micro credenciales UPO
nuevos cursos de desarrollo profesional avanzado

Cyber Security Foundations

Modalidad	Fechas de impartición	ECTS/Horas de docencia	Precio
Virtual/Online	Del 19/02/2024 al 21/03/2024	7 ECTS 52 horas de docencia	650€

* El coste del certificado-diploma de aprovechamiento es de 10,00 € (en concepto de gestión de expediente y emisión)

Dirección académica:
Francisco Martínez Álvarez. Catedrático de la Universidad Pablo de Olavide.

Coordinación:
The Bridge Schools.

1. Objetivos del curso

Las empresas, en mayor o menor medida, están inmersas en procesos de transformación digital. Por ello nuestras redes y sistemas son más vulnerables y se encuentran menos protegidos; incluso hay quien afirma que “todo es hackeable”. Por ello la importancia del conocimiento en Ciberseguridad para cualquier perfil tecnológico.

Este programa intensivo tiene como objetivo formar a cualquier persona que quiera especializarse en seguridad informática.

Aprende a gestionar la seguridad de una empresa utilizando las herramientas y técnicas más actuales del mercado.

2. Resultados de aprendizaje

Una vez haya finalizado esta microcredencial relacionada con el sector de la ciberseguridad, los alumnos que la hayan estudiado podrán trabajar como técnico o analista de ciberseguridad; Pentester o hacker ético; consultor compliance de seguridad; consultor de seguridad de aplicaciones móviles; analista forense y muchos más puestos relacionados con la ciberseguridad.

3. Descripción y planificación de contenidos

Esta acción formativa cuenta con la siguiente metodología:

Módulo 1 - Fundamentos de HW y Sistemas Operativo

Objetivo

Este módulo introduce al alumno los diferentes componentes hardware que interactúan en un sistema informático actual. Sobre esa base se practicarán los conceptos generales de los diferentes sistemas operativos con los que se operará durante el curso.

De esta forma, el alumno tendrá una primera aproximación a la virtualización y se profundizará en la gestión de sistemas operativos (Linux)

Módulo 2 - Fundamentos de programación

Objetivo

En este módulo se definen los fundamentos del lenguaje de programación Python, ampliamente utilizado en ciberseguridad como lenguaje de scripting y de desarrollo de exploits.

Adicionalmente, este módulo tiene el objetivo de que el alumno interiorice la sintaxis común con otros lenguajes de programación, y desarrolle la capacidad de entender bloques de código independientemente del lenguaje utilizado.

Módulo 3 - Fundamentos de redes

Objetivo

En este módulo se definen los fundamentos de las redes de comunicación en las que se basan los sistemas informáticos en la actualidad. Para ello se realiza un enfoque descendente que permita conocer a bajo nivel la implementación y el funcionamiento de las comunicaciones del día a día.

Módulo 4 - Fundamentos de criptografía

Objetivo

El aspecto principal en el que se basa la ciberseguridad es la protección de la información. Para ello, es importante no sólo garantizar su confidencialidad, sino que en función de la clasificación de la información las compañías necesitarán también garantizar otros aspectos como la integridad y disponibilidad.

Este módulo engloba los fundamentos en los que se basa la criptografía, los diferentes tipos y su despliegue e implementación en los diferentes procesos de ciberseguridad.

Módulo 5 - Iniciación a la seguridad informática

Objetivo

Este módulo sirve de antesala al comienzo del core del bootcamp y define los conceptos básicos desde el punto de vista organizativo y metodológico de los ejercicios de Red Team / Blue Team realizados por las organizaciones.

Descripción del contenido en general:

Los contenidos de esta microcredencial son los siguientes:

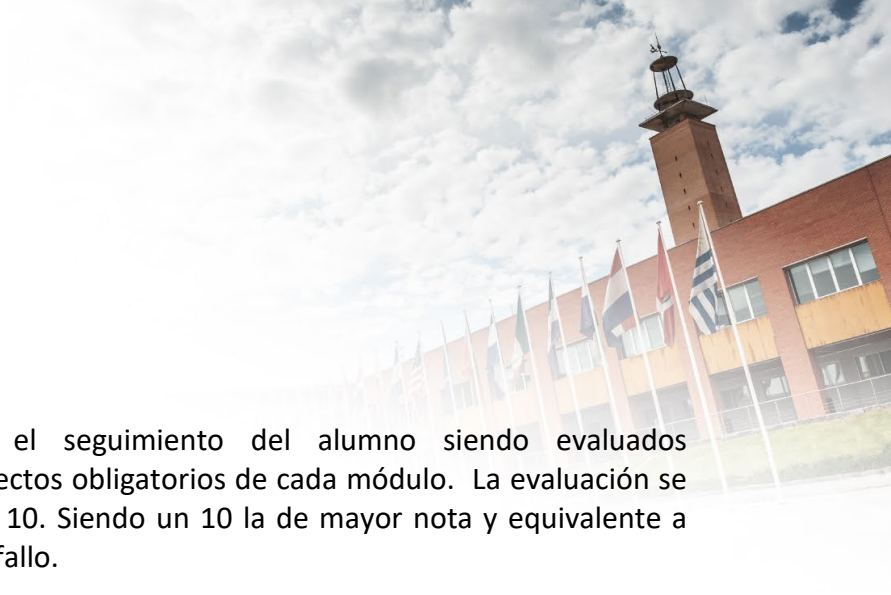
1. Componentes básicos de un ordenador
2. Redes: Modelo OSI, TCP / IP, Protocolos: DNS, SMTP, HTTP, HTTPS, SMB, ICMP, etc.
3. Conocimientos de Sistemas Operativos: Sistema operativo Windows, Sistema operativo Linux
4. Conocimientos de programación: Python, Powershell, Bash, PHP, Ruby
5. Conocimientos básicos de seguridad informática: Amenazas, Ataques, Vulnerabilidades, Cifrado, Métricas de medición del riesgo, Auditorías de seguridad: Definición y tipos, Red Team vs Pentest, Red Team vs Blue Team
6. Metodologías de ataque: MITRE, CAT, Diamond, Kill Chain
7. Fases de ataque en ejercicios de Red Team
8. Funciones de un equipo Blue Team
9. Roles en equipos de CiberSeguridad

4. Perfil del alumnado

Alumnos con orientación a la parte de nuevas tecnologías, con interés en la parte de ciberseguridad. Requisitos mínimos formativos Bachillerato.

5. Sistema de evaluación

Durante las dos primeras semanas el estudiante aprenderá y consolida los conceptos básicos y herramientas clave para que obtenga el nivel suficiente para afrontar las siguientes fases del bootcamp con éxito.



Los ejercicios se revisarán para el seguimiento del alumno siendo evaluados numéricamente únicamente los proyectos obligatorios de cada módulo. La evaluación se realizará de forma numérica del 0 al 10. Siendo un 10 la de mayor nota y equivalente a haber resuelto el ejercicio sin ningún fallo.

Evaluación de la calidad:

La Fundación Universidad Pablo de Olavide realizará la evaluación de la calidad de la formación a través de un cuestionario de satisfacción dirigido a estudiantes y docentes.

Esta evaluación consistirá, por un lado, en un cuestionario de satisfacción en el que las/los estudiantes evaluarán la gestión realizada por la organización, la información recibida antes y durante la formación, los recursos audiovisuales y de docencia, la duración y calidad de la jornada y la valoración general de la gestión.

Del mismo modo se evaluarán los contenidos de la acción formativa, el programa y su cumplimiento, el interés y profundización de los temas tratados y la calidad de las/los docentes. Por otro lado, se realizará la evaluación de la satisfacción de las/los docentes, valorando el servicio prestado por la organización antes y durante la acción formativa, las infraestructuras y plataforma de enseñanza online, los medios técnicos y audiovisuales y la gestión en general.

Todas estas consideraciones, junto a las sugerencias aportadas por estudiantes y docentes, serán remitidas al equipo de coordinación de los Cursos de Desarrollo Profesional Avanzado con el objeto de mejorar todos los puntos críticos en futuras ediciones y alcanzar la calidad deseada mediante los procesos de mejora continua.

6. Calendario de la microcredencial

Esta acción formativa arranca el 19 de febrero de 2024 y finaliza el 21 de marzo. El calendario de esta microcredencial es el que se muestra a continuación:

feb-24						
Lu	Ma	Mi	Ju	Vi	Sa	Do
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29			

marzo 2024						
Lu	Ma	Mi	Ju	Vi	Sa	Do
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21*	22	23	24
25	26	27	28	29	30	31

7. Link a la página de la microcredencial

A través de este enlace puede acceder al resto de información del curso, así como proceder a la matriculación o enviar una consulta sobre el mismo:

https://www.upo.es/formacionpermanente/microcredenciales/ciber-security-foundations/

8. Entidades colaboradoras

THE BRIDGE