vuela | Junta de Andalucía

Ethical Hacking Certified

Curso Blended | *Nivel Avanzado* | *40h* | *26/06 al 18/07* | *De 25 a 45 plazas*

¿QUÉ VAS A APRENDER?

Este curso de tiene como objetivo enseñar a los estudiantes técnicas avanzadas de hacking ético, con el fin de identificar y mitigar vulnerabilidades de seguridad en sistemas, redes, aplicaciones y dispositivos.

Es importante que los profesionales de seguridad de la información adquieran estas habilidades avanzadas en ethical hacking, ya que la industria necesita cada vez más expertos capaces de identificar, prevenir y mitigar ataques de hackers malintencionados. También es importante que los profesionales de seguridad de la información puedan poner en práctica estas técnicas en su organización, con el fin de garantizar la seguridad y protección de los datos confidenciales de la empresa.

Parte eLearning → 20 horas

OBJETIVOS:

Comprender los principios fundamentales de la seguridad de la información, identificar los diferentes tipos de ataques y técnicas comunes utilizadas en los mismos, conocer los estándares de seguridad aplicables, entender los diferentes tipos de hackers y las herramientas de hacking ético.

CONTENIDOS:

Módulo 1. Introducción a la seguridad de la información (4 horas)

1. Principios de seguridad.
2. Tipos de ataques.
3. Normativa y estándares de seguridad.
4. La Cyber Kill Chain.
5. Tipos de hackers y herramientas de hacking ético.

Actividad → El alumno deberá desarrollar un plan de ataque a una empresa ficticia donde describa detalladamente todas las fases de la CKC.

OBJETIVOS:

Conocer que el malware y las técnicas de hacking son una amenaza constante, mientras que las técnicas de hacking son los procedimientos o tácticas utilizadas por los atacantes para explotar vulnerabilidades en sistemas y redes. Conocer algunas las técnicas que emplea la Ingeniería Social.

CONTENIDOS:

Módulo 2. Malware y técnicas de hacking (4horas)

1. Tipos de malware.
2. Creación de malware y encriptación avanzada del payload.
3. Ataques offline y online al password.
4. Técnicas de Ingeniería Social.

Actividad → Creación de un malware indetectable

OBJETIVOS:

Conocer que la inspección de tráfico es una técnica utilizada con fines de seguridad. Comprender que en los ataques de MitM (Man-in-the-middle), el atacante intercepta y manipula la comunicación entre dos partes para obtener información o causar daño y que los ataques de denegación de servicio (DoS) atacan a la disponibilidad de la información.

CONTENIDOS:

Módulo 3. Inspección de tráfico, MitM con Kali y ataques de Denegación de Servicio (4 horas)

1. Inspección de tráfico con WireShark.
2. Man in the Middle.
3. Descubrir un ataque de denegación de servicio.
4. Ataque a la capa de sesión de la pila TCP/IP.

Actividad → Crear un documento donde se detallen las herramientas y pasos a realizar para hacer un ataque de sslstriping en una red local.

OBJETIVOS:

Conocer que las vulnerabilidades están presentes a nivel de sistema operativo, servidor o aplicación. Estudiar las debilidades más frecuentes encontradas en el desarrollo web y determinar los tipos de inyección más habituales hoy en día.

CONTENIDOS:

Módulo 4. Vulnerabilidades en sistemas y aplicaciones Web (4 horas)

1. Ataques a servidores de aplicación
2. OWASP y las debilidades en las aplicaciones.
3. Ataques a aplicaciones web

Actividad → Localizar en las bases de datos 3 vulnerabilidades con un CVSS mayor o igual a 9. Para cada uno de ellos, estudiar la vulnerabilidad y proponer una herramienta de ataque para explotarla.

OBJETIVOS:

Comprender los ataques a los que se enfrentan los protocolos inalámbricos comunes, y extender este conocimiento a redes bluetooth.

Entender las amenazas a las que se enfrenta la telefonía móvil.

CONTENIDOS:

Módulo 5. Ataques a redes inalámbricas y dispositivos móviles (4 horas)

1. Protocolos inalámbricos.
2. El protocolo Bluetooth y sus debilidades.
3. Ataques a teléfonos móviles.

Actividad → Determinar las herramientas más apropiadas para hacer una suplantación de un punto de acceso realizando una denegación de servicio al verdadero. Explicar cómo se realiza el ataque.

Sesiones online en directo → 20 horas

OBJETIVOS:

El principal objetivo de estas sesiones es que apliquen la parte elearning mediante ejercicios prácticos. Por ello, se usará la metodología flipped clasroom.

CONTENIDOS:

Sesión 1 Despliegue del laboratorio. Footprinting y reconocimiento. Escaneo de la red local y enumeración → 4 horas.
(Relacionado con el módulo 1)

- **Temática a tratar**: Despliegue del laboratorio para hacer las prácticas. Footprinting usando motores de búsqueda, servicios web, redes sociales, sitios web, Whois, DNS, Recon-ng, Maltego, OSRFramework, FOCA y osintFramework. Descubrimiento de hosts en la red local. Evasión de firewall/IDS. Enumeración NETBIOS, SNMP, LDAP, NFS, SMB/SAMBA.

Sesión 2 Evaluación de vulnerabilidades y hackeo.→ 4 horas.
(Relacionado con módulos 1, 3 y 4)

- **Temática a tratar:** Búsqueda de vulnerabilidades en CWE, CVE y NVD. Instalación de herramientas Open VAS, Nessus, LanGuard y Nikto.Usar Responder para robar hashes. Auditar credenciales con L0phtCrack. Elevación de privilegios en sesión de Meterpreter. Ocultar el rastro. ARP Spoofing para MitM. Denegación de servicios mediante Yersinia. Detección de ataques MitM. Ataques DoS.

Sesión 3 Ingeniería social y ataque a aplicaciones web (I) → 4 horas.
(Relacionado con módulos 2 y 4)

- **Temática a tratar:** Usar SET y SocialFish para ataques de Ingeniería Social. Despliegue de JuiceShop. Descubrir el score board. Ataques de inyección de SQL. Romper autenticación, Exposición de datos sensibles.

Sesión 4 Ataque a aplicaciones web (II) y exploit de vulnerabilidades → 4 horas.
(Relacionado con módulo 4)

- **Temática a tratar:** Validación de entrada de datos inapropiada. Romper la autenticación. CVE-2015-3306. CVE-22014-6271. Vulnerabilidad WebDAV. Escalado de privilegio no_root_squash.

Sesión 5 Técnicas avanzadas de hacking→ 4 horas. (Relacionado con módulos 1, 2, 3 y 4).

- **Temática a tratar:** Ofuscación de PowerShell. Exfiltrar información evadiendo el sistema DLP. Evasión del antivirus usando Shelter.

La impartición de esta acción formativa se realizará mediante la modalidad flipped classroom más online en directo de la siguiente forma:

- El **contenido interactivo** estará **disponible** en la **plataforma** online, de manera que será de **libre consulta** para el alumnado y este deberá haberse organizado de manera autónoma bajo las recomendaciones que se le marquen para haber consultado la lección o módulo correspondiente.
    - Con ello lo que se busca es un mayor protagonismo en el proceso de E-A y que el alumnado se involucre más en el mismo, mejorando su trabajo individual.
- Posteriormente, en la **sesión online**, se tratará el caso de uso de lo que ya el estudiante ha visto y leído, por lo que su participación y motivación será mucho más activa.
    - El objetivo de esto es fomentar un aprendizaje más profundo y significativo de manera que son ellos los que buscan construir sus conocimientos, a la par que esto permitirá mejorar el trabajo colectivo mediante los proyectos que compartan.

Valor añadido → Permite atender a la diversidad del aula

Los alumnos visionan los contenidos tantas veces como quieran y tienen las tutorías del profesor para resolver sus dudas de manera individualizada.

¿A QUIÉN ESTÁ DIRIGIDO?

- Profesionales del sector TIC en Andalucía.
- Perfiles TIC de empresas de Andalucía.

CRITERIOS DE SELECCIÓN

Para la selección del público participante de esta acción formativa, se tendrá en cuenta por estricto orden de llegada de la solicitud:

- Que tenga estudios universitarios o de Formación Superior relacionada con la materia a impartir, como ingeniería, informática, matemáticas, estadística, física o asimiladas.
- Que sea trabajador del sector TIC andaluz, o que tenga perfil TIC y que trabaje en una empresa andaluza de cualquier otro sector.

En caso de que no se llenen las plazas totales del curso (45) se dará paso a otro tipo de perfiles.

CONOCIMIENTOS MÍNIMOS REQUERIDOS POR PARTE DEL ALUMNADO:

- Acceso a Internet
- Conocer algún lenguaje de programación.
- Conocimientos de ciberseguridad a nivel básico/medio.

REQUISITOS PARA REALIZAR LA PARTE DE LAS CLASES EN DIRECTO DE MANERA ÓPTIMA

- El alumno deberá disponer de un equipo con VirtualBox instalado. con un mínimo de 16GB de RAM y 4 cores.
- Previo al inicio de la parte online en directo, que se descarguen las VMs.
- La configuración del laboratorio se hará el primer día del online en directo.

EQUIPO DOCENTE

Antonio Salazar Graván

Ingeniero Técnico Informático por la Universidad de Cádiz, MCT de Microsoft desde 2012.

Especialista en Ciberseguridad e infraestructuras con más de 20 años de experiencia en formación y consultoría

https://www.linkedin.com/in/antonio-salazar-gravan/

CALENDARIO:

- **Fecha inicio del curso:**
  16/10/2023
- **Fecha impartición sesiones online en directo:**
- 23 al 27 de octubre en horario de 9 a 13 horas.
- **Fecha fin del curso:**
  22/11/2023

EVALUACIÓN:

Obligatorio para obtener el certificado:

- **[20%] La asistencia a las clases** o su visionado posterior. Estos vídeos se subirán a la plataforma y se establecerán los mecanismos para verificar que el alumnado que no asistió sí que visualizó el vídeo de manera asíncrona.
  - El mínimo de vídeos o asistencia a las clases para la titulación es de 4.
- **[30%] Visualización de contenido formativo.** Por medio de la lectura del SCORM.
  - Deberán ver al menos el 75% del contenido o lo que equivale a 4 módulos.
- **[30%] Realización de pruebas de conocimientos.** Que se colgarán mediante una batería de preguntas en la plataforma con orden aleatorio.
  - Deberán sacar un mínimo de un 5 al menos en 4 de los 5 módulos.

No es obligatorio, pero sí muy recomendable:

- **[20%] Actividades.** Serán de carácter no evaluable, pero servirá de preparación para las sesiones online en directo y además se ofrecerá retroalimentación.

CERTIFICADO

Una vez superadas todas las evaluaciones de los módulos del curso y habiendo asistido al número mínimo de clases exigido, podrás obtener la certificación.

El certificado se emitirá digitalmente en formato pdf incluyendo la siguiente información:

- Datos del alumno.
- Datos del curso: título, fecha de impartición, duración, contenidos impartidos.
- Sello y firma digitalizada de la empresa impartidora del curso. El certificado no lleva firma digital ni sello/firma de la Junta de Andalucía

Ten en cuenta que estos cursos no tienen validez académica ni acreditación de créditos universitarios.

OTRAS CUESTIONES DE INTERÉS DE ESTA ACCIÓN FORMATIVA:

Una posible orientación al tiempo dedicado al estudio, lectura y visualización del contenido sería la siguiente:

- Tiempo de consulta de contenidos y vídeos: 15 horas.
- Tiempo de realización de actividades: 1,5 horas.
- Tiempo de realización de exámenes: 2 horas.
- Tiempo de consulta en foros e interacción con los compañeros: 1,5 horas.
- Asistencia a las sesiones online en directo: 20 horas.

De todas formas y al tratarse de un curso abierto y parcialmente en línea, cada alumno podrá seguir su propio ritmo de aprendizaje siempre y cuando cumpla con los criterios mínimos de evaluación para la obtención del certificado de formación.