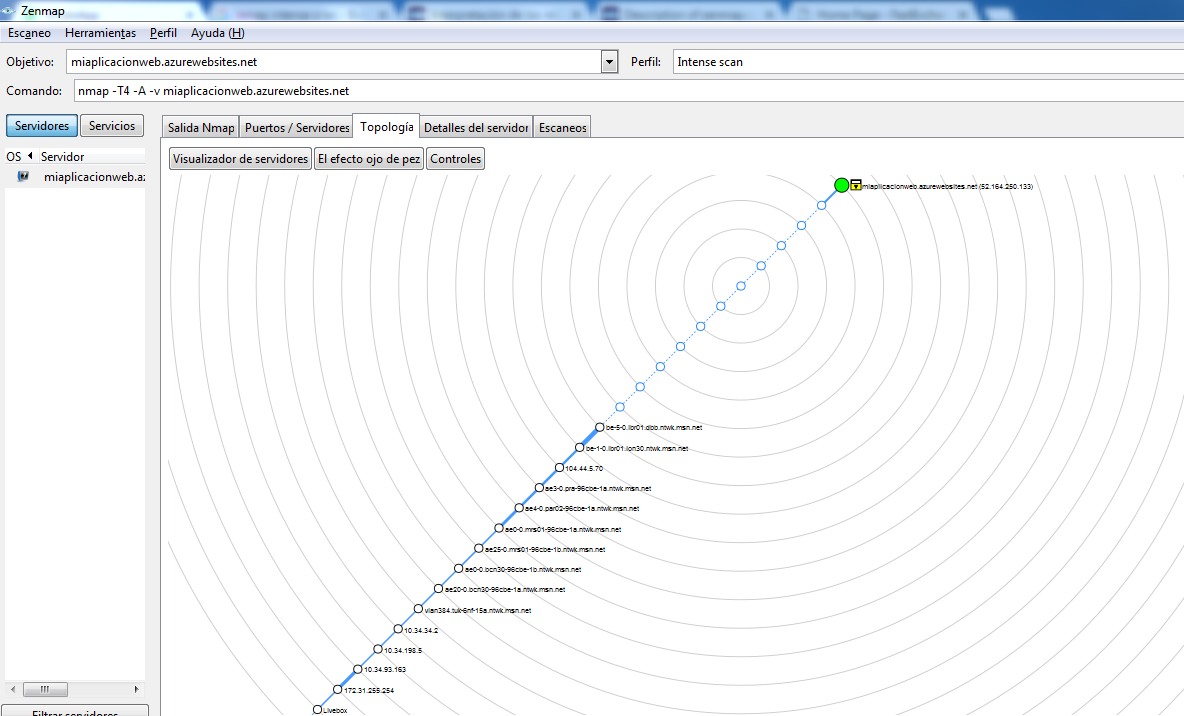
Observamos el nombre del servidor que se encuentra en el apartado izquierdo, en la pestaña de “Salida Nmap” que es la que se muestra en la anterior imagen, muestra de forma predeterminada cuando se ejecuta una exploración o búsqueda.

Pasamos de pestaña para consultar los Puertos / Servidores y nos lo detalla:

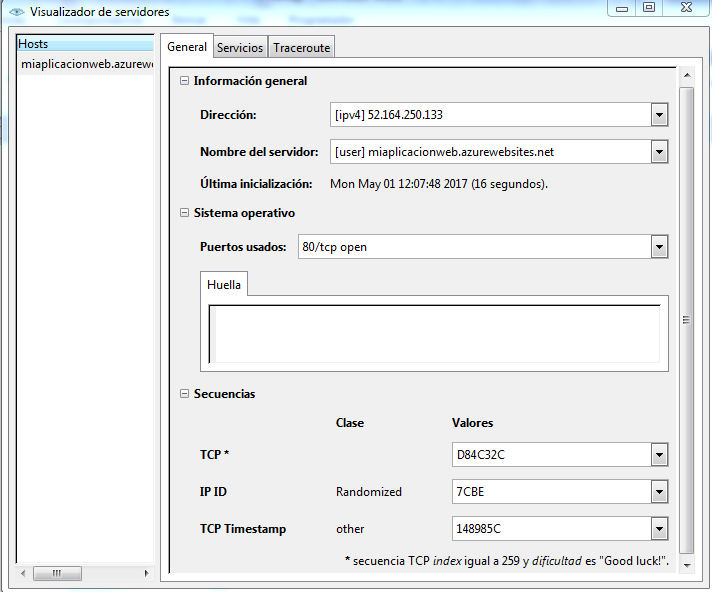


Podemos comprobar que esta página se basa en 2 puertos: 80 y el 443 y se están usando de una manera correcta sin ningún tipo de fallo y abierto al estar de color verde, si estuviera de color rojo se encontraría cerrado por algún tipo de fallo.

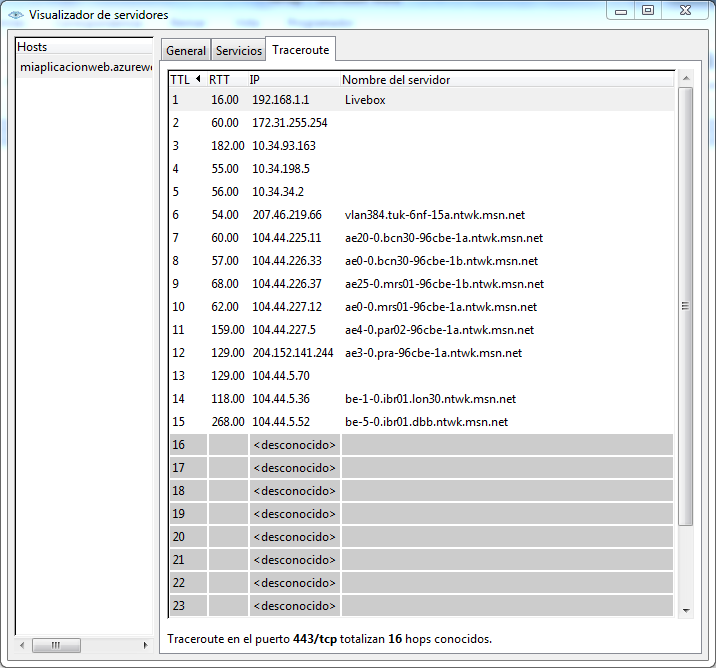
En la pestaña de “Topología” nos muestra el camino que pasa el ping que realizamos desde nuestro Router (Livebox) hasta el servidor final de la página web. Nos muestra el efecto Ojo de pez en una gráfica:



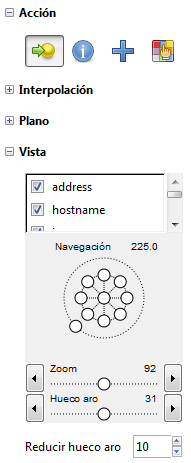
Si clicamos sobre la opción del Visualizador de servidores, nos muestra toda la información de estos:



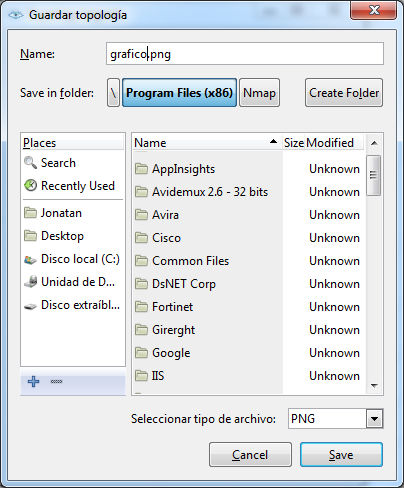
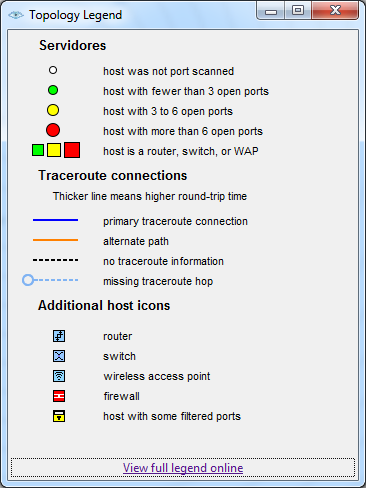
Además de ello si nos vamos a la pestaña de Traceroute nos comenta de una manera más detalla todas las IP que ha localizado y las que no añadiéndolas como desconocidas, en nuestro caso 16:



Si damos al botón de efecto de ojo de pez, se nos muestra de manera aumentada el gráfico. Además cabe destacar el botón de Controles, ya que nos da la opción de personalizar el gráfico a nuestro antojo:



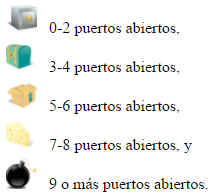
Y como últimas opciones que nos da la Tipología es la Leyenda del gráfico y la opción de Guardar el mismo:



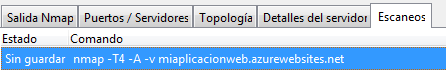
Continuamos ahora con la pestaña “Detalles del servidor”:



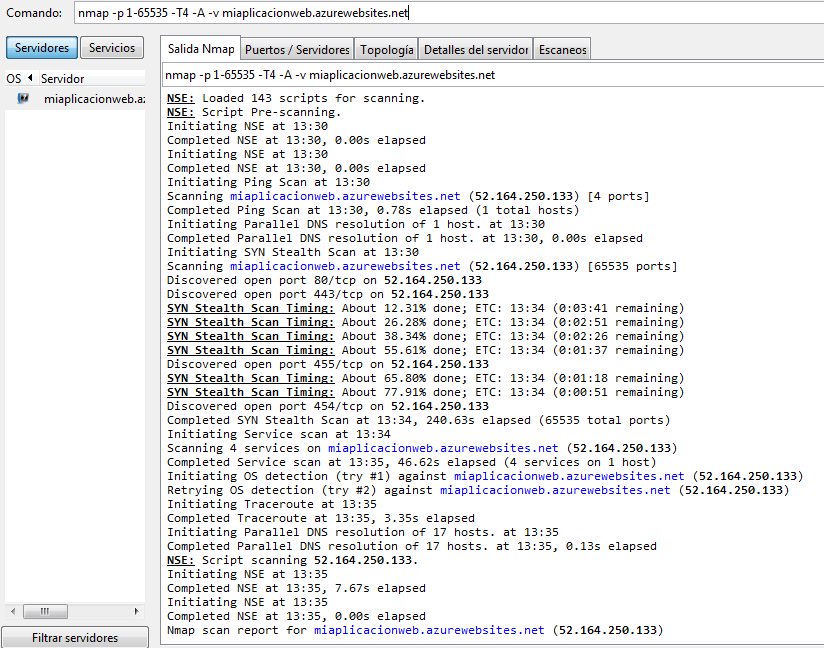
Nos informa el estado del servidor, la IP del mismo o los puertos abiertos y cerrados entre otras cosas. Apreciamos en la imagen una caja fuerte, indicando la seguridad que da Nmap, este es su rango de decreto en elegir un icono:



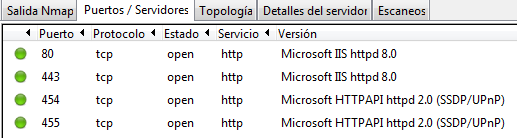
Y por último descubrimos la pestaña de “Escaneos” que nos informa de los comandos que hemos realizado para analizar la web seleccionada:



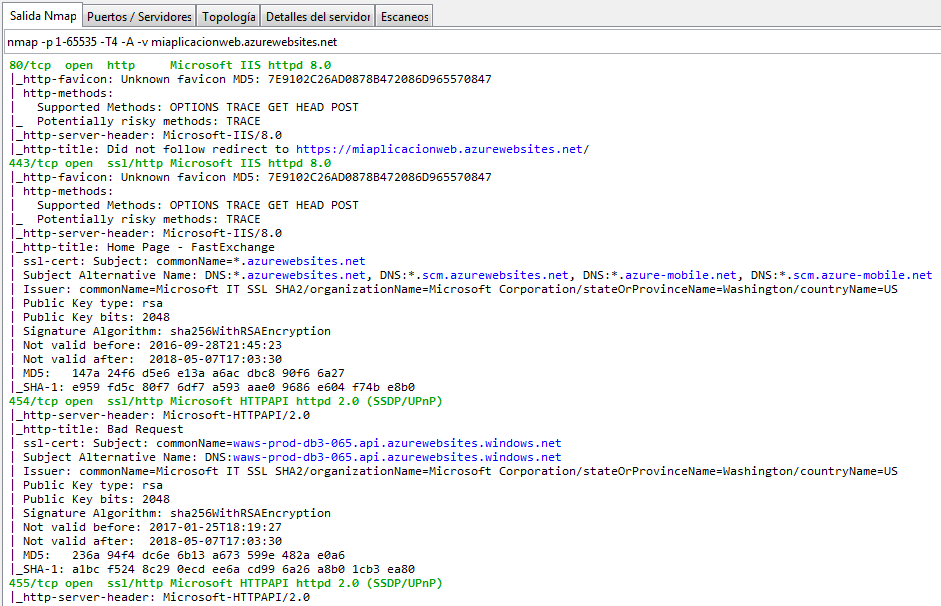
Después de este general vamos a centrarnos exclusivamente en los puertos, por lo que realizaremos un análisis más profundo de los mismos mediante el comando: nmap -p 1-65535 -T4 -A -v miaplicacionweb.azurewebsites.net



Observamos los nuevos puertos que hemos descubierto al analizar la web profundamente (pasando de 2 a 4 puertos):

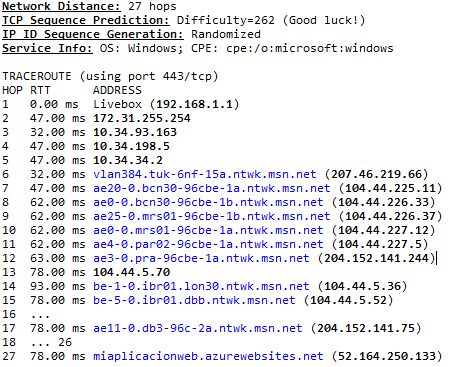


Con una información muy detallada de los mismos en la Salida Nmap:



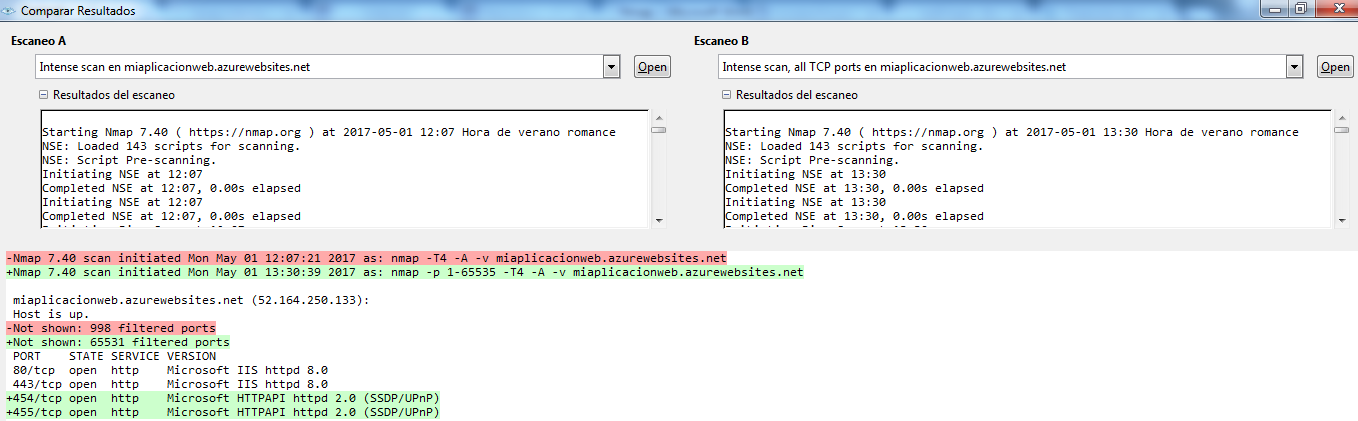
En esta imagen podemos descubrir el tipo de claves públicas que usan (rsa) y los bits de cifrado (2048), así como su encriptación y la validez del certificado de los protocolos de seguridad SSL y HTTPS, como nos muestra Nmap dichos certificados de seguridad caducan justo dentro de 1 año, por lo que nos podemos planificar un nuevo gasto por dicha renovación (si fuera nuestra Web). También podemos decir que dicha web está cifrada por el método Hash de criptografía MD5.

Por último podemos indicar que estos protocolos de seguridad están respaldados por Microsoft Corporation, ya sabiendo que es una empresa tecnológica muy prestigiosa.

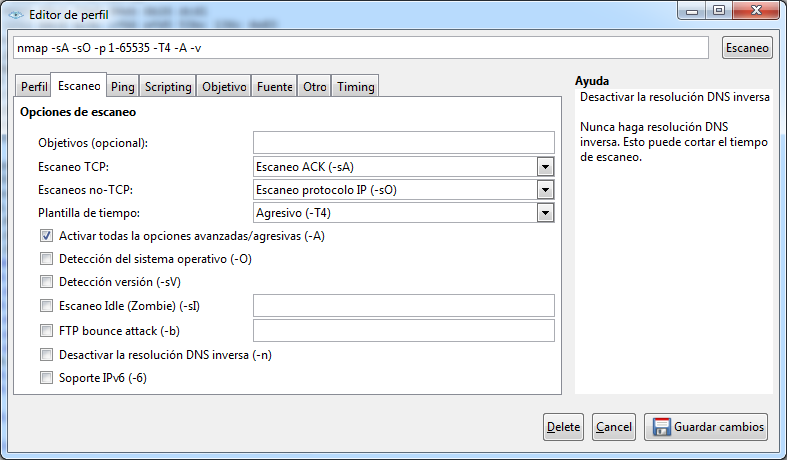


Además nos comunica este comando la distancia de la red para saber los host con su correspondiente IP que hay por medio desde nuestro router del trabajo o la casa hasta la web a analizar. En este caso hay 27 de por medio. También nos comenta la Predición de las Secuencias de TCP, que en este caso nos analiza de una dificultad alta (262) para poder atacar de manera maliciosa la web analizada, por ello añade un mensaje irónico de Buena suerte (Good Luck!). Nos añade información sobre los servicios, que usan sistemas de Microsoft Windows.

Como hemos visto anteriormente si nos vamos a la pestaña de “Herramientas” y damos a “Comparar los resultados” nos compara los escaneos que hemos realizado anteriormente eligiendo los que deseamos comparar:



También nos podemos crear un perfil, eligiendo las funciones y características que queremos analizar concluyendo en un comando final. A este comando se le puede dar un nombre de Perfil para tenerlo guardado con el nombre que se quiera para los próximos análisis a la misma web u otras webs de otros proyectos, todo ello se puede demostrar en la siguiente imagen:



Por último para finalizar los informes que se pueden realizar para analizar los errores de la web se puede hacer en el entorno de línea de comandos (Lo más usado por los profesionales en la materia) ya que no en todos los sistemas operativos se dispone de esta interfaz gráfica, como por ejemplo es Linux.

Si deseamos realizar escaneos más personalizados y profundos será necesario hacerlo mediante la consola de comandos (cmd), los cuales podremos añadir estos puertos, dependiendo de lo que se quiera analizar:

* -sS (Sondeo TCP SYN): SYN es la opción por defecto de exploración y más popular por buenas razones. Se puede realizar de forma rápida, el escaneo de miles de puertos por segundo en una red rápida no obstaculizado por los cortafuegos restrictivos. También es relativamente discreto y cauteloso ya que nunca termina las conexiones TCP. Esta técnica se refiere a menudo como la exploración entreabierta, porque no abre una conexión TCP completa. Se envía un paquete SYN, como si se va a abrir una conexión real y luego esperar una respuesta.
* -sT (Conexión TCP exploración): Es el tipo de escaneo TCP por defecto cuando el sondeo SYN no es una opción. Este es el caso cuando un usuario no tiene privilegios. Nmap pide al sistema operativo subyacente para establecer una conexión con la máquina de destino y el puerto mediante la emisión de la llamada al sistema. Esta es la misma llamada al sistema de alto nivel que los navegadores web, clientes P2P, y la mayoría de otras aplicaciones de red utilizan para establecer una conexión. Nmap tiene menos control sobre el alto nivel de llamadas que con los paquetes, por lo que es menos eficiente.
* -sU (exploraciones UDP): Aunque la mayoría de los servicios populares de Internet se ejecutan a través del protocolo TCP, UDP servicios están ampliamente desplegados. DNS, SNMP y DHCP son tres de los más comunes. Debido a que el escaneo UDP es generalmente más lento y más difícil que TCP, algunos auditores de seguridad ignoran estos puertos. Esto es un error, ya que los servicios UDP son bastante comunes y los atacantes sin duda no ignoran todo el protocolo. Afortunadamente, Nmap puede ayudar a los puertos UDP de inventario. Nmap detecta limitación de velocidad y reduce la velocidad en consecuencia para evitar la inundación de la red con paquetes inútiles
* -sY (Exploración INIT SCTP): SCTP es relativamente una nueva alternativa a los protocolos TCP y UDP, la combinación de la mayoría de las características de TCP y UDP. SCTP exploración INIT SCTP es el equivalente de un sondeo TCP SYN. Se puede realizar de forma rápida, el escaneo de miles de puertos por segundo en una red rápida no obstaculizado por los cortafuegos restrictivos. Al igual que el sondeo SYN, exploración INIT es relativamente discreto y cauteloso, ya que nunca se completa asociaciones SCTP. También permite la diferenciación fiable entre los estados de los puertos abiertos, cerrados y filtrados.
* -sN; -sF; -sX(TCP NULL, escaneos FIN, y Xmas): Al escanear sistemas compatibles con este texto RFC, cualquier paquete que no contiene SYN, RST, o los bits ACK resultará en una RST devuelto si el puerto está cerrado y no hay respuesta en absoluto si el puerto está abierto. Nmap explota esto con tres tipos de análisis:
  + Scan Null ( -sN): No establece ningún bit (cabecera indicador TCP es 0)
  + Escaneo FIN ( -sF): Establece simplemente el bit TCP FIN.
  + Exploración de Xmas ( -sX): Establece las banderas FIN, PSH, URG y, encendiendo el paquete como un árbol de Xmas.

La ventaja clave de estos tipos de análisis es que pueden colarse a través de ciertos cortafuegos y routers de filtrado de paquetes. Otra ventaja es que este tipo de análisis son un poco más sigilosos que incluso un sondeo SYN.

* -sA (Sondeo TCP ACK): Esta exploración es diferente a los demás discuten hasta el momento en que nunca se determina abierto. Se utiliza para trazar conjuntos de reglas de firewall, para determinar si son o no con estado y los puertos que se filtran.
* -sW (Exploración ventana TCP): Exploración de la ventana es exactamente el mismo que el ACK scan excepto que explota un detalle de implementación de ciertos sistemas para diferenciar los puertos abiertos de los cerrados. Esto se hace examinando el campo de la ventana TCP de los paquetes RST devueltos.
* -sM (Sondeo TCP Maimón): La exploración Maimón lleva el nombre de su descubridor, Uriel Maimón. Esta técnica es exactamente el mismo que NULL, FIN, y las exploraciones de Xmas, excepto que la sonda está FIN / ACK.
* --scanflags (Sondeo TCP personalizado): Permite diseñar tu propia exploración mediante la especificación de indicadores TCP arbitrarias.
* -sZ (Exploración SCTP COOKIE ECHO): SCTP exploración COOKIE ECHO es una exploración SCTP más avanzada. Se aprovecha del hecho de que las implementaciones SCTP debe caer en silencio paquetes que contienen trozos COOKIE ECHO sobre los puertos abiertos, pero enviar un ANULAR si el puerto está cerrado. La ventaja de este tipo de análisis es que no es tan obvio un escaneo de puertos de una exploración INIT.
* -sI *<zombie host>*[:*<probeport>*] (Análisis de inactividad): Este método de exploración avanzada permite un escaneo de puertos TCP verdaderamente ciega del objetivo (es decir, no hay paquetes se envían al destino desde su dirección IP real). En cambio, un ataque de canal lateral única explota predecible ID fragmentación generación de la secuencia IP en el host zombie de recoger información sobre los puertos abiertos en el objetivo.
* -sO (Exploración de protocolo IP): Exploración protocolo IP le permite determinar qué protocolos IP (TCP, ICMP, IGMP, etc.) son compatibles con los equipos de destino. Esto no es técnicamente un escaneo de puertos, ya que gira a través de los números de protocolo IP en lugar de TCP o UDP números de puerto.
* -b *<FTP relay host>* (Exploración de rebote FTP): Una característica interesante del protocolo FTP es el soporte para las llamadas conexiones FTP proxy. Esto permite a un usuario conectarse a un servidor FTP y pedir que los archivos se enviarán a un servidor de terceros. Esta característica permite que está causando el servidor FTP para escaneo de puertos otros anfitriones. Simplemente pedir al servidor FTP para enviar un archivo a cada puerto interesante de un host de destino a su vez. El mensaje de error se describen si el puerto está abierto o no. Esta es una buena manera de eludir los cortafuegos porque los servidores FTP de organización a menudo se colocan en el que tienen más acceso a otros hosts internos que cualquier host de Internet de edad lo haría.

Ahora probaremos uno de estos parametros en la línea de comandos ejecutando Nmap con un análisis más profundo y por lo que tarda mucho más tiempo en realizar este análisis:

