

Contenido

1. Autores del trabajo, planificación y entrega.....	3
1.1 Autores.....	3
1.2 Planificación	3
1.3 Entrega	3
2. Requisitos del prototipo a implementar	4
2.1 Requisitos funcionales.....	4
2.2 Otros requisitos	5
3. Criterios de comparación en la implementación	5
3.1 Criterio 1: Tiempo de ejecución	5
3.2 Criterio 2: Tipos de escaneo.....	5
3.3 Criterio 3: Grado de detalle.....	5
3.4 Criterio 4: Clasificación de errores.....	5
3.5 Criterio 5: Recomendaciones	6
3.6 Criterio 6: Profundidad del análisis	6
3.7 Criterio 7: Horas empleadas	6
3.8 Criterio 8: Facilidad de uso	6
3.9 Criterio 9: Preparación para la implementación	6
3.10 Criterio 10: Recopilación de información	6
3.11 Criterio 11: Precio.....	6
4. Proyecto de implementación de un prototipo del sistema utilizando la herramienta Netsparker.....	7
4.1 Documentación de Descarga e Instalación.....	7
4.2 Documentación del Diseño.....	10
4.3 Documentación de la Preparación de la Ejecución.....	13
4.4 Documentación de los Informes de Errores.....	16
5. Proyecto de implementación de un prototipo del sistema utilizando la herramienta Nmap.....	21
5.1 Documentación de Descarga e Instalación.....	21
5.2 Documentación del Diseño.....	24
5.3 Documentación de la Preparación de la Ejecución.....	25
5.4 Documentación de los Informes de Errores.....	26
6. Comparación de las dos implementaciones	37
6.1 Evaluación de los criterios en la implementación usando Netsparker	37
6.2 Evaluación de los criterios en la implementación usando Nmap.....	38
7. Comparación de la implementación de las tecnologías.....	39
8. Conclusiones	40

1. Autores del trabajo, planificación y entrega

1.1 Autores

Somos el grupo T4 formado por:

- Jonatan Viñuelas Caballero (Coordinador).
- Ana Olmeda Fernández.
- Miguel Domingo Calvo.

1.2 Planificación

Hay que tener en cuenta que cada participante del grupo debe tener asignadas tareas que sumen al menos 45 horas. El peso de este trabajo en la calificación total de la asignatura es de un 30%, por tanto requiere de una dedicación de 45 horas del total de 150 horas de la asignatura.

Como bien dice el enunciado al ser este trabajo el 10% de la calificación total de la asignatura, requiere una dedicación mínima de 15 horas de las 150 horas que tiene la asignatura.

Por lo que al estar formado el grupo por 3 miembros el tiempo mínimo sería de 45 horas, pero nosotros le hemos dedicado alrededor de 52 horas al llevarnos mucha investigación y formación para comparar correctamente los dos prototipos de dicho proyecto. Estas horas se pueden apreciar claramente en el siguiente diagrama:

Planificación TG3 (Grupo T4)

Se han repartido las tareas de una forma equitativa, apartando las tareas del coordinador del resto del grupo.

Al principio cada integrante del grupo se especializó en una tecnología, pero acabamos compartiendo información y desarrollando nuestras propias conclusiones de cada tecnología en consenso, mediante diversos debates de opiniones documentadas.

1.3 Entrega

El enlace a nuestro repositorio es el siguiente:

<https://github.com/JonatanVinuelasCaballero/TG3>

En este apartado debe incluirse un enlace (URL) a un repositorio en GitHub o en BitBucket creado para el trabajo. En dicho repositorio debe encontrarse, al menos los siguientes archivos en la rama máster:

- TG3_final.docx TG3_final.pptx
- Prototipos obtenidos implementando cada una de las tecnologías (deben incluir el código fuente y todos los archivos necesarios para la instalación y uso de cada prototipo):
 - PrototipoTecnologiaA_final.zip (o .rar)
 - PrototipoTecnologiaB_final.zip (o .rar).

Dichos archivos serán los que se tendrán en cuenta para la calificación del trabajo.

2. Requisitos del prototipo a implementar

Se va a desarrollar una página web como prototipo para realizar las pruebas de ambas herramientas (Nmap y Netsparker) y poder compararlas entre ellas. Esta página web está destinada a realizar intercambios entre personas, que estén interesadas en aprender algún idioma, eligiendo la familia del país donde querrán ir así como la posibilidad de que una familia quiera recibir a alguna de estas personas. Cada usuario de la web tendrá un perfil personal donde se registrará como miembro familia, el cual busca una familia donde ir a aprender un idioma, o como miembro familia anfitriona, el cual está dispuesto a recibir a una persona.

Todos los usuarios podrán crear ofertas a las cuales cada usuario accederá según sus intereses. Por tanto al almacenar datos personales es conveniente que estos estén lo más seguro posible para que no puedan ser robados o usados con malas intenciones.

2.1 Requisitos funcionales

REQ.	DESCRIPCIÓN
RF01	Registro de usuarios mediante correo electrónico y contraseña.
RF02	Confirmación de contraseña.
RF03	Uso de un Captcha.
RF04	Acceso al sistema mediante un usuario registrado.
RF05	Acceso mediante distintas plataformas como Facebook.
RF06	Cierre de sesión.
RF07	Acceso al perfil personal.
RF08	Modificación del perfil personal.
RF09	Visualización de ofertas solo a usuarios registrados.
RF10	Filtro de búsqueda de ofertas.
RF11	Acceso a un apartado de ayuda.
RF12	Acceso a página de contacto.
RF13	Creación de ofertas de “miembro familia” y “miembro familia anfitriona”
RF14	Chat de soporte.
RF15	Selección de idioma de la web
RF16	Problemas de cross-site Scripting
RF17	Mal uso de los puertos asociados a protocolos como SSL y TSL, HTTPS...
RF18	Problemas de CRLF
RF19	Errores de diseño y desarrollo
RF20	Facilidad de inclusión de archivos remotos

REQ.	DESCRIPCIÓN
RF21	Recursos ocultos.
RF22	Vulnerabilidad de Google Sitemap

2.2 Otros requisitos

REQ.	DESCRIPCIÓN
R01	Las interfaces gráficas son legibles por personas que tengan una agudeza visual limitada.
R02	Un usuario del sistema es capaz de aprender a crear y buscar ofertas en menos de 5 minutos
R03	El sistema debe funcionar en los navegadores más usados como Google Chrome o Mozilla Firefox.
R04	El sistema debe poder ser usado desde distintos sistemas operativos como Windows o iOS.
R05	Se deberá desarrollar usando lenguajes de programación estandarizados como C#... además de usar CSS, Javascript...

3. Criterios de comparación en la implementación

3.1 Criterio 1: Tiempo de ejecución

Nombre del criterio: Tiempo ejecución.

Descripción: Tiempo invertido en realizar el escaneo de un sitio web.

Tipo de valor: Numérico.

3.2 Criterio 2: Tipos de escaneo

Nombre del criterio: Tipos de escaneo.

Descripción: Posibles escaneos de los que dispone la herramienta para realizar.

Tipo de valor: Texto libre.

3.3 Criterio 3: Grado de detalle

Nombre del criterio: Grado de detalle.

Descripción: Es el grado de detalle que tiene el informe proporcionado al final del análisis.

Tipo de valor: Texto libre.

3.4 Criterio 4: Clasificación de errores

Nombre del criterio: Clasificación de errores.

Descripción: Es la capacidad para clasificar los errores encontrados según su gravedad.

Tipo de valor: Booleano (SI / NO).

3.5 Criterio 5: Recomendaciones

Nombre del criterio: Recomendaciones.

Descripción: Trata de ver si la herramienta proporciona recomendaciones para solucionar los errores encontrados o mejorar la seguridad del sitio web.

Tipo de valor: Booleano (SI / NO).

3.6 Criterio 6: Profundidad del análisis

Nombre del criterio: Profundidad del análisis.

Descripción: Trata de ver si el análisis ha sido superficial centrándose en aspectos generales o si ha profundizado llegando a detectar errores muy específicos.

Tipo de valor: Texto libre.

3.7 Criterio 7: Horas empleadas

Nombre del criterio: Horas empleadas.

Descripción: Cantidad de horas empleadas para llevar a cabo desde la instalación de la herramienta hasta el análisis de una plataforma web.

Tipo de valor: Numérico.

3.8 Criterio 8: Facilidad de uso

Nombre del criterio: Facilidad de uso.

Descripción: Complejidad para llevar a cabo el uso de las herramientas y realización del análisis.

Tipo de valor: Texto libre.

3.9 Criterio 9: Preparación para la implementación

Nombre del criterio: Preparación para la implementación.

Descripción: Necesidades que tenemos para llevar a cabo el escaneo como por ejemplo escribir código.

Tipo de valor: Texto libre.

3.10 Criterio 10: Recopilación de información

Nombre del criterio: Recopilación de información.

Descripción: Información recopilada sobre la herramienta para realizar el escaneo con éxito.

Tipo de valor: Booleano (SI / NO).

3.11 Criterio 11: Precio

Nombre del criterio: Precio.

Descripción: Cuánto cuesta la herramienta.

Tipo de valor: Texto libre.

4. Proyecto de implementación de un prototipo del sistema utilizando la herramienta Netsparker

4.1 Documentación de Descarga e Instalación

Vamos a la página oficial de Netsparker cuyo enlace es el siguiente:
<https://www.netsparker.com/web-vulnerability-scanner/>

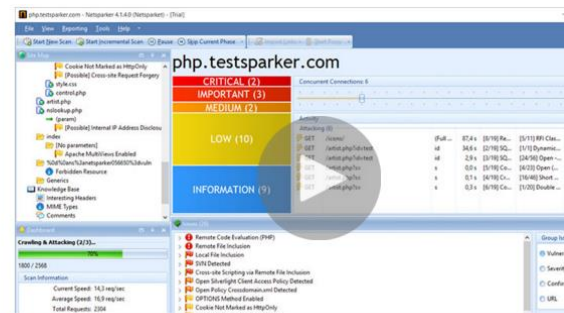
Ante todo, hay que decir que Netsparker es una herramienta disponible para los sistemas de Microsoft Windows Vista en adelante disponible únicamente en el idioma de Inglés.

Ya en la página principal lo primero que nos aparece es el apartado para la descarga de la demo gratuita de la herramienta ya que esta es una herramienta de pago, por lo que pulsaremos dicho botón para acceder a la página de las descargas.

What is Netsparker Desktop?

Netsparker Desktop is available as a Windows application and is an easy-to-use web application security scanner that uses the advanced Proof-Based vulnerability scanning technology and has built-in penetration testing and reporting tools.

DOWNLOAD DEMO



Una vez aquí rellenamos el siguiente cuestionario para proceder a la descarga.

netsparker

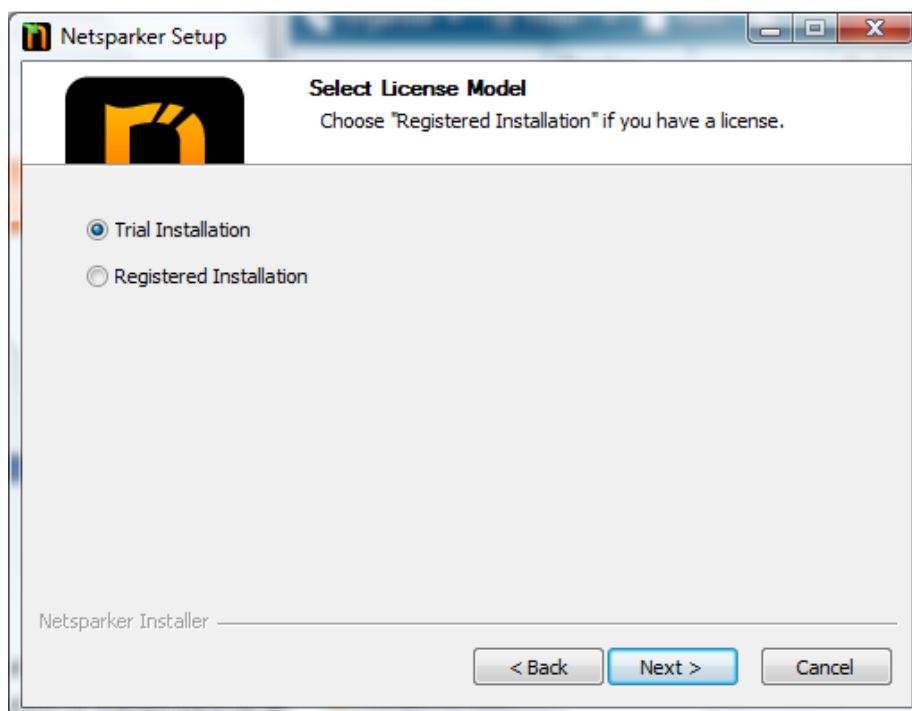
Download the demo of Netsparker Desktop to see how many vulnerabilities it can identify on your websites.

DOWNLOAD NOW

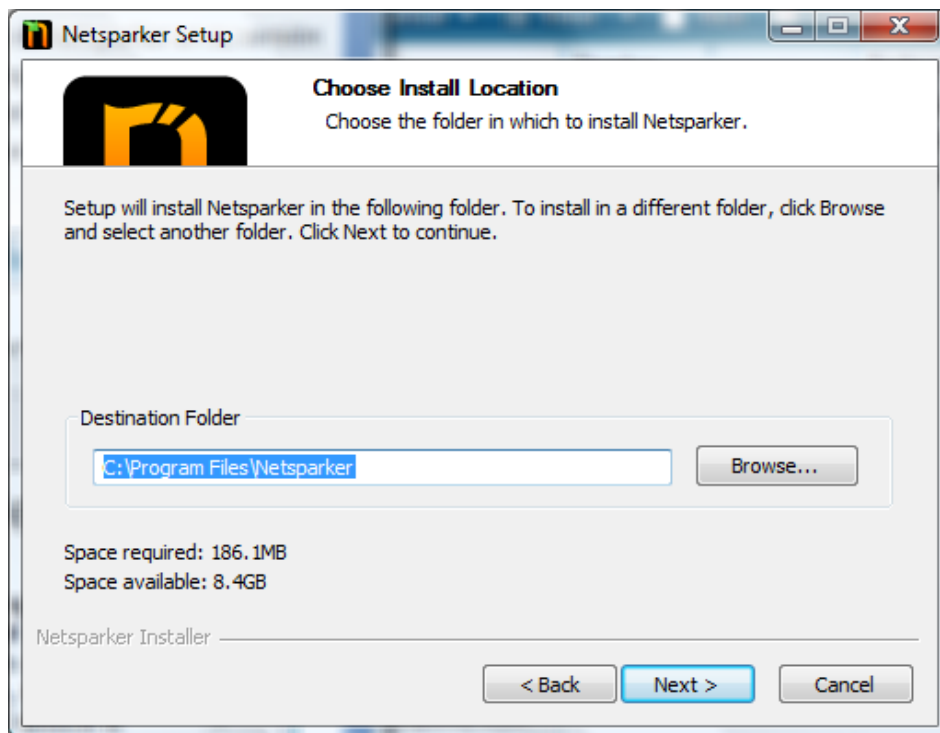
Una vez hemos rellenado el cuestionario descargamos el archivo de Netsparker en su versión de escritorio. Esta versión requiere una instalación previa en el equipo para su uso por lo que no es portable. Cuando tengamos el archivo descargado descargado ejecutamos el instalador llamado "NetsparkerSetup.exe". Lo primero que tenemos que hacer es aceptar los términos y condiciones legales.



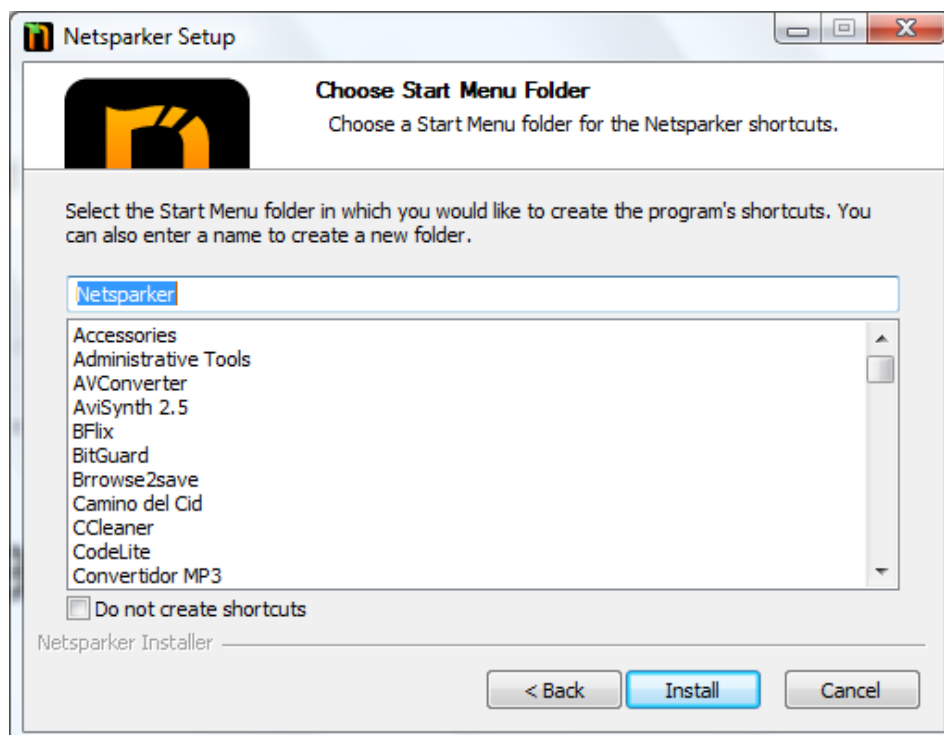
Aceptamos los términos y continuamos. Ahora elegimos el tipo de instalación, en este caso la versión de prueba.



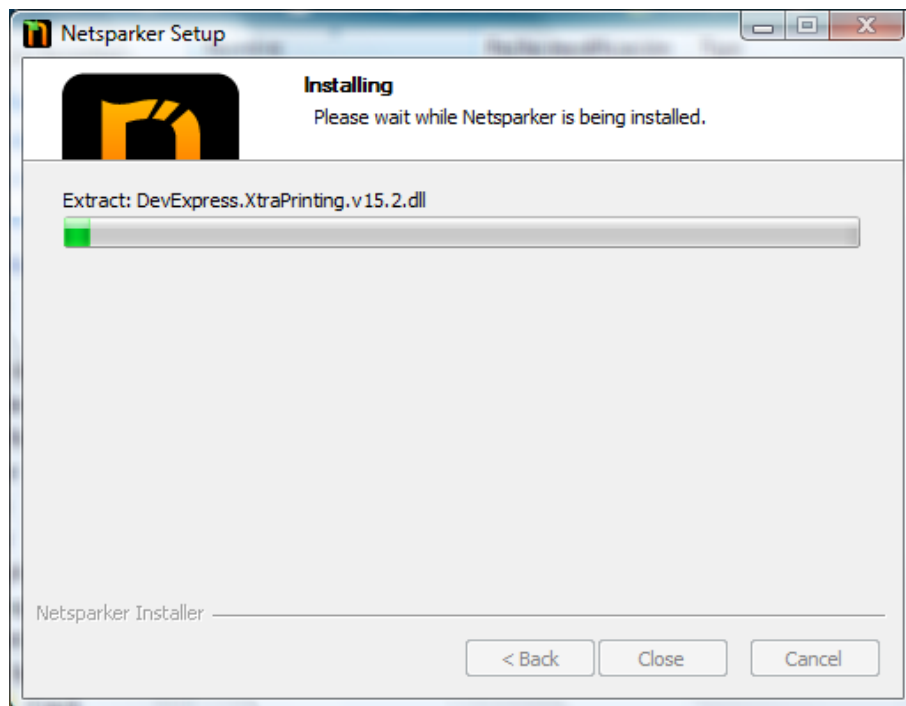
Ahora tendremos que seleccionar la ubicación donde instalaremos la herramienta.



Después nos pide que seleccionemos un atajo para acceder rápidamente al programa.

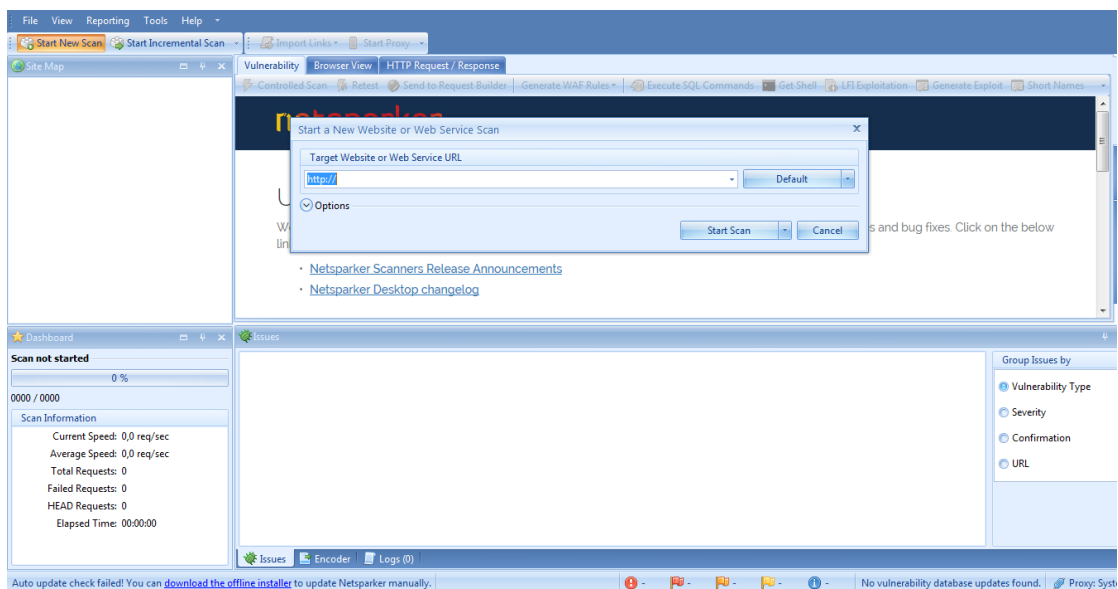


Y por último procedemos a instalar la herramienta:



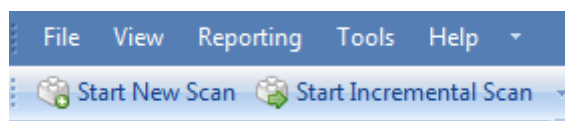
4.2 Documentación del Diseño

La primera vez que abrimos Netsparker nos aparece un mensaje informándonos del producto instalado y nos proporciona la forma de contacto con el representante de ventas de Netsparker en nuestro país, en este caso la representante es Marina Lekova y nos proporciona su correo electrónico y su número de teléfono. Una vez cerramos el mensaje nos aparece esta pantalla:



Desde el primer momento ya nos ofrece el escaneo de una web.

El programa consta de varios apartados para su manejo antes y después de realizar el escaneo de un sitio web.

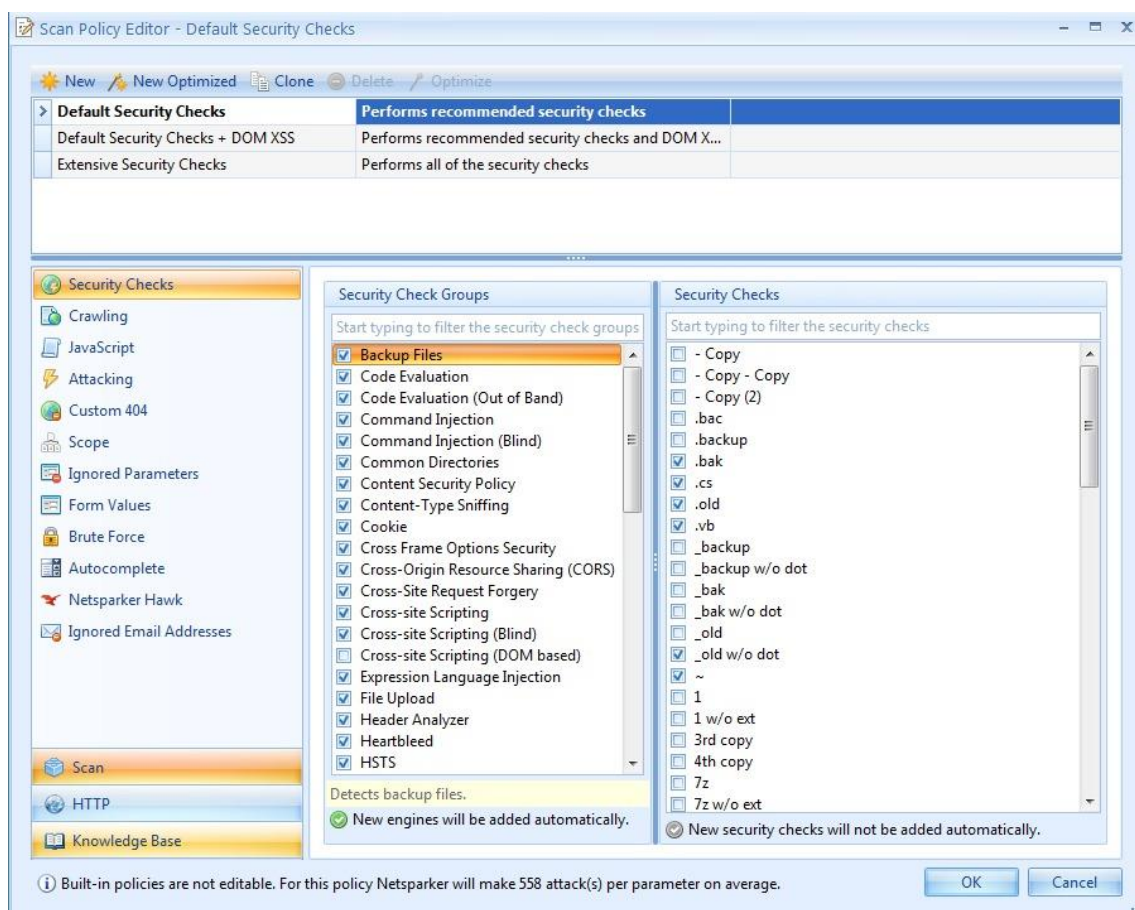


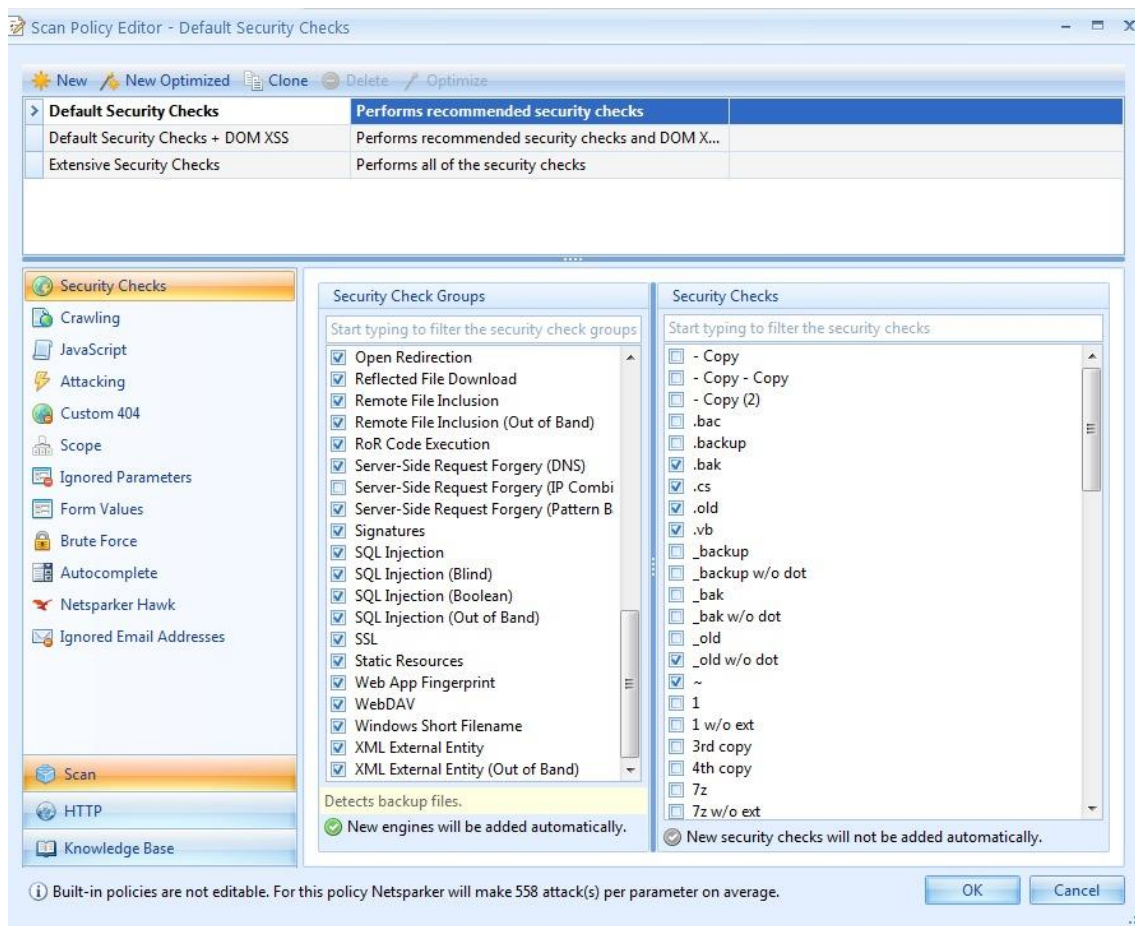
En "File" podemos encontrar opciones de importar y exportar, además de otras funciones específicas relacionadas con el escaneo como la de iniciar escaneo o analizar nuevo escaneo.

En "View" podemos habilitar y deshabilitar las distintas ventanas de Netsparker las cuales la mayor parte de ellas están habilitadas.

En "Reporting" tenemos las distintas formas en las que podemos ver los resultados del informe, tanto opciones como formatos.

En "Tools" podemos modificar las opciones de la herramienta acerca del proxy, almacenamiento, actualizaciones... y además podemos editar la política de exploración cuando vayamos a realizar un escaneo pudiendo seleccionar que elementos de seguridad queremos examinar y también podemos restablecer la configuración por defecto.

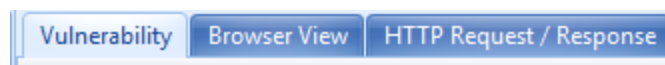




Aunque en la Demo de la realización de las pruebas no se pueden marcar más casillas para el análisis de la seguridad

En "Help" tenemos las opciones de ayuda así como actualizar licencias y cargarlas y soporte.

Aparte de esto tenemos estas ventanas que nos van a proporcionar información acerca del escaneo:

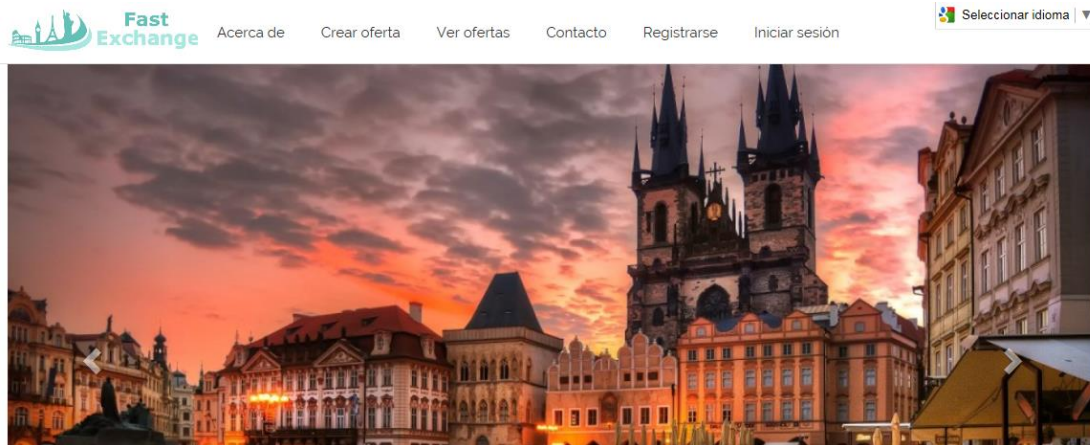


En la pestaña de "Vulnerability" vamos a poder ver todos los problemas de seguridad detectados por Netsparker una vez se haya realizado el escaneo. En la pestaña de "Browser View" podemos ver la web como si estuviéramos en el navegador y en la pestaña de "HTTP Request / Response" podemos ver el código de las cabeceras, parámetros, XML... de la web, pero solo nos va a dejar verlo en la versión de pago.

