Contenido

[1. Autores del trabajo, planificación y entrega 3](#_Toc478660023)

[1.1 Autores 3](#_Toc478660024)

[1.2 Planificación 3](#_Toc478660025)

[1.3 Entrega 3](#_Toc478660026)

[2. Descripción de las tecnologías 4](#_Toc478660027)

[2.1 Descripción de la tecnología Netsparker 4](#_Toc478660028)

[2.2 Descripción de la tecnología Nmap 5](#_Toc478660029)

[3. Criterios de comparación 7](#_Toc478660030)

[3.1 Categoría A: Características generales 7](#_Toc478660031)

[3.1.1 Criterio A.1: Madurez y versiones 7](#_Toc478660032)

[3.1.2 Criterio A.2: Coste 7](#_Toc478660033)

[3.1.3 Criterio A.3: Desarrollador 7](#_Toc478660034)

[3.1.4 Criterio A.4: Flexibilidad de idiomas 7](#_Toc478660035)

[3.1.5 Criterio A.5: Lenguajes de programación 7](#_Toc478660036)

[3.1.6 Criterio A.6: Instalación 7](#_Toc478660037)

[3.1.7 Criterio A.7: Popularidad 8](#_Toc478660038)

[3.1.8 Criterio A.8: Competitividad 8](#_Toc478660039)

[3.2 Categoría B: Soporte 8](#_Toc478660040)

[3.2.1 Criterio B.1: Respaldo 8](#_Toc478660041)

[3.2.2 Criterio B.2: Garantía 8](#_Toc478660042)

[3.2.3 Criterio B.3: Soporte 8](#_Toc478660043)

[3.2.4 Criterio B.4: Cantidad de Información 8](#_Toc478660044)

[3.3 Categoría C: Funcionalidad 9](#_Toc478660045)

[3.3.1 Criterio C.1: Configuración 9](#_Toc478660046)

[3.3.2 Criterio C.2: Interfaz intuitiva 9](#_Toc478660047)

[3.3.3 Criterio C.3: Dificultad de uso 9](#_Toc478660048)

[3.3.4 Criterio C.4: Exportación de resultados 9](#_Toc478660049)

[3.3.5 Criterio C.5: Integración 9](#_Toc478660050)

[3.3.6 Criterio C.6: Plataformas disponibles 9](#_Toc478660051)

[3.3.7 Criterio C.7: Complejidad 10](#_Toc478660052)

[3.3.8 Criterio C.8: Tiempo ejecución 10](#_Toc478660053)

[3.3.9 Criterio C.9: Calidad Informe 10](#_Toc478660054)

[3.4 Categoría D: Seguridad 10](#_Toc478660055)

[3.4.1. Criterio D.1: XSS (Cross-site Scripting) 10](#_Toc478660056)

[3.4.2 Criterio D.2: Rechazo de la inyección/respuesta de cabecera CRLF/HTTP 10](#_Toc478660057)

[3.4.3 Criterio D.3: Inclusiones de archivos remotos 11](#_Toc478660058)

[3.4.4 Criterio D.4: Mal uso de los puertos SSL y TSL para los pagos 11](#_Toc478660059)

[3.4.5 Criterio D.5: Mal uso de los puertos HTTPS 11](#_Toc478660060)

[3.4.6 Criterio D.6: Errores de desarrollo 11](#_Toc478660061)

[3.4.7 Criterio D.7: Errores de diseño 11](#_Toc478660062)

[4. Evaluación de los criterios por tecnología 12](#_Toc478660063)

[4.1 Evaluación de los criterios para la tecnología Netsparker 12](#_Toc478660064)

[4.2 Evaluación de los criterios para la tecnología Nmap 14](#_Toc478660065)

[5. Comparación de las tecnologías 16](#_Toc478660066)

[6. Recomendaciones 20](#_Toc478660067)

[6.1 Situación 1 20](#_Toc478660068)

[6.1.1 Descripción de la situación 20](#_Toc478660069)

[6.1.2 Recomendación de tecnología a utilizar 20](#_Toc478660070)

[6.2 Situación 2 21](#_Toc478660071)

[6.2.1 Descripción de la situación 21](#_Toc478660072)

[6.2.2 Recomendación de tecnología a utilizar 21](#_Toc478660073)

[6.3 Situación 3 22](#_Toc478660074)

[6.3.1 Descripción de la situación 22](#_Toc478660075)

[6.3.2 Recomendación de tecnología a utilizar 23](#_Toc478660076)

[7. Conclusión 24](#_Toc478660077)

# 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

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 51 horas al llevarnos mucha investigación por falta de información para comparar las dos herramientas de dicho proyecto. Estas horas se pueden apreciar claramente en el siguiente diagrama:

[Planificación TG2 (Grupo T4)](https://app.ganttpro.com/shared/token/4cc4c133d73d03205296864dc1b89932ffb075db9224e5171475814e66427d65%20)

Se han repartido las tareas de una forma equitativa y equivalente, 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.

Para finalizar, se ha añadido un punto adicional, el cual es 7, que se basa en la conclusión de dicho proyecto, por lo que creemos conveniente añadirlo.

## 1.3 Entrega

El enlace a nuestro repositorio es el siguiente:

[**https://github.com/JonatanVinuelasCaballero/TG2**](https://github.com/JonatanVinuelasCaballero/TG2)

# 2. Descripción de las tecnologías

Hemos elegido las herramientas Netsparker y Nmap para trabajar, ya que nos parecen las más interesantes.

## 2.1 Descripción de la tecnología Netsparker



[Mavituna Security](http://www.mavitunasecurity.com/) es una pequeña empresa que desarrolla un producto de análisis de vulnerabilidades web llamado [NetSparker](http://www.mavitunasecurity.com/netsparker/), que es el único escáner de seguridad de aplicaciones web falso-positivo-libre.

Simplemente apuntas a tu sitio web y se detectará automáticamente los defectos que podrían dejarte peligrosamente expuesto.

Es compatible con AJAX / JavaScript, y puede mostrar si la inyección de SQL es explotable y el impacto de la misma. También escanea HTML5, SPA, aplicaciones Web 2.0 y cualquier otro tipo de aplicación web.

Utiliza la avanzada tecnología de escaneo de vulnerabilidades Prueba-base y se ha incorporado en las pruebas de penetración y herramientas de reporte.

Muestra las vulnerabilidades y problemas de control de calidad muy bien presentados en los informes.

Es muy fácil de utilizar, cualquier persona puede hacerlo.

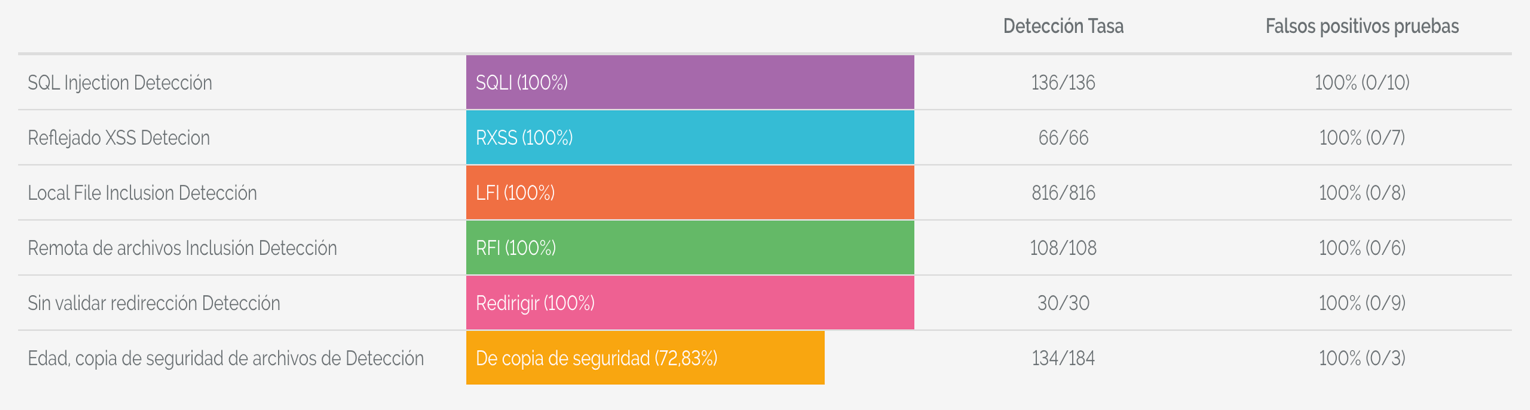
Esta herramienta es de pago, pero nos ofrece una prueba gratuita. Puedes elegir entre Netsparker de escritorio o en la nube, y según la elección tendremos una tabla de precios:

NUBE: Netsparker Cloud es una solución escalable multi-usuario en línea de aplicaciones web de análisis de seguridad con herramientas de flujo de trabajo incorporadas.

ESCRITORIO: Netsparker Desktop está disponible como una aplicación de Windows y es un escáner de seguridad fácil de usar. Aplicación web que utiliza la avanzada tecnología de escaneo de vulnerabilidades basada en pruebas y se ha incorporado en las pruebas de penetración y herramientas de reporte.

****

EJEMPLO:



Estadísticas 2014/15 de aplicaciones web escáneres de seguridad Benchmark SecToolMarket.

## 2.2 Descripción de la tecnología Nmap



Es una herramienta de código abierto que sirve para efectuar un rastreo de puertos. Fue escrito originalmente por Gordon Lyon (más conocido por su alias Fyodor Vaskovich) y cuyo desarrollo se encuentra hoy a cargo de una comunidad.

Fue creado originalmente para Linux aunque actualmente es multiplataforma. Se usa para evaluar la seguridad de sistemas informáticos, así como para descubrir servicios o servidores en una [red](https://es.wikipedia.org/wiki/Red_de_computadores) [informática](https://es.wikipedia.org/wiki/Inform%C3%A1tica), para ello Nmap envía unos paquetes definidos a otros equipos y analiza sus respuestas.

Este software posee varias funciones para sondear [redes de computadores](https://es.wikipedia.org/wiki/Redes_de_computadores), incluyendo detección de equipos, servicios y [sistemas operativos](https://es.wikipedia.org/wiki/Sistemas_operativos). Estas funciones son extensibles mediante el uso de scripts para proveer servicios de detección avanzados, detección de vulnerabilidades y otras aplicaciones. Además, durante un escaneo, es capaz de adaptarse a las condiciones de la [red](https://es.wikipedia.org/wiki/Red_de_computadores) incluyendo [latencia](https://es.wikipedia.org/wiki/Latencia) y [congestión](https://es.wikipedia.org/wiki/Congesti%C3%B3n_de_red) de la misma.

Nmap es reconocido como el scanner de puertos más poderoso. Fue diseñado para escanear rápidamente grandes redes, aunque funciona bien contra el anfitrión individuales. Se utiliza comúnmente para las auditorías de seguridad, aunque a muchos sistemas y administradores de red les resulta útil para tareas de rutina, tales como inventario de la red, los horarios de actualización de servicio de gestión, monitoreo y anfitrión o un tiempo de servicio, y para recolectar información para futuros ataques (hackers).

Nmap puede funcionar en sistemas operativos basados en Unix (GNU/Linux, Solaris, BSD y Mac OS X) y también en otros sistemas operativos como Microsoft Windows y AmigaOS.

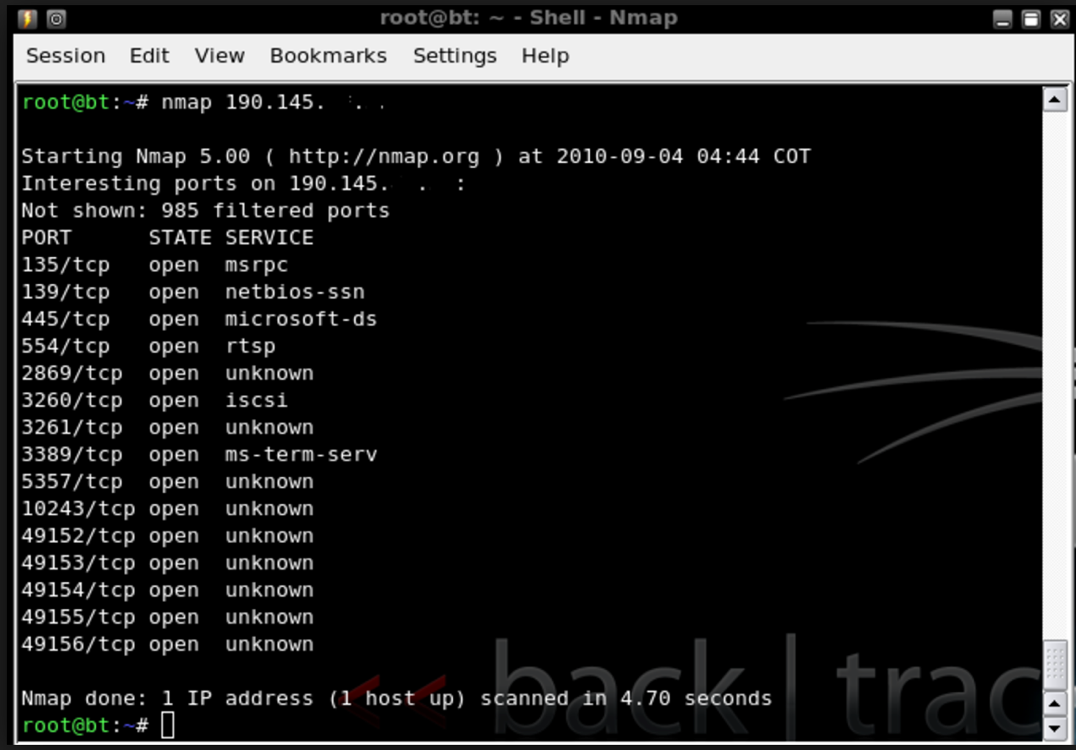
Respecto a su funcionamiento, es capaz se utilizar diferentes técnicas de evasión de detección como escaneo sealth. Soporta escaneos sobre ciertos puertos específicos, entre rangos IP específicos, uso se paquetes Null, FIN, Xmas y ACK, además SYN que es el paquete por defecto. Esto significa que se mandan cierto tipo de paquetes a cada puerto y estos responderán con alguna señal que permitirá a scanner encontrar versiones y servicios.

Sus principales características son las siguientes:

* Descubrimiento de [servidores](https://es.wikipedia.org/wiki/Servidores): Identifica computadoras en una red, por ejemplo listando aquellas que responden [ping](https://es.wikipedia.org/wiki/Ping).
* Identifica [puertos](https://es.wikipedia.org/wiki/Puerto_(computaci%C3%B3n)) abiertos en una [computadora](https://es.wikipedia.org/wiki/Computadora) objetivo.
* Determina qué servicios está ejecutando la misma.
* Determinar qué [sistema operativo](https://es.wikipedia.org/wiki/Sistema_operativo) y versión utiliza dicha computadora, (esta técnica es también conocida como [fingerprinting](https://es.wikipedia.org/wiki/Fingerprinting)).
* Obtiene algunas características del hardware de red de la máquina objeto de la prueba.

Nmap es una gran herramienta de carácter gratuito.

EJEMPLO de uso:



# 3. Criterios de comparación

## 3.1 Categoría A: Características generales

### 3.1.1 Criterio A.1: Madurez y versiones

-Nombre del criterio: Madurez y versiones

-Descripción: Disponibilidad de versiones que mejoran la aplicación.

-Tipo de valor: Texto libre.

### 3.1.2 Criterio A.2: Coste

-Nombre del criterio: Coste de la herramienta

-Descripción: Si la herramienta es gratuita o de pago, y si es de pago saber cuánto cuesta.

-Tipo de valor: Numérico

### 3.1.3 Criterio A.3: Desarrollador

-Nombre del criterio: Desarrollador de la herramienta

-Descripción: Nombre de la persona, institución o empresa que ha creado la herramienta.

-Tipo de valor: Texto libre.

### 3.1.4 Criterio A.4: Flexibilidad de idiomas

-Nombre del criterio: Flexibilidad de idiomas

-Descripción: Idiomas en los que está disponible la herramienta.

-Tipo de valor: Texto libre.

### 3.1.5 Criterio A.5: Lenguajes de programación

-Nombre del criterio: Lenguajes de programación

-Descripción: Lenguajes que detecta y que integra la herramienta.

-Tipo de valor: Texto libre.

### 3.1.6 Criterio A.6: Instalación

-Nombre del criterio: Instalación

-Descripción: Facilidad de instalación de la herramienta en los dispositivos.

-Tipo de valor: Texto libre.

### 3.1.7 Criterio A.7: Popularidad

-Nombre del criterio: Popularidad

-Descripción: Grado de popularidad en el uso de la herramienta.

-Tipo de valor: Texto libre.

### 3.1.8 Criterio A.8: Competitividad

-Nombre del criterio: Competitividad

-Descripción: Nos indica la competitividad existente en dicho sector.

-Tipo de valor: Texto Libre.

## 3.2 Categoría B: Soporte

### 3.2.1 Criterio B.1: Respaldo

-Nombre del criterio: Respaldo o sitios de ayuda

-Descripción: Conjunto de ayudas disponibles para el correcto y satisfactorio uso de la herramienta por parte del usuario.

-Tipo de valor: Texto libre.

### 3.2.2 Criterio B.2: Garantía

-Nombre del criterio: Garantía de la herramienta

-Descripción: Indica la garantía que nos proporciona la herramienta para su uso.

-Tipo de valor: Texto Libre.

### 3.2.3 Criterio B.3: Soporte

-Nombre del criterio: Soporte de incidencias

-Descripción: Nos indica el apoyo y soporte de los problemas surgidos en las herramientas.

-Tipo de valor: Booleano (Si/No).

### 3.2.4 Criterio B.4: Cantidad de Información

-Nombre del criterio: Cantidad de Información

-Descripción: Nos indica la cantidad existente de información cuantificable.

-Tipo de valor: Texto Libre.

## 3.3 Categoría C: Funcionalidad

### 3.3.1 Criterio C.1: Configuración

-Nombre del criterio: Configuración

-Descripción: Facilidad y grado de configuración de la herramienta en los dispositivos.

-Tipo de valor: Texto libre.

### 3.3.2 Criterio C.2: Interfaz intuitiva

-Nombre del criterio: Interfaz intuitiva

-Descripción: Si la interfaz que contiene el gestor de contenido es intuitiva y fácil de utilizar por el usuario.

-Tipo de valor: Booleano (Si/No).

### 3.3.3 Criterio C.3: Dificultad de uso

-Nombre del criterio: Dificultad de uso

-Descripción: Si el usuario es capaz de utilizar la herramienta con facilidad.

-Tipo de valor: Booleano (Si/No).

### 3.3.4 Criterio C.4: Exportación de resultados

-Nombre del criterio: Exportación de resultados

-Descripción: Posibilidad de exportar los resultados a distintos formatos.

-Tipo de valor: Texto libre.

### 3.3.5 Criterio C.5: Integración

-Nombre del criterio: Capacidad de integración con otras herramientas

-Descripción: Nos ofrece la capacidad que tiene las tecnologías para integrarse con distintas herramientas para potenciar sus funcionalidades.

-Tipo de valor: Texto Libre.

### 3.3.6 Criterio C.6: Plataformas disponibles

-Nombre del criterio: Plataformas disponibles

-Descripción: Conjunto de sistemas operativos para los que se puede utilizar la herramienta.

-Tipo de valor: Texto libre.

### 3.3.7 Criterio C.7: Complejidad

-Nombre del criterio: Complejidad

-Descripción: Nos indica el grado de complejidad y dificultad del uso de las herramientas.

-Tipo de valor: Texto Libre.

### 3.3.8 Criterio C.8: Tiempo ejecución

-Nombre del criterio: Tiempo ejecución

-Descripción: Nos indica el tiempo cuantificable que tarda en ejecutarse.

-Tipo de valor: Texto Libre.

### 3.3.9 Criterio C.9: Calidad Informe

-Nombre del criterio: Calidad del Informe

-Descripción: Nos indica el nivel de calidad de la información.

-Tipo de valor: Texto Libre.

## 3.4 Categoría D: Seguridad

### 3.4.1. Criterio D.1: XSS (Cross-site Scripting)

-Nombre del criterio: XSS (Cross-site Scripting)

-Descripción: capacidad que tiene la herramienta para detectar si es posible que un atacante inyecte un archivo remoto en el sitio para ejecutar JavaScript en la página actual y de detectar los problemas de secuencias de comandos entre sitios en URL.

-Tipo de valor: Booleano (SI/NO).

### 3.4.2 Criterio D.2: Rechazo de la inyección/respuesta de cabecera CRLF/HTTP

-Nombre del criterio: Rechazo de la inyección / respuesta de cabecera CRLF / HTTP

-Descripción: Capacidad que tiene la herramienta para detectar problemas de inyección de CRLF que pueden causar serios problemas en aplicaciones web, como llevar a Cross-site Scripting y ataques de secuestro de sesión.

-Tipo de valor: Booleano (SI/NO).

### 3.4.3 Criterio D.3: Inclusiones de archivos remotos

-Nombre del criterio: Inclusiones de archivos remotos

-Descripción: Capacidad que tiene la herramienta para detectar si la aplicación es vulnerable a Inclusiones de archivos remotos que permiten a un atacante inyectar un archivo remoto y ejecutar código en el servidor.

-Tipo de valor: Booleano (SI/NO).

### 3.4.4 Criterio D.4: Mal uso de los puertos SSL y TSL para los pagos

-Nombre del criterio: Mal uso de los puertos SL y SSL para los pagos

-Descripción: Capacidad que tiene la herramienta para detectar un mal uso de los puertos SSL y TSL para los pagos.

-Tipo de valor: Booleano (SI/NO).

### 3.4.5 Criterio D.5: Mal uso de los puertos HTTPS

-Nombre del criterio: Mal uso de los puertos HTTPS

-Descripción: Capacidad que tiene la herramienta para detectar un mal uso de los puertos HTTPS para la seguridad de la navegación.

-Tipo de valor: Booleano (SI/NO).

### 3.4.6 Criterio D.6: Errores de desarrollo

-Nombre del criterio: Errores de desarrollo

-Descripción: Capacidad que tiene la herramienta para detectar errores comunes en el desarrollo de una aplicación web, los cuales pueden ser el foco de posibles ataques.

-Tipo de valor: Booleano (SI/NO).

### 3.4.7 Criterio D.7: Errores de diseño

-Nombre del criterio: Errores de diseño

-Descripción: Capacidad que tiene la herramienta para detectar errores comunes en el diseño de una aplicación web, los cuales pueden ser el foco de posibles ataques.

-Tipo de valor: Booleano (SI/NO).

# 4. Evaluación de los criterios por tecnología

## 4.1 Evaluación de los criterios para la tecnología Netsparker

|  |  |
| --- | --- |
| **CRITERIO** | **EVALUACIÓN** |
| Criterio A.1: Madurez y versiones | Dispone de una gran cantidad de versiones, donde algunas de ellas son 3.1, 3.5.5, 4, 4.1. Aunque también hay distintas actualizaciones en la versión de escritorio y en la versión de la nube. |
| Criterio A.2: Coste | Estandar: 1.195$ / Proffesional: 5.950$ |
| Criterio A.3: Desarrollador | Navituna Security. Ferruh se asoció con los cofundadores Peter Edgeler y Mark Lane para crear Netsparker Limited |
| Criterio A.4: Flexibilidad de idiomas | Inglés |
| Criterio A.5: Lenguajes de programación | PERL, SQL, HTML5, XSS… |
| Criterio A.6: Instalación | Sencillo |
| Criterio A.7: Popularidad | Es una herramienta muy utilizada y nombrada en cursos de seguridad, por lo que es popular aunque no haya muchos cursos sobre esta. |
| Criterio A.8: Competitividad | Hay una gran cantidad de herramientas para analizar la seguridad web pero no solo esta herramienta, sino que hay más y de caracter gratuito |
| Criterio B.1: Respaldo | Hay una serie de cursos gratuitos y de pago relacionados con esta herramienta, aunque no son muy abundantes. |
| Criterio B.2: Garantía | Proporciona actualizaciones regulares de firmas, actualizaciones de versiones |
| Criterio B.3: Soporte | Soporte de clase mundial durante el período de suscripción |
| Criterio B.4: Cantidad de información | Información acerca de cursos no hay mucha pero en la web oficial se pueden enviar dudas. |
| Criterio C.1: Configuración | Fácil y limitada aunque muy extensa. |
| Criterio C.2: Interfaz intuitiva | Si |
| Criterio C.3: Dificultad de uso | No |
| Criterio C.4: Exportación de resultados | Se pueden exportar en HTML, PDF, CSV y XML aunque también se pueden exportar plataformas como gitu hub. |
| Criterio C.5: Integración | Tiene una gran capacidad de integración con otras herramientas como Metasploit, Threadfix Vulenability Manager o Lunarline. |
| Criterio C.6: Plataformas disponibles | Windows Vista o superiores. |
| Criterio C.7: Complejidad | Fácil uso. Es muy simple |
| Criterio C.8 Tiempo de ejecución | Dependerá del objeto y del método utilizado. |
| Criterio C.9: Calidad del informe | Buena calidad de la información, que puede mostrarse en informes profesionales que usan plantillas de informes detallados, para hacer comparaciones, de cumplimiento PCI e informes OWASP 10, aunque no incluye recomendaciones. |
| Criterio D.1: XSS (Cross-site Scripting) | Si |
| Criterio D.2: Rechazo de la inyección / respuesta de cabecera CRLF / HTTP | Si |
| Criterio D.3: Inclusión de archivos remotos | Si |
| Criterio D.4: Mal uso de los puertos SSL y TSL pala los pagos | No |
| Criterio D.5: Mal uso de los puertos HTTPS | No |
| Criterio D.6: Errores de desarrollo | Si |
| Criterio D.7: Errores de diseño | Si |

-Criterio A.1: Madurez y versiones:

Hay una gran cantidad de versiones ya que en su web pone que hacen alrededor de 5 versiones al año. Algunas de estas versiones son las siguientes: 3.0, 3.1, 3.1.4, 3.1.7, 3.5, 3.5.5, 4, 4.1… aunque hay muchas más versiones. La versión de la nube también tiene gran variedad de versiones.

-Criterio C.5: Integración:

* Metasploit, Metasploit Express y Metasploit Pro
* Threadfix Vulnerability Manager (vea este seminario en línea para más información)
* Vulnerabilidad de Seguridad de Kenna y Inteligencia de Riesgo (anteriormente Panel de Control de Vulnerabilidad de Riesgo I / O)
* LunarLine Vulnerability Scan Converter y Dradis Framework
* Fiddler, Paros, Burp y otros proxies y herramientas populares.

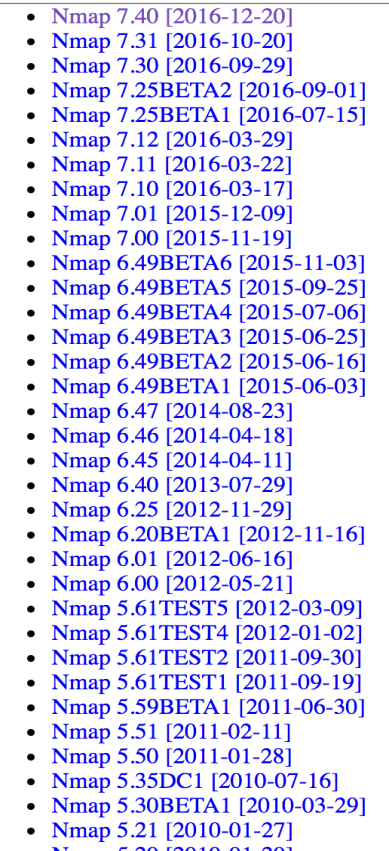
-Criterio B.3: Soporte:

El soporte de clase mundial es una parte vital de todo el paquete. La seguridad de aplicaciones web no es exactamente el trabajo más fácil y la tecnología de uso de herramientas modernas es muy complejo, por lo que se necesita a alguien que pueda ayudarte cuando surgen problemas, o incluso cuando sólo tiene una pregunta sobre el trabajo a mano. Este soporte es ofrecido por Netsparker.

## 4.2 Evaluación de los criterios para la tecnología Nmap

|  |  |
| --- | --- |
| CRITERIOS | EVALUACIONES |
| Criterio A.1: Madurez y versiones | Dispone de muchas versiones y formatos ya que está disponible para varios sistemas operativos. Algunas son Nmap7.40, Nmap 7.31, Nmap 7.30 \* |
| Criterio A.2: Coste | 0 € |
| Criterio A.3: Desarrollador | Gordon Lyon (más conocido por su alias Fyodor Vaskovich) |
| Criterio A.4: Flexibilidad de idiomas | Inglés |
| Criterio A.5: Lenguajes de programación | C, C++, Phyton, Java y Perl |
| Criterio A.6: Instalación | Fácil, Nmap ofrece una guía de ayuda para la instalación |
| Criterio A.7: Popularidad | Elevada al ser una herramienta gratuita, con tantas versiones y de las más competitivas |
| Criterio A.8: Competitividad | Aparece entre las 10 mejores herramientas de seguridad en distintos artículos. \* |
| Criterio B.1: Respaldo | Hay disponible un montón de libros, foros, artículos y video tutoriales donde se ofrece ayuda. La propia página de Nmap muestra una guía |
| Criterio B.2: Garantía | Alta |
| Criterio B.3: Soporte | Si |
| Criterio B.4: Cantidad de información | Proporciona una gran variedad de información. \* |
| Criterio C.1: Configuración | Fácil, limitada y extensa |
| Criterio C.2: Interfaz intuitiva | Si |
| Criterio C.3: Dificultad de uso | Si |
| Criterio C.4: Exportación de resultados | HTML,XML, NMAP, grepeable y script kiddies |
| Criterio C.5: Integración | Alta, con herramientas como Lunarline, Phyton… Tiene 3 herramientas integradas: NCAT, NDIFF y NPING |
| Criterio C.6: Plataformas disponibles | Linux, Windows Microsoft, Mac os x, FreeDSD, OpenBSD, NetBSD,  Sun Solaris, Amiga, HP-UX y AIX |
| Criterio C.7: Complejidad | Media |
| Criterio C.8: Tiempo ejecución | Dependerá del objeto a escanear y del método de escaneo: ping, paquetes timestamp, paquetes netmask request, sólo el paquete ACK dirigiéndolo a un puerto determinado, paquetes SYN al puerto 20, paquetes UDP al puerto 20 |
| Criterio C.9: Calidad informe | Alta |
| Criterio D.1: XSS (Cross-site Scripting) | No |
| Criterio D.2: Rechazo de la inyección / respuesta de cabecera CRLF / HTTP | No |
| Criterio D.3: Inclusiones de archivos remotos | No |
| Criterio D.4: Mal uso de los puertos SSL y TSL para los pagos | Si |
| Criterio D.5: Mal uso de los puertos HTTPS | Si |
| Criterio D.6: Errores de desarrollo | Si |
| Criterio D.7: Errores de diseño | Si |

-Criterio A.1: Madurez y versiones: Más versiones:



-Criterio A.8: Competitividad: Esta fuente nos muestra las 8 mejores herramientas de seguridad y hacking, entre las que aparece Nmap.

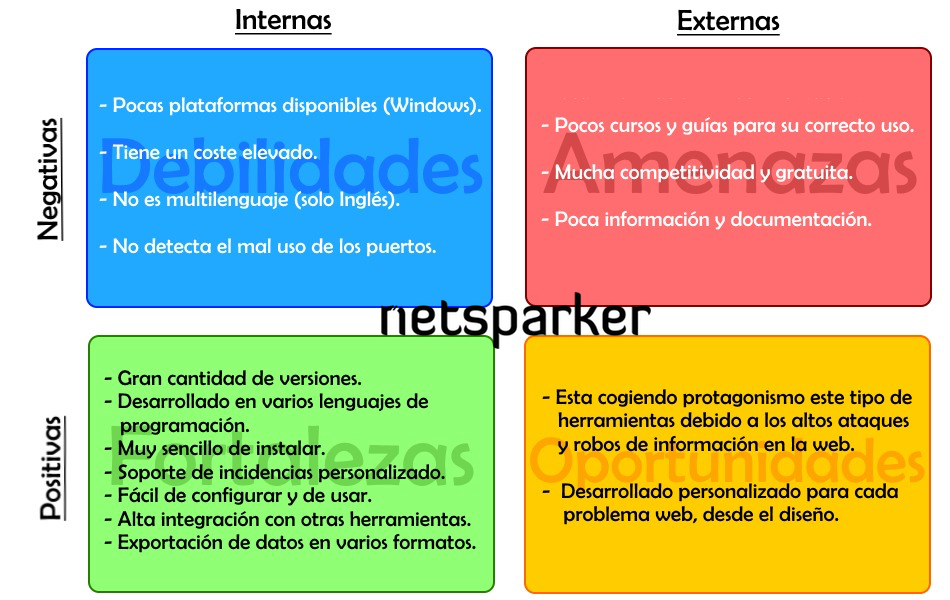
[**http://blog.capacityacademy.com/2012/07/11/las-8-mejores-herramientas-de-seguridad-y-hacking/**](http://blog.capacityacademy.com/2012/07/11/las-8-mejores-herramientas-de-seguridad-y-hacking/)

-Criterio B.4: Cantidad de información:

* Descubrimiento de [servidores](https://es.wikipedia.org/wiki/Servidores): Identifica computadoras en una red, por ejemplo listando aquellas que responden [ping](https://es.wikipedia.org/wiki/Ping).
* Identifica [puertos](https://es.wikipedia.org/wiki/Puerto_(computaci%C3%B3n)) abiertos en una [computadora](https://es.wikipedia.org/wiki/Computadora) objetivo.
* Determina qué servicios está ejecutando la misma.
* Determinar qué [sistema operativo](https://es.wikipedia.org/wiki/Sistema_operativo) y versión utiliza dicha computadora, (esta técnica es también conocida como [*fingerprinting*](https://es.wikipedia.org/wiki/Fingerprinting)).
* Obtiene algunas características del hardware de red de la máquina objeto de la prueba.

# 5. Comparación de las tecnologías

**Dafo Netsparker:**



**Dafo Nmap:**



|  |  |  |  |
| --- | --- | --- | --- |
| CRITERIOS | NETSPARKER | NMAP | COMENTARIOS |
| A.1: Madurez y Versiones | Gran cantidad de versiones | Gran cantidad de versiones | En ambos casos existe una gran variedad de versiones y se van actualizando regularmente. |
| A.2: Coste | Entre 1.195$ y 5.950$ | Gratis | En el aspecto económico Netsparker es de pago y Nmap es gratuito por lo que es un aspecto a tratar y puede ser un punto de inflexión a la hora de decantarse por uno. |
| A.3: Desarrollador | Navituna Security | Gordon Lyon | En el caso de Netsparker la herramienta fue desarrollada por una empresa, mientras que en el caso de Nmap fue por una sola persona. |
| A.4: Flexibilidad de idiomas | Inglés | Inglés | Ambos están desarrollados en inglés como idioma por defecto. |
| A.5: Lenguajes de Programación | 4 (Perl, SQL, HTML5 y XSS) | 5 (C, C++, Phyton, Java y Perl) | *Netsparker se ha desarrollado en lenguajes basados en texto plano web, mientras que Nmap se ha desarrollado en lenguajes basados en aplicaciones web. Cada uno cubriendo su parte.* |
| A.6: Instalación | Sencillo | Sencillo | *En ninguno de los dos casos existe una licencia para programar, solo para publicar la app en la tienda oficial de cada uno.* |
| A.7: Popularidad | Popular, pero pocos cursos | Muy elevada | Nmap tiene mayor expectación al ser una herramienta gratuita, ya que al ser gratis, el público se anima más a usarla y a realizar tutoriales de uso, por encima del Netsparker al ser de pago. |
| A.8: Competitividad | Mucha y sobretodo gratuita | Mucha | Existe mucha competitividad entre herramientas similares, pero aquí destaca Nmap al encontrarse más consagrada en el mercado estando siempre en el top de las 10 mejores herramientas de seguridad. El pago de la herramienta en estos casos es una parte a tener en cuenta. |
| B.1: Respaldo | Pocos cursos y referencias | Muchos recursos y referencias disponibles | Es muy importante tener varias referencias y recursos para conocer cualquier herramienta, por lo que es un aspecto muy importante tener referencias para documentarse bien sobre el uso de las mismas por lo que Netsparker no tiene nada que hacer con Nmap en este sentido. |
| B.2: Garantía | Alta | Alta | En este caso en las dos herramientas se preocupan de actualizar regularmente las versiones para garantizar el buen uso y funcionamiento de las mismas. |
| B.3: Soporte | Sí | Sí | Las dos herramientas disponen de soporte de incidencias, solo que en Netsparker está más especializado y personalizado al ser de pago por suscripción. |
| B.4: Cantidad de Información | Poca | Gran variedad | Nmap también arrasa en este sentido al ser una herramienta de libre acceso y al tener muchos recursos que la propia web, foros, libros e incluso los más curiosos generan posibilita a que la cantidad de información aumente considerablemente por encima de Netsparker. |
| C.1: Configuración | Fácil, limitada y muy extensa | Fácil, limitada y extensa | En este sentido son realmente similares, ya que la configuración es sencilla en las dos herramientas, pero limitada en ambos casos*.* |
| C.2: Interfaz Intuitiva | Sí | Sí | Las dos herramientas tienen un diseño de la interfaz bastante intuitiva. |
| C.3: Dificultad de uso | No | Sí | En este caso Netsparker se lleva la palma, al ser de pago tienen más cuidado y atención en la usabilidad de la herramienta, por lo que tienen varios expertos tratando de mantener esta ventaja por encima de Nmap. |
| C.4: Exportación de resultados | HTML, PDF, CSV, XML y plataformas como Git Hub. | HTML,XML, grepeable y script kiddies | En este caso también Netsparker se lleva el gato al agua, ya que se puede exportar en los formatos más usados en las empresas e incluso en nuestra vida cotidiana como es el caso de HTML (Web), PDF, CSV (BBDD) o XML. |
| C.5: Integración | Alta | Alta | Las dos herramientas disponen de una gran capacidad de integración con otras herramienta, tanto es así que por defecto Netsparker lleva integradas 5 herramientas, mientras que Nmap tiene 3 herramientas integradas. |
| C.6: Plataformas disponibles | Windows | Windows, Mac OS X, AmigaOS y Unix | En este sentido, Nmap destaca por encima de Netsparker al ser este multiplataforma, mientras que Netsparker solo desarrolla para Windows, por lo que Nmap abarca la mayoría de los entornos de trabajo disponibles. |
| C.7: Complejidad | Baja | Media | En este caso, la complejidad en Netsparker apenas hay, ya que es una herramienta muy simple y fácil de usar lo que posibilita un mejor entendimiento con el cliente. Por otro lado Nmap tiene una complejidad media, por lo que con un poco de formación bastaría. |
| C.8 Tiempo de ejecución | Dependerá del objeto y del método utilizado. | Dependerá del método de escaneo | En este caso el tiempo de ejecución variará en el caso de Netsparker por el objeto y método utilizado, mientras que en Nmap por el método de escaneo usado. |
| C.9: Calidad del informe | Buena | Alta | La calidad del informe no es pobre en ningún caso de estos dos, pero si cabe destacar que es algo mejor el informe resultante de Nmap que del Netsparker al no incluir recomendaciones. |
| D.1: XSS (Cross-site Scripting) | Sí | No | En este caso Netsaparker sí controla este tipo de vulnerabilidad y resolviéndola sin ningún reparo, mientras que Nmap no presenta solución a esta inseguridad. |
| D.2: Rechazo de la inyección / respuesta de cabecera CRLF / HTTP | Sí | No | Ocurre lo mismo que en el caso anterior, Netsparker sí detecta este tipo de problema y propone soluciones para esta, mientras que en Nmap no se da este caso. |
| D.3: Inclusión de archivos remotos | Sí | No | En este caso Nmap no detecta si se ha incluido un archivo remotamente sin que nos diéramos cuenta, por lo que correría peligro nuestra web, mientras que Netsparker sí lo hace. |
| D.4: Mal uso de los puertos SSL y TSL para los pagos | No | Sí | En este sentido, Netsparker no detecta los puertos que tiene abiertos la web, mientras que en Nmap sí lo puede hacer y por tanto puede detectar si se usa de buena manera los protocolos de seguridad para el tema de pagos online. |
| D.5: Mal uso de los puertos HTTPS | No | Sí | Como en el caso anterior Nmap si detecta el uso de puertos y en este caso los puertos para una navegación segura, lo que nos hace descubrir si se usa de una manera adecuada o no estos puertos. Por el otro lado Netsparker no tiene esta funcionalidad. |
| D.6: Errores de desarrollo | Sí | Sí | Ambas tienen esta capacidad, por lo que se detectaría los errores que se cometen a la hora de desarrollar una web y por tanto corregir estos errores para evitar futuros problemas. |
| D.7: Errores de diseño | Sí | Sí | En este caso las dos herramientas sí disponen de esta funcionalidad, lo que hace evitar errores que se cometen a la hora de diseñar la web, ya que este tipo de errores son más visibles. |

# 6. Recomendaciones

## 6.1 Situación 1

### 6.1.1 Descripción de la situación

Una empresa de telefonía móvil quiere hacer un análisis de la seguridad de su sitio web, específicamente para ver la vulnerabilidad de los puertos, ya que esta web tiene problemas de robo de contraseñas, y así poder corregir los fallos de seguridad ya que en se almacenan los datos personales de todos los clientes y esto puede dar lugar a robos, suplantación de identidad...

### 6.1.2 Recomendación de tecnología a utilizar

|  |  |  |
| --- | --- | --- |
| **Criterios relevantes para la decisión** | **Ventajas tecnología 1 Netsparker** | **Ventajas tecnología 2 Nmap** |
| Criterio D.4: Mal uso de los puertos SSL y TSL para los pagos | No puede detectar el uso deficiente o las vulnerabilidades de dichos puertos. | Es capaz de detectar vulnerabilidades en los puertos SSL y TSL. |
| Criterio D.5: Mal uso de los puertos HTTPS | No puede detectar el mal uso de los puertos HTTPS. | Puede detectar el uso erróneo de los puertos HTTPS. |
| Criterio D.6: Errores de desarrollo | Pueden identificar más detalladamente los errores en el desarrollo de la web. | Pueden detectar los errores en el desarrollo de la web. |
| Criterio D.7: Errores de diseño | Puede identificar de manera más detallada y específica los errores en el diseño de una web. | Es capaz de identificar los errores en el diseño de la web. |

Este problema se debe principalmente a la conexión actual de la web en la cual los datos se transfieren en texto plano, por lo que cualquiera que se conecte a tu red wifi o tenga acceso a la comunicación entre tu ordenador y el servidor puede ver todo los datos que envías y recibes, por lo que podrían ver tus contraseñas y datos privados. Aquí entra en juego el uso de los puertos de SSL/TLS para enviar paquetes cifrados.

Recomendamos el uso de la herramienta Nmap ya que esta es una herramienta especializada en el análisis de puertos capaz de detectar vulnerabilidades en los puertos que usan los protocolos SSL, TLS, HTTPS… además de muchos otros puertos solo con poner una dirección IP o el nombre de la web, por lo que obtendremos un informe detallado de los problemas que tenemos en cada puerto. Netsparker no hace un estudio de seguridad orientado a las vulnerabilidades de los puertos por lo que con esta herramienta no podríamos detectar si algún puerto específico no está siendo usado correctamente o si puede ser un foco para posibles ataques. Respecto a los errores en el desarrollo y en el diseño de la web, ambas herramientas son buenas para la detección de vulnerabilidades aunque Netsparker es un más detallada, pero en este caso nos centramos específicamente en la seguridad de los puertos por lo que usaríamos Nmap.

## 6.2 Situación 2

### 6.2.1 Descripción de la situación

Los alumnos de la Universidad de Alcalá del Grado Ingeniería Informática han tenido que realizar un proyecto para la asignatura Ingeniería del Software Avanzada, en el que han desarrollado una página web para realizar intercambios dentro de la Unión Europea. Los niños elegirán un país, una duración y fecha de la estancia y una familia.

Como se almacenará una gran cantidad de datos sobre los niños que realizarán el intercambio y sus familias, estos alumnos quieren llevar a cabo un informe para ver la seguridad de su página web escrita en Java.

Queremos hacer un análisis detallado de la seguridad del sitio web, para encontrar vulnerabilidades tanto en los puertos de acceso como en el código fuente, analizando bases de datos, direcciones IP, posibles inclusiones de archivos remotos…

### 6.2.2 Recomendación de tecnología a utilizar

|  |  |  |
| --- | --- | --- |
| **Criterios relevantes para la decisión** | **Ventajas tecnología 1 Netsparker** | **Ventajas tecnología 2 Nmap** |
| Criterio A.2: Coste | La versión de escritorio tiene un precio de 1.195$ | Es gratuita. |
| Criterio C.6: Plataformas disponibles | Solo está disponible para el sistema operativo de Windows. | Está disponible para una gran variedad de sistemas, donde algunos de ellos son Windows o Linux. |
| Criterio D.1: XSS (Cross-site Scripting) | Permite detectar si se puede introducir un ejecutable de JavaScirpt. | No puede detectar la introducción de código. |
| Criterio D.2: Rechazo de la inyección / respuesta de cabecera CRLF / HTTP | Es capaz de detectar la inyección de CRLF. | No puede detectar la inyección de CRLF. |
| Criterio D.3: Inclusiones de archivos remotos | Es capaz de detectar la inyección de archivos remotos. | No es capaz de detectar la inyección de archivos remotos. |
| Criterio D.4: Mal uso de los puertos SSL y TSL para los pagos | No puede detectar las vulnerabilidades de los puertos de SSL / TLS. | Es capaz de detectar vulnerabilidades en los puertos SSL y TSL. |
| Criterio D.5: Mal uso de los puertos HTTPS | No puede detectar el uso de los puertos de HTTPS. | Puede detectar el uso erróneo de los puertos de HTTPS. |
| Criterio D.6: Errores de desarrollo | Pueden identificar más detalladamente los errores en el desarrollo de la web. | Pueden detectar los errores en el desarrollo de la web. |
| Criterio D.7: Errores de diseño | Puede identificar de manera más detallada y específica los errores en el diseño de una web. | Es capaz de identificar los errores en el diseño de la web. |

Netsparker se centra en el escaneo del código fuente detectando la posibilidad de inyecciones de código ejecutable en JavaScript en la aplicación web así como de detectar posibles secuencias de comandos entre los distintos sitios.

Realizará un análisis de Cross-Site Scriptitng y ataques de secuestro de sesión además de detectar la inyección de archivos ejecutables remotos que puedan ejecutar códigos en el servidor o la redirección a otras web que pueden ser hackeadas para re direccionar a sitios maliciosos y muchas cosas más. Pero tiene el problema de que no analiza la seguridad de los puertos correspondientes al acceso y a los protocolos. Por eso necesita la ayuda de la herramienta Nmap.

Nmap va a hacer un escaneo exhaustivo de los puertos para ver cuáles son las vulnerabilidades que hay. Para ello se analizará el uso de los puertos de los protocolos SSL /TLS y HTTPS además de muchos otros para ver los problemas que puede haber con el robo de información personal, los datos enviados y recibidos así como el cifrado de los paquetes que se envían y reciben. Además podremos analizar con ambas herramientas los errores en el desarrollo y la programación de la web.

Por lo tanto, en este caso recomendamos el uso de ambas herramientas ya que son complementarias y una fortalece los puntos débiles de la otra por lo que podremos obtener un resultado muy completo y detallado para ver las vulnerabilidades de la web y poder corregirlas.

## 6.3 Situación 3

### 6.3.1 Descripción de la situación

Una tienda que vende artículos y accesorios para animales de compañía, que se ha constituido recientemente, se encuentra con la situación de que le han llegado rumores de que se han desarrollado ataques cibernéticos en toda la zona en la que se ha ubicado la empresa, además de sus propios compañeros del sector que les informaron de este tipo de actos vandálicos.

Ahora mismo, disponen de una web a modo de tienda virtual (E-commerce), en la que se dedica a vender a todos los usuarios online de manera nacional. Para poder comprar en esta web será necesario registrarse en la aplicación. Por lo que se necesitará almacenar todos los datos personales de dicho usuario como pueden ser: la dirección, teléfono de contacto, DNI o NIF, etc.

Esta página web está desarrollada de una manera sencilla con el lenguaje de programación de C++. Por lo que el propietario de la organización necesita saber los errores o debilidades que tiene en la web así como en el diseño y desarrollo de esta. Y si se da el caso de tener entrometido ya algún virus o archivo remoto.

### 6.3.2 Recomendación de tecnología a utilizar

|  |  |  |
| --- | --- | --- |
| **Criterios relevantes para la decisión** | **Ventajas tecnología 1 Netsparker** | **Ventajas tecnología 2 Nmap** |
| Criterio A.2: Coste | Coste de 1.195$ | Gratuita. |
| Criterio C.6: Plataformas disponibles | Solo se encuentra disponible para el Sistema Operativo de Windows. | Está disponible para una gran variedad de sistemas como Windows o Linux. |
| Criterio D.1: XSS (Cross-site Scripting) | Detecta la intrusión de scrips ejecutables. | No puede detectar la introducción de código. |
| Criterio D.3: Inclusiones de archivos remotos | Es capaz de detectar la inyección de archivos remotos. | No es capaz de detectar la inyección de archivos remotos. |
| Criterio D.4: Mal uso de los puertos SSL y TSL para los pagos | No puede detectar las vulnerabilidades de los puertos de los protocolos SSL / TLS. | Es capaz de detectar vulnerabilidades en los puertos de los protocolos SSL y TSL. |
| Criterio D.5: Mal uso de los puertos HTTPS | No puede detectar el uso de los puertos de los protocolos de seguridad de HTTPS. | Puede detectar el uso erróneo de los puertos de los protocolos de seguridad de HTTPS. |
| Criterio D.6: Errores de desarrollo | Pueden identificar más detalladamente los errores en el desarrollo de la web. | Pueden detectar los errores en el desarrollo de la web. |
| Criterio D.7: Errores de diseño | Puede identificar de manera más detallada y específica los errores en el diseño de una web. | Es capaz de identificar los errores en el diseño de la web. |

En este caso como Netsparker se centra en el escaneo e investigación del código fuente, detecta la posibilidad de la intrusión de código ejecutable en C++ (lenguaje de programación muy utilizado para actos maliciosos) en la aplicación web así como de detectar posibles secuencias de comandos entre los distintos sitios.

Realizará un análisis de todos los posibles scripts introducidos y ataques de robo de información, así como la suplantación de indentidad en el inicio de sesión, además de detectar la inyección de archivos ejecutables remotos que puedan ejecutar códigos en el servidor o la redirección a otras web que pueden ser hackeadas para redireccionar a sitios maliciosos y muchas cosas más. Pero tiene el problema de que no analiza la seguridad de los puertos de seguridad de los protocolos usados.

Por eso será necesaria la aportación de la herramienta Nmap, ya que esta realizará una investigación exhaustiva de los puertos para ver cuáles son las vulnerabilidades existentes. Para ello se analizará el uso de los puertos de seguridad de los protocolos SSL/TLS (Para la compras de artículos) y HTTPS (Para la navegación segura de los usuarios) además de muchos otros relacionados con el robo de información personal, los datos enviados y recibidos así como el cifrado de los paquetes que se envían y reciben.

Además de ello también será necesario analizar con ambas herramientas los errores existentes en el diseño y desarrollo de la página web.

Por lo tanto, en esta situación recomendamos el uso de ambas herramientas para una correcta y completa investigación, ya que estas dos son complementarias, por lo que se obtendrá un informe muy detallado de todas las posibles vulnerabilidades y debilidades del sitio web, para poder sanarlas a tiempo.

# 7. Conclusión

Ambas herramientas son muy potentes y buenas para la realización de escaneos de seguridad y cada una tiene sus puntos más fuertes y sus puntos más débiles, lo cual no significa que una sea mejor que otra a la hora de hacer algo con ellas.

Cada una aporta un conocimiento diferente ya que Nmap está enfocada a la seguridad de puertos, mientras que Netsparker está más enfocado a la seguridad del código web. Una vez sepamos que queremos hacer decidiremos que herramienta es más adecuada para el caso.

Para llevar a cabo un informe muy completo y exhaustivo podemos emplear las dos herramientas ya que podríamos decir que son complementarias.