

Máster en

Offensive Security



9
meses



Live
Streaming



Bolsa
De empleo

Descubre el Máster en Offensive Security

En un entorno digital cada vez más complejo y amenazado por ciberataques sofisticados, **la demanda de profesionales en seguridad ofensiva se ha disparado**. Las organizaciones necesitan expertos capaces de pensar como un atacante para anticiparse a sus movimientos, detectar vulnerabilidades antes de que sean explotadas y diseñar estrategias efectivas de defensa. Ya no basta con protegerse: es imprescindible identificar proactivamente los puntos débiles de los sistemas, redes y aplicaciones para minimizar riesgos y garantizar la continuidad del negocio.

El **Máster en Offensive Security de KSchool** tiene como objetivo principal formar profesionales altamente capacitados en **técnicas avanzadas de seguridad ofensiva**, preparados para detectar vulnerabilidades y fortalecer la protección de sistemas, redes y aplicaciones en entornos reales. A través de un enfoque práctico e intensivo, esta titulación permite dominar el pensamiento ofensivo para anticiparse a posibles ataques y proteger de forma proactiva a las organizaciones frente a amenazas cibernéticas.

Con acceso a laboratorios prácticos y liderado por expertos del sector como Alejandro Ramos (Telefónica Tech), el máster te brinda una sólida base técnica para en el caso que quieras dar un paso más para obtener las **certificaciones OSCP y CEH**, puedas desarrollar las habilidades prácticas necesarias para superar sus exigentes desafíos.

Además, el programa incorpora el uso de herramientas clave en el mercado, como Kali, Metasploit, Burp Suite y muchas más. Al finalizar, los estudiantes estarán capacitados para **evaluar infraestructuras TI, elaborar informes técnicos, y aplicar prácticas éticas y legales en ciberseguridad ofensiva**, obteniendo un título propio que avala sus competencias profesionales.

Descubre el Máster en Offensive Security

En KSchool, creemos que la especialización es la mejor carta en el mercado laboral y, para ello, hemos preparado este máster que se compone de diez módulos que te permitirán avanzar paso a paso, resolviendo retos y consolidando lo aprendido para mejorar continuamente y alcanzar el máximo nivel. ¡Aquí formamos a los mejores!

MÁSTER OFFENSIVE SECURITY

MÓDULO 1.
**Introducción al hacking. Explotación
en host y web hacking**

MÓDULO 2.
**Enumeración y
Obtención de información**

MÓDULO 3.
Sistemas y aplicaciones

MÓDULO 4.
Sistemas y aplicaciones II

MÓDULO 5.
Web

MÓDULO 6.
Redes

MÓDULO 7.
**Enterprise Hacking:
Active Directory**

MÓDULO 8.
Exploiting

MÓDULO 9.
IOT y Hardware

MÓDULO 10.
IA

Objetivos

Con el Máster en Offensive Security de KSchool serás capaz de:

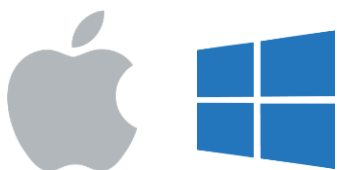
- 1.** Identificar y explotar vulnerabilidades en sistemas y redes usando técnicas avanzadas de seguridad ofensiva.
- 2.** Aplicar metodologías profesionales de pruebas de penetración siguiendo estándares internacionales.
- 3.** Evaluar críticamente la seguridad de infraestructuras TI, identificando debilidades y proponiendo soluciones.
- 4.** Utilizar herramientas y técnicas avanzadas de seguridad en entornos reales y controlados..
- 5.** Aplicar principios éticos y legales en la seguridad ofensiva, respetando las mejores prácticas de seguridad informática.
- 6.** Elaborar informes técnicos claros, documentando hallazgos y recomendaciones de manera estructurada.
- 7.** Obtener dos certificaciones clave en el mercado laboral: OSCP y CEH, ambas muy valoradas por empresas que buscan profesionales en ciberseguridad ofensiva

Material necesario

A lo largo de este Máster se trabajará con la máquina virtual VirtualBox.
Para ello necesitarás:

- Procesador Intel o AMD con soporte de 64 bits. Verifica que la tecnología de virtualización (Intel VT-x o AMD-V) esté habilitada en la BIOS.
- Memoria RAM mínima de 8 GB.
- Espacio en disco de al menos 120GB.
- Pantalla con una resolución de 800x600 píxeles o superior.

*Si estás utilizando un equipo MacOS, te recomendamos verificar si tu procesador admite la virtualización. Ten en cuenta que los modelos que contienen el chip M1 tienen algunas excepciones para instalar VirtualBox.



Perfil del alumno

Profesionales de tecnologías de la información, o telecomunicaciones, administradores de sistemas y redes, analistas de ciberseguridad, consultores de seguridad informática y estudiantes avanzados de ingeniería informática o carreras afines que deseen especializarse en seguridad ofensiva y pruebas de penetración.

Conocimientos técnicos previos requeridos:

- Sistemas operativos: manejo de entornos Linux y Windows a nivel de administración básica.
- Redes: comprensión de protocolos TCP/IP, modelos OSI y conceptos de redes locales.
- Programación: conocimientos básicos de scripting (preferentemente en Bash, Python o PowerShell).
- Seguridad informática: nociones básicas de ciberseguridad, tipos de vulnerabilidades y funcionamiento de firewalls y antivirus.

() Se facilitará material de apoyo previo al programa, en el caso de ser necesario.*

Salidas profesionales

Al finalizar el máster, estarás preparado para trabajar como:

- **Pentester.**
- **Consultor de ciberseguridad ofensiva**
- **Analista de vulnerabilidades**
- **Especialista en Red Team**
- **Auditor técnico de seguridad informática**
- **Asesor en evaluación de riesgos de sistemas y redes**

Modalidad Online con clases en directo

Lo mejor de nuestro presencial, ahora desde casa.

Nuestro método de estudio en el **Máster en Offensive Security** es flexible, personalizado y eficaz. Te permitirá asistir a las clases según tus posibilidades y compaginar tus estudios con tu vida personal y el trabajo. Será como estar en KSchool, pero desde la silla de tu escritorio allá donde estés.



**Clases en directo en
horario entre semana**



**¡Grabamos
todas las sesiones!**



Acceso al campus virtual para ver las clases y consultar material adicional, grabaciones y ejercicios.



Foros y contacto directo con el profesorado para poder resolver dudas.



Acceso vitalicio a la bolsa de empleo de KSchool.



Invitación a eventos exclusivos solo para alumnos.

Temario

Durante el máster tendrás clases en las que adquirirás conocimientos, realizarás proyectos en los que pondrás en práctica lo aprendido e irás avanzando con TFM

Contenido	
Módulos	Temario
Módulo 1. Introducción al hacking	• Máquinas Virtuales e Instalación de Kali Linux. • Metodologías de hacking y organización. • Escribiendo un informe
Módulo 2. Enumeración y obtención de información	• Recopilación de información pasiva • Recopilación de información activa • Ingeniería Social y Técnicas de phishing • Tutoría 1
Máster Class. 1	
Módulo 3. Sistemas y Aplicaciones	• Análisis de vulnerabilidades • Búsqueda y ejecución de exploits • Ataques de contraseñas • Ataques a servicios comunes • Metasploit framework • Meterpreter Mimikatz • Shells y payloads • Tutoría 2

Contenido

Módulos	Temario
Módulo 4. Sistemas y aplicaciones II	• Escalada de privilegios en Linux • Escalada de privilegios en Windows • Client-Side Attacks • Antivirus Evasion
Máster Class. 2	
Módulo 5. Web	• OWASP • Fuzzing y Crawling • Web Proxys - BurpSuite y ZAP • SQL Injections • Command Injection • Cross-Site Scripting (XSS) • File Inclusion (LFI/RFI) • APIs hacking • Hacking en CMS (Wordpress) • Tutoría 3
Módulo 6. Redes	• Análisis de Red • Man in the Middle • Auditoria a aplicaciones moviles • Ataques a Redes WiFi • Tutoría 4
Máster Class 3	

Contenido

Módulos	Temario
Módulo 7. Enterprise Hacking: Módulo 7. Active Directory	• Enumeración en Active Directory • Bloodhound • Volcado de credenciales en Active Directory • Password Spraying • Kerberoasting Pivoting • Tutoría 5
Módulo 8. Exploiting	• Credential Hunting - Linux y Windows • Buffer overflow Linux • Buffer overflow Windows • Backdoor en binarios • Command & Control (C2) • Borrado de evidencias • Tutoría 6
Módulo 9. OT y Hardware	• Introducción • BusPirate, Analizador Lógico, UART, JTAG • Implantes Físicos Keyboard
Módulo 10. IA	• Introducción • OWASP Top 10 IA • OWASP Machine Learning Security Top 10 • MCP Testing
Máster Class. 4	

TFM

10

Metodología y trabajo de evaluación

Al lo largo del Máster, los alumnos dispondrán de tutorías en las que, de manera individual y acompañados de un tutor, **realizarán laboratorios simulando entornos reales**. El tutor elegirá un enfoque para atacar este laboratorio y el alumno tras la práctica, deberá presentar un informe final con los resultados obtenidos y las conclusiones alcanzadas.

Estos ejercicios, que servirán para evaluar tus avances, se plantearán en **formato similar CTF ("Capture de Flag")** y, al contrario de lo que sucede en otras formaciones, estarán tutorizados. De este modo, podrás resolver las dudas que te surjan durante su realización.

Los CTF son juegos de competencia que ponen a prueba tus conocimientos y habilidades como hacker. Estos juegos consisten en diferentes modalidades de retos, en los que el objetivo es conseguir una «bandera», es decir, un código que confirma que has resuelto el desafío. Estos CTF están presentes en la mayoría de los eventos de ciberseguridad y también son usados como pruebas técnicas, en procesos de contratación de muchas empresas.

Por lo tanto, estos laboratorios te servirán de ejemplo para conocer a qué te enfrentarás en posibles ofertas de trabajo o si decides presentarte a competiciones CTF."

Herramientas

En el Máster de Offensive Security aprenderás a utilizar con soltura las herramientas más demandadas en las ofertas de empleo:



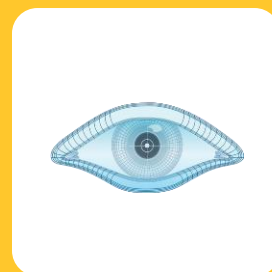
Kali



Wireshark



Docker



NMap



Burp Suite



Metasploit



Hashcat



John the
Ripper

¡Y muchas más!

Inscripción y precio

Ponemos a tu disposición las mejores alternativas para financiar el importe total de la formación. ¡Tú eliges!

Reserva tu plaza

```
graph TD; A[Reserva tu plaza] --> B[Pago único  
Descuento extra]; A --> C[Cómodas Cuotas*  
¿Necesitas más tiempo?  
Estudiaremos tu situación  
de forma personalizada  
para encontrar la solución  
más adecuada.];
```

Pago único
Descuento extra

**Cómodas
Cuotas***

¿Necesitas más tiempo?
Estudiaremos tu situación
de forma personalizada
para encontrar la solución
más adecuada.

*Consulta con nuestros asesores las diferentes opciones de financiación que tenemos

Bolsa de empleo

En KSchool contamos con una Bolsa de Empleo propia donde las mejores empresas buscan talento.

Nos enorgullece decir que el 96% de nuestros alumnos están trabajando y que muchos de ellos consiguieron su primer empleo en el sector digital o lograron cambiar su puesto gracias a la Bolsa de Empleo.

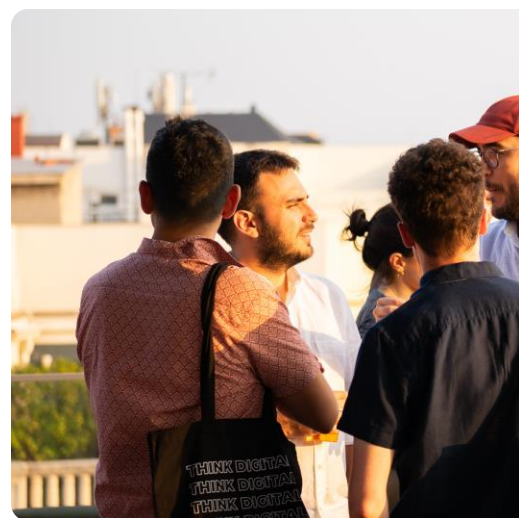
Pero, ¿cómo funciona esta Bolsa de Empleo?

- 
- **Tienes que ser alumno de KSchool**
 - **Revisa la plataforma para conocer las nuevas ofertas**
Además, solo recibirás las que vayan dirigidas a tu área de formación. ¡Todo bien filtrado para que solo te lleguen las ofertas de empleo que de verdad te interesan!
 - **Aplicas a la oferta y si todo va bien...**
 - **La empresa te contactará para que hagas una entrevista y puedas formar parte de su proceso de selección.**
 - **Este es el punto que más nos gusta:**
cuando os eligen para cubrir su vacante y nos escribís para contárnoslo :)
¡Es genial cada vez que un/a KSchoolero/a nos dice que tiene un nuevo trabajo gracias a la Bolsa de Empleo!

Eventos y Networking

Además de poder aprender mucho en clase, desde KSchool os invitamos a eventos, masterclass, talleres y conferencias que os servirán para ampliar vuestros conocimientos y para contactar con grandes profesionales.

Síguenos a través de las redes sociales para estar al tanto de estas acciones y revisa tu mail. ¡Algunos de nuestros eventos son exclusivos para alumnos!



Los números de KSchool

Nacimos en 2011 con una idea en la cabeza: formar a los nuevos perfiles profesionales que la red demanda de forma constante y hacerlo de la mejor forma posible. Por ello, nos definimos como “La escuela de los profesionales de Internet”.

La experiencia y los grandes profesionales con los que contamos como profesores nos avalan. Como siempre decimos, en ciertos sectores a día de hoy, el valor no lo aporta un título si no lo que el profesional sabe hacer.

Desde 2011

Formando perfiles

+6.000

Alumnos

+1.600

Empresas han buscado talento en nuestra bolsa de empleo

94%

Alumnos Trabajando

Preguntas frecuentes

Para resolver cualquier duda podéis escribirnos a admisiones@kschool.com o llamarnos al 91 910 09 54, pero a continuación recogemos algunas de las preguntas que más nos hacéis. ¡Esperamos que os sean de ayuda!

¿Qué pasa si no puedo acudir a una clase?

En la modalidad online las clases quedan grabadas, ¡así que podrás verla en cualquier otro momento!.

¿Para qué sirve el Campus Virtual?

Desde Campus Virtual podrás acceder a las clases en directo y volver a ver las grabaciones.

Encontrarás ejercicios y materiales complementarios para que puedas mejorar tus habilidades y conocimientos. Además, también tendrás acceso a las presentaciones que los profesores utilizarán en sus clases y podrás comunicarte con tus compañeros y profesores para resolver dudas a través de los foros.

¿Hay exámenes?

¡No! Durante las clases realizaréis ejercicios prácticos y la evaluación final que nos permitirá ver si habéis adquirido los conocimientos necesarios se realizará a través del Trabajo de Fin de Máster. En algunas de nuestras formaciones, también tendrás test y ejercicios evaluables en cada módulo.

¿Necesito un título universitario para cursar un máster en KSchool?

No, no necesitas ningún título previo. Existen formaciones donde sí es necesario contar con unos conocimientos básicos, pero no te preocupes por esto ya que antes de realizar la reserva te preguntaremos por tu preparación previa y si fuese necesario te solicitaríamos el CV. ¡Queremos que aproveches al máximo tu paso por KSchool!

Manifiesto KSchool

- Si el sistema no está preparado para darnos el conocimiento que necesitamos lo vamos a conseguir por nuestra cuenta.
- Hoy, en ciertos sectores el valor no lo aporta un título. Lo aporta lo que cada profesional sabe hacer.
- Si dependemos de nosotros mismos, vamos a pensar por nosotros mismos.
- No queremos, ni podemos sentarnos a esperar a que alguien se fije en nosotros.
- No hay ningún mapa. Debemos hacer nuestro camino, y es un camino que muchas veces no ha sido explorado, pavimentado, ni señalado.
- Nuestro conocimiento es la clave de nuestro desarrollo personal y profesional.
- Todo el mundo tiene algo que enseñar. Queremos aprender todos de todos.
- En el mundo del conocimiento, cuanto más se comparte más se tiene.
- Lo que aprendemos es lo que practicamos.
- Especializarse es ponerle un apellido a nuestra profesión. Es echarle especias a nuestro ingrediente principal.
- Queremos construirnos un futuro fuera del rebaño. Para eso vamos a pensar y hacer las cosas de forma diferente.
- No vamos a seguir instrucciones a ciegas, no vamos a ser pelotas, no vamos a mantener la cabeza agachada. Esas formas no van con nosotros.
- Vamos a estar siempre en movimiento. No vamos a parar de movernos. Somos inquietos, y nos gusta ser así.
- Como queremos resultados diferentes, vamos a hacer las cosas de forma diferente.
- Las pirámides son monumentos funerarios. Nos divierte verlas en los libros de historia, no sufrirlas en nuestro trabajo.
- Nuestro mercado no es el de los empleos. Es el de las oportunidades.
- Queremos colaborar con nuestras empresas a generar ingresos, no queremos tener un simple empleo.
- Queremos avanzar elaborando mejores recetas, no cocinando más.
- Queremos poner vida a los años, no solo años a la vida.
- Somos mucho más que un perfil y unas competencias. Somos algo más que las hojas de nuestro CV.
- Queremos levantarnos con ilusión los próximos 40 años. Queremos hacer las cosas con pasión, cariño y humanidad.

