Ciberseguridad

Bootcamp Online

GeeksHubs academy

Índice

Introducción

Actualmente no paramos de encontrarnos nuevas noticias sobre ciberataques a empresas, brechas de seguridad que filtran millones de datos de usuarios y que son publicados en Internet, un ransomware que secuestra los datos y pide un rescate en criptomonedas para recuperarlos (no siempre con un buen final) y aunque parezca mentira esto puede llegar incluso a destruir una PyME...

Los ataques a las empresas se han visto incrementados. Las empresas tienen cada vez mayor volumen de negocio en Internet, por lo que sus activos se encuentran más activos en la gran red de redes, y el perfil de experto en ciberseguridad es cada vez más demandado. En el bootcamp se aprenderá a disponer de una visión global y efectiva en la parte más ofensiva de la ciberseguridad, así como en la parte más defensiva. De esta forma se cierra un círculo en lo que a la protección de activos se refiere.

Y no solo hay ataques a empresas, las personas de a pie tampoco nos libramos de los ataques: ataques a las redes wifi de nuestros hogares, o el temido y conocido phising: recibimos un email de que nuestra cuenta de algún servicio está en riesgo y debemos cambiar la contraseña. Nos facilitan un enlace para cambiar la contraseña o incluso debemos introducir los datos de la tarjeta de crédito para deshabilitar algún servicio que supuestamente tenemos contratado, ¿quién no ha vivido esto alguna vez?

Todos estos riesgos y amenazas están presentes y ponen a prueba la concienciación que tenemos en la seguridad de las nuevas tecnologías. Nos damos cuenta de que la ciberseguridad cubre un papel muy importante tanto en las empresas y como en las personas. Cada día hay más profesionales formándose para cubrir la actual demanda de este sector que las empresas cada vez ven más necesario.

A lo largo de este bootcamp se tocan distintas disciplinas que entran dentro de la ciberseguridad: ataques de ingeniería social, a redes empresariales, a redes inalámbricas, ataques a aplicaciones web, forense digital... Varias temáticas que harán obtener una visión general del estado de la ciberseguridad actual y obtener perfiles orientados a técnico de ciberseguridad, analista de seguridad, pentester, analista forense... y por supuesto cómo protegerse ante los principales riesgos y amenazas que ponen en jaque a las empresas.

Adquiere nuevas habilidades y aprende

- **Criptografía**
- **Ciberinteligencia**
- **Auditoría de redes y sistemas**
- **Hardening de redes y servidores**
- **Hacking web y de sistemas**
- **Exploiting**
- **Ingenieria inversa**
- **Análisis forense**
- **SecDevOps**

y realiza ***prácticas en entorno real*** guiadas y tutorizadas por profesionales expertos.

A quién va dirigido

Profesionales con experiencia que quieran mejorar sus habilidades en esta área, especializarse en Ciberseguridad.

- **Empresas** que son conscientes de la necesidad de formar a empleados de su equipo IT en ciberseguridad, para evitar riesgos y ser proactivos en la defensa de sus sistemas.
- **Desarrolladores** que tengan claro que la ciberseguridad es un campo crítico de alto crecimiento que tiene y seguirá teniendo alta demanda de profesionales especializados.
- **Desarrolladores** que quieran dar un salto cualitativo en su carrera profesional.
- **Fuerzas y cuerpos de seguridad.**
- **Administradores** que quieren entender los riesgos a los que se exponen las infraestructuras y las redes.
- **Estudiantes** que quieren especializarse en un campo con una gran demanda y necesidades de profesionales.

Perfiles: Técnicos en Ciberseguridad | Analista de seguridad | Pentester | Administradores de seguridad | Analista forense | Auditores de seguridad

¿Qué vas a conseguir?

Realizando el **Bootcamp Ciberseguridad** adquirirás los conocimientos y competencias necesarios para desempeñar distintas tareas, tales como:

- Conocerás el mundo de la ciberseguridad y sus diferentes ramas de actuación.
- Aprenderás a realizar auditorías de seguridad y evaluar la seguridad de una organización.
- Conocerás las técnicas ofensivas que son empleadas por los profesionales del sector.
- Conocerás los secretos de la fortificación de redes y sistemas.
- Aprenderás a proteger entornos cloud y los mínimos requeridos en el mundo DevOps.
- Especialízate en un perfil cada vez más necesario y demandado.

Programa

BLOQUE 1. Ciberseguridad y Seguridad Informática

Aprenderás qué es y podrás diferenciar la seguridad de la información, la seguridad informática y la ciberseguridad. Además, conocerás los conceptos básicos y los principios de la auditoría como la recopilación de información a través de fuentes abiertas (OSINT) y el análisis de metadatos.

- *¿Qué es la Seguridad de la Información?*
- *¿Qué es la Seguridad Informática?*
- *¿Qué es la ciberseguridad?*
- *Recopilación de información y Footprinting*
- *Metadatos*
- *OSINT*

BLOQUE 2. Ciberinteligencia

En este módulo aprenderás las metodologías aplicadas a la ciberinteligencia y los sistemas que se utilizan. Se practicará con técnicas aplicadas a entornos reales con ejemplos y casos de uso prácticos. La rama de la ciberinteligencia es una de las más demandadas, así que no dudes en conocer cómo trabaja un analista en su día a día.

- *Introducción a la ciberinteligencia*
- *Metodologías aplicadas*
- *Sistemas de ciberinteligencia*
- *Técnicas aplicadas en un entorno real*
- *Ejemplos y casos*

BLOQUE 3. Auditoría y Hacking de Sistemas

Las auditorías de sistemas son un eje central en un proyecto de hacking ético. Además, las técnicas que se pueden conocer en este tipo de auditorías son utilizadas, a menudo, en los ejercicios ofensivos de Red Team. Aprenderás las técnicas más modernas para llevar a cabo este tipo de auditoría.

- *Introducción*
- *Recopilación de información*
- *Análisis de activos*
- *Detección de vulnerabilidades*
- *Explotación de vulnerabilidades*

Programa

- *Post-Explotación*
- *Metasploit*
- *Entrenamiento y ejercicios reales*
- *Hardware Hacking*

BLOQUE 4. Auditoría y Hacking Web

El mundo de las aplicaciones web ha evolucionado en gran medida durante las últimas décadas. Esto es debido a los avances de la tecnología. Los riesgos en el mundo web han ido evolucionando con la tecnología. Conoce de primera mano la evolución de las vulnerabilidades web y las nuevas técnicas de ataque.

- *Perspectiva y enfoque del atacante*
- *Reconocimiento y fingerprinting*
- *Descubrimiento de vulnerabilidades*
- *Explotación de vulnerabilidades*
- *Análisis de escáneres de vulnerabilidades web*
- *Entrenamiento en plataformas. Ejercicios y casos prácticos*

BLOQUE 5. Evaluación de la seguridad en la red

Las redes han sido y siguen siendo el eje central de toda organización. Ya sean redes locales, redes como Internet o el fascinante mundo del Cloud, la red está presente. Es importante conocer los riesgos y poder evaluar cuando una red está siendo amenazada o puede ser comprometida. Conoce el punto de vista de los ataques y la parte más ofensiva para, posteriormente, poder contrarrestarlos.

- *Introducción a la seguridad de redes*
- *Análisis de tráfico*
- *Análisis de tráfico en Capa 2 - Capa de enlace*
- *Manipulación de paquetes en IPv4*
- *Ataques en IPv6*
- *Ataques en Capa de Aplicación*
- *Casos reales y pruebas de auditoría en redes IPv4 e IPv6*

Programa

BLOQUE 6. Auditoría de redes inalámbricas

Las redes inalámbricas llevan con nosotros décadas, sin embargo, ¿Qué es de la seguridad de estos sistemas? En este módulo se analizan los riesgos que tienen las redes inalámbricas tanto personales como empresariales, así como distintas pruebas de evaluación de la red.

- *Introducción*
- *Conceptos básicos*
- *Tipos de redes inalámbricas*
- *Ataques a cifrados de redes particulares*
- *Ataques a cifrados de redes empresariales*
- *Ataques a clientes*
- *Generación de pruebas de auditoría Wireless*

BLOQUE 7. Hardening de redes empresariales

Diversos elementos podemos encontrar en una red corporativo con el objetivo de poder medir la seguridad de ésta y defenderla. Miles de elementos de logs son registrados y distribuidos. Muchas amenazas pueden comprometer tu red. Aprende a fortificar la red y configurar diferentes elementos de red con el objetivo de buscar la máxima seguridad.

- *Conceptos básicos de la fortificación de redes*
- *Direccionamiento*
- *Segmentación*
- *VPN*
- *Sistemas IDS*
- *Sistemas IPS*
- *Snort*

BLOQUE 8. Hardening de servidores

Los servidores almacenan mucha información importante para las empresas. Tener estos bien protegidos es una base fundamental de la seguridad. Mínimo privilegio posible, mínima exposición y defensa en profundidad son tres pilares clave de la fortificación de servidores. Durante el módulo se aprenderá a fortificar a fondo tanto servidores Windows como servidores GNU/Linux.

- *Conceptos*
- *Fortificación Sistemas Windows*
- *Fortificación Sistemas GNU/Linux*

Programa

BLOQUE 9. Criptografía aplicada a la Ciberseguridad

La criptografía es una de las bases del mundo de la ciberseguridad. La confidencialidad, la privacidad, la seguridad se apoyan en este hermoso y matemático campo. En esta ocasión, no te enseñaremos la criptografía clásica. Haremos que la criptografía se aplique al mundo de la empresa, que notes la importancia de este elemento en la ciberseguridad. La criptografía te protege, pero también sufre ataques. ¿Quieres verlo?

- *Métodos criptográficos*
- *Certificación y autenticación*
- *Firma Digital*
- *Cifrado correo electrónico*
- *Evolución del cifrado*
- *Ataques a la criptografía*

BLOQUE 10. Exploiting e Ingeniería Inversa

El exploiting y la ingeniería inversa son ramas de la ciberseguridad para los investigadores más avanzados. Conocer cómo trabaja un programa o proceso en su interior para intentar modificar su comportamiento no es algo trivial, pero sí apasionante.

- *Arquitectura de computadores (x86, x64)*
- *Introducción al lenguaje ensamblador*
- *Formatos binarios*
- *Análisis*
- *Shellcodes*
- *Herramientas*
- *Casos de exploiting*
- *Buffer Overflow*
- *SEH Overflow*
- *Protecciones: DEP, ASLR, Stack Cookies*
- *Bypass protecciones*

BLOQUE 11. Forense digital y respuesta ante incidentes

El análisis forense pretende dar respuestas a las preguntas que surgen en un incidente de seguridad. ¿Qué ha pasado? ¿Cómo ha ocurrido? ¿Quién lo ha hecho? Aprende cómo realizar un proceso de análisis forense en diferentes entornos y conoce cómo trabajan los profesionales que día a día se esfuerzan en poder dar respuestas a las organizaciones.

Programa

- *Introducción al Análisis Forense*
- *Adquisición y recopilación de evidencias*
- *Análisis de imágenes*
- *Tipos de Forense*
- *Incident Response*

BLOQUE 12. SecDevOps

SecDevOps o DevSecOps es la integración de los procesos DevOps y la Seguridad en el mismo flujo. ¿Cómo de madura es tu organización? Aprende a utilizar las bases de DevOps con Docker y cuáles son las principales herramientas de integración. Aprenderás a trabajar y fortificar contenedores Docker, así como las redes y la orquestación de estos. Un nuevo perfil a tu alcance.

- *Introducción a Docker*
- *DockerFile*
- *Imágenes*
- *Contenedores*
- *Redes*
- *Introducción a Kubernetes*
- *Seguridad en Docker*
- *SecDevOps*

Proyecto Final

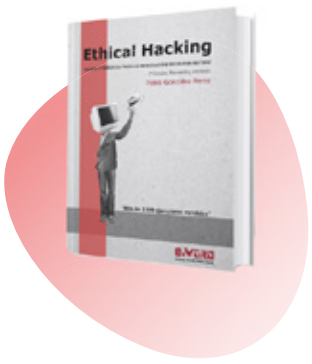
El Proyecto Final del Bootcamp tiene como objetivo confirmar que has interiorizado los conceptos tratados durante la formación. Por este motivo, el reto que te proponemos es un trabajo de temática libre, donde podrás demostrar tus habilidades en un escenario real: Máquinas virtuales preparadas para test de intrusión, vulnerabilidades web, escalada de privilegios... ¿Estás preparado para el reto?

+ Una sesión exclusiva Q&A con **Chema Alonso** para todos los participantes del Bootcamp

DATOS CLAVE

Duración	*12 semanas / 120 horas*
Modalidad	*100% Online con Masterclass en directo.*
Horario	*Viernes de 15:00 a 20:00 y sábado de 9:00 a 14:00.*
Profesores	*Cada módulo será impartido por un profesor experto en la materia.*

Ventajas exclusivas 0xWord y MyPublicInbox



Por ser alumno del Bootcamp recibe de forma gratuita en casa el libro Cómo protegerse de los peligros en Internet de 0xWord, la editorial de **Chema Alonso**.
Y además, **500 tempos** en MyPublicInbox para contactar con los mejores profesionales tech.

My Public Inbox ® 0xWORD

Equipo Docente

Profesionales en activo de primer nivel, con reconocida **experiencia docente** impartiendo conferencias, workshops y cursos de formación en escuelas de negocio, entidades y empresas

Director Bootcamp

Álvaro Núñez

Security Researcher en ElevenPaths

Pablo González

Technical Manager & Security Telefónica Digital España

Ángel Álvarez

MCT Microsoft Certified Trainer & Azure Solutions Architect Microsoft MVP Cloud y Datacenter Management

Marta Barrio

Application Security Architect en Beam Suntory

Jézer Ferreira

OSINT Instructor | Formador/Consultor de Ciberinteligencia y Ciberdefensa para FFCCSE

David Meléndez

I+D Software Embebido | DEFCON USA Speaker, BlackHat | Autor del libro "Hacking con Drones"

Carmen Torrano

Senior Researcher at Eleven Paths

Rafael Sánchez

Security Architect en BBVA

Fran Ramírez

Investigador de Seguridad Informática en Telefónica

Iván Portillo

Innovación sobre Inteligencia de Amenazas para el sector financiero

Jesús Alcalde

Responsable de Seguridad en DevOps en Zerolynx

Valentín Martín

Administrador de Sistemas en Indra

Daniel González

COO & Co-founder at Zerolynx

Hablan de nosotros

Empresas que confían en nosotros

GeeksHubs
academy _

formacion@geekshubs.com