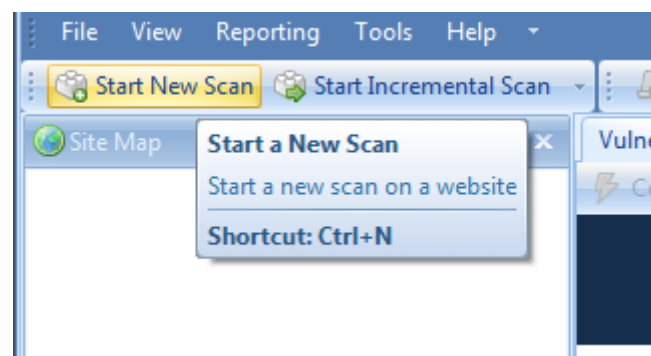
4.3 Documentación de la Preparación de la Ejecución

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.

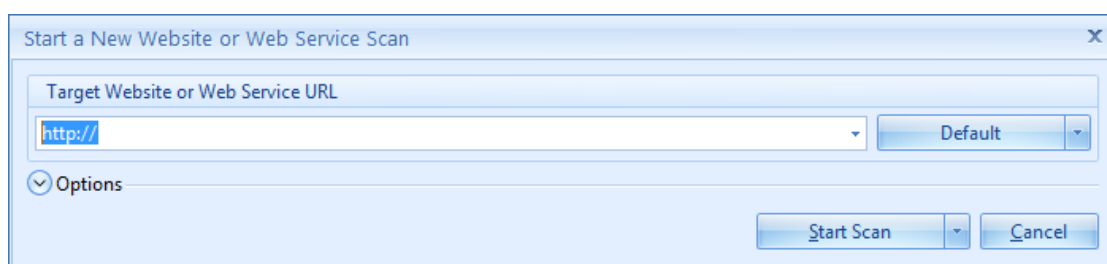
<https://miaplicacionweb.azurewebsites.net/>



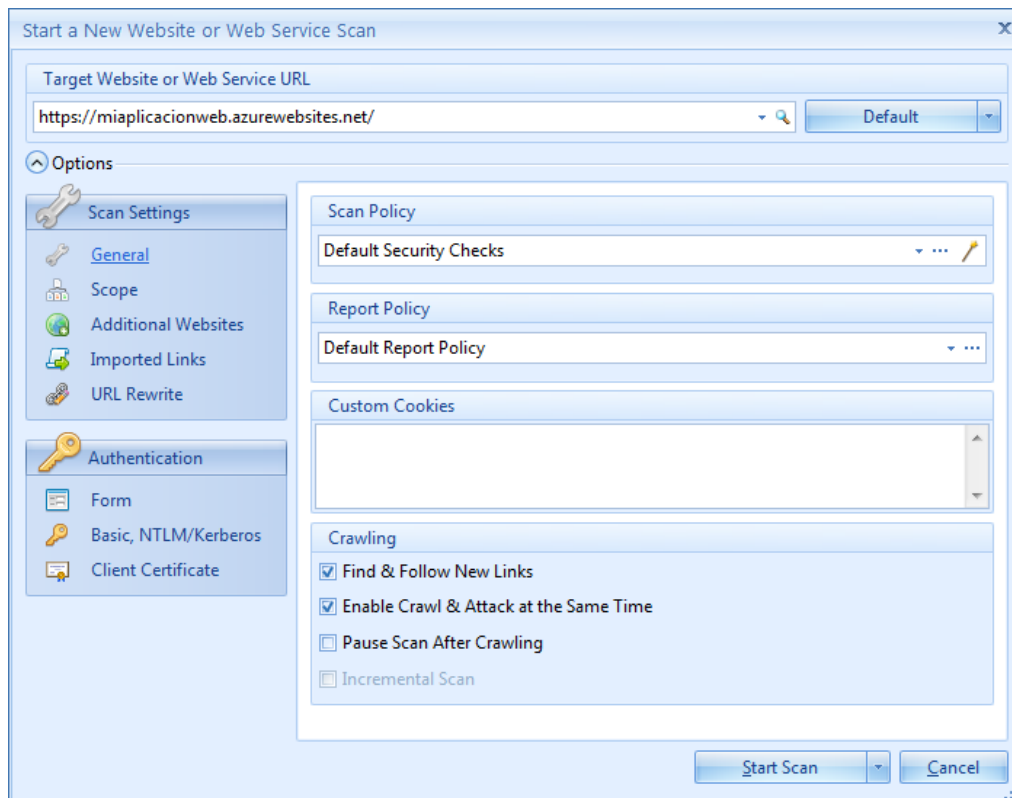
Lo primero que vamos a hacer en Netsparker es darle al botón de "Start New Scan" el cual lo podemos encontrar en el desplegable de "File" o en la interfaz principal.



Se abrirá la siguiente ventana sobre la que pondremos la dirección de la web y daremos a Options:

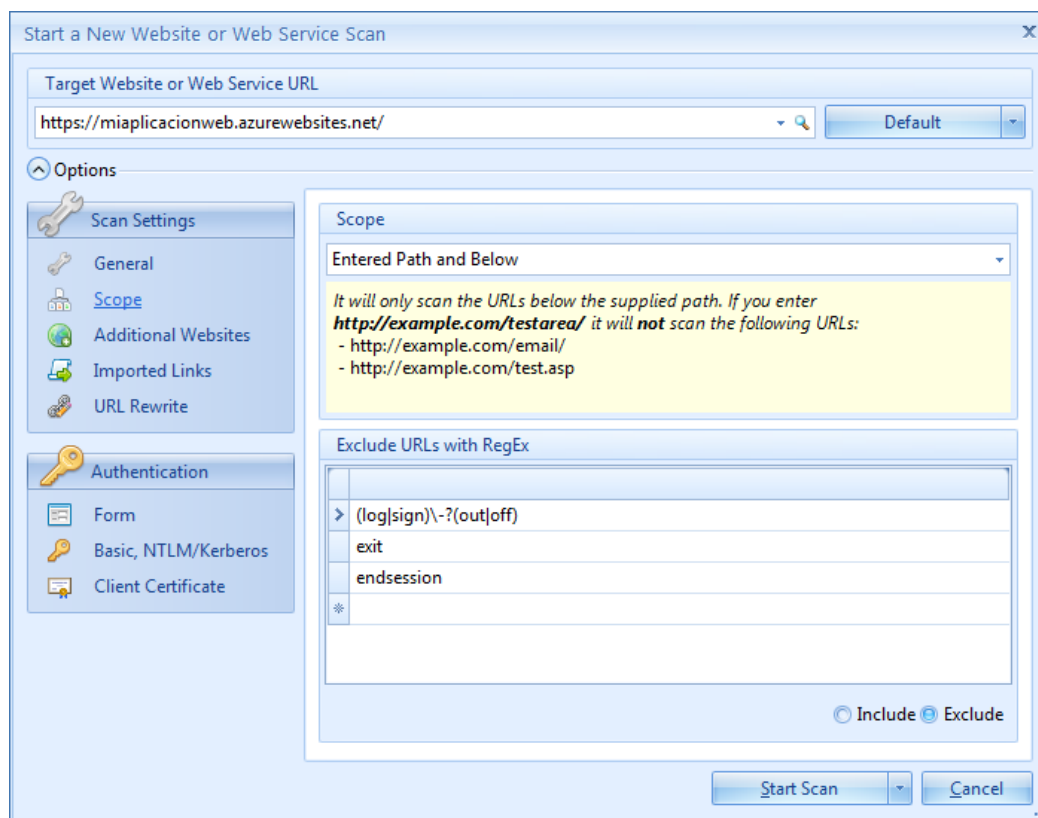


Quedaría de la siguiente manera:

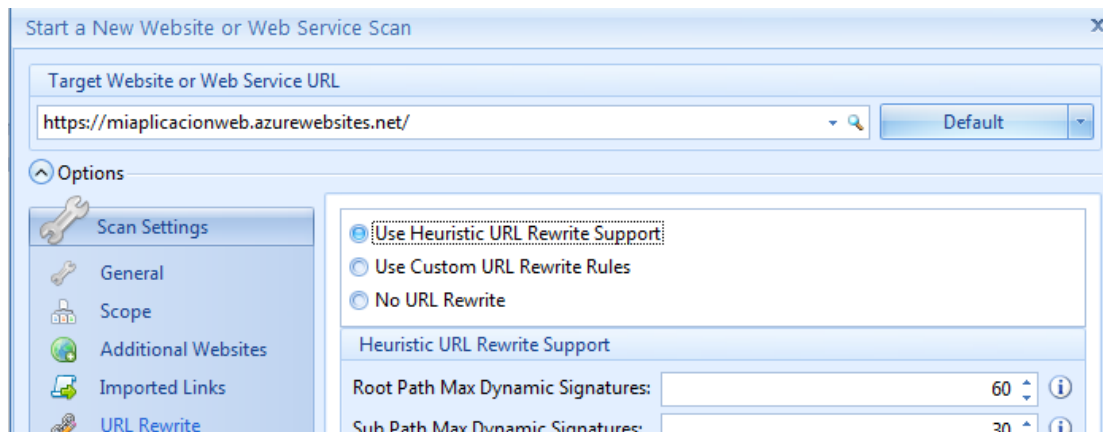


En las opciones generales no vamos a cambiar nada porque la política de escaneo predeterminada va analizar la seguridad de una manera bastante completa aunque si queremos lo podemos modificar. En las opciones de Scope seleccionaremos "Entered Path and Below" queremos que escanee la dirección principal y las que están por debajo como pueden ser:

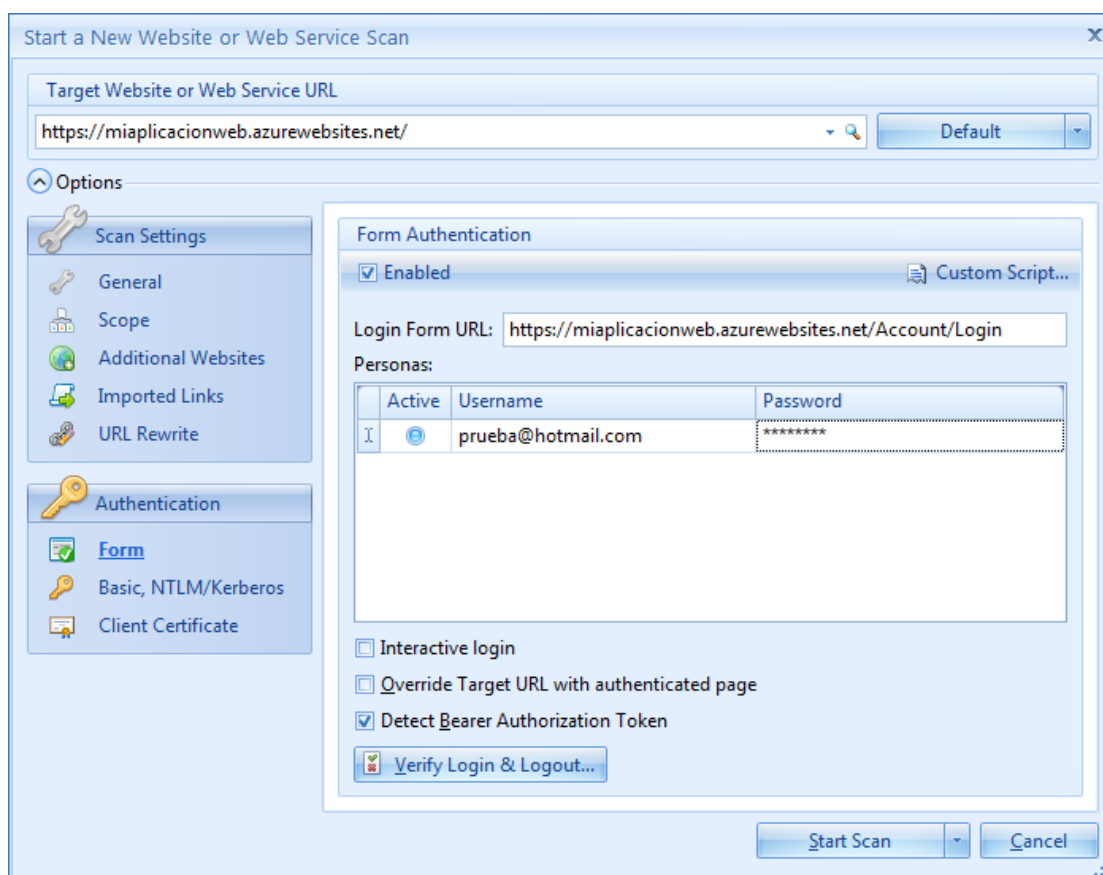
<https://miaplicacionweb.azurewebsites.net/CrearOferta/CrearOferta>



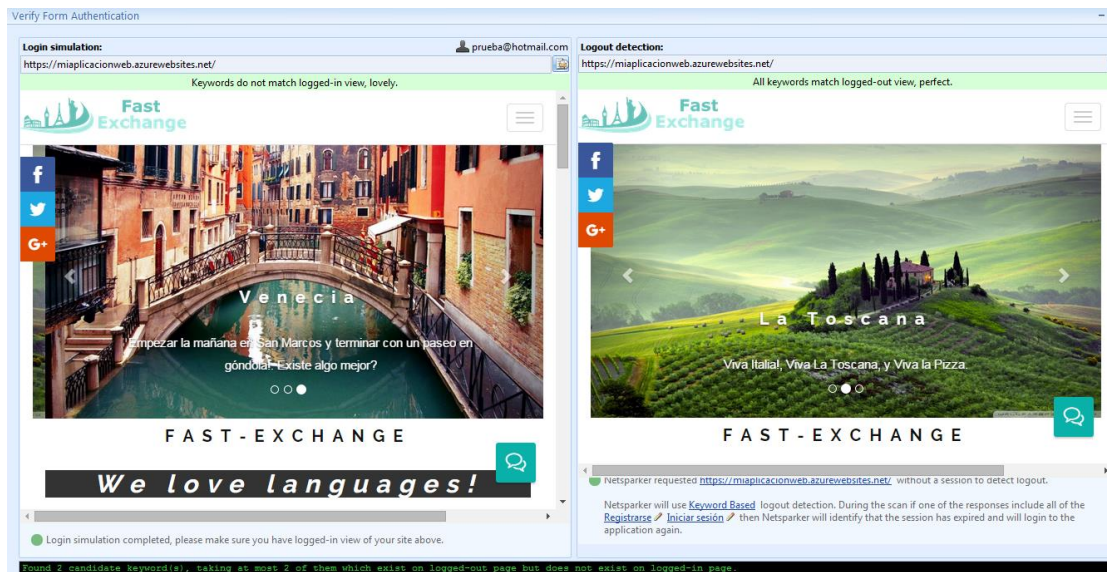
En Additional Websites no vamos a poner nada porque no tenemos enlaces a otros dominios disitintos. En Imported Links tampoco vamos a poner nada porque es para aplicar las reglas de alcance de exploración a los enlaces importados durante la exploración, pero nosotros no tenemos ninguno. En URL rewrite seleccionaremos "Uses Heuristic URL Rewrite Support" de tal forma que se identifiquen y analicen todos los parámetros.



Por último nos vamos a Form donde activaremos la casilla de Enabled y pondremos la URL para poder registrarnos. Además le tendremos que decir el nombre de usuario y contraseña. De esta forma Netsparker podrá analizar las funcionalidades que tenga un usuario determinado.



Después le damos al botón de verify y saldrá la siguiente pantalla donde comprobara que funciona correctamente tanto el log in como el logout del usuario con esos datos.



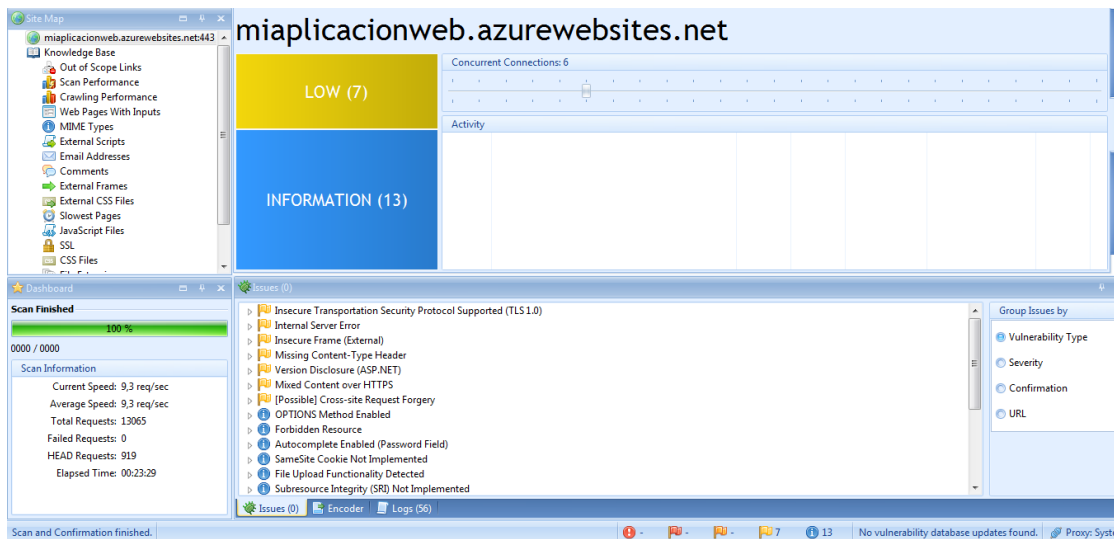
Una vez hecho eso le damos al botón de "Start Scan" y comenzaría la ejecución del escaneo del sitio web.

4.4 Documentación de los Informes de Errores

El análisis se realiza en tres fases en las cuales se realiza el escaneo de los errores de seguridad de distintos tipos. Las fases son las siguientes:

- Crawling.
- Crwiling & attacking.
- Recrawling.

Una vez terminado el escaneo nos muestra la siguiente pantalla:



En la parte inferior izquierda nos muestra un resumen del tiempo, velocidad y algunos datos más acerca del escaneo realizado.

Como podemos ver tenemos 7 errores leves y 13 errores de información. En la parte de abajo de la imagen podemos cada uno de los errores y si pichamos en uno de ellos nos saldrá una descripción del error encontrado.

Insecure Transportation Security Protocol Supported (TLS 1.0) CONFIRMED LOW

The technical details for this vulnerability are not available in the trial edition of Netsparker Desktop.

VULNERABILITY DETAILS

Netsparker detected that insecure transportation security protocol (TLS 1.0) is supported by your web server.

TLS 1.0 has several flaws. An attacker can cause connection failures and they can trigger the use of TLS 1.0 to exploit vulnerabilities like BEAST (Browser Exploit Against SSL/TLS).

Websites using TLS 1.0 will be considered non-compliant by PCI after 30 June 2018.

CLASSIFICATION	
PCI 3.1	6.5.4
PCI 3.2	6.5.4
OWASP 2013	A6
CWE	327
CABES	347

Issues (0)

- Insecure Transportation Security Protocol Supported (TLS 1.0)
- Internal Server Error
- Insecure Frame (External)
- Missing Content-Type Header
- Version Disclosure (ASP.NET)
- Mixed Content over HTTPS

Group Issues by:

- Vulnerability Type
- Severity
- Confirmation

Como podemos ver, hay una parte subrayada en amarillo. Esta nos indica que los para obtener los detalles técnicos de vulnerabilidad de dicho error necesitamos adquirir la versión de pago. Además si le damos a la flecha del error para que nos muestre más detalles nos dice esto:

Issues (0)

- Insecure Transportation Security Protocol Supported (TLS 1.0)
 - This path is only reported in the Standard and Professional editions of Netsparker
 - Internal Server Error
 - This path is only reported in the Standard and Professional editions of Netsparker [Variations:10]
 - Insecure Frame (External)

Dentro de la descripción del error nos dice el impacto que ha tenido y algunos remedios que puede tener además de algunas referencias externas. Los errores de seguridad que hemos encontrado son los siguientes:

Issues (0)

- Insecure Transportation Security Protocol Supported (TLS 1.0)
- Internal Server Error
- Insecure Frame (External)
- Missing Content-Type Header
- Version Disclosure (ASP.NET)
- Mixed Content over HTTPS
- [Possible] Cross-site Request Forgery
- OPTIONS Method Enabled
- Forbidden Resource
- Autocomplete Enabled (Password Field)
- SameSite Cookie Not Implemented
- File Upload Functionality Detected
- Subresource Integrity (SRI) Not Implemented
- ASP.NET Identified
- Version Disclosure (IIS)
- Content Security Policy (CSP) Not Implemented
- Email Address Disclosure
- Out-of-date Version (jQuery)
- HTTP Strict Transport Security (HSTS) Policy Not Enabled
- Missing X-XSS Protection Header
- Knowledge Base

Los errores de mayor gravedad son los siguientes:

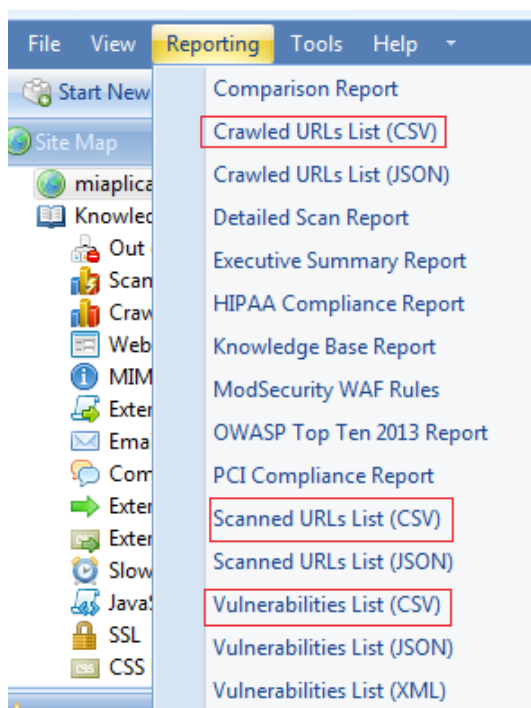
- Insecure Transportation Security Protocol Supported (TLS 1.0): Se detectó que el protocolo de seguridad de transporte inseguro (TLS 1.0) es compatible con el servidor web. TLS 1.0 tiene varios defectos. Un atacante puede causar fallos de conexión y pueden activar el uso de TLS 1.0 para explotar vulnerabilidades como BEAST (explorador contra SSL / TLS). Los atacantes pueden realizar ataques man-in-the-middle y observar el tráfico de cifrado entre su sitio web y sus visitantes.
- Internal Server Error: El servidor respondió con un estado HTTP 500, indicando que hay un error en el lado del servidor. Las razones pueden variar, y el comportamiento debe ser analizado cuidadosamente. En general, esto indica que las prácticas de codificación utilizadas en la web son deficientes y no es suficiente la comprobación de errores. Sin embargo, podría haber un problema más grande, como la inyección de SQL.
- Insecure Frame (External): Se identificó un iframe externo inseguro o mal configurado. Cuando se establece el atributo sandbox contenido iframe se trata como si fuese de un origen único y el contenido en área reducida se vuelve a alojar en el navegador con varias restricciones. Cuando no se ha configurado o se ha configurado erróneamente sandbox o el atributo seamless tiene fisuras puede que tengamos problemas como que el sitio Web comprometido en el iframe puede afectar a los usuarios en la aplicación web principal.
- Missing Content – Type Header: Se detectó un encabezado missing Content-Type lo que significa que este sitio web podría estar en riesgo de ataques MIME-sniffing. El problema surge una vez que un sitio web permite a los usuarios cargar contenido que luego se publica en el servidor web. Si un atacante puede realizar ataques XSS (Cross-site Scripting) manipulando el contenido de manera que sea aceptado por la aplicación web y representada como HTML por el navegador, es posible inyectar código en, por ejemplo, un archivo de imagen y hacer que La víctima lo ejecuta viendo la imagen.
- Version Disclosure (ASP.NET): Se identificó una revelación de versión (ASP.NET) en la respuesta HTTP del servidor web de destino. Esta información puede ayudar a un atacante obtener una mayor comprensión de los sistemas en uso y potencialmente desarrollar nuevos ataques dirigidos a la versión específica de ASP.NET. Un atacante podría usar la información divulgada para recolectar vulnerabilidades de seguridad específicas para la versión identificada.
- Mixed Content Over HTTPS: Se detectó un contenido mixto cargado en HTTP dentro de una página HTTPS. Si la página HTTPS incluye contenido recuperado a través de HTTP normal y de texto claro, la conexión sólo se cifra parcialmente. El contenido sin cifrar es accesible para los sniffers. Un atacante en el medio puede interceptar la solicitud para el contenido HTTP y también reescribir la respuesta para incluir código JavaScript malicioso. El contenido activo malintencionado puede robar las credenciales del usuario, adquirir datos confidenciales sobre el usuario o intentar instalar malware en el sistema del usuario (aprovechando las vulnerabilidades del navegador o de sus complementos, por ejemplo) y, por lo tanto, la conexión ya no está protegida.
- (Possible) Cross – site Request Forgery: Se identificó un posible Cross-Site Request Falsificación. CSRF es una vulnerabilidad muy común. Es un ataque que obliga al usuario a ejecutar acciones no deseadas en una aplicación web en la que el usuario está actualmente autenticado. Dependiendo de la aplicación, un atacante puede montar cualquiera de las acciones que puede realizar el usuario, como agregar un usuario, modificar el contenido o eliminar datos. Toda la funcionalidad disponible para la víctima puede ser utilizada por el atacante. La única excepción a esta regla es una página que requiere

información adicional que sólo el usuario legítimo puede conocer (como la contraseña del usuario).

Una vez terminado el análisis podemos exportar los resultados de varias maneras. Una es ir a "Files y dar a export el cual nos guardará los resultados del análisis en un formato para poder ser leídos y abiertos desde Netsparker otra vez.



También lo que podemos hacer es irnos al desplegable de "Reporting" y decir como lo queremos. En este caso vamos a guardar tres informes en los formatos que vemos en la siguiente imagen:



Crawled URLs List (CSV):

URL	Method	POST Params	JSON Params	XML Params	Response Status Code	Response Time	Parsing Source
https://miaplicacio	GET				200	262,7	StartLink
https://miaplicacio	GET				404	54,7	RelatedLink
https://miaplicacio	GET				200	62,5	RelatedLink
https://miaplicacio	GET				200	54,7	TextParser
https://miaplicacio	GET				200	54,7	TextParser
https://miaplicacio	GET				403	109,4	RelatedLink
https://miaplicacio	GET				200	62,5	RelatedLink
https://miaplicacio	GET				200	179,7	TextParser
https://miaplicacio	GET				200	46,9	TextParser
https://miaplicacio	GET				200	54,7	RelatedLink
https://miaplicacio	GET				200	54,7	TextParser
https://miaplicacio	GET				200	54,7	TextParser
https://miaplicacio	GET				403	62,5	RelatedLink
https://miaplicacio	GET				200	234,4	RelatedLink
https://miaplicacio	GET				200	156,3	TextParser
https://miaplicacio	GET				200	62,5	RelatedLink
https://miaplicacio	GET				200	54,7	TextParser
https://miaplicacio	GET				200	65,4	TextParser
https://miaplicacio	GET				404	74,2	RelatedLink
https://miaplicacio	GET				200	81,1	TextParser
https://miaplicacio	GET				404	62,5	RelatedLink
https://miaplicacio	GET				200	86,9	TextParser
https://miaplicacio	GET				200	96,7	TextParser

Scanned URLs List (CSV):

URL	Method	POST Param	JSON Param	XML Param	Attacked Parameters	Response Status Code	Response Time
https://miaplicacionweb.a:GET						200	262,7
https://miaplicacionweb.a:GET						404	54,7
https://miaplicacionweb.a:GET						200	62,5
https://miaplicacionweb.a:GET					v	200	54,7
https://miaplicacionweb.a:GET						403	109,4
https://miaplicacionweb.a:GET						200	62,5
https://miaplicacionweb.a:GET					v	200	179,7
https://miaplicacionweb.a:GET						200	54,7
https://miaplicacionweb.a:GET					v	200	54,7
https://miaplicacionweb.a:GET						403	62,5
https://miaplicacionweb.a:GET						200	234,4
https://miaplicacionweb.a:GET					v	200	156,3
https://miaplicacionweb.a:GET						200	62,5
https://miaplicacionweb.a:GET						200	54,7
https://miaplicacionweb.a:GET						200	65,4
https://miaplicacionweb.a:GET						404	74,7

Vulnerabilities URLs List (CSV):

Vulnerability	URL	Severity	Parameter	ParameterType
Internal Server Error		Low		
Version Disclosure (ASP.NET)		Low		
Insecure Frame (External)		Low		
Missing Content-Type Header		Low		
Insecure Transportation Security Protocol Supported (TLS 1.0)		Low		
[Possible] Cross-site Request Forgery		Low		
Mixed Content over HTTPS		Low		
Forbidden Resource		Information		
File Upload Functionality Detected		Information		
ASP.NET Identified		Information		
Email Address Disclosure		Information		
Version Disclosure (IIS)		Information		
HTTP Strict Transport Security (HSTS) Policy Not Enabled		Information		
OPTIONS Method Enabled		Information		
Autocomplete Enabled (Password Field)		Information		
Out-of-date Version (jQuery)		Information		
Missing X-XSS Protection Header		Information		
SameSite Cookie Not Implemented		Information		
Subresource Integrity (SRI) Not Implemented		Information		
Content Security Policy (CSP) Not Implemented		Information		

Y por último aquí nos deja Netsparker su resumen de los resultados que ha obtenido:

NETSPARKER SCAN REPORT SUMMARY

TARGET URL	https://miaplicacionweb.azurewebsites.net/	Total Requests	13065
SCAN DATE	29/04/2017 23:21:36	Average Speed	9,26 req/sec.
REPORT DATE	01/05/2017 13:57:32		
SCAN DURATION	00:23:31		
NETSPARKER VERSION	4.8.1.14376-4.8.1-hf1-9a19bce		

20
Identified

9
Confirmed

0
Critical

13
Informational

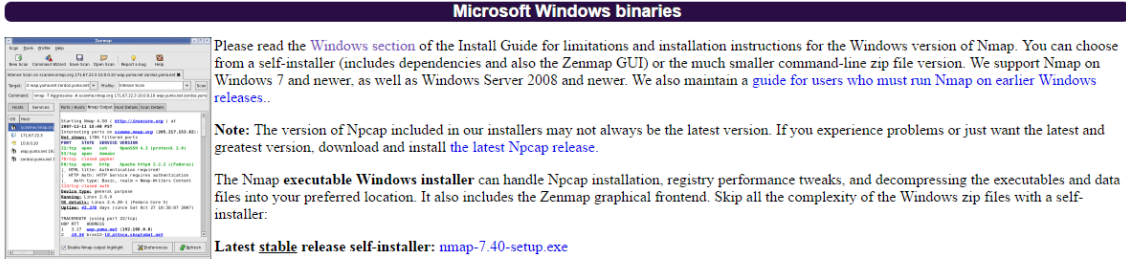
SCAN SETTINGS

ENABLED ENGINES	SQL Injection, SQL Injection (Boolean), SQL Injection (Blind), Cross-site Scripting, Command Injection, Command Injection (Blind), Local File Inclusion, Remote File Inclusion, Code Evaluation, HTTP Header Injection, Open Redirection, Expression Language Injection, Web App Fingerprint, RoR Code Execution, WebDAV, Reflected File Download, Insecure Reflected Content, XML External Entity, File Upload, Windows Short Filename, Server-Side Request Forgery (Pattern Based), Cross-Origin Resource Sharing (CORS), HTTP Methods, Server-Side Request Forgery (DNS), SQL Injection (Out of Band), XML External Entity (Out of Band), Cross-site Scripting (Blind), Remote File Inclusion (Out of Band), Code Evaluation (Out of Band)	Authentication Scheduled
URL REWRITE MODE	Heuristic	
DETECTED URL	/Intercambios/Edit/{param1}	
REWRITE RULES	/Intercambios/Details/{param1} /Intercambios/Delete/{param1} /FacturaIntercambios/Delete/{param1} /FacturaIntercambios/Edit/{param1} /FacturaIntercambios/Details/{param1}	

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

5.1 Documentación de Descarga e Instalación

Nos vamos a la sección de [Descargas](#) 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.



Microsoft Windows binaries

Please read the [Windows section](#) of the Install Guide for limitations and installation instructions for the Windows version of Nmap. You can choose from a self-installer (includes dependencies and also the Zenmap GUI) or the much smaller command-line zip file version. We support Nmap on Windows 7 and newer, as well as Windows Server 2008 and newer. We also maintain a [guide for users who must run Nmap on earlier Windows releases](#).

Note: The version of Npcap included in our installers may not always be the latest version. If you experience problems or just want the latest and greatest version, download and install the [latest Npcap release](#).

The Nmap executable Windows installer can handle Npcap installation, registry performance tweaks, and decompressing the executables and data files into your preferred location. It also includes the Zenmap graphical frontend. Skip all the complexity of the Windows zip files with a self-installer:

Latest stable release self-installer: [nmap-7.40-setup.exe](#)

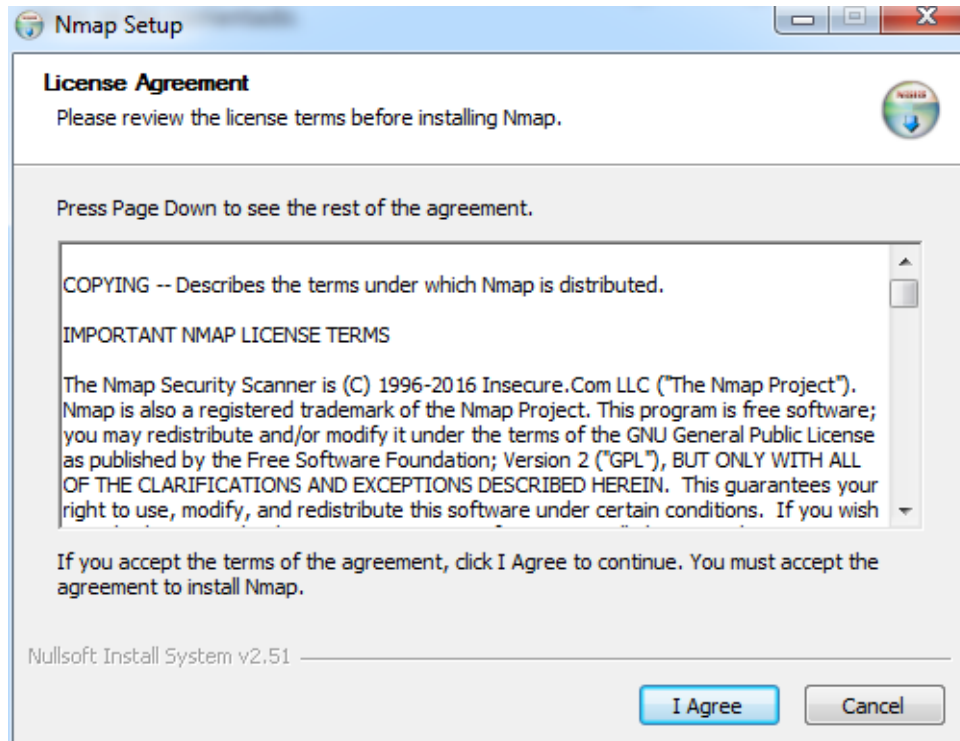
We have written [post-install usage instructions](#). Please [notify us](#) if you encounter any problems or have suggestions for the installer.

For those who prefer the command-line zip files ([Installation Instructions](#); [Usage Instructions](#)), they are still available. The Zenmap graphical interface is *not* included with these, so you need to run nmap.exe from a DOS/command window. Or you can download and install a superior command shell such as those included with the free [Cygwin system](#). Also, you need to run the [Npcap](#) and [Microsoft Visual C++ 2013 Redistributable Package](#) installers which are included in the zip file. The main advantage is that these zip files are a fraction of the size of the executable installer:

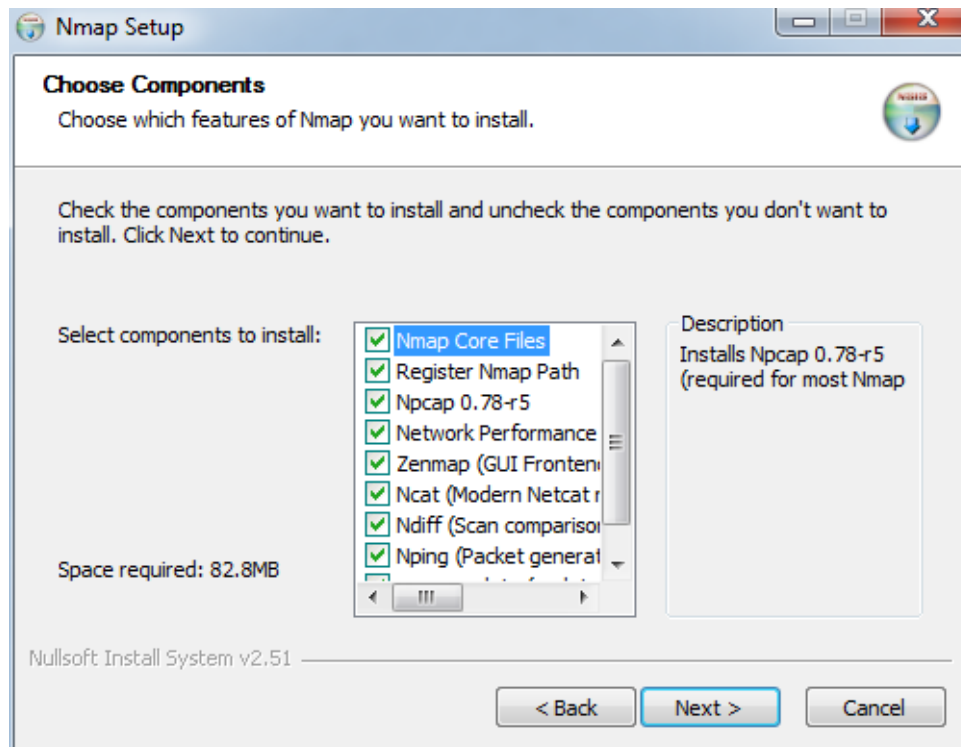
Latest stable command-line zipfile: [nmap-7.40-win32.zip](#)

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

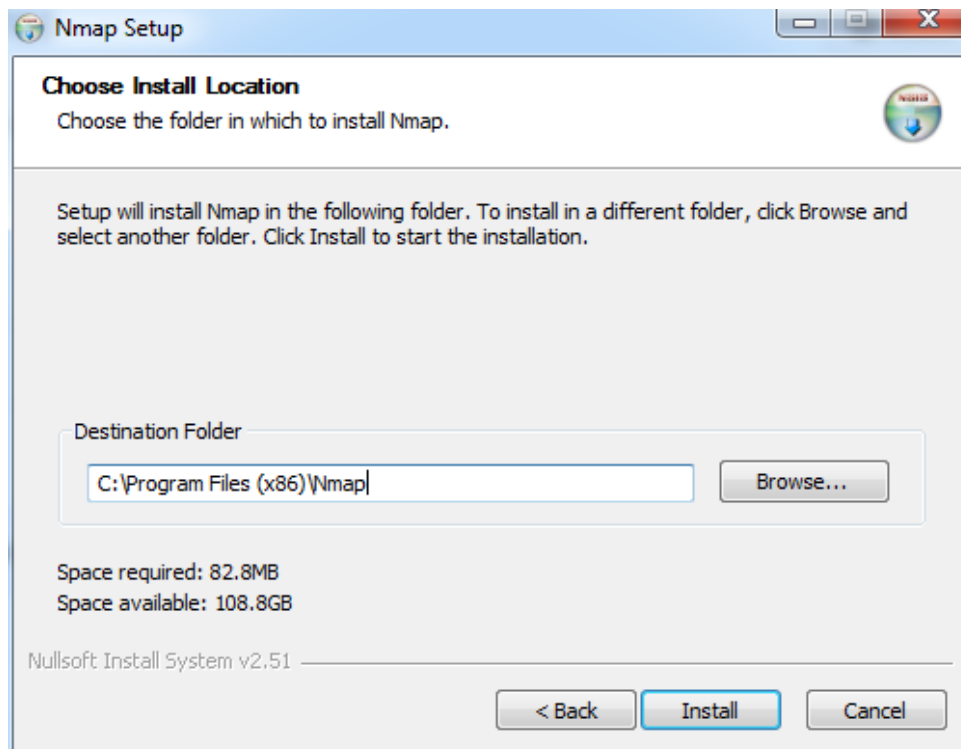
Al empezar la instalación lo primero que nos indica es que tenemos que aceptar los términos y condiciones de la herramienta:



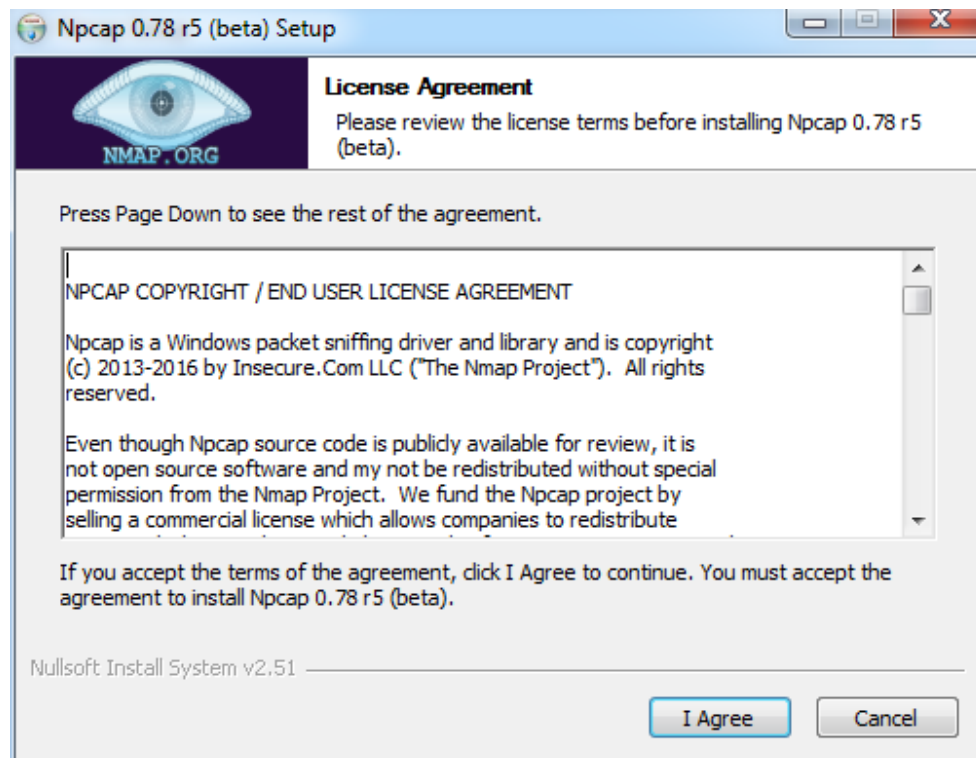
Ahora elegimos todos los componentes que queremos instalar para un profundo análisis de la herramienta:



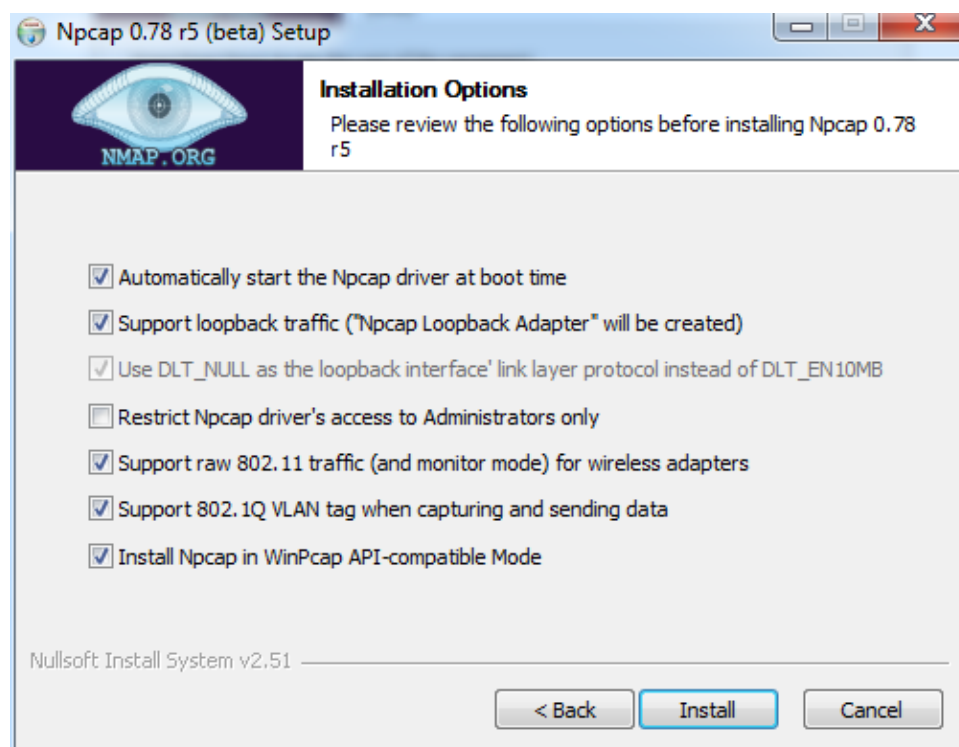
Ahora elegimos el directorio donde se ubicará la instalación:



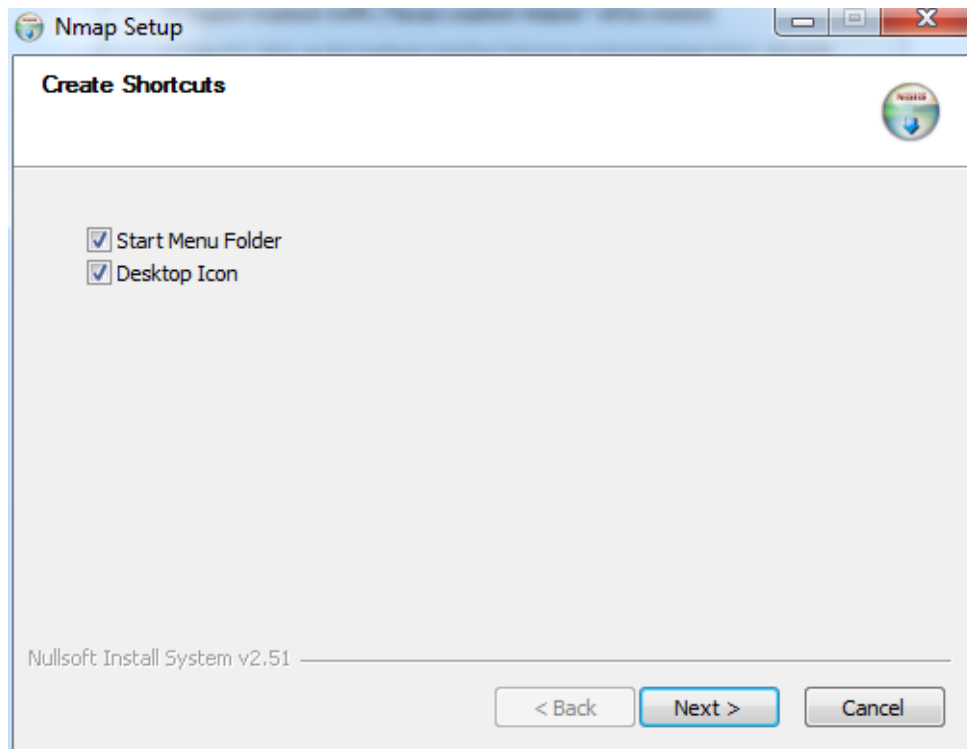
Mientras se instala la herramienta nos ofrecen instalar la función de Npcap:



Lo instalamos con los siguientes requisitos:



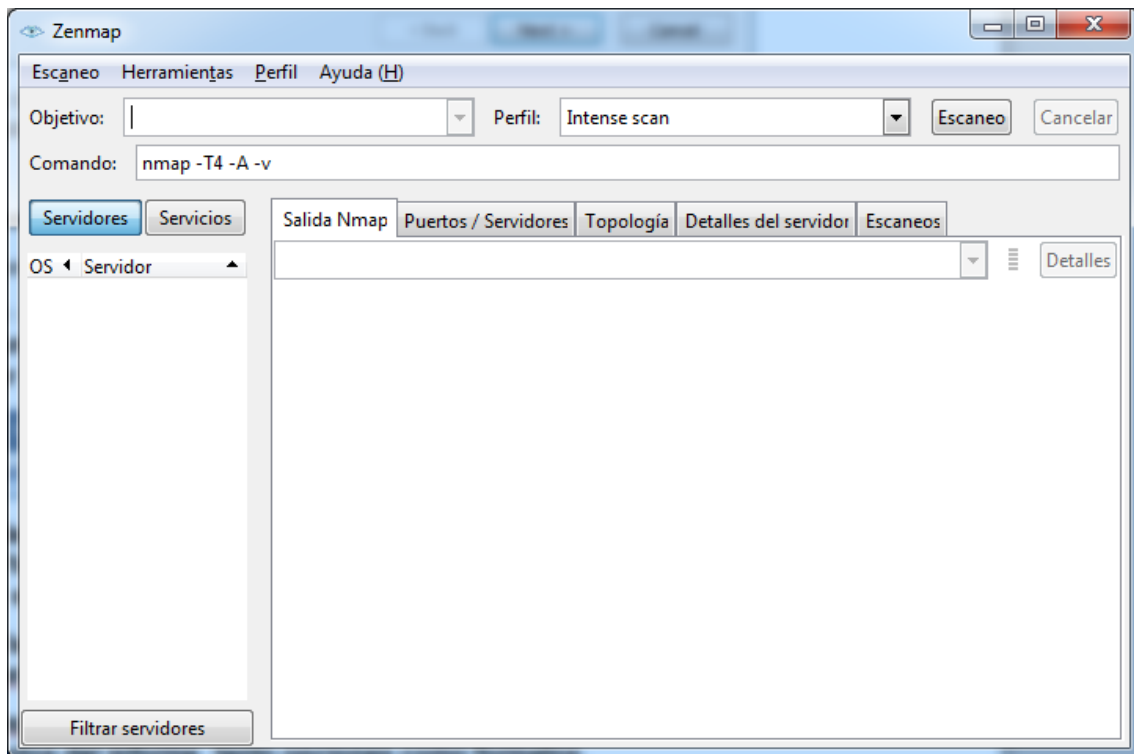
Al finalizar la instalación nos da la opción de crearnos un acceso directo en el Menú de Inicio y/o en el Escritorio:



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

5.2 Documentación del 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:



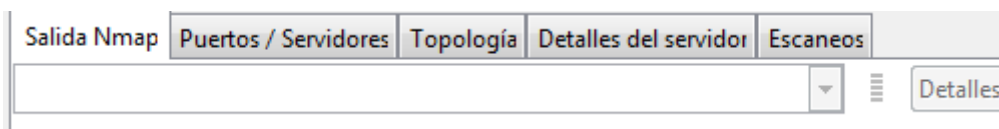
En la pestaña "Escaneo" podemos encontrar opciones de abrir un nuevo escaneo, guardarlo o salir de la aplicación.

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.

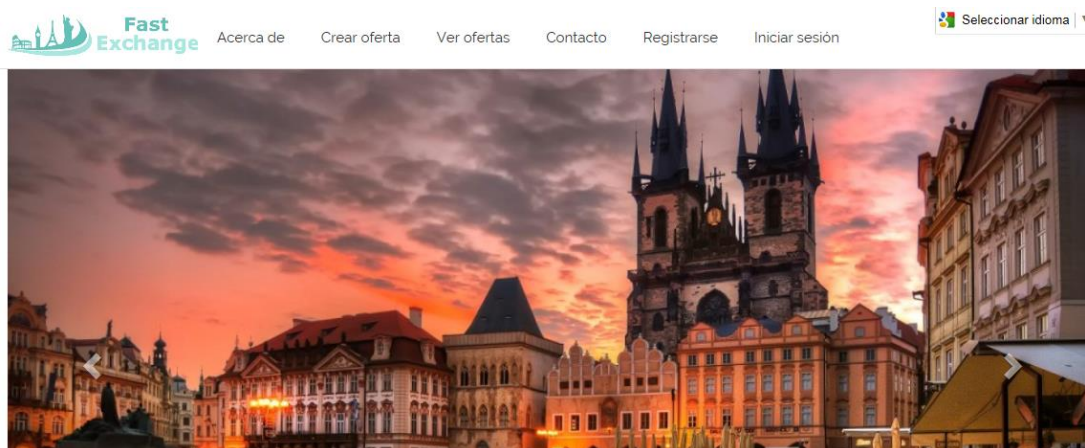
Aparte de estas cuatro pestañas tenemos las siguientes ventanas que nos dará información acerca del escaneo realizado:



5.3 Documentación de la Preparación de la Ejecución

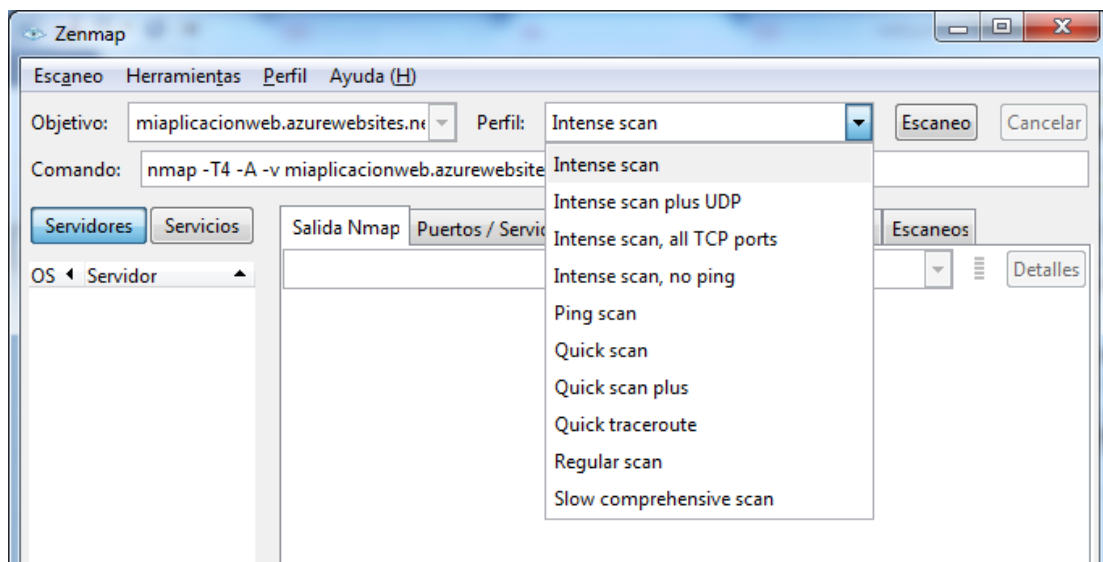
Este es el sitio web del prototipo, llamado Fast Exchange, sobre el cual vamos a hacer el análisis de seguridad con la herramienta de Netsparker.

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



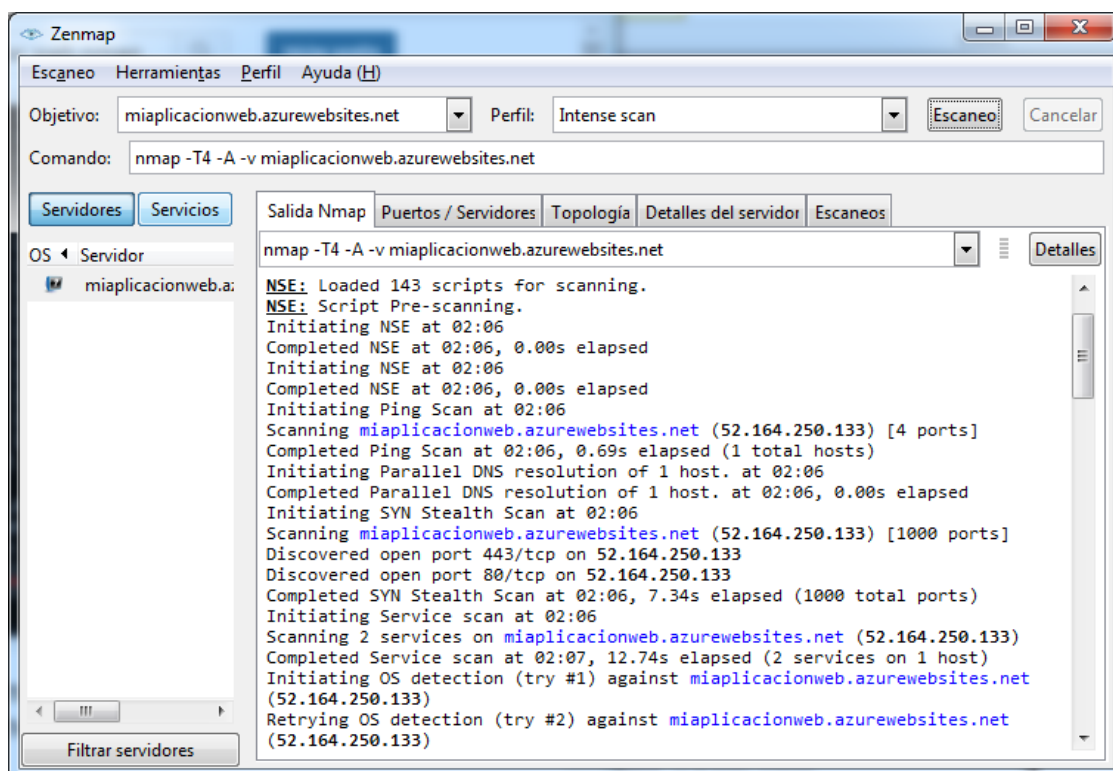
Lo primero que vamos a hacer en Nmap es poner la dirección en el apartado de "Objetivo", después elegir el Perfil o Comando a ejecutar y clicamos en "Escaneo".

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):



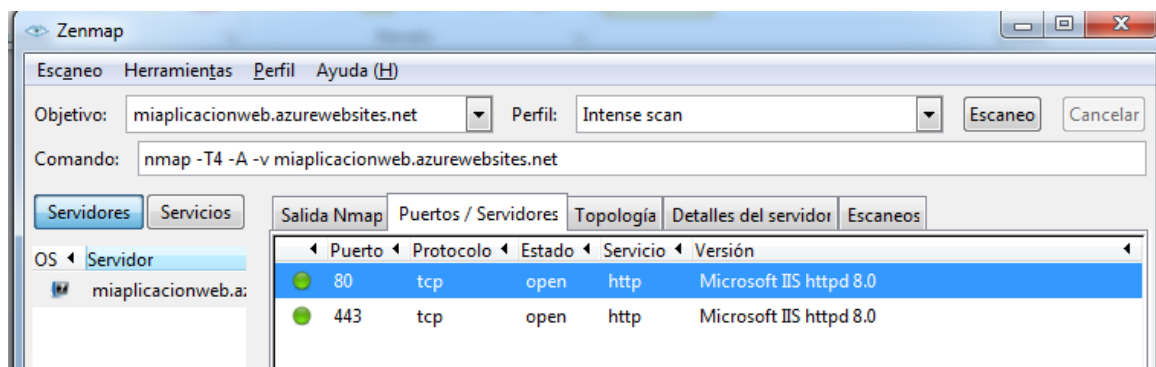
5.4 Documentación de los Informes de Errores

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:



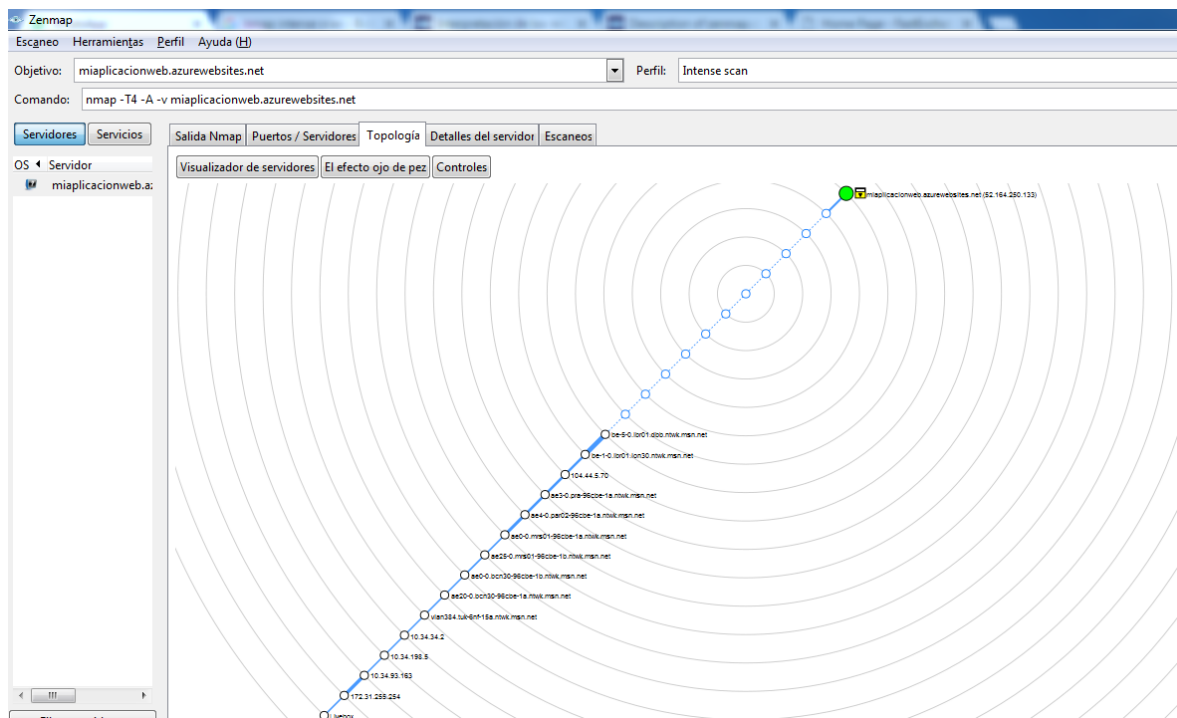
Observamos el nombre del servidor que se encuentra en el apartado izquierdo, en la pestaña de “Salida Nmap” que es la que se muestra en la anterior imagen, muestra de forma predeterminada cuando se ejecuta una exploración o búsqueda.

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

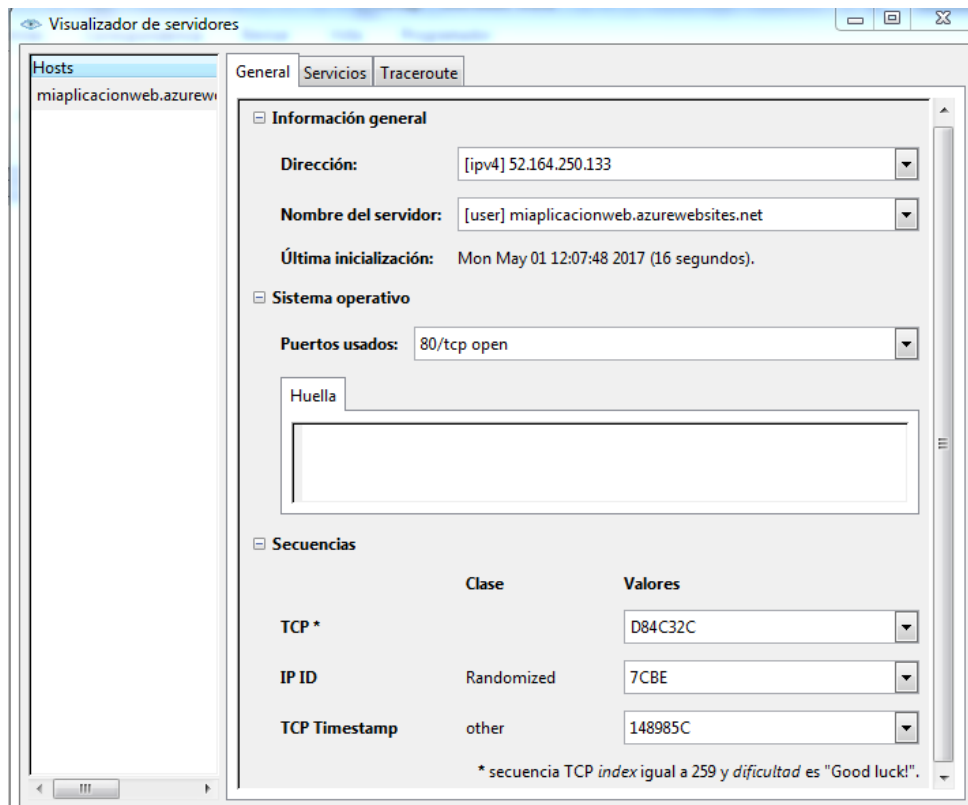


Podemos comprobar que esta página se basa en 2 puertos: 80 y el 443 y se están usando de una manera correcta sin ningún tipo de fallo y abierto al estar de color verde, si estuviera de color rojo se encontraría cerrado por algún tipo de fallo.

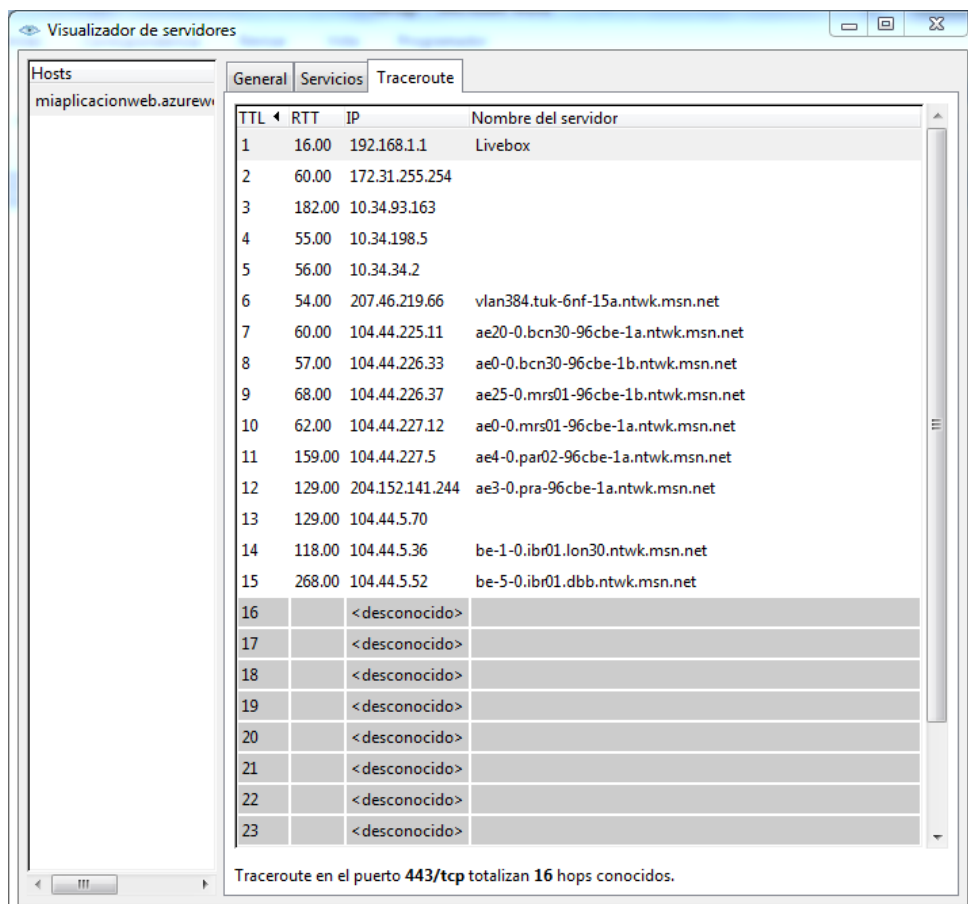
En la pestaña de “Topología” nos muestra el camino que pasa el ping que realizamos desde nuestro Router (Livebox) hasta el servidor final de la página web. Nos muestra el efecto Ojo de pez en una gráfica:



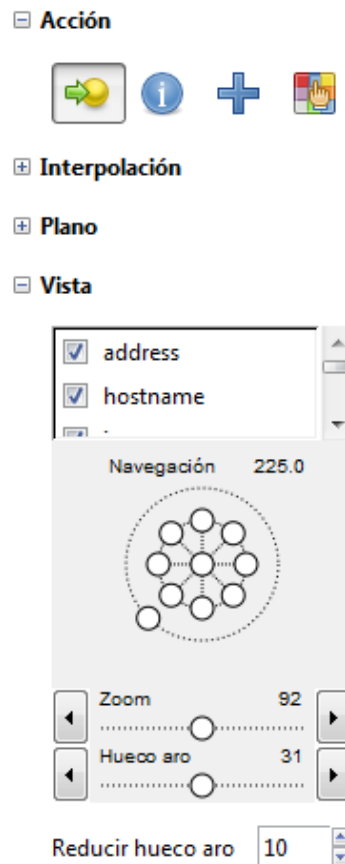
Si clicamos sobre la opción del Visualizador de servidores, nos muestra toda la información de estos:



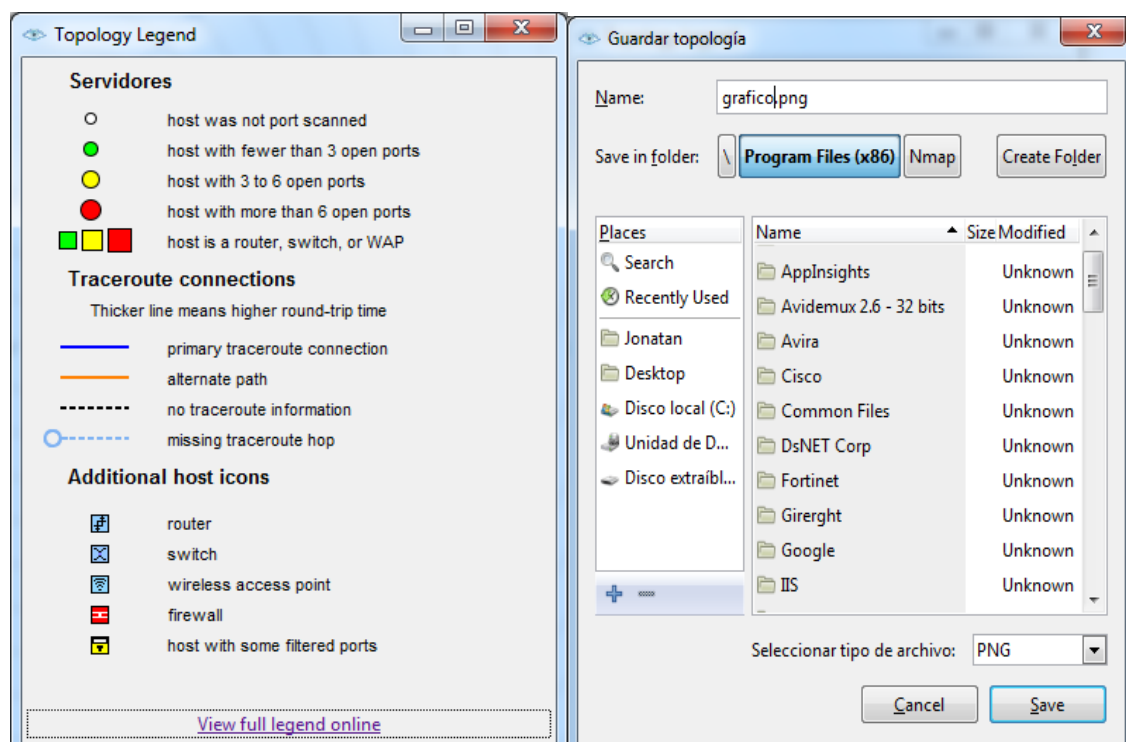
Además de ello si nos vamos a la pestaña de Traceroute nos comenta de una manera más detalla todas las IP que ha localizado y las que no añadiéndolas como desconocidas, en nuestro caso 16:



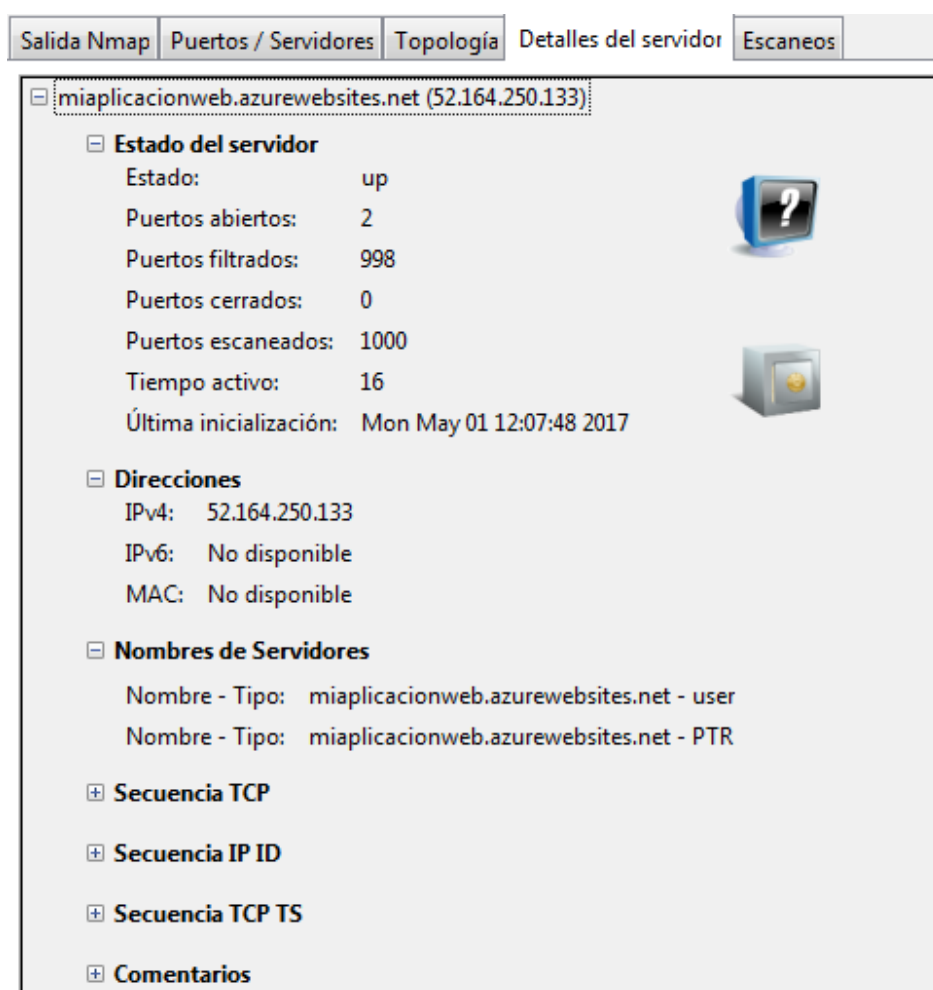
Si damos al botón de efecto de ojo de pez, se nos muestra de manera aumentada el gráfico. Además cabe destacar el botón de Controles, ya que nos da la opción de personalizar el gráfico a nuestro antojo:



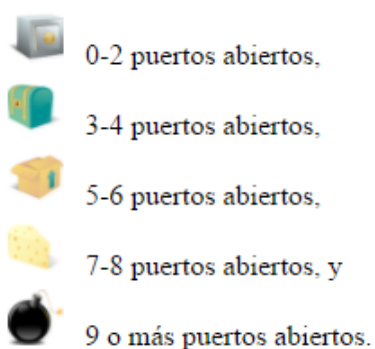
Y como últimas opciones que nos da la Tipología es la Leyenda del gráfico y la opción de Guardar el mismo:



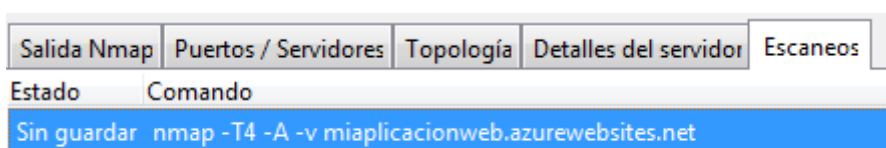
Continuamos ahora con la pestaña “Detalles del servidor”:



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
```

Comando: `nmap -p 1-65535 -T4 -A -v miaplicacionweb.azurewebsites.net`

ServidoresServicios

OS Servidor

miaplicacionweb.a

Salida Nmap

Puertos / Servidores

Topología

Detalles del servidor

Escaneos

nmap -p 1-65535 -T4 -A -v miaplicacionweb.azurewebsites.net

NSE: Loaded 143 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 13:30
Completed NSE at 13:30, 0.00s elapsed
Initiating NSE at 13:30
Completed NSE at 13:30, 0.00s elapsed
Initiating Ping Scan at 13:30
Scanning miaplicacionweb.azurewebsites.net (52.164.250.133) [4 ports]
Completed Ping Scan at 13:30, 0.78s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:30
Completed Parallel DNS resolution of 1 host. at 13:30, 0.00s elapsed
Initiating SYN Stealth Scan at 13:30
Scanning miaplicacionweb.azurewebsites.net (52.164.250.133) [65535 ports]
Discovered open port 80/tcp on 52.164.250.133
Discovered open port 443/tcp on 52.164.250.133
SYN Stealth Scan Timing: About 12.31% done; ETC: 13:34 (0:03:41 remaining)
SYN Stealth Scan Timing: About 26.28% done; ETC: 13:34 (0:02:51 remaining)
SYN Stealth Scan Timing: About 38.34% done; ETC: 13:34 (0:02:26 remaining)
SYN Stealth Scan Timing: About 55.61% done; ETC: 13:34 (0:01:37 remaining)
Discovered open port 455/tcp on 52.164.250.133
SYN Stealth Scan Timing: About 65.80% done; ETC: 13:34 (0:01:18 remaining)
SYN Stealth Scan Timing: About 77.91% done; ETC: 13:34 (0:00:51 remaining)
Discovered open port 454/tcp on 52.164.250.133
Completed SYN Stealth Scan at 13:34, 240.63s elapsed (65535 total ports)
Initiating Service scan at 13:34
Scanning 4 services on miaplicacionweb.azurewebsites.net (52.164.250.133)
Completed Service scan at 13:35, 46.62s elapsed (4 services on 1 host)
Initiating OS detection (try #1) against miaplicacionweb.azurewebsites.net (52.164.250.133)
Retrying OS detection (try #2) against miaplicacionweb.azurewebsites.net (52.164.250.133)
Initiating Traceroute at 13:35
Completed Traceroute at 13:35, 3.35s elapsed
Initiating Parallel DNS resolution of 17 hosts. at 13:35
Completed Parallel DNS resolution of 17 hosts. at 13:35, 0.13s elapsed
NSE: Script scanning 52.164.250.133.
Initiating NSE at 13:35
Completed NSE at 13:35, 7.67s elapsed
Initiating NSE at 13:35
Completed NSE at 13:35, 0.00s elapsed
Nmap scan report for miaplicacionweb.azurewebsites.net (52.164.250.133)

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

Salida Nmap	Puertos / Servidores	Topología	Detalles del servidor	Escaneos	
PuertoProtocoloEstadoServicioVersión					
	80	tcp	open	http	Microsoft IIS httpd 8.0
	443	tcp	open	http	Microsoft IIS httpd 8.0
	454	tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
	455	tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

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

31

Salida Nmap	Puertos / Servidores	Topología	Detalles del servidor	Escaneos
nmap -p 1-65535 -T4 -A -v miaplicacionweb.azurewebsites.net				
<pre> 80/tcp open http Microsoft IIS httpd 8.0 _http-favicon: Unknown favicon MD5: 7E9102C26AD0878B472086D965570847 _http-methods: Supported Methods: OPTIONS TRACE GET HEAD POST Potentially risky methods: TRACE _http-server-header: Microsoft-IIS/8.0 _http-title: Did not follow redirect to https://miaplicacionweb.azurewebsites.net/ 443/tcp open ssl/http Microsoft IIS httpd 8.0 _http-favicon: Unknown favicon MD5: 7E9102C26AD0878B472086D965570847 _http-methods: Supported Methods: OPTIONS TRACE GET HEAD POST Potentially risky methods: TRACE _http-server-header: Microsoft-IIS/8.0 _http-title: Home Page - FastExchange _ssl-cert: Subject: commonName=*.azurewebsites.net _Subject Alternative Name: DNS:*.azurewebsites.net, DNS:*.scm.azurewebsites.net, DNS:*.azure-mobile.net, DNS:*.scm.azure-mobile.net _Issuer: commonName=Microsoft IT SSL SHA2/organizationName=Microsoft Corporation/stateOrProvinceName=Washington/countryName=US _Public Key type: rsa _Public Key bits: 2048 _Signature Algorithm: sha256WithRSAEncryption _Not valid before: 2016-09-28T21:45:23 _Not valid after: 2018-05-07T17:03:30 _MD5: 147a 24f6 d5e6 e13a a6ac dbc8 90f6 6a27 _SHA-1: e959 fd5c 80f7 6df7 a593 aae0 9686 e604 f74b e8b0 454/tcp open ssl/http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP) _http-server-header: Microsoft-HTTPAPI/2.0 _http-title: Bad Request _ssl-cert: Subject: commonName=waws-prod-db3-065.api.azurewebsites.windows.net _Subject Alternative Name: DNS:waws-prod-db3-065.api.azurewebsites.windows.net _Issuer: commonName=Microsoft IT SSL SHA2/organizationName=Microsoft Corporation/stateOrProvinceName=Washington/countryName=US _Public Key type: rsa _Public Key bits: 2048 _Signature Algorithm: sha256WithRSAEncryption _Not valid before: 2017-01-25T18:19:27 _Not valid after: 2018-05-07T17:03:30 _MD5: 236a 94f4 dc6e 6b13 a673 599e 482a e0a6 _SHA-1: a1bc f524 8c29 0ecd ee6a cd99 6a26 a8b0 1cb3 ea80 455/tcp open ssl/http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP) _http-server-header: Microsoft-HTTPAPI/2.0 </pre>				

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.

Network Distance: 27 hops
TCP Sequence Prediction: Difficulty=262 (Good luck!)
IP ID Sequence Generation: Randomized
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

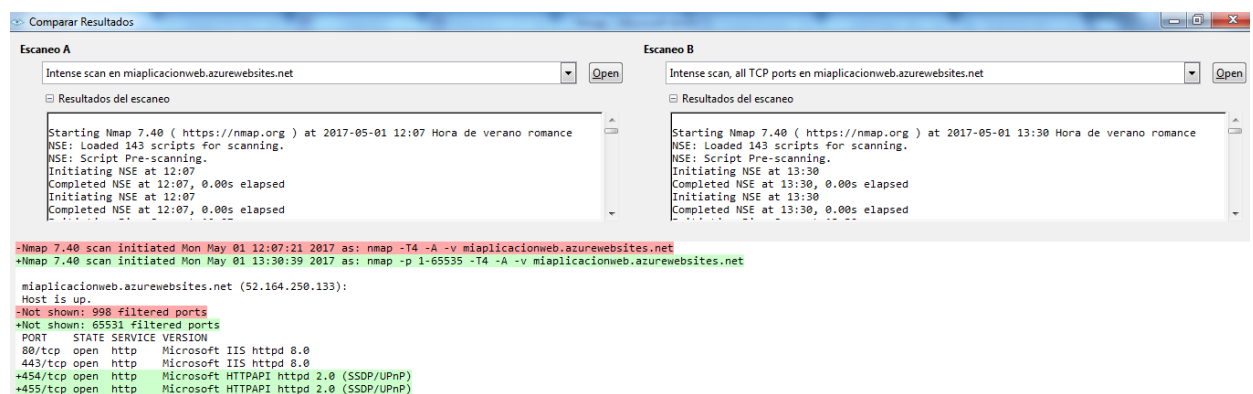
```

TRACEROUTE (using port 443/tcp)
HOP RTT      ADDRESS
1   0.00 ms   Livebox (192.168.1.1)
2   47.00 ms   172.31.255.254
3   32.00 ms   10.34.93.163
4   47.00 ms   10.34.198.5
5   47.00 ms   10.34.34.2
6   32.00 ms   vlan384.tuk-6nf-15a.ntwk.msn.net (207.46.219.66)
7   47.00 ms   ae20-0.bcn30-96cbe-1a.ntwk.msn.net (104.44.225.11)
8   62.00 ms   ae0-0.bcn30-96cbe-1b.ntwk.msn.net (104.44.226.33)
9   62.00 ms   ae25-0.mrs01-96cbe-1b.ntwk.msn.net (104.44.226.37)
10  62.00 ms   ae0-0.mrs01-96cbe-1a.ntwk.msn.net (104.44.227.12)
11  62.00 ms   ae4-0.par02-96cbe-1a.ntwk.msn.net (104.44.227.5)
12  63.00 ms   ae3-0.pra-96cbe-1a.ntwk.msn.net (204.152.141.244)
13  78.00 ms   104.44.5.70
14  93.00 ms   be-1-0.ibr01.lon30.ntwk.msn.net (104.44.5.36)
15  78.00 ms   be-5-0.ibr01.dbb.ntwk.msn.net (104.44.5.52)
16  ...
17  78.00 ms   ae11-0.db3-96c-2a.ntwk.msn.net (204.152.141.75)
18  ... 26
27  78.00 ms   miaplicacionweb.azurewebsites.net (52.164.250.133)

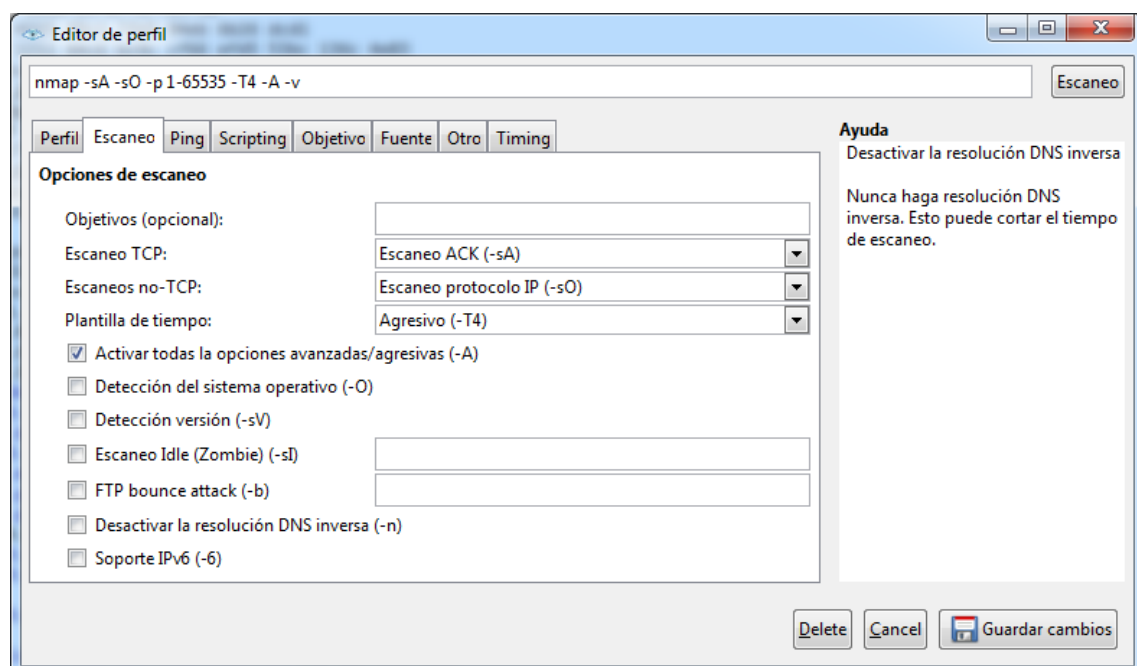
```


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 Predicción 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.
- -sl <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 envíen 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 parámetros en la línea de comandos ejecutando Nmap con un análisis más profundo y por lo que tarda mucho más tiempo en realizar este análisis:

```

C:\Windows\system32\cmd.exe
C:\Users\Jonatan>nmap -sS -sU -T4 -A -v miaplicacionweb.azurewebsites.net

Starting Nmap 7.40 ( https://nmap.org ) at 2017-05-01 16:13 Hora de verano roman
ce
NSE: Loaded 143 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 16:13
Completed NSE at 16:13, 0.00s elapsed
Initiating NSE at 16:13
Completed NSE at 16:13, 0.00s elapsed
Initiating Ping Scan at 16:13
Scanning miaplicacionweb.azurewebsites.net (52.164.250.133) [4 ports]
Completed Ping Scan at 16:13, 0.70s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:13
Completed Parallel DNS resolution of 1 host. at 16:13, 0.00s elapsed
Initiating SYN Stealth Scan at 16:13
Scanning miaplicacionweb.azurewebsites.net (52.164.250.133) [1000 ports]
Discovered open port 443/tcp on 52.164.250.133
Discovered open port 80/tcp on 52.164.250.133
Completed SYN Stealth Scan at 16:13, 7.58s elapsed (1000 total ports)
Initiating UDP Scan at 16:13
Scanning miaplicacionweb.azurewebsites.net (52.164.250.133) [1000 ports]
Completed UDP Scan at 16:13, 8.21s elapsed (1000 total ports)
Initiating Service scan at 16:13
Scanning 1002 services on miaplicacionweb.azurewebsites.net (52.164.250.133)
Service scan Timing: About 0.40% done
Service scan Timing: About 3.29% done; ETC: 17:52 (1:35:26 remaining)
Service scan Timing: About 6.29% done; ETC: 17:31 (1:12:47 remaining)
Service scan Timing: About 9.28% done; ETC: 17:23 (1:03:32 remaining)

C:\Windows\system32\cmd.exe
>
Completed NSE at 16:22, 50.29s elapsed
Initiating NSE at 16:22
Completed NSE at 16:22, 8.43s elapsed
Nmap scan report for miaplicacionweb.azurewebsites.net (52.164.250.133)
Host is up (0.091s latency).
Not shown: 1000 open/filtered ports, 998 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http      Microsoft IIS httpd 8.0
|_http-favicon: Unknown favicon MD5: 7E9102C26AD0878B472086D965570847
|_http-methods:
|_Supported Methods: OPTIONS TRACE GET HEAD POST
|_Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/8.0
|_http-title: Did not follow redirect to https://miaplicacionweb.azurewebsites.n
et/
443/tcp    open  ssl/http  Microsoft IIS httpd 8.0
|_http-methods:
|_Supported Methods: OPTIONS TRACE GET HEAD POST
|_Potentially risky methods: TRACE
|_http-title: Home Page - FastExchange
|_ssl-cert: Subject: commonName=*.azurewebsites.net
|_Subject Alternative Name: DNS:*.azurewebsites.net, DNS:*.scm.azurewebsites.net
|_DNS:*.azure-mobile.net, DNS:*.scm.azure-mobile.net
|_Issuer: commonName=Microsoft IT SSL SHA2/organizationName=Microsoft Corporatio
n/stateOrProvinceName=Washington/countryName=US
|_Public Key type: rsa
|_Public Key bits: 2048
|_Signature Algorithm: sha256WithRSAEncryption
|_Not valid before: 2016-09-28T21:45:23
|_Not valid after: 2018-05-07T17:03:30
|_MD5: 147a 24f6 d5e6 e13a a6ac dbc8 90f6 6a27
|_SHA-1: e959 fd5c 80f7 6df7 a593 aae0 9686 e604 f74b e8b0
Warning: OSScan results may be unreliable because we could not find at least 1 o
pen and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplet
e
No OS matches for host
Uptime guess: 0.001 days (since Mon May 01 16:21:07 2017)
Network Distance: 26 hops
TCP Sequence Prediction: Difficulty=253 (Good luck!)
IP ID Sequence Generation: Randomized
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE (using port 443/tcp)

```

6. Comparación de las dos implementaciones

6.1 Evaluación de los criterios en la implementación usando Netsparker

CRITERIO	EVALUACIÓN
Criterio 1: Tiempo de ejecución	23,56 min.
Criterio 2: Tipos de escaneo	Uno, en el que puedes elegir en que aspectos de seguridad quieres centrarte
Criterio 3: Grado de detalle	Alto (la versión de prueba es menos detallada) Analiza errores de interfaz, bases de datos, funcionalidades de usuarios y seguridad
Criterio 4: Clasificación de errores	Si (leves, medios, graves)
Criterio 5: Recomendaciones	Si
Criterio 6: Profundidad del análisis	Elevada; error, impacto, recomendaciones, referencias externas
Criterio 7: Horas empleadas	28 min.
Criterio 8: Facilidad de uso	Si
Criterio 9: Preparación para la implementación	Configuración a través de interfaz (verificar, parámetros...)
Criterio 10: Recopilación de información	No (intuitivo, en inglés)
Criterio 11: Precio/año	Versión Prueba: 0\$ Versión Estándar: 1.950\$ Versión Profesional: 5.950\$

6.2 Evaluación de los criterios en la implementación usando Nmap

CRITERIO	EVALUACIÓN
Criterio 1: Tiempo de ejecución	Escaneo más intenso con todos los puertos TCP (+completo) = 5,13 min.
Criterio 2: Tipos de escaneo	Hay muchos; el rápido, el regular, el intenso, el intenso con todos los puertos TCP, el intenso con uso del UDP, escaneo sin hacer ping, escaneo de solo hacer ping y otros rápidos.
Criterio 3: Grado de detalle	Dependerá del tipo de escaneo pero en general está enfocado a los puertos que usa, muestra IPS que va pasando la trama si queremos hacer un ping en su web, huella que dejamos, servicios y protocolos usados y sus certificaciones de respaldo...
Criterio 4: Clasificación de errores	No
Criterio 5: Recomendaciones	No
Criterio 6: Profundidad del análisis	Dependerá del tipo de escaneo elegido
Criterio 7: Horas empleadas	4 horas y 5,13 min
Criterio 8: Facilidad de uso	Si
Criterio 9: Preparación para la implementación	Con los comandos que vienen por defecto; pones dirección web, tipo de escaneo y escanear. Si no hay que introducir la línea de comando también.
Criterio 10: Recopilación de información	Si (en cursos y tutoriales nombrados en anteriores trabajos, y en la web oficial para interpretar los resultados)
Criterio 11: Precio/año	Gratuita

7. Comparación de la implementación de las tecnologías

CRITERIOS	NETSPARKER	NMAP	COMENTARIOS
Criterio 1: Tiempo de ejecución	23,56 minutos	5,13 minutos	Netsparker a diferencia de Nmap clasifica y resalta los errores y advertencias.
Criterio 2: Tipos de escaneo	1	10	Nmap te da 10 variantes (por defecto) para analizar, calibrando la profundidad de la búsqueda.
Criterio 3: Grado de detalle	Alto	Medio	Nmap dependiendo de los comandos que introduzcas, dará menos o más información en sus informes de los análisis.
Criterio 4: Clasificación de errores	Si	No	Netsparker clasifica los errores en 3 secciones siendo una gran ventaja frente a Nmap que el usuario debe interpretarlos.
Criterio 5: Recomendaciones	Si	No	Netsparker a gran diferencia de Nmap, recomienda soluciones para subsanar todos los errores hallados.
Criterio 6: Profundidad del análisis	Elevada	Personalizable	Nmap dependerá del comando introducido para saber la profundidad del análisis. Netsparker al tener solo una opción es bastante completa.
Criterio 7: Horas empleadas	28 minutos	4 horas y 5,13 min	Gran diferencia, dado que Nmap necesita una configuración previa y dispone de varios comandos para ir probando y utilizando, ya que con cada uno se analizaban distintas funciones.
Criterio 8: Facilidad de uso	Si	Si	Las dos herramientas no tienen ninguna dificultad para ejecutar un análisis general.
Criterio 9: Preparación para la implementación	Interfaz	Comandos e Interfaz	Nmap te da la posibilidad de realizar el escaneo por la interfaz de la herramienta o por comandos en la misma o en una consola, terminal o CMD.
Criterio 10: Recopilación de información	No	Si	Netsparker no es necesario recopilar esta información ya que es muy sencillo realizar un análisis, a diferencia con Nmap que sí existen para la correcta interpretación de los resultados.
Criterio 11: Precio/año	1.950\$ - 5.950\$	Gratuita	Aunque Netsparker sea de pago, esta herramienta ofrece un periodo de prueba gratuito para conocer la eficacia de la misma, a diferencia de Nmap que es gratuita de por vida.

8. Conclusiones

A partir de la información obtenida anteriormente podemos sacar diversas conclusiones.

La tecnología Netsparker gracias a su facilidad de uso, ya que es una herramienta intuitiva nos permite realizar una rápida implementación, a diferencia de Nmap que nos ha llevado más horas y hemos tenido que consultar tutoriales y guías ya nombradas en anteriores trabajos, sin embargo tarda más que Nmap en realizar el escaneo para mostrarnos el análisis.

Netsparker realiza un gran análisis de la web, ya que analiza errores de interfaz, bases de datos, funcionalidades de usuarios y seguridad muy detallado. Además realiza una clasificación de errores y nos aporta recomendaciones para su posible solución.

Nmap nos permite elegir qué tipo de escaneo queremos realizar y se centra en temas relacionados con los puertos como por ejemplo muestra IPS que va pasando la trama si queremos hacer un ping en su web, huella que dejamos, servicios y protocolos usados y sus certificaciones de respaldo... Pero a diferencia de Netsparker no nos muestra una clasificación de errores ni recomendaciones, sino que tú tienes que interpretarlo con la información obtenida.

Por lo que evaluando los criterios y realizando una comparación la herramienta Netsparker sería mejor, más completa, pero su gran pega es que es una herramienta de pago (ofreciendo una prueba gratuita) a diferencia de Nmap.

Para realizar un análisis de una plataforma web lo más completo posible nosotros recomendaríamos emplear ambas herramientas ya que son complementarias.