Contenido

[1. Autores del trabajo, planificación y entrega 3](#_Toc477618088)

[1.1 Autores 3](#_Toc477618089)

[1.2 Planificación 3](#_Toc477618090)

[1.3 Entrega 3](#_Toc477618091)

[2. Descripción del tipo de tecnología 3](#_Toc477618092)

[3. Fuentes de información (documentos) 4](#_Toc477618093)

[3.1 Fuentes sobre el tipo de tecnología en general 4](#_Toc477618094)

[**3.1.1** 4](#_Toc477618095)

[**3.1.2** 4](#_Toc477618096)

[**3.1.3** 4](#_Toc477618097)

[**3.1.4** 4](#_Toc477618098)

[3.2 Fuentes sobre la tecnología Netsparker 5](#_Toc477618099)

[3.2.1 5](#_Toc477618100)

[3.2.2 5](#_Toc477618101)

[3.2.3 5](#_Toc477618102)

[3.2.4 5](#_Toc477618103)

[3.3 Fuentes sobre la tecnología Nmap 5](#_Toc477618104)

[3.3.1 5](#_Toc477618105)

[3.3.2 5](#_Toc477618106)

[3.3.3 5](#_Toc477618107)

[3.3.4 5](#_Toc477618108)

[3.3.5 6](#_Toc477618109)

[3.3.6 6](#_Toc477618110)

[4. Fuentes de información (cursos no gratuitos) 6](#_Toc477618111)

[4.1 Cursos no gratuitos sobre el tipo de tecnología en general 6](#_Toc477618112)

[4.1.1 Escuela IT: Seguridad en el Desarrollo Web 6](#_Toc477618113)

[4.1.2 IT Master professional Training: Curso de Seguridad en Aplicaciones Web 7](#_Toc477618114)

[4.1.3 Video2Brain: Fundamentos de la programación: Seguridad web 7](#_Toc477618115)

[4.1.4 Global Knowledge: Securing the Web with Cisco Web Security Applicance v2.1 8](#_Toc477618116)

[4.1.5 EducaciónIT: Curso de Seguridad Web: SQL Injection & XSS 9](#_Toc477618117)

[4.2 Cursos no gratuitos sobre la tecnología Netsparker 10](#_Toc477618118)

[4.2.1 PenTest: Netsparker Web Application Scanner - Introduction + Lab Setup (W14) 10](#_Toc477618119)

[4.2.2 Redtech Aceademy: "Ethical hacking Nivel 1" 10](#_Toc477618120)

[4.2.3 Digital Tech Institute: ltinerario en seguridad IT 11](#_Toc477618121)

[4.3 Cursos no gratuitos sobre la tecnología Nmap 12](#_Toc477618122)

[4.3.1 Nmap: Network Scanning Basics and Advanced Techniques 12](#_Toc477618123)

[4.3.2 Nmap para Pentester 13](#_Toc477618124)

[4.3.3 Experto en Nmap para Hacking Ético 13](#_Toc477618125)

[4.3.4 Curso Virtual de Nmap 14](#_Toc477618126)

[5. Fuentes de información (cursos gratuitos) 15](#_Toc477618127)

[5.1 Cursos gratuitos sobre el tipo de tecnología en general 15](#_Toc477618128)

[5.1.1 Curso Hacker 15](#_Toc477618129)

[5.1.2 Sistemas Avanzados de Seguridad y SI 15](#_Toc477618130)

[5.1.3 Ciberseguridad: formación, promoción de talento e investigación 16](#_Toc477618131)

[5.1.4 Temas Avanzados en Seguridad y SI 17](#_Toc477618132)

[5.2 Cursos gratuitos sobre la tecnología Netsparker 17](#_Toc477618133)

[5.2.1 Hackxcrack: Curso de Seguridad Informática Básico 17](#_Toc477618134)

[5.2.2 Netsparker, canal de youtube 18](#_Toc477618135)

[5.2.3 Netsparker, página oficial 19](#_Toc477618136)

[5.3 Cursos gratuitos sobre la tecnología Nmap 19](#_Toc477618137)

[5.3.1 Uso de la herramienta Nmap - Ed 17/01 19](#_Toc477618138)

[5.3.2 Nmap Básico: Curso de Seguridad Informática 2017 20](#_Toc477618139)

[5.3.3 Video Wiki: Proyecto Nmap - Todo sobre Nmap 21](#_Toc477618140)

[6. Ayudas económicas para estudiar las tecnologías 21](#_Toc477618141)

[7. Recursos para implementar las tecnologías 26](#_Toc477618142)

[7.1 Recursos para implementar la tecnología Netsparker 26](#_Toc477618143)

[7.1.1 Recursos gratuitos 26](#_Toc477618144)

[7.1.1.1 26](#_Toc477618145)

[7.1.1.2 26](#_Toc477618146)

[7.1.1.3 26](#_Toc477618147)

[7.1.2 Recursos no gratuitos 27](#_Toc477618148)

[7.1.2.1 27](#_Toc477618149)

[7.1.2.2 28](#_Toc477618150)

[7.1.2.3 28](#_Toc477618151)

[7.1.2.4 29](#_Toc477618152)

[7.1.2.5 29](#_Toc477618153)

[7.1.2.7 29](#_Toc477618154)

[7.2 Recursos para implementar la tecnología Nmap 30](#_Toc477618155)

[7.2.1 Recursos gratuitos 30](#_Toc477618156)

[7.2.2 Recursos no gratuitos 31](#_Toc477618157)

[8. Conclusiones 31](#_Toc477618158)

# 1. Autores del trabajo, planificación y entrega

## 1.1 Autores

Somos el grupo T4 formado por:

* Jonatan Viñuelas Caballero \*
* 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 45 horas, pero nosotros le hemos dedicado 50 horas al llevarnos mucha investigación por falta de información de dicho proyecto. Estas horas se pueden apreciar claramente en el siguiente diagrama:

[**Planificación TG1 (Grupo T4)**](https://app.ganttpro.com/shared/token/b8f0262e0ed911fce78cebe0d3971b1dd8bf59238feb055e046c3e0858c19d9a)

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.

## 1.3 Entrega

El enlace a nuestro repositorio es el siguiente:

[**https://github.com/JonatanVinuelasCaballero/TG1**](https://github.com/JonatanVinuelasCaballero/TG1)

# 2. Descripción del tipo de tecnología

En este trabajo vamos a centrarnos en Web testing tools: Security, ya que la seguridad es un tema importante, actual y de futuro.

Las herramientas de pruebas web se encargan de realizar pruebas software. Estas pruebas pueden ayudar a abordar problemas antes de que el sistema se revele al público. Se encargan de cuestiones tales como la seguridad de la aplicación web, la funcionalidad básica del sitio, su accesibilidad para los usuarios…

Las pruebas de seguridad Web nos dicen si los requisitos de las aplicaciones basadas en Web se cumplen cuando son sometidos a datos de entrada maliciosos.

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

* Netsparker: 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.

Fácil de usar, y utiliza la avanzada tecnología de escaneo de vulnerabilidades Prueba-base y se ha incorporado en las pruebas de penetración y herramientas de reporte. Esta herramienta es de pago, pero nos ofrece una prueba gratuita.

* Nmap: Es una herramienta de código abierto para la exploración de red y auditoría de seguridad. 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. Esta herramienta es gratuita.

# 3. Fuentes de información (documentos)

## 3.1 Fuentes sobre el tipo de tecnología en general

### **3.1.1**

[**https://es.wikipedia.org/wiki/Seguridad\_de\_aplicaciones\_web**](https://es.wikipedia.org/wiki/Seguridad_de_aplicaciones_web)

Esta fuente nos informa sobre que es la seguridad de aplicaciones web, estándares de seguridad, tecnología de seguridad y amenazas de seguridad.

### **3.1.2**

[**https://www.certsuperior.com/Blog/tipos-de-seguridad-informatica-herramientas-vitales-para-tu-estadia-en-internet**](https://www.certsuperior.com/Blog/tipos-de-seguridad-informatica-herramientas-vitales-para-tu-estadia-en-internet)

Esta fuente nos informa sobre los tipos de seguridad informática: Herramientas vitalespara tu estadía en internet.

### **3.1.3**

[**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/)

Esta fuente nos muestra las 8 mejores herramientas de seguridad y hacking, entre las que aparece Nmap.

### **3.1.4**

[**http://www.seguridad.unam.mx/documento/?id=17**](http://www.seguridad.unam.mx/documento/?id=17)

Esta fuente nos informa sobre los Aspectos Básicos de la Seguridad en Aplicaciones Web.

## 3.2 Fuentes sobre la tecnología Netsparker

### **3.2.1**

[**http://www.kitploit.com/2015/03/netsparker-4-easier-to-use-more.html?utm\_source=feedburner&utm\_medium=email&utm\_campaign=Feed%3A+PentestTools+%28PenTest+Tools%29**](http://www.kitploit.com/2015/03/netsparker-4-easier-to-use-more.html?utm_source=feedburner&utm_medium=email&utm_campaign=Feed%3A+PentestTools+%28PenTest+Tools%29)

Esta fuente nos informa sobre la utilización de la herramienta Netsparker, detallándola con pantallazos.

### **3.2.2**

[**https://www.netsparker.com/web-vulnerability-scanner/overview/**](https://www.netsparker.com/web-vulnerability-scanner/overview/)

Esta fuente nos informa sobre los principales beneficios de Netsparker.

### **3.2.3**

[**http://www.securitybydefault.com/2010/01/un-vistazo-netsparker-de-mavituna.html**](http://www.securitybydefault.com/2010/01/un-vistazo-netsparker-de-mavituna.html)

Esta fuente nos informa sobre la empresa [Mavituna Security](http://www.mavitunasecurity.com/)  que desarrolla un producto de análisis de vulnerabilidades web llamado [Netsparker](http://www.mavitunasecurity.com/netsparker/) . Nos informa sobre sus características y las posibilidades que ofrece, acompañado de de pantallazos.

### **3.2.4**

[**https://www.netsparker.com/web-vulnerability-scanner/built-in-penetration-testing-tools/**](https://www.netsparker.com/web-vulnerability-scanner/built-in-penetration-testing-tools/)

Esta fuente nos informa sobre las herramientas integradas de Netsparker.

## 3.3 Fuentes sobre la tecnología Nmap

### **3.3.1**

[**https://nmap.org/book/man.html**](https://nmap.org/book/man.html)

Esta fuente nos muestra una Guía de referencia de Nmap.

### **3.3.2**

[**https://paraisolinux.com/que-es-y-como-usar-nmap/**](https://paraisolinux.com/que-es-y-como-usar-nmap/)

Esta fuente nos informa sobre que es Nmap y como se usa, además de enseñarnos algunos conceptos básicos importantes como que es un puerto, un servicio, un firewall…

### **3.3.3**

[**https://conocimientolibre.wordpress.com/2007/06/30/nmap-a-fondo-escaneo-de-redes-y-hosts/**](https://conocimientolibre.wordpress.com/2007/06/30/nmap-a-fondo-escaneo-de-redes-y-hosts/)

Esta fuente nos informa a fondo sobre Nmap: escaneo de redes y hosts.

### **3.3.4**

[**http://es.wikihow.com/ejecutar-un-simple-escaneo-de-Nmap**](http://es.wikihow.com/ejecutar-un-simple-escaneo-de-Nmap)

Esta fuente es una guía de cómo ejecutar un simple escaneo con Nmap.

### **3.3.5**

[**https://www.youtube.com/results?search\_query=escaneo+basico+con+nmap**](https://www.youtube.com/results?search_query=escaneo+basico+con+nmap)

En esta fuente podemos encontrar una gran variedad de vídeo tutoriales de cómo hacer un escaneo básico con Nmap y otros temas.

### **3.3.6**

[**https://svn.nmap.org/nmap/docs/nmap.usage.txt**](https://svn.nmap.org/nmap/docs/nmap.usage.txt)

Aquí podemos encontrar una lista con todas las funciones posibles que tiene Nmap.

# 4. Fuentes de información (cursos no gratuitos)

## 4.1 Cursos no gratuitos sobre el tipo de tecnología en general

### **4.1.1 Escuela IT: Seguridad en el Desarrollo Web**

|  |  |
| --- | --- |
| **NOMBRE** | Seguridad en el Desarrollo Web |
| **TECNOLOGÍA** | Seguridad Web |
| **IMPARTIDOR** | Escuela IT |
| **URL** | [**https://escuela.it/cursos/seguridad-en-el-desarrollo-web**](https://escuela.it/cursos/seguridad-en-el-desarrollo-web) |
| **PRECIO** | 90€ |
| **DURACIÓN** | 8 horas aprox. |
| **MODALIDAD** | Online |
| **DESCRIPCIÓN** | El objetivo general de esta nueva iniciativa es capacitar al profesional para incorporar técnicas de Seguridad tanto a su profesión como a sus aplicaciones. Este curso se dirige a todos aquellos desarrollares, diseñadores y administradores de un sitio web  que quieran crear o participar en proyectos robustos gracias a un código seguro protegiendo la información sensible y crítica manejada en una aplicación web. |

### 

### **4.1.2 IT Master professional Training: Curso de Seguridad en Aplicaciones Web**

|  |  |
| --- | --- |
| **NOMBRE** | Curso de Seguridad en Aplicaciones Web |
| **TECNOLOGÍA** | Seguridad Web |
| **IMPARTIDOR** | IT Master professional Training |
| **URL** | [**https://www.itmaster.com.ar/cursos/curso-seguridad-web**](https://www.itmaster.com.ar/cursos/curso-seguridad-web) |
| **PRECIO** | A consultar |
| **DURACIÓN** | 18 horas aprox. |
| **MODALIDAD** | Personalizado / In Company |
| **DESCRIPCIÓN** | Conviértete en un profesional de seguridad aplicada al desarrollo web, conociendo todas las técnicas de ataques a sitios web, como DoS, SQL Injection, Cross Site Scripting, así como ataques a servidores Apache, Internet Information Server y bases de datos MySQL y SQL Server. |

### **4.1.3 Video2Brain: Fundamentos de la programación: Seguridad web**

|  |  |
| --- | --- |
| **NOMBRE** | Fundamentos de la programación: Seguridad web |
| **TECNOLOGÍA** | Seguridad Web |
| **IMPARTIDOR** | Video2Brain |
| **URL** | [**https://www.video2brain.com/es/cursos/fundamentos-de-la-programacion-seguridad-web**](https://www.video2brain.com/es/cursos/fundamentos-de-la-programacion-seguridad-web) |
| **PRECIO** | Prueba 10 días Gratis / Mensual 19,95€ / Anual198€ /  Plan anual completo 298€ |
| **DURACIÓN** | 3 horas aprox. |
| **MODALIDAD** | Online |
| **DESCRIPCIÓN** | Si una aplicación va a ser accedida por múltiples usuarios, y sobre todo, si va a estar conectada a una red accesible desde la web, debemos asegurar que únicamente se puede acceder a ella por los canales que hemos diseñado y que cumple con unos requisitos mínimos de seguridad. De esta manera, la seguridad se convierte en uno de los pilares fundamentales del diseño de aplicaciones, en ocasiones incluso por delante de otros ejes de desarrollo. Aprende cuáles son los medios y los canales más comunes para acceder a una aplicación web, cuáles son sus debilidades y cómo programar aplicaciones que bloqueen los accesos no autorizados o cómo corregir deficiencias en aplicaciones ya existentes. |

### **4.1.4 Global Knowledge: Securing the Web with Cisco Web Security Applicance v2.1**

|  |  |
| --- | --- |
| **NOMBRE** | Securing the Web with Cisco Web Security Applicance |
| **TECNOLOGÍA** | Seguridad Web |
| **IMPARTIDOR** | Global Knowledge |
| **URL** | [**https://www.globalknowledge.es/cursos/cisco/seguridad/swsa.html**](https://www.globalknowledge.es/cursos/cisco/seguridad/swsa.html) |
| **PRECIO** | 1290€ |
| **DURACIÓN** | A consultar |
| **MODALIDAD** | In Company / Presencial / Online |
| **DESCRIPCIÓN** | Este curso ha sido diseñado para ayudar a los estudiantes a entender cómo instalar, configurar, administrar y solucionar problemas de una solicitud de Cisco Web Security Applicance (WSA). Los estudiantes aprenderán a diseñar, configurar, administrar, monitorear y solucionar problemas de Cisco Web Security Appliance (WSA) en pequeñas y medianas empresas y en instalaciones empresariales. Los extensos ejercicios de laboratorio proporcionan a los asistentes una experiencia práctica crítica con el producto, proporcionando un entorno seguro para experimentar con malware, etc. |

### **4.1.5 EducaciónIT: Curso de Seguridad Web: SQL Injection & XSS**

|  |  |
| --- | --- |
| **NOMBRE** | Curso de Seguridad Web: SQL Injection & XSS |
| **TECNOLOGÍA** | Seguridad Web |
| **IMPARTIDOR** | EducaciónIT |
| **URL** | [**http://www.educacionit.com/curso-de-seguridad-web**](http://www.educacionit.com/curso-de-seguridad-web) |
| **PRECIO** | 65€ |
| **DURACIÓN** | 15 horas |
| **MODALIDAD** | Presencial / Online |
| **DESCRIPCIÓN** | En este curso aprenderas las técnicas más utilizadas por los hackers para vulnerar aplicaciones web y cómo utilizarlas para analizar la seguridad de las aplicaciones empresariales, realizando ataques como SQL Injection y Cross Site Scripting (XSS). |

## 4.2 Cursos no gratuitos sobre la tecnología Netsparker

### **4.2.1 PenTest: Netsparker Web Application Scanner - Introduction + Lab Setup (W14)**

|  |  |
| --- | --- |
| **NOMBRE** | Netsparker Web Application Scanner - Introduction + Lab Setup (W14) |
| **TECNOLOGÍA** | Netsparker |
| **IMPARTIDOR** | PenTest |
| **URL** | [**https://pentestmag.com/course/netsparker-web-application-scanner-w14-2/**](https://pentestmag.com/course/netsparker-web-application-scanner-w14-2/) |
| **PRECIO** | PentTest Premium 790$ / IT Pack Premium 1890$  \*Obligatorio para este curso elegir uno de estos dos planes |
| **DURACIÓN** | A consultar |
| **MODALIDAD** | Online |
| **DESCRIPCIÓN** | Netsparker es una herramienta cuya detección única y las técnicas de explotación segura le permiten ser exactos, de ahí que sea el primer y único escáner de vulnerabilidad de Web False Positive Free, por lo que los usuarios de este curso pueden centrarse en la corrección de vulnerabilidades y problemas de seguridad informados sin perder tiempo en aprender cómo utilizar el escáner de vulnerabilidad web o verificar sus resultados ya que es muy sencillo de aprender. |

### **4.2.2 Redtech Aceademy: "Ethical hacking Nivel 1"**

|  |  |
| --- | --- |
| **NOMBRE** | Ethical hacking Nivel 1 |
| **TECNOLOGÍA** | Netsparker |
| **IMPARTIDOR** | Redtech Aceademy |
| **URL** | [**http://www.redtechhackingshop.com/product-page/preventa-curso-dvd-ethical-hacking-nivel-1**](http://www.redtechhackingshop.com/product-page/preventa-curso-dvd-ethical-hacking-nivel-1) |
| **PRECIO** | 950$ |
| **DURACIÓN** | ·35 vídeos o clases |
| **MODALIDAD** | Presencial / DVD |
| **DESCRIPCIÓN** | Es un curso de 35 videos que abarcan horas de información y contenido en donde al alumno se le mostrará y se le llevará de la mano para que pueda realizar desde cero una prueba de penetración en diferentes tipos de sistemas y plataformas, de tal forma que el alumno aprenderá a usar de manera correcta las distintas herramientas, entre las que se encuentra Netsparker, para determinar la mejor forma de atacar un sistema y como protegerse de dichos ataques. |

### **4.2.3 Digital Tech Institute: ltinerario en seguridad IT**

|  |  |
| --- | --- |
| **NOMBRE** | ltinerario en seguridad IT / Master en seguridad IT |
| **TECNOLOGÍA** | Netsparker |
| **IMPARTIDOR** | Digital Tech Institute |
| **URL** | [**http://www.digitaltechinstitute.com/formacion-in-company/itinerario-seguridad-it/**](http://www.digitaltechinstitute.com/formacion-in-company/itinerario-seguridad-it/) |
| **PRECIO** | A consultar |
| **DURACIÓN** | ·8 semanas |
| **MODALIDAD** | Presencial / In Company |
| **DESCRIPCIÓN** | Este curos está diseñado para compañías o particulares, ya que también se ofrece el master, que quieran invertir en la formación de sus empleados y aumentar sus conocimientos en ciberseguridad informática y hacking ético. Con la llegada del IoT y el Cloud, los peligros relacionados con el espionaje industrial y la pérdida de información confidencial pueden acarrear graves problemas para las compañías. De ahí que sea de vital importancia contar con formación in company en seguridad IT para potenciar las habilidades de seguridad de los profesionales de las empresas. Dentro de este curso se van a tratar diversos temas y diversas tecnologías, donde habrá un apartado para Netsparker. |

## 4.3 Cursos no gratuitos sobre la tecnología Nmap

### **4.3.1 Nmap: Network Scanning Basics and Advanced Techniques**

|  |  |
| --- | --- |
| **NOMBRE** | Network Scanning Basics and Advanced Techniques |
| **TECNOLOGÍA** | Nmap |
| **IMPARTIDOR** | Jason Wood |
| **URL** | [**https://www.udemy.com/nmap-scan/**](https://www.udemy.com/nmap-scan/) |
| **PRECIO** | 15€ |
| **DURACIÓN** | 3 horas aprox. |
| **MODALIDAD** | Online |
| **DESCRIPCIÓN** | Este curso tratará los conceptos básicos de escaneo en red con Nmap y se moverá hacia cómo puede utilizarlo de forma segura y eficaz en su red. Se utilizará ejemplos prácticos y demostraciones para mostrar cómo puede utilizar Nmap ahora mismo y desde cero. |

### **4.3.2 Nmap para Pentester**

|  |  |
| --- | --- |
| **NOMBRE** | Nmap para Pentester |
| **TECNOLOGÍA** | Nmap |
| **IMPARTIDOR** | Ingeniero en Computación Misael Banales |
| **URL** | [**https://backtrackacademy.com/curso/nmap**](https://backtrackacademy.com/curso/nmap)  [**https://openwebinars.net/blog/nmap-uso-basico-para-rastreo-de-puertos/**](https://openwebinars.net/blog/nmap-uso-basico-para-rastreo-de-puertos/) |
| **PRECIO** | 16,79€ |
| **DURACIÓN** | 8 horas aprox. |
| **MODALIDAD** | Online |
| **DESCRIPCIÓN** | Este curso explica como Nmap permite a los auditores de seguridad realizar un completo escaneo de puertos, detectar si un host se encuentra activo, además permite detectar servicios con sus respectivas versiones. Por otro lado esta herramienta no es solo un simple escáner de puertos, ya que permite detectar vulnerabilidades a través de sus scripts personalizados. |

### **4.3.3 Experto en Nmap para Hacking Ético**

|  |  |
| --- | --- |
| **NOMBRE** | Experto en Nmap para Hacking Ético |
| **TECNOLOGÍA** | Nmap |
| **IMPARTIDOR** | Comunix Group |
| **URL** | [**https://www.comunixgroup.com/producto/experto-nmap-hacking-etico/**](https://www.comunixgroup.com/producto/experto-nmap-hacking-etico/) |
| **PRECIO** | 79€ |
| **DURACIÓN** | 120 horas aprox. |
| **MODALIDAD** | Online |
| **DESCRIPCIÓN** | El curso es totalmente práctico y online, ya que proporciona una excelente guía para utilizar todas las funcionalidades y características de Nmap. Así mismo, es una excelente fuente de conocimiento tanto para aquellos recién iniciándose con esta herramienta, como para aquellos profesionales ya utilizándola. |

### **4.3.4 Curso Virtual de Nmap**

|  |  |
| --- | --- |
| **NOMBRE** | Curso Virtual de Nmap |
| **TECNOLOGÍA** | Nmap |
| **IMPARTIDOR** | Alonso Eduardo Caballero Quezada |
| **URL** | [**http://www.reydes.com/archivos/cursos/Curso\_Nmap.pdf**](http://www.reydes.com/archivos/cursos/Curso_Nmap.pdf) |
| **PRECIO** | 32,60€ |
| **DURACIÓN** | 6 horas aprox. |
| **MODALIDAD** | Online |
| **DESCRIPCIÓN** | El curso es totalmente práctico y online, y en este se expondrá la utilidad de esta herramienta para tareas como realizar un inventario de la red, gestionar horarios para la actualización de servicios, además de vigilancia de hosts o tiempo de funcionamiento de un servicio. |

# 5. Fuentes de información (cursos gratuitos)

## 5.1 Cursos gratuitos sobre el tipo de tecnología en general

### **5.1.1 Curso Hacker**

|  |  |
| --- | --- |
| **NOMBRE** | Curso Hacker |
| **TECNOLOGÍA** | Seguridad Web |
| **IMPARTIDOR** | Grupo SanValero |
| **URL** | [**http://cursohacker.es/curso-hacking-online-completo**](http://cursohacker.es/curso-hacking-online-completo) |
| **PRECIO** | Gratis |
| **DURACIÓN** | 3 horas |
| **MODALIDAD** | Online |
| **DESCRIPCIÓN** | Se tratarán temas de seguridad informática, pentesting e intrusiones en entornos controlados. Organizan la web como un curso hacker debido a que los conocimientos que se expondrán serán prácticas que todo hacker domina y que todo buen administrador de sistemas debe de controlar. |

### **5.1.2 Sistemas Avanzados de Seguridad y SI**

|  |  |
| --- | --- |
| **NOMBRE** | Sistemas Avanzados de Seguridad y SI |
| **TECNOLOGÍA** | Seguridad Web |
| **IMPARTIDOR** | Universidad Politécnica de Madrid |
| **URL** | [**https://www.tutellus.com/ciencias-aplicadas/informatica/sistemas-avanzados-de-seguridad-y-si-1889**](https://www.tutellus.com/ciencias-aplicadas/informatica/sistemas-avanzados-de-seguridad-y-si-1889) |
| **PRECIO** | Gratis |
| **DURACIÓN** | 10 horas |
| **MODALIDAD** | Online |
| **DESCRIPCIÓN** | Se tratarán temas sobre sistemas avanzados de seguridad y de Sistemas de la Información, con lo que se podrá aprender las últimas técnicas y futuras tendencias en un sector lleno de oportunidades laborales, como la Ciberdefensa o la Ciberdelincuencia. |

### **5.1.3 Ciberseguridad: formación, promoción de talento e investigación**

|  |  |
| --- | --- |
| **NOMBRE** | Ciberseguridad: formación, promoción de talento e investigación |
| **TECNOLOGÍA** | Seguridad Web |
| **IMPARTIDOR** | Miguel Rego, Director General de INCIBE (Instituto Nacional de Ciberseguridad) |
| **URL** | [**https://www.tutellus.com/ciencias-aplicadas/informatica/ciberseguridad-formacion-promocion-de-talento-e-investigacion-10638**](https://www.tutellus.com/ciencias-aplicadas/informatica/ciberseguridad-formacion-promocion-de-talento-e-investigacion-10638) |
| **PRECIO** | Gratis |
| **DURACIÓN** | 1 hora |
| **MODALIDAD** | Online |
| **DESCRIPCIÓN** | Este curso se basa en la Ciberseguridad, porque es un espacio lleno de incógnitas. Aunque no se para de innovar, es un sector muy desconocido. También se comentará las últimas tendencias en el sector, la importancia de encontrar gente formada y experta en seguridad informática y dejará algunas pinceladas del futuro del sector. |

### **5.1.4 Temas Avanzados en Seguridad y SI**

|  |  |
| --- | --- |
| **NOMBRE** | Temas Avanzados en Seguridad y SI |
| **TECNOLOGÍA** | Seguridad Web |
| **IMPARTIDOR** | Universidad Politécnica de Madrid |
| **URL** | [**https://www.tutellus.com/ciencias-aplicadas/informatica/temas-avanzados-en-seguridad-y-si-2012-696**](https://www.tutellus.com/ciencias-aplicadas/informatica/temas-avanzados-en-seguridad-y-si-2012-696) |
| **PRECIO** | Gratis |
| **DURACIÓN** | 10 horas |
| **MODALIDAD** | Online |
| **DESCRIPCIÓN** | Este curso trata de dar a conocer los últimos avances en materia de seguridad informática y protección de la información desde diversos puntos de vista: redes, datos, gestión, legislación, estándares. Así como dar a conocer los nuevos avances en tecnologías de la información y fomentar el conocimiento crítico de la sociedad de la información con sus aspectos positivos de desarrollo así como sus amenazas. Además de analizar el impacto social, ambiental y ético del uso de las tecnologías de la información, los entornos de libertad y privacidad del ser humano. Conocer la realidad empresarial, industrial y de organismos del estado relacionada con la seguridad y la sociedad de la información. |

## 5.2 Cursos gratuitos sobre la tecnología Netsparker

### **5.2.1 Hackxcrack: Curso de Seguridad Informática Básico**

|  |  |
| --- | --- |
| **NOMBRE** | Curso de Seguridad Informática Básico |
| **TECNOLOGÍA** | Netsparker |
| **IMPARTIDOR** | Hackxcrack |
| **URL** | [**https://foro.hackxcrack.net/hacking/curso-de-seguridad-informatica-basico-intermedia-(gratis)-por-grizzlysec/**](https://foro.hackxcrack.net/hacking/curso-de-seguridad-informatica-basico-intermedia-(gratis)-por-grizzlysec/) |
| **PRECIO** | Gratis |
| **DURACIÓN** | Serie de videos de 2 horas y 30 min cada uno |
| **MODALIDAD** | Online |
| **DESCRIPCIÓN** | En este curso se van a tratar temas de distintos ámbitos y tecnologías de seguridad desde footprinting, tecnincas de anonimato, explotación de vulnerabilidades hasta sacanning, donde podremos encontrar la herramienta de Nesparker, |

### **5.2.2 Netsparker, canal de youtube**

|  |  |
| --- | --- |
| **NOMBRE** | Netsparker |
| **TECNOLOGÍA** | Netsparker |
| **IMPARTIDOR** | Netsparker Youtube |
| **URL** | [**https://www.youtube.com/user/netsparker**](https://www.youtube.com/user/netsparker) |
| **PRECIO** | Gratis |
| **DURACIÓN** | Serie de videos |
| **MODALIDAD** | Online |
| **DESCRIPCIÓN** | Este es el canal oficial de Netsparker donde podemos ver una gran cantidad de tutoriales sobre como usar dicha herramienta. |

### **5.2.3 Netsparker, página oficial**

|  |  |
| --- | --- |
| **NOMBRE** | Guía de Netsparker |
| **TECNOLOGÍA** | Netsparker |
| **IMPARTIDOR** | Netsparker |
| **URL** | [**https://www.netsparker.com/support/**](https://www.netsparker.com/support/) |
| **PRECIO** | Gratis |
| **DURACIÓN** | Depende del usuario |
| **MODALIDAD** | Online |
| **DESCRIPCIÓN** | En la página oficial de Netsparker podemos encontrar una guía para el uso de esta herramienta, tanto en la nube como en la aplicación de escritorio. En estas guías vamos a ver desde cómo se hace la instalación de la herramienta hasta preguntas frecuentes. |

## 5.3 Cursos gratuitos sobre la tecnología Nmap

### **5.3.1 Uso de la herramienta Nmap - Ed 17/01**

|  |  |
| --- | --- |
| **NOMBRE** | Uso de la herramienta Nmap - Ed 17/01 |
| **TECNOLOGÍA** | Nmap |
| **IMPARTIDOR** | CSIRT-CV |
| **URL** | [**http://www.saps.gva.es/oferta-formativa/?show=50&lang=es**](http://www.saps.gva.es/oferta-formativa/?show=50&lang=es) |
| **PRECIO** | Gratis |
| **DURACIÓN** | 1 hora |
| **MODALIDAD** | Online |
| **DESCRIPCIÓN** | Este curso gratuito tratará sobre el uso de la herramienta Nmap, orientado a profesionales de las TIC (administradores de sistemas, ingenieros de comunicaciones y auditores de seguridad o penetration testers), estudiantes o aficionados interesados en la informática, las redes y la seguridad. En él se aprenderán los fundamentos básicos de la herramienta Nmap, la cual resulta muy útil para la realización de tareas como inventario de red o monitorización de sistemas y servicios. La herramienta puede averiguar los equipos que están levantados, los servicios que ofrecen y el sistema operativo de los mismos. |

### **5.3.2 Nmap Básico: Curso de Seguridad Informática 2017**

|  |  |
| --- | --- |
| **NOMBRE** | Nmap Básico: Curso de Seguridad Informática 2017 |
| **TECNOLOGÍA** | Nmap |
| **IMPARTIDOR** | ViinVideos |
| **URL** | [**https://www.youtube.com/watch?v=Z\_9AnQzeE4Y**](https://www.youtube.com/watch?v=Z_9AnQzeE4Y)  [**https://openwebinars.net/blog/nmap-uso-basico-para-rastreo-de-puertos/**](https://openwebinars.net/blog/nmap-uso-basico-para-rastreo-de-puertos/) |
| **PRECIO** | Gratis |
| **DURACIÓN** | 32 minutos |
| **MODALIDAD** | Online |
| **DESCRIPCIÓN** | Se basa en explicar por qué Nmap coloca todos los puertos cerrados, además de uso y conocimiento de los comandos básicos de este. |

### **5.3.3 Video Wiki: Proyecto Nmap - Todo sobre Nmap**

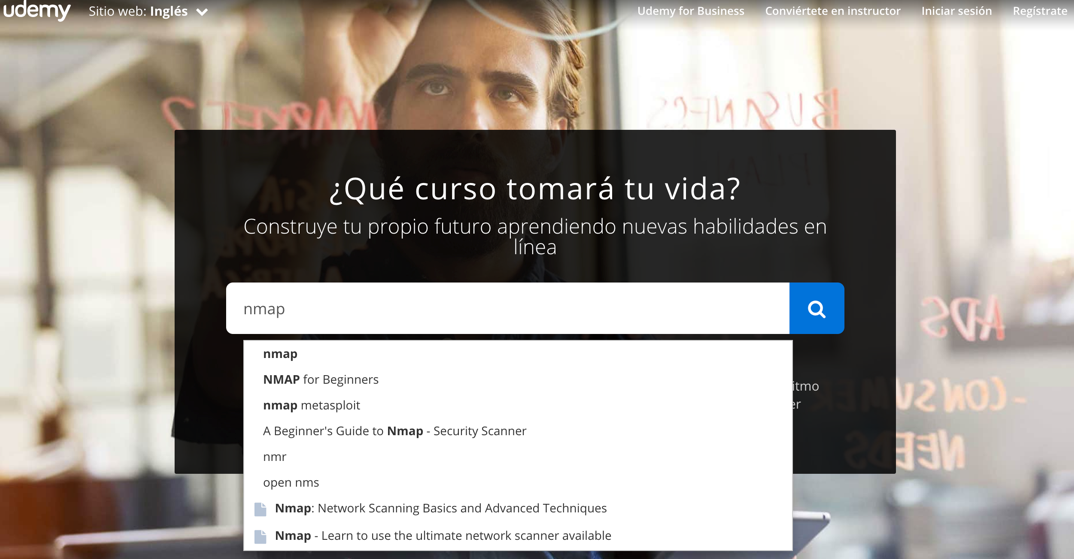
|  |  |
| --- | --- |
| **NOMBRE** | Video Wiki: Proyecto Nmap - Todo sobre Nmap |
| **TECNOLOGÍA** | Nmap |
| **IMPARTIDOR** | OHCS |
| **URL** | [**https://www.youtube.com/watch?v=LXVjhMc0ukg&list=PL1UnfB2evouFU3soYrISSJw5oqSZbb-nW**](https://www.youtube.com/watch?v=LXVjhMc0ukg&list=PL1UnfB2evouFU3soYrISSJw5oqSZbb-nW) |
| **PRECIO** | Gratis |
| **DURACIÓN** | 1 hora y 15 minutos |
| **MODALIDAD** | Online |
| **DESCRIPCIÓN** | El curso es un conjunto de 6 vídeos en los que trata en profundidad esta herramienta, explicando paso a paso el uso y todo lo que se puede hacer con este. Por lo que en cada sesión explica las técnicas usadas con Nmap. |

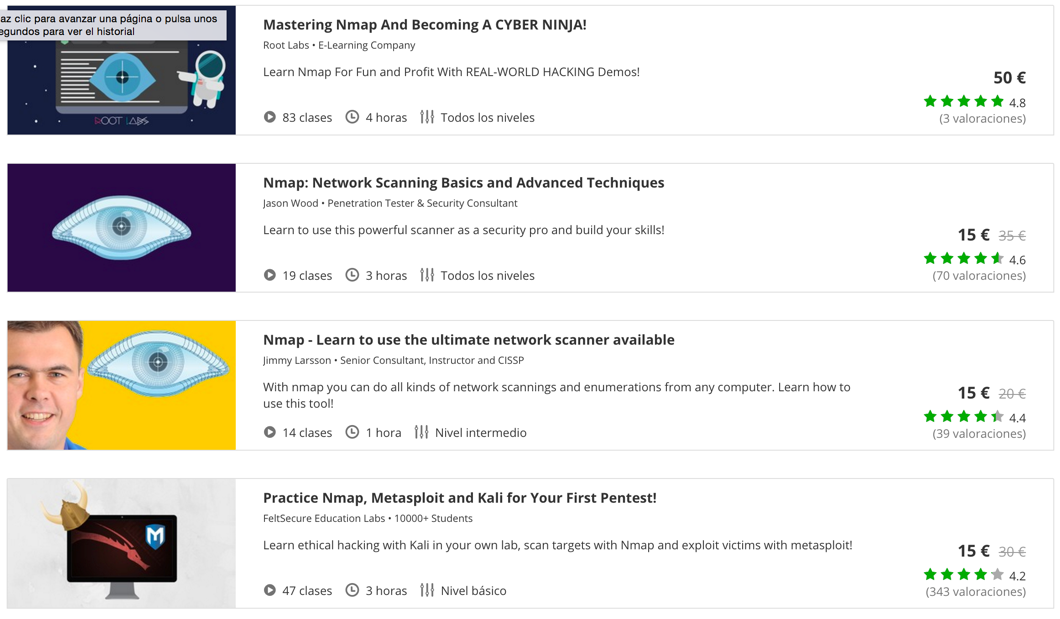
# 6. Ayudas económicas para estudiar las tecnologías

* Ayudas en descuentos para la formación:

- En la plataforma web de Udemy podemos encontrar cursos sobre seguridad, y entre ellos sobre Nmap. Muchos de estos cursos ya suelen aparecer con una rebaja hecha por la propia web:

**https://www.udemy.com/courses/search/?ref=home&src=ukw&q=nmap&sort=highest-rated**





- Pero además hemos encontrado una página que ofrece cupones de descuentos para Udemy.

[**https://www.mascupon.es/tiendas/cupon-descuento-udemy/**](https://www.mascupon.es/tiendas/cupon-descuento-udemy/)



- El curso de Experto en Nmap para Hacking Ético ofertado por Comunix Group, ofrece el curso con un 84% de descuento. El coste del curso pasa de costar 500 euros a 79 euros.



**https://www.comunixgroup.com/producto/experto-nmap-hacking-etico/**

- En el curso Escuela IT: Seguridad en el Desarrollo Webteníamos el objetivo de conocer, descubrir y protegernos de las amenazas más comunes en la nueva era del desarrollo web. En este curso nos ofrecen un descuento de 30€ por lo que pasa de 120€ a 90€.



[**https://escuela.it/cursos/seguridad-en-el-desarrollo-web**](https://escuela.it/cursos/seguridad-en-el-desarrollo-web)

- En el curso IT Master professional Training: Curso de Seguridad en Aplicaciones Webseasegura tus desarrollos web con las más modernas y efectivas técnicas de defensa de ataques en aplicaciones web. Analizarás todas las técnicas de ataque y cómo defenderse, como SQL Injection o XSS, junto a teoría de Seguridad Informática. Tiene las siguientes promociones vigentes:

-10% de descuento por grupos de 3 alumnos

-15% de descuento por grupos de 5 alumnos

-Hasta 12 cuotas fijas con Tarjeta de Crédito

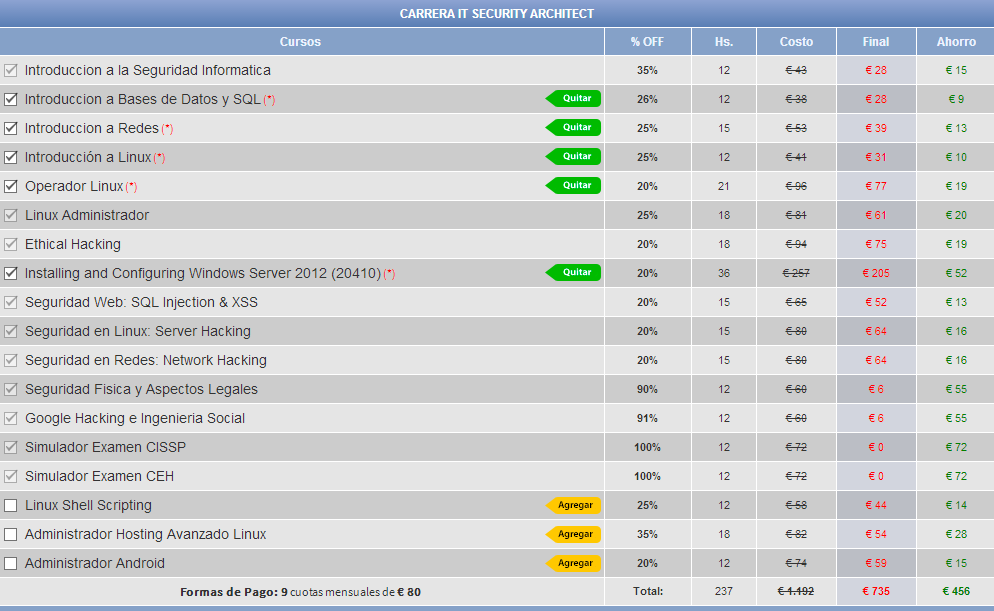
[**https://www.itmaster.com.ar/cursos/curso-seguridad-web**](https://www.itmaster.com.ar/cursos/curso-seguridad-web)

- En la plataforma Video2Brain: Fundamentos de la programación: Seguridad web se ofrece proporciona un periodo de prueba gratuito de 10 días donde podremos acceder a todos los cursos disponibles.

[**https://www.video2brain.com/es/cursos/fundamentos-de-la-programacion-seguridad-web**](https://www.video2brain.com/es/cursos/fundamentos-de-la-programacion-seguridad-web)

- El curso EducaciónIT: Curso de Seguridad Web: SQL Injection & XSS está dentro de una carrera de seguridad de IT, en la cual podemos hacer partes del curso por separado o hacer el curso completo en el cual como podemos ver en la imagen algunas de las partes del curso son opcionales (los que tienen indicadores verdes y amarillos). Todas las partes del curso completo tienen descuentos, en este caso nuestro curso tendría un descuento de 13€, pero para obtener este descuento tendríamos que inscribirnos en el curso completo y no solo en este apartado del curso.

El curso completo saldría por 355€ sin las partes opcionales, por lo que obtendríamos un descuento de casi el 50%.



[**http://www.educacionit.com/curso-de-seguridad-web**](http://www.educacionit.com/curso-de-seguridad-web)

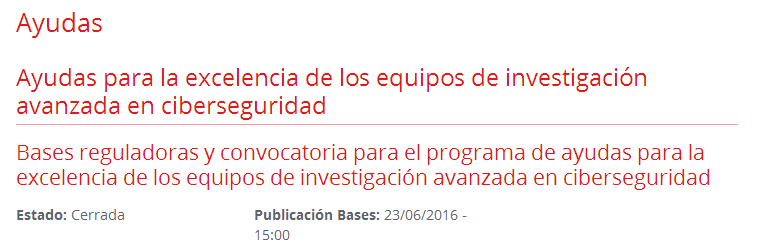
- La plataforma Redtech Aceademy: "Ethical hacking Nivel 1" tiene una promoción Promoción ex alumno en la que si ya has realizado algún curso en la plataforma vas a recibir un descuento de $500.00 sobre el curso que elijas, pero las promociones no son acumulables. (curso sobre Nestparker)

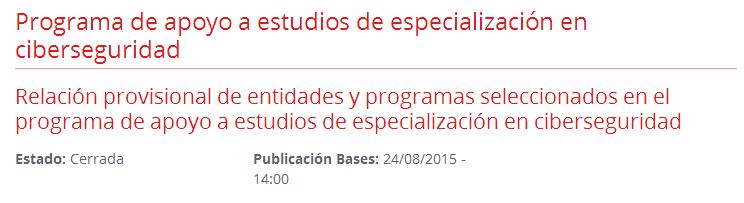
[**http://www.redtechhackingshop.com/product-page/preventa-curso-dvd-ethical-hacking-nivel-1**](http://www.redtechhackingshop.com/product-page/preventa-curso-dvd-ethical-hacking-nivel-1)

* Ayudas para investigación:

- La organización Incibe (Insituto nacional de ciberseguridad)proporciona ayudas para la excelencia de los equipos de investigación avanzada en ciberseguridad. El problema es que el plazo está cerrado y no podemos ver las subvenciones proporcionadas, pero probablemente el próximo año volverán a proporcionar esta ayuda. También proporcionan un programa de apoyo a estudios de especialización en ciberseguridad pero como en el caso anterior los plazos están cerrado. Por lo que podemos ver en la web, cada año suben ayudas sobre ciberseguridad.

[**https://www.incibe.es/ayudas**](https://www.incibe.es/ayudas)





* Becas para el estudio de un Master:

-El Master en Ciberseguridad desarrollado por Deloitte ofrece la posibilidad de optar a una beca con el 50% de descuento de dicho Master.



**http://www.imf-formacion.com/programas/masters-ciberseguridad?o=4325&sp=1&utm\_source=Google\_Adwords&pkw=Master%20En%20Seguridad%20Informatica&utm\_medium=cpc&utm\_campaign=14498-ADWORDS-CIBERSEGURIDAD&gclid=CJOjlOrg2tICFYM4Gwod4s0N3w**

-El Master Universitario en Ciberseguridad dirigido por el profesor Andrés Marín López en la Universidad Carlos III de Madrid, ofrece la posibilidad de optar a 4 ayudas o becas por un importe de 3.000 euros.



**https://www.uc3m.es/ss/Satellite/Postgrado/es/Detalle/Estudio\_C/1371209197821/1371219633369/Master\_Universitario\_en\_Ciberseguridad#becas**

# 7. Recursos para implementar las tecnologías

## 7.1 Recursos para implementar la tecnología Netsparker

### **7.1.1 Recursos gratuitos**

### **7.1.1.1**

[**https://www.netsparker.com/web-vulnerability-scanner/download/**](https://www.netsparker.com/web-vulnerability-scanner/download/)

Web oficial de Netsparker donde se explica su funcionamiento y cuáles son los beneficios de usar esta herramienta, además de ver cuáles son las vulnerabilidades que puede detectar. En esta web podemos conseguir la versión de prueba de la herramienta de Netsparker.

### **7.1.1.2**

[**https://www.telerik.com/download/fiddler**](https://www.telerik.com/download/fiddler)

Fiddler es una herramienta complementaria a Netsparker que realiza tareas de depuración web, pruebas de rendimiento, preubeas de seguridad, HTTP/HTTPS grabación Traffic… Netsparker actualmente puede importar datos de sesión de Fiddler y otras herramientas como Paros, Burp u otros proxies y herramientas populares. Esta herramienta es gratuita y la podemos obtener en el siguiente enlace.

### **7.1.1.3**

[**https://github.com/netsparker**](https://github.com/netsparker)

[**https://github.com/zkvL7/secutils**](https://github.com/zkvL7/secutils)

[**https://www.netsparker.com/blog/**](https://www.netsparker.com/blog/)

Hay una serie de entradas en github en las cuales encontramos funcionalidades que podemos añadir, ejemplos de vulnerabilidades sacadas del uso de la herramienta de Netsparker… Además la página oficial de Netsparker tiene un blog de seguridad donde trata temas de la herramienta y de seguridad.

**7.1.1.4**

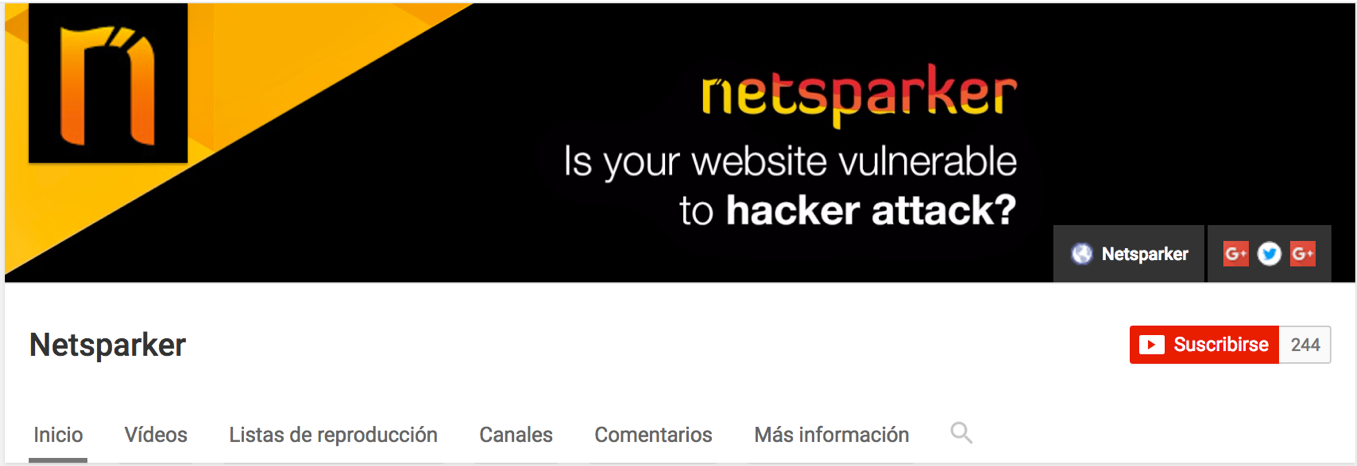
[**https://msdn.microsoft.com/es-es/library/bb386448(v=vs.100).aspx**](https://msdn.microsoft.com/es-es/library/bb386448(v=vs.100).aspx)

ViewState Visor es una herramienta que usa Netsparker y complementaria que consiste en un método que utiliza el marco de las páginas ASP.NET para conservar los valores de página y control. Cuando se representa el HTML de la página, el estado actual de la página y los valores que se deben conservar durante la devolución de datos se serializan en cadenas codificadas en base64. Esta información se coloca a continuación en el campo o campos ocultos del estado de vista.

**7.1.1.5 Youtube**

[**https://www.youtube.com/user/netsparker**](https://www.youtube.com/user/netsparker)

Este es el canal oficial de Netsparker donde podemos ver una gran cantidad de tutoriales sobre como usar dicha herramienta.



### **7.1.2 Recursos no gratuitos**

### **7.1.2.1**

[**https://www.netsparker.com/pricing/**](https://www.netsparker.com/pricing/)

En la web oficial de Netsparker, aparte de la versión de prueba que está disponible podemos optar por la versión de pago de la herramienta de escritorio en la que tenemos varios planes:

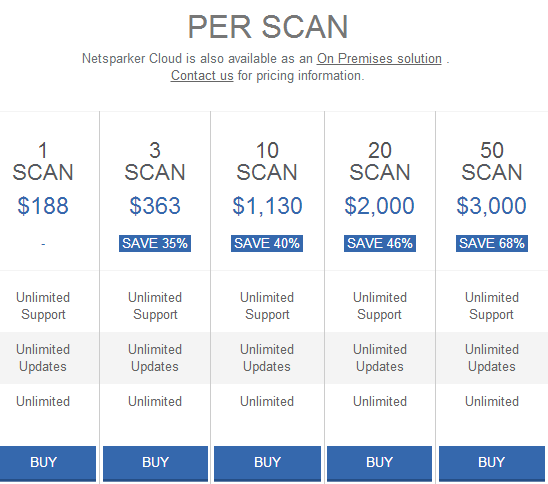


El uso de Netsparker Desktop está licenciado como parte de una suscripción anual que le proporciona actualizaciones regulares de firmas, actualizaciones de versiones y soporte de clase mundial durante el período de suscripción. Al final del período de suscripción, se le ofrecerá la oportunidad de renovar su suscripción, pero si decide no renovar, ya no podrá utilizar Netsparker.

### **7.1.2.2**

[**https://www.netsparker.com/pricing/**](https://www.netsparker.com/pricing/)

En la web oficial de Netsparker, aparte de todas las versiones que ya hemos visto, que serían la versión de prueba y la versión de escritorio que ya es de pago, también tenemos una herramienta para la nube. Estas son sus tarifas:



Para precios de volumen de más de 50 sitios web o escáneres, hay que contactar con Netsparker. La herramienta de Netsparker Cloud también está disponible como solución local.

### **7.1.2.3**

[**https://www.rapid7.com/products/metasploit/download/**](https://www.rapid7.com/products/metasploit/download/)

Netsparker ha sido diseñado para interactuar con productos para que pueda integrarse fácilmente en su ciclo de vida de desarrollo de software (SDLC). Las herramientas que actualmente interactúan con Netsparker incluyen la herramienta de Metasploit , que es un software de pruebas de penetración que ayuda a verificar las vulnerabilidades y gestionar las evaluaciones de seguridad. Es un software es de pago pero tiene una versión de prueba gratuita:

### **7.1.2.4**

[**https://www.threadfix.it/download/trial/**](https://www.threadfix.it/download/trial/)

ThreadFix es una de las herramientas que interactúa y actua como herramienta complementaria de Netsparker. Es una plataforma de resolución de vulnerabilidades líder en la industria que proporciona una ventana en el estado de los programas de seguridad de aplicaciones para las organizaciones que construyen software. Es una herramienta de pago pero tiene una versión gratuita de prueba de 30 días:

### **7.1.2.5**

[**https://www.kennasecurity.com/pricing/**](https://www.kennasecurity.com/pricing/)

Kenna Security: Vulnerability Management & Risk Intelligence es una herramienta complementaria a Netsparker. Entre las funcionalidades de esta herramienta se encuentran la priorización de las vulnerabilidades, medición e información sobre el riesgo, automatización del análisis de los datos de las vulnerabilidades recopiladas…. Esta herramienta es de pago pero también cuenta con una versión de prueba gratuita.

**7.1.2.6**

[**https://lunarline.com/vulnerability-scan-converter**](https://lunarline.com/vulnerability-scan-converter)

[**https://lunarline.dpdcart.com/**](https://lunarline.dpdcart.com/)

LunarLine Vulnerability Scan Converter VSC es otra herramienta complementaria a Netsparker que convierte instantáneamente archivos desde el escáner de vulnerabilidades en una hoja de Excel consolidada en un formato legible.

Después de procesar los datos, se compila la información de su vulnerabilidad en un solo libro de Excel. El usuario solo tendrá acceso a las hojas de cálculo con información sobre cada instancia de cada vulnerabilidad encontrada aunque también hay hojas de trabajo que proporcionan información adicional de vulnerabilidad, incluyendo el nivel de riesgo que plantea la vulnerabilidad, así como una lista de hosts donde se encontró una vulnerabilidad determinada. También se organizan los libros de hojas de cálculo en formatos comunes de evaluación, tales como NIST, DIACAP, e incluso FedRAMP.

Es una herramienta cuya licencia es de pago pero también tiene una versión gratuita de prueba. El precio de la licencia sería de 999$.

### **7.1.2.7**

La función Enviar a la acción en Netsparker Desktop le permite integrar el escáner de seguridad de aplicaciones web con su sistema de seguimiento de problemas o el sistema de administración de código fuente. Esta integración le permite importar vulnerabilidades identificadas como problemas con sólo unos pocos clics del ratón. Es posible integrar Netsparker con los siguientes sistemas:

* Jira: Es una herramienta de pago pero también dispone de un tiempo de prueba. [**https://es.atlassian.com/software/jira/try**](https://es.atlassian.com/software/jira/try)
* Github: Es una herramienta que tiene planes gratuitos y otros que son de pago. [**https://github.com/pricing**](https://github.com/pricing)

## 7.2 Recursos para implementar la tecnología Nmap

### **7.2.1 Recursos gratuitos**

**7.2.1.1**

[**https://github.com/nmap/nmap/tree/master/scripts**](https://github.com/nmap/nmap/tree/master/scripts)

[**https://github.com/cldrn/nmap-nse-scripts**](https://github.com/cldrn/nmap-nse-scripts)

Hay varias entradas en github en las cuales encontramos funcionalidades que podemos añadir, ejemplos de vulnerabilidades sacadas del uso de la herramienta de Nmap…

**7.2.1.2**

**https://nmap.org/download.html**

Aquí podemos encontrar las distintas posibilidades de descarga ya que Nmap se puede emplear en distintos sistemas operativos como son Linux, Windows, Mac OS X… También podemos encontrar el código fuente de distribución.

**7.2.1.3**

**https://nmap.org/book/nse-library.html**

Aquí podemos encontrar cuales son las librerías de Nmap.

**7.2.1.4 Youtube**

En esta plataforma podemos encontrar un montón de vídeos para ayudarnos a trabajar con Nmap como guías, ejemplos...



**7.2.1.5 Foros**

[**http://foro.elhacker.net/hacking\_basico/maneras\_interesantes\_de\_usar\_nmap-t314304.0.html**](http://foro.elhacker.net/hacking_basico/maneras_interesantes_de_usar_nmap-t314304.0.html)

[**http://www.forospyware.com/t508875.html**](http://www.forospyware.com/t508875.html)

**http://es.stackoverflow.com/questions/10382/localizar-un-servicio-a-traves-de-python-nmap**

También hemos encontrado estos foros dedicados a Nmap, en los que otra gente que ya ha empleado esta herramienta nos puede ayudar.

**7.2.1.6**

[**http://www.flu-project.com/2014/03/ejecutando-nmap-desde-python.html**](http://www.flu-project.com/2014/03/ejecutando-nmap-desde-python.html)

Aquí podemos encontrar una guía detallada para implementar Nmap con Phyton.

**7.2.1.7**

Nmap se desarrolla en entornos gratuitos basados en los sistemas operativos GNU/Linux, Solaris, BSD y Mac OS X.

Unix: **https://es.wikipedia.org/wiki/Unix**

### **7.2.2 Recursos no gratuitos**

**7.2.2.1**

[**https://lunarline.com/vulnerability-scan-converter**](https://lunarline.com/vulnerability-scan-converter)

LunarLine Vulnerability Scan Converter VSC es una herramienta complementaria a Nmap que convierte instantáneamente archivos desde el escáner de vulnerabilidades en una hoja de Excel consolidada en un formato legible.

Después de procesar los datos, se compila la información de su vulnerabilidad en un solo libro de Excel. El usuario solo tendrá acceso a las hojas de cálculo con información sobre cada instancia de cada vulnerabilidad encontrada aunque también hay hojas de trabajo que proporcionan información adicional de vulnerabilidad, incluyendo el nivel de riesgo que plantea la vulnerabilidad, así como una lista de hosts donde se encontró una vulnerabilidad determinada. También se organizan los libros de hojas de cálculo en formatos comunes de evaluación, tales como NIST, DIACAP, e incluso FedRAMP. También tendrá acceso a una hoja de cálculo que proporciona información sobre todos los puertos que escanea Nmap.

Es una herramienta cuya licencia es de pago pero también tiene una versión gratuita de prueba. El precio de la licencia sería de 999$.

**7.2.2.2**

Nmap también se desarrolla en entornos de pago basados en los sistemas operativos Microsoft Windows y AmigaOS, por lo que esta herramienta es multisistema.

Microsoft Windows: [**https://www.microsoft.com/es-es/windows/**](https://www.microsoft.com/es-es/windows/)

AmigaOS: [**http://www.amigaos.net/**](http://www.amigaos.net/)

# 8. Conclusiones

La seguridad es más importante cada día que pasa ya que cada vez el entorno está mas informatizado, y a todos nos gusta poder tener la confianza y seguridad de que ya no solo nuestra plataforma es segura, sino de que toda nuestra información de la red está a salvo. Existen una gran variedad de herramientas y esto nos da la posibilidad de elegir cual se adapta mejor a nuestras necesidades.

Cada vez aumenta más la comunidad de desarrolladores de seguridad debido a la gran importancia que tiene este tema y debido al avance tecnológico constante. Como se da una gran variedad de sistemas operativos los desarrolladores tienen muchas posibilidades a la hora de desarrollar su herramienta, pueden especificarse en uno o hacerla para varios sistemas operativos y una vez tomada esa decisión pueden elegir entre una gran variedad de características para implementar en su herramienta.

En relación al estudio realizado sobre las herramientas disponibles para medir la seguridad de plataformas web nos damos cuenta de que hay una tendencia clara a que las herramientas reduzcan su complejidad y a que cada vez sean más completas, es decir que sean para más de un sistema operativo y que tengan muchas opciones para mostrarnos la información lo más detallada posible.

Existe una gran variedad de cursos y recursos sobre estas herramientas, aunque algunos nos ha costado un poco encontrarlos. Vemos que Nmap al ser una herramienta gratuita tiene más recursos gratuitos y Netsparker al ser una herramienta de pago, sus recursos también son de pago.

Siempre podemos encontrar ayuda e información en foros y plataformas como Youtube ya que hay gente que ha trabajado con estas herramientas y amablemente ha decidido compartir su información sobre ellas.