FORMACIÓN E-LEARNING

Curso Online de

Ciberseguridad y Hacking ético para empresas

Implementación práctica de medidas de seguridad basadas en auditorías éticas.

CURSO BONIFICABLE

Iniciativas Empresariales
estrategias de formación

MANAGER BUSINESS SCHOOL

Tel. 900 670 400 - attcliente@iniciativasempresariales.com
www.iniciativasempresariales.com

BARCELONA - BILBAO - MADRID - SEVILLA - VALENCIA - ZARAGOZA

Ciberseguridad y Hacking ético para empresas

Presentación

En el mundo actual, la ciberseguridad es una prioridad para todas las empresas. El hacking ético es una disciplina crucial que permite detectar y corregir vulnerabilidades en los sistemas informáticos. Este curso le ofrece una formación integral que abarca desde la comprensión del perfil del hacker hasta la implementación de medidas de seguridad avanzadas, pasando por la evaluación de vulnerabilidades y la utilización de herramientas especializadas.

Le proporcionará, además, las herramientas, conocimientos y metodologías necesarias para proteger sus sistemas informáticos y asegurar la operatividad de sus organizaciones frente a posibles ciberataques.

La Formación E-learning

Los cursos online se han consolidado como un método educativo de éxito en la empresa ya que aportan flexibilidad al proceso de aprendizaje, permitiendo al alumno escoger los momentos más adecuados para su formación. Con más de 35 años de experiencia en la formación de directivos y profesionales, Iniciativas Empresariales y la Manager Business School presentan sus cursos e-learning. Diseñados por profesionales en activo, expertos en las materias impartidas, son cursos de corta duración y eminentemente prácticos, orientados a ofrecer herramientas de análisis y ejecución de aplicación inmediata en el puesto de trabajo.

Nuestros cursos e-learning dan respuesta a las necesidades formativas de la empresa permitiendo:

1. La posibilidad de *escoger* el momento y lugar más adecuado para su formación.
2. *Interactuar* con otros estudiantes enriqueciendo la diversidad de visiones y opiniones y su aplicación en situaciones reales.
3. *Aumentar sus capacidades* y competencias en el puesto de trabajo en base al estudio de los casos reales planteados en el curso.
4. *Trabajar* con los recursos que ofrece el entorno on-line.

Tel. 900 670 400 - attcliente@iniciativasempresariales.com - www.iniciativasempresariales.com

Ciberseguridad y Hacking ético para empresas

Objetivos del curso:

- Aplicar una metodología ágil en la organización para la identificación de intrusiones y amenazas en la red a través de herramientas específicas, conociendo las peculiaridades de los distintos tipos de ciberataques y las técnicas empleadas.
- Conocer de manera introductoria el mundo hacker, comparando el retrato del ciberdelincuente tradicional con otras imágenes reales del hacker asociadas al campo de la ciberseguridad.
- Conocer las mecánicas y metodologías del sistema CVSS (Common Vulnerability Scoring System) y cómo podemos usarlo para evaluar y puntuar vulnerabilidades.
- Profundizar en el concepto ciberataque, conociendo cómo es el ciclo de vida de un ataque cibernético junto con un importante método de análisis de intrusión que es empleado por los hackers éticos con idea de entender las acciones del atacante y poder combatirlo mediante una sólida defensa.
- Abordar el concepto malware como herramienta clave de los ciberataques, conociendo los distintos tipos de programas maliciosos, sus funciones y cómo afectan a la seguridad de los sistemas de la empresa.
- Diseñar arquitecturas de red seguras, escalables y sostenibles, destacando la necesidad de contar con sistemas de controles independientes y suficientes para garantizar la operatividad de las organizaciones y su buen funcionamiento.
- Adquirir conocimientos sobre fallos de seguridad en dispositivos de red para explotar las vulnerabilidades encontradas, conociendo las particularidades de los protocolos de seguridad para redes WiFi.
- Crear un entorno de entrenamiento o laboratorio de Pentesting virtual utilizando la aplicación VirtualBox.
- Comprometer las redes Wireless rompiendo la seguridad aprovechando las vulnerabilidades en los protocolos WEP, WPA/WPA2 y WPS.
- Asegurar el ejercicio correcto de la profesión de hacker ético conociendo, tanto los límites marcados por el Código Penal como la manera de definir un plan de trabajo de calidad apoyándose en referencias normativas de la familia de estándares ISO 27000.

Dirigido a:

Todas aquellas personas que ocupan cargos y responsabilidades de gestión en los diferentes departamentos de la empresa y puedan ser objeto de ataques informáticos, así como a cualquier persona interesada en conocer en profundidad y de manera práctica los conceptos de ciberseguridad y hacking ético aplicados a la empresa.

Tel. 900 670 400 - attcliente@iniciativasempresariales.com - www.iniciativasempresariales.com

Ciberseguridad y Hacking ético para empresas

Estructura y Contenido del curso

El curso tiene una duración de 80 horas lectivas 100% online que se realizan a través de la plataforma e-learning de Iniciativas Empresariales que permite el acceso de forma rápida y fácil a todo el contenido:

Manual de Estudio
13 módulos de formación que contienen el temario que forma parte del curso y que ha sido elaborado por profesionales en activo expertos en la materia.

Material Complementario
En cada uno de los módulos que le ayudará en la comprensión de los temas tratados.

Ejercicios de aprendizaje y pruebas de autoevaluación
para la comprobación práctica de los conocimientos adquiridos.

Bibliografía y enlaces de lectura
recomendados para completar la formación.

Metodología 100% E-learning

Aula Virtual *
Permite el acceso a los contenidos del curso desde cualquier dispositivo las 24 horas del día los 7 días de la semana.
En todos nuestros cursos es el alumno quien marca su ritmo de trabajo y estudio en función de sus necesidades y tiempo disponible.

Soporte Docente Personalizado
El alumno tendrá acceso a nuestro equipo docente que le dará soporte a lo largo de todo el curso resolviendo todas las dudas, tanto a nivel de contenidos como cuestiones técnicas y de seguimiento que se le puedan plantear.

* El alumno podrá descargarse la APP Moodle Mobile (disponible gratuitamente en Google Play para Android y la Apple Store para iOS) que le permitirá acceder a la plataforma desde cualquier dispositivo móvil y realizar el curso desde cualquier lugar y en cualquier momento.

Tel. 900 670 400 - attcliente@iniciativasempresariales.com - www.iniciativasempresariales.com

Ciberseguridad y Hacking ético para empresas

Contenido del Curso

MÓDULO 1. Planeta hacker

5 horas

Son muchas las actividades que están orientadas a comprometer la seguridad informática, la seguridad de las redes y la de los dispositivos inteligentes. Estas actividades o *hackeos* son artimañas técnicas que cuentan también con grandes componentes psicológicos, que hacen del *hacker* un ser realmente atractivo y poderoso. Sin embargo, y en términos generales, suele concebirse al *hacker* como un delincuente cibernético capaz de ejercitar tácticas maliciosas.
Este punto, que da inicio a la temática de ciberseguridad, es un buen momento para recordar que la intención de esta formación es prepararle para dominar y gestionar las funciones, herramientas, procesos y regulación que dominan las actuaciones del *hacker* ético.

1.1. Hackers:
1.1.1. Clasificaciones de hackers.
1.1.2. Comunidad hacker.
1.1.3. Gurús hackers.
1.1.4. Comunidad Anonymous.
1.1.5. Mujeres hackers.

1.2. El fenómeno hacker.

1.3. Manifiesto hacker ético:
1.3.1. Actitudes del hacker ético.
1.3.2. Valores del hacker ético.
1.3.3. Emblema hacker.

MÓDULO 2. Auditorías de hacking ético o pentesting

5 horas

Cada vez es más frecuente ver como empresas de distintos tamaños optan por buscar perfiles profesionales capaces de proteger el núcleo operativo del negocio. En la mayoría de los casos, este complejo centro neurálgico cuenta con elementos tan básicos como la red, ordenadores, programas informáticos, *routers*, dispositivos móviles, etc.
Sin estos recursos informáticos ni las conexiones a Internet, difícilmente podrían desempeñarse actividades empresariales, es más, a medida que una empresa va creciendo, cada vez es más necesario implementar un mayor número de instrumentos tecnológicos y adoptar nuevas tecnologías que hacen que la seguridad de los sistemas informáticos y la seguridad de la información y la comunicación sea aún más compleja de gestionar.

2.1. Pentesting:

Tel. 900 670 400 - attcliente@iniciativasempresariales.com - www.iniciativasempresariales.com

2.1.1. Tipos de Pentesting.
2.1.2. Fases del Pentesting.

2.2. Beneficios de las auditorías de hacking ético:
2.2.1. Ámbito de actuación de las auditorías de ciberseguridad.

2.3. Principios de protección de la seguridad de la información.

2.4. Amenazas clave para la gestión de la seguridad de la información de una organización:
2.4.1. Clasificación de la información.
2.4.2. Fuentes de amenazas.
2.4.3. Principales amenazas para la gestión de la seguridad informática en la empresa.
2.4.4. El riesgo.
2.4.5. Medición de los riesgos de los activos de información.

2.5. Pentesting y gestión de riesgos.

2.6. Common Vulnerabilities and Exposures (CVE).

MÓDULO 3. Análisis de vulnerabilidades

8 horas

Una de las cuestiones donde la ciberseguridad pone más el foco de atención es en el estudio y la gestión de vulnerabilidades. La idea es saber valorar la peligrosidad de los agujeros de seguridad a los que se someten empresas, profesionales y organizaciones, sabiendo determinar la gravedad que implica cada vulnerabilidad encontrada. Todo ello facilita la toma de decisiones estratégicas para abordar los problemas con mayor eficacia.

3.1. Registro y clasificación de las vulnerabilidades:
3.1.1. Registro de nuevas vulnerabilidades en Common Vulnerabilities and Exposures (CVE).
3.1.2. Common Vulnerability Scoring System (CVSS): grupo de métricas CVSS.
3.1.3. Versiones CVSS.
3.1.4. Proceso de evaluación de vulnerabilidades con CVSS.

3.2. Herramientas para calcular el valor CVSS:
3.2.1. Puntaje de los grupos de métricas CVSS.
3.2.2. Vulnerabilidad con valores de métricas base distintas.

MÓDULO 4. Ciberataques

5 horas

El incremento durante los últimos tiempos de los ataques informáticos y del nivel de sofisticación y peligrosidad de los ciberataques, hacen que la ciberseguridad cobre un papel importante en la ciberresiliencia de los usuarios, organizaciones, empresas, instituciones y gobiernos. Cualquier tipo de actividad, ya sea de carácter económico, social, cultural, político, etc., y que forme parte del dinamismo de los diferentes sectores de una sociedad, puede verse afectada por la labor de cibercriminales.

4.1. ¿Qué es un ataque cibernético?:
4.1.1. Clasificación de ataques cibernéticos.
4.1.2. Ciclo de vida de un ciberataque.

4.2. La cadena asesina Cyber Kill Chain:
4.2.1. Fundamentos del modelo de intrusión Cyber Kill Chain.
4.2.2. Aplicación de la cadena de exterminio en entornos móviles.
4.2.3. Análisis de intrusión de ataques cibernéticos en la industria 4.0.

MÓDULO 5. Malware

5 horas

Los cibercriminales se valen cada vez más de la sofisticación de los virus informáticos para llevar a cabo sus ciberataques. Además, crece la complejidad para abordar esta problemática no solo por la variedad de dispositivos electrónicos conectados a Internet, sino por la ausencia o falta de conciencia en temas de ciberseguridad. Con idea de que cualquier usuario u organización pueda contar con sólidos sistemas de protección, es necesario profundizar y distinguir entre una gran variedad de softwares y sus intenciones maliciosas. Todos ellos pueden acarrear un daño inmenso valiéndose de cualquier dispositivo conectado con independencia del tamaño. El daño por el impacto de un malware puede ser irreparable o con un coste de reparación incalculable.

5.1. Definición de malware.

5.2. Tipos de malware:
5.2.1. Virus.
5.2.2. Troyanos.
5.2.3. Gusanos.
5.2.4. Spyware.
5.2.5. Adware.
5.2.6. Trojan-clickers.
5.2.7. Ransomware.
5.2.8. RAT.
5.2.9. Exploits.

5.2.10. Cryptojacking.
5.2.11. Botnets.
5.2.12. Apps maliciosas.

5.3. Características del malware.

5.4. Procedimiento de inyección de un malware.

MÓDULO 6. Arquitectura de redes

8 horas

En la actualidad la mayoría de las organizaciones enfocan su actividad futura con una perspectiva de estandarización de infraestructuras basadas en la nube. Esto permite una mayor escalabilidad, sencillas conexiones y un importante ahorro de costes a la hora de gestionar herramientas y recursos. No obstante, muchas empresas ya disponen de una red propia alojada en un centro de datos o *Data Center*, con soluciones dirigidas a mejorar la manera tradicional de instalar soluciones *software* en local, evitando así cierta responsabilidad a nivel de seguridad, disponibilidad y gestión de estos recursos que dependerían de otro modo de la existencia física de un departamento específico de sistemas.
Por ello, por el incremento del trabajo remoto y con idea de mejorar la conectividad y la seguridad de las comunicaciones, muchas empresas necesitan crear nuevas infraestructuras de redes y entornos de trabajo a distancia, a la misma vez que aprovechan infraestructuras en locales ya existentes.

6.1. Network.

6.2. Arquitectura de redes:
6.2.1. Características de la arquitectura de redes.
6.2.2. Arquitectura de red por capas o niveles.
6.2.3. Componentes de una arquitectura de red.

6.3. Protocolos de comunicación:
6.3.1. Protocolos SNA (Systems Network Architecture).
6.3.2. Protocolos NetWare.
6.3.3. Protocolos AppleTalk.
6.3.4. Protocolos NetBEUI (NetBIOS Extended User Interface).
6.3.5. Protocolos TCP/IP (Transmission Control Protocol/Internet Protocol).

6.4. Estándares de Internet.

6.5. Vulnerabilidades en las redes de nueva generación:
6.5.1 Arquitectura de redes inalámbricas 5G.

Ciberseguridad y Hacking ético para empresas

MÓDULO 7. Routers y puertas

5 horas

7.1. ¿Son seguras las redes inalámbricas?
7.1.1. Routers y puertas.
7.1.2 Puertos del router.

7.2. Auditorías WIFI:
7.2.1 Software de hacking ético para auditar redes Wireless.

7.3. Protocolos de seguridad WIFI:
7.3.1. Seguridad WEP.
7.3.2. Seguridad WPA/WPA2.
7.3.3. Seguridad WPS.
7.3.4. Seguridad WPA3.
7.3.5. Seguridad WPA6.

MÓDULO 8. Laboratorio de entrenamiento del hacker ético

5 horas

8.1. Plataformas para entrenar:
8.1.1. Tipos de máquinas virtuales.
8.1.2. Funcionamiento y uso de las máquinas virtuales.

8.2. Instalación de VirtualBox.

8.3. Creación de máquinas virtuales.

MÓDULO 9. Password cracking

8 horas

Aunque es bien sabido que facilitar la conexión inalámbrica proporciona innumerables beneficios a los usuarios, ello también implica una mayor accesibilidad por parte de los ciberdelincuentes. Debido a la toma de conciencia sobre los riesgos que implican las redes wifi abiertas, se han ido desaconsejando y los especialistas han proporcionado protocolos de seguridad con mayores garantías a las redes inalámbricas cerradas.

9.1. Ciberataques a redes Wireless:
9.1.1. Técnica para burlar la ocultación del SSID de la red.
9.1.2. Técnica para burlar el filtro de direcciones MAC.
9.1.3. Técnicas para burlar los DHCP inhabilitados.

Tel. 900 670 400 - attcliente@iniciativasempresariales.com - www.iniciativasempresariales.com

9.2. Hackeo WPA/WPA2.

9.3. Hackeo WEP.

9.4. Hackeo WPS:
9.4.1. Romper redes inalámbricas WPA y WPA2 con WPS mediante ataque de fuerza bruta.
9.4.2. Romper redes inalámbricas WPA y WPA2 con WPS mediante ataque PixieDust.

9.5. Medidas de protección de las redes inalámbricas:
9.5.1. Vigilar la configuración básica de la seguridad de las redes inalámbricas.
9.5.2. Implementar servidores de identificación.
9.5.3. Proteger los puntos de acceso.
9.5.4. Actualizar software y firmware.
9.5.5. Reducir la potencia de la antena wifi.
9.5.6. Gestionar con eficacia las redes de invitados.
9.5.7. Incorporar elementos de alerta de intrusos en la infraestructura de red.

MÓDULO 10. Método de investigación y recolección de datos

5 horas

10.1. Tráfico en red: técnica de captura pasiva
10.1.1. Ciberataques activos.
10.1.2. Ciberataques pasivos.
10.1.3. Herramienta de captura pasiva.
10.1.4. Medidas de protección.

10.2. Ciberataques específicos a redes LAN:
10.2.1. Spoofing.
10.2.2. Man in the Middle Attack (MitM).
10.2.3. Otros tipos de ciberataques a redes locales.

10.3. Método de investigación y recolección de datos.

MÓDULO 11. Infraestructuras de la tecnología y vulnerabilidades de los sistemas

8 horas

11.1. La infraestructura de la tecnología:
11.1.1. Gestión de la infraestructura de la tecnología de la información.
11.1.2. Infraestructuras hiperconvergentes.

11.2. Infraestructuras Linux y Windows:
11.2.1. Infraestructura Linux.
11.2.2. Infraestructura Windows.

11.3. Crackeando sistemas:
11.3.1. Ataques sobre credenciales.
11.3.2. La función hash y hasheo de contraseñas.
11.3.3. Herramientas para comprometer credenciales.
11.3.4. Fórmulas para proteger las credenciales en sistemas operativos Linux y Windows.

11.4 Exploits:
11.4.1. Herramienta de auditoría para crear y ejecutar exploits.
11.4.2. Ejemplo de ataque con Metasploit.

MÓDULO 12. Disciplinas de la ciberseguridad y el aprendizaje de hacking ético con CTF

5 horas

12.1 Disciplinas de ciberseguridad:
12.1.1. Autenticación criptográfica.
12.1.2. Generación de claves.
12.1.3 Principios fundamentales de la criptografía.
12.1.4. Métodos criptográficos.

12.2. Aprendiendo hacking con CTF:
12.2.1. Categorías de los CTF.
12.2.2. Las reglas de las cibercompeticiones CTF.
12.2.3. Plataformas CTF.
12.2.4. ¿Dónde practicar hacking de forma individual?

MÓDULO 13. Marco legal del hacking

8 horas

13.1. Marco legal del hacking:
13.1.1. Ley del hacking.

13.2. Familia de Normas ISO 27000:
13.2.1. Norma ISO 27000.
13.2.2. Norma ISO 27001.
13.2.3. Norma ISO 27002.
13.2.4. Norma ISO 27003.

Ciberseguridad y Hacking ético para empresas

13.2.5. Norma ISO 27004.
13.2.6. Norma ISO 27005.
13.2.7. Norma ISO 27007.
13.2.8. Norma ISO 27008.
13.2.9. Norma ISO 27013.
13.2.10. Norma ISO 27014.
13.2.11. Norma ISO 27021.

Ciberseguridad y Hacking ético para empresas

Tutor

Xavier Navarro
Ingeniero Superior en Informática por la Universidad de Barcelona, cuenta con amplia experiencia en temas de ciberseguridad y modelos de negocio 2.0. Es, además, consultor y formador en proyectos informáticos.

Titulación

Una vez finalizado el curso el alumno recibirá el diploma que acreditará el haber superado de forma satisfactoria todas las pruebas propuestas en el mismo